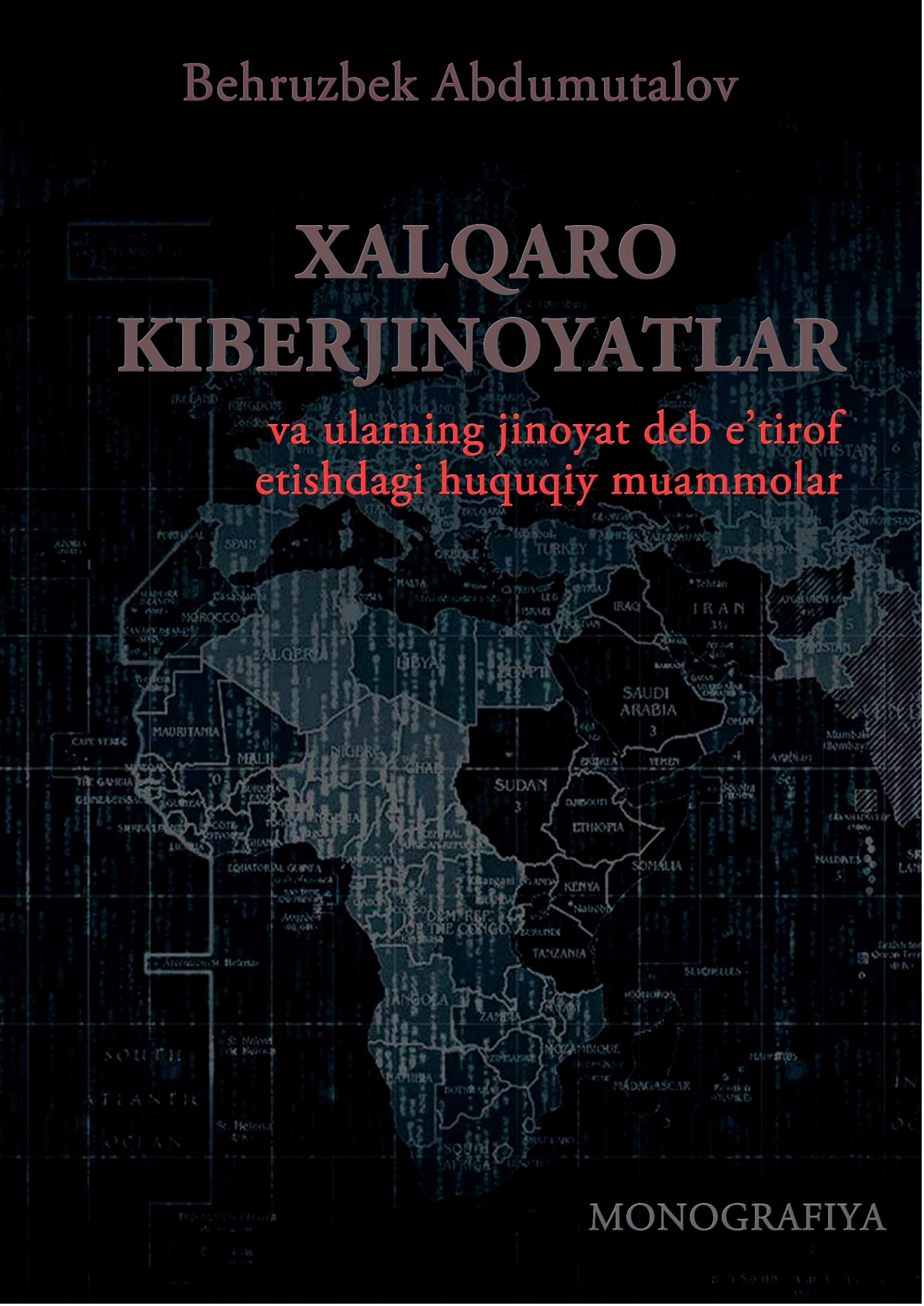
Behruzbek Abdumutalov

XALQARO KIBERJINOYATLAR

va ularning jinoyat deb e'tirof etishdagi huquqiy muammolar



MONOGRAFIYA

O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSYALAR VAZIRLIGI

Abdumutalov Behruzbek Ma’rufjonovich

XALQARO KIBERJINOYATLAR VA ULARNI JINOYAT DEB E’TIROF ETISHDAGI HUQUQIY MUAMMOLAR

(MONOGRAFIYA)

«Al-Bilol» nashriyoti – 2025

UDK 343.9:004.42

B.M.Abdumutalov. Xalqaro kiberjinoyatlar va ularni jinoyat deb e’tirof etishdagi huquqiy muammolar. [monografiya] – «Al-Bilol» nashriyoti. Toshkent – 2025. – 173 b.

Mas’ul muharrir:
Ijtimoiy falsafa ixtisosligi bo‘yicha falsafa doktori (PhD
Karimov Elmurod Salimjonovich

Pedagogika fanlari bo‘yicha falsafa doktori (PhD), dotsent
Mohigul Shaniyazovna Qurbonova

Taqrizchilar:
Pedagogika fanlari doktori (DSc), professor
Qurbonniyoz Berdiyevich Panjiyev

Ijtimoiy falsafa ixtisosligi bo‘yicha falsafa doktori (PhD
Karimov Elmurod Salimjonovich

Ushbu monografiya "Xalqaro kiberjinoyatlar va ularni jinoyat deb e’tirof etishdagi huquqiy muammolar" mavzusiga bag‘ishlangan bo‘lib, kiberjinoyatlar va ularning global miqyosda huquqiy e’tirof etilishi, xalqaro hamkorlik va qonuniy tartibga solish masalalarini chuqur tahlil qiladi. Monografiyada kiberjinoyatlarining rivojlanish tarixi, ularning turli shakllari, zamonaviy tahdidlar va jinoyat sifatida e’tirof etilishidagi muammolar keng yoritilgan. Ayniqsa, kiberjinoyatlarni aniqlash, ularni tergov qilish, dalillarni to‘plash va xalqaro huquq nuqtai nazaridan ularni jinoyat sifatida tan olish borasida yuzaga keladigan muammolarni ilmiy tarzda tahlil etish maqsad qilingan.

Monografiya huquqshunoslar, siyosatchilar, xalqaro tashkilotlar vakillari, kiberxavfsizlik mutaxassislari, yuridik va texnologik ilmiy tadqiqotlar sohasidagi tadqiqotchilar hamda davlat organlari uchun muhim manba bo‘lib xizmat qilishi mumkin. Ushbu ilmiy ish nafaqat kiberjinoyatlarning huquqiy muammolarini, balki ularning xalqaro miqyosda qanday hal etilishini, yuridik muammolarni samarali tarzda hal qilishni o‘rganishda foydalidir. Bundan tashqari, monografiya umumiy kiberxavfsizlik strategiyalarini ishlab chiqish, xalqaro huquqning kiberjinoyatlarga ta’sirini o‘rganish, va zamonaviy texnologiyalar orqali huquqiy tartibga solishni rivojlantirish maqsadida foydalanish mumkin.

Monografiya so‘nggi yillarda kiberjinoyatlarni jinoyat sifatida tan olish va ularni xalqaro darajada tartibga solish bo‘yicha mavjud bo‘lgan bo‘shliqlarni aniqlash, yangi huquqiy yondashuvlar va takliflarni ilgari surish, kiberjinoyatlarga qarshi kurashishda samarali strategiyalarni ishlab chiqishga qaratilgan.

So‘z boshi

Bugungi kunda, raqamli texnologiyalar va internet tarmog‘ining jadal rivojlanishi bilan birga, kiberjinoyatlar ham global miqyosda keng tarqalmoqda. Kiberjinoyatlar faqatgina huquqiy, balki iqtisodiy va ijtimoiy sohalarda ham katta tahdidlarga sabab bo‘lmoqda. Ularning murakkab va transmilliy xususiyatlari, shuningdek, huquqiy tartibga solishning cheklanganligi, xalqaro miqyosda samarali kurashish zaruratini tug‘diradi. Bu esa, o‘z navbatida, kiberjinoyatlarni jinoyat sifatida tan olish va ularga qarshi kurashishda yangi yondashuvlar, normativ va texnologik yechimlarni ishlab chiqishni talab etadi.

Ushbu monografiya, kiberjinoyatlar sohasidagi huquqiy muammolarni o‘rganishga va ularni xalqaro darajada samarali tarzda hal qilish uchun zarur bo‘lgan qonuniy, texnik va metodologik yondashuvlarni ishlab chiqishga qaratilgan. Asarda, kiberjinoyatlarning global miqyosdagi ta’siri, xalqaro huquq va milliy qonunlar o‘rtasidagi uyg‘unlik, shuningdek, bu jinoyatlarga qarshi kurashishda xalqaro hamkorlikning muhimligi tahlil etiladi. Monografiya, shuningdek, kiberjinoyatlarga qarshi kurashishning huquqiy jihatlariga oid ilg‘or tajribalar va takliflarni o‘z ichiga oladi, bu esa ilgari surilgan masalalarga ilmiy asoslangan yangi yondashuvlarni taqdim etadi.

Kiberjinoyatlarni huquqiy jihatdan tan olish va ular bilan kurashishda yuzaga keladigan muammolarni hal qilish bugungi kunda faqatgina yuridik sohadagi mutaxassislar uchun emas, balki davlat organlari, xalqaro tashkilotlar, texnologik kompaniyalar va keng jamoatchilik uchun ham dolzarbdir. Ushbu monografiyada taklif etilgan yondashuvlar va tahlillar, kiberjinoyatlar bilan kurashish bo‘yicha xalqaro va milliy qonunlar va amaliyotdagi bo‘shliqlarni aniqlashga, shuningdek, bu bo‘yicha samarali strategiyalarni ishlab chiqishga xizmat qiladi.

Ushbu tadqiqot ishini yozish jarayonida men kiberjinoyatlar sohasidagi jiddiy huquqiy masalalarni o‘rganish va bu muammolarni hal qilish uchun ilmiy yondashuvlarni ishlab chiqishga harakat qildim. Kiberjinoyatlar va ularga qarshi kurashish bo‘yicha ushbu monografiya, barcha huquqshunoslar, siyosatchilar, davlat va xususiy sektor vakillari uchun foydali manba bo‘lishi va kiberjinoyatlarga qarshi kurashishda samarali yechimlarni yaratishda xizmat qilishi mumkin.

Muallifdan

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi zamonaviy jamiyat hayotining deyarli barcha jabhalariga chuqur kirib bordi. Bugungi kunda insoniyat taraqqiyotining ajralmas qismi sifatida internet, sun'iy intellekt, "bulutli" texnologiyalar va raqamli platformalar millionlab odamlarning kundalik faoliyatida asosiy vositaga aylangan. Shu bilan birga, texnologik taraqqiyot nafaqat ijtimoiy va iqtisodiy yuksalish imkoniyatlarini kengaytirdi, balki yangi turdagi tahdidlarni ham yuzaga keltirdi. Aynan shu jihat, ya'ni axborot makonidagi jinoyatchilik — ya'ni kiberjinoyatlar — global xavfsizlikning asosiy muammolaridan biriga aylanganini koʻrsatmoqda.

Kiberjinoyatlar transmilliy xarakterga ega boʻlib, ularning sodir etilishi zamonaviy jinoiy guruhlarning milliy chegaralarga tobe boʻlmagan, murakkab, koʻp bosqichli faoliyatini ifodalaydi. Bu esa, oʻz navbatida, kiberjinoyatlarga qarshi kurashda xalqaro hamkorlik, umumiy yondashuv va yagona huquqiy mezonlarni ishlab chiqishni talab etadi. Ammo hozirgi paytda xalqaro huquq sohasida bu boradagi normativ bazaning yetarlicha aniqlashtirilmagani, kiberjinoyatlarning aniqlanishi, tasnifi va jinoyat deb e'tirof etilishi masalalaridagi tafovutlar jiddiy muammolarni keltirib chiqarmoqda.

Mazkur monografiya ana shu muhim va dolzarb masalalarga bagʻishlangan boʻlib, kiberjinoyatlarning huquqiy mohiyatini ochib berish, ularning xalqaro miqyosda jinoyat deb e'tirof etilishida uchrayotgan huquqiy boʻshliqlar va qarama-qarshiliklarni tahlil qilishga intiladi. Asarda xalqaro huquq me'yorlari, xorijiy davlatlar tajribasi, xalqaro shartnomalar va konvensiyalar asosida tahliliy yondashuv qoʻllanilgan boʻlib, mavjud muammolarni aniqlash va ularni bartaraf etish yoʻllari taklif qilinadi.

Shuningdek, monografiyada raqamli makonda jinoyatchilikka qarshi kurashishning samarali usullarini shakllantirishda xalqaro institutlar, davlatlar oʻrtasidagi axborot almashinuvi, yurisdiktsiya masalalari, ekstraditsiya amaliyoti va suverenitet masalalarining oʻzaro uygʻunligi yoritilgan. Bu yoʻnalishdagi tadqiqotlar nafaqat nazariy, balki amaliy jihatdan ham muhim ahamiyatga ega boʻlib, huquqshunos olimlar, siyosatchilar, huquqni muhofaza qiluvchi organlar va xalqaro tashkilotlar uchun muhim manba boʻlib xizmat qiladi.

Monografiyaning maqsadi — xalqaro kiberjinoyatlarni aniqlash, ularni huquqiy jihatdan toʻgʻri tasniflash va ularga qarshi kurashishda yagona va

samarali huquqiy mexanizmlarni shakllantirish zaruratini asoslashdir. Shu asosda, ushbu asar kiberjinoyatlarga qarshi xalqaro kurash tizimini takomillashtirish, jinoyatlarni oldini olish va jinoyatchilarni javobgarlikka tortishda huquqiy asoslarni mustahkamlashga qaratilgan izlanishlarning bir bo‘lagi sifatida qaraladi.

Kiberjinoyatlarning global miqyosda ortib borayotgan xavfi va dolzarbligi. So‘nggi yillarda insoniyat raqamli transformatsiya bosqichiga keskin qadam tashladi. Axborot-kommunikatsiya texnologiyalari (AKT) hayotimizning barcha sohalariga kirib kelgani sababli, nafaqat ijtimoiy-iqtisodiy yutuqlar, balki yangi turdagi xavf-xatarlar ham yuzaga kelmoqda. Aynan shunday xavflarning eng jiddiylaridan biri bu — **kiberjinoyatlar** bo‘lib, ular global xavfsizlik, iqtisodiy barqarorlik va shaxsiy erkinlikka tahdid solmoqda.

Kiberjinoyatlar sonining o‘sishi va ularning murakkablashuvi. Global miqyosda statistik tahlillar shuni ko‘rsatadiki, har yili millionlab kiberhujumlar sodir etilmoqda. Xalqaro kiberxavfsizlik tashkilotlari, xususan Interpol, Europol va ITU (International Telecommunication Union) ma’lumotlariga ko‘ra, 2020–2024 yillar oralig‘ida kiberjinoyatlarning soni yiliga o‘rtacha 15–20% ga oshgan. Ayniqsa, **ransomware (fidyaga olinadigan dasturiy viruslar)**, **phishing (yolg‘on axborot orqali ma’lumotlarni qo‘lga kiritish)** va **DDoS hujumlar** eng keng tarqalgan va zararli shakllari sifatida qayd etilgan.

Kiberjinoyatlarning xavfini yanada kuchaytiradigan jihat — ularning tobora murakkablashuvi va ixtisoslashib borayotganidir. Endilikda, kiberjinoyatchilar oddiy firibgarlardan tortib to yaxshi moliyalashtirilgan, texnik jihatdan kuchli jinoiy guruhlargacha bo‘lgan keng ko‘lamli tuzilmalarni tashkil etishmoqda. Ularda sun’iy intellekt, “dark web”, kriptovalyutalar va boshqa zamonaviy vositalardan foydalanish hollari ortib bormoqda.

Kiberjinoyatlarning iqtisodiy va siyosiy xavflari. Kiberjinoyatlar global iqtisodiyotga katta zarar yetkazmoqda. Masalan, Cybersecurity Ventures tadqiqotiga ko‘ra, dunyo bo‘yicha kiberjinoyatlar tufayli 2025-yilga borib korporativ va davlat sektoriga yetkaziladigan yillik zarar **10,5 trillion AQSH dollari** atrofida bo‘lishi kutilmoqda. Bunday tahdidlar nafaqat tijorat va moliya sohalariga, balki infratuzilma, energetika, sog‘liqni saqlash va mudofaa tizimlariga ham jiddiy ta’sir ko‘rsatmoqda.

Bundan tashqari, kiberjinoyatlar koʻplab siyosiy inqirozlar va gibrid urushlar vositasi sifatida ham foydalanilmoqda. Kiberhujumlar orqali saylov tizimlariga aralashish, davlat organlarining maxfiy ma’lumotlarini egallash, ijtimoiy tarmoqlar orqali dezinformatsiyalar tarqatish bugungi kunda global geosiyosiy muvozanatga tahdid solmoqda.

Xavfning transmilliy xarakteri va huquqiy javobgarlikdagi murakkabliklar. Kiberjinoyatlarning eng asosiy xususiyatlaridan biri — ularning **transmilliy** (chegaradan tashqari) xarakterga egaligidir. Jinoyat bir davlat hududida sodir etilishi, ammo uning qurbonlari boshqa davlatda boʻlishi mumkin. Natijada, jinoyatni aniqlash, aybdorni qoʻlga olish va sudga tortish masalalari jiddiy huquqiy toʻsiqlarga duch keladi.

Aksariyat hollarda turli mamlakatlar oʻrtasida **yagona huquqiy ta’riflar, yurisdiktsiya normalari va hamkorlik mexanizmlarining yoʻqligi** sababli kiberjinoyatchilar javobgarlikdan chetda qolmoqda. Shuningdek, koʻplab davlatlarda bu boradagi qonunchilik bazasi eskirgan, kiberjinoyatlarni jinoyat deb tan olishdagi yondashuvlar esa bir-biridan keskin farq qiladi.

Dolzarblik: global hamkorlik va huquqiy moslashuv zarurati. Yuqoridagi holatlar shuni koʻrsatadiki, kiberjinoyatlarga qarshi kurashishda **xalqaro huquqiy mexanizmlarni takomillashtirish**, **yagona ta’rif va mezonlarni belgilash**, hamda davlatlar oʻrtasidagi **axborot almashinuvi va jinoyatchilarni ekstraditsiya qilish tizimini soddalashtirish** nihoyatda dolzarb masalaga aylanmoqda.

Masalan, Budapesht Konvensiyasi (2001) kiberjinoyatlarga qarshi xalqaro huquqiy asoslarni yaratishda muhim qadam boʻlgan boʻlsa-da, uni barcha davlatlar ratifikatsiya qilmagan. Shu sababli, kelajakda keng qamrovli va yangilangan xalqaro huquqiy hujjatlarni ishlab chiqish, milliy qonunchilikni global standartlarga moslashtirish muhim ahamiyat kasb etadi.

Monografiya maqsadi, tadqiqot obyekti va metodologiyasi. Ushbu monografiyaning asosiy maqsadi — xalqaro miqyosda kiberjinoyatlar tushunchasi va ularni jinoyat deb e’tirof etishdagi huquqiy asoslarni chuqur tahlil qilish, bu sohada mavjud boʻlgan normativ-huquqiy tafovutlar, amaliy muammolar va qarama-qarshiliklarni aniqlash, shuningdek, bu muammolarni bartaraf etish boʻyicha ilmiy asoslangan taklif va tavsiyalar ishlab chiqishdan iborat.

Shu bilan birga, monografiyada kiberjinoyatlarning xalqaro huquqiy jihatdan tan olinishi, ularni jinoyat sifatida malakalashda mamlakatlar

o‘rtasida mavjud tafovutlar, xalqaro konvensiyalarning ahamiyati va yetarli darajada universal bo‘lmaganligi, shuningdek yurisdiktsiya, ekstraditsiya va transmilliy hamkorlikdagi huquqiy to‘siqlar atroflicha yoritiladi.

Mazkur asar amaldagi xalqaro huquqiy hujjatlar, sud amaliyoti, xalqaro tashkilotlarning tavsiyalari va zamonaviy global xavf-xatarlar tahlili asosida ishlab chiqilgan bo‘lib, u ilg‘or huquqiy yondashuvlarni aniqlash va kiberjinoyatlarga qarshi kurashishning samarali huquqiy modelini ishlab chiqishga xizmat qiladi.

Tadqiqot obyekti. Monografiyaning tadqiqot obyekti sifatida **kiberjinoyatlar va ularning xalqaro huquqda jinoyat sifatida e’tirof etilishi bilan bog‘liq munosabatlar tizimi** tanlangan. Bu munosabatlar quyidagilarni o‘z ichiga oladi:

- ✓ Xalqaro va transmilliy kiberjinoyatlarning turlari va ularning huquqiy xususiyatlari;
- ✓ Kiberjinoyatlarni jinoyat deb tan olishdagi xalqaro normativ-huquqiy hujjatlar (Budapesht Konvensiyasi, Afrika Ittifoqining Malabo Konvensiyasi, ASEAN, Yevroittifoq va boshqa mintaqaviy bitimlar);
- ✓ Xalqaro va milliy huquqning o‘zaro muvofiqligi (yoki muvofiqlik yetishmovchiligi);
- ✓ Kiberjinoyatlarda yurisdiktsiya qo‘llash va jinoyatchilarni javobgarlikka tortishdagi amaliy huquqiy to‘siqlar;
- ✓ Xalqaro hamkorlik, ekstraditsiya va axborot almashinuvi tizimlari.

Tadqiqot doirasida nafaqat xalqaro huquq me’yorlari, balki ayrim rivojlangan va rivojlanayotgan mamlakatlarning milliy qonunchiligi, sud-huquq amaliyoti ham tahlil qilinadi. Bu yondashuv global standartlar va milliy tizimlar o‘rtasidagi nomuvofiqliklarni ko‘rsatishga xizmat qiladi.

Tadqiqot metodologiyasi. Tadqiqotda qo‘llanilgan metodologik asoslar ilmiy obyektivlik, tizimlilik, tarixiylik va taqqoslash prinsiplariga tayanadi. Quyidagi ilmiy metodlar qo‘llanilgan:

- ➢ **Tahliliy-metodik yondashuv** — mavjud xalqaro huquqiy hujjatlar va ularning amaliy tatbiqini tahlil qilish orqali kiberjinoyatlarni jinoyat sifatida e’tirof etishdagi ziddiyatlarni aniqlash;
- ➢ **Taqqoslash huquqshunosligi (komparativistika)** — turli mamlakatlar qonunchiligi, amaliyoti va xalqaro konvensiyalar o‘rtasidagi farq va o‘xshashliklarni aniqlash va baholash;

- **Solishtirma tarixiy metod** — kiberjinoyatga oid huquqiy yondashuvlarning shakllanishi va evolyutsiyasini tarixiy nuqtai nazardan o‘rganish;
- **Normativ tahlil** — xalqaro shartnomalar, konvensiyalar, deklaratsiyalar va rezolyutsiyalar matnining mazmunan tahlili orqali ularning huquqiy kuchi va samaradorligini aniqlash;
- **Pragmatik yondashuv** — xalqaro tashkilotlar va milliy davlatlar darajasidagi amaliy harakatlarni tahlil qilish orqali real takliflar ishlab chiqish.

Bundan tashqari, monografiyada **empirik ma’lumotlar** — xalqaro statistika, ekspert tahlillari, xalqaro sudlarning qarorlari, xalqaro konferensiya va forumlarda bildirilgan fikrlar asosida dalillarga boy yondashuv qo‘llanilgan.

Ilmiy yangilik, nazariy va amaliy ahamiyat. Mazkur monografiyada kiberjinoyatlar muammosi xalqaro huquqiy kontekstda o‘rganilishi, ularni jinoyat deb e’tirof etishdagi normativ tafovutlar va mintaqaviy yondashuvlar chuqur tahlil qilinishi bilan ajralib turadi. Asarning ilmiy yangiligi quyidagi jihatlarda namoyon bo‘ladi:

- **Kiberjinoyatlarni xalqaro jinoyat sifatida e’tirof etishdagi yondashuvlarning tizimli tahlili** amalga oshirilgan. Xususan, xalqaro konvensiyalar, mintaqaviy bitimlar va ayrim mamlakatlarning milliy qonunchiligi o‘rtasidagi huquqiy tafovutlar aniqlanib, ularning zamiridagi asosiy sabablarga ilmiy asosda izoh berilgan.
- **Yangi takliflar ishlab chiqilgan**, ya’ni monografiyada xalqaro darajada umumiy, universal va majburiy bo‘lgan kiberjinoyatlarga oid huquqiy definitsiyalar, tasniflash mezonlari, yurisdiktsiya doiralari va huquqiy javobgarlik mexanizmlarini shakllantirish zarurati asoslab berilgan.
- **Kiberjinoyatlarning transmilliy tabiati va ularni jinoyat deb tan olishdagi normativ-huquqiy ziddiyatlarning huquqiy-falsafiy tahlili** berilgan. Ayniqsa, davlat suvereniteti, yurisdiktsiya va kiberxavfsizlik o‘rtasidagi nozik muvozanat ilmiy yondashuv asosida baholangan.
- Ilgari nisbatan kam o‘rganilgan mavzular — **kiberjinoyatlar bilan bog‘liq ekstraditsiya amaliyoti, xalqaro huquq subyektlarining o‘zaro axborot almashinuvi mexanizmlari, kiberfazoda inson huquqlari bilan bog‘liq kolliziyalar** alohida o‘rganilgan.

Bu yondashuvlar natijasida mazkur monografiya nafaqat mavjud nazariy qarashlarni boyitadi, balki yangi ilmiy munozaralar uchun asos yaratadi.

Nazariy ahamiyat. Monografiya kiberjinoyatlarni xalqaro huquqiy sistemaga integratsiya qilish, ularni jinoyat deb tan olish mezonlarini aniqlash, va shu orqali huquqiy ta’rif va yondashuvlarni uyg‘unlashtirishga qaratilgan nazariy asoslarni shakllantiradi. Uning nazariy ahamiyati quyidagilarda namoyon bo‘ladi:

- **Xalqaro jinoyat huquqining zamonaviy rivojlanish tendensiyalariga mos holda** kiberjinoyatlarga oid normativ-huquqiy yondashuvlar tizimlashtirilgan;
- **Kiberjinoyatlar va xalqaro xavfsizlik** o‘rtasidagi huquqiy munosabatlar chuqur o‘rganilib, ularning xalqaro tinchlik va barqarorlikka ta’siri tahlil qilingan;
- **Kiberjinoyatlarga qarshi kurashishdagi universal huquqiy mezonlarning shakllanishiga zarurat** nazariy jihatdan asoslab berilgan;
- Monografiya **huquqshunos olimlar, magistrantlar, doktorantlar va ilmiy tadqiqotchilar** uchun metodologik va kontseptual asos bo‘lib xizmat qiladi, ayniqsa xalqaro jinoyat huquqi va kiberhuquq sohasi bo‘yicha izlanish olib boruvchilar uchun muhim manbadir.

Amaliy ahamiyat. Ushbu monografiya nafaqat nazariy, balki **amaliy jihatdan ham yuqori dolzarblik** kasb etadi. Uning natijalari quyidagi yo‘nalishlarda qo‘llanilishi mumkin:

- **Qonunchilikka oid takliflar ishlab chiqishda**, ya’ni kiberjinoyatlarni jinoyat deb e’tirof etishning huquqiy asoslarini mustahkamlash uchun milliy qonunchilikni xalqaro standartlarga moslashtirishda foydali bo‘lishi mumkin;
- **Davlatlararo hamkorlikni kuchaytirishda**, ayniqsa xalqaro shartnomalar, ikki tomonlama ekstraditsiya bitimlari, axborot almashinuvi va yurisdiktsiya doiralarini aniqlashda huquqiy asos sifatida xizmat qiladi;
- **Huquqni muhofaza qiluvchi organlar faoliyatida** – xalqaro kiberjinoyatchilikka qarshi kurashayotgan organlar, ayniqsa sudlar, prokuratura va tergov idoralari uchun amaliy ko‘rsatmalar, modellar va yondashuvlar sifatida qo‘llanishi mumkin;
- **Kiberxavfsizlik strategiyalarini ishlab chiqishda** – davlatlar, xalqaro tashkilotlar yoki yirik kompaniyalar tomonidan xavfsizlik siyosatini ishlab chiqish va himoya mexanizmlarini shakllantirishda monografiyada bayon etilgan huquqiy risklar va yondashuvlardan foydalanish mumkin.

Shuningdek, monografiya mazmuni tegishli oliy ta’lim muassasalarining “Xalqaro huquq”, “Axborot xavfsizligi huquqi”, “Jinoyat huquqi” va “Kiberhuquq” kabi fanlar doirasida o‘quv qo‘llanmasi sifatida ham foydalanishga mos keladi.

I BOB. KIBERJINOYATLARNING MOHIYATI VA XALQARO TASNIFI

Zamonaviy raqamli inqilob insoniyat taraqqiyotining barcha jabhalariga chuqur kirib bordi. Internet texnologiyalarining jadal rivojlanishi, global tarmoq tizimlarining integratsiyalashuvi, “raqamli iqtisodiyot” va “raqamli suverenitet” kabi yangi tushunchalarning paydo bo‘lishi nafaqat ijtimoiy-iqtisodiy jarayonlarga, balki huquqiy munosabatlarga ham tubdan ta’sir ko‘rsatmoqda. Shu bilan birga, raqamli makonda sodir etilayotgan jinoyatlar — ya’ni **kiberjinoyatlar** — xalqaro hamjamiyat uchun dolzarb xavf-xatar manbai sifatida e’tirof etilmoqda. Kiberjinoyatlar o‘zining transmilliy tabiati, yuqori texnologik murakkabligi va tezkor rivojlanish xususiyatlari bilan boshqa an’anaviy jinoyatlardan tubdan farq qiladi.

Kiberjinoyatlar, keng ma’noda, axborot-kommunikatsiya texnologiyalari (AKT) vositasida yoki shu vositalarga qarshi sodir etiladigan noqonuniy harakatlarni o‘z ichiga oladi. Bunday jinoyatlar jumlasiga kompyuter tizimlariga noqonuniy kirish, zararli dasturlar orqali tizimlarni ishdan chiqarish, shaxsiy ma’lumotlarni o‘g‘irlash, raqamli firibgarlik, kiberterrorizm va boshqa ko‘plab huquqbuzarliklar kiradi. Ularning global miqyosdagi o‘sishi, transchegaraviy tarqalish imkoniyati va turli huquqiy tizimlarga sig‘maydigan shakllari xalqaro huquq uchun jiddiy muammolarni yuzaga keltirmoqda.

Shu bois kiberjinoyatlarning **huquqiy mohiyatini aniqlash**, **ularni xalqaro miqyosda tasniflash**, hamda **jinoyat deb e’tirof etish mezonlarini ishlab chiqish** xalqaro huquqiy hamjamiyatning ustuvor vazifasiga aylanmoqda. Zero, ayni paytda kiberjinoyatlar yagona universal huquqiy ta’rifga ega emas, ularni malakalashda turli mamlakatlar va xalqaro tashkilotlar o‘rtasida sezilarli tafovutlar mavjud. Masalan, Yevropa Kengashining **Budapesht Konvensiyasi** (2001) kiberjinoyatga oid birinchi xalqaro huquqiy hujjat sifatida e’tirof etiladi, biroq u ham barcha davlatlar tomonidan universal qabul qilingan emas.

Bundan tashqari, xalqaro huquqda kiberjinoyatlarni **jinoyat kategoriyasi**ga kiritish bo‘yicha o‘ziga xos yondashuvlar mavjud bo‘lib, ular kiberjinoyatlarning qaysi turlari xalqaro xavf darajasiga ega ekanligini, qaysi holatlarda universal yurisdiktsiya qo‘llanishi mumkinligini aniqlashda muhim ahamiyat kasb etadi. Aynan shu muammolarni hal qilish uchun kiberjinoyatlarni huquqiy jihatdan chuqur anglash va ularning tasnifini aniqlash masalasi dolzarb bo‘lib qolmoqda.

Mazkur bobda, avvalo, kiberjinoyat tushunchasi va uning huquqiy tabiatiga izoh beriladi. Shuningdek, xalqaro va mintaqaviy tashkilotlar tomonidan taklif etilgan kiberjinoyat tasniflari tahlil qilinib, ularning ustun va zaif tomonlari baholanadi. Bob yakunida esa xalqaro huquqiy hujjatlar asosida **kiberjinoyatlarning turkumlanishi** va ularni **jinoyat sifatida malakalash mezonlari** ishlab chiqiladi. Bu, o‘z navbatida, keyingi boblarda kiberjinoyatlarni jinoyat deb e’tirof etishdagi huquqiy muammolarni tahlil qilish uchun nazariy asos bo‘lib xizmat qiladi.

Axborot texnologiyalarining rivojlanishi va jinoyatchilikdagi yangi shakllar. XXI asrda axborot-kommunikatsiya texnologiyalari (AKT) misli ko‘rilmagan sur’atlar bilan rivojlanib, insoniyat faoliyatining barcha sohalariga tubdan o‘zgarishlar olib kirdi. Internet texnologiyalarining keng tarqalishi, sun’iy intellekt, bulutli texnologiyalar, IoT (Internet of Things), katta hajmdagi ma’lumotlar (Big Data) va blokcheyn kabi innovatsiyalar orqali jamiyatda yangi imkoniyatlar yaratilgan bo‘lsa-da, shu bilan birga, yangi xavf-xatar va jinoyatchilik shakllarining paydo bo‘lishiga ham zamin hozirlandi. Endilikda jinoyatlar nafaqat an’anaviy jismoniy makonda, balki raqamli fazoda ham sodir etilmoqda.

1.1. Kiberjinoyat tushunchasining shakllanishi va rivojlanishi

Kiberjinoyatlar - bu axborot texnologiyalari va raqamli tizimlardan foydalanish orqali amalga oshiriladigan jinoyatlar bo‘lib, ular XXI asrda yuzaga kelgan eng yangi va dolzarb huquqiy masalalardan biridir. Kiberjinoyatlarning mohiyati, tuzilishi va shakllanishi bilan bog‘liq ko‘plab o‘zgarishlar, raqamli texnologiyalar va internetning rivojlanishi bilan bevosita bog‘liqdir. Ushbu jinoyatlar an’anaviy jinoyat turlaridan ajralib turadi, chunki ular ko‘pincha virtual muhitda sodir bo‘ladi va ularni amalga oshirishda maxsus bilimlar va texnologik vositalar zarur bo‘ladi. Shu sababli,

kiberjinoyatlar tushunchasining shakllanishi ham vaqt o‘tishi bilan o‘zgarib, yuksalib borgan.

Kiberjinoyat tushunchasining rivojlanishi, asosan, axborot texnologiyalarining tezkor taraqqiyoti, internet tarmog‘ining keng tarqalishi va global digitalizatsiya jarayonlari bilan bog‘liqdir. Birinchi navbatda, kiberjinoyatlar sohasida mavjud bo‘lgan tushunchalar turli xil huquqiy, ijtimoiy va texnologik omillar ta’sirida shakllandi. Bu jinoyatlar ko‘pincha shaxsiy ma’lumotlarni o‘g‘irlash, moliyaviy firibgarliklar, dasturiy ta’minotlarga zarar yetkazish, onlayn tahdidlar va axborot tizimlariga noqonuniy kirish kabi holatlar bilan ifodalanadi.

Ushbu bo‘limda kiberjinoyat tushunchasining shakllanish jarayoni va uning rivojlanish tarixiga to‘xtalib o‘tiladi. Dastlab, kiberjinoyatlarning yuridik jihatlari va global kontekstdagi ahamiyati, shuningdek, dunyo miqyosida kiberjinoyatlar bilan kurashishda qabul qilingan xalqaro yondashuvlar tahlil qilinadi. Bu jarayonda, kiberjinoyatlar tushunchasining o‘zgarishi, yuridik tizimlarda bu soha uchun yangi qonunlar va normalar yaratish zaruriyati ham muhokama qilinadi.

Kiberjinoyatlarning shakllanishi va rivojlanishi ko‘plab yuridik, texnik va siyosiy aspektlarni o‘z ichiga oladi, shuning uchun ularning tasnifini va huquqiy asoslarini to‘liq tushunish, bugungi kunda ilmiy tadqiqotlar va amaliy qonunlarni yaratishda zaruriy ahamiyatga ega. Shuningdek, kiberjinoyatlar global miqyosda keng tarqalganligi sababli, xalqaro huquq doirasida ham bu masalalar yechimini topish uchun hamkorlik va yangi yondashuvlar muhim rol o‘ynaydi.

Axborot texnologiyalari va jinoyat muhitining transformatsiyasi. Axborot texnologiyalarining jinoyat muhiti va jinoyatchilik dinamikasiga ta’siri ko‘p qirrali bo‘lib, u jinoyatlarni rejalashtirish, amalga oshirish, yashirish va jinoyat faoliyatidan olingan daromadlarni legallashtirish usullarini keskin o‘zgartirdi. Raqamli asrda jinoyatchilik “aqlli” va ko‘p hollarda davlat chegaralarini tan olmasdan harakat qiluvchi ko‘rinishlarga ega bo‘ldi.

Quyidagilar AKT asosida shakllanayotgan jinoyatchilikning yangi shakllari sifatida e’tirof etiladi:

- **Kiberhujumlar (cyberattacks)** — bu turdagi hujumlar kompyuter tizimlari, serverlar yoki tarmoqlarga noqonuniy kirish yoki ularni ishdan chiqarishga qaratilgan. DDoS hujumlar, viruslar, zararli dasturlar va

ransomware (ma’lumotlarni bloklab, tovlamachilik qilish) bunga misol bo‘la oladi.

- **Shaxsiy ma’lumotlar va maxfiy axborotni o‘g‘irlash** — bu sohada identifikatsiya ma’lumotlari (login, parol, bank kartalari ma’lumotlari) eng ko‘p nishonga olinadigan axborotlardir.
- **Ijtimoiy muhandislik (social engineering)** — bu usul orqali jinoyatchilar foydalanuvchilarning e’tiboridan foydalanib, ularni o‘z axborotlarini ixtiyoriy tarzda berishga undaydi. Masalan, fishing, vishing va spear phishing kabilar.
- **Virtual moliyaviy jinoyatlar** — kriptovalyutalardan noqonuniy foydalanish, moliyaviy firibgarlik, onlayn investitsiya sxemalari, NFT orqali pullarni legallashtirish.
- **Kiberterrorizm** — axborot infratuzilmasiga zarar yetkazish yoki jamiyatda vahima uyg‘otish maqsadida amalga oshiriladigan raqamli hujumlar.
- **Darknet va anonim platformalar orqali jinoyatlar** — giyohvand moddalar, qurol, odam savdosi, bolalar pornografiyasi va boshqa noqonuniy tovarlar bilan bog‘liq faoliyat asosan darknet orqali amalga oshiriladi.

Ilmiy va huquqiy jihatdan muammo: Yangi jinoyatlar – eski qonunlar. Axborot texnologiyalarining tezkor rivojlanishi huquqiy tizimlar uchun jiddiy chaqiriq bo‘lib qolmoqda. Ko‘plab davlatlarning milliy qonunchiligi yangi shakldagi jinoyatlarga mos ravishda modernizatsiya qilinmagan. Misol uchun:

- Ko‘plab mamlakatlarda **kiberjinoyatlar uchun alohida normativ-huquqiy asos** mavjud emas;
- Raqamli jinoyat vositalarini aniqlashda **ekspertiza va texnik imkoniyatlar yetarli emas**;
- Jinoyatchilar harakat qilayotgan virtual maydon **milliy yurisdiktsiyadan tashqarida** bo‘ladi, bu esa javobgarlikka tortishni qiyinlashtiradi;
- Transchegaraviy jinoyatlarda **xalqaro huquqiy hamkorlik mexanizmlari zaif** ishlaydi yoki mavjud emas.

Bundan tashqari, axborot texnologiyalariga asoslangan jinoyatlar ko‘p hollarda **sodda ko‘rinishda** sodir etiladi va ularni aniqlash va isbotlash murakkab jarayonni talab qiladi. Masalan, fishing orqali foydalanuvchining ma’lumotlarini olish — oddiy bir havola yuborish bilan sodir bo‘lishi mumkin,

ammo bu jinoyatning huquqiy isboti texnik izlar, log fayllar va ma’lumot oqimini to‘liq tahlil qilishni talab etadi.

Jinoyatchilikning evrilanishi va xalqaro tasnifga ehtiyoj. Axborot texnologiyalari asosida yuzaga kelayotgan jinoyatlarning shakli, uslubi va miqyosi ularni an’anaviy jinoyat huquqi doirasida baholashni murakkablashtiradi. Shu sababli, kiberjinoyatlarni alohida kategoriyalarga bo‘lish, ularni xalqaro miqyosda **bir xil tasniflash** va **yagona definitsiyalarga ega bo‘lish** ehtiyoji kuchaymoqda. Bu tasnif quyidagi omillar asosida tuzilishi mumkin:

- Jinoyatning maqsadi (moliyaviy foyda, siyosiy bosim, shaxsiy zarar yetkazish va h.k.);
- Jinoyat vositasi (dasturiy ta’minot, tarmoq texnologiyalari, axborot vositalari);
- Jabrlanuvchining turi (individ, tashkilot, davlat);
- Hududiy xususiyat (ichki, transchegaraviy, global tarmoq asosida sodir etilgan jinoyatlar).

Xulosa qilib aytganda, axborot texnologiyalarining rivojlanishi jinoyatchilik tabiatini mutlaqo yangi bosqichga olib chiqdi. Bu jarayon nafaqat yangi jinoyat turlarining paydo bo‘lishiga, balki mavjud jinoyatlarning raqamli muhitga ko‘chishiga ham sabab bo‘lmoqda. Natijada, jinoyat huquqi, xalqaro hamkorlik va jinoyatga qarshi kurashish institutlari oldida yangicha yondashuvlar zarurati vujudga keldi. Shu nuqtai nazardan, kiberjinoyatlarni huquqiy jihatdan tahlil qilish va ularni xalqaro miqyosda samarali tasniflash zamonaviy huquqshunoslik fanining dolzarb yo‘nalishlaridan biriga aylanmoqda.

Ilk kiberjinoyatlar va ularning turlari. Axborot-kommunikatsiya texnologiyalarining jamiyat hayotiga chuqur kirib borishi bilan birga, jinoyatchilikning yangi, ilgari noma’lum bo‘lgan turlari ham yuzaga keldi. Kiberjinoyatlar deganda, kompyuter tizimlari, tarmoqlar, dasturiy vositalar va raqamli ma’lumotlar orqali yoki ularni nishonga olib sodir etilgan jinoyat harakatlari tushuniladi. Bugungi kunda bu tushuncha xalqaro miqyosda tan olingan bo‘lsa-da, uning ilk paydo bo‘lishi va rivojlanish bosqichlari muhim tarixiy va huquqiy tahlilni talab etadi.

Ilk kiberjinoyatlar tarixi. Dastlabki kiberjinoyatlar 1960–1970-yillarda AQShda yirik kompyuter tizimlaridan foydalana boshlangandan keyin paydo bo‘lgan. Bu davrda kiberjinoyatlar odatda ichki tizimga ega bo‘lgan

tashkilotlarda ishlovchi mutaxassislar tomonidan amalga oshirilgan boʻlib, ularning harakati dasturiy manipulyatsiya, ruxsatsiz kirish va moliyaviy manipulyatsiyalarga qaratilgan edi.

Tarixiy misollar:

- ✓ **1971-yilda "Blue Box" texnologiyasi** yordamida telefon tarmoqlarini buzgan Steve Wozniak va Steve Jobs (keyinchalik Apple asoschilari) tomonidan amalga oshirilgan amaliyotlar dastlabki kiberjinoyatlardan biri sifatida qayd etiladi.
- ✓ **1983-yilda AQShda "The 414s" nomi bilan tanilgan guruh** hukumat va universitet tizimlariga noqonuniy kirib, kiberxavfsizlik masalasini global darajada koʻtarib chiqqan.

Shu bilan birga, ilk kiberjinoyatlar rasmiy ravishda "jinoyat" sifatida tan olinmagan, koʻproq odob-axloq yoki tashkiliy tartibni buzish sifatida baholangan. Biroq vaqt oʻtishi bilan bunday harakatlarning jamiyat xavfsizligiga tahdidi ortgani sayin, ular jinoyat deb e'tirof etila boshlandi.

Kiberjinoyatlarning dastlabki turlari. Ilk bosqichdagi kiberjinoyatlarni quyidagi asosiy toifalarga ajratish mumkin:

- ➢ **Kompyuter tizimlariga noqonuniy kirish (unauthorized access):** Bu kiberjinoyat turi foydalanuvchi ruxsatisiz kompyuter tizimlariga kirishni anglatadi. Ilk hollarda bunday harakatlar "qiziqish" yoki "intellektual chaqiriq" sifatida baholangan boʻlsa-da, ularning oqibatida tizimlar buzilishi, ma'lumotlar yoʻqolishi yoki oʻgʻirlanishi kuzatilgan.
- ➢ **Dasturiy hujumlar (malware tarqatish):** Viruslar, qurtlar, troyanlar kabi zararli dasturiy ta'minotlarning yaratilishi va tarqatilishi ilk kiberjinoyatlardan boʻlib, ularning asosiy maqsadi foydalanuvchi tizimini ishdan chiqarish yoki yashirin tarzda nazorat qilish edi. Eng mashhur dastlabki viruslardan biri bu **1986-yilda yaratilgan "Brain" virusi** boʻlgan.
- ➢ **Elektron firibgarlik (cyber fraud):** Elektron pochta orqali aldov, moliyaviy ma'lumotlarni oʻgʻirlash va yolgʻon toʻlov tizimlari orqali foyda olish ilk yillarda ham uchragan. Ular koʻpincha bank tizimlariga nisbatan amalga oshirilgan.
- ➢ **Axborotni buzish va oʻgʻirlash:** Bu holatlar kompyuter tizimida saqlanayotgan ma'lumotlarning ruxsatsiz oʻzgartirilishi, yoʻq qilinishi yoki nusxalanishi koʻrinishida namoyon boʻlgan.

- **Shaxsiy va davlat sirlarini buzish:** Dastlabki kiberjosuslik holatlari sovuq urush davrida sodir etilgan bo‘lib, ular harbiy yoki sanoat sirlarini o‘g‘irlashga qaratilgan edi.

Ilk kiberjinoyatlarni jinoyat deb tan olishdagi qiyinchiliklar. Kiberjinoyatlarning dastlabki davrlarida ularga nisbatan huquqiy baho berishda muhim to‘siqlar mavjud edi:

- ✓ **Huquqiy bo‘shliqlar:** Dastlabki yillarda ko‘plab davlatlarning jinoyat kodekslarida kiberjinoyatlar uchun maxsus modda mavjud emas edi.
- ✓ **Texnik yetishmovchilik:** Jinoyatlarni aniqlash, isbotlash va forensik tahlil qilish texnologiyalari rivojlanmagan edi.
- ✓ **Javobgarlikni aniqlashdagi murakkablik:** Virtual fazoda sodir etilgan jinoyatlarda jinoyatchining aniq shaxsini aniqlash mushkul bo‘lgan.
- ✓ **Transmilliy xususiyat:** Jinoyat bir davlatda sodir etilib, boshqa davlatga zarar yetkazgan hollarda yurisdiktsiya masalasi bahsli bo‘lgan.

Ilmiy manbalar va xalqaro yondashuvlar. Ilk kiberjinoyatlarni o‘rganishda AQSh Federal Tergov Byurosi (FBI), Interpol, Yevropa Ittifoqining ENISA agentligi, shuningdek, Budapesht konvensiyasi (2001) kabi hujjatlar muhim manbalar hisoblanadi. Bu konvensiya ilk marotaba xalqaro miqyosda kiberjinoyatlarni rasmiy ravishda jinoyat deb tan olgan huquqiy asoslardandir.

Yangi davrda ilmiy doiralarda ilk kiberjinoyatlarni quyidagicha tasniflash taklif etilgan:

- **Kompyuterga qaratilgan jinoyatlar** (computer-targeted crimes);
- **Kompyuter vositasida amalga oshirilgan jinoyatlar** (computer-assisted crimes);
- **Kompyuterda saqlanayotgan ma’lumotlarni nishonga olgan jinoyatlar** (data-related crimes).

Xulosa qilib aytganda, ilk kiberjinoyatlar zamonaviy jinoyatchilikning raqamli shakliga asos solgan va bu yo‘nalishda xalqaro huquqiy tizimda yangi yondashuvlarni shakllantirish zaruriyatini yuzaga keltirgan. Ularning shakllanishi, turlari va jinoyat deb tan olinishi bo‘yicha olib borilgan tahlillar bugungi kunda kiberjinoyatlarga qarshi kurashishda muhim tarixiy va nazariy asos bo‘lib xizmat qilmoqda. Shuningdek, bu yo‘nalishda xalqaro hamkorlik, huquqiy muvofiqlashtirish va texnologik infratuzilmani takomillashtirish orqali jinoyatchilikning oldini olish mumkin.

“Kiberjinoyat” atamasining xalqaro huquqdagi shakllanishi. So‘nggi o‘n yilliklarda axborot-kommunikatsiya texnologiyalarining jadal sur’atlar bilan rivojlanishi natijasida jamiyat hayotining deyarli barcha jabhalarida tub o‘zgarishlar yuz berdi. Biroq texnologik taraqqiyot bilan bir qatorda, global miqyosda raqamli jinoyatchilik — ya’ni **kiberjinoyatlar** xavfi ham ortdi. Bu holat xalqaro huquq tizimida mazkur hodisani rasmiy huquqiy tushuncha sifatida e’tirof etish va uni tartibga solishga qaratilgan yangi yondashuvlarni shakllantirish zaruratini tug‘dirdi.

“Kiberjinoyat” atamasi: semantik va huquqiy yondashuv. “Kiberjinoyat” (ingl. *cybercrime*) atamasi dastlab ilmiy adabiyotlarda va texnologik jargon doirasida shakllangan bo‘lib, asta-sekin huquqiy diskursga ham kirib keldi. Bu atama **“cyber”** (ya’ni kompyuter yoki raqamli tarmoq bilan bog‘liq) va **“crime”** (jinoyat) so‘zlarining birikmasidan tashkil topgan bo‘lib, kompyuter tizimlari, tarmoqlar yoki raqamli qurilmalar orqali yoki ularga qarshi sodir etiladigan har qanday noqonuniy harakatlarni anglatadi.

Ammo bu atamaning huquqiy jihatdan rasmiy tan olinishi oson kechmadi. Chunki:

- ✓ “Kiberjinoyat” texnik jihatdan juda murakkab va o‘zgaruvchan kategoriya hisoblanadi;
- ✓ Turli mamlakatlarda bu atama va unga kiruvchi jinoyatlar tarkibi bo‘yicha **bir xillik yo‘q**;
- ✓ Har bir davlatning **milliy xavfsizlik, axborot erkinligi va huquqiy madaniyati** darajasi turlicha bo‘lgani uchun ularning yondashuvi ham farqlanadi.

Shu bois, xalqaro huquqda bu tushunchaning bir xilda tan olinishi uzoq va bosqichma-bosqich kechgan.

Xalqaro huquqdagi asosiy bosqichlar

1. Budapesht konvensiyasi (2001 yil) – birinchi universal huquqiy yondashuv. Yevropa Kengashi tomonidan qabul qilingan “Kompyuter jinoyatlari to‘g‘risidagi konvensiya” yoki **Budapesht konvensiyasi** xalqaro maydonda “kiberjinoyat” tushunchasini huquqiy jihatdan tan olgan **birinchi va hozirgacha eng nufuzli hujjat** hisoblanadi.

Konvensiyada “kiberjinoyatlar” quyidagi toifalarga ajratiladi:

- ➢ Kompyuter tizimiga ruxsatsiz kirish (unauthorized access);
- ➢ Kompyuter ma’lumotlarini noqonuniy o‘zgartirish yoki o‘chirish (data interference);

- Tarmoq uzilishiga sabab bo‘lish (system interference);
- Kompyuter orqali firibgarlik va tovlamachilik;
- Pornografiya, ayniqsa bolalar pornografiyasi bilan bog‘liq harakatlar;
- Mualliflik huquqlarini buzish.

Budapesht konvensiyasi “kiberjinoyat” atamasini bevosita ta’riflamagan bo‘lsa-da, **amalda bu tushunchani huquqiy normalar asosida tarkibiy jihatdan shakllantirgan**. Shuningdek, konvensiya kiberjinoyatlarga qarshi xalqaro hamkorlik, ekstraditsiya, isbotlash va tezkor ma’lumot almashinuvi masalalarini tartibga soladi.

2. BMT (UNODC) tashabbuslari va yondashuvlari. Birlashgan Millatlar Tashkilotining Giyohvandlik va jinoyatchilikka qarshi kurash boshqarmasi (UNODC) tomonidan olib borilgan ko‘plab forumlar, maxsus sessiyalar va hisobotlarda **“cybercrime”** tushunchasi doirasida quyidagi yondashuvlar mavjud:

- Kiberjinoyatlar ikki guruhga ajratiladi: **kompyuterga qarshi jinoyatlar** va **kompyuter vositasida sodir etilgan jinoyatlar**;
- Har bir davlat kiberjinoyatlarni milliy qonunchiligida tan olish orqali BMT umumiy tavsiyalariga mos harakat qilishga chaqiriladi;
- Kiberjinoyatlarga qarshi kurashda **inson huquqlari va erkinliklariga putur yetkazmaslik** muhim prinsip sifatida e’tirof etiladi.

Hozirgi kunda BMT tomonidan **xalqaro kiberjinoyat konvensiyasi** ishlab chiqilmoqda (2023-yil holatiga ko‘ra loyihaviy bosqichda) va bu hujjat Budapesht konvensiyasiga global muqobil bo‘lishi kutilmoqda.

3. Interpol va Europol doirasidagi huquqiy yondashuvlar. Interpol va Europol o‘z faoliyatida “kiberjinoyat” atamasiga quyidagicha yondashadi:

- Bu jinoyatlar transchegaraviy xarakterga ega va global kooperatsiyani talab etadi;
- Har qanday raqamli infrastrukturaga qarshi qilingan harakat “kiberjinoyat” sifatida qaraladi;
- Maxsus “Cybercrime Directorate”lar tashkil etilgan bo‘lib, ular jinoyat turlarini aniqlash, tasniflash va tarmoqlarni himoya qilishda markaziy rol o‘ynaydi.

Interpol kiberjinoyatlarni uch toifaga bo‘ladi:

1. **Raqamli infrastrukturaga hujumlar** (DDoS, viruslar, kiberterrorizm);

2. **Moliyaviy va firibgarlik jinoyatlari** (phishing, spoofing, kriptovalyuta firibgarligi);

3. **Shaxsiy va axloqiy jinoyatlar** (kiberbulling, shaxsiy ma’lumotlarni tarqatish, onlayn zo‘ravonlik).

Atamaning huquqiy noaniqliklari va muammolari. Xalqaro huquqda “kiberjinoyat” atamasi bilan bog‘liq hali ham mavjud bo‘lgan ayrim muammolar quyidagilardan iborat:

- **Universallikning yo‘qligi:** Turli xalqaro tashkilotlar va davlatlar bu atamani turlicha talqin qilmoqda;
- **Huquqiy vakillik darajasining farqlanishi:** Ayrim mamlakatlar bu atamani qonunchilikka joriy qilmagan;
- **Texnologik o‘zgaruvchanlik:** Yangi jinoyatlar doimiy ravishda yuzaga kelmoqda va mavjud huquqiy ta’riflar ularni qamrab ololmayapti;
- **Inson huquqlari bilan ziddiyat:** Raqamli nazorat va monitoring tadbirlari ko‘plab holatlarda maxfiylik huquqiga zid kelishi mumkin.

Xulosa qilib aytganda, “Kiberjinoyat” atamasi xalqaro huquqda nisbatan yangi, ammo tez sur’atlarda shakllanayotgan tushuncha bo‘lib, uning to‘liq va umumiy qabul qilingan huquqiy ta’rifi hozircha mavjud emas. Shunga qaramay, Budapesht konvensiyasi, BMT tashabbuslari va xalqaro tashkilotlar tomonidan qabul qilingan tamoyillar ushbu atamani huquqiy muomalaga joriy etishda muhim qadam bo‘lib xizmat qilmoqda. Kiberjinoyatlarning global tahdidga aylanishi ularni xalqaro huquqiy doirada rasmiy tartibga solishni nafaqat dolzarb, balki zarur masalaga aylantiradi. Shu nuqtai nazardan, kiberjinoyat atamasining xalqaro huquqiy shakllanishi zamonaviy huquqshunoslikda o‘ta muhim va dinamik rivojlanayotgan yo‘nalishlardan biridir.

1.2. Zamonaviy xalqaro kiberjinoyat turlari

XXI asr axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi bilan ajralib turadi. Raqamli inqilob natijasida insoniyat hayotining deyarli barcha sohalari – iqtisodiyot, siyosat, sog‘liqni saqlash, ta’lim, moliya, madaniyat, hatto harbiy strategiyalar ham – raqamli maydonga ko‘chdi. Biroq bu yutuqlar bilan bir qatorda, **kiberjinoyatchilikning globallashuvi va murakkablashuvi** ham kuzatilmoqda. Ayniqsa, xalqaro kiberjinoyatlar — ya’ni bir davlat hududida amalga oshirilgan, ammo boshqa davlatlarga zarar

yetkazuvchi yoki bir nechta mamlakatlarni qamrab oluvchi kiberhujumlar — bugungi kunda eng jiddiy global xavf sifatida baholanmoqda.

Bu holat nafaqat milliy xavfsizlik, balki xalqaro huquqiy tartibot uchun ham ulkan chaqiriq bo‘lib qolmoqda. Kiberjinoyatlar turli shakl va mazmun kasb etmoqda: moliyaviy firibgarlik, shaxsiy ma’lumotlarni o‘g‘irlash, mualliflik huquqlarini buzish, kiberterrorizm, davlat sirlari yoki infrastrukturasiga qarshi hujumlar, sun’iy intellektdan noqonuniy foydalanish va boshqalar. Mazkur jinoyatlar ko‘pincha transchegaraviy xarakterga ega bo‘lib, ularni aniqlash, isbotlash va jazolashda an’anaviy huquqiy vositalar yetarli bo‘lmay qolmoqda.

Zamonaviy xalqaro kiberjinoyatlar bir necha jihatdan o‘ziga xosdir:

✓ Ular **yuqori texnologik darajada amalga oshiriladi** va doimiy ravishda yangilanib boradi;

✓ Ko‘p hollarda **kiberjinoyatchilar jismoniy shaxslar emas, balki tashkilotli guruhlar yoki hatto davlatlar bo‘lishi mumkin**;

✓ Jinoyatlar **bir vaqtning o‘zida bir nechta huquqiy yurisdiksiyalarni buzishi** mumkin, bu esa ularni tergov qilishni murakkablashtiradi;

✓ Ular **moliyaviy, siyosiy, ma’naviy yoki axborot strategiyasi asosida motivatsiyalangan bo‘lishi** mumkin.

Shu bois, zamonaviy xalqaro kiberjinoyatlarni to‘g‘ri tasniflash, ularni aniqlovchi asosiy belgi va mezonlarni aniqlash, xalqaro huquqda ularning o‘rnini aniq belgilash – zamonaviy yuridik fan oldidagi dolzarb vazifalardan biridir. Ushbu bandda aynan kiberjinoyatlarning zamonaviy va xalqaro miqyosda eng ko‘p uchraydigan turlari, ularning xususiyatlari, amalga oshirish usullari, maqsadlari va xavflilik darajalari tahlil qilinadi.

Mazkur tahlil, bir tomondan, xalqaro jinoyat huquqi doirasida kiberjinoyatlarni huquqiy jihatdan tan olish uchun nazariy asos yaratadi; boshqa tomondan esa, amaliyotda ularning oldini olish va jazolash mexanizmlarini takomillashtirishga xizmat qiladi.

Raqamli firibgarlik, fishing, spoofing va botnetlar: zamonaviy xalqaro kiberjinoyatlarning asosiy ko‘rinishlari. Zamonaviy axborot-kommunikatsiya texnologiyalari taraqqiyoti insoniyat hayotini soddalashtirish, tezkor axborot almashinuvi va raqamli iqtisodiyotni rivojlantirish imkonini bersa-da, bu qulayliklar bilan bir qatorda jinoyatchilikning yangi shakllari – ayniqsa, raqamli firibgarlik turlarining global miqyosda kengayishiga ham sabab

bo‘lmoqda. Xalqaro kiberjinoyatlar orasida **raqamli firibgarlik, fishing (phishing), spoofing va botnetlar orqali amalga oshiriladigan jinoyatlar** eng ko‘p uchraydigan va iqtisodiy, ijtimoiy hamda xavfsizlik jihatidan eng xavfli ko‘rinishlar sirasiga kiradi.

Raqamli firibgarlik (Digital fraud). Raqamli firibgarlik — bu raqamli qurilmalar, internet va axborot-kommunikatsiya texnologiyalari vositasida sodir etiladigan, aldamchilik yoki ishonchdan suiiste’mol qilish orqali moliyaviy, ma’lumot yoki boshqa boyliklarni noqonuniy yo‘l bilan qo‘lga kiritish harakatidir. Bu turdagi jinoyat xalqaro miqyosda quyidagi shakllarda sodir etilishi mumkin:

- **Onlayn moliyaviy tranzaksiyalarni buzish** (masalan, bank hisob raqamlariga noqonuniy kirish);
- **Soxta elektron do‘konlar yoki investitsiya platformalari orqali pullarni tovlamachilik yo‘li bilan olish**;
- **Kriptovalyutalar orqali amalga oshiriladigan piramida sxemalari yoki token firibgarligi**.

Raqamli firibgarlik odatda yuqori darajadagi texnik bilimga ega jinoyatchilar tomonidan amalga oshiriladi va ularning faoliyati transchegaraviy xarakterga ega bo‘lib, turli yurisdiksiyalarning ishtirokini talab etadi. Budapesht konvensiyasi (2001) va BMTning UNODC doirasidagi hujjatlarda bu turdagi jinoyatlar kiberfiribgarlik (cyberfraud) shaklida alohida tasnif etilgan.

Fishing (Phishing). Fishing — bu ijtimoiy muhandislik (social engineering) usullaridan foydalanib, foydalanuvchilarning maxfiy ma’lumotlarini (masalan: parollar, bank kartasi raqamlari, loginlar) aldov yo‘li bilan qo‘lga kiritishga qaratilgan kiberjinoyat turidir. Ushbu jinoyat ko‘p hollarda quyidagi yo‘llar orqali amalga oshiriladi:

- Soxta (gohda rasmiy ko‘rinishga ega) elektron pochta xabarlari yuborish;
- Soxta veb-saytlar yaratish va foydalanuvchini ularga yo‘naltirish;
- Ijtimoiy tarmoqlarda firibgarlik xabarlarini tarqatish.

Fishing xalqaro miqyosda yuqori tahdid darajasiga ega, chunki:

- Bu usul orqali **foydalanuvchining shaxsiy hayoti va moliyaviy axborotlari buziladi**;
- Jinoyatchilar **bir nechta davlat hududida faoliyat yuritadi**, bu esa ularni aniqlash va jazolashni murakkablashtiradi;

- Fishingdan foydalanib **keyingi jinoyatlar sodir etilishi mumkin**, masalan: bank o‘g‘riligi, identifikatsiyani qalbakilashtirish, noqonuniy sotuvlar.

2020 yildan boshlab COVID-19 pandemiyasi davrida fishing hujumlari global miqyosda rekord darajaga yetdi. Microsoft, Google, FBI va Interpol ma’lumotlariga ko‘ra, bu jinoyatlar asosan sog‘liqni saqlash tizimi, elektron tijorat va bank sektoriga qaratilgan.

Spoofing. Spoofing — bu texnik jihatdan murakkab bo‘lgan va aldamchilikka asoslangan kiberjinoyat turidir. Jinoyatchi bu usul orqali o‘zini boshqa ishonchli shaxs yoki tizim sifatida ko‘rsatib, foydalanuvchi yoki kompyuter tizimini chalg‘itadi. Spoofingning asosiy turlari quyidagilardan iborat:

- **IP-spoofing** – soxta IP manzildan foydalanib tarmoqqa ruxsatsiz kirish;
- **Email-spoofing** – soxta email manzildan xat yuborish orqali foydalanuvchini aldatish;
- **Caller ID spoofing** – telefon raqamini soxtalashtirish;
- **DNS-spoofing** – tarmoqda foydalanuvchini soxta saytga yo‘naltirish.

Spoofingning xavfi shundaki, u ko‘pincha boshqa jinoyatlar bilan birgalikda qo‘llaniladi — masalan, fishing, firibgarlik yoki zararli dastur tarqatish. Bundan tashqari, bu jinoyat xalqaro aloqa tarmoqlari, internet provayderlari va pochta serverlaridan foydalanadi, bu esa uni aniqlash va huquqiy baholashni yanada qiyinlashtiradi.

Botnetlar. Botnet (robot tarmog‘i) — bu kiberjinoyatchi tomonidan nazorat qilinayotgan, turli joylardagi “zombi-kompyuterlar”dan iborat tarmoq bo‘lib, ular avtomatik tarzda jinoyat maqsadlarida qo‘llaniladi. Odatda foydalanuvchi kompyuteri maxsus zararli dastur orqali “infektsiyalanadi” va u haqda egasi bilmasligi mumkin.

Botnetlar orqali quyidagi jinoyatlar amalga oshiriladi:

- **DDoS hujumlar** (server yoki veb-saytni ishdan chiqarish);
- **Spam va fishing xabarlari tarqatish**;
- **Kriptovalyuta qazib olish (cryptojacking)** uchun resurslarni noqonuniy egallash;
- **Zararli dasturlarni keng miqyosda tarqatish**.

Botnetlar ko‘pincha bir nechta mamlakatdagi minglab qurilmalardan iborat bo‘ladi. Shu boisdan, ular xalqaro jinoyat sifatida baholanadi va jiddiy

tahdid hisoblanadi. Interpol va Europol doirasida botnetlar bilan bog‘liq operatsiyalar muntazam o‘tkazilib kelinmoqda, masalan: “Avalanche”, “GameOver Zeus” yoki “Emotet”ga qarshi global kampaniyalar.

Xulosa qilib aytganda, Raqamli firibgarlik, fishing, spoofing va botnetlar — zamonaviy xalqaro kiberjinoyatlarning eng keng tarqalgan, dinamik rivojlanayotgan va ijtimoiy-iqtisodiy oqibatlari chuqur bo‘lgan turlaridir. Ularning umumiy jihati – texnologik asosda sodir etilishi, transchegaraviy xarakteri, yuqori darajadagi yashirinligi va tezkor evolyutsiyalanishidir. Bu jinoyatlar faqat texnik choralar bilan emas, balki kompleks huquqiy, xalqaro va institutsional yondashuvlar bilan nazoratga olinishi lozim. Shu sababli, ularni huquqiy jihatdan jinoyat deb e’tirof etishdagi aniqlik va barqarorlik global xavfsizlik nuqtayi nazaridan alohida ahamiyat kasb etadi.

Ransomware va zararli dasturlar orqali hujumlar. Zamonaviy kiberjinoyatchilikning eng xavfli va iqtisodiy jihatdan eng zararli turlaridan biri — **ransomware hujumlari** (mahsulot yoki xizmatni talab qilish uchun teskari zararli dasturlar orqali hujumlar)dir. Ushbu hujumlar bugungi kunda nafaqat biznes va davlat tashkilotlari, balki oddiy fuqarolarni ham nishon qilib, ularning kompyuter tizimlarini yoki mobil qurilmalarini zararlash orqali ulardan moliyaviy foyda olishga qaratilgan. Ransomware va boshqa zararli dasturlar (malware) ko‘plab xalqaro kiberjinoyatlarda qo‘llanilmoqda, chunki ular o‘zlarining texnologik murakkabligi va yuksak darajadagi yashirinligi bilan xavfli hisoblanadi.

Ransomware: ta’rif, xususiyatlar va turli shakllari. Ransomware (ransom + software — “talab qiluvchi dastur”) — bu zararli dastur bo‘lib, foydalanuvchi tizimiga kirib, unga shifrlashni amalga oshiradi, keyin esa shifrlangan ma’lumotlarni qayta tiklash uchun ma’lum miqdorda pul talab qiladi. Ransomware harakati odatda quyidagicha sodir bo‘ladi:

- **Kompyuter tizimi yoki tarmog‘iga kirish** — kiberjinoyatchilar phishing, zararli e-pochta xabarlar yoki ekspluatatsiya qilinadigan zaifliklar orqali tizimga kirishadi;
- **Ma’lumotlarni shifrlash** — dastur fayllarni yoki butun tizimni shifrlab, foydalanuvchidan bu ma’lumotlarni tiklash uchun to‘lov talab qiladi;
- **To‘lovni talab qilish** — jinoyatchilar odatda **kriptovalyuta** (masalan, Bitcoin) orqali to‘lovni talab qiladi, bu esa ularning shaxsini yashirinishiga yordam beradi;

- **Ma’lumotlarni qayta tiklash yoki o‘chirish** — to‘lov amalga oshirilsa, jinoyatchilar zararli dastur yordamida shifrlangan ma’lumotlarni qayta tiklaydi yoki shartlar bajarilmasa, ma’lumotlarni o‘chirib yuborishi mumkin.

Ransomware hujumlari ko‘p hollarda **kriptovalyutalarni talash**, **kompaniya sirlarini o‘g‘irlash**, yoki **tashkilotlarning tarmoq infratuzilmasini ishlamaydigan holga keltirish** kabi iqtisodiy yoki siyosiy maqsadlarni ko‘zlaydi. Ularning global ta’siri juda katta bo‘lib, jumladan, 2020-yilgi statistikaga ko‘ra, har yili butun dunyo bo‘ylab bir necha milliard dollar miqdorida zarar yetkaziladi.

Ransomware hujumlari turli shakllarda sodir etiladi, ularning eng keng tarqalganlari quyidagilar:

- **Crypto ransomware** — bu hujumda, tizimdagi fayllar shifrlanadi va foydalanuvchidan to‘lov talab qilinadi.
- **Locker ransomware** — tizimga kirish imkoniyati to‘siladi, ya’ni foydalanuvchi o‘zining kompyuteriga yoki tizimiga kira olmaydi.
- **Scareware** — foydalanuvchiga tizimning zarar ko‘rganligini bildiruvchi, ammo aslida ishlamaydigan dastur orqali foydalanuvchidan pul talab qilinadi.

Zararli dasturlar (Malware) orqali hujumlar. Zararli dasturlar (malware) — bu kiberjinoyatchilar tomonidan tizimlarga kirish va zarar yetkazish uchun ishlatiladigan har qanday dasturiy ta’sir ko‘rsatish vositalaridir. Malware turlari juda ko‘p, shuningdek, ular quyidagi toifalarda tasniflanadi:

- **Viruslar** — tizimga kirib, boshqa dasturlarga yoki fayllarga zarar yetkazadigan dasturlar. Viruslar ko‘pincha foydalanuvchi noto‘g‘ri xatti-harakatlari orqali, masalan, zararli fayllarni ochish yoki o‘rnatish orqali tarqaladi;
- **Trojanlar** — foydalanuvchining yoki tizimning xavfsizligini buzish uchun yaratilgan dasturlar. Trojanlar o‘zlarining zararli xatti-harakatlarini ko‘rsatmasdan, legitimit tarzda ishlashni davom ettiradi;
- **Worms** — internet orqali o‘z-o‘zidan tarqaladigan va boshqa tizimlarga kirib zarar yetkazadigan dasturlar;
- **Spyware** — foydalanuvchining shaxsiy va moliyaviy ma’lumotlarini sirg‘alab o‘g‘irlaydigan dasturlar;

- **Keyloggers** — foydalanuvchining barcha klaviatura harakatlarini yozib oluvchi dasturlar.

Malware zararli dasturlari odatda **kompaniya sirlarini o‘g‘irlash**, **moliyaviy firibgarliklarni amalga oshirish**, **kiberterrorizm** va **tizimlarning uzilishiga olib kelish** kabi maqsadlarda ishlatiladi. Raqamli jinoyatchilar bu turdagi dasturlarni yuqori darajadagi yashirinlikni ta’minlaydigan mexanizmlar orqali qo‘llaydilar.

Ransomware va zararli dasturlarni xalqaro miqyosda jazolash va oldini olish. Ransomware va boshqa zararli dasturlar orqali amalga oshiriladigan hujumlar xalqaro xavfsizlikka jiddiy tahdid soladi. Buning uchun:

- **Xalqaro hamkorlik va qonunlar**: Interpol, Europol va boshqa xalqaro tashkilotlar kiberjinoyatchilikka qarshi birgalikda kurashish uchun o‘zaro hamkorlikda faoliyat yuritadi. Shuningdek, BMT tomonidan ishlab chiqilgan **Budapesht konvensiyasi** (2001) va boshqa xalqaro huquqiy hujjatlar orqali kiberjinoyatlar bo‘yicha huquqiy asoslar yaratilgan.
- **Milliy xavfsizlik va huquqiy mexanizmlar**: Ko‘plab davlatlar o‘zining ichki qonunchiligini takomillashtirish orqali ransomware va zararli dasturlarni o‘chirib tashlash, ularni tarqatish va ularga qarshi kurashish usullarini ishlab chiqishmoqda. Masalan, ko‘plab davlatlar **cybersecurity** sohasida milliy agentliklar va kompyuter xavfsizligi bo‘yicha boshqaruv tizimlarini joriy etgan.

Ransomware va zararli dasturlarning oldini olish uchun quyidagi yondashuvlar talab etiladi:

- **Zararli dasturlarni aniqlash va ularni bloklash** uchun zamonaviy antivirus tizimlarini ishlab chiqish va kengaytirish;
- **Kompyuter tarmoqlarining himoya tizimlarini mustahkamlash** va foydalanuvchilarga xavfsizlik bo‘yicha bilimlarni oshirish;
- **Xalqaro hamkorlik va axborot almashish**ni kuchaytirish, global kiber jinoyatga qarshi kurashish uchun standartlar yaratish.

Xulosa qilib aytganda, Ransomware va zararli dasturlar orqali amalga oshiriladigan hujumlar zamonaviy kiberjinoyatlarning eng xavfli turlaridan biridir. Ushbu hujumlar kiberjinoyatchilar uchun katta moliyaviy foyda keltirish, shuningdek, biznes va davlat tizimlarining faoliyatini buzish imkonini beradi. Bu jinoyatlar xalqaro miqyosda tobora kuchayib borayotgan xavf sifatida e’tirof etilmoqda va ularni bartaraf etish uchun faqat texnologik

yondashuvlar emas, balki huquqiy, ijtimoiy va global hamkorlikka asoslangan tizimli choralar ham zarurdir.

Kompyuter tizimlariga noqonuniy kirish va ma’lumotlar o‘g‘irligi. Zamonaviy axborot texnologiyalarining rivojlanishi va raqamli tizimlarning kundalik hayotdagi o‘rni ortishi bilan, kiberjinoyatlarning ko‘payishi va ularning ijtimoiy-iqtisodiy xavf-xatarlarining jiddiylashishi aniq ko‘rinmoqda. Shu nuqtai nazardan, **kompyuter tizimlariga noqonuniy kirish** va **ma’lumotlarni o‘g‘irlash** — eng keng tarqalgan va global miqyosda xavf tug‘diruvchi kiberjinoyatlar sirasiga kiradi. Ushbu jinoyatlar zamonaviy raqamli infratuzilmalarning zaif joylaridan foydalanish orqali amalga oshiriladi, bu esa ularni nafaqat texnik, balki huquqiy jihatdan ham yanada murakkab va xavfli qiladi.

Kompyuter tizimlariga noqonuniy kirish: ta’rif va usullari. Kompyuter tizimlariga noqonuniy kirish — bu kiberjinoyatchining tizimga, tarmoqqa yoki kompyuterga ruxsatsiz va qonunbuzarlik sifatida kirishi hamda tizimdagi ma’lumotlarga, resurslarga yoki xizmatlarga noqonuniy ulanishidir. Tizimga kirishning maqsadi, odatda, foydalanuvchi ma’lumotlarini o‘g‘irlash, tarmoq infratuzilmasini buzish, zararli dasturlarni tarqatish yoki boshqa jinoyatlarni amalga oshirish bo‘ladi.

Noqonuniy kirish usullari ko‘plab shakllarda sodir etiladi, ularning eng keng tarqalganlari quyidagilar:

- **Parolni sindirish (brute force)** — kiberjinoyatchi tizimga kirish uchun foydalanuvchining parolini aniqlashga harakat qiladi. Bu usulda maxsus dasturlar yordamida turli xil parollar kiritilib, tizimga kirish imkoniyati tekshiriladi.
- **Zaifliklarni ekspluatatsiya qilish (exploitation of vulnerabilities)** — tizim yoki dasturdagi zaifliklardan foydalangan holda tizimga ruxsatsiz kirish amalga oshiriladi. Masalan, eski dasturiy ta’minotdagi zaifliklar yoki yangilanishlarni o‘tkazib yuborish.
- **Social engineering (ijtimoiy muhandislik)** — foydalanuvchilarning ishonchini suiiste’mol qilish orqali tizimga kirish. Bu usulda kiberjinoyatchi, masalan, soxta xatlar yoki telefon qo‘ng‘iroqlari orqali odamlarni aldaydi va ularning tizimga kirish huquqini qo‘lga kiritadi.
- **Phishing hujumlari** — zararli elektron pochta xabarlari orqali foydalanuvchidan tizimga kirish uchun zarur ma’lumotlar (masalan, parollar) olinadi va tizimga noqonuniy kirish uchun foydalaniladi.

Bu usullar orqali kompyuter tizimlariga noqonuniy kirish osonlikcha amalga oshiriladi, chunki koʻplab tashkilotlar va fuqarolar zaif xavfsizlik tizimlariga ega boʻlishi mumkin. Bu esa jinoyatchilarga osonlik bilan tizimlarni buzish va oʻz maqsadlariga erishish imkoniyatini beradi.

Ma'lumotlarni oʻgʻirlik: ta'rif va keng tarqalgan usullar. Ma'lumotlarni oʻgʻirlik — bu kompyuter tizimlariga noqonuniy kirish orqali foydalanuvchining yoki tashkilotning shaxsiy, moliyaviy yoki boshqa muhim ma'lumotlarini olishni anglatadi. Ma'lumotlarni oʻgʻirlik qilishning maqsadi koʻpincha iqtisodiy foyda olish boʻlib, bu orqali kiberjinoyatchilar kompaniyalar yoki shaxslar ustidan nazorat oʻrnatishga harakat qiladilar.

Ma'lumotlarni oʻgʻirlashning asosiy usullari quyidagilardir:

- **Identifikatsiya ma'lumotlarini oʻgʻirlash** (identity theft) — foydalanuvchilarning shaxsiy ma'lumotlarini (masalan, pasport, kredit karta ma'lumotlari) oʻgʻirlash orqali firibgarlikni amalga oshirish. Bunday jinoyatlar koʻpincha phishing va social engineering usullari orqali sodir boʻladi.
- **Tijorat sirlarini oʻgʻirlash** (industrial espionage) — tashkilotlarning tijorat sirlarini yoki texnologik maxfiy ma'lumotlarini oʻgʻirlash. Bunday jinoyatlar koʻpincha raqobatchilar tomonidan amalga oshiriladi va ular biznes faoliyatiga zarar yetkazish yoki raqobatchilarni ortda qoldirishga qaratilgan.
- **Moliyaviy ma'lumotlarni oʻgʻirlash** — bank hisob raqamlaridan, kredit kartalaridan yoki elektron tijorat tizimlaridan ma'lumotlarni oʻgʻirlash. Bunday jinoyatlar odatda kiberjinoyatchilarning moliyaviy manfaatlarini qondirishga qaratilgan boʻladi.
- **Ma'lumotlarni sotish** — oʻgʻirlangan ma'lumotlarni qora bozor orqali sotish. Masalan, foydalanuvchi ma'lumotlari, kredit karta raqamlari yoki shaxsiy identifikatsiya ma'lumotlari noqonuniy ravishda sotiladi.

Kompyuter tizimlariga noqonuniy kirish orqali amalga oshiriladigan ma'lumotlar oʻgʻirligi, ayniqsa, korporativ sektorda katta xavf tugʻdiradi. Tashkilotlar va kompaniyalar uchun ma'lumotlarning xavfsizligini ta'minlash juda muhimdir, chunki ularning strategik ahamiyatga ega boʻlgan maxfiy axborotlari va mijozlarga oid ma'lumotlar oʻgʻirlangan taqdirda, kompaniya obroʻsi, moliyaviy holati va hatto oʻz faoliyatini davom ettirish imkoniyati jiddiy tahdid ostiga tushadi.

Xalqaro yuridik koʻlamda ma'lumotlarni oʻgʻirlikka qarshi kurash. Kompyuter tizimlariga noqonuniy kirish va **ma'lumotlarni oʻgʻirlik** kiberjinoyatchilarning transchegaraviy faoliyatining keng tarqalgan

shakllaridan biri bo‘lib, bu global miqyosda yirik xavf tug‘diradi. Bu jinoyatlarning oldini olish va ularga qarshi kurashish uchun xalqaro hamkorlik zarur.

Hozirgi kunda **BMTning Kiberjinoyatlar to‘g‘risidagi Budapesht konvensiyasi** (2001) va boshqa xalqaro huquqiy asoslar bu turdagi jinoyatlar bilan kurashishni nazarda tutadi. Xalqaro tashkilotlar, jumladan, **Interpol** va **Europol**, kiberjinoyatchilarni aniqlash va ushlab olish bo‘yicha doimiy hamkorlikni ta’minlamoqda. Bunday faoliyatlar qatoriga davlatlar o‘rtasida kiberjinoyatlar bo‘yicha axborot almashish, qo‘shma operatsiyalarni o‘tkazish va jinoyatchilarni qidirish kiradi.

Shuningdek, milliy qonunchilikka kiritilgan o‘zgarishlar, masalan, ma’lumotlarni himoya qilish qonunlari (GDPR), kiberjinoyatlarning oldini olish va ularga qarshi samarali kurashishda muhim rol o‘ynaydi.

Kiberjinoyatlarning oldini olish va tizim xavfsizligini oshirish. Kompyuter tizimlariga noqonuniy kirish va ma’lumotlarni o‘g‘irlikning oldini olish uchun quyidagi yondashuvlar talab etiladi:

- **Tizim xavfsizligini mustahkamlash**: Kompaniyalar va davlat tashkilotlari tizimlarining xavfsizligini ta’minlash uchun zamonaviy antivirus dasturlari, xavfsizlik devorlari va boshqa himoya vositalarini joriy qilish.
- **Kadrlar uchun ta’lim va treninglar**: Kiberxavfsizlik bo‘yicha xodimlarni muntazam ravishda o‘qitish va treninglar o‘tkazish, xususan, phishing va ijtimoiy muhandislikka qarshi kurashishda yordam beruvchi metodlarni o‘rgatish.
- **Axborot va ma’lumotlar xavfsizligini boshqarish siyosatini ishlab chiqish**: Kompaniyalarga, davlatlarga va foydalanuvchilarga ma’lumotlarni himoya qilishning samarali siyosatlarini joriy etish.

Xulosa qilib aytganda, Kompyuter tizimlariga noqonuniy kirish va ma’lumotlarni o‘g‘irlik kiberjinoyatlarning eng keng tarqalgan shakllaridan biri bo‘lib, ular zamonaviy raqamli dunyoning xavfli tomonlarini ochib beradi. Bu jinoyatlar nafaqat iqtisodiy, balki siyosiy, ijtimoiy va madaniy ta’sirlar keltirishi mumkin. Shuning uchun, kiberxavfsizlikni ta’minlash, xalqaro va milliy darajadagi hamkorlikni rivojlantirish, shuningdek, samarali huquqiy mexanizmlarni yaratish bu jinoyatlarni kamaytirish va oldini olishda muhim rol o‘ynaydi.

1.3. Kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlar

Kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlarni tahlil qilish, kiberjinoyatlarning tabiati va ularning joriy tizimdagi o‘rni haqida yaxshiroq tushuncha hosil qilish uchun zarurdir. Kiberjinoyatlar, asosan, axborot texnologiyalari va raqamli infratuzilmalardan foydalanishni o‘z ichiga olgan jinoyatlar bo‘lib, ular an’anaviy jinoyatlarning ta’rifidan ko‘ra alohida xususiyatlarga ega. Shu sababli, kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlarni chuqur o‘rganish, nafaqat ularni identifikatsiyalash, balki ularning oldini olish va ularga qarshi kurashish choralarini samarali belgilash uchun ham juda muhimdir.

Kiberjinoyatlar va an’anaviy jinoyatlar: asosiy farqlar. Kiberjinoyatlar va **an’anaviy jinoyatlar** o‘rtasidagi eng asosiy farq, ular tomonidan qo‘llaniladigan vositalar va jinoyatning sodir bo‘lish joyidir. Kiberjinoyatlar, odatda, **raqamli texnologiyalar** yordamida amalga oshiriladi, an’anaviy jinoyatlar esa ko‘pincha **jismoniy joylarda**, bevosita shaxsiy ishtirok bilan sodir bo‘ladi. Shu bilan birga, kiberjinoyatlar, ular o‘zgacha turdagi huquqiy, iqtisodiy va ijtimoiy xavflar yaratganligi sababli, ko‘plab yangi yuridik va amaliy muammolarni keltirib chiqaradi.

Bundan tashqari, kiberjinoyatlar **global** va **transchegaraviy** xususiyatga ega bo‘lib, bu ularning huquqiy nazoratini murakkablashtiradi. Kiberjinoyatlarning sodir etilishi uchun jismoniy joy yoki davlat chegaralari zarur emas. Ular internet orqali, bir davlatdan boshqasiga tezda tarqalishi mumkin. Bunday holatda, an’anaviy jinoyatlarning o‘zgacha hududiy va vaqtinchalik chegara bilan ta’minlanganligi kuzatiladi.

Jinoyatning realizatsiya usullari. An’anaviy jinoyatlar, masalan, o‘g‘irlik, bosqinchilik, yoki kiritishlar odatda **jismoniy vositalar** orqali amalga oshiriladi. Ularning qurbonlari bevosita jinoyatchi bilan muloqotda bo‘ladi, va jinoyatni sodir etish uchun ko‘plab holatlarda faqatgina jismoniy kuch ishlatish talab etiladi. Bunda jinoyatning oqibatlari ko‘pincha bevosita ko‘rinadi, va bu jarayonlar odatda xodimlar yoki guvohlar tomonidan kuzatiladi.

Kiberjinoyatlar esa, o‘z navbatida, **raqamli vositalar** orqali amalga oshiriladi va ular ko‘pincha kompyuter tarmoqlari, internet, mobil qurilmalar, elektron pochta va boshqa raqamli platformalardan foydalangan holda sodir etiladi. **Ma’lumotlar, parollar, shaxsiy ma’lumotlar** va boshqa raqamli resurslar jinoyatning asosiy ob’ekti bo‘lib xizmat qiladi. Shu sababli,

kiberjinoyatlar koʻpincha insonning jismoniy mavjudligini talab qilmaydi va masofadan turib ham amalga oshirilishi mumkin.

Jinoyatchining shaxsiyati va faoliyati. Kiberjinoyatlarni amalga oshiradigan shaxslar koʻpincha **an'anaviy jinoyatchilardan** farq qiladi. An'anaviy jinoyatlarda jinoyatchilar koʻpincha oʻzlarining jismoniy qobiliyatlari, kuch ishlatish yoki jismoniy hiyla-nayranglardan foydalanadi. Kiberjinoyatchilar esa, oʻzlarining mahoratini va bilimlarini axborot texnologiyalarida qoʻllaydi. Kiberjinoyatchilar uchun zarur boʻlgan asosiy qobiliyatlar — **kompyuter tarmoqlarini bilish**, **dasturlash**, **ma'lumotlarni tahlil qilish** va **axborot xavfsizligi**ga oid bilimlardir.

Kiberjinoyatlarning **avtomatlashtirilgan jarayonlar** orqali amalga oshirilishi mumkin. Masalan, botnetlar yordamida, jinoyatchi avtomatik tarzda oʻnlab, yuzlab yoki minglab qurilmalarga zarar yetkazishi mumkin. Bu esa, an'anaviy jinoyatlarga qaraganda, **tezlik** va **masshtabdagi oʻzgarishlar**ni yaratadi, bu esa koʻplab qurbonlarga zarar yetkazishga olib keladi.

Yuridik muammolar va yurisdiktsiya. Kiberjinoyatlar va **an'anaviy jinoyatlar** oʻrtasidagi farqlarni belgilashda huquqiy masalalar alohida oʻrin tutadi. An'anaviy jinoyatlar uchun huquqiy me'yorlar aniq belgilangan va ular odatda **milliy** qonunlar bilan boshqariladi. Kiberjinoyatlar esa koʻpincha **global** va **transchegaraviy** xarakterga ega boʻlib, bir nechta davlatlarning hududiga ta'sir qilishi mumkin. Bu esa xalqaro huquq va huquqiy yordam masalalarini oʻz ichiga oladi.

Kiberjinoyatlar tufayli, ayniqsa, **kompyuter tarmoqlaridan foydalanish** va **ma'lumotlarni uzatish** bilan bogʻliq boʻlgan turli huquqiy me'yorlarning kelib chiqishi kerak boʻlgan yangi masalalar mavjud. Bunday holatlar uchun milliy va xalqaro darajada yangi qonunchiliklarni ishlab chiqish va amalga oshirish zarurati mavjud.

Xulosa qilib aytganda, Kiberjinoyatlar va an'anaviy jinoyatlar oʻrtasidagi farqlarni tahlil qilish, kiberjinoyatlarning xususiyatlarini toʻliq tushunishga yordam beradi. Kiberjinoyatlar oʻzining **global** va **masofaviy** xususiyatlari bilan an'anaviy jinoyatlardan ajralib turadi. Shu bilan birga, ular nafaqat jinoyatchining oʻziga, balki global axborot tizimlariga, iqtisodiyotga va ijtimoiy tuzilmalarga jiddiy ta'sir koʻrsatadi. Bu farqlarni hisobga olib, kiberjinoyatlarga qarshi samarali kurash strategiyalarini ishlab chiqish va ularning ijtimoiy, huquqiy va iqtisodiy ta'sirlarini minimallashtirish imkoniyati yaratiladi.

Jinoyat maydonining fizik emas, virtual xarakteri. Kiberjinoyatlarning an’anaviy jinoyatlardan ajralib turadigan eng muhim xususiyatlaridan biri, ularning **virtual** va **raqamli maydonda** sodir bo‘lishidir. An’anaviy jinoyatlar odatda jismoniy makon yoki hududda amalga oshiriladi, ya’ni jinoyat sodir bo‘lishi uchun jinoyatchi va qurbon o‘rtasida to‘g‘ridan-to‘g‘ri muloqot yoki mavjudlik zarur bo‘ladi. Bunday jinoyatlarda, jismoniy joy, vaqt va jinoyatni amalga oshirishning aniq joyi ko‘pincha huquqiy baholashni osonlashtiradi. Shu bilan birga, kiberjinoyatlar, **virtual va raqamli muhitda** sodir bo‘lishi bilan ajralib turadi, va bu esa kiberjinoyatchilikka xos yangi yuridik va texnologik murakkabliklarni keltirib chiqaradi.

Virtual maydonning tabiati va uning huquqiy ahamiyati. Virtual maydon deb, asosan, **internet tarmoqlari**, **kompyuter tizimlari**, **ma’lumotlar bazalari** va boshqa raqamli platformalardan tashkil topgan, geografik yoki jismoniy chegaralar bilan cheklanmagan makon tushuniladi. Kiberjinoyatlar shu maydonlarda sodir bo‘ladi, bu esa ularni an’anaviy jinoyatlardan ajratib turadi. **Kompyuter tarmoqlari** yoki **raqamli tizimlar** orqali amalga oshirilgan jinoyatlar, jinoyatning sodir bo‘lgan joyi haqida aniq geosiyosiy axborot berolmaydi. Bunday holatda, kiberjinoyatchilar bir davlat hududidan boshqa davlat hududiga osonlik bilan o‘ta olishlari va jinoyatni boshqalar tomonidan sezilmasdan amalga oshirishi mumkin.

Shu sababli, kiberjinoyatlar virtual maydonda sodir bo‘lgani uchun, ular huquqiy nuqtai nazardan **yurisdiktsiya** masalasini murakkablashtiradi. Chunki har bir davlat o‘z hududidagi jinoyatlar uchun javobgarlikni ta’minlashga harakat qiladi, ammo virtual maydon chegarasiz bo‘lganligi sababli, jinoyatning qayerda sodir bo‘lishini aniqlash va bu yerda qonunlarni qo‘llash murakkablashadi.

Virtual jinoyatlarning sodir bo‘lish mexanizmi. Kiberjinoyatlar amalga oshiriladigan virtual maydonning o‘ziga xos xususiyatlaridan biri, **raqamli vositalar** va **axborot texnologiyalaridan foydalanish**dir. Jinoyatchi, fizikaning amaliy maydonida bo‘lmagan holda, **kompyuter tizimlari**, **mobil qurilmalar**, **internet tarmoqlari** yoki **bulutli texnologiyalar** orqali jinoyatni amalga oshirishi mumkin. Bu holatda, jinoyatchi uchun hech qanday jismoniy resurs kerak emas. Uning bunday jinoyatlarni sodir etishi uchun zarur bo‘lgan yagona narsa — bu texnik vositalar va internetga kirish imkoniyati.

Virtual maydonning yana bir muhim xususiyati shundaki, jinoyatning **fizik izlari** deyarli qolmaydi. Agar an’anaviy jinoyatda, jinoyatchining **fizik ishi** (masalan, gunohni sodir qilish vaqtida qoldirilgan izlar, shubhali guvohlar va boshqalar) bo‘lishi mumkin bo‘lsa, kiberjinoyatlarda bunday izlarni aniqlash juda qiyin bo‘ladi. Buning o‘rniga, **elektron izlar** — internetga kirishdagi IP-manzillar, serverlar orqali o‘tkazilgan ma’lumotlar, tizimning saqlangan log fayllari va boshqa raqamli ma’lumotlar ko‘pincha kiberjinoyatlarni aniqlashda yordam beradi.

Kiberjinoyatlarning anonimlik va masofaviylik xususiyati. Kiberjinoyatlar, an’anaviy jinoyatlardan farqli ravishda, **anonimlik** va **masofaviylik** xususiyatlariga ega. Jinoyatchilar internet va raqamli texnologiyalarni ishlatish orqali o‘z kimligini yashirishlari mumkin. Masalan, **IP-manzillarni yashirish**, **VPN (Virtual Private Network)** yoki **proksi-serverlar** yordamida jinoyatchi o‘z joylashuvini o‘zgartirishi va jinoyatni sodir etishi mumkin. Bu esa, jinoyatni amalga oshirgan shaxsni aniqlashni sezilarli darajada qiyinlashtiradi.

Shuningdek, kiberjinoyatlarning **masofaviy** xususiyati ham muhimdir. Jinoyatni sodir etish uchun jinoyatchi va qurbonning jismoniy yaqinligi zarur emas. Jinoyatni bir davlatda yashovchi kiberjinoyatchi boshqa davlatda yashovchi qurbonning tizimiga kiritib, ma’lumotlarni o‘g‘irlashi yoki zarar yetkazishi mumkin. Bu holatda, jinoyatchi va qurbon o‘rtasida hech qanday jismoniy muloqot bo‘lmaydi, lekin jinoyat hali ham sodir bo‘ladi.

Huquqiy va ijtimoiy muammolar. Jinoyat maydonining **virtual xarakteri** kiberjinoyatlar bilan bog‘liq bo‘lgan huquqiy va ijtimoiy muammolarni keltirib chiqaradi. Kiberjinoyatlarning sodir bo‘lishi uchun geografik chegaralar zarur emas, shuning uchun ularni **yuridik nazorat** qilishda xalqaro darajada yangi tizimlar va mexanizmlar zarur bo‘ladi. Kiberjinoyatchilar ko‘pincha o‘zlarining jinoyatlarini chet elda amalga oshiradilar, bu esa jismoniy joy va huquqiy yuridik jarayonlarning o‘rtasidagi uzilishlarni keltirib chiqaradi.

Bundan tashqari, virtual maydonning tasiri **iqtisodiy** va **ijtimoiy** sohalarda ham o‘z aksini topadi. Kiberjinoyatlar nafaqat shaxsiy ma’lumotlar yoki moliyaviy mablag‘larni o‘g‘irlash, balki mamlakatlar orasida axborot urushlarini keltirib chiqarishi mumkin. Masalan, **kiberhujumlar** orqali davlatlar o‘zaro ma’lumotlarni o‘g‘irlamoqda yoki tashqi siyosiy muammolarni hal etishga harakat qilmoqdalar.

Xulosa qilib aytganda, Kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlarni aniqlashda, eng katta e’tibor **virtual maydon**ning xususiyatlariga qaratilishi kerak. Jinoyatning **fizik emas, balki virtual xarakteri** kiberjinoyatlarni alohida sinfga kiritadi va bu holat ularni tahlil qilishni va ularga qarshi kurashish choralarini ishlab chiqishni qiyinlashtiradi. Kiberjinoyatlar faqatgina yangi texnologiyalarni talab qilmaydi, balki ularga qarshi kurashish uchun yangicha huquqiy, iqtisodiy va ijtimoiy mexanizmlar ishlab chiqishni ham talab etadi. Bu esa, o‘z navbatida, xalqaro hamkorlik va yangi qonunchilik tizimlarini talab qiladi.

Ishtirokchilar anonimligi va isbotlashdagi murakkablik. Kiberjinoyatlarning boshqa an’anaviy jinoyatlardan eng katta farqlaridan biri bu jinoyatlarni amalga oshirayotgan ishtirokchilarning **anonimligi**dir. Anonimlik, o‘z navbatida, kiberjinoyatlar uchun isbotlash jarayonlarini murakkablashtiradi, chunki jinoyatning kim tomonidan va qanday amalga oshirilgani haqida aniq dalillarni taqdim etish ko‘pincha qiyin bo‘ladi. Kiberjinoyatlarning xususiyatlari va raqamli muhitda amalga oshirilishi, ularni **jismoniy mavjudlik**dan ajratib turadi va jinoyatchilarni aniq aniqlashni juda qiyinlashtiradi. Shuningdek, **anonimlik** va **masofaviylik**ning ta’siri, ishtirokchilarning kimligini aniqlashni, jinoyatni sodir etgan shaxsni ta’qib qilishni va jazolashni murakkablashtiradi.

Kiberjinoyatlarda anonimlikning ahamiyati. Kiberjinoyatlar sodir bo‘lish jarayonida, jinoyatchilar o‘z kimligini yashirishlari uchun turli usullarni qo‘llashlari mumkin. **IP-manzillarni yashirish**, **VPN (Virtual Private Network)** texnologiyalari, **proxy-serverlar** va boshqa anonimlashtirish vositalari kiberjinoyatchilarga o‘z joylashuvini va kimligini yashirish imkonini beradi. Ushbu vositalar yordamida jinoyatchilar o‘zlarining haqiqiy identifikatsiyasini qiyinlashtiradi va ular o‘z jinoyatlarini ko‘plab davlatlarda sodir qilib, xech qanday to‘g‘ridan-to‘g‘ri geosiyosiy aloqalar qoldirmasdan o‘z ishtirokini yashirishi mumkin.

Anonimlik, kiberjinoyatchilarga shuningdek, jinoyatni masofadan amalga oshirish imkoniyatini yaratadi. Bunday holda, jinoyatni sodir etgan shaxs va qurbon o‘rtasida hech qanday jismoniy muloqot bo‘lmaydi. Buning natijasida jinoyatni amalga oshirgan shaxsning kimligini aniqlash juda mushkul bo‘ladi, chunki hech qanday jismoniy dalil yoki to‘g‘ridan-to‘g‘ri guvohlar mavjud emas. Bu anonimlik jinoyatchilarga raqamli tizimlardan samarali foydalanish imkonini beradi va ular o‘z jinoyatlarini qoplashni ancha osonlashtiradi.

Isbotlashdagi murakkabliklar. Ishtirokchilarning anonimligi, kiberjinoyatlarni isbotlashni va jinoyatchini ta’qib qilishni qiyinlashtiradi. An’anaviy jinoyatlarda, masalan, **o‘g‘irlik** yoki **bosqinchilik** kabi jinoyatlar sodir etilgan joyda to‘g‘ridan-to‘g‘ri dalillar, guvohlar yoki jismoniy izlar qoldiradi, bu esa ishtirokchilarni aniqlash va jinoyatni isbotlash jarayonini nisbatan osonlashtiradi. Kiberjinoyatlarda esa, bu jismoniy dalillar deyarli mavjud emas, chunki jinoyat **elektron tizimlar** orqali amalga oshiriladi va har bir faoliyat **raqamli izlar** bilan cheklanadi.

Raqamli izlarning o‘ziga xos xususiyati, ular ko‘pincha **dinamik** va o‘zgarmas bo‘lmasligi mumkin. Misol uchun, jinoyatchining IP-manzili yoki foydalangan elektron manzili osonlik bilan o‘zgartirilishi mumkin, bu esa jinoyatni isbotlashni yanada murakkablashtiradi. Bundan tashqari, **kriptografiya** va boshqa xavfsizlik vositalaridan foydalanish, jinoyatni amalga oshirish jarayonida iz qoldirmaslikka yordam beradi. Shu sababli, ishtirokchilarni aniq aniqlash va jinoyatning kim tomonidan amalga oshirilganligini tasdiqlashda huquqni muhofaza qiluvchi organlar va sudlar uchun sezilarli qiyinchiliklar yuzaga keladi.

Raqamli izlar va ularning isbotdagi roli. Kiberjinoyatlarni isbotlashda **raqamli izlar** juda muhim rol o‘ynaydi. Bular **log-fayllar**, **IP-manzillar**, **serverlarda saqlangan ma’lumotlar** va boshqa raqamli ko‘rsatkichlarni o‘z ichiga oladi. Biroq, bu izlar ko‘pincha o‘zgartirilishi yoki manipulyatsiya qilinishi mumkin. Masalan, kiberjinoyatchi tizimga kirmoqchi bo‘lganida, o‘z harakatlarini yashirish uchun zarur bo‘lgan dasturiy ta’minotlardan foydalanishi mumkin. Shuningdek, **falsifikatsiya qilish** yoki **ochiq ma’lumotlarga kirish huquqidan foydalangan holda** izlarni o‘zgartirish mumkin.

Bundan tashqari, kiberjinoyatlarda **ko‘p bosqichli hujumlar** amalga oshiriladi, masalan, **phishing** (fraudulent e’lonlar orqali foydalanuvchilardan shaxsiy ma’lumotlarni olish), **DDoS (Distributed Denial of Service)** hujumlari, yoki **ransomware** (zararli dasturlar orqali tizimlarni qulflash) kabi harakatlar. Har bir bosqichda qoldirilgan raqamli izlar turli serverlar va platformalar orqali tarqalishi mumkin, bu esa jinoyatni izlashda **ko‘p qatlamli** va **tarqalgan** izlarni kuzatishga olib keladi.

Xalqaro huquqiy muammolar. Kiberjinoyatlarning anonimligi va isbotlashdagi murakkabliklar nafaqat milliy darajada, balki xalqaro miqyosda ham muammolarni keltirib chiqaradi. Xalqaro huquqiy tizimlar va muqobil

ekspert tizimlari koʻpincha **yurisdiktsiya** va **hududiy** cheklovlar bilan bogʻliq qiyinchiliklarga duch keladi. Kiberjinoyatchilar oʻzlarining faoliyatini bir davlatdan boshqasiga tezda koʻchirishlari mumkin, bu esa jinoyatni toʻgʻri isbotlash va jinoyatchini jinoiy javobgarlikka tortish uchun zarur boʻlgan malakali huquqiy mexanizmlar va xalqaro hamkorlikni talab qiladi.

Shuningdek, **anonimlikni** yanada kuchaytirgan texnologiyalar, masalan, **kripto-valyutalar** va **blockchain** tizimlari, kiberjinoyatlarni aniqlashda yangi **yuridik va texnologik** muammolarni keltirib chiqaradi. Bu texnologiyalar jinoyatchilarga oʻz faoliyatini anonim qilish imkoniyatini beradi, lekin shu bilan birga, huquqni muhofaza qiluvchi organlar uchun yangi yuridik vositalarni ishlab chiqishni talab qiladi.

Xulosa qilib aytganda, Kiberjinoyatlar va an’anaviy jinoyatlar oʻrtasidagi farqlarni oʻrganishda, ishtirokchilarning anonimligi va isbotlashdagi murakkabliklar alohida ahamiyatga ega. Anonimlik kiberjinoyatchilarga oʻz faoliyatlarini yashirish va ishtirokchilarning kimligini aniqlashni qiyinlashtirish imkonini beradi. Shu sababli, kiberjinoyatlar sodir etilayotgan virtual muhitda izlar qoldirish va jinoyatni aniqlash juda murakkab holga keladi. Bu, oʻz navbatida, kiberjinoyatchilikka qarshi kurashish uchun huquqiy tizimlarni modernizatsiya qilish va xalqaro hamkorlikni yanada kuchaytirishni talab qiladi.

Hududiy cheklovlarning yoʻqligi. Kiberjinoyatlar va an’anaviy jinoyatlar oʻrtasidagi eng muhim farqlardan biri **hududiy cheklovlarning yoʻqligi**dir. An’anaviy jinoyatlar, odatda, jismoniy hududda yoki ma’lum bir geografik hududda sodir boʻladi. Bu turdagi jinoyatlar qonuniy nuqtai nazardan aniq bir **yuridik hududda** va **geografik chegaralar ichida** sodir boʻlganligi sababli, ular oʻsha hududning ichki qonunlariga muvofiq sudga olinadi va jazolanadi. Bunday holatlarda jinoyatchining qayerda yashashini va jinoyatni qayerda sodir etganini aniqlash nisbatan oson boʻladi.

Biroq, kiberjinoyatlar oʻta **hududiy chegaralarga befarq** boʻlgan jinoyat turlarini tashkil etadi. Kiberjinoyatlar virtual muhitda sodir boʻlganligi sababli, ular **geografik yoki davlat chegaralarini** tanimaydi. Jinoyatni amalga oshirgan shaxs va jinoyatning qurboni oʻrtasidagi masofa, qaysi davlatda yashayotganligi yoki qanday qonunlarga amal qilishi hech qanday ahamiyatga ega emas. Kiberjinoyatlar **internet** yoki **raqamli tizimlar** orqali sodir boʻlishi mumkin va ular uchun jismoniy joy yoki davlat chegaralari mavjud emas.

Geografik chegaralarning yo‘qligi. Kiberjinoyatlarning hududiy cheklovlarsizligi global miqyosda hal qilishni talab qiladigan muammolarga olib keladi. Misol uchun, kiberjinoyatchi bir davlatdan boshqa davlatga hujum qilib, ma’lumotlarni o‘g‘irlaydi yoki zararli dasturlarni tarqatadi. Bunday holatlarda jinoyatni sodir etish joyini aniqlash juda qiyin bo‘ladi, chunki jinoyat virtual muhitda sodir bo‘ladi va jinoyatchi o‘z joylashuvini yashirish uchun zamonaviy texnologiyalardan foydalanishi mumkin.

Xalqaro huquq nuqtai nazaridan, kiberjinoyatlarning **hududiy chegaralarning yo‘qligi** bu jinoyatlarning qayerda sodir bo‘lganligini aniqlashda katta qiyinchiliklar yaratadi. Agar an’anaviy jinoyatlarda jinoyat sodir bo‘lgan joyda sud yuridik javobgarlikni belgilasa, kiberjinoyatlarda hududiy chegaralar o‘zgarganligi sababli, bu holatlarning **yuridik ta’siri** va **javobgarligi** ko‘plab davlatlar o‘rtasida kelishmovchiliklarga olib kelishi mumkin. Kiberjinoyatlarni amalga oshirgan shaxsning kimligini aniqlash, uning davlatdagi yoki global tarmoqdagi faoliyatini kuzatish uchun ko‘plab yangi yuridik mexanizmlar ishlab chiqilishi zarur.

Yurisdiktsiya va xalqaro hamkorlik muammolari. Kiberjinoyatlarning hududiy cheklovlarining yo‘qligi, **yurisdiktsiya** masalasini murakkablashtiradi. **Yurisdiktsiya** — bu davlatning jinoyatlarni o‘z hududida amalga oshirgan shaxslarga nisbatan huquqiy javobgarlikni belgilash huquqidir. An’anaviy jinoyatlarda, masalan, bir odam jinoyatni o‘z davlatining hududida amalga oshirgan bo‘lsa, bu davlat uning jinoiy javobgarligini to‘liq nazorat qilishi mumkin. Biroq, kiberjinoyatlar virtual muhitda sodir bo‘lganligi sababli, ularning **yurisdiktsiya** masalalari, ayniqsa, **ko‘p davlatlarda amalga oshirilgan hujumlar** bo‘lganda, hal etilishi qiyin bo‘ladi.

Misol uchun, kiberjinoyatni amalga oshirgan shaxsning IP-manzili yoki boshqa raqamli izlari bir davlatda bo‘lishi mumkin, ammo jinoyatning ta’siri boshqa bir davlatda seziladi. Bu esa, jinoyatchini ta’qib qilish va jinoiy javobgarlikka tortish jarayonini murakkablashtiradi. Bunday holatlar ko‘pincha **yuridik ko‘prikla**rni yoki **xalqaro kelishuvlarni** talab qiladi. Hozirgi vaqtda kiberjinoyatlar bilan kurashishda xalqaro hamkorlik, jumladan, turli davlatlar o‘rtasida axborot almashish, to‘g‘ridan-to‘g‘ri adliya tizimlarining integratsiyasi va **o‘rganish tizimlari** ustida hamkorlik qilish muhim ahamiyatga ega.

Kiberjinoyatlarni jinoyat deb e’tirof etishning qiyinchiliklari. Kiberjinoyatlar davlatlar o‘rtasida o‘zaro kelishuvlar, qonunlar va standartlar farqlari tufayli **xalqaro jinoyat sifatida tan olinmaydi**. Aksariyat davlatlar kiberjinoyatlarni **mahalliy darajada** jinoyat deb tan oladilar, lekin ular xalqaro miqyosda jinoyat sifatida ko‘rilmasligi mumkin. Shu bilan birga, kiberjinoyatlarni hukm qilishda ko‘plab huquqiy tizimlar orasida farqlar mavjud. Masalan, bir davlatda kiberjinoyat sifatida ko‘rilgan bir harakat boshqa bir davlatda shu darajada jiddiy jinoyat deb e’tirof etilmasligi mumkin. Bunday farqlar kiberjinoyatlar bilan bog‘liq muammolarni hal qilishni murakkablashtiradi va **xalqaro huquq**ni rivojlantirish zaruratini keltirib chiqaradi.

Kiberjinoyatlar va xalqaro huquqiy mexanizmlar. Kiberjinoyatlar hududiy cheklovlarning yo‘qligi, xalqaro huquqiy mexanizmlarning samaradorligini baholashni talab qiladi. **BMT**, **Evropa Ittifoqi**, **Interpol** kabi xalqaro tashkilotlar va ko‘plab davlatlar kiberjinoyatlarni oldini olish uchun o‘zaro hamkorlik qilishmoqda. Bunday xalqaro tashkilotlar tomonidan ishlab chiqilgan standartlar, konvensiyalar va shartnomalar orqali davlatlar kiberjinoyatlar bilan kurashish uchun birlashmoqda.

Misol uchun, **BMTning Kiberjinoyatlar to‘g‘risidagi Konvensiyasi** yoki **Yevropa Ittifoqining Kiberjinoyatlar haqidagi Shartnomasi** kabi xalqaro huquqiy hujjatlar kiberjinoyatlarni oldini olish, jinoyatchilarni ta’qib qilish va ular bilan samarali kurashish uchun birgalikda harakat qilishni nazarda tutadi. Bu huquqiy mexanizmlar kiberjinoyatlarning **hududiy cheklovlaridan** ajralib chiqishi va ularni xalqaro miqyosda ko‘rib chiqishni talab qiladi.

Xulosa qilib aytganda, Kiberjinoyatlarning **hududiy cheklovlarning yo‘qligi** kiberjinoyatchilikni an’anaviy jinoyatlardan ajratib turadi va bu holatlarning tahlilini, hal etilishini va jazolashni murakkablashtiradi. Kiberjinoyatchilar hududiy chegaralardan befarq holda jinoyatlarni amalga oshirishlari mumkin, bu esa global miqyosda yangi yuridik mexanizmlar va xalqaro hamkorlikni talab qiladi. Kiberjinoyatlarning geografik yoki hududiy chegaralarga befarq bo‘lishi, o‘z navbatida, jinoyatlarni aniqlash va jazolashda bir nechta yuridik va texnologik qiyinchiliklarni keltirib chiqaradi. Shu sababli, kiberjinoyatlarni oldini olish va ularga qarshi kurashishda xalqaro miqyosdagi huquqiy tizimlarning yaxshilanishi va davlatlar o‘rtasidagi hamkorlikni rivojlantirish zarurdir.

1.4. Kiberjinoyatlarni aniqlash va dalillarni huquqiy jihatdan rasmiylashtirish

Kiberjinoyatlar sohasida zamonaviy texnologiyalar va raqamli infratuzilmaning rivojlanishi bilan birga, ushbu jinoyatlar ta’rifi, aniqlanishi va ularning huquqiy jihatdan rasmiylashtirilishi masalalari yanada murakkablashgan. **Kiberjinoyatlarni aniqlash** va ularning dalillarini to‘plash, huquqiy jihatdan rasmiylashtirish o‘ta muhim va o‘ziga xos talablarni o‘rinlashtiradi. Chunki kiberjinoyatlarning asosan **raqamli muhitda** amalga oshirilishi, ko‘plab **anonimlik** va **hududiy cheklovlarning yo‘qligi** kabi yangi omillarni keltirib chiqaradi. Shuning uchun, kiberjinoyatlarni aniqlash va dalilni to‘plashda an’anaviy jinoyatlarga nisbatan alohida yondashuvlar va metodologiyalar zarur.

Kiberjinoyatlarni aniqlash jarayoni, odatda, **kompyuter tizimlarining** himoyasini buzish, **ma’lumotlarni o‘g‘irlash**, **zararli dasturlarni tarqatish** kabi holatlar bilan bog‘liq bo‘ladi. Bunday jinoyatlar **elektron tizimlar**da sodir bo‘lishi sababli, **raqamli izlar**ni to‘plash, **texnologik vositalar** yordamida ularni **huquqiy jihatdan rasmiylashtirish** talablari kiberjinoyatlarni aniqlashdagi eng katta qiyinchiliklarni yuzaga keltiradi. Bunday jarayonlarda **dalil sifatida raqamli ma’lumotlar**, **log-fayllar**, **IP-manzillar**, **serverlarda saqlangan ma’lumotlar** va boshqa hujjatlar muhim ahamiyatga ega. Ammo, raqamli dalillarni to‘plash va ulardan foydalanishda **maxfiylikni ta’minlash**, **tasdiqlashning huquqiy asoslari** va **dalilning yuridik kuchi** kabi masalalar alohida diqqatga sazovordir.

Shu o‘rinda, kiberjinoyatlarni aniqlashda yuridik tizimlarning, ayniqsa, **xalqaro** miqyosda bir-biri bilan muvofiqligi, axborot almashishdagi ishonchli mexanizmlar va **yuridik hujjatlar**ning ahamiyati ortadi. Xalqaro huquqiy tizimlar, ayniqsa, kiberjinoyatlarni oldini olish va jinoyatchilarga qarshi kurashishda birlashish zaruriyatini taqozo etadi. Kiberjinoyatlarni aniqlashning **huquqiy jihatlari**ni to‘g‘ri tasdiqlash va dalilni rasmiylashtirish, sud tizimining samarali ishlashiga yordam beradi, shu bilan birga, **kiberjinoyatchilikka qarshi kurashishda** ko‘p davlatlar o‘rtasidagi yuridik hamkorlikni rivojlantirishni ta’minlaydi.

Bundan tashqari, **dalillarni to‘plash va ularni rasmiylashtirish** jarayonida jinoyatni aniqlashga oid har bir harakatning **huquqiy shakllari**, **muvofiqligi** va **ishonchliligi** yuqori bo‘lishi kerak. Bu jarayonda kiberjinoyatchilarning faoliyatini aniqlash va o‘z ishtirokini huquqiy jihatdan

isbotlash uchun maxsus texnologik va yuridik vositalardan foydalanish muhim hisoblanadi. Shu bilan birga, **xalqaro hamkorlik** va **xalqaro shartnomalar** orqali jinoyatlarni aniqlashning to‘g‘ri mexanizmlari va dalilni rasmiylashtirishda yetarli **huquqiy kafolatlar** yaratish zarurati tug‘iladi.

Xulosa qilib aytganda, Kiberjinoyatlarni aniqlash va dalillarni huquqiy jihatdan rasmiylashtirish masalalari nafaqat texnologik jihatdan, balki yuridik tizimlar o‘rtasida samarali hamkorlik va **xalqaro yuridik mexanizmlar**ni ishlab chiqishni talab qiladi. Raqamli tizimlarda sodir bo‘ladigan jinoyatlarning o‘ziga xos xususiyatlarini hisobga olgan holda, to‘plangan dalillarni **huquqiy asosda tasdiqlash** va ular bilan bog‘liq jarayonlarni **an’anaviy huquqiy tizimlar** bilan uyg‘unlashtirish juda muhimdir.

Elektron dalillarning texnik xususiyatlari. Kiberjinoyatlar bilan bog‘liq dalillarni to‘plash va rasmiylashtirishda, **elektron dalillar**ning texnik xususiyatlari eng muhim masalalardan biridir. Raqamli tizimlarda sodir bo‘lgan jinoyatlarni aniqlashda to‘plangan dalillar faqatgina texnologik jihatdan to‘g‘ri, balki huquqiy nuqtai nazardan ham ishonchli bo‘lishi kerak. Elektron dalillarning o‘ziga xos texnik xususiyatlari, ularni **to‘plash**, **saqlash**, **tahlil qilish** va **taqdim etish** jarayonlarini murakkablashtiradi. Shu bilan birga, bu dalillarni **huquqiy rasmiylashtirish**da ishonchlilik va isbotlash talablarini to‘liq qondirishi zarur.

Elektron dalillarning xususiyatlari. Elektron dalillar, odatda, **raqamli ma’lumotlar** sifatida taqdim etiladi va ular **fizik jihatdan mavjud emas**. Ular **digital shaklida** saqlanadi, masalan, **log-fayllar**, **IP-manzillar**, **e-mail xabarlar**, **video va audio yozuvlar**, **serverlardan olingan ma’lumotlar** va boshqa raqamli ko‘rinishdagi hujjatlar. Bunday dalillarni to‘plashda eng katta qiyinchiliklardan biri – bu ma’lumotlarning **o‘zgarmasligini** ta’minlash va ularning **dalil sifatida qabul qilinishini** kafolatlashdir**.**

Elektron dalillarni tekshirishda qo‘llaniladigan texnik vositalar va metodlar turli xususiyatlarga ega. Ulardan ba’zilari quyidagilardan iborat:

- **Hash-funksiyalar** – Elektron fayllarni **yuzaga kelgan o‘zgarishlarni aniqlash** uchun ishlatiladi. Hash-funksiyalar ma’lumotning o‘zgarishsizligiga ishonch hosil qilish imkonini beradi, chunki ular har bir faylga noyob **hash qiymatini** beradi. Bu qiymatning o‘zgarishi faylning o‘zgarganligini bildiradi.
- **Tegishli metadata** – Fayllar va hujjatlar bilan bog‘liq qo‘shimcha ma’lumotlar, masalan, yaratilgan vaqt, faylning o‘zgartirilganligi, muallifi va boshqalar. Bu ma’lumotlar dalil sifatida muhim rol o‘ynaydi, chunki ular

jinoyatni amalga oshirgan shaxsning faoliyatiga oid qo‘shimcha ma’lumotlar beradi.

- **Raqamli imzolar** – Elektron xujjatlarning **yuridik ahamiyatini** tasdiqlovchi elementlar bo‘lib, bu imzolar ma’lumotning haqiqiyligini va o‘zgarmasligini isbotlaydi.
- **IP-manzillar va tarmoq izlari** – Internet orqali amalga oshirilgan kiberjinoyatlarda, **IP-manzil** va **tarmoq izlari**ni to‘plash juda muhimdir. Bular jinoyatchining qayerdan va qanday tarmoqdan foydalanganligini aniqlashga yordam beradi. Shu bilan birga, IP-manzilning o‘zgarishi yoki anonimlashtirish vositalari yordamida jinoyatchi o‘z izlarini yashirishga harakat qilishi mumkin, bu esa tekshiruvni murakkablashtiradi.
- **Zararli dasturlar va kodlar** – Kiberjinoyatlar ko‘pincha **zararli dasturlar** yoki **viruslar** yordamida amalga oshiriladi. Bunday dasturlarni tahlil qilish, ularning qanday ishlashini va qanday ma’lumotlarni o‘g‘irlaganini aniqlash uchun zarur bo‘lgan texnik vositalar va metodologiyalar mavjud. Dastur kodining tahlili, ayniqsa, kiberhujumni amalga oshirgan shaxsning harakatlarini tushunish uchun juda muhimdir.

Elektron dalillarning saqlanishi va himoyasi. Elektron dalillarning texnik jihatidan ishonchli bo‘lishi uchun ularning **saqlanishi va himoyasi** juda muhim ahamiyatga ega. Bunday dalillarni saqlashda quyidagi talablar muhimdir:

- **Saqlash vositalarining himoyasi** – Elektron dalillarni saqlash uchun qo‘llaniladigan vositalar, masalan, qattiq disklar, serverlar yoki bulutli tizimlar, zarur hollarda himoyalangan bo‘lishi kerak. Bu vositalarda ma’lumotlarning **o‘zgarmasligi** va **yo‘qolib ketmasligi** ta’minlanishi lozim.
- **Zaxira nusxalarini yaratish** – Elektron dalillarning yo‘qolishini oldini olish uchun ularning zaxira nusxalari yaratiladi. Bu zaxira nusxalari o‘zgarmas va asl nusxaga muvofiq bo‘lishi kerak. Zaxira nusxalarining ham **ruxsatsiz o‘zgartirilishini** oldini olish uchun kerakli texnik chora-tadbirlar ko‘riladi.
- **Saqlash joylarining xavfsizligi** – Elektron dalillarni saqlash joylari xavfsiz bo‘lishi, **shifrlash** usullari orqali himoyalanishi kerak. Boshqa so‘z bilan aytganda, dalillarning **maxfiyligi** va **butunligini** ta’minlash uchun ularni himoya qilish zarur.
- **Elektron dalillarning tahlil qilinishi.** Elektron dalillarni tahlil qilishda muhim texnik xususiyatlar quyidagilarni o‘z ichiga oladi:

- **Tahlil qilish metodikasi** – Raqamli dalillarni to‘plashdan so‘ng, ularni to‘g‘ri tahlil qilish va tekshirish uchun maxsus metodikalar qo‘llaniladi. Bu metodikalar dalillarni huquqiy qabul qilish uchun zarur bo‘lgan shaklda tasdiqlanishini ta’minlaydi.
- **Kengaytirilgan tahlil vositalari** – Elektron dalillarni tahlil qilishda **kiberxavfsizlik dasturlari** va boshqa maxsus tahlil vositalaridan foydalanish muhimdir. Bu vositalar orqali zaruriy **iqtisodiy, texnik va yuridik** tahlillar amalga oshiriladi.
- **Dalilga tegishli xatoliklarni aniqlash** – Elektron dalillarni tahlil qilishda, ularning haqiqiyligini tasdiqlashdan oldin, **xatoliklar** va **o‘zgartirishlar** aniqlanishi lozim. Bu jarayonda, dalillarning **ishonchliligi** va **yuridik qadrini** belgilash uchun muhim qadamlar amalga oshiriladi.

Elektron dalillarning huquqiy jihatdan tasdiqlanishi. Elektron dalillarning huquqiy jihatdan tasdiqlanishi, ular to‘plangan paytda ham, keyinchalik sud jarayonida ham muhimdir. Elektron dalillarni huquqiy jihatdan tasdiqlash jarayoni quyidagilarni o‘z ichiga oladi:

- **Dalilni rasmiylashtirish** – Elektron dalillarni sudda qabul qilishdan oldin, ularni to‘g‘ri rasmiylashtirish zarur. Bu jarayonda dalilning **sifatli** va **to‘g‘ri saqlanganligi**ni isbotlash uchun texnik hujjatlar tayyorlanadi.
- **Dalilning ishonchliligi** – Elektron dalillarni sudda qabul qilish uchun, ularning **ishonchliligi** tasdiqlanishi lozim. Bu tasdiqlash jarayonida, yuqoridagi texnik vositalardan foydalanib, dalillarning **yuridik kuchi** isbotlanadi.

Xulosa qilib aytganda, **Elektron dalillarning texnik xususiyatlari**, kiberjinoyatlarni aniqlash va ularga huquqiy ta’sir ko‘rsatish jarayonida muhim rol o‘ynaydi. Bu dalillarni to‘plash, saqlash, tahlil qilish va sudga taqdim etishning texnik jihatlari jiddiy e’tiborni talab qiladi. Elektron dalillarning **o‘zgarmasligi**, **ishonchliligi** va **maxfiyligini** ta’minlash, ularni **yuridik jihatdan tasdiqlash**da eng muhim masalalar hisoblanadi. Kiberjinoyatlar sohasidagi texnologik o‘zgarishlarni hisobga olgan holda, elektron dalillarning huquqiy ahamiyatini to‘g‘ri baholash va ularga asoslanib to‘g‘ri sud qarorlarini chiqarish hamda **xalqaro hamkorlik**ni rivojlantirish zarurati ortib bormoqda.

Digital forensika va dalil to‘plash texnologiyalari. Kiberjinoyatlar, asosan, **raqamli muhitda** amalga oshirilgan jinoyatlar bo‘lgani uchun, ularni aniqlash va ularga dalil to‘plashda an’anaviy jinoyatlarni aniqlash texnikalari

va usullaridan farqli ravishda maxsus yondashuvlar va texnologiyalarni qo‘llash zarur. Bu jarayonning samarali amalga oshirilishi uchun **digital forensika** va **dalil to‘plash texnologiyalari** katta ahamiyatga ega. Digital forensika – bu raqamli tizimlarda sodir bo‘lgan jinoyatlarni aniqlash, tekshirish va ularga oid dalillarni to‘plash, saqlash, tahlil qilish va yuridik jihatdan tasdiqlash bilan shug‘ullanuvchi ilmiy va amaliy soha hisoblanadi.

Digital Forensikaning asosiy vazifalari va vaziyatlari. Digital forensika, o‘zining mohiyati va amaliy ahamiyati bilan, ayniqsa, kiberjinoyatlar sohasida juda muhimdir. Bu soha, nafaqat **jinoyatlarni aniqlash** va **dalil to‘plash**, balki **dalilning yuridik tasdiqligi**ni ta’minlashga ham katta e’tibor qaratadi. Digital forensikaning asosiy vazifalari quyidagilardan iborat:

- **Dalilni to‘plash va saqlash** – Kiberjinoyatlar sodir bo‘lgan paytda, tizimlardan olingan ma’lumotlarning ishonchliligini ta’minlash zarur. Dalillarni to‘plashda ularning **o‘zgarmasligi** va **maxfiyligi**ni ta’minlash muhimdir. Bunga qadar foydalanilgan texnik vositalar va metodikalar quyidagi talablar bilan bog‘liq:
  - ✓ Dalilni to‘plash jarayonida ularni **ta’sir qilmaslik** va **o‘zgartirmaslik**;
  - ✓ Dalilni to‘plashda **huquqiy asos** va **ruxsatnoma**ning mavjudligi.
- **Dalilni tahlil qilish** – Dalillarni to‘plaganidan so‘ng, ular tahlil qilinadi. Tahlil jarayonida **ma’lumotlarning turini**, **manbasini** va **integrallik**ni aniqlash muhim ahamiyatga ega. **Tarmoq tahlili**, **dasturiy ta’minot tahlili**, **ma’lumotlar bazasi tahlili** va boshqa ko‘plab metodikalar qo‘llaniladi.
- **Dalilning yuridik ahamiyatini tasdiqlash** – Digital forensikaning eng muhim jihatlaridan biri, to‘plangan dalillarning **yuridik tasdiqligini** ta’minlashdir. Bu, dalilning ishonchliligi, uning originalligini va o‘zgarmasligini isbotlashni talab etadi. Shuning uchun **forensik audit** va **xarakteristik tahlil** muhim ahamiyatga ega.

Dalil to‘plash texnologiyalari. Kiberjinoyatlarni aniqlashda foydalaniladigan texnologiyalar, asosan, raqamli tizimlarning turli qatlamlarida faoliyat ko‘rsatadigan vositalardan iborat. Ular yordamida **zaruriy dalillar**ni to‘plash va **ma’lumotlarni saqlash** jarayoni quyidagi texnologik vositalar orqali amalga oshiriladi:

- **Forensik Dasturlar va Asboblar** – Digital forensika sohasida mavjud ko‘plab dasturlar va asboblar, jumladan, **EnCase**, **FTK (Forensic Toolkit)**, **X1 Social Discovery**, **Cellebrite** va boshqa dasturlar, kiberjinoyatlarni tekshirishda juda samarali vositalardir. Ushbu dasturlar yordamida turli turdagi ma’lumotlar, jumladan, **log-fayllar**, **disk izlari**, **e-mail ma’lumotlari** va boshqa **elektron hujjatlar**ni tahlil qilish mumkin. Ular ma’lumotlarni xavfsiz tarzda saqlash va tizimdan chiqarish jarayonida **dalilni o‘zgartirmaslik**ni ta’minlaydi.
- **Zararli Dasturlarni Tahlil Qilish** – **Malware (zararli dastur)** va **virus** tahlil qilish, kiberjinoyatlar bilan bog‘liq bo‘lgan dalil to‘plashning ajralmas qismidir. Bunda, tizimlar va qurilmalarda aniqlangan **zararli dasturlar**ni o‘rganish, ularning qanday ishlashini va qanday ma’lumotlarni o‘g‘irlaganini aniqlash zarur. Bu jarayonda, zararli dastur kodini tahlil qilish va uning **hujum usullarini** aniqlash uchun maxsus dasturlar va texnologiyalardan foydalaniladi.
- **Tarmoq Forensikasi** – Kiberjinoyatlar ko‘pincha internet tarmog‘i orqali amalga oshiriladi, shuning uchun **tarmoq forensikasi** bu jarayonda muhim rol o‘ynaydi. **Wireshark**, **Tcpdump** kabi vositalar yordamida tarmoq orqali amalga oshirilgan **malumot almashish jarayonlarini** aniqlash mumkin. Bu orqali, jinoyatni amalga oshirgan shaxsning **IP-manzilini** yoki **ma’lum bir tarmoqda sodir bo‘lgan harakatlarni** aniqlash mumkin.
- **Disk Forensikasi** – Disk forensikasi yordamida **hard disklar**, **SSD (solid-state disk)** yoki boshqa saqlash qurilmalarida **ma’lumotlarni tiklash**, **loglar** va **faylla**rni to‘plash mumkin. Bu jarayonda **write-blocker** texnologiyalaridan foydalanish, ya’ni diskga o‘zgartirish kiritmaslik, ma’lumotlarni o‘zgartirmaslik va saqlash jarayonini xavfsiz o‘tkazish zarur.

Forensik ma’lumotlarni saqlash va himoyasi. Dalillarning ishonchli va xavfsiz saqlanishi uchun, digital forensika jarayonida quyidagi **saqlash va himoya qilish** usullari qo‘llaniladi:

- **Saqlash Vositalari va Texnologiyalar** – Digital forensikada to‘plangan dalillarni xavfsiz saqlash uchun maxsus saqlash vositalari va texnologiyalar qo‘llaniladi. Bu saqlash vositalari, jumladan, **Zaxira nusxalarini yaratish**, **kriptografik usullar** yordamida ma’lumotlarni shifrlash va **RAID texnologiyalaridan** foydalanishni o‘z ichiga oladi.
- **Ruxsatnomalar va Xavfsizlik Protokollari** – Dalillarning saqlanish jarayonida ruxsatnomalar, huquqiy va xavfsizlik protokollari juda muhimdir.

Dalillarni saqlash joylariga kirishni faqat ruxsatnoma asosida amalga oshirish, tizimga kiritilgan har bir harakatni kuzatish, uning vaqtini va ma’lumotlar izini taqdim etish zarur.

Digital Forensika va xalqaro hamkorlik. Kiberjinoyatlar global miqyosda sodir bo‘lishi sababli, **digital forensika** jarayonlari ko‘pincha **xalqaro** miqyosda hamkorlikni talab etadi. Xalqaro huquqiy tizimlar, forensik ma’lumotlarni almashish, **yo‘riqnomalar** va **standartlar**ni ishlab chiqish bo‘yicha hamkorlikni kuchaytirishga intilmoqda. Bu jarayonning samarali amalga oshirilishi uchun, xalqaro me’yorlar va **yuridik asoslar** ishlab chiqilgan bo‘lishi kerak.

Xulosa qilib aytganda, Digital forensika va dalil to‘plash texnologiyalari, kiberjinoyatlar sohasida ishonchli va huquqiy ravishda tasdiqlangan dalillarni taqdim etish uchun zarur vositalar va usullardir. Ushbu texnologiyalar nafaqat jinoyatni aniqlash, balki dalillarning **yuridik tasdiqligini** ta’minlashda ham katta ahamiyatga ega. Kiberjinoyatlarni aniqlashda texnologik yondashuvlar va xalqaro hamkorlikni kuchaytirish, samarali forensik tahlillarni amalga oshirish imkonini beradi va shu bilan birga, kiberjinoyatlarni jazolashda hal qiluvchi omil hisoblanadi.

Sudga taqdim etiladigan dalillarning haqiqiyligini tasdiqlash. Kiberjinoyatlarni aniqlashda va ular bilan bog‘liq dalillarni sudga taqdim etishda, bu dalillarning **haqiqiyligi**ni isbotlash juda muhim. Kiberjinoyatlar, o‘zining tabiati va amalga oshirilish shakli bilan, an’anaviy jinoyatlardan farq qiladi. Bu esa dalil to‘plash va saqlash jarayonlarida qo‘llaniladigan usullarni maxsuslashtiradi. Sudda kiberjinoyatlar bo‘yicha dalil sifatida taqdim etilgan ma’lumotlar, to‘g‘ridan-to‘g‘ri jinoyatni tasdiqlovchi asos sifatida qabul qilinishi uchun, dalilning haqiqiyligi va ishonchliligi qat’iy ravishda tasdiqlanishi kerak.

Dalilning haqiqiyligini tasdiqlashning asosiy tamoyillari. Dalillarning sudda qabul qilinishi uchun ularning haqiqiyligini tasdiqlashga alohida e’tibor qaratish kerak. Haqiqiylikni tasdiqlashning asosiy tamoyillari quyidagilardan iborat:

- **Zarar ko‘rmaslik (Inviolability)** – Kiberjinoyatlar bilan bog‘liq dalillarni to‘plash jarayonida, har qanday manipulyatsiya yoki o‘zgartirish dalilni yo‘qotishiga yoki uning ishonchliligini kamayishiga olib keladi. Shuning uchun dalil to‘planganda va saqlanganda uning **integralligi** va **saqlanish holati**ni saqlash talab etiladi.

➢ **Xavfsiz saqlash (Security)** – Dalillarni saqlashda ularning xavfsizligini ta’minlash zarur. Buning uchun dalilni saqlash uchun **yopiq tizimlar** va **maxfiylikni ta’minlash mexanizmlari** qo‘llaniladi. Har bir saqlash amaliyoti huquqiy nuqtai nazardan tasdiqlanishi kerak, ya’ni dalilni har qanday tasodifiy yoki noxush ta’sirdan saqlash ta’minlanishi lozim.

➢ **Tizimatik rasmiylashtirish (Chain of Custody)** – Dalilni to‘plashdan tortib, uni sudga taqdim qilishgacha bo‘lgan barcha bosqichlar, jumladan, har bir shaxsning dalil bilan aloqasi va saqlash jarayonlari **yuridik jihatdan rasmiylashtirilishi** kerak. Har bir harakat va qaror **huquqiy asosda yozib borilishi** kerak, bu esa dalilning ishonchli ekanligini isbotlaydi.

Dalilni rasmiylashtirishda qo‘llaniladigan texnik usullar. Dalillarning haqiqiyligini tasdiqlashda qo‘llaniladigan texnik usullar va vositalar kiberjinoyatlar sohasidagi xatoliklarni kamaytirish va dalilni tasdiqlashda qo‘l keladi. Quyidagi texnik usullar muhim ahamiyatga ega:

➢ **Hash-funktsiyalar** – Dalil to‘plashda **hash-funktsiyalar** (masalan, MD5, SHA-1, SHA-256) yordamida ma’lumotlarning haqiqiyligi tekshiriladi. Hash-funktsiyasi ma’lumotlar blokidan olingan unikallikni ko‘rsatadi, va agar ma’lumot o‘zgargan bo‘lsa, hash qiymati ham o‘zgaradi. Bunda dalilning **integralligi**ni ta’minlashga xizmat qiladi.

➢ **Forensik Texnikalar** – **Forensik uskunalar** yordamida tizimlar va qurilmalardan olinadigan ma’lumotlar, aniq va tasdiqlangan texnik usullar orqali tekshiriladi. Dalil to‘planganda, tizimni o‘zgartirish yoki ustidan hukm qilish imkoniyatlari minimallashtiriladi, shuning uchun uskunalar va dasturiy ta’minotlar rasmiy xalqaro standartlarga mos bo‘lishi zarur.

➢ **Digital Signature (Raqamli Imzo)** – Dalilni rasmiylashtirishda **raqamli imzo** ham muhim ahamiyatga ega. Raqamli imzo, axborotning **haqiqiyligini** va **o‘zgarmasligini** isbotlaydigan vosita hisoblanadi. Raqamli imzolar ma’lum bir shaxsning tizimda mavjud bo‘lishini isbotlashga yordam beradi, shuningdek, bu imzo ma’lumotning tashqi ta’sirlar tomonidan o‘zgartirilmaganligini ta’minlaydi.

➢ **Zaxira nusxalari (Backup Copies)** – Dalilni xavfsiz saqlash uchun, tizimlardan va qurilmalardan olingan ma’lumotlarning zaxira nusxalari (backup copies) yaratish zarur. Bu, dalilni yo‘qotmaslik va o‘zgartirilmaganligini ta’minlash uchun muhim ahamiyatga ega. Zaxira nusxalari ham xavfsiz joyda saqlanishi kerak, bu esa sudda tasdiqlangan dalil sifatida foydalanishga imkon beradi.

Sudda dalilning haqiqiyligini tasdiqlash. Sudga kiberjinoyatlar bilan bog‘liq dalil taqdim etilayotganda, dalillarning **haqiqiyligini tasdiqlash** juda muhim ahamiyatga ega. Sudda dalillarning haqiqiyligini tasdiqlash quyidagi usullar bilan amalga oshiriladi:

- **Chain of Custody (Dalilni Saqlash Zanjiri)** – Sudda kiberjinoyatlar bo‘yicha dalil taqdim etishda, dalilni saqlash va kuzatish tizimi muhim rol o‘ynaydi. **Chain of Custody** deb ataladigan tizim orqali, dalilni har qanday saqlash joyidan, uni yig‘ishdan to sudda taqdim etishgacha bo‘lgan barcha bosqichlar rasmiylashtiriladi. Har bir saqlash va harakat bosqichi hujjatlashtiriladi va tasdiqlanadi.
- **Ekspert Tahlili** – Sudda dalilning haqiqiyligini tasdiqlashda, **digital ekspert** yoki **kompyuter ekspertlari** tomonidan olib borilgan tahlil muhim ahamiyatga ega. Ekspertlar o‘zlarining bilim va tajribalariga asoslanib, dalilning ishonchliligini, tizimdagi o‘zgartirishlarning mavjudligini yoki mavjud emasligini aniqlaydilar.
- **Sudda Dalilni Ta’riflash** – Sudda dalil taqdim etilganda, u aniq va to‘liq ta’riflanishi kerak. Dalilni ta’riflashda, uning qanday olinganligi, qanday saqlanganligi va qanday tahlil qilinganligi haqida ma’lumot berish zarur. Bu jarayon, dalilning haqiqiyligini tasdiqlashda sudga yordam beradi.
- **Raqamli Imzo va Identifikatsiya** – Sudga taqdim etilgan dalil, agar zarur bo‘lsa, raqamli imzo yordamida tasdiqlanadi. Bu, dalilning asl nusxasi ekanligini va undan hech qanday manipulyatsiya o‘tkazilmaganligini isbotlaydi. Raqamli imzo bilan tasdiqlangan dalil, uning asl holatida saqlanishini ta’minlaydi.

Xalqaro me’yorlar va standartlar. Kiberjinoyatlar bilan bog‘liq dalillarni to‘plash va rasmiylashtirishda **xalqaro standartlar** va **me’yorlar**ga amal qilish zarur. Xalqaro miqyosda **ISO/IEC 27037**, **ISO/IEC 27041** kabi standartlar mavjud bo‘lib, ular raqamli dalillarni to‘plash va tasdiqlash jarayonlariga doir umumiy talablarni belgilaydi. Bu standartlar dalilni to‘plash va saqlash jarayonlarini birxillashtirishga yordam beradi, shuningdek, kiberjinoyatlarni tergov qilishda xalqarolikni ta’minlaydi.

Xulosa qilib aytganda, Sudga taqdim etiladigan dalillarning haqiqiyligini tasdiqlash, kiberjinoyatlarni tergov qilishning markaziy jihatlaridan biridir. **Dalilning ishonchliligi** va **haqiqiyligini tasdiqlash** uchun qo‘llaniladigan texnik va huquqiy vositalar sudning yakuniy qaroriga ta’sir ko‘rsatadi. Kiberjinoyatlar sohasida dalil to‘plash va rasmiylashtirishda ilg‘or

texnologiyalar, xalqaro standartlar va yuqori darajadagi huquqiy asoslar kerakli ishonchlilikni ta’minlashga xizmat qiladi.

BOB BO‘YICHA UMUMIY XULOSALAR

Monografiyaning ushbu bobi, **kiberjinoyatlarning mohiyati** va **xalqaro tasnifi**ga doir keng va mukammal tahlillarni o‘z ichiga oladi. Kiberjinoyatlar zamonaviy dunyoning eng muhim huquqiy muammolaridan biriga aylanib, ularning shakllanishi va rivojlanishi, xalqaro jinoyat huquqi bilan bog‘liq turli jihatlar, o‘ziga xos xususiyatlar va turlariga oid chuqur tahlillarni talab etadi. Shu bilan birga, kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlarni tushunish, ularni aniqlashda yuzaga keladigan qiyinchiliklar va dalillarni huquqiy jihatdan rasmiylashtirish jarayonidagi amaliy yondashuvlar muhim o‘rin tutadi.

✓ **Kiberjinoyat tushunchasining shakllanishi va rivojlanishi** bo‘limida kiberjinoyatlar, raqamli texnologiyalar va internetning rivojlanishi bilan birga yangicha shakllarini topib, ularning jinoyat huquqi doirasidagi o‘rni ko‘rsatilgan. Kiberjinoyatlar faqatgina ma’lumotlarni o‘g‘irlash yoki zarar yetkazish bilan cheklanmaydi, balki kompleks tizimlarda tizimning ishlashiga putur yetkazish, axborotlar bilan manipulyatsiya qilish va boshqa yangi jinoyat shakllarini ham o‘z ichiga oladi.

✓ **Zamonaviy xalqaro kiberjinoyat turlari** bo‘limi esa kiberjinoyatlarning bugungi kundagi kengaygan va murakkab turlarini tahlil qildi. Zamonaviy kiberjinoyatlar, ko‘plab davlatlar va xalqaro tashkilotlar uchun jiddiy xavf tug‘diradi, chunki ular tezda global miqyosda yoyilishi mumkin. Hujumlar, firibgarlik, tarmoqni buzish, kiberterrorizm va boshqa turli jinoyatlar zamonaviy jamiyatda tobora ko‘proq uchramoqda.

✓ **Kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlar** bo‘limi, kiberjinoyatlarning jismoniy dunyodagi jinoyatlardan farqini o‘rganib chiqdi. Kiberjinoyatlar virtual muhitda sodir bo‘lishi va tez tarqalishi bilan o‘ziga xos, ammo jinoyatlarning asosiy tuzilmalari, jinoyatchilikning motivlari va maqsadlari an’anaviy jinoyatlarga o‘xshash bo‘lishi mumkin. Biroq, texnologik xususiyatlari, global ta’siri va anonimlik kabi omillar, ularning xalqaro miqyosda aniqlanishi va jinoyat sifatida e’tirof etilishida o‘ziga xos qiyinchiliklar yaratadi.

✓ **Kiberjinoyatlarni aniqlash va dalillarni huquqiy jihatdan rasmiylashtirish** bo‘limida, kiberjinoyatlarni aniqlashning texnik va huquqiy

jihatlari chuqur tahlil qilindi. Kiberjinoyatlarni aniqlashda, **digital forensika** va zamonaviy texnologiyalar yordamida to‘plangan dalillarni rasmiylashtirish, ularning haqiqiyligini tasdiqlash, sudga taqdim etishda ishonchliligi hamda yuridik jihatdan tasdiqlanishi kerakligi muhim omil sifatida ko‘rsatilgan.

Umuman olganda, monografiya kiberjinoyatlar sohasidagi zamonaviy muammolarni va ularning xalqaro huquqiy doirada e’tirof etilishidagi murakkabliklarni o‘rganishga katta hissa qo‘shadi. Kiberjinoyatlar bilan kurashishda xalqaro hamkorlik, texnologik innovatsiyalar va huquqiy me’yorlarning samarali integratsiyasi kiberjinoyatlarni jazolashda va ularning oldini olishda katta ahamiyatga ega. Kiberjinoyatlar va an’anaviy jinoyatlar o‘rtasidagi farqlarni hisobga olgan holda, ular bilan kurashish bo‘yicha kompleks yondashuvlar ishlab chiqilishi zarur.

II BOB. KIBERJINOYATLARNI JINOYAT DEB E’TIROF ETISHDAGI HUQUQIY MUAMMOLAR

Kiberjinoyatlar o‘zining global tarqalishi, tez rivojlanishi va ko‘plab yangi jinoyat turlarini yaratishi bilan zamonaviy huquqiy tizimlarni jiddiy sinovdan o‘tkazmoqda. Xalqaro miqyosda kiberjinoyatlarni jinoyat sifatida e’tirof etish va ularni jinoyat sifatida jazolashning huquqiy muammolari, mavjud milliy va xalqaro huquqiy normativlarning yetarli emasligi, kiberjinoyatlar sohasidagi maxsus texnologik bilimlarning mavjud emasligi kabi masalalar hal etilishi zarur bo‘lgan jiddiy masalalar hisoblanadi.

Bu bo‘limda kiberjinoyatlarni jinoyat sifatida tan olish va ularga nisbatan huquqiy choralar ko‘rishda yuzaga keladigan huquqiy muammolarni o‘rganish maqsad qilingan. Kiberjinoyatlar odatdagi jinoyatlarga nisbatan o‘ziga xos xususiyatlarga ega bo‘lib, bu esa mavjud huquqiy tizimlarda yangi qarorlar va qonunlarni ishlab chiqishni talab qiladi. Xususan, kiberjinoyatlarning milliy va xalqaro huquqiy me’yorlarda aniq va bir xil tasniflanishi, ularning sodir etilishiga taalluqli huquqiy javobgarlikni belgilashda doimiy murakkabliklar mavjud.

Bo‘limning birinchi qismida, kiberjinoyatlarni jinoyat sifatida tasniflashda yuzaga kelayotgan **huquqiy noaniqliklar** va **ayrim mamlakatlardagi qonunlar**ning bir-biriga mos kelmasligi ko‘rsatilgan. Kiberjinoyatlarni jinoyat deb e’tirof etishning muhim jihatlari, ularning xalqaro miqyosda qanday jinoyat turlari sifatida qaralishi, **jinoyatlarni**

tasniflash va ularni **jamiyat uchun xavf darajasi**ni hisobga olgan holda qanday yondashish kerakligi o‘rganiladi.

Bo‘limning ikkinchi qismida esa, kiberjinoyatlar bilan kurashishda **xalqaro huquq** va **internatsional hamkorlik** masalalari yoritiladi. Bugungi kunda kiberjinoyatlar bir mamlakat hududidan boshqa hududga o‘tib, xalqaro miqyosda sodir bo‘lishi mumkin, shuning uchun kiberjinoyatlar bilan kurashishning samarali yo‘li, davlatlararo hamkorlikni rivojlantirish va **xalqaro huquqiy me’yorlar**ni ishlab chiqishdan o‘tadi.

Shuningdek, bo‘limda, **kiberjinoyatlarni jinoyat sifatida tasniflashdagi qiyinchiliklar** va **sud amaliyotidagi muammolar** ham ko‘rib chiqiladi. Kiberjinoyatlarning turli shakllari, texnologik o‘zgarishlar va jinoyatlarni amalga oshirishdagi yangi metodlar, ularni aniq va adolatli jazolashda yuridik tizimlarning nozikligini oshiradi. Bu esa sudlar tomonidan olib boriladigan sudlov va jinoyatni tasniflash jarayonida huquqiy tizimlar o‘rtasidagi tafovutlarni keltirib chiqaradi.

Shu tariqa, bu bo‘limda kiberjinoyatlarni jinoyat sifatida tasniflashda yuzaga kelayotgan muammolarni, ularni hal etishning xalqaro va milliy yuridik tizimlardagi me’yorlarini va amaliy muammolarni kengaytirilgan holda tahlil qilishga harakat qilinadi. Bu tahlil, kiberjinoyatlar bilan kurashishning huquqiy yondashuvlarini takomillashtirish va kiberjinoyatchilikka qarshi samarali strategiyalarni ishlab chiqishda yordam beradi.

2.1. Xalqaro jinoyat huquqida “kiberjinoyat” tushunchasining mavqei

Xalqaro jinoyat huquqi tizimi, o‘zining asosiy maqsadi bo‘lgan xalqaro tinchlik va xavfsizlikni ta’minlashga xizmat qiluvchi huquqiy vosita sifatida, tez o‘zgaruvchan va kompleks bo‘lgan kiberjinoyatlarni o‘z ichiga olishda katta qiyinchiliklarga duch kelmoqda. Yangi texnologiyalar, raqamli infrastrukturadagi o‘zgarishlar va internetning tezkor tarqalishi kiberjinoyatlar sohasini global miqyosda yangi xavf-xatarlar bilan to‘ldirdi. Shunday qilib, kiberjinoyatlar xalqaro jinoyat huquqining an’anaviy doirasiga qo‘shilishi va bu yangi jinoyat shakllariga nisbatan samarali huquqiy me’yorlar ishlab chiqilishi zarurati tug‘ildi.

Bu bo‘limda kiberjinoyatlarning xalqaro jinoyat huquqida qanday tasniflanishi, "kiberjinoyat" tushunchasining bu huquqiy tizimdagi mavqei va

uning asosiy huquqiy normativlar bilan qanday aloqada ekanligi o‘rganiladi. Kiberjinoyatlarning hukuki maqomi va ularning jinoyat sifatida e’tirof etilishi, faqatgina milliy qonunchilik doirasida emas, balki **xalqaro huquq** me’yorlari asosida ham samarali hal etilishi zarurdir. Kiberjinoyatlarning xalqaro jinoyat huquqiga kirishi, ayniqsa, **kompyuter tizimlariga noqonuniy kirish**, **ma’lumotlar o‘g‘irligi**, **kiberterrorizm** va boshqa xalqaro miqyosda sodir bo‘ladigan jinoyatlar o‘rtasida aniq farqlar va yangi yondashuvlarni talab etadi.

Kiberjinoyatlarni **xalqaro jinoyat huquqida tan olish** uchun, kiberjinoyatlarning odatiy jinoyatlar bilan solishtirganda, ularning geosiyosiy, texnologik va kommunikatsion xususiyatlarini chuqur tahlil qilish lozim. Kiberjinoyatlarning xalqaro miqyosda jinoyat sifatida tan olinishi, ularga qarshi kurashish uchun global hamkorlikni kuchaytirishni talab etadi. Shu bois, kiberjinoyatlar bilan kurashishda xalqaro jinoyat huquqi va milliy qonunlar o‘rtasidagi o‘zaro bog‘liqlik va o‘zaro qarorlar ishlab chiqish zarurati mavjud.

Shu nuqtai nazardan, **kiberjinoyat** tushunchasining xalqaro jinoyat huquqida qanday rivojlanishi, uning **jinoyat turlari** sifatida tasniflanishi, xalqaro jinoyat huquqining yangi yondashuvlarini ishlab chiqishning dolzarb masalalari bo‘lib qolmoqda. Bu bo‘limda kiberjinoyatlarning xalqaro jinoyat huquqidagi o‘rni va uni rasmiy ravishda jinoyat sifatida tasniflashda yuzaga keladigan huquqiy qiyinchiliklar, xalqaro hamkorlik va normativ asoslar tahlil qilinadi.

Xalqaro jinoyatlar (genotsid, terrorizm) va kiberjinoyatlar o‘rtasidagi farq. Xalqaro jinoyat huquqi, xalqaro xavfsizlikni ta’minlash, tinchlikni saqlash va inson huquqlarini himoya qilish maqsadida jahon miqyosida sodir bo‘ladigan jinoyatlar bilan kurashishga yo‘naltirilgan huquqiy tizimni tashkil etadi. An’anaviy xalqaro jinoyatlar, masalan, genotsid, urush jinoyatlari va terrorizm, zamonaviy davrda odamlar va davlatlar uchun jiddiy xavf tug‘dirishga davom etmoqda. Biroq, so‘nggi yillarda kiberjinoyatlar yangi tahdid sifatida paydo bo‘ldi, va ularning xalqaro jinoyatlar bilan taqqoslanishi huquqiy tizimlarda yangi yondashuvlarni talab qilmoqda.

Genotsid va **terrorizm** kabi xalqaro jinoyatlar, o‘zining xususiyatlariga ko‘ra, aniq qoidalar, jinoyatlarni aniqlash, jazolash va xalqaro hamkorlikning belgilangan tartiblariga asoslanadi. Ular xalqaro huquq doirasida alohida normativlarning va xalqaro sudlarning, masalan, **Xalqaro Jinoyat Sudi (XJS)**, tomonidan aniqlanadi va tartibga solinadi. Bunday jinoyatlar o‘zining jismoniy va odamiy zarar keltirishi bilan ajralib turadi, va davlatlar tomonidan

maxsus jazo choralariga tortiladi. Genotsid, asosan, bir etnik yoki diniy guruhga qarshi amalga oshirilgan ommaviy qirg‘in, jinoyat va terrorizm esa, davlatlar yoki jamoalar tomonidan o‘z maqsadlariga erishish uchun qo‘llaniladigan har qanday zo‘ravonlik yoki qo‘rqitish amaliyotlari sifatida aniq belgilanadi.

Kiberjinoyatlar esa o‘zining an’anaviy jinoyatlardan ajralib turadigan bir qator xususiyatlarga ega. Kiberjinoyatlar, asosan, **internet va kompyuter texnologiyalari** orqali amalga oshiriladigan jinoyatlar bo‘lib, ularning tarkibi har doim yangi texnologik rivojlanishlarga mos keladi. Bu jinoyatlar, ko‘pincha, **ma’lumotlarni o‘g‘irlash**, **kompyuter tizimlariga noqonuniy kirish**, **virüslar tarqatish**, **tizimlarni ishga solish yoki buzish** va boshqa raqamli texnologiyalarni suiiste’mol qilish bilan bog‘liqdir. Shu bilan birga, kiberjinoyatlar an’anaviy jinoyatlar singari jismoniy zarar keltirmaydi, balki virtual muhitda turli axborotlar va tizimlar bilan manipulyatsiya qilish orqali iqtisodiy va siyosiy zarar yetkazadi.

Xalqaro jinoyatlar va **kiberjinoyatlar** o‘rtasidagi eng katta farqlardan biri ularning **geografik va virtual xarakteri**dir. Xalqaro jinoyatlar, masalan, genotsid yoki terrorizm, ko‘pincha aniq geografik hududda, jismoniy joylashgan aholiga yoki davlatlarga zarar yetkazadi. Ushbu jinoyatlar doimiy ravishda aniq jinoyat joyi va jismoniy shaxslarni ta’sir qiladi. Kiberjinoyatlar esa virtual muhitda sodir bo‘lib, jinoyatchilar va qurbonlar orasidagi masofa bevosita fizik hududdan ajralib turadi. Shuningdek, kiberjinoyatlarning global xarakteri, ularning turli davlatlar orasida tez tarqalishi va zarar yetkazishi, jismoniy hududda sodir bo‘ladigan jinoyatlardan farq qiladi.

Kiberjinoyatlar, shuningdek, **anomaliyalik va anonimlik** xususiyatlariga ega. Ko‘plab kiberjinoyatlar, masalan, **hakerlik** yoki **phishing** hujumlari, ko‘pincha anonimlikni ta’minlaydi va jinoyatchilarni aniqlashda muammolarni keltirib chiqaradi. Xalqaro jinoyatlar esa an’anaviy ravishda, odatda, aniq jinoyatchilar yoki guruhlar tomonidan amalga oshiriladi va ularni aniqlashda davlatlararo hamkorlikda yuridik mexanizmlar mavjud.

Bundan tashqari, **kiberjinoyatlar** ko‘pincha **axborot resurslariga zarar yetkazish** yoki **ma’lumotlarni o‘g‘irlash** bilan bog‘liq bo‘lib, bu esa ularni **moliyaviy** va **iqtisodiy** zarar keltirishga olib keladi. Misol uchun, **ransomware** hujumlari yoki **kredit kartalarini o‘g‘irlash** kabi kiberjinoyatlar davlatlararo iqtisodiy aloqalarga zarar yetkazishi mumkin.

Xalqaro jinoyatlar esa asosan **inson huquqlari** va **xalqaro tinchlikni** xavf ostiga qo‘yadi.

Xulosa qilib aytganda, **kiberjinoyatlar** va **xalqaro jinoyatlar** o‘rtasidagi farqlar, ularning **geografik ta’siri**, **maniakalar** (anomaliyalar), **anonimlik** va **virtual va jismoniy zararning turli shakllari**ni o‘z ichiga oladi. Kiberjinoyatlar o‘zining yangi xususiyatlari va global tarqalishi bilan an’anaviy jinoyatlarni yangi yuridik yondashuvlar va normativlar asosida qayta ko‘rib chiqishni talab qilmoqda. Shu sababli, kiberjinoyatlar bilan kurashish uchun xalqaro hamkorlik va texnologik innovatsiyalarni birlashtirgan huquqiy mexanizmlar zarur bo‘lib qoladi.

Kiberjinoyatlarning jinoiy javobgarlikka tortilishi masalasi. Kiberjinoyatlar, o‘zining maxsus va murakkab xususiyatlari bilan, an’anaviy jinoyat huquqiga nisbatan yangi yuridik yondashuvlarni talab qilmoqda. Bugungi kunda raqamli texnologiyalarning tez rivojlanishi va global internet tarmoqlarining keng tarqalishi kiberjinoyatlarning kutilganidan ancha tez sur’atlar bilan ko‘payishiga olib keldi. Shu bilan birga, kiberjinoyatlarni jinoiy javobgarlikka tortishning huquqiy masalalari xalqaro miqyosda o‘ziga xos qiyinchiliklar yaratmoqda.

Kiberjinoyatlarning jinoiy javobgarlikka tortilishiga doir masalalar, odatda, bir nechta yuridik sohalarda o‘z aksini topadi. Birinchidan, bu jinoyatlarning **ta’riflanishi** va **tasniflanishi** muhim ahamiyatga ega. Xalqaro jinoyat huquqida kiberjinoyatlarning qaysi turdagi jinoyatlar sifatida e’tirof etilishi, ularning qaysi xususiyatlarga ega bo‘lishi va jinoyat sifatida qanday jazolanishi haqidagi aniq normativlar mavjud emas. Bu, o‘z navbatida, milliy va xalqaro sud tizimlarida kiberjinoyatlarni jinoyat sifatida tasniflash va ularni javobgarlikka tortishda qiyinchiliklarni keltirib chiqaradi.

Kiberjinoyatlar turli mamlakatlarning ichki qonunchiligida ham turlicha ko‘rsatilgan va huquqiy qarorlar ham bir-biridan farq qiladi. Bu davlatlar o‘rtasida yuridik uyg‘unlikning yetishmasligi kiberjinoyatlarni aniq aniqlash va ularni jinoiy javobgarlikka tortishda huquqiy xatoliklar va kechikishlarga olib kelmoqda. Xalqaro jinoyat huquqi doirasida kiberjinoyatlarni jinoyat sifatida e’tirof etishda **xalqaro hamkorlik** va **juridik yondashuvlar**ni yaxshilash zarurati mavjud.

Kiberjinoyatlarning jinoiy javobgarlikka tortilishi masalasi, shuningdek, kiberjinoyatchilarni aniqlash va ularni jazolashda mavjud bo‘lgan **texnologik** va **jinoyatchilikni aniqlashdagi** muammolarni ham o‘z ichiga

oladi. Kiberjinoyatlar odatda internet orqali amalga oshiriladi, bu esa ularning aniqlanishini qiyinlashtiradi. Kiberjinoyatchilar koʻpincha anonimlikni taʼminlaydigan vositalardan foydalanadilar, shuningdek, ular oʻz jinoyatlarini amalga oshirish uchun zamonaviy texnologiyalarni ishlatadilar. Shu sababli, kiberjinoyatlarni aniqlash va javobgarlikka tortish jarayonida texnologik vositalar va xususiy texnik bilimlarning ahamiyati oshadi. Bu holat xalqaro sudlarga va boshqa yuridik institutlarga jinoyatchilarni aniqlashda yanada murakkabliklarni keltirib chiqaradi.

Kiberjinoyatlarni jinoiy javobgarlikka tortishdagi muhim bir jihat — **hukumatlarning jinoiy javobgarlikni** qoʻllashdagi **ulardagi yuridik doira**ni belgilashdir. Baʼzi mamlakatlarda kiberjinoyatlar, umuman, maxsus qonunlar va koʻrsatmalar bilan qatʼiy tartibga solingan boʻlsa-da, boshqa davlatlarda bu masalalar aniqlikdan yiroqdir. Xalqaro jinoyat huquqida, ayniqsa, **jinoyatga qarshi xalqaro hamkorlikni rivojlantirish** va **xalqaro yuridik muvofiqlik**ni taʼminlash uchun davlatlar oʻrtasida kelishuvlar va bitimlar zarur boʻladi.

Kiberjinoyatlarning jinoiy javobgarlikka tortilishidagi muammolarni bartaraf etish uchun xalqaro huquqiy asoslarni qayta koʻrib chiqish, **tekshirish jarayonlarini markazlashtirish**, **yuridik texnologiyalarni rivojlantirish** va **xalqaro hamkorlikni kuchaytirish** zarur. Kiberjinoyatchilikning murakkab va tez oʻzgaruvchan xususiyatlari, shu bilan birga, internet tarmogʻida sodir etiladigan jinoyatlar orasida qoʻllaniladigan standartlarga boʻlgan ehtiyojni yanada oshiradi. Shu nuqtai nazardan, kiberjinoyatlarni jinoiy javobgarlikka tortishning samarali yoʻllarini ishlab chiqish, **xalqaro jinoyat huquqi**ga yangi yondashuvlarni talab qiladi.

Shuningdek, kiberjinoyatlarni jinoiy javobgarlikka tortish masalasida **yuridik maʼlumotlar va dalillarni toʻplash**ning muhimligi alohida eʼtiborga loyiqdir. Kiberjinoyatlarning tez rivojlanayotgan tabiati va ular amalga oshirilayotgan texnologik vositalar, jinoyatga oid dalillarni toʻplash va ularga asoslangan hukmlar chiqarishda katta qiyinchiliklar tugʻdiradi. Bu, ayniqsa, xalqaro miqyosda sodir etilayotgan jinoyatlarda muhim rol oʻynaydi, chunki dalillarni toʻplashda hamkorlik qiluvchi davlatlar oʻrtasida muvofiqlik zarurati mavjud.

Xulosa qilib aytganda, kiberjinoyatlar jinoiy javobgarlikka tortishdagi huquqiy masalalar, xalqaro huquq va milliy qonunchilik oʻrtasidagi uygʻunlikni topish, texnologiyalarning yangi rivojlanishiga mos keladigan normativlar ishlab chiqish va jinoyatchilarni aniqlashda hamkorlikni

kuchaytirishni talab qiladi. Bu sohada muvaffaqiyatli ishlash uchun xalqaro hamkorlik va huquqiy tizimlarning zamonaviy texnologik yondashuvlar bilan uyg‘unlashtirilishi lozim.

Yagona huquqiy standartlarning yo‘qligi. Kiberjinoyatlar, o‘zining murakkab va dinamik tabiati bilan, xalqaro jinoyat huquqi doirasida yagona huquqiy standartlarning yo‘qligini keltirib chiqarmoqda. Bugungi kunda global miqyosda raqamli jinoyatlar tobora kengayib bormoqda, ammo bu jinoyatlarni aniq va yagona huquqiy nuqtai nazardan tasniflashda, ular uchun belgilangan jinoiy javobgarlikni qo‘llashda hali ko‘plab muammolar mavjud. Kiberjinoyatlar uchun yagona, universal huquqiy norma va standartlarning yo‘qligi, shu bilan birga, ushbu jinoyatlarni xalqaro darajada samarali kurashish, ular bilan bog‘liq jazolarni joriy etish va global miqyosda ularni jinoyat sifatida e’tirof etish bo‘yicha yetarli yuridik mexanizmlar yaratishdagi qiyinchiliklarni oshiradi.

Kiberjinoyatlarni tasniflashdagi noaniqlik va **turli yuridik tizimlar o‘rtasidagi tafovutlar** - bu masalaning eng muhim jihatlaridan biridir. Ba’zi davlatlar kiberjinoyatlar uchun aniq ta’riflarni ishlab chiqqan bo‘lsa, boshqalarida bu borada muayyan huquqiy belgilashlar mavjud emas. Shu bilan birga, ba’zi mamlakatlarda kiberjinoyatlar jinoiy javobgarlikka tortilish uchun tegishli qonunlar va normativ hujjatlar mavjud, boshqalarda esa bu sohada qonunchilik hali rivojlanmagan yoki to‘liq amalga oshirilmagan. Shuningdek, xalqaro miqyosda kiberjinoyatlar uchun yagona standartlarga ega bo‘lgan xalqaro huquqiy hujjatlarning yo‘qligi, davlatlar o‘rtasidagi hamkorlikni murakkablashtiradi.

Yagona huquqiy standartlarning yo‘qligi kiberjinoyatlar bilan bog‘liq bo‘lgan bir nechta yuridik qiyinchiliklarni yaratadi.

- ✓ ***Birinchidan,*** har bir davlat o‘z hududida amalga oshirilgan kiberjinoyatlar uchun o‘z qonunlari va normalariga asoslanadi, bu esa xalqaro hamkorlikni cheklaydi va jinoyatlarni qamrab olishda davlatlar o‘rtasida farqlarni keltirib chiqaradi. Ko‘plab davlatlarda kiberjinoyatlar haqidagi qonunchilik juda keng qamrovli yoki umuman mavjud emas. Aksariyat hollarda, mamlakatlar o‘rtasida bu turdagi jinoyatlarni tasniflash va ularga qarshi qaysi choralar ko‘rish kerakligini aniq belgilashda yuridik standartlarning yo‘qligi katta muammo sifatida mavjud.
- ✓ ***Ikkinchidan,*** **xalqaro sudlar va huquqiy muassasalar** kiberjinoyatlar bo‘yicha har xil normativlarga ega. Masalan, Xalqaro Jinoyat

Sudi (XJS) o‘zining an’anaviy jinoyatlar — genotsid, urush jinoyatlari, insoniyatga qarshi jinoyatlar — bo‘yicha belgilangan va xalqaro qoidalarga asoslangan qarorlar chiqaradi. Ammo kiberjinoyatlar bu tizimga to‘liq kiritilgan emas. Kiberjinoyatlar bo‘yicha mavjud bo‘lgan yuridik normativlar va bitimlar, ko‘pincha, umumiy tarzda bo‘lib, ma’lum bir jinoyatni tasniflash va ularni jazolashda noaniqlik yaratadi. Shu sababli, kiberjinoyatlar bo‘yicha xalqaro sudlar, huquqiy tartiblar va normativlarni yagona tizimga kiritish ehtiyoji tug‘iladi.

✓ ***Uchinchidan,*** kiberjinoyatlarni xalqaro darajada tasniflash va jazolashda **normativlar o‘rtasidagi muvofiqlik** yo‘qligi tufayli qiyinchiliklar yuzaga keladi. Har bir davlat kiberjinoyatlar bilan kurashishda o‘z qonunlaridan foydalansa-da, bu normativlar bir-biriga mos kelmasligi mumkin. Masalan, bir davlatda internet orqali amalga oshirilgan firibgarlikni jinoiy javobgarlikka tortishga doir aniq qoidalar mavjud bo‘lsa, boshqa bir mamlakatda bu turdagi jinoyatlar faqat ma’muriy jazolar bilan cheklanadi. Xalqaro huquqda esa bunday farqlarni bartaraf etish va yagona normativni ishlab chiqish zarurati ortadi.

Bundan tashqari, kiberjinoyatlar uchun huquqiy standartlarning yo‘qligi, **internetni boshqarish va davlatlararo qonuniy muloqotlar**da ham muammolarni keltirib chiqaradi. Internetning transmilliy xarakteri tufayli, kiberjinoyatlar ko‘pincha bir mamlakat hududidan boshqa mamlakat hududiga o‘tishi yoki bir nechta mamlakatlarning qonunlari bilan bog‘lanishi mumkin. Bu holatda, kiberjinoyatni amalga oshirgan jinoyatchini aniqlash, uni javobgarlikka tortish va jazo choralarini qo‘llashda xalqaro hamkorlik va yagona standartlarning mavjudligi juda muhimdir. Shu bilan birga, bunday jinoyatlarni jinoyat deb e’tirof etish, ularga qarshi kurashish va jazolashda yuridik tizimlar o‘rtasidagi tartiblarning uyg‘un bo‘lishi zarur.

Xulosa qilib aytganda, kiberjinoyatlar uchun yagona huquqiy standartlarning yo‘qligi, global miqyosda bu turdagi jinoyatlar bilan samarali kurashishning oldidagi asosiy to‘siqlardan biridir. Kiberjinoyatlarni xalqaro darajada e’tirof etish va ularni jinoiy javobgarlikka tortish masalalari muhim yuridik va texnologik qiyinchiliklarni keltirib chiqaradi. Shu sababli, kiberjinoyatlar bilan kurashish uchun yagona va universal huquqiy me’yorlarni ishlab chiqish, xalqaro hamkorlikni rivojlantirish va davlatlar o‘rtasidagi qonuniy uyg‘unlikni ta’minlash zarur.

2.2. Davlatlarning kiberjinoyatlarga nisbatan turlicha yondashuvi

Kiberjinoyatlar bugungi kunda global miqyosda tobora kengayib borayotgan muammo bo‘lib, ularni jinoyat deb e’tirof etish va ularga qarshi kurashishda davlatlar turlicha yondashuvlarni qo‘llamoqdalar. Raqamli texnologiyalar va internetning global miqyosda keng tarqalishi, kiberjinoyatlarning samarali oldini olishni, aniqlashni va jazolashni qiyinlashtirmoqda. Har bir davlat kiberjinoyatlarga qarshi kurashishda o‘z qonunlari, me’yoriy hujjatlari va yuridik tizimlaridan foydalanadi, ammo ularning yondashuvlari ko‘pincha bir-biridan farq qiladi. Shu bois, davlatlarning kiberjinoyatlarga nisbatan turlicha yondashuvi jahonning turli burchaklarida qiyin tushuncha va amaliyotlarga olib keladi.

Davlatlarning kiberjinoyatlarga qarshi kurashishdagi yondashuvlar, birinchi navbatda, har bir mamlakatning **hukukiy tizimi**, **iqtisodiy rivojlanish darajasi** va **madaniy an’analari** bilan bog‘liqdir. Ba’zi davlatlar kiberjinoyatlarga qarshi qat’iy qonunlar va tegishli normativ hujjatlar joriy qilgan bo‘lsa, boshqalarida bu borada hali aniq qoidalar va yo‘riqnomalar mavjud emas. Shu sababli, kiberjinoyatlarga nisbatan har xil yondashuvlar, jinoiy javobgarlikni belgilash, jinoyatchilarni aniqlash va jazolashda bir-biridan farq qiladi.

✓ Birinchi yondashuvni **milliy qonunchilik tizimiga asoslangan** yondashuvlar tashkil etadi. Ba’zi davlatlar kiberjinoyatlar uchun maxsus qonunlar yaratib, ularni o‘z ichiga olgan alohida jinoyat turlarini ishlab chiqqan. Misol uchun, AQSH va Yevropa Ittifoqi kabi mamlakatlar o‘z hududlarida kiberjinoyatlarga qarshi maxsus qonunlar qabul qilgan va raqamli jinoyatlar uchun aniq tasniflashlar, jazolarni belgilagan. Boshqa tomondan, ba’zi mamlakatlarda kiberjinoyatlar faqat umumiy jinoyat qonunchiligi asosida ko‘rib chiqiladi va kiberjinoyatlar odatdagi jinoyatlar bilan tenglashtiriladi. Bu esa kiberjinoyatlarni aniqlash va jazolashda normativ notekisliklarga olib keladi.

✓ Ikkinchi yondashuvni **xalqaro hamkorlikka asoslangan** yondashuvlar tashkil etadi. Kiberjinoyatlar ko‘pincha transmilliy xarakterga ega bo‘lgani uchun, davlatlar o‘rtasidagi hamkorlikni rivojlantirish muhimdir. Bir qator xalqaro bitimlar va kelishuvlar kiberjinoyatlar bilan kurashishga bag‘ishlangan. Xalqaro huquq doirasida kiberjinoyatlarni aniqlash, jinoyatga qarshi kurashish, va ularga jazolarni qo‘llash uchun hamkorlik qilish davlatlar uchun katta ahamiyatga ega. Xalqaro yuridik tizimlar va tashkilotlar

kiberjinoyatlarga qarshi umumiy siyosatlarni ishlab chiqish va milliy qonunchiliklarga ta’sir ko‘rsatishda muhim rol o‘ynaydi. Masalan, **Birlashgan Millatlar Tashkiloti (BMT)**, **Evropa Ittifoqi (EU)** va **Interpol** kabi xalqaro tashkilotlar kiberjinoyatlar bo‘yicha kelishuvlar va yo‘riqnomalarni ishlab chiqishda faol ishtirok etadilar.

✓ Uchinchi yondashuvni **texnologik yondashuvlar** tashkil etadi. Kiberjinoyatlar ko‘pincha yuqori texnologiyalarni talab qiladi, shuning uchun ba’zi mamlakatlar bu sohada yangi texnologiyalarga mos keladigan yuridik va texnik choralarni ishlab chiqishadi. Misol uchun, **digital forensika** va **kiberxavfsizlik texnologiyalari** orqali jinoyatlarning izlarini aniqlash va jinoyatchilarni topishda yuqori samarali texnologiyalarni qo‘llash mumkin. Boshqa tomondan, ayrim davlatlar faqatgina an’anaviy jinoyatchilikni oldini olishga mo‘ljallangan choralarni ko‘rib chiqadilar, bu esa zamonaviy kiberjinoyatlar uchun yetarli bo‘lmasligi mumkin.

Davlatlarning kiberjinoyatlarga qarshi turlicha yondashuvi, shuningdek, **madaniy va iqtisodiy omillar** bilan ham bog‘liqdir. Ba’zi mamlakatlarda kiberjinoyatlarning xavfini jiddiy qabul qilish va ularga qarshi kurashish birinchi o‘rinda turadi, boshqalarda esa bu soha hali keng o‘rganilmagan. Misol uchun, rivojlangan davlatlar, raqamli texnologiyalarni o‘z hududida keng qo‘llagan holda, kiberjinoyatlar bilan kurashishda aniq va qat’iy yondashuvlarni qo‘llaydi. Aksincha, rivojlanayotgan davlatlarda iqtisodiy va texnologik cheklovlar tufayli kiberjinoyatlar bilan kurashishdagi resurslar va imkoniyatlar cheklangan bo‘lishi mumkin.

Shu bilan birga, davlatlar o‘rtasidagi **huquqiy farqlar** ham muhim rol o‘ynaydi. Har bir mamlakatning o‘zining mustaqil qonunchilik tizimi va yuridik strukturasi mavjud bo‘lib, bu tizimlar kiberjinoyatlarni tasniflashda, aniqlashda va jazolashda turlicha qarorlar qabul qilishga olib keladi. Masalan, ayrim mamlakatlarda kiberjinoyatlar juda keng qamrovli bo‘lishi mumkin, boshqalarida esa faqat muayyan turdagi jinoyatlar jinoiy javobgarlikka tortiladi. Bu holat, kiberjinoyatlarga nisbatan davlatlararo bir xilda yondashuvni amalga oshirishda to‘siq bo‘ladi.

Xulosa qilib aytganda, Kiberjinoyatlarga nisbatan davlatlarning turlicha yondashuvi, ularning qonunchilik tizimlari, iqtisodiy rivojlanish darajasi, texnologik imkoniyatlar va madaniy an’analari bilan chambarchas bog‘liqdir. Biroq, global miqyosda kiberjinoyatlarga qarshi samarali kurashish uchun davlatlar o‘rtasida muvofiqlik va hamkorlikni kuchaytirish, yagona yuridik

me’yorlarni ishlab chiqish va texnologik imkoniyatlarni rivojlantirish zarur bo‘ladi. Davlatlar o‘rtasidagi turlicha yondashuvlar, shuningdek, kiberjinoyatlar bilan kurashishda xalqaro hamkorlik va standartlarga bo‘lgan ehtiyojni oshiradi.

AQSh: Federal Computer Fraud and Abuse Act (CFAA). AQShda kiberjinoyatlarga qarshi kurashish uchun joriy qilingan eng muhim huquqiy hujjatlardan biri **Federal Computer Fraud and Abuse Act (CFAA)** hisoblanadi. Ushbu qonun 1986-yilda qabul qilingan bo‘lib, uning asosiy maqsadi kompyuter tizimlariga noqonuniy kirish, axborot tizimlaridan noqonuniy foydalanish, kompyuterda ma’lumotlarni o‘g‘irlash yoki zarar etkazish kabi jinoyatlarga qarshi kurashishni ta’minlashdir. CFAA AQShda kiberjinoyatlar bilan kurashishda muhim huquqiy asoslardan biridir va hozirgi kunda global miqyosda kiberjinoyatlarni aniqlash va jinoyatchilarga nisbatan javobgarlikni belgilashda asosiy me’yoriy hujjatlardan biri bo‘lib xizmat qiladi.

CFAA ning asosiy mazmuni. CFAA 1986-yilda qabul qilingan bo‘lib, dastlab faqat federal hukumat tizimlari va kompyuterlaridan noqonuniy foydalanish va zarar yetkazish bilan kurashish uchun mo‘ljallangan edi. Ammo vaqt o‘tishi bilan ushbu qonun kengaytirildi va bugungi kunda uni kiberjinoyatlar turli shakllarini qamrab oladigan holatga keltirildi. Hozirda CFAA, kompyuter tizimlarida qonunga xilof harakatlarni amalga oshirishga oid ko‘plab jinoyatlarni belgilaydi va ularga jinoiy javobgarlikni ta’minlaydi.

CFAAning asosiy qoidalari quyidagilardan iborat:

✓ **Noqonuniy Kirish (Unauthorized Access)** – CFAA kompyuter tizimlariga, internet saytlari, tarmoq resurslariga yoki boshqa axborot tizimlariga noqonuniy kirishni jinoyat sifatida belgilaydi. Bu, masalan, tizimga ruxsatsiz kirish, parollarni buzish yoki tarmoq xavfsizlik choralari orqali kirishga urinishlarni o‘z ichiga oladi.

✓ **Ma’lumotlarni O‘g‘irlik va Zarar Etkazish (Theft and Destruction of Information)** – CFAA maqsadlaridan biri kompyuter tizimlaridagi ma’lumotlarni o‘g‘irlash, bu ma’lumotlarga ruxsatsiz kirish va ularni yo‘q qilish, buzish yoki o‘zgartirish kabi harakatlarni jinoyat sifatida belgilashdir. Bu, kompaniya ma’lumotlarini o‘g‘irlagan yoki tashkilot tarmog‘ini buzgan shaxslar uchun qo‘llaniladi.

✓ **Kompyuter Tizimlaridan Noqonuniy Foydalanish (Fraudulent Use of Computer Systems)** – Kompyuter tizimlaridan noqonuniy foydalangan

holda moliyaviy foyda olish, masalan, internetda firibgarlik qilish, soxta shaxslar yaratish yoki hujjatlarni manipulyatsiya qilish CFAA tomonidan jinoyat deb e’tirof etiladi.

✓ **Hukumat Kompyuterlariga Noqonuniy Kirish (Unauthorized Access to Government Computers)** – CFAA hukumati tomonidan boshqariladigan kompyuter tizimlarida noqonuniy kirishni alohida jinoyat sifatida belgilaydi. Ayniqsa, davlat xavfsizligiga yoki mamlakatning muhim infrastrukturasiga zarar yetkazish holatlarida bu jinoyatlar jiddiy jazolanishi mumkin.

✓ **Kiberhujumlar va DDoS (Distributed Denial of Service) Hujumlar** – CFAA tomonidan kiberhujumlar, ayniqsa, DDoS hujumlari, ya’ni tizimlarni faoliyatdan to‘xtatish va serverlar orqali tizimlarga ortiqcha yuklarni kiritish jinoyatlar sifatida ko‘riladi.

CFAA ning ilg‘or texnologiyalarni hisobga olishi. Federal Computer Fraud and Abuse Act dastlab 1986-yilda qabul qilingan bo‘lsa-da, texnologiyaning rivojlanishi bilan birga CFAA ham yangilanishlarga uchradi. Ayniqsa, kompyuter va tarmoq texnologiyalarining rivojlanishi kiberjinoyatlarning yangi turlarini paydo qildi va CFAA qonuni ushbu o‘zgarishlarga moslashishi zaruriyatini keltirib chiqardi.

1996-yilda CFAA ning qayta ko‘rib chiqilishi va yangilanishi, ushbu qonunning turli turdagi zamonaviy kiberjinoyatlar bilan kurashishga tayyor bo‘lishini ta’minladi. Shu bilan birga, CFAA 2001-yilda **USA PATRIOT Act**ning qabul qilinishi orqali qo‘shimcha kuchaytirildi va davlat xavfsizligiga ta’sir qiluvchi kiberjinoyatlarga qarshi kurashishda kengaytirildi. Bugungi kunda CFAA raqamli huquqlar va axborot xavfsizligi bilan bog‘liq keng qamrovli yuridik bazani tashkil qiladi.

CFAA ning cheklovlari va tanqidlar. CFAA ning amaliyotda qo‘llanilishi ba’zan tanqid qilinadi. Ayniqsa, qonunning ba’zi normativlari, masalan, “noqonuniy kirish” yoki “ma’lumotlar buzilishi” kabi tushunchalar juda keng talqin qilinishi mumkin, bu esa ba’zi hollarda noxush natijalarga olib keladi. Misol uchun, CFAA, ba’zi hollarda internetda foydalanuvchilarning odatiy faoliyatini jinoyat sifatida ko‘rib chiqishiga olib kelishi mumkin, chunki ko‘plab internet foydalanuvchilari ruxsatsiz tizimlarga kirish yoki ma’lumotlarga ta’sir ko‘rsatish bilan bog‘liq bo‘lgan harakatlar natijasida jinoiy javobgarlikka tortilishi mumkin.

Shuningdek, **CFAA** qonuni ba’zan texnologik yangilanishlarni hisobga olmasdan tuzilganligi sababli, uning ba’zi qoidalari o‘z vaqtida yangilanmaydi va zamonaviy kiberjinoyatlar bilan kurashishda samarali bo‘lmasligi mumkin. Ayrim ekspertlar CFAA ning ko‘p hollarda faqat “kiberjinoyatlar”ni aniqlashda eng umumiy va keng qarorlar bilan ishlashini, shuningdek, bu qonunning yangilanishi va takomillashtirilishini talab etishini ta’kidlamoqda.

Xulosa qilib aytganda, **Federal Computer Fraud and Abuse Act (CFAA)** AQShda kiberjinoyatlarga qarshi kurashishda eng muhim huquqiy instrumentlardan biridir. U kompyuter tizimlaridan noqonuniy foydalanish, ma’lumotlarni o‘g‘irlash, zarar etkazish kabi harakatlarni jinoyat sifatida belgilaydi va ularga jinoiy javobgarlikni ta’minlaydi. CFAA ning kengaytirilgan talqinlari va yangilanishlari, zamonaviy kiberjinoyatlar bilan kurashish uchun zarur bo‘lgan yuridik bazani tashkil qiladi, lekin ularning cheklovlari va tanqidlariga qarshi kurashishda yanada samarali yondashuvlar va qonunchilikni takomillashtirish zarurati mavjud. Bu qonun AQShning kiberjinoyatlarni jinoyat deb e’tirof etishdagi eng muhim va kompleks yuridik vositalaridan biridir.

Yevropa: GDPR va boshqa himoya mexanizmlari. Yevropa Ittifoqi (YI) mamlakatlari kiberjinoyatlarga qarshi kurashishda muhim yuridik va normativ choralarga ega. Ularning asosiy yo‘nalishlaridan biri – shaxsiy ma’lumotlarni himoya qilish va axborot xavfsizligini ta’minlashdir. Yevropa Ittifoqi o‘z hududidagi kiberjinoyatlarga qarshi kurashish bo‘yicha keng qamrovli va samarali tizimlar yaratishga harakat qilmoqda. Bu tizimlarning asosiy qismlaridan biri shaxsiy ma’lumotlar va axborot xavfsizligini ta’minlashga qaratilgan normativ hujjatlar, jumladan, **Yevropa Ittifoqining Umumiy Ma’lumotlar Himoyasi To‘g‘risidagi Reglamenti (GDPR)** va boshqa turli himoya mexanizmlarini o‘z ichiga oladi.

1. GDPR (General Data Protection Regulation) – Umumiy Ma’lumotlar Himoyasi To‘g‘risidagi Reglament. GDPR (General Data Protection Regulation) Yevropa Ittifoqi tomonidan 2016-yil 27-aprelda qabul qilingan va 2018-yil 25-maydan kuchga kirgan, shaxsiy ma’lumotlarning himoyasini ta’minlashga qaratilgan huquqiy hujjatdir. GDPR nafaqat Yevropa Ittifoqidagi, balki butun dunyodagi kompaniyalar va tashkilotlar uchun ahamiyatli bo‘lib, bu qonun shaxsiy ma’lumotlarga bo‘lgan munosabatni o‘zgartirib, yangi xavfsizlik talablarini o‘rnatdi.

GDPR ning asosiy qoidalari. GDPR shaxsiy ma’lumotlarni to‘plash, ishlov berish va saqlash bo‘yicha qat’iy talablarni belgilaydi. Uning asosiy qoidalari quyidagilardan iborat:

- **Ma’lumotlarni yig‘ishning o‘ziga xos shartlari** – Ma’lumotlarni to‘plash faqat aniq va qonuniy maqsadlarda amalga oshirilishi kerak. Shaxsiy ma’lumotlarni yig‘ishdan oldin foydalanuvchidan aniq rozilik olinishi lozim. Bu shart, ma’lumotlarni to‘plashni shaffof qilishni, shuningdek, odamlarning o‘z ma’lumotlariga bo‘lgan nazoratini kuchaytirishni ta’minlaydi.
- **Ma’lumotlarni minimalizatsiyasi** – Shaxsiy ma’lumotlarni faqat maqsadga muvofiq miqdorda va sifatda to‘plash kerak. Yani, faqat kerakli ma’lumotlar to‘planishi kerak, maqsadsiz yoki keraksiz ma’lumotlar yig‘ilmasligi lozim.
- **Shaxsiy ma’lumotlarning saqlanishi** – Shaxsiy ma’lumotlar faqat maqsadga muvofiq ravishda va zarur bo‘lgan muddatga saqlanishi kerak. Bu vaqt o‘tishi bilan ortiqcha yoki eskirgan ma’lumotlarning yo‘q qilinishini ta’minlashni talab qiladi.
- **Shaxsiy ma’lumotlarning xavfsizligi** – GDPR, ma’lumotlarga nisbatan yuqori xavfsizlik choralarini qo‘llashni talab qiladi. Bu, ma’lumotlarning nojo‘ya o‘g‘irlanishi, yo‘qolishi yoki buzilishidan himoya qilishni nazarda tutadi. Kiberjinoyatlar, jumladan, ma’lumotlarni o‘g‘irlash yoki buzish kabi holatlar, GDPR bilan belgilangan xavfsizlik talablarini buzgan hisoblanadi.
- **Shaxsiy ma’lumotlarni faollashtirish va saqlashda shaffoflik** – GDPR odamlarning o‘z ma’lumotlariga nisbatan huquqlarini kuchaytiradi. Foydalanuvchilar o‘z ma’lumotlari bilan nima bo‘layotganini bilib borishi va ularga qanday ishlov berilayotganini tushunishi kerak. Shu bilan birga, ular o‘z ma’lumotlarini to‘plashni, saqlashni va ishlatishni istamagan holda, o‘z ma’lumotlarini o‘zgartirish yoki o‘chirib tashlash huquqiga egadirlar.

GDPR ning kiberjinoyatlar va ma’lumotlar xavfsizligi bilan bog‘liqligi. GDPR o‘zining qat’iy talablaridan biri sifatida kiberjinoyatlar va ma’lumotlar xavfsizligini alohida ta’kidlaydi. Xususan, shaxsiy ma’lumotlarni to‘plash yoki ishlov berishdagi noqonuniy harakatlar, masalan, kiberhujumlar yoki ma’lumotlarni o‘g‘irlash GDPR bilan jiddiy ravishda buzilishi hisoblanadi. Shuningdek, GDPR, ma’lumotlarni noto‘g‘ri ishlov berish yoki saqlash holatlarida, tizimning xavfsizligi va shaxsiy ma’lumotlarni saqlash bo‘yicha talablarni buzganlikni belgilaydi.

GDPR, kiberjinoyatlarni aniqlash va ularga qarshi kurashishda davlatlar va kompaniyalar o‘rtasida hamkorlikni talab qiladi. Ma’lumotlarni himoya qilish bo‘yicha yangi mexanizmlar, tizimlarda kiberhujumlarni oldini olish va ma’lumotlarni o‘g‘irlanishiga yo‘l qo‘ymaslik uchun ilg‘or texnologiyalarni tatbiq etishni rag‘batlantiradi. Masalan, kiberxavfsizlikni ta’minlashda **kriptografiya**, **ma’lumotlarni shifrlash** va **multi-faktorli autentifikatsiya** kabi xavfsizlik choralarini qo‘llashni talab qiladi.

2. Yevropada boshqa himoya mexanizmlari. GDPRdan tashqari, Yevropa Ittifoqi kiberjinoyatlar bilan kurashish va axborot xavfsizligini ta’minlashda boshqa bir qancha muhim mexanizmlar yaratgan. Ushbu mexanizmlar, axborot tizimlarining xavfsizligini ta’minlash, kiberhujumlarni oldini olish va kiberjinoyatlar bilan bog‘liq risklarni boshqarishning muhim vositalarini taqdim etadi.

NIS Directive (Network and Information Security Directive). NIS Direktivi, 2016-yilda Yevropa Ittifoqi tomonidan qabul qilingan va Yevropa Ittifoqi mamlakatlarini kiberxavfsizlikni kuchaytirishga chaqiradi. Ushbu direktiva, yuqori xavfli infratuzilma (elektr energiyasi, transport, banklar va boshqalar) va raqamli xizmatlar (internet xizmatlari, raqamli platformalar) uchun xavfsizlik talablarini belgilaydi. NIS direktivasi barcha Yevropa Ittifoqi a’zolari uchun majburiydir va ular kiberhujumlar, tarmoq xavfsizligi va tizim buzilishlari bilan kurashishda o‘z resurslarini va choralarini yaxshilashlari lozim.

Cybersecurity Act (Kiberxavfsizlik to‘g‘risidagi qonun). 2019-yilda Yevropa Ittifoqi kiberxavfsizlik bo‘yicha yangi qonunni qabul qildi, bu esa kiberxavfsizlikni kuchaytirishga yordam beradi va Yevropaning barcha davlatlarida bir xilda kiberxavfsizlikni ta’minlashni nazarda tutadi. Cybersecurity Act, kiberxavfsizlikni boshqarish va kiberhujumlarni oldini olishda davlatlar o‘rtasidagi hamkorlikni kuchaytiradi va yangi xavfsizlik me’yorlari yaratadi.

ePrivacy Directive (Elektron maxfiylik to‘g‘risidagi Direktiva). ePrivacy Directive Yevropa Ittifoqida elektron aloqa va raqamli axborot almashinuvi sohasidagi maxfiylikni ta’minlashga qaratilgan qonunlardir. U, ma’lumotlarni yig‘ish va tarmoqlar orqali almashish bilan bog‘liq bo‘lgan maxfiylikni himoya qilishga qaratilgan. ePrivacy Direktivasining maqsadi, foydalanuvchilarning shaxsiy ma’lumotlarini va kommunikatsiyalarini himoya qilish va ularni noqonuniy ishlov berishdan himoya qilishdir.

Xulosa qilib aytganda, Yevropa Ittifoqi kiberjinoyatlarga qarshi kurashish va axborot xavfsizligini ta’minlash uchun keng qamrovli yuridik asoslarni ishlab chiqqan. **GDPR** bu sohada asosiy huquqiy hujjat bo‘lib, shaxsiy ma’lumotlarni himoya qilishga qaratilgan qat’iy qoidalar belgilaydi. Shuningdek, **NIS Directive**, **Cybersecurity Act** va **ePrivacy Directive** kabi hujjatlar ham axborot tizimlarining xavfsizligini ta’minlashda muhim o‘rin tutadi. Yevropa Ittifoqining bu qonun va mexanizmlari, kiberjinoyatlarga qarshi kurashish, shaxsiy ma’lumotlarni himoya qilish va kiberhujumlarning oldini olishga qaratilgan samarali yuridik va texnologik yondashuvlarni taqdim etadi.

Rossiya va Xitoy: Axborot Suverenitetiga asoslangan yondashuv. Rossiya va Xitoy kiberjinoyatlar va kiberxavfsizlikni tartibga solishdagi yondashuvlarini axborot suvereniteti asosida qurmoqda. Axborot suvereniteti – bu davlatlarning o‘z hududidagi axborot va kommunikatsiya texnologiyalarini nazorat qilish, ma’lumotlarni boshqarish va himoya qilish bo‘yicha mustaqil huquqiy va siyosiy huquqlarga ega bo‘lishini anglatadi. Ushbu yondashuvlar, xalqaro kiberjinoyatlarni aniqlash va ularga qarshi kurashishda an’anaviy yuridik va texnologik me’yorlardan farq qiladi va o‘ziga xos milliy xavfsizlikni ta’minlash maqsadida shakllangan.

1. Rossiyada axborot suvereniteti va kiberxavfsizlikka yondashuv. Rossiya Federatsiyasi, kiberxavfsizlik va axborot suverenitetini o‘zining ichki siyosatida va tashqi siyosatida muhim o‘rin tutgan element sifatida ko‘rishga intiladi. Rossiya hukumati kiberjinoyatlar bilan kurashishda axborot suverenitetiga asoslangan yondashuvni o‘zining asosiy strategik maqsadlaridan biri sifatida belgilaydi.

Rossiya Federatsiyasining kiberxavfsizlik strategiyasi. Rossiya kiberxavfsizlik sohasida o‘zining mustaqil yondashuvlarini rivojlantirishga intilmoqda, bu o‘z ichiga axborot muhitini mustahkamlash va xorijiy ta’sirlardan himoya qilishni oladi. 2016-yilda Rossiya hukumati kiberxavfsizlikni mustahkamlashga qaratilgan bir qancha hujjatlarni qabul qildi. Rossiya uchun kiberxavfsizlik nafaqat iqtisodiy yoki texnologik masala, balki milliy xavfsizlik va davlatning mustaqilligini ta’minlashning muhim vositasidir.

Rossiya o‘zining kiberxavfsizlik sohasidagi strategiyasini ishlab chiqishda davlatning nazorati ostidagi axborot tizimlarini yaratishga e’tibor qaratadi. Bu o‘z navbatida xorijiy ma’lumotlarga bog‘lanish va global

tarmoqdan tashqarida axborot almashinuvi bilan bog‘liq xavflarni kamaytirishga imkon beradi. Rossiyaning axborot suvereniteti siyosati xalqaro kiberjinoyatlar va axborot oqimlariga qarshi kurashishda davlatning nazoratini kuchaytirishni nazarda tutadi.

Axborot suvereniteti va xalqaro hamkorlik. Rossiya axborot suverenitetiga asoslangan kiberxavfsizlik siyosatida, xalqaro hamkorlikka ehtiyojni tan oladi, lekin bu hamkorlik, davlatlar o‘rtasida axborot va ma’lumotlarning chegaralangan o‘tkazilishi bilan bog‘liq bo‘ladi. Rossiya ko‘pincha internetning global bo‘ylab erkin oqimiga qarshi chiqadi va o‘zining davlat ichidagi internetni maxsus nazorat ostida ushlab turishni afzal ko‘radi. Shu nuqtai nazardan, Rossiya, xalqaro kiberjinoyatlarga qarshi kurashishda faqatgina o‘zining milliy qoidalariga asoslanib, milliy manfaatlarni ustuvor hisoblaydi.

2. Xitoyda axborot suvereniteti va kiberxavfsizlikka yondashuv. Xitoy kiberxavfsizlik va axborot suverenitetiga oid yondashuvni ko‘plab qonunlar, strategiyalar va amaliyotlar orqali amalga oshirmoqda. Xitoyning axborot suverenitetiga asoslangan yondashuvi davlatning ichki nazoratini kuchaytirish, xorijiy axborotlar va texnologiyalarga qarshi himoya qilish va milliy xavfsizlikni ta’minlashga qaratilgan.

Xitoyning kiberxavfsizlik qonunlari. Xitoy hukumati 2017-yilda qabul qilgan **Xitoy Kiberxavfsizlik To‘g‘risidagi Qonuni** (Cybersecurity Law of the People’s Republic of China) axborot suverenitetini ta’minlashning asosiy huquqiy ramkalaridan biri bo‘lib, mamlakatning kiberxavfsizlik siyosatini tartibga soladi. Ushbu qonun, kiberjinoyatlarni aniqlash va oldini olishda davlatning nazoratini kuchaytirish, shuningdek, xalqaro axborot oqimlaridan xavfsizlikni ta’minlash maqsadida qabul qilingan.

Xitoyning kiberxavfsizlik qonunlari shuningdek, milliy xavfsizlikni ta’minlash uchun xorijiy kompaniyalar va texnologiyalarga nisbatan qat’iy talablarni belgilaydi. Bu qonunlar, ma’lumotlarni saqlash va ishlov berishning maqsadga muvofiqligini ta’minlashda Xitoyning milliy qoidalariga muvofiq ishlashni taqozo qiladi. Xitoyda shuningdek, raqamli xizmatlar, axborot almashish va internetda amalga oshirilgan faoliyatlar ustidan keng qamrovli davlat nazorati mavjud.

Axborot suverenitetining Xitoydagi ta’minlanishi. Xitoyning axborot suverenitetiga asoslangan yondashuvi, axborot almashinishiga nisbatan davlatning qat’iy nazoratini o‘rnatishdan iborat. Xitoy hukumatining internetni

va raqamli infratuzilmani nazorat qilish siyosati, milliy xavfsizlikni ta’minlash va axborotlarni xorijiy tasirlar orqali o‘g‘irlanishiga yo‘l qo‘ymaslikka qaratilgan. Xitoy, shuningdek, xorijiy texnologiyalarni va internet platformalarini mamlakatda faoliyat yuritishi uchun o‘ziga xos talablarni qo‘yadi.

Xitoyning **Great Firewall** (Buyuk Firewall) tizimi, xorijiy axborot oqimlarini va internet xizmatlarini mamlakat ichki tarmog‘idan ajratib turish imkonini beradi. Bu tizim kiberjinoyatlar bilan kurashishda Xitoyning milliy axborot xavfsizligini ta’minlashga xizmat qiladi va kiberjinoyatlarning xalqaro ta’sirini minimallashtirishga yordam beradi.

Xalqaro kiberjinoyatlar va Yevropa Xitoyning yondashuvi. Xitoyning kiberxavfsizlik siyosati, davlatlarning axborot suverenitetini himoya qilishga intilayotgan boshqa davlatlar bilan o‘zaro hamkorlikka turtki bo‘lishi mumkin. Xitoy o‘zining kiberxavfsizlik strategiyasida axborotlarni himoya qilishni, xalqaro kiberjinoyatlarni aniqlash va ularga qarshi kurashishda o‘zining milliy manfaatlariga qarab ishlaydi. Biroq, Xitoyning bu yondashuvi ba’zi hollarda, xalqaro kiberjinoyatlar bilan kurashishda ko‘proq izolyatsiya va xavfsizlikni ta’minlashga qaratilgan bo‘lishi mumkin, bu esa davlatlar o‘rtasida hamkorlikka muammolar yaratadi.

Xulosa qilib aytganda, Rossiya va Xitoyning axborot suverenitetiga asoslangan yondashuvlari kiberjinoyatlar va kiberxavfsizlikni tartibga solishda o‘ziga xos milliy nazoratni ta’minlashga qaratilgan. Har ikkala davlatning yondashuvi, global axborot oqimlarini boshqarish, xorijiy ta’sirlardan himoya qilish va milliy xavfsizlikni ta’minlashga qaratilgan bo‘lib, ular xalqaro kiberjinoyatlarga qarshi kurashishda o‘zlarining milliy siyosatlarini amalga oshirmoqdalar. Bu yondashuvlar, kiberjinoyatlar bilan kurashishda xalqaro hamkorlikni kuchaytirish va global xavfsizlik tizimining samaradorligini ta’minlashni o‘z ichiga oladi.

2.3. Ekstraditsiya va Yurisdiksiya masalalari

Kiberjinoyatlar global xarakterga ega bo‘lib, ular bir yoki bir nechta davlatlarning hududiga ta’sir ko‘rsatishi mumkin. Bu holat, kiberjinoyatlar bilan kurashishda xalqaro hamkorlikni, yurisdiksiya va ekstraditsiya masalalarini o‘rganishni juda dolzarb qiladi. Yurisdiksiya va ekstraditsiya – kiberjinoyatlar bo‘yicha jinoiy javobgarlikni ta’minlashda, shuningdek, jinoyatchilarning qo‘lga olinishi va jazolanishi uchun zarur huquqiy asoslardir.

Ekstraditsiya – xalqaro hamkorlikning asosiy elementi. Ekstraditsiya, bir davlatning boshqa davlatdan jinoyatni amalga oshirgan shaxsni jazolash uchun talab qilish huquqidir. Kiberjinoyatlar koʻpincha davlatlararo chegaralarni kesib oʻtadi va shu sababli, jinoyatchilar bir mamlakatdan boshqasiga qochishi yoki yashirinish uchun internetni ishlatishlari mumkin. Kiberjinoyatlar uchun jinoyatga oid normalar va yuridik mezonlar turlicha boʻlishi mumkin, bu esa ekstraditsiya masalasida katta muammolarni keltirib chiqaradi. Masalan, kiberjinoyatlarning turlari, ularning ogʻirligi va xususiyatlari har xil boʻlishi mumkin, shuning uchun koʻp hollarda ekstraditsiya talablarini bajarishda davlatlar oʻrtasida kelishmovchiliklar yuzaga keladi.

Bundan tashqari, ba’zi davlatlar kiberjinoyatlar uchun ekstraditsiyani faqat muayyan shartlar asosida amalga oshiradilar, masalan, jinoyat uchun jazolash muddati va jinoyatchilarning millatiga qarab. Koʻpgina davlatlar oʻzlarining kiberjinoyatlarni jinoyat deb tan olgan qonunlari boʻlishiga qaramasdan, boshqa davlatlar oʻz yuridik tizimlarida bunday jinoyatlar uchun javobgarlikni tan olmaydi. Shu sababli, ekstraditsiya soʻrovlari ba’zan muayyan davlatlarning yurisdiktsiya va huquqiy qarorlariga qarab rad etilishi mumkin.

Yurisdiksiya masalalari. Kiberjinoyatlarning yurisdiktsiyasi masalasi xalqaro huquqdagi eng murakkab mavzulardan biridir. Kiberjinoyatlar koʻpincha bir nechta davlatlar oʻrtasidagi hududiy chegaralarni kesib oʻtadi, shuningdek, jinoyatlarning joylashuvi va amalga oshirilishi bilan bogʻliq boʻlgan ma’lumotlar koʻp hollarda xalqaro internet infratuzilmasiga bogʻliq boʻladi. Shu sababli, kiberjinoyatlar uchun yurisdiksiya masalasi juda murakkab boʻlib, bir nechta davlatlarning sud organlari va huquqiy tizimlari oʻrtasida kelishmovchiliklarga sabab boʻlishi mumkin.

Kiberjinoyatlarni sudlovchilarning yurisdiktsiyasi, asosan, quyidagi omillarga bogʻliq boʻladi:

- **Jinoyatni amalga oshirgan shaxsning joylashuvi:** Ba’zi davlatlar oʻz hududlarida amalga oshirilgan kiberjinoyatlarni sudlash huquqiga ega boʻladi, boshqa davlatlar esa kiberjinoyatlarning ta’siridan zarar koʻrgan shaxslarning yuridik manfaatlarini himoya qilishni afzal koʻrishadi.
- **Zarar koʻrgan davlat:** Kiberjinoyatlarning ta’siri bir yoki bir nechta davlatlarga boʻlishi mumkin, va zarar koʻrgan davlatlar, oʻz hududlarida amalga oshirilgan jinoyatlarni sudlashga intilishadi.

➢ **Xalqaro huquq va bitimlar:** Kiberjinoyatlar boʻyicha sudlovchi yurisdiktsiya koʻpincha davlatlar oʻrtasidagi xalqaro bitimlar, kelishuvlar va konventsiyalar asosida aniqlanadi. Misol uchun, **Budapesht Konvensiyasi** (2001-yilda imzolangan va kiberjinoyatlarga qarshi kurashish uchun asosiy xalqaro huquqiy hujjat) davlatlarga kiberjinoyatlarga qarshi birgalikda kurashish va sudlovchilik yurisdiksiyasini tartibga solish imkonini beradi.

Xalqaro xavfsizlik va kiberjinoyatlar bilan kurashishda Yurisdiksiya va Ekstraditsiya muammolari. Yurisdiksiya va ekstraditsiya masalalari nafaqat kiberjinoyatlarni aniqlash va jazolashda, balki davlatlar oʻrtasidagi hamkorlikni shakllantirishda ham muhim oʻrin tutadi. Xalqaro hamkorlikka asoslangan yuridik mexanizmlar, ayniqsa, kiberjinoyatlar boʻyicha huquqiy kelishuvlar va ekstraditsiya bitimlari muhim hisoblanadi. Biroq, kiberjinoyatlarning hududiy chegaralarga bogʻlanmagan xususiyati, baʼzan davlatlar oʻrtasida samarali ekstraditsiya jarayonlarini amalga oshirishni qiyinlashtiradi.

Shu nuqtai nazardan, xalqaro hamkorlikni mustahkamlash, kiberjinoyatlarning turli turlariga nisbatan yagona va samarali yuridik javobgarlikni oʻrnatish, ekstraditsiya va yurisdiksiya masalalarida davlatlar oʻrtasidagi kelishuvlarni muvofiqlashtirish dolzarb boʻladi. Bu masalalar, kiberjinoyatlar bilan kurashishdagi xalqaro huquqning samaradorligini oshirishga va jinoyatchilarning jazolanishi uchun zarur boʻlgan huquqiy asoslarga asoslanishga yordam beradi.

Xulosa qilib aytganda, Ekstraditsiya va yurisdiksiya masalalari kiberjinoyatlarni jinoyat deb eʼtirof etish va ularga qarshi kurashishda eng murakkab huquqiy masalalardan hisoblanadi. Kiberjinoyatlar global xarakterga ega boʻlgani sababli, davlatlar oʻrtasidagi hamkorlik, yurisdiksiyaga oid kelishuvlar va ekstraditsiya bitimlari jinoiy javobgarlikni taʼminlashda katta rol oʻynaydi. Biroq, kiberjinoyatlarning xususiyati va turli davlatlar oʻrtasidagi yuridik farqlar, bu masalalarga oid muammolarni murakkablashtiradi. Shu sababli, kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlik va kelishuvlarni yaxshilashga intilish zarur.

Jinoyat sodir etilgan joyni aniqlash muammosi. Kiberjinoyatlar, ularning xususiyati va amalga oshirilishi jihatidan, anʼanaviy jinoyatlardan sezilarli farq qiladi. Bu jinoyatlar asosan internet va boshqa raqamli texnologiyalar orqali amalga oshiriladi va koʻpincha geografik chegaralarni kesib oʻtadi. Shu sababli, kiberjinoyatlar boʻyicha yurisdiksiya va ekstraditsiya

masalalarida eng murakkab masalalardan biri jinoyat sodir etilgan joyni aniqlash muammosidir. Bu masala, huquqiy tizimlar oʻrtasida kelishmovchiliklarga va samarali sudlovchilik tizimining yoʻqligiga olib kelishi mumkin.

Kiberjinoyatlarning geografik chegaralari. Kiberjinoyatlarning hududiy chegarasi koʻpincha aniqlanmagan yoki nisbatan noaniq boʻladi. Kiberjinoyatlarni amalga oshirish uchun zarur boʻlgan texnologik infratuzilma, masalan, internet, koʻplab davlatlar oʻrtasidagi axborot almashinuvi va raqamli tarmoqlarni oʻz ichiga oladi. Bu esa jinoyatni amalga oshirgan shaxsning yoki jinoyatni sodir etish joyining aniq joylashuvi haqida aniq ma'lumot olishni qiyinlashtiradi. Bunday jinoyatlar oʻz vaqtida aniqlanmagan yoki ilgari tushunilmagan, shuning uchun ularni jinoyat deb tan olish va toʻgʻri yuridik javobgarlikni oʻrnatish uchun muhim huquqiy kelishuvlar zarur.

Masalan, biror shaxsning kompyuteri yoki tarmoq serveri bir davlatda joylashgan boʻlishi mumkin, ammo jinoyatni amalga oshirish uchun zarur boʻlgan ma'lumotlar yoki hujum boshqa davlat hududida amalga oshirilgan boʻlishi mumkin. Bu holatda, jinoyatni sodir etilgan joyni aniqlash ancha murakkablashadi, chunki koʻplab huquqiy tizimlar oʻrtasida har bir davlatning oʻziga xos yuridik qoidalari va muhokama qilish mexanizmlari mavjud.

Jinoyat sodir etish joyini aniqlashda yurisdiksiya masalalari. Kiberjinoyatlar koʻpincha internetda, ya'ni virtual muhitda sodir etiladi. Buning oqibatida, jinoyatning aniq joyi va geografik hududi aniqlashda qiyinchiliklar yuzaga keladi. Internetda sodir etilgan jinoyatning joyini aniqlash uchun uchta asosiy usul qoʻllanilishi mumkin:

- **Jinoyatchining manzilini aniqlash:** Koʻpincha jinoyatni amalga oshirgan shaxsning geografik joylashuvi yoki manzili asosida yurisdiktsiya belgilanadi. Biroq, internet orqali amalga oshirilgan jinoyatlarda jinoyatchining aniq joylashuvini topish juda qiyin, chunki ularning tarmoq faoliyati koʻplab serverlar orqali yoʻnaltiriladi va anonimlikni ta'minlash uchun VPN (virtual xususiy tarmoq) kabi texnologiyalar ishlatiladi.
- **Jinoyatni amalga oshirgan tarmoq joyi:** Ba'zan jinoyatning aniq joyi tarmoq serveri yoki saqlash joyi (masalan, ma'lumotlar bazasi)ning joylashuvi orqali aniqlanadi. Ammo, bu usulning samaradorligi ham, yuqorida ta'kidlanganidek, kiberjinoyatchilar koʻpincha serverlarni oʻz hududidan tashqarida joylashtirishadi, va bu holat joyni aniqlashni qiyinlashtiradi.

- **Zarar ko‘rgan shaxsning joylashuvi:** Kiberjinoyatlarning bir nechta ta’sirlangan tomonlari bo‘lishi mumkin, shuning uchun zarar ko‘rgan tomonning joylashuvi ham muhim ahamiyatga ega. Agar biror davlatda jinoyatning qurboni bo‘lgan shaxs yashasa, bu davlatda ham sudlovchi yurisdiktsiya bo‘lishi mumkin. Biroq, zarar ko‘rgan shaxsning joylashuvi aniq bo‘lsa ham, jinoyatning o‘zi turli davlatlarga ta’sir qilishi mumkin.

Xalqaro huquq va jinoyat sodir etgan joyni aniqlash. Xalqaro huquqda kiberjinoyatlarning sodir etilgan joyini aniqlash masalasi ancha murakkabdir, chunki bu sohada hali ham bir qator yuridik nomutanosibliklar mavjud. Ko‘p holatlarda, xalqaro huquqiy bitimlar yoki kelishuvlar, kiberjinoyatlarning joylashuvini aniqlashga yordam bermaydi, chunki ular odatda an’anaviy jinoyatlar uchun mo‘ljallangan. Shu bilan birga, ko‘plab davlatlar o‘rtasida kiberjinoyatlar bo‘yicha yuridik hamkorlikni mustahkamlash maqsadida bitimlar tuzilgan, ammo ularning ko‘plari aniq joyni aniqlashni talab qilmaydi.

Misol uchun, **Budapesht Konvensiyasi** (2001) kiberjinoyatlarga qarshi kurashishda bir nechta xalqaro yuridik mexanizmlarni belgilaydi, ammo bu konvensiya ham kiberjinoyatlarning aniq joyini aniqlash bo‘yicha qat’iy va bir xilda qo‘llaniladigan qoidalar yaratmaydi. Aksincha, u faqatgina davlatlarga kiberjinoyatlar bo‘yicha umumiy me’yorlarni belgilab beradi va hamkorlikni osonlashtiradi, lekin sudlovchi yurisdiktsiya masalalarini hal qilishda maxsus yondashuvlarni talab qiladi.

Praktik muammolar va yechimlar. Kiberjinoyatlarning geografik joyini aniqlashda yuzaga keladigan amaliy muammolarni hal qilish uchun bir qator yechimlar taklif qilinmoqda. Ularning ba’zilari quyidagilar:

- **Xalqaro hamkorlik va muvofiqlashtirish:** Xalqaro hamkorlikni kuchaytirish va huquqiy bitimlar asosida davlatlar o‘rtasida muvofiqlashtirilgan yuridik chora-tadbirlarni qo‘llash muhimdir. Misol uchun, davlatlar o‘rtasida kiberjinoyatlar bo‘yicha aniq yuridik mexanizmlar va bitimlarni ishlab chiqish zarur.
- **Texnologik yechimlar:** Jinoyat joyini aniqlashda yangi texnologiyalar, masalan, blockchain, raqamli izlar va trafikni kuzatish tizimlarini qo‘llash orqali jinoyatning aniq joyini aniqlash imkoniyatlari kengaytirilishi mumkin.
- **Yuridik moslashuvchanlik:** Yurisdiktsiyani aniqlashda yuridik tizimlarning moslashuvchanligini ta’minlash muhimdir. Bunday holatlarda

davlatlar o‘rtasida huquqiy yordamni tezkor tarzda ta’minlash uchun o‘zaro kelishuvlar tuzilishi kerak.

Xulosa qilib aytganda, Kiberjinoyatlarning geografik joyini aniqlash masalasi xalqaro jinoyat huquqi va yuridik tizimlar uchun katta qiyinchiliklarni keltirib chiqaradi. Bu masala kiberjinoyatlarni jinoyat deb tan olishda, davlatlar o‘rtasidagi hamkorlikni mustahkamlashda, shuningdek, adolatli va samarali sudlovchi yurisdiktsiyani ta’minlashda muhim ahamiyatga ega. Shu bois, kiberjinoyatlarning joylashuvini aniqlashda xalqaro hamkorlikni yaxshilash, texnologik yechimlardan foydalanish va yuridik moslashuvchanlikni ta’minlash zarur.

Ko‘p davlatlar ishtirokidagi jinoyatlar. Kiberjinoyatlar zamonaviy jinoyatlarning yangi shakli bo‘lib, ko‘plab davlatlar o‘rtasidagi hududiy chegaralarni kesib o‘tadi. Bular, ayniqsa, onlayn xakerlik, axborot o‘g‘irlash, kompaniyalar va davlatlarga qarshi kiberhujumlar kabi jinoyatlar bo‘lib, bir nechta mamlakatlarning hududiga ta’sir qiladi. Bu turdagi jinoyatlar o‘ziga xos tarzda ko‘p davlatlar ishtirokida amalga oshirilishi mumkin, chunki kiberjinoyatchilar tomonidan amalga oshirilgan hujumlar ko‘pincha bir nechta mamlakatlar infratuzilmasini, tizimlarini yoki foydalanuvchilarini ta’sir qiladi.

Ko‘p davlatlar ishtirokidagi jinoyatlar masalasi, nafaqat jinoyatni sodir etish joyi, balki jinoyatchilarni aniqlash, ularni jinoiy javobgarlikka tortish va jazolash bilan bog‘liq muammolarni ham keltirib chiqaradi. Bunda ekstraditsiya, yurisdiksiya, sudlovchilik va hamkorlik masalalari dolzarb bo‘lib, ular ko‘plab davlatlar o‘rtasida yuridik kelishuvlar va xalqaro bitimlar doirasida hal etiladi.

Ko‘p davlatlar ishtirokidagi jinoyatlarning xususiyatlari. Ko‘p davlatlar ishtirokidagi jinoyatlar bir nechta mamlakatlar hududida sodir etilishi mumkin va ular turli shakllarda namoyon bo‘ladi:

✓ **Xalqaro xakerlik hujumlari:** Xakerlar bir necha davlatlarning axborot tizimlariga kirish orqali ma’lumotlarni o‘g‘irlaydilar yoki zararli dasturlarni tarqatadilar. Bunday jinoyatlar ko‘pincha bir nechta davlatlarning infratuzilmasiga ta’sir ko‘rsatadi va shu sababli ularni hal qilishda ko‘plab yurisdiktsiyalarni hisobga olish zarur.

✓ **Xalqaro firibgarlik va moliyaviy jinoyatlar:** Bank tizimlariga yoki moliyaviy tashkilotlarga qarshi amalga oshirilgan xakerlik hujumlari yoki firibgarliklar, masalan, pul o‘g‘irliklari, naqd pul yoki valyuta o‘tkazmalarini

noqonuniy tarzda amalga oshirish holatlari, koʻplab mamlakatlarga zarar yetkazadi.

✓ **Axborot jinoyatlari:** Dasturlarni noqonuniy tarzda ishlab chiqish yoki axborot bazalarini oʻgʻirlash, davlatlarning axborot xavfsizligi tizimlariga ta’sir qilish, shuningdek, oʻzaro axborot almashish orqali amalga oshirilgan jinoyatlar koʻp davlatlar ishtirokida sodir etilishi mumkin.

Koʻp davlatlar ishtirokidagi jinoyatlar juda tez amalga oshirilishi mumkin, chunki ular internetda, onlayn platformalarda yoki global tarmoqlarda sodir etiladi. Bu turdagi jinoyatlar xalqaro hamkorlikni talab etadi, chunki ular bir mamlakatning ichki huquqiy tizimi bilan hal etilishi qiyin boʻladi.

Ekstraditsiya masalalari. Koʻp davlatlar ishtirokidagi jinoyatlar boʻyicha jinoyatchilarni jazolashda ekstraditsiya masalalari juda muhim rol oʻynaydi. Ekstraditsiya — bu bir davlatning boshqa davlatdan jinoyatni amalga oshirgan shaxsni olib kelish va jinoiy javobgarlikka tortish uchun soʻrovnoma yuborish jarayonidir. Kiberjinoyatlar koʻplab davlatlar oʻrtasida sodir boʻlishi va ular koʻpincha hududiy chegaralarni kesib oʻtadi. Shu sababli, ekstraditsiya jarayonlari odatda juda murakkab boʻladi, chunki ba’zi davlatlar oʻzlarining yuridik tizimlariga yoki kiberjinoyatlar boʻyicha maxsus normativ-huquqiy tartiblarga ega emaslar.

Koʻp davlatlar ishtirokidagi jinoyatlarda ekstraditsiya soʻrovining muvaffaqiyatli amalga oshirilishi uchun quyidagi omillar muhimdir:

✓ **Ekstraditsiya bitimlari:** Davlatlar oʻrtasida oʻzaro ekstraditsiya bitimlari mavjudligi kiberjinoyatchilarni olib kelish imkoniyatlarini oshiradi. Ammo, har bir davlatning oʻz ekstraditsiya siyosati va yuridik tizimi mavjud, shuning uchun ba’zan, bir davlat jinoyatni sodir etgan shaxsni ekstraditsiya qilishni rad etishi mumkin.

✓ **Jinoyatning xalqaro tabiatga ega boʻlishi:** Agar jinoyat bir necha davlatning hududlariga zarar yetkazgan boʻlsa, ekstraditsiya jarayoni sodir boʻlishi uchun xalqaro hamkorlikni kuchaytirish zarur boʻladi. Bu yerda global kelishuvlar va yuridik kelishuvlar (masalan, **Budapesht Konvensiyasi**) juda muhim ahamiyatga ega.

✓ **Jinoyatchining yashash joyi:** Koʻpincha, kiberjinoyatni amalga oshirgan shaxs boshqa mamlakatda yashashi mumkin, bu esa ekstraditsiyani amalga oshirishni yanada murakkablashtiradi. Shu sababli, davlatlar oʻrtasida ekstraditsiya kelishuvlari mavjud boʻlishi muhimdir.

Yurisdiksiya masalalari. Koʻp davlatlar ishtirokidagi jinoyatlar yurisdiksiya masalasini ham oʻrnatadi. Kiberjinoyatlar odatda bir davlatning hududidan boshqa davlat hududiga oʻtadi va bu holatda jinoyatni sudlovchi yurisdiktsiyani aniqlash juda muhimdir. Bunday jinoyatlar uchun quyidagi yurisdiksiya masalalari yuzaga keladi:

- ✓ **Jinoyat sodir etilgan joyning aniqlanishi:** Kiberjinoyatlarning koʻp davlatlar ishtirokidagi holatida, jinoyatning aniq sodir etilgan joyini aniqlash juda qiyin boʻlishi mumkin. Ba’zan jinoyat asosan internetda sodir boʻladi, bu esa davlatlar oʻrtasida sudlovchilik va yurisdiktsiya masalalarini murakkablashtiradi.
- ✓ **Zarar koʻrgan davlatlar:** Koʻp davlatlar ishtirokidagi jinoyatlarda zarar koʻrgan tomonlar bir nechta boʻlishi mumkin. Bunday holatlarda, har bir zarar koʻrgan davlat oʻz hududidagi sudlovchilikni amalga oshirishni talab qilishi mumkin, bu esa yurisdiksiya qarorlarini murakkablashtiradi.
- ✓ **Jinoyatchining joylashuvi:** Ba’zan jinoyatchining joylashuvi ham yurisdiksiyani aniqlashda muhim omil hisoblanadi. Agar jinoyatchi bir davlat hududida boʻlsa, oʻsha davlat sudlovchilikni oʻtkazish uchun yurisdiktsiyaga ega boʻlishi mumkin. Biroq, koʻplab davlatlar, shu jumladan, **Budapesht Konvensiyasining** qoidalariga asosan, oʻzaro hamkorlikda, bir davlat jinoyatchini boshqa davlatga ekstraditsiya qilishi mumkin.

Xalqaro hamkorlik va bitimlar. Koʻp davlatlar ishtirokidagi jinoyatlar bilan kurashishda xalqaro hamkorlik va bitimlar muhim ahamiyatga ega. Xalqaro huquqda bir necha bitimlar mavjud boʻlib, ular davlatlarga kiberjinoyatlar boʻyicha hamkorlikni kuchaytirish va sudlovchilikni amalga oshirishda yordam beradi:

- ✓ **Budapesht Konvensiyasi (2001):** Ushbu konvensiya, kiberjinoyatlarga qarshi kurashish va davlatlar oʻrtasida hamkorlikni kuchaytirish uchun asosiy xalqaro huquqiy hujjatlardan biridir. U kiberjinoyatlar bilan kurashishda yurisdiktsiya va ekstraditsiya masalalarini tartibga soladi.
- ✓ **Xalqaro kriminologik hamkorlik bitimlari:** Koʻplab xalqaro tashkilotlar, jumladan, **Interpol** va **Europol**, davlatlar oʻrtasida kiberjinoyatlar boʻyicha hamkorlikni ta’minlaydi. Bu tashkilotlar kiberjinoyatchilarni aniqlash va ularga qarshi kurashishda xalqaro hamkorlikni mustahkamlashda muhim rol oʻynaydi.

Xulosa qilib aytganda, koʻp davlatlar ishtirokidagi jinoyatlar — kiberjinoyatlar sohasida yuzaga kelgan dolzarb huquqiy muammolardan biridir. Bu turdagi jinoyatlar koʻplab davlatlarning hududiga ta’sir qilishi va davlatlar oʻrtasidagi hamkorlikni talab qiladi. Ekstraditsiya va yurisdiksiya masalalari, shu bilan birga, xalqaro hamkorlikning rivojlanishi bu masalalarning muvaffaqiyatli hal etilishini ta’minlash uchun muhimdir. Kiberjinoyatlar bilan kurashishda xalqaro yuridik mexanizmlar va bitimlar muhim ahamiyatga ega, chunki ular koʻplab davlatlarning hamkorligini ta’minlaydi.

Ekstraditsiya qilishdagi siyosiy va huquqiy toʻsiqlar. Kiberjinoyatlar boʻyicha davlatlar oʻrtasidagi hamkorlik, ayniqsa, ekstraditsiya jarayonida koʻplab siyosiy va huquqiy toʻsiqlarga duch keladi. Ekstraditsiya — bu jinoyatni sodir etgan shaxsni bir davlatdan boshqa davlatga olib kelish va sudlov uchun jinoiy javobgarlikka tortish jarayonidir. Bu jarayon xalqaro huquq va davlatlar oʻrtasidagi bitimlar asosida amalga oshiriladi, biroq kiberjinoyatlarning murakkab tabiati va xalqaro hamkorlikdagi cheklovlar bu jarayonni ancha qiyinlashtiradi.

Siyosiy toʻsiqlar. Ekstraditsiya jarayonidagi siyosiy toʻsiqlar, koʻpincha, davlatlarning ichki siyosatiga, tashqi siyosatga va xalqaro aloqalariga bogʻliq. Siyosiy toʻsiqlarni quyidagi asosiy omillar orqali koʻrib chiqish mumkin:

- **Diplomatik va siyosiy munosabatlar.** Davlatlar oʻrtasidagi diplomatik munosabatlar ekstraditsiya jarayonining muvaffaqiyatini ta’minlashda katta ahamiyatga ega. Agar ikki davlat oʻrtasidagi siyosiy aloqalar kuchli va hamkorlikni ta’minlashga tayyor boʻlsa, ekstraditsiya jarayoni ancha soddalashadi. Aksincha, siyosiy masalalar, iqtisodiy sanktsiyalar, yoki diplomatik nizolar mavjud boʻlsa, ekstraditsiya soʻrovlarini rad etish ehtimoli ortadi. Masalan, davlatlar oʻrtasida mavjud boʻlgan siyosiy qarama-qarshiliklar yoki bir mamlakatning kiberjinoyatchini ekstraditsiya qilishda qandaydir siyosiy maqsadlar kuzatishlari ekstraditsiya jarayoniga toʻsiq boʻlishi mumkin.
- **Siyosiy jinoyatlarni ajratish.** Koʻp davlatlar, ekstraditsiya talabini rad etishning asosiy sabablaridan biri sifatida, "siyosiy jinoyat" tushunchasini qoʻllashadi. Xalqaro huquqda, siyosiy jinoyatlar, odatda, davlatga qarshi jinoyatlar sifatida tasniflanadi va bunday jinoyatlar ekstraditsiya qilinmasligi mumkin. Misol uchun, aksariyat davlatlar oʻz fuqarolarini siyosiy sabablarga koʻra boshqa davlatga ekstraditsiya qilishni rad etadilar. Kiberjinoyatlar

koʻpincha davlatlar oʻrtasidagi siyosiy yoki ideologik kelishmovchiliklarga asoslangan boʻlishi mumkin, bu esa ekstraditsiya masalalarida murakkabliklarga olib keladi.

- **Siyosiy bosim va diplomatik muomala.** Ba'zi holatlarda, ekstraditsiya qilish toʻgʻrisidagi soʻrovlar siyosiy bosimning bir shakli boʻlishi mumkin. Masalan, davlatlarning oʻzining xalqaro siyosiy manfaatlarini himoya qilish yoki diplomatik hamkorlikni kuchaytirish uchun ekstraditsiya talablarini yuborishi mumkin. Bunday siyosiy bosimlar davlatlarning ekstraditsiya qilishni rad etishiga sabab boʻlishi mumkin, chunki ular oʻzining siyosiy nuqtai nazarini ilgari surishga harakat qiladilar.

Huquqiy toʻsiqlar. Ekstraditsiya jarayonidagi huquqiy toʻsiqlar, asosan, davlatlar oʻrtasidagi huquqiy tizimlarning farqlari, xalqaro huquq me'yorlarining uygʻun emasligi va ekstraditsiya bitimlarining mavjud emasligi bilan bogʻliq. Bu toʻsiqlarni quyidagi nuqtalar orqali tahlil qilish mumkin:

- **Ekstraditsiya bitimlarining mavjud emasligi yoki cheklanganligi.** Davlatlar oʻrtasidagi ekstraditsiya bitimlarining mavjudligi yoki mavjud boʻlmasligi, kiberjinoyatchilarni boshqa davlatlarga olib kelish jarayonini belgilovchi asosiy omil hisoblanadi. Ba'zi davlatlar oʻrtasida ekstraditsiya bitimlari mavjud boʻlmasligi yoki ular faqat ma'lum jinoyatlarni oʻz ichiga olishi kiberjinoyatlar boʻyicha ekstraditsiya jarayonlarini qiyinlashtirishi mumkin. Misol uchun, ba'zi davlatlar faqat oʻz hududida sodir etilgan jinoyatlar boʻyicha ekstraditsiya qilishga ruxsat berishi mumkin. Shu bilan birga, davlatlar oʻrtasidagi ekstraditsiya bitimlarining noaniqligi va nizolar mavjud boʻlsa, ekstraditsiya jarayoni uzayishi yoki rad etilishi mumkin.
- **Xalqaro huquqning uyg'un bo'lmasligi.** Koʻplab davlatlar oʻrtasida xalqaro huquqiy normalar farq qiladi, bu esa ekstraditsiya jarayonini murakkablashtiradi. Misol uchun, kiberjinoyatlar uchun jazolar turli mamlakatlarda farq qilishi mumkin, va bu, oʻz navbatida, ekstraditsiya qilishda qoʻllaniladigan mezonlarga ta'sir qiladi. Ba'zi davlatlar kiberjinoyatchilarga qarshi an'anaviy jinoyatlar kabi yondashadilar, boshqalari esa maxsus jinoyat sifatida koʻrishadi, bu esa ekstraditsiya bitimlarining mavjudligini yoki talablarini tasdiqlashda turli yondashuvlarni yuzaga keltiradi.
- **Jinoyatchilikni aniqlash va dalillarni rasmiylashtirishdagi farqlar.** Ekstraditsiya qilishda kiberjinoyatchilarni aniqlash va ularning jinoyatlarini isbotlashda huquqiy toʻsiqlar yuzaga kelishi mumkin. Kiberjinoyatlar koʻpincha transchegaraviy xususiyatga ega boʻlganligi sababli,

jinoyatni isbotlashda va dalillarni rasmiylashtirishda ba’zi davlatlar o‘rtasida farqlar mavjud. Ba’zi davlatlar axborot texnologiyalarini tartibga soluvchi o‘z qonunlarini mustahkamlagan, boshqalari esa ular bo‘yicha aniq huquqiy mexanizmlarga ega emas. Shuning uchun, kiberjinoyatchilarni bir davlatdan boshqa davlatga ekstraditsiya qilishda isbotlangan dalillar va huquqiy me’yorlarning uyg‘unlashmaganligi ekstraditsiya jarayonining to‘siqlariga aylanishi mumkin.

- **Axborot xavfsizligi va maxfiylik.** Ba’zi davlatlar axborot xavfsizligi yoki milliy xavfsizlikni himoya qilish maqsadida, boshqa davlatlarga o‘z hududidagi jinoyatchilarni ekstraditsiya qilishni rad etishadi. Kiberjinoyatlarni aniqlashda ishlatilgan texnologiyalar va ma’lumotlar ko‘pincha yuqori darajadagi maxfiylikka ega bo‘ladi. Shu sababli, davlatlar, o‘zining axborot xavfsizligini yoki maxfiylikni himoya qilish maqsadida, kiberjinoyatchilarni ekstraditsiya qilishni rad etishlari mumkin.

Ekstraditsiya to‘siqlarini engishning imkoniyatlari. Bunday siyosiy va huquqiy to‘siqlarni engish uchun xalqaro hamkorlikni kuchaytirish, huquqiy tizimlarni uyg‘unlashtirish va kiberjinoyatlar bo‘yicha aniq va xalqaro tan olingan bitimlar ishlab chiqish zarur. Ekstraditsiya bitimlarini kengaytirish va huquqiy asoslarni yangilash kiberjinoyatlar bo‘yicha jinoyatchilarni jazolashni osonlashtiradi. Shuningdek, davlatlar o‘rtasidagi axborot almashish mexanizmlarini rivojlantirish va kiberjinoyatlar bo‘yicha global hamkorlikni ta’minlash muhimdir. Xalqaro yuridik hujjatlar, jumladan **Budapesht Konvensiyasi**, davlatlar o‘rtasidagi to‘siqlarni kamaytirishga yordam beradi.

Xulosa qilib aytganda, Ekstraditsiya va yurisdiksiya masalalari kiberjinoyatlar bilan kurashishda eng murakkab huquqiy muammolardan biridir. Siyosiy va huquqiy to‘siqlar ekstraditsiya jarayonini kechiktirishi yoki rad etilishiga olib kelishi mumkin. Biroq, xalqaro hamkorlik va bitimlar orqali bu to‘siqlarni engish va kiberjinoyatlarni jazolash jarayonini soddalashtirish mumkin.

2.4. Elektron dalillarning huquqiy maqomi

Kiberjinoyatlar bo‘yicha sudlov jarayonida elektron dalillar muhim o‘rin tutadi, chunki ko‘plab kiberjinoyatlar faqat raqamli tizimlar, tarmoqlar va axborot texnologiyalari yordamida sodir etiladi. Elektron dalillar, ya’ni raqamli axborot yoki ma’lumotlar, jinoyatni isbotlash, shaxsni javobgarlikka tortish va jinoyatni aniqlashda muhim vosita hisoblanadi. Biroq, elektron

dalillarni to‘plash, saqlash va taqdim etishdagi huquqiy muammolar xalqaro yuridik tizimning dolzarb masalalaridan biri hisoblanadi.

Elektron dalillarning huquqiy maqomi, ularning qonuniyligi, haqiqatga mosligi va adolatli sudlovni ta’minlashdagi o‘rni yuridik tizimlar o‘rtasidagi farqlarga, shuningdek, xalqaro huquqning rivojlanishiga bog‘liqdir. Elektron dalillarni taqdim etishda va sudlov jarayonida ularning ishonchliligi va qonuniyligini ta’minlash juda muhimdir, chunki raqamli ma’lumotlar osonlik bilan manipulyatsiya qilinishi yoki o‘zgartirilishi mumkin. Shuningdek, elektron dalillarning o‘ziga xos xususiyatlari, masalan, ularning virtual xususiyati, axborot tizimlarida saqlanishi va uzoq masofada yuborilishi, bunday dalillarning huquqiy maqomini aniqlashda qo‘shimcha muammolarni keltirib chiqaradi.

Elektron dalillarning yuridik tan olinishi. Elektron dalillarni sudda tan olish, ularning haqiqiyligini va qonuniyligini isbotlash, kiberjinoyatlarni aniqlashda muhim qadamdir. Biroq, ko‘plab davlatlar uchun elektron dalillarning yuridik maqomi hali to‘liq aniqlanmagan. Ba’zi yurisdiktsiyalar elektron dalillarni qog‘ozdagi hujjatlar kabi sudda qabul qilishadi, boshqalari esa faqat elektron formatdagi ma’lumotlarni qayd etish va taqdim etishda maxsus tartib va me’yorlarga rioya qilishni talab etadi. Xalqaro miqyosda elektron dalillarni tan olish masalasi yanada murakkablashadi, chunki turli davlatlar axborot xavfsizligi va maxfiylikka oid turli qonunlarga ega bo‘lib, bu elektron dalillarni o‘zaro qabul qilishni qiyinlashtiradi.

Elektron dalillarni yig‘ish, saqlash va taqdim etishdagi huquqiy masalalar. Elektron dalillarning huquqiy maqomi shuningdek, ularni yig‘ish, saqlash va taqdim etish tartibi bilan ham chambarchas bog‘liq. Yuridik tizimlar o‘rtasidagi farqlar, masalan, "adalatli sud" tamoyili, maxfiylikni saqlash va fuqarolarning huquqlarini himoya qilish zarurati elektron dalillarni to‘plashda sezilarli cheklovlar kiritadi. Elektron dalillarni to‘plash va saqlashda huquqiy asoslarning mavjudligi, ularning qonuniy ravishda olinganligini va muayyan jinoyatga oidligini tasdiqlash jarayonlarini soddalashtiradi. Biroq, elektron dalillarni noto‘g‘ri yoki noqonuniy yig‘ish va saqlash, ular sudda ishonchli dalil sifatida e’tirof etilmasligiga olib kelishi mumkin.

Elektron dalillarning xalqaro yuridik tan olinganligi. Xalqaro huquqning rivojlanishiga parallel ravishda, elektron dalillarning xalqaro yuridik tan olinganligi ham muhim ahamiyatga ega. Bugungi kunda, ko‘plab xalqaro bitimlar va konvensiyalar elektron dalillarning sudda qo‘llanishini

tasdiqlaydi. Masalan, **Budapesht konvensiyasi** va **Nyu-York konvensiyasi** kabi xalqaro huquqiy hujjatlar, raqamli dalillarni o‘tkazish va to‘plashda davlatlar o‘rtasidagi hamkorlikni mustahkamlaydi. Shuningdek, elektron dalillarni olish va ularga huquqiy baho berish, sudlar va prokuraturalar o‘rtasida global hamkorlikni rivojlantirishga yordam beradi.

Biroq, elektron dalillarning xalqaro miqyosda qabul qilinishida ba’zi qiyinchiliklar mavjud. Har bir davlatning yuridik tizimi va axborot xavfsizligi qonunlari o‘ziga xos va bu davlataro aloqalarga to‘sqinlik qilishi mumkin. Shuningdek, turli mamlakatlarda elektron dalillarning saqlanishi va uzatilishi bilan bog‘liq qonuniy cheklovlar ham muammolarni keltirib chiqaradi. Bu xususiyatlar global miqyosda bir xil yuridik standartlarni yaratish va elektron dalillarni xalqaro sudlarda tan olishni osonlashtirishni talab qiladi.

Xulosa qilib aytganda, Elektron dalillarning huquqiy maqomi kiberjinoyatlar bo‘yicha sudlov jarayonining samaradorligini ta’minlashda muhim omil hisoblanadi. Ularning qonuniyligi va haqiqiyligini isbotlash jarayoni, maxsus qonunlar, xalqaro bitimlar va davlatlar o‘rtasidagi hamkorlik orqali yanada soddalashtirilishi kerak. Elektron dalillarni yig‘ish, saqlash va taqdim etishda birxillikni ta’minlash, shuningdek, ularni xalqaro miqyosda qonuniy tan olish muhim ahamiyatga ega bo‘lib, kiberjinoyatlarni jazolashda samarali yuridik mexanizmlarning shakllanishini ta’minlaydi.

Elektron dalil sifatida server yozuvlari va IP-manzillar. Kiberjinoyatlar bo‘yicha sudlov jarayonida raqamli dalillar, jumladan, server yozuvlari va IP-manzillar, jinoyatni isbotlashda asosiy rol o‘ynaydi. Elektron tizimlar orqali amalga oshirilgan jinoyatlarning faqat raqamli izlari, ya’ni server yozuvlari va IP-manzillar orqali aniqlanishi mumkin. Bu turdagi dalillar ko‘pincha jinoyatni o‘tkazgan shaxsni aniqlash va uning jinoyatga aloqadorligini tasdiqlash uchun ishlatiladi. Ammo bunday dalillarni to‘plash, saqlash va sudda taqdim etish jarayonida bir qator huquqiy va texnik muammolar yuzaga keladi.

Server yozuvlari: ma’lumotlarni saqlash va huquqiy muammolar. Server yozuvlari (logs) kompyuter tarmoqlarida yoki internetdagi serverlarda foydalanuvchilarning harakatlarini yozib boradigan tizimlar hisoblanadi. Bu yozuvlar, odatda, foydalanuvchining tizimga kirish va undan chiqish vaqti, amalga oshirilgan so‘rovlar, yuklangan yoki o‘zgartirilgan fayllar va boshqa harakatlar haqida ma’lumot beradi. Kiberjinoyatlar holatida server yozuvlari jinoyatchining faoliyatini aniqlashda asosiy dalil bo‘lib xizmat qilishi mumkin.

Masalan, xakerlik hujumlari, phishing hujumlari yoki viruslar orqali amalga oshirilgan hujumlar server yozuvlari yordamida aniqlanadi.

Biroq, server yozuvlarining ishonchli va qonuniyligini tasdiqlashda bir nechta huquqiy muammolar mavjud. Birinchidan, server yozuvlari o‘zining xususiyati bilan osonlikcha tahrirlanishi yoki o‘zgartirilishi mumkin, bu esa ularning sudda ishonchli dalil sifatida qabul qilinishini murakkablashtiradi. Shuningdek, server yozuvlarining qayerda va qanday saqlanishi, ularning davomiyligi va ma’lumotlar xavfsizligi masalalari ham ahamiyatga ega. Ko‘plab mamlakatlarda server yozuvlarini saqlash muddatlari va shaxsiy ma’lumotlarning maxfiyligini ta’minlashga oid qat’iy qonunlar mavjud bo‘lib, bu dalillarni to‘plashda qo‘shimcha cheklovlar yaratadi.

IP-manzillar: huquqiy ahamiyati va masalalar. IP-manzil (Internet Protocol address) - bu internetda yoki tarmoqda alohida qurilmaning identifikatsiya qilish uchun ishlatiladigan raqamli manzil hisoblanadi. Kiberjinoyatlar holatida IP-manzil jinoyatni amalga oshirgan shaxsni aniqlashda juda muhim axborot beradi. IP-manzil, bir tomondan, jinoyatni amalga oshirgan qurilmaning tarmoqdagi o‘rni va uning qayerdan ishlatilganini ko‘rsatadi. Boshqa tomondan, IP-manzilni to‘g‘ri tahlil qilish orqali jinoyatchining joylashuvini yoki boshqa aloqador ma’lumotlarni aniqlash mumkin.

Biroq, IP-manzilning huquqiy maqomi va uning ishonchliligi bilan bog‘liq ba’zi muammolar mavjud. Masalan, dinamik IP-manzillar, ya’ni vaqtincha beriladigan IP-manzillar, jinoyatni amalga oshirgan shaxsni aniqlashda qiyinchiliklar keltirib chiqaradi, chunki ular tez-tez o‘zgarib turadi va ba’zan jinoyatning aynan qaysi shaxs tomonidan amalga oshirilganini aniq bilish qiyin bo‘ladi. Bundan tashqari, IP-manzilni faqatgina bir qurilma bilan bog‘lash mumkin emas, chunki bitta IP-manzil bir nechta foydalanuvchilar tomonidan ishlatilishi mumkin, masalan, umumiy tarmoqda yoki kafe, ofis kabi jamoat joylarida.

IP-manzillarni yuridik jihatdan talqin qilish. IP-manzilning yuridik maqomini belgilashda, shu jumladan uning jinoyat dalili sifatida qabul qilinishida, ba’zi muammolar mavjud. Birinchidan, IP-manzilni tekshirish orqali jinoyatchini aniqlashda, bunday manzillarni noto‘g‘ri talqin qilish ehtimoli bor, chunki IP-manzilning o‘rganilishi, ayniqsa anonim tarmoq yoki VPN orqali amalga oshirilgan bo‘lsa, manzilni to‘g‘ri tahlil qilishning murakkabligi oshadi. Shuningdek, IP-manzilni yuridik jihatdan ishonchli dalil

sifatida taqdim etish uchun uni sudda tasdiqlash va bu manzilning o‘sha jinoyatga aloqadorligini isbotlash zarur.

Server yozuvlari va IP-manzillarni xalqaro miqyosda qabul qilish. Xalqaro huquq nuqtai nazaridan, server yozuvlari va IP-manzillarni dalil sifatida qabul qilish va ularni xalqaro sudlarda taqdim etish jarayoni ko‘plab murakkabliklarni o‘z ichiga oladi. Birinchidan, har bir mamlakatning axborot xavfsizligi va shaxsiy ma’lumotlarni himoya qilishga oid o‘ziga xos qonunlari mavjud. Bu qonunlar turlicha bo‘lishi mumkin va bir davlatdagi elektron dalillarni boshqa davlatda qabul qilishni murakkablashtirishi mumkin. Xalqaro hamkorlikni kuchaytirish va axborot almashishning ishonchliligini ta’minlash uchun, ko‘plab xalqaro tashkilotlar, jumladan, **Budapesht konvensiyasi** kabi hujjatlar, server yozuvlari va IP-manzillarni to‘plash, saqlash va taqdim etish uchun umumiy standartlarni belgilashga harakat qilmoqda.

Xulosa qilib aytganda, Server yozuvlari va IP-manzillar, kiberjinoyatlar bo‘yicha sudlov jarayonida asosiy dalillar sifatida yuridik ahamiyatga ega. Biroq, bu dalillarni to‘plash va ularga huquqiy baho berish jarayonida bir qator huquqiy va texnik muammolar mavjud. Server yozuvlari va IP-manzillarni jinoyatni aniqlashda samarali foydalanish uchun ularning qonuniyligi, ishonchliligi va haqiqiyligini tasdiqlash zarur. Shu bilan birga, bu turdagi elektron dalillarni xalqaro miqyosda qabul qilish va hamkorlikni rivojlantirish uchun yagona standartlarni joriy etish muhim ahamiyatga ega.

Kriptografiya va raqamli imzo asosida tasdiqlash. Elektron dalillarning huquqiy maqomi va ularning sudda ishonchli dalil sifatida e’tirof etilishi masalasi, asosan, elektron tizimlar va raqamli axborotlar orqali amalga oshirilgan jinoyatlarning maxfiyligini va xavfsizligini ta’minlash bilan bog‘liq. Kriptografiya va raqamli imzolar bu sohada elektron ma’lumotlarning qonuniyligini tasdiqlashda muhim vositalar sifatida xizmat qiladi. Ushbu bandda, kriptografiya va raqamli imzolar asosida elektron dalillarning tasdiqlanishi, ularning ishonchliligi va sud jarayonida qo‘llanishi masalalari keng va ilmiy asosda tahlil qilinadi.

Kriptografiya va uning huquqiy ahamiyati. Kriptografiya — ma’lumotlarni himoya qilish, saqlash va uzatishda ularning maxfiyligini ta’minlash uchun ishlatiladigan ilmiy texnologiya. Kriptografiya elektron tizimlar va internet orqali uzatiladigan ma’lumotlarning haqiqiyligini, yaxlitligini va maxfiyligini saqlashda muhim ahamiyatga ega. Elektron jinoyatlar, jumladan, xakerlik, phishing, onlayn firibgarlik va boshqa ko‘plab

jinoyatlar, koʻpincha maxfiy yoki shaxsiy maʼlumotlarni oʻgʻirlash va ulardan noqonuniy foydalanishni oʻz ichiga oladi. Bunday jinoyatlar bilan kurashish uchun, maʼlumotlarni himoya qilishning ishonchli va yuqori darajadagi texnologiyalari zarur. Kriptografiya, ayniqsa, maʼlumotlarni maxfiy saqlash, shuningdek, uzatilgan maʼlumotlarning oʻzgarishsizligini taʼminlashda samarali vosita boʻlib xizmat qiladi.

Kriptografik usullar yordamida shaxsiy yoki maxfiy axborotlarni himoya qilish, uni uzatish yoki saqlash jarayonida maʼlumotlarning yaxlitligini va ishonchliligini taʼminlash mumkin. Raqamli imzolar va shifrlash tizimlari orqali maʼlumotning asl egalari va oʻzgarishsizligini ishonchli tarzda tasdiqlash mumkin, bu esa elektron dalillarni sudda taqdim etishda muhim rol oʻynaydi. Kriptografiya, shu bilan birga, maʼlumotlarni muhofaza qilishda va kiberjinoyatlarni aniqlashda foydalaniladigan eng samarali texnologiyalardan biridir.

Raqamli imzo va uning huquqiy maqomi. Raqamli imzo, kriptografiyaning bir turi boʻlib, elektron hujjatning haqqoniyligini, yaxlitligini va asl muallifini tasdiqlashda ishlatiladi. Raqamli imzo, fizik imzo bilan taqqoslanishi mumkin, ammo u elektron shaklda ishlatiladi va elektron tizimlarda hujjatlarning haqiqiyligini tasdiqlashda muhim rol oʻynaydi. Raqamli imzoning asosiy xususiyati, uning asl muallifiga xos boʻlishi va shu bilan birga, uning oʻzgartirilmasligini taʼminlaydigan kriptografik algoritmlar asosida ishlashidir.

Raqamli imzo yordamida, elektron hujjatlar va boshqa raqamli axborotlarning haqiqiyligi va maʼlumotlarning oʻzgartirilmaganligi tasdiqlanadi. Misol uchun, biron-bir hujjatni elektron tarzda imzolagan shaxsning identifikatsiyasi va ularning imzosining haqiqiyligi, sudda taqdim etilgan elektron dalilning ishonchliligi uchun zarur boʻladi. Sud tizimlarida raqamli imzolar yordamida maʼlumotlarning oʻzgartirilmaganligini isbotlash, ayniqsa, huquqiy jarayonlarda muhim ahamiyatga ega, chunki bu elektron dalilni qonuniy va ishonchli sifatida taqdim etish imkonini beradi.

Raqamli imzo faqatgina shaxsning haqiqatdan ham oʻzini imzolaganligini tasdiqlash bilan cheklanmaydi. Shuningdek, bu imzo orqali hujjatning oʻzgarishsizligiga ishonch hosil qilish mumkin. Agar hujjatdagi maʼlumotlar oʻzgartirilsa, raqamli imzo bu oʻzgarishlarni avtomatik ravishda aniqlaydi va hujjatning haqiqiy emasligini koʻrsatadi. Shu bilan birga, raqamli imzolarni ishlatish va tasdiqlashda huquqiy muammolar ham mavjud, chunki har bir

mamlakatda raqamli imzolarni tan olish va ularni sudda dalil sifatida qabul qilish tartibi turlicha bo‘lishi mumkin.

Raqamli imzolarni xalqaro tan olish. Xalqaro miqyosda raqamli imzolarni tan olish, ularning huquqiy maqomini belgilash va sudlovda qo‘llash muhim ahamiyatga ega. Bu jarayon, xalqaro hamkorlik va turli davlatlar o‘rtasidagi yuridik aloqalarni mustahkamlashga yordam beradi. Masalan, **Xalqaro savdo palatasi** (ICC) tomonidan taqdim etilgan elektron imzolarni tan olish bo‘yicha ko‘plab xalqaro bitimlar mavjud. Shuningdek, **Birlashgan Millatlar Tashkiloti** (BMT) va **Yevropa Ittifoqi** (EU) kabi tashkilotlar raqamli imzolarni qo‘llashning umumiy standartlarini belgilash va global miqyosda bu tizimni joriy etish uchun huquqiy me’yorlarni ishlab chiqmoqda.

Shu bilan birga, raqamli imzolarni tan olish masalasi davlatlarning ichki qonunlariga ham bog‘liq. Ba’zi mamlakatlarda, ayniqsa, rivojlanayotgan davlatlarda, raqamli imzolarni sudlarda tan olish va ularga qonuniy baho berish jarayonida murakkabliklar yuzaga kelishi mumkin. Elektron tizimlar va raqamli imzolarni tan olish, shuningdek, ma’lumotlarning maxfiyligini himoya qilishga oid davlatlarning yuridik tamoyillari ham turlicha bo‘lishi mumkin. Shu sababli, xalqaro huquq doirasida raqamli imzolarni taqdim etish va ularni qonuniy ahamiyatga ega deb topish uchun yagona global standartlarni joriy etish zarur.

Kriptografiya va raqamli imzolarni qo‘llashdagi huquqiy muammolar. Kriptografiya va raqamli imzolarni elektron dalillarni tasdiqlashda qo‘llashda ba’zi huquqiy muammolar yuzaga keladi. Bularning eng muhimi — ma’lumotlarning maxfiyligini saqlash va shaxsiy huquqlarni himoya qilishdir. Raqamli imzolarni ishlatish uchun shaxslarning roziligi talab qilinishi mumkin, bu esa shaxsiy ma’lumotlarni qayta ishlash va uzatish bo‘yicha qo‘shimcha huquqiy qiyinchiliklarni keltirib chiqaradi. Kriptografik tizimlarni ishlab chiqishda va ma’lumotlarni shifrlashda foydalaniladigan usullar va texnologiyalar davlatlarning axborot xavfsizligi qonunlariga to‘g‘ri kelishi kerak, shuningdek, ular xalqaro bitimlar bilan hamohang bo‘lishi lozim.

Xulosa qilib aytganda, Kriptografiya va raqamli imzolar elektron dalillarning haqiqiyligini, yaxlitligini va qonuniyligini tasdiqlashda muhim vosita sifatida ishlatiladi. Bular elektron jinoyatlar bo‘yicha sudlov jarayonida ma’lumotlarning ishonchliligini ta’minlash, ularning haqiqiyligini isbotlash va jinoyatni aniqlashda zarur bo‘lgan texnologik asoslardir. Shuningdek, raqamli imzolar va kriptografiyaning xalqaro miqyosda qabul qilinishi va yagona

standartlar asosida qo‘llanilishi global hamkorlikni rivojlantirish va elektron jinoyatlarni jazolashda samarali mexanizmlarni ta’minlashga yordam beradi.

Sud organlarining texnik bilimga ega bo‘lishi zarurati. Kiberjinoyatlar va elektron dalillarning huquqiy maqomini to‘g‘ri baholash, ularni sud jarayonlarida ishonchli va qonuniy tarzda taqdim etish uchun sud organlarining texnik bilimga ega bo‘lishi zarur. Bu talab, ayniqsa, raqamli axborotlar va elektron tizimlarning kundalik hayotimizda va huquqiy tizimlarda tobora muhim ahamiyatga ega bo‘lishi bilan bog‘liq. Elektron dalillar, jumladan, server yozuvlari, IP-manzillar, elektron pochta xabarlari, raqamli fotosuratlar va videolar, kiberjinoyatlar holatida jinoyatni aniqlash va isbotlashda juda muhim o‘rin tutadi. Shu sababli, sudyalar va huquqshunoslar, faqatgina yuridik bilimga emas, balki texnik bilimlarga ham ega bo‘lishlari lozim.

Elektron dalillarning xususiyatlari va ularning huquqiy baholanishi. Elektron dalillar, o‘z tabiati va strukturasiga ko‘ra, an’anaviy dalillarga nisbatan bir qator farqlarga ega. Ular tezda o‘zgarishi mumkin, o‘chirilishi yoki tahrirlanishi oson, shuningdek, turli xil texnik vositalar yordamida o‘zgartirilishi mumkin. Shu sababli, elektron dalilning ishonchliligi va haqiqiyligi, sud jarayonida katta rol o‘ynaydi. Bunday dalillarga nisbatan xatoliklarni oldini olish, ularning to‘g‘ri talqin qilinishi va qo‘llanilishi uchun sud organlarining texnik bilimga ega bo‘lishi zarur. Misol uchun, server yozuvlarini tekshirishda ular o‘zgartirilmaganligini yoki tahrirlanmaganligini aniqlashda, sudya yoki ekspertning texnik bilimga ega bo‘lishi muhim ahamiyatga ega.

Texnik bilimlarning zarurati. Kiberjinoyatlar ko‘pincha murakkab texnik jarayonlarni o‘z ichiga oladi, masalan, kompyuter tarmoqlariga hujum qilish, ma’lumotlarni o‘g‘irlash, xakerlik va boshqa turdagi raqamli jinoyatlar. Bunday jinoyatlarni tekshirish va sudlov jarayonida ishonchli dalillarni taqdim etish uchun, sud organlarining texnik jihatdan tayyor bo‘lishi kerak. Sudyalarning texnik bilimlari ularga quyidagi vazifalarni samarali bajarishga yordam beradi:

- **Dalilning to‘g‘riligi va haqiqiyligini baholash** – Sudya, elektron dalillarning o‘zgarishsizligini aniqlash va ularning huquqiy ahamiyatini belgilashda texnik bilimga ega bo‘lishi kerak. Misol uchun, kompyuter tarmog‘idan olingan server yozuvlari yoki IP-manzil haqida sudya to‘g‘ri baho bera olishi kerak.

- **Elektron tizimlarning xususiyatlarini tushunish** – Sudya, kiberjinoyatlarni o‘rganishda ishlatiladigan texnologiyalarni tushunishi zarur. Bu, masalan, internet protokollari, shifrlash tizimlari, serverlar va tarmoqlarni o‘z ichiga oladi. Sud organi texnik bilimga ega bo‘lmasa, elektron dalilni tahlil qilish va to‘g‘ri baholashda qiyinchiliklarga duch kelishi mumkin.
- **Ekspertiza va malakali mutaxassislarni jalb qilish** – Sudya texnik ekspertlarni jalb qilish va ularning xulosalarini to‘g‘ri talqin qilishda malakaga ega bo‘lishi kerak. Ekspertiza jarayonida elektron dalillarni tahlil qilish uchun texnik bilimlar talab qilinadi, shu sababli sud organi ekspertlar bilan samarali hamkorlikni yo‘lga qo‘yishi zarur.

Texnik bilimga ega bo‘lmagan sud organlarining xatolari. Texnik bilimlarga ega bo‘lmagan sud organlari, ko‘plab holatlarda, elektron dalillarni to‘g‘ri talqin qilmasligi yoki ularni noto‘g‘ri baholashi mumkin. Masalan, server yozuvlari yoki IP-manzillarni noto‘g‘ri tahlil qilish, xakerlik hujumining asl sabablarini aniqlashda xatolikka olib kelishi mumkin. Bunday holatlar, sudning noto‘g‘ri qarorlar chiqarishiga, kiberjinoyatlarni o‘z vaqtida aniqlashda qiyinchiliklarga olib keladi. Bundan tashqari, texnik bilimga ega bo‘lmagan sud organi, ekspertiza natijalarini noto‘g‘ri talqin qilishi yoki axborot texnologiyalari va kiberjinoyatlar bilan bog‘liq barcha jihatlarni tushunmasligi mumkin.

Xalqaro tajriba va huquqiy ko‘rsatmalar. Xalqaro miqyosda, kiberjinoyatlar va elektron dalillarni to‘g‘ri baholashda texnik bilimlarning zarurligi tan olingan. Bir nechta xalqaro huquqiy normativ hujjatlar va tavsiyalar, jumladan, **Budapesht Konvensiyasi** va **BMTning elektron jinoyatlar bo‘yicha qo‘llanmalari**, sud organlarining texnik bilimga ega bo‘lishi zaruratini ta’kidlaydi. Bunda, kiberjinoyatlarni aniqlashda va ularni qonuniy ravishda jinoyat sifatida e’tirof etishda sudyalar, prokurorlar va advokatlar uchun texnik malakani oshirishga alohida e’tibor qaratiladi.

Bundan tashqari, **Yevropa Ittifoqi** va boshqa bir qator davlatlar, elektron dalillarni sudda qabul qilish va ularni to‘g‘ri talqin qilish jarayonida yuridik va texnik bilimlarning integratsiyasini kuchaytirish uchun maxsus o‘quv kurslari va treninglar tashkil etmoqda. Bu jarayonlar sud organlarining elektron tizimlar bilan ishlashda samaradorligini oshiradi va kiberjinoyatlarga qarshi kurashishda muhim qadam hisoblanadi.

Xulosa qilib aytganda, Sud organlarining texnik bilimga ega bo‘lishi, kiberjinoyatlarni o‘rganish va elektron dalillarni sudda to‘g‘ri baholashda

zaruriy shartdir. Elektron tizimlar va ma’lumotlar tez o‘zgarishi, ularning tahrirlanishi va o‘zgartirilishi mumkinligi, sud organlarining texnik ko‘nikmalarni rivojlantirishni talab qiladi. Shuningdek, xalqaro tajriba va huquqiy normativlar, sudyalar va boshqa huquqshunoslarni texnik bilimlarga ega bo‘lishga undaydi. Bu, o‘z navbatida, kiberjinoyatlar bilan kurashishda samaradorlikni oshiradi va elektron dalillarni qonuniy ravishda e’tirof etishga yordam beradi.

BOB BO‘YICHA UMUMIY XULOSALAR

Kiberjinoyatlar zamonaviy dunyoning eng katta xavf-xatarlari qatoriga kirib, xalqaro huquq va ichki milliy qonunchilik tizimlarida yangi va murakkab huquqiy muammolarni yuzaga keltirmoqda. Ushbu bobda kiberjinoyatlarning jinoyat deb e’tirof etilishi jarayonidagi asosiy huquqiy muammolar tahlil qilindi va muayyan yuridik yondashuvlar bilan baholandi. Kiberjinoyatlarning xalqaro jinoyat huquqida qanday mavqega ega ekanligi, davlatlarning bu jinoyatlarga nisbatan turlicha yondashuvlari, ekstraditsiya va yurisdiksiya masalalari hamda elektron dalillarning huquqiy maqomi kiberjinoyatlar bilan kurashishda yuzaga kelayotgan eng dolzarb masalalardir.

- **Xalqaro jinoyat huquqida “kiberjinoyat” tushunchasining mavqei.** Xalqaro jinoyat huquqida kiberjinoyatlarning mavqei haqida gapirganda, bu jinoyatlar ko‘pincha milliy va xalqaro qonunchilikda yagona ta’rifga ega emas. Kiberjinoyatlar bir qator an’anaviy jinoyatlardan farq qiladi, chunki ular global miqyosda tarqalgan va tez o‘zgarib turadi. Xalqaro jinoyat huquqida kiberjinoyatlar uchun aniq bir qat’iy ta’rif berilmasligi, ularning qamrovini cheklab qo‘yadi va bu holat, jinoyatchilarni jazo berish jarayonida qiyinchiliklarni keltirib chiqaradi. Xalqaro hamkorlikning kuchayishi, yangi shartnomalar va konventsiyalar ishlab chiqilishi, kiberjinoyatlarning huquqiy asoslarini mustahkamlashga yordam beradi.
- **Davlatlarning kiberjinoyatlarga nisbatan turlicha yondashuvi.** Davlatlar o‘rtasida kiberjinoyatlarga qarshi kurashishda turlicha yondashuvlarning mavjudligi, bu sohadagi huquqiy tizimlarning bir-biriga qarama-qarshi bo‘lishi yoki to‘liq integratsiyalashmaganligi kiberjinoyatlarga qarshi kurashishda muammolarni keltirib chiqaradi. Ayrim davlatlar axborot suverenitetiga asoslangan yondashuvni qo‘llashni afzal ko‘rishadi, bu esa ularning internetdagi va raqamli muhitdagi faoliyatlarini nazorat qilishni kuchaytiradi. Yevropa davlatlari, jumladan, GDPR va boshqa himoya

mexanizmlarini joriy etishda kuchli tartibga solish va axborot himoyasini ta’minlashga alohida e’tibor qaratmoqda. Shuningdek, Rossiya va Xitoy kabi ba’zi davlatlar axborot xavfsizligi va suverenitetiga ta’sir qiluvchi kiberjinoyatlarni o‘zlarining ichki siyosiy va iqtisodiy manfaatlariga ko‘ra baholashadi. Bunday turlicha yondashuvlar kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlikni murakkablashtiradi.

- **Ekstraditsiya va yurisdiksiya masalalari.** Kiberjinoyatlarning murakkabligi, ayniqsa, ularning global tabiati, xalqaro ekstraditsiya va yurisdiksiya masalalarini yanada muhimroq qilib qo‘ydi. Kiberjinoyatlar ko‘pincha hududiy chegaralarni bilmaydi, shu sababli jinoyatchilar bir mamlakatdan boshqa mamlakatga osonlik bilan qochishlari mumkin. Bu esa, jinoyatchilarni ushlash va sudga tortish uchun mamlakatlar o‘rtasida hamkorlikning zarurligini anglatadi. Xalqaro ekstraditsiya shartnomalarining mavjudligi kiberjinoyatchilikka qarshi kurashishda muhim omil hisoblanadi. Lekin, davlatlar o‘rtasida yurisdiksiya masalalari va ekstraditsiya bo‘yicha farqlar, ba’zi hollarda jinoyatlarni jazolashda kechikishlarga olib keladi. Shu bilan birga, ekstraditsiya shartnomalari va xalqaro hamkorlikning o‘zaro kelishilgan shakllari kiberjinoyatlar bilan samarali kurashishga yordam beradi.
- **Elektron dalillarning huquqiy maqomi.** Elektron dalillar, kiberjinoyatlar bo‘yicha huquqiy jarayonlarda eng muhim rol o‘ynaydi. Biroq, elektron dalillarning ishonchliligi va qabul qilinishi, ko‘plab huquqiy tizimlarda noaniqliklar va turlicha qarashlarni keltirib chiqaradi. Elektron dalillarning tahrirlanishi, o‘chirilishi yoki ularni manipulyatsiya qilish imkoniyati, sud jarayonida bunday dalillarning qonuniyligini tasdiqlashni qiyinlashtiradi. Shuningdek, raqamli imzolar va kriptografik texnologiyalar yordamida elektron dalillarni tasdiqlash huquqiy jixatdan ko‘p mamlakatlarda normativ asoslar bilan ta’minlanmoqda. Biroq, elektron dalillarning huquqiy maqomini belgilashda davlatlar o‘rtasidagi farqlar va xalqaro me’yorlarning yetishmasligi, elektron dalillarni samarali ishlatishda qiyinchiliklarga olib keladi.

Xulosa qilib aytganda, ushbu bobda kiberjinoyatlar va ularni jinoyat sifatida e’tirof etishdagi huquqiy muammolar tizimli tahlil qilindi. Xalqaro jinoyat huquqida kiberjinoyatlar uchun bir xil va universal ta’rifning mavjud emasligi, davlatlarning turlicha yondashuvlari, ekstraditsiya va yurisdiksiya masalalarining murakkabligi hamda elektron dalillarning ishonchliligi va qonuniy maqomi kiberjinoyatlarni jazolashda samarali mexanizmlarni

yaratishda yirik to‘siqlarni tashkil etadi. Biroq, xalqaro hamkorlikni rivojlantirish, yagona standartlarni joriy etish va texnologik yondashuvlarni mustahkamlash orqali, kiberjinoyatlar bilan kurashishning samaradorligini oshirish mumkin. Yaxshi ishlab chiqilgan xalqaro huquqiy asoslar, davlatlar o‘rtasida kiberjinoyatlarga qarshi kurashishda yanada samarali hamkorlikni ta’minlashi zarur.

III BOB. KIBERJINOYATLARGA QARSHI XALQARO HAMKORLIK TAJRIBASI

Zamonaviy kiberjinoyatlarning globallashuvi va ularga qarshi kurashishdagi qiyinchiliklar, xalqaro hamkorlikni zaruriyatga aylantirmoqda. Kiberjinoyatlar, ko‘p hollarda bir nechta mamlakatlarning hududiga tarqalgan holda amalga oshiriladi, bu esa ular bilan kurashishda yagona milliy yondashuvning yetarli emasligini ko‘rsatadi. Shu sababli, davlatlar o‘rtasida samarali va integratsiyalashgan hamkorlikni rivojlantirish kiberjinoyatlarning oldini olish va jazolashning eng muhim omili bo‘lib qolmoqda.

Bu bobda, kiberjinoyatlarni samarali ravishda aniqlash, tergov qilish va jazolashda xalqaro hamkorlikning o‘rni tahlil qilinadi. Xalqaro hamkorlikni mustahkamlashda xalqaro huquqiy me’yorlar, shartnomalar, ta’sirchan tashkilotlar va milliy qonunchiliklar o‘rtasidagi uyg‘unlikka e’tibor qaratiladi. Kiberjinoyatlarga qarshi global miqyosda kurashish jarayonida, zamonaviy texnologiyalar, tarmoq xavfsizligi va axborot huquqi doirasida ko‘plab muvaffaqiyatli tajribalar mavjud bo‘lib, ularni o‘rganish va amaliyotga joriy etish kiberjinoyatlar bilan kurashishda samarali vositalarni yaratishda muhim ahamiyatga ega.

Bundan tashqari, xalqaro hamkorlikni rivojlantirishda eng asosiy yuridik mexanizmlar va platformalarning samaradorligini tahlil qilish muhimdir. Xalqaro shartnomalar, ta’sirchan tashkilotlar (masalan, Yevropa Ittifoqi, BMT, INTERPOL, Europol) va mamlakatlar o‘rtasida huquqiy yordam, ekstraditsiya va tergov amaliyotlaridagi hamkorlikning asosiy usullari kiberjinoyatlarni jazolash jarayonida qanday rol o‘ynashini tushunish zarur.

Shu bilan birga, xalqaro hamkorlikda mavjud bo‘lgan muammolar va cheklovlar ham ko‘rib chiqiladi. Bularning ichida mamlakatlar o‘rtasidagi siyosiy qarama-qarshiliklar, huquqiy farqlar, texnologik tarmoqdagi xavfsizlik muammolari va resurslarning yetishmasligi kabi omillar mavjud. Ushbu muammolarni bartaraf etish uchun yanada samarali huquqiy va texnologik

chora-tadbirlar, hamkorlikni mustahkamlash uchun xalqaro tashkilotlar va davlatlar o‘rtasida doimiy muloqot va kelishuvlar zarur.

III bobda kiberjinoyatlarga qarshi xalqaro hamkorlikning amaliy tajribasi va undagi mavjud huquqiy mexanizmlar haqida batafsil ma’lumot beriladi. Bu, kiberjinoyatlar bilan kurashishda samarali xalqaro tizimni shakllantirish uchun muhim yuridik asoslarni va yondashuvlarni o‘rganish imkonini beradi. Xalqaro hamkorlikning ilg‘or tajribalarini o‘rganish, bu sohada o‘zgaruvchan ehtiyojlarni inobatga olgan holda yangi, innovatsion va samarali yondashuvlarni ishlab chiqish imkonini beradi.

3.1. Budapest konvensiyasi: mazmuni va huquqiy asoslari

Kiberjinoyatlar bilan kurashishda xalqaro hamkorlikning muhim huquqiy asoslaridan biri sifatida Budapest konvensiyasi, yoki to‘liq nomi bilan "Kiberjinoyatlar bo‘yicha Yevropa Kengashi Konvensiyasi" (Convention on Cybercrime of the Council of Europe), o‘zining tarixiy ahamiyatiga ega. Ushbu konvensiya 2001-yilda Yevropa Kengashining tashabbusi bilan ishlab chiqilgan va kiberjinoyatlarga qarshi samarali kurashishda davlatlar o‘rtasida hamkorlikni mustahkamlashga qaratilgan birinchi xalqaro yuridik hujjat bo‘lib, uni amalga oshirish uchun yuridik, texnologik va axborot xavfsizligi sohalarida mustahkam asoslar yaratdi.

Budapest konvensiyasining mazmuni va huquqiy asoslari, kiberjinoyatlarni oldini olish, ularga qarshi kurashishda zamonaviy yuridik mexanizmlar yaratish, shuningdek, davlatlar o‘rtasida ma’lumot almashinuvi va huquqiy hamkorlikni ta’minlashda muhim ahamiyatga ega. Bu konvensiya, ayniqsa, huquqiy yordam va axborot almashinuvi masalalarida davlatlar o‘rtasida yangi normativ asoslarni joriy etish, ekstraditsiya, elektron dalillarning qabul qilinishi va ularga oid xalqaro tartiblarni belgilashda hal qiluvchi rol o‘ynaydi.

Budapest konvensiyasi o‘zining qamrovli va tizimli yondashuvi bilan kiberjinoyatlar sohasida xalqaro hamkorlikni rivojlantirishga katta hissa qo‘shdi. Ushbu hujjat, kiberjinoyatlarni jinoyat deb e’tirof etish, ularni aniqlash va tergov qilishda tegishli standartlarni ishlab chiqadi va yuridik tizimlarning ushbu jinoyatlarga qarshi birgalikda kurashish imkoniyatlarini oshiradi. Bundan tashqari, konvensiya kiberjinoyatlar bo‘yicha yuridik tizimlarning o‘zaro mosligini ta’minlaydi va uning talablari, davlatlar

tomonidan qabul qilinishi orqali, xalqaro huquqning samarali ishlashiga asos yaratadi.

Shuningdek, Budapest konvensiyasi huquqiy jihatdan hal qilinishi kerak bo‘lgan ko‘plab muammolarni keltirib chiqarmoqda. Xususan, bu hujjat global miqyosda keng tarqalgan va o‘zgaruvchan texnologiyalarni hisobga olib, yangi jinoyat turlari va ularga qarshi kurashish usullarini doimiy ravishda yangilab borishni taqozo etadi. Ushbu konvensiya mamlakatlar o‘rtasida yuqori darajada hamkorlik va axborot almashishning zarurligini tushunish va ularga xos yuridik me’yorlarni joriy etish uchun muhim yuridik vositadir.

Shu bois, Budapest konvensiyasining mazmuni va huquqiy asoslari haqida chuqur tahlil olib borish, uning kiberjinoyatlarni jinoyat deb e’tirof etishdagi o‘rni va xalqaro huquqiy tizimda qanday muhim rol o‘ynashini tushunish uchun zarurdir.

Konvensiyaning asosiy moddalari va maqsadi. Budapest konvensiyasi (2001-yil 23-noyabrda qabul qilingan) yoki to‘liq nomi bilan "Kiberjinoyatlar bo‘yicha Yevropa Kengashi Konvensiyasi" kiberjinoyatlarga qarshi xalqaro hamkorlikni kuchaytirish maqsadida tuzilgan birinchi yuridik hujjatdir. Bu hujjat xalqaro huquqning kiberjinoyatlar bo‘yicha maxsus shartnomasi sifatida, dunyo miqyosida yagona normativ huquqiy asos yaratib, mamlakatlar o‘rtasidagi yuridik hamkorlikni va kiberjinoyatlarga qarshi kurashishda samarali usullarni ishlab chiqishni ta’minladi.

Konvensiyaning asosiy maqsadi — kiberjinoyatlarni oldini olish, ularga qarshi kurashishda davlatlar o‘rtasida hamkorlikni rivojlantirish va zaruriy huquqiy mexanizmlarni ta’minlashdir. Ushbu maqsadga erishish uchun, konvensiya bir qancha asosiy moddalardan tashkil topgan bo‘lib, har bir modda o‘ziga xos yuridik talablar, me’yorlar va tartiblarni belgilaydi. Ushbu bo‘limda, konvensiyaning asosiy moddalari va uning maqsadlarini ilmiy asosda tahlil qilamiz.

✓ **Kiberjinoyatlar va ularni aniqlashga oid moddalari**. Konvensiyaning dastlabki moddalari kiberjinoyatlar turini aniq belgilaydi va ularga qarshi kurashish uchun zarur bo‘lgan yuridik asoslarga e’tibor qaratadi. Kiberjinoyatlar, ularning turlari, aniqlanishi, tergov qilinishi, hibsga olinishi va jazolanishi konvensiyaning birinchi bo‘limlarida muhim o‘rin egallaydi. Konvensiya "kiberjinoyat"ni keng ma’noda, ya’ni kompyuter tizimlariga, dasturiy ta’minot va axborot tarmoqlariga zarar yetkazish, noqonuniy kirish, firibgarlik va boshqa o‘zgartirishlarni kiritishni o‘z ichiga olgan holda

tasvirlaydi. Ushbu moddalarda, davlatlar tomonidan kiberjinoyatlar to‘g‘risida qonunchilikni ishlab chiqish va uni amalga oshirish, shuningdek, kiberjinoyatlarni aniqlash uchun zarur huquqiy mexanizmlar yaratish alohida ko‘rsatilgan.

✓ **Axborot almashinuvi va huquqiy yordam**. Konvensiyaning ikkinchi bo‘limi axborot almashinuvi va huquqiy yordamga qaratilgan. Ushbu modda davlatlar o‘rtasida axborot almashinuvi tizimlarini rivojlantirish, axborotlarni to‘plash, uzatish va maxfiylikni ta’minlashga qaratilgan qoidalarni belgilaydi. Konvensiya kiberjinoyatlarni tergov qilishda o‘zaro yordamni rivojlantirishga, axborot xavfsizligini ta’minlash va bu jarayonda shaxsiy huquqlarga hurmat bilan yondashishga urg‘u beradi. Yuridik yordam ko‘rsatilishi kerak bo‘lgan sohalar, masalan, kiberjinoyatlar bo‘yicha tergovlar, xususiy ma’lumotlarning almashinuvi va axborot tizimlarining tekshirilishi ko‘rsatilgan.

✓ **Ekstraditsiya va yuridik yordamning mexanizmi**. Konvensiyaning muhim jihatlaridan biri ekstraditsiya masalasini hal qilishdir. Ushbu bo‘limda, kiberjinoyatlarni amalga oshirgan shaxslarni bir davlatdan boshqasiga ekstraditsiya qilishda yuzaga keladigan huquqiy tartiblar belgilab qo‘yilgan. Konvensiyada ekstraditsiyaning asosiy talablari va shartlari, shuningdek, ayrim holatlarda ekstraditsiya qilinmaslik sabablarini ko‘rsatish orqali davlatlar o‘rtasida adolatli, to‘liq va o‘zaro manfaatli mexanizmlar yaratishga harakat qilingan.

✓ **Elektron dalillarning huquqiy maqomi**. Konvensiyaning boshqa bir muhim bo‘limi elektron dalillarning qabul qilinishi va ularning yuridik jihatdan tan olinishi masalasiga bag‘ishlangan. Kiberjinoyatlarni tergov qilishda elektron dalillar (kompyuter ma’lumotlari, tarmoq faoliyati, elektron pochta xabarlaridan to‘plangan ma’lumotlar va h.k.) asosiy dalil sifatida qaraladi. Konvensiya davlatlarga elektron dalillarning yuridik maqomini tasdiqlash va ularni boshqa davlatlar bilan almashish imkoniyatini yaratish bo‘yicha me’yorlarni o‘rnatadi. Shuningdek, elektron dalillarning to‘planganidan keyin ularni tahlil qilish va hukumatning tegishli organlariga taqdim etish bo‘yicha tegishli protseduralarni ham belgilaydi.

✓ **Kiberjinoyatlar uchun jazolar**. Konvensiyaning yakuniy moddalari kiberjinoyatlar uchun belgilangan jazolarni ko‘rsatadi. Har bir kiberjinoyat turiga qarab, milliy qonunchilikda belgilangan jazolar (hibsga olish, jarima,

majburiy mehnat va boshqalar) hamda kiberjinoyatlarni jazolashda xalqaro hamkorlikni kuchaytirish uchun zarur mexanizmlar ta’minlanadi.

Konvensiyaning maqsadi. Budapest konvensiyasining asosiy maqsadi — kiberjinoyatlar bilan kurashishda xalqaro hamkorlikni rivojlantirish va yangi texnologiyalarni hisobga olgan holda global xavfsizlikni ta’minlashdir. Ushbu maqsadga erishish uchun konvensiya davlatlarga kiberjinoyatlarni oldini olish, ularni aniqlash, tergov qilish va jazolashda zarur huquqiy asoslar yaratishni nazarda tutadi. Konvensiyaning yana bir maqsadi — elektron axborot xavfsizligini ta’minlash va bu borada davlatlar o‘rtasida samarali hamkorlikni rivojlantirishdir.

Shu bilan birga, konvensiya kiberjinoyatlarga qarshi kurashishda jamiyatlar va davlatlar o‘rtasida o‘zaro ishonchni mustahkamlashni, jinoyatchilarni jazolashda xalqaro hamkorlikni kuchaytirishni va huquqiy mexanizmlar yaratishda ilg‘or tajribalardan foydalanishni ko‘zda tutadi.

A’zo davlatlar majburiyatlari. Budapest konvensiyasi, 2001-yilda Yevropa Kengashi tomonidan qabul qilingan bo‘lib, kiberjinoyatlarni aniqlash, tergov qilish va ularga qarshi kurashish bo‘yicha xalqaro hamkorlikni rivojlantirishda muhim huquqiy asos yaratdi. Ushbu konvensiya, kiberjinoyatlarga qarshi kurashishda davlatlar o‘rtasidagi o‘zaro hamkorlikni kuchaytirishni va global axborot xavfsizligini ta’minlashni maqsad qilgan. A’zo davlatlar, konvensiyaga imzo chekkanlaridan so‘ng, bir qator majburiyatlarni bajarishga rozilik bildiradilar. Bu majburiyatlar, o‘z ichiga kiberjinoyatlar bilan bog‘liq jinoyatlarni aniqlash, ularni tergov qilish, jinoyatchilarni jazolash, shuningdek, kiberjinoyatlarga qarshi samarali huquqiy mexanizmlarni ishlab chiqish va amalga oshirishni o‘z ichiga oladi.

A’zo davlatlarning majburiyatlari quyidagi asosiy yo‘nalishlarga bo‘linadi:

✓ **Kiberjinoyatlar haqida qonunchilikni ishlab chiqish**. Budapest konvensiyasining eng asosiy majburiyatlaridan biri — a’zo davlatlar kiberjinoyatlar to‘g‘risida aniq va tizimli qonunlarni ishlab chiqishidir. Har bir davlat, konvensiya imzolanganidan keyin, kiberjinoyatlarni jinoyat deb e’tirof etadigan va ularni jazolashga yo‘l qo‘yayotgan qonunlarni qabul qilishni o‘z zimmasiga oladi. Bunga kiberjinoyatlarning turli turlari, jumladan, kompyuter tizimlariga noqonuniy kirish, axborotlarni o‘g‘irlash, zararli dasturlarni tarqatish va boshqalar kiradi. A’zo davlatlar bu qonunlarni faqatgina o‘z

hududida emas, balki xalqaro miqyosda ham muvofiqlashtirishni ta’minlaydilar.

✓ **Ma’lumotlar va axborot almashish**. Konvensiyaning boshqa muhim majburiyati — a’zo davlatlar o‘rtasida ma’lumotlar almashinishni ta’minlashdir. Bu, kiberjinoyatlarni tergov qilishda va jinoyatchilarni aniqlashda samarali bo‘lishi uchun zarurdir. Konvensiya, shuningdek, kiberjinoyatlar bilan bog‘liq axborotni tezda almashish, tergov materiallarini uzatish va muvofiqlashtirishni ta’minlashni talab qiladi. A’zo davlatlar o‘zaro axborot almashinishda adolat, shaffoflik va maxfiylikni saqlashga majburdirlar.

✓ **Ekstraditsiya va yuridik yordam**. A’zo davlatlar kiberjinoyatlar uchun ekstraditsiya mexanizmlarini ishlab chiqish va amalga oshirish majburiyatiga egadirlar. Agar bir davlatda kiberjinoyat sodir bo‘lsa va jinoyatchi boshqa davlatda yashayotgan bo‘lsa, ekstraditsiya jarayonlari yordamida jinoyatchini adolatli hukmga tortish uchun tegishli mamlakatga yuborish kerak. Konvensiya, ekstraditsiyaning qanday amalga oshirilishi, qanday shartlar asosida amalga oshirilishi va boshqa yuridik yordamning turlari haqida o‘rgatadi. A’zo davlatlar, shu bilan birga, xalqaro huquq normalariga muvofiq, qachonki jinoyatchi boshqa davlatga ekstraditsiya qilinsa, uning inson huquqlari va erkinliklariga rioya qilinishi lozim.

✓ **Tergov va huquqiy yordam ko‘rsatish**. A’zo davlatlar, kiberjinoyatlarni tergov qilishda boshqa davlatlar bilan huquqiy yordam ko‘rsatish majburiyatiga egadirlar. Bu, o‘z navbatida, kiberjinoyatlarni tergov qilishda axborotlarni to‘plash, shaxsiy ma’lumotlarni himoya qilish, muhim dalillarni to‘plash va ularni boshqa davlatlarga taqdim etish imkoniyatlarini yaratadi. Tergov va huquqiy yordam ko‘rsatishning asosiy maqsadi jinoyatchilarning javobgarlikka tortilishi va jinoyatlarning aniqlanishini ta’minlashdir.

✓ **Elektron dalillarni tan olish va ulardan foydalanish**. A’zo davlatlar, elektron dalillarni tan olish va ularni tergovda va sud ishlarida yuridik jihatdan qabul qilish majburiyatiga egadirlar. Kiberjinoyatlarni tergov qilishda elektron tizimlar, kompyuterlar, internet va boshqa texnologiyalarga oid dalillar muhim rol o‘ynaydi. Konvensiya, shuningdek, elektron dalillarning xalqaro huquqiy qadriyatlarini belgilaydi va ularni rasmiylashtirish bo‘yicha ko‘rsatmalar beradi.

✓ **Xalqaro hamkorlikni rivojlantirish**. A’zo davlatlar o‘rtasida doimiy ravishda xalqaro hamkorlikni rivojlantirish zarurligini ta’kidlaydi. Kiberjinoyatlarga qarshi samarali kurashish uchun barcha a’zo davlatlar o‘rtasida o‘zaro ishonch va hamkorlikka asoslangan tarmoqni shakllantirish zarur. Konvensiya, shuningdek, har bir davlatning o‘zining milliy qonunlariga asoslangan holda boshqa davlatlar bilan samarali hamkorlik qilishni, axborotlarni almashish va muvofiqlashtirishni ta’minlaydi.

✓ **Kiberjinoyatlarga qarshi yangi texnologiyalarni rivojlantirish** A’zo davlatlar o‘z hududida yangi texnologiyalarni rivojlantirish, kiberjinoyatlar uchun ilg‘or usullarni ishlab chiqish va ularni xalqaro hamkorlikda qo‘llashni majburiyat qilib olishadi. Konvensiya, yangi texnologiyalar va internet xususiyatlariga qarshi samarali kurashish uchun, davlatlarni texnologik imkoniyatlarni doimiy ravishda yangilab borishga undaydi.

Xulosa qilib aytganda, Budapest konvensiyasi a’zo davlatlarga kiberjinoyatlarga qarshi kurashishda zarur bo‘lgan barcha huquqiy asoslarni yaratadi. Har bir davlat, o‘z milliy qonunchiligini konvensiyaning talablariga muvofiq ravishda ishlab chiqishi va amalga oshirishi lozim. A’zo davlatlar o‘rtasida o‘zaro hamkorlikni kuchaytirish, axborot almashish, tergov qilish, elektron dalillarni rasmiylashtirish va jinoyatchilarni jazolashda samarali mexanizmlar yaratish — konvensiyaning asosiy majburiyatlaridir. Bu majburiyatlar, xalqaro kiberjinoyatlarga qarshi kurashishda muvaffaqiyatli natijalarga erishish uchun muhim yuridik va amaliy asoslarni ta’minlaydi.

O‘zbekistonning unga qo‘shilish istiqbollari. Budapest konvensiyasi, yoki to‘liq nomi bilan **“Kiberjinoyatlar to‘g‘risidagi Yevropa Konvensiyasi”**, 2001-yilda Yevropa Kengashi tomonidan kiberjinoyatlar bilan kurashish va xalqaro hamkorlikni ta’minlash maqsadida qabul qilingan huquqiy hujjatdir. Ushbu konvensiya, ayniqsa, axborot texnologiyalari va internetning jadal rivojlanishi bilan yuzaga kelgan yangi jinoyat turlariga qarshi samarali kurashish, davlatlar o‘rtasida axborot almashish va huquqiy yordamni ta’minlashni nazarda tutadi. Ushbu konvensiya, kiberjinoyatlarni qayd etish, ularni tergov qilish va jinoyatchilarni jazolash bo‘yicha xalqaro standartlarni ishlab chiqadi va ularni amalga oshirishga intiladi.

O‘zbekistonning bu konvensiyaga qo‘shilishi, uning xalqaro huquqiy me’yorlari bilan muvofiqlashishi va kiberjinoyatlar bilan kurashish bo‘yicha xalqaro hamkorlikka qo‘shilishini anglatadi. O‘zbekistonning Budapest

konvensiyasiga qo‘shilishi istiqbollari, davlatning huquqiy tizimiga qanday ta’sir ko‘rsatishini va xalqaro miqyosda kiberjinoyatlarga qarshi kurashishda qanday rol o‘ynashini o‘rganish muhimdir.

O‘zbekistonning xalqaro hamkorlikdagi o‘rni. O‘zbekiston, kiberjinoyatlar va internet xavfsizligi sohasida faol siyosat olib borayotgan davlatlardan biri bo‘lib, o‘zining axborot xavfsizligini ta’minlash, kiberjinoyatlarga qarshi kurashish va xalqaro hamkorlikni rivojlantirish maqsadida bir qator huquqiy, amaliy va texnologik tadbirlarni amalga oshirgan. Misol uchun, O‘zbekiston 2019-yilda axborot xavfsizligini ta’minlash bo‘yicha milliy strategiyasini ishlab chiqdi va joriy etdi. Shuningdek, davlat axborot tizimlarining himoyasini kuchaytirish, fuqarolarning shaxsiy ma’lumotlarini himoya qilish va kiberhujumlar oldini olishga qaratilgan qonunchilikni yaxshilash bo‘yicha islohotlarni davom ettirmoqda.

Biroq, kiberjinoyatlar sohasidagi xalqaro hamkorlikni yanada mustahkamlash va zamonaviy kiberjinoyatlarga qarshi kurashishda yanada samarali bo‘lish uchun O‘zbekiston uchun Budapest konvensiyasiga qo‘shilish katta ahamiyatga ega. Ushbu konvensiyaga qo‘shilish, O‘zbekistonni xalqaro huquqiy tizimga integratsiya qilish va xalqaro miqyosda kiberjinoyatlar bilan kurashishda samarali hamkorlikni ta’minlash uchun zarur huquqiy asoslarni yaratadi.

O‘zbekistonning qo‘shilishidagi muhim jihatlar

- ✓ **Qonunchilikni yaxshilash va moslashtirish**. Budapest konvensiyasiga qo‘shilishi bilan O‘zbekiston o‘z qonunchiligini xalqaro talablar va standartlarga muvofiqlashtirish zaruratiga duch keladi. Bu, o‘z navbatida, kiberjinoyatlar to‘g‘risidagi milliy qonunlarni takomillashtirishni, yangi jinoyat turlarini qonunda belgilashni va o‘zaro hamkorlikda jinoyatchilarni jazolash mexanizmlarini yaratishni talab qiladi. O‘zbekiston, shuningdek, kiberjinoyatlar bilan bog‘liq barcha jinoyatlarni aniq belgilab, ularni jazolash uchun zarur bo‘lgan huquqiy mexanizmlarni yaratishi kerak.
- ✓ **Xalqaro axborot almashish va huquqiy yordam**. O‘zbekiston, Budapest konvensiyasiga qo‘shilish orqali, kiberjinoyatlar bilan bog‘liq ma’lumotlarni boshqa davlatlar bilan tezda almashish imkoniyatini qo‘lga kiritadi. Bu, o‘z navbatida, kiberjinoyatlarni aniqlash, tergov qilish va jinoyatchilarni jazolashda samarali yordam beradi. Shuningdek, O‘zbekiston

xalqaro yuridik yordam koʻrsatish va ekstraditsiya jarayonlarida ham qatnashishga tayyor boʻlishi zarur.

✓ **Elektron dalillarni qabul qilish va rasmiylashtirish**. Elektron dalillarni tan olish va rasmiylashtirish, kiberjinoyatlarni tergov qilishda muhim oʻrin tutadi. Budapest konvensiyasi elektron dalillarning huquqiy maqomini belgilaydi va ularni rasmiylashtirishning aniq standartlarini ishlab chiqadi. Oʻzbekiston, konvensiyaga qoʻshilgan holda, elektron dalillarni toʻplash, saqlash va ulardan foydalanish boʻyicha xalqaro me'yorlarga mos tizim yaratishi lozim. Bu, oʻz navbatida, kiberjinoyatlarni tergov qilishda va jinoyatchilarni jazolashda Oʻzbekistonning samarali qatnashishini ta'minlaydi.

✓ **Xalqaro hamkorlikni rivojlantirish**. Budapest konvensiyasi davlatlar oʻrtasida kiberjinoyatlarga qarshi kurashishda hamkorlikni kuchaytirish, resurslarni birlashtirish va tajriba almashish imkoniyatlarini yaratadi. Oʻzbekiston, konvensiyaga qoʻshilish orqali, boshqa davlatlar bilan yangi texnologiyalar va usullarni sinovdan oʻtkazish, kiberjinoyatlar bilan kurashish boʻyicha xalqaro tajriba almashish imkoniyatiga ega boʻladi. Bu, oʻz navbatida, mamlakatning kiberxavfsizlik sohasidagi salohiyatini oshiradi va global kiberjinoyatlarga qarshi kurashishda faolligini ta'minlaydi.

✓ **Inson huquqlarini himoya qilish**. Budapest konvensiyasining muhim jihatlaridan biri — u davlatlar oʻrtasida inson huquqlarini himoya qilishni ta'minlaydi. Oʻzbekiston, kiberjinoyatlar bilan kurashishda inson huquqlariga rioya qilishni oʻzining xalqaro majburiyatlari sifatida belgilab olish zarur. Shuningdek, konvensiya, hukumatlarning axborot va kommunikatsiyalarni erkin va xavfsiz tarzda boshqarish imkoniyatlarini ta'minlashga qaratilgan. Bu, Oʻzbekistonning global axborot xavfsizligi tizimidagi oʻrnini mustahkamlashga xizmat qiladi.

Xulosa qilib aytganda, Oʻzbekistonning Budapest konvensiyasiga qoʻshilishi, uning kiberjinoyatlarga qarshi kurashishdagi xalqaro hamkorlikka qoʻshilishining muhim bosqichi boʻlishi mumkin. Bu Oʻzbekistonning xalqaro miqyosda axborot xavfsizligi sohasida faoliyatini mustahkamlash, kiberjinoyatlarga qarshi samarali kurashish va global xavfsizlikka hissa qoʻshish imkoniyatini yaratadi. Oʻzbekiston, konvensiyaning talablariga muvofiq ravishda oʻz qonunlarini takomillashtirib, xalqaro axborot almashish va yuridik yordam koʻrsatishda ishtirok etishi kerak. Shu tarzda, Oʻzbekiston kiberjinoyatlar va axborot xavfsizligini ta'minlash boʻyicha dunyo hamjamiyatining bir qismi sifatida oʻz oʻrnini mustahkamlaydi.

3.2. Xalqaro tashkilotlarning roli

Xalqaro kiberjinoyatlar bilan kurashish va ularni jinoyat deb e’tirof etishdagi huquqiy muammolarni hal qilishda xalqaro tashkilotlar muhim rol o‘ynaydi. Kiberjinoyatlar, o‘z mohiyati bilan davlatlararo chegara va hududlarni buzib o‘tgan global muammolarga aylanmoqda. Bunday jinoyatlar internet va axborot texnologiyalarining tez sur’atlarda rivojlanishi bilan birga, nafaqat milliy xavfsizlikni, balki global barqarorlikni ham tahdid qilishda davom etmoqda. Shu sababli, xalqaro hamkorlikni ta’minlash, samarali huquqiy mexanizmlar yaratish va kiberjinoyatlarni jazolashda yirik xalqaro tashkilotlar o‘rtasidagi aloqalar va hamkorlik muhim ahamiyat kasb etadi.

Xalqaro tashkilotlar, o‘z faoliyatida kiberjinoyatlarga qarshi kurashish, ularga nisbatan qonunchilikni muvofiqlashtirish, davlatlar o‘rtasida hamkorlikni rivojlantirish va axborot xavfsizligini ta’minlashda muhim tashabbuskorlar hisoblanadi. Ushbu tashkilotlar nafaqat kiberjinoyatlar bilan bog‘liq huquqiy me’yorlar va standartlarni ishlab chiqishda, balki davlatlar o‘rtasida o‘zaro ishonchni mustahkamlash, axborot almashish va umumiy siyosatlarni shakllantirishda ham muhim rol o‘ynaydi.

Dunyo bo‘ylab faoliyat yuritayotgan yirik xalqaro tashkilotlar, masalan, BMT, Yevropa Kengashi, Interpol va boshqa mutaxassis tashkilotlar, kiberjinoyatlarga qarshi kurashishda yagona strategiyalarni ishlab chiqishda va ularni amalga oshirishda faol qatnashmoqda. Shuningdek, ushbu tashkilotlar, kiberjinoyatlarning yangi turlari va texnologiyalari yuzasidan dolzarb muammolarni hal qilishda yordam berish, davlatlar o‘rtasida muvofiqlashtirilgan huquqiy yondashuvni ta’minlashda eng asosiy o‘ringa ega.

Ushbu bobda, xalqaro tashkilotlarning kiberjinoyatlar bilan kurashishdagi roli va ularga qarshi kurashish uchun qanday tashkiliy va huquqiy mexanizmlar yaratishda faol ishtirok etayotganliklarini tahlil qilishga harakat qilamiz. Shuningdek, bu tashkilotlarning davlatlar o‘rtasida hamkorlikni rivojlantirish, resurslarni birlashtirish va global kiberxavfsizlikni ta’minlashdagi muhim rolini ko‘rsatishga intilamiz.

INTERPOL va Europol faoliyati. Kiberjinoyatlar global miqyosda keng tarqalgan va ularga qarshi kurashishning samarali usullari faqat davlatlararo hamkorlikda amalga oshirilishi mumkin. Xalqaro jinoyatlarni oldini olish va ularga qarshi kurashish sohasida faoliyat yuritayotgan ikki muhim tashkilot — INTERPOL (Xalqaro Jinoyat Politsiyasi Tashkiloti) va Europol (Yevropa

Ittifoqining Jinoyatlarni tekshirish va oldini olish agentligi) kiberjinoyatlarning oldini olish va jinoyatchilarni jazolashda muhim o‘rin egallaydi. Ushbu tashkilotlar, dunyo bo‘ylab kiberjinoyatlarga qarshi kurashish uchun qonuniy, texnik va tashkiliy nuqtai nazardan bir qator muhim ishlarni amalga oshirmoqda.

INTERPOL faoliyati. INTERPOL 1923-yilda tashkil etilgan bo‘lib, global miqyosda davlatlar o‘rtasida jinoyatlarni tekshirish, jinoyatchilarni qidirish, jinoiy aloqalarni o‘rganish va ularni xalqaro miqyosda jazolashga yordam berish uchun faoliyat yuritadi. INTERPOLning kiberjinoyatlar bilan kurashishdagi asosiy vazifalaridan biri — barcha a’zo davlatlar o‘rtasida kiberjinoyatlar haqida ma’lumot almashish va texnik yordam ko‘rsatishdir. Shuningdek, tashkilot kiberjinoyatchilikka qarshi kurashish uchun maxsus bo‘limlar va tarmoq hosil qiladi. INTERPOLning "Kiberjinoyatlar bo‘yicha maxsus guruh"i kiberxavfsizlik va kiberjinoyatlarni tergov qilishda, zaruriy texnik resurslarni taqdim etishda va o‘qituvchilarni tayyorlashda faol qatnashadi.

INTERPOL kiberjinoyatlar bilan bog‘liq muammolarni hal qilishda davlatlarga huquqiy yordami, ekspertiza, o‘quv kurslari, jinoyatlarning texnik tahlili va boshqa sohalarda yordam ko‘rsatib, milliy politsiya xizmatlarining kiberjinoyatlarni aniqlashdagi qobiliyatlarini oshirishga yordam beradi. INTERPOLning kiberjinoyatlarni aniqlash va ularga qarshi kurashishdagi faoliyati asosan quyidagi yo‘nalishlarga yo‘naltirilgan:

- **Global hamkorlik**: INTERPOL xalqaro hamkorlikni ta’minlash, davlatlar o‘rtasidagi axborot almashish va operativ ko‘mak ko‘rsatish orqali kiberjinoyatlarni aniqlash va tergov qilishda ishtirok etadi.
- **Tegishli o‘quv dasturlari va texnik yordam**: INTERPOL kiberxavfsizlik sohasida malakali mutaxassislarni tayyorlash, yangi texnologiyalarni tushunish va davlatlarga amaliy yordam ko‘rsatishda muhim rol o‘ynaydi.
- **Xalqaro operatsiyalar**: INTERPOL o‘zining a’zo davlatlari bilan birgalikda global miqyosda kiberjinoyatlar bilan bog‘liq jinoyatlarni aniqlash va ularni jazolash uchun katta operatsiyalarni amalga oshiradi.

Europol faoliyati. Europol, 1999-yilda Yevropa Ittifoqining jinoyatchilikka qarshi kurashish agentligi sifatida tashkil etilgan. Europolning asosiy vazifasi — Yevropa Ittifoqi a’zo davlatlari o‘rtasida jinoyatchilikka qarshi kurashish va ayniqsa, kiberjinoyatlarga qarshi kurashishda muhim

koʻmak koʻrsatishdir. Europol oʻzining "Kiberjinoyatlarni tekshirish boʻlimi" orqali kiberjinoyatlar bilan bogʻliq barcha turdagi jinoyatlarni aniqlash, oldini olish va jinoyatchilarni qidirish bilan shugʻullanadi.

Europolning faoliyati quyidagi asosiy yoʻnalishlarga qaratilgan:

- **A'zo davlatlar oʻrtasidagi hamkorlikni kuchaytirish**: Europol, Yevropa Ittifoqi davlatlari oʻrtasidagi axborot almashish va kiberjinoyatlar boʻyicha umumiy siyosatlarni ishlab chiqishga koʻmaklashadi.
- **Kiberjinoyatlarni oldini olish**: Europol, kiberjinoyatlarni oldini olish va bu sohada huquqiy yordam koʻrsatish uchun keng qamrovli tadbirlarni tashkil qiladi. Bu, oʻz ichiga, xavfsizlikka ta'sir etuvchi yangi xavf-xatarlar va texnologiyalarni tahlil qilishni oladi.
- **Maxsus operatsiyalar va tarmoq tahlili**: Europolning Kiberjinoyatlarni tekshirish boʻlimi, a'zo davlatlar bilan birgalikda, kiberjinoyatlarni aniqlash uchun murakkab tarmoq tahlilini amalga oshiradi va global operatsiyalarni tashkil qiladi.

Europol va INTERPOLning hamkorligi, kiberjinoyatlarni globallashgan va turli milliy va yuridik tizimlarga ega boʻlgan jinoyatlar sifatida qarashga imkon beradi. Shu bilan birga, ushbu tashkilotlar orqali amalga oshirilgan xalqaro operatsiyalar, kiberjinoyatlarni oldini olishda global miqyosda izlanishlarni davom ettirishga yordam beradi. Xalqaro hamkorlik, bu tashkilotlarning kiberjinoyatlarni aniqlashdagi muvaffaqiyatini oshirish va yangi texnologiyalarni qoʻllash imkoniyatlarini kengaytirish imkonini beradi.

UNODC (BMT Giyohvandlik va jinoyatchilik boshqarmasi) tashabbuslari. Xalqaro miqyosda kiberjinoyatlarga qarshi kurashishda Birlashgan Millatlar Tashkiloti (BMT) tarkibidagi Giyohvandlik va jinoyatchilik boshqarmasi (UNODC) muhim tashabbuslarni ilgari surib, koʻplab davlatlarning samarali hamkorlikda faoliyat yuritishiga yordam bermoqda. UNODC, asosan, kiberjinoyatlarning global tahdid sifatida ta'sirini kamaytirish va ularni jinoyat deb e'tirof etish uchun zarur huquqiy va texnik asoslarni taqdim etish yoʻlida jahon miqyosida faoliyat olib bormoqda. Bu tashkilot, kiberjinoyatlarni aniqlash, oldini olish, tergov qilish va ular bilan bogʻliq xalqaro hamkorlikni kuchaytirish borasida asosiy roʻl oʻynaydi.

UNODCning kiberjinoyatlarga qarshi kurashishda oʻrni va asosiy tashabbuslari. UNODCning kiberjinoyatlarga qarshi kurashish boʻyicha faoliyatlari asosan quyidagi yoʻnalishlarga qaratilgan:

- **Kiberjinoyatlar bilan bog‘liq xalqaro normativ-huquqiy bazaning shakllanishi.** UNODC, BMTning boshqa organlari bilan hamkorlikda, kiberjinoyatlarga qarshi kurashishda xalqaro huquqiy me’yorlar va standartlarni ishlab chiqish va joriy etishda muhim rol o‘ynaydi. Ushbu tashabbuslar, kiberjinoyatlar uchun umumiy ta’rif va jinoyat sifatida ularni e’tirof etishning global tizimini yaratishga qaratilgan. UNODC, davlatlarni o‘z qonunchilik tizimlarini kiberjinoyatlar bilan bog‘liq xalqaro standartlarga moslashtirishga undaydi va bu borada texnik yordam ko‘rsatadi.
- **Xalqaro hamkorlikni rivojlantirish**. UNODC, kiberjinoyatlar yuzasidan xalqaro hamkorlikni kuchaytirish uchun ko‘plab dasturlarni amalga oshiradi. Tashkilot, davlatlar o‘rtasida axborot almashishni rivojlantirish va resurslarni birlashtirish orqali kiberjinoyatlar bilan bog‘liq murojaatlar va tergovlarni amalga oshirishni osonlashtiradi. UNODCning tashabbuslari, xalqaro miqyosda kiberjinoyatlarni nazorat qilishni va ularni oldini olish uchun samarali usullarni ishlab chiqishni o‘z ichiga oladi.
- **Kiberxavfsizlikni ta’minlash va resurslarni taqdim etish**. UNODC, davlatlarga kiberjinoyatlarga qarshi kurashishda zarur bo‘lgan texnik resurslar va bilimlarni taqdim etadi. Bu, ayniqsa, kam rivojlangan va rivojlanayotgan mamlakatlarda ahamiyatlidir, chunki bu davlatlar o‘zlarining kiberxavfsizlik tizimlarini yaratishda yordamga muhtojdir. UNODC, o‘quv dasturlari, seminarlar va amaliy kurslar orqali davlatlarga kiberjinoyatlar bilan kurashish bo‘yicha zarur bilimlarni etkazib beradi. Bu, ayniqsa, kiberxavfsizlikni oshirish va jinoyatlarni tergov qilish uchun zarur texnologik vositalar va mutaxassislarni tayyorlashda muhim rol o‘ynaydi.
- **Kiberjinoyatlarga qarshi kurashishda normativ-huquqiy yordam**. UNODC, kiberjinoyatlarni oldini olish va ularga qarshi kurashishda normativ-huquqiy yordamni taqdim etadi. Tashkilot, BMTning boshqa organlari bilan hamkorlikda, kiberjinoyatlarning jinoyat sifatida tan olinishi uchun qonuniy asoslarni yaratish bo‘yicha ishlaydi. Shuningdek, bu tashabbuslar, davlatlarning kiberjinoyatlarni aniqlash, tergov qilish va jinoyatchilarni jazolash bo‘yicha huquqiy asoslarni mustahkamlashga qaratilgan.
- **Ochiqlik va global hamkorlikni ta’minlash**. UNODC, xalqaro kiberxavfsizlikni ta’minlashda global hamkorlikni kuchaytirish va ochiqlikni rivojlantirishga qaratilgan tashabbuslar bilan shug‘ullanadi. Tashkilot, davlatlar o‘rtasida mavjud bo‘lgan axborot xavfsizligi va kiberjinoyatlar bilan

bog‘liq masalalarda mutaxassislarni birlashtirish va global miqyosda ko‘rib chiqish imkoniyatlarini yaratadi. UNODC, shuningdek, xalqaro hamkorlik va ma’lumot almashish uchun muhim mexanizmlar ishlab chiqishga yordam beradi.

- **Kiberjinoyatlarga qarshi global siyosatni shakllantirish**. UNODC, kiberjinoyatlar va ularning oldini olishga qaratilgan global siyosatlarni shakllantirishda ham ishtirok etadi. Tashkilot, davlatlarning o‘zaro hamkorligini kuchaytirish, kiberxavfsizlik siyosatlarini ishlab chiqish va global miqyosda kiberjinoyatlarga qarshi kurashish uchun xalqaro siyosatlarni ishlab chiqishga yordam beradi. Bunday tashabbuslar, dunyo bo‘ylab kiberjinoyatlarni kamaytirish va global xavfsizlikni oshirishga yordam beradi.

Xulosa qilib aytganda, UNODC kiberjinoyatlarga qarshi kurashishda yirik xalqaro tashkilot sifatida, global hamkorlikni rivojlantirish, kiberjinoyatlarni oldini olish, davlatlar o‘rtasidagi axborot almashishni osonlashtirish va resurslarni birlashtirishda muhim rol o‘ynaydi. Tashkilot, kiberjinoyatlar bilan bog‘liq me’yoriy-huquqiy bazani shakllantirish, texnik va huquqiy yordam ko‘rsatish, o‘quv dasturlarini tashkil etish orqali samarali kiberxavfsizlikni ta’minlashga hissa qo‘shadi. UNODCning tashabbuslari, ayniqsa, rivojlanayotgan mamlakatlar uchun kiberjinoyatlarga qarshi kurashishda muhim qo‘llab-quvvatlovchi mexanizm sifatida xizmat qiladi.

Maxsus kiberpolitsiya bo‘linmalari. Kiberjinoyatlar tez sur’atlar bilan rivojlanayotgan va murakkablashayotgan global tahdiddir. Ushbu jinoyatlarning oldini olish va ularga qarshi kurashish davlatlar uchun muhim va dolzarb masala bo‘lib, faqat milliy darajada emas, balki xalqaro hamkorlikda samarali hal etilishi zarur. Kiberjinoyatlar bilan kurashish va kiberxavfsizlikni ta’minlash uchun har bir davlatning milliy politsiyasi, shuningdek, xalqaro darajadagi maxsus kiberpolitsiya bo‘linmalari faoliyat yuritadi. Ushbu bo‘linmalar, o‘zaro hamkorlikda ishlash orqali kiberjinoyatlar va kiberxavfsizlik tahdidlariga qarshi kurashishning samarali mexanizmlarini yaratishadi. Xalqaro kiberpolitsiya bo‘linmalarining asosiy vazifalari orasida jinoyatchilarni aniqlash, kiberjinoyatlarni tergov qilish, xalqaro operatsiyalarni boshqarish va kiberxavfsizlik bo‘yicha yirik tashabbuslarni amalga oshirish kiradi.

Maxsus kiberpolitsiya bo‘linmalarining tashkil etilishi va faoliyatining mohiyati. Maxsus kiberpolitsiya bo‘linmalari, asosan, davlatlarning politsiya tizimlarida kiberjinoyatlarga qarshi kurashishga

mo‘ljallangan alohida bo‘limlar sifatida faoliyat yuritadilar. Ularning asosiy vazifasi, kiberjinoyatlarni aniqlash, tergov qilish, jinoyatlarni aniqlash uchun zarur bo‘lgan texnik resurslarni taqdim etish va davlatlar o‘rtasida xalqaro hamkorlikni rivojlantirishdir.

Kiberjinoyatlarga qarshi kurashish uchun tashkil etilgan maxsus bo‘linmalar ko‘pincha politsiya yoki xavfsizlik organlarining yuqori darajali mutaxassislaridan iborat bo‘lib, ular kiberjinoyatlarning turli turlarini aniqlash va ularga samarali javob berish uchun malakali bilim va texnik vositalarga ega. Bunday bo‘linmalar, kiberjinoyatlarni oldini olish, jinoyatchilarni ushlash va jinoyatlarni tergov qilishda, davlatlar o‘rtasida axborot almashish va umumiy siyosatlarni ishlab chiqishda muhim o‘rin tutadi.

Xalqaro kiberpolitsiya bo‘linmalarining tashkiloti va funktsiyalari. Kiberpolitsiya bo‘linmalarining tashkiloti va faoliyatlari quyidagi asosiy yo‘nalishlarga asoslanadi:

✓ **Kiberjinoyatlarni aniqlash va tergov qilish**. Kiberpolitsiya bo‘linmalari, avvalo, kiberjinoyatlarning o‘ziga xos xususiyatlarini hisobga olgan holda, yangi turdagi jinoyatlar va ularning jinoyatga oid barcha aloqalarini aniqlashga qaratilgan ishlarga e’tibor qaratadi. Bular orasida, kiberhujumlar, axborotlarni o‘g‘irlash, moliyaviy firibgarliklar, tarmoq hujumlari, odam savdosi, Internet orqali tahdidlar va boshqa kiberjinoyatlar mavjud. Kiberpolitsiya bo‘linmalari, jinoyatni tergov qilishda kerakli texnik vositalar va ekspertizani taqdim etadi.

✓ **Xalqaro hamkorlikni rivojlantirish**. Kiberjinoyatlar ko‘pincha xalqaro o‘lchamga ega bo‘lib, global miqyosda texnologiyalar orqali amalga oshiriladi. Shuning uchun, kiberpolitsiya bo‘linmalari, mamlakatlar o‘rtasida hamkorlikni kuchaytirish, birgalikda tergov ishlari olib borish va kiberjinoyatlarni aniqlashda global tarmoqda ma’lumot almashish uchun zarur mexanizmlar yaratadi. Maxsus kiberpolitsiya bo‘linmalari, xalqaro tashkilotlar bilan hamkorlikda kiberjinoyatlar bo‘yicha global miqyosdagi operatsiyalarni amalga oshiradi.

✓ **Kiberxavfsizlik va texnik yordami taqdim etish**. Maxsus kiberpolitsiya bo‘linmalari, o‘z faoliyatini olib borishda, davlatlarga texnik yordami va malakali maslahatlar taqdim etadi. Bu, kiberjinoyatlar bilan kurashish uchun zarur bo‘lgan bilimlar va tajribalarni o‘rgatish, texnologik vositalarni ishlatish, shuningdek, xavfsizlikni ta’minlash uchun maxsus uskunalarni taqdim etishni o‘z ichiga oladi. Kiberpolitsiya bo‘linmalari, yangi

kiberxavflarni oldini olish va ularning oldini olish bo‘yicha maslahatlar bilan ta’minlashda ham ishtirok etadi.

✓ **Xalqaro operatsiyalarni amalga oshirish**. Kiberpolitsiya bo‘linmalari, keng qamrovli xalqaro operatsiyalarni amalga oshirishda muhim rol o‘ynaydi. Bunday operatsiyalar, bir necha davlatlarning kiberpolitsiya bo‘linmalari ishtirokida, global miqyosda kiberjinoyatchilarni aniqlash va jazolash, jinoyatlarni oldini olish va tergov qilishga qaratilgan bo‘ladi. Masalan, INTERPOL va Europolning kiberjinoyatlar bo‘yicha operatsiyalarini olib borish uchun maxsus kiberpolitsiya bo‘linmalari ishtirok etadi.

Maxsus kiberpolitsiya bo‘linmalari va xalqaro hamkorlik. Xalqaro miqyosda maxsus kiberpolitsiya bo‘linmalari bir-biri bilan yaqindan hamkorlik qiladi va o‘zaro ma’lumot almashish orqali kiberjinoyatlarni tezda aniqlash va tergov qilish imkonini beradi. Bunday hamkorlik, o‘zaro ishonchni mustahkamlash, operatsiyalarni muvofiqlashtirish va xalqaro sudlarda huquqiy asoslar yaratish uchun zarurdir.

Xalqaro tashkilotlar, xususan, INTERPOL va Europolning kiberjinoyatlar bo‘yicha faoliyatlarini muvofiqlashtirishda maxsus kiberpolitsiya bo‘linmalari muhim rol o‘ynaydi. Ular davlatlar o‘rtasida operativ ma’lumot almashish, texnik yordam ko‘rsatish va kiberjinoyatlarni oldini olishga qaratilgan birgalikdagi tashabbuslarni amalga oshiradilar. Bunday hamkorlik, global miqyosda kiberjinoyatlarni aniqlash va ularni oldini olishda samarali va tezkor javob choralarini ko‘rishga yordam beradi.

Xulosa qilib aytganda, Maxsus kiberpolitsiya bo‘linmalari, davlatlar o‘rtasida samarali hamkorlikni ta’minlash, kiberjinoyatlarni aniqlash va tergov qilish, kiberxavfsizlikni oshirish, va xalqaro operatsiyalarni amalga oshirishda muhim vosita hisoblanadi. Ular, faqat milliy darajada emas, balki xalqaro hamkorlikda kiberjinoyatlarga qarshi kurashishda samarali mexanizmlar yaratishga yordam beradi. Bunday maxsus bo‘linmalar, davlatlar o‘rtasida xavfsizlikni ta’minlash va kiberjinoyatlarning oldini olishning global tizimiga asoslanadi, shu bilan birga, kiberjinoyatlar bilan bog‘liq murakkab masalalarni hal etish uchun zarur bo‘lgan texnik va huquqiy resurslarni taqdim etadi.

3.3. Huquqni muhofaza qiluvchi organlararo hamkorlik

Xalqaro kiberjinoyatlarga qarshi kurashishda huquqni muhofaza qiluvchi organlarning o‘zaro hamkorligi muhim ahamiyatga ega. Kiberjinoyatlar global tahdid sifatida mamlakatlarning ichki xavfsizligini tahdid qilib, ularni samarali

tarzda bartaraf etish uchun faqat milliy darajadagi choralardan foydalanish yetarli emas. Kiberjinoyatlar koʻpincha davlatlararo chegaralarni kesib oʻtadigan va ularda turli yuridik tizimlar va siyosiy muhitlar mavjud boʻlgan xususiyatlarga ega. Shuning uchun huquqni muhofaza qiluvchi organlararo hamkorlik nafaqat samarali jinoyatlarni aniqlash va tergov qilishda, balki jinoyatlarni oldini olishda ham muhim rol oʻynaydi.

Kiberjinoyatlarning murakkabligi, ularning tez rivojlanishi va xalqaro darajada keng tarqalishi huquqni muhofaza qiluvchi organlarning oʻzaro koordinatsiyalashgan faoliyatini talab qiladi. Huquqni muhofaza qiluvchi organlar, shu jumladan politsiya, sud tizimi, prokuratura va boshqa mutasaddi idoralar kiberjinoyatlarni aniqlash va ularga qarshi kurashishda oʻzaro hamkorlikda ishlashlari kerak. Bu hamkorlik, turli mamlakatlar orasidagi axborot almashish, operatsion yordam va umumiy muammolarga qarshi hamkorlik qilishni oʻz ichiga oladi.

Huquqni muhofaza qiluvchi organlararo hamkorlikning ahamiyati

✓ **Xalqaro yuridik va siyosiy muhitdagi qiyinchiliklar**. Kiberjinoyatlar, koʻpincha davlatlararo yuridik tizimlar oʻrtasidagi farqlarni yuzaga keltiradi. Shu sababli, huquqni muhofaza qiluvchi organlarning hamkorligi, ayniqsa, kiberjinoyatlar boʻyicha tergov va sud jarayonlarida jiddiy ahamiyatga ega. Organlar oʻrtasidagi mustahkam hamkorlik, davlatlar oʻrtasidagi huquqiy muammolarni bartaraf etishga yordam beradi. Shuningdek, bunday hamkorlik, kiberjinoyatlar bilan bogʻliq barcha huquqiy masalalarni hal qilishda zarur boʻlgan resurslar va bilimlarni birlashtirishga imkon yaratadi.

✓ **Axborot almashish va operatsiyalarni muvofiqlashtirish**. Kiberjinoyatlar koʻpincha turli mamlakatlar va hududlarda amalga oshiriladi, shuning uchun huquqni muhofaza qiluvchi organlar oʻrtasida axborot almashish va operatsiyalarni muvofiqlashtirish zarur. Xalqaro miqyosda kiberjinoyatlarni aniqlash va tergov qilish jarayonida, maxsus politsiya boʻlinmalari, kiberxavfsizlik xizmatlari va boshqa mutasaddi idoralar birgalikda ishlash orqali samarali javob choralarini koʻrishadi. Axborot almashish, xususan, kiberjinoyatlarning oldini olish va jinoyatchilarni ushlashda samarali usul hisoblanadi.

✓ **Global tarmoqda kooperatsiyaning kuchayishi**. Kiberjinoyatlar koʻpincha yirik transmilliy jinoyat tarmoqlarini oʻz ichiga oladi. Shunday qilib, huquqni muhofaza qiluvchi organlar oʻrtasida xalqaro hamkorlikni

mustahkamlash, global tarmoqda jinoyatchilarga qarshi samarali kurashish uchun zarurdir. Har bir mamlakatda kiberjinoyatlarni aniqlash, oldini olish va jazolash uchun alohida tizimlar mavjud bo‘lsa-da, ularning xalqaro hamkorlikda ishlashi, jinoyatlarning transmilliy xususiyatlarini hisobga olgan holda, sezilarli darajada samaraliroq bo‘ladi.

✓ **Samarali kiberpolitsiya faoliyatining ta’minlanishi**. Huquqni muhofaza qiluvchi organlararo hamkorlik, kiberpolitsiya faoliyatining muvaffaqiyatli bo‘lishi uchun zarur. Kiberpolitsiya va huquqni muhofaza qiluvchi boshqa organlar o‘rtasidagi o‘zaro hamkorlik, nafaqat jinoyatlarni aniqlash va tergov qilish, balki jinoyatchilarni ushlash, huquqiy javobgarlikni ta’minlash va jinoyatlarni oldini olishda ham muhim rol o‘ynaydi. Xalqaro hamkorlik, maxsus operatsiyalarni tashkil etish va jinoyatlarni aniqlashda ta’minlaydigan resurslar va bilimlarni birlashtirish imkoniyatini yaratadi.

Xalqaro huquqni muhofaza qiluvchi organlararo hamkorlikning asosiy mexanizmlari

✓ **Interpol va Europolning roli**. Xalqaro hamkorlikni ta’minlashda Interpol va Europol kabi tashkilotlar asosiy o‘rin tutadi. Interpol, asosan, huquqni muhofaza qiluvchi organlar o‘rtasida ma’lumot almashish va transmilliy jinoyatlarga qarshi kurashishda koordinator sifatida faoliyat yuritadi. Europol esa, yevropa davlatlarining xavfsizlik va huquqni muhofaza qilish tizimlari o‘rtasida hamkorlikni kuchaytirish va operatsiyalarni muvofiqlashtirishda muhim rol o‘ynaydi.

✓ **Global axborot almashish tarmoqlari**. Huquqni muhofaza qiluvchi organlararo hamkorlikning muhim tarkibiy qismi global axborot almashish tarmoqlaridir. Bunday tarmoqlar, davlatlar va tashkilotlar o‘rtasida kiberjinoyatlar bilan bog‘liq axborotlarni tezkor almashish imkonini beradi. Xalqaro tarmoqlar, ayniqsa, jinoyatlarni tergov qilishda operativlikni ta’minlashda muhim vosita bo‘lib xizmat qiladi.

✓ **Kiberjinoyatlar bo‘yicha xalqaro sudlar va tribunallar**. Xalqaro huquqni muhofaza qiluvchi organlararo hamkorlik, shuningdek, kiberjinoyatlar bo‘yicha xalqaro sudlar va tribunallarni tashkil etish va ularda jinoyatchilarni jazolashda ham o‘z aksini topadi. Bu kabi sudlar, transmilliy jinoyatlar uchun universal yuridik asoslarni yaratish va global miqyosda huquqni muhofaza qiluvchi organlar o‘rtasida hamkorlikni yanada mustahkamlashga xizmat qiladi.

Xulosa qilib aytganda, Kiberjinoyatlarga qarshi kurashishda huquqni muhofaza qiluvchi organlararo hamkorlik juda muhim ahamiyatga ega. Bu hamkorlik, kiberjinoyatlar bilan bog‘liq transmilliy va hududlararo muammolarni samarali hal etishga yordam beradi. Xalqaro miqyosda axborot almashish, operatsiyalarni muvofiqlashtirish va kiberjinoyatlarni aniqlashda huquqni muhofaza qiluvchi organlarning birgalikdagi harakatlari kiberjinoyatlarni oldini olish va ularni tergov qilishda muhim rol o‘ynaydi. Huquqni muhofaza qiluvchi organlar o‘rtasidagi hamkorlikni rivojlantirish, kiberxavfsizlikni ta’minlash va global xavfsizlikni kuchaytirish uchun zarur vosita hisoblanadi.

Ma’lumot almashish protokollari. Xalqaro kiberjinoyatlarga qarshi kurashishda huquqni muhofaza qiluvchi organlararo hamkorlikning muhim elementlaridan biri ma’lumot almashishdir. Kiberjinoyatlar ko‘pincha davlatlararo chegaralarni kesib o‘tgan holda amalga oshiriladi, shu bois, huquqni muhofaza qiluvchi organlar o‘rtasida samarali ma’lumot almashish, jinoyatchilarni aniqlash, ularga qarshi kurashish va jinoyatlarni oldini olishda muhim vosita hisoblanadi. Xalqaro darajada axborot almashishning aniq va samarali mexanizmlarini ishlab chiqish, huquqni muhofaza qiluvchi organlar o‘rtasidagi hamkorlikni mustahkamlashga yordam beradi. Bunday protokollar jinoyatlarni tergov qilish va sud jarayonlarini olib borishda, shuningdek, kiberjinoyatlarni tez va samarali aniqlashda zarur bo‘lgan axborotning o‘z vaqtida almashilishini ta’minlaydi.

Ma’lumot almashish protokollarining maqsadi va ahamiyati

✓ **Kiberjinoyatlar bilan kurashish samaradorligini oshirish**. Kiberjinoyatlar ko‘pincha transmilliy xususiyatga ega bo‘lib, bir mamlakatning hududidan boshqa mamlakatning hududiga o‘tishi yoki bir necha mamlakatlarning resurslaridan foydalanish orqali amalga oshiriladi. Shu sababli, ma’lumot almashish protokollari kiberjinoyatlar bo‘yicha tergovlarni tezkor va samarali olib borish uchun zarur. Bunday protokollar, ayniqsa, xalqaro darajada qo‘llaniladigan ma’lumot almashish tizimlari, davlatlar o‘rtasidagi o‘zaro ishonchni mustahkamlash, ma’lumotni tez va xavfsiz uzatishni ta’minlashda muhim ahamiyatga ega.

✓ **Axborot almashishning huquqiy asoslari**. Ma’lumot almashish protokollari, shuningdek, xalqaro huquqiy tizimda o‘z o‘rniga ega bo‘lib, ular o‘rtasida aniq huquqiy asoslarni yaratadi. Har bir davlatda huquqiy tizim va qonunchilik farq qiladi, lekin ma’lumot almashishning standartlashtirilgan

mexanizmlari va protokollari orqali davlatlar o‘rtasida qonuniy va xavfsiz axborot almashish mumkin bo‘ladi. Shu bilan birga, ma’lumot almashishning shaffofligi va xavfsizligini ta’minlash, jinoyatlarni aniqlashda ishonchni oshiradi.

✓ **Xavfsizlik va maxfiylikni ta’minlash**. Kiberjinoyatlar bilan kurashishda ma’lumot almashish jarayonida xavfsizlik va maxfiylik masalalari katta ahamiyatga ega. Bunday protokollar, axborotning noxush shaxslar tomonidan qo‘lga kiritilishining oldini olish, shuningdek, jinoyatchilarni aniqlash uchun zarur bo‘lgan ma’lumotni to‘g‘ri va xavfsiz uzatishni ta’minlaydi. Shuningdek, axborot almashishning samarali mexanizmlari jinoyatchilarga qarshi xalqaro miqyosda kurashda davom etayotgan harakatlarning muvaffaqiyatiga katta ta’sir ko‘rsatadi.

Ma’lumot almashish protokollari va xalqaro tashkilotlarning roli

✓ **Interpol va Europolning axborot almashishdagi o‘rni**. Xalqaro miqyosda ma’lumot almashishning muhim tashkilotlari Interpol va Europoldir. Interpol, o‘zining global tarmog‘i orqali, huquqni muhofaza qiluvchi organlar o‘rtasida axborot almashishni osonlashtiradi. Europol esa, ayniqsa, Yevropa hududida, kiberjinoyatlarga qarshi kurashish va axborot almashishda muhim rol o‘ynaydi. Boshqa xalqaro va mintaqaviy tashkilotlar ham, shu jumladan, BMTning Kriminalishlar bo‘yicha ofisi va boshqa hududiy tashkilotlar, axborot almashishning samarali mexanizmlarini yaratish va takomillashtirishda ishtirok etadi.

✓ **Xalqaro shartnomalar va huquqiy kelishuvlar**. Ma’lumot almashish protokollari xalqaro shartnomalar va kelishuvlarga asoslanadi. Masalan, **Budapeştdagi Kiberjinoyatlar to‘g‘risidagi Konvensiya** (2001), kiberjinoyatlar bo‘yicha davlatlar o‘rtasida axborot almashish va hamkorlik qilishni qo‘llab-quvvatlovchi huquqiy asosni yaratadi. Ushbu konvensiya kiberjinoyatlarga qarshi kurashishda davlatlarning hamkorligini kuchaytirishga xizmat qiladi va axborot almashishning texnik jihatlarini belgilaydi. Bunday shartnomalar va kelishuvlar, axborot almashishning xalqaro darajadagi samaradorligini ta’minlaydi.

✓ **Global axborot tarmoqlari va tizimlar**. Ma’lumot almashish protokollari, ayniqsa, global axborot tarmoqlari orqali amalga oshiriladi. Ushbu tarmoqlar, jinoyatlarni aniqlash va ushlashda yordam beradi, shuningdek, mamlakatlar o‘rtasida real vaqt rejimida axborot almashish imkoniyatini yaratadi. Global axborot almashish tizimlarining rivojlanishi,

kiberjinoyatlarni tezkor tarzda aniqlash, tergov qilish va jinoyatchilarni qidirish imkonini beradi. Bunday tizimlar, shuningdek, davlatlar o‘rtasida xavfsizlikni mustahkamlashga yordam beradi.

Axborot almashish protokollarining huquqiy va amaliy jihatlari

✓ **Standartlashgan axborot almashish protokollari**. Kiberjinoyatlar bilan kurashishda ma’lumot almashishning standartlashtirilgan protokollari, axborotni uzatishning samarali va xavfsiz yo‘lini yaratadi. Axborot almashishning yuqori darajadagi xavfsizlikni ta’minlaydigan protokollarni ishlab chiqish, barcha ishtirokchilar uchun aniq qoidalar va me’yorlarni belgilaydi. Shuningdek, bunday protokollar jinoyatchilarni qidirishda ko‘rsatilgan axborotni to‘g‘ri va samarali tarzda uzatish imkoniyatini yaratadi.

✓ **Xalqaro miqyosda axborot almashishning ehtiyojlari**. Ma’lumot almashishning xalqaro darajadagi ehtiyojlari kiberjinoyatlarning o‘ziga xos xususiyatlari bilan bog‘liq. Davlatlar, kiberjinoyatlarga qarshi kurashishda umumiy strategiyalar va tizimlar asosida axborot almashishni amalga oshiradilar. Bu axborot almashish, kiberjinoyatlarni aniqlash va jinoyatlarni oldini olishda muhim omil bo‘lib xizmat qiladi.

Xulosa qilib aytganda, Ma’lumot almashish protokollari kiberjinoyatlarga qarshi xalqaro hamkorlikni samarali ta’minlashda muhim rol o‘ynaydi. Xalqaro miqyosda axborot almashishning huquqiy va texnik asoslarini yaratish, huquqni muhofaza qiluvchi organlar o‘rtasidagi ishonchni kuchaytiradi, jinoyatlarni aniqlash va ularga qarshi kurashishda samaradorlikni oshiradi. Shu bois, xalqaro axborot almashish protokollari global kiberjinoyatlarga qarshi kurashishda mustahkam huquqiy va amaliy asos bo‘lib xizmat qiladi.

Tezkor javob berish guruhlari (CERT, CSIRT). Kiberjinoyatlar bilan kurashishda muhim o‘rin tutadigan tushunchalardan biri – bu Tezkor javob berish guruhlari (CERT – Computer Emergency Response Team yoki CSIRT – Computer Security Incident Response Team). Ular kiberxavfsizlikni ta’minlash va kiberjinoyatlarga tezkor va samarali javob berish uchun maxsus tashkil etilgan jamoalar bo‘lib, ularning asosiy maqsadi kiberhujumlar, xavfsizlik teshiklari, va boshqa kiberxavf-xatarlarni bartaraf etishda faoliyat yuritishdan iboratdir. CERT yoki CSIRT tashkilotlari global miqyosda huquqni muhofaza qiluvchi organlar bilan hamkorlikda kiberjinoyatlarni aniqlash, oldini olish va bartaraf etishda muhim rol o‘ynaydi.

Tezkor javob berish guruhlari, asosan, kiberhujumlar yuzaga kelgan paytda tezkor tarzda harakat qilish, zararni minimallashtirish va kerakli chora-tadbirlarni amalga oshirishga qaratilgan. Ularning faoliyati, axborot tizimlarining xavfsizligini ta’minlash, kiberhujumlar, viruslar va zararli dasturlarni tahlil qilish, huquqiy va texnik yordam ko‘rsatish, shuningdek, boshqa davlatlar va xalqaro tashkilotlar bilan hamkorlikda ishlashni o‘z ichiga oladi.

Tezkor javob berish guruhlarining asosiy vazifalari va faoliyat yo‘nalishlari

✓ **Kiberhujumlarni aniqlash va javob berish**. Tezkor javob berish guruhlari o‘zining asosiy vazifalaridan biri sifatida kiberhujumlarni tezda aniqlash va ularga samarali javob berishni ko‘zda tutadi. Ular tarmoqda yuzaga kelgan xavfsizlik teshiklarini tahlil qilib, hujumlarni to‘xtatish uchun zaruriy choralarni ko‘radilar. Shu bilan birga, zararlangan tizimlarni tiklash, hujumchilarning izini kuzatish va ular bilan bog‘liq malumotlarni to‘plash ham guruhlarning vazifalaridan biridir.

✓ **Axborot almashish va hamkorlik**. CERT va CSIRT guruhlari kiberhujumlar haqida axborot almashish va boshqa xavfsizlik guruhlari bilan hamkorlik qilishda muhim rol o‘ynaydi. Kiberxavfsizlik bo‘yicha axborot almashish, kiberhujumlarning oldini olishda va bartaraf etishda katta ahamiyatga ega. Xalqaro hamkorlik, global kiberjinoyatlarga qarshi kurashishda samarali usul bo‘lib xizmat qiladi. CERT va CSIRT guruhlari o‘zaro ma’lumot almashish, umumiy xavfsizlik choralari ishlab chiqish va kiberhujumlarning keng tarqalishini oldini olish uchun samarali ish olib boradi.

✓ **Xavfsizlikni yaxshilash va oldini olish**. CERT va CSIRT guruhlari, shuningdek, kiberhujumlarning oldini olishga yo‘naltirilgan chora-tadbirlarni ishlab chiqishda faol ishtirok etadi. Kiberxavfsizlik siyosatlari va protokollarini ishlab chiqish, xavfsizlikni mustahkamlash bo‘yicha treninglar o‘tkazish va ehtimoliy xavf-xatarlar haqida axborot tarqatish kabi faoliyatlar amalga oshiriladi. Bu guruhlar, o‘z faoliyatlarini amalga oshirayotganda, bir vaqtning o‘zida tarmoq xavfsizligini yaxshilash va foydalanuvchilarni kiberhujumlardan himoya qilishga qaratilgan choralarni ko‘rishadi.

✓ **Favqulodda holatlar uchun reja ishlab chiqish**. CERT va CSIRT guruhlari uchun favqulodda vaziyatlarga tayyor turish juda muhimdir. Ular o‘z faoliyatlarini doimiy ravishda optimallashtirib, kiberhujumlar yuzaga kelgan

taqdirda qanday tezkor javob berish kerakligini belgilab olishadi. Favqulodda holatlar uchun reja ishlab chiqish, masalan, zarur texnik vositalar va malakali xodimlarni tayyorlash, jamoaning samarali ishlashini ta’minlaydi. Bunday reja tayyorlash nafaqat milliy, balki xalqaro darajadagi kiberhujumlarni ham tezda bartaraf etishga imkon yaratadi.

✓ **Zarar ko‘rgan tizimlarni tiklash**. Kiberhujumlardan keyin tizimlar va tarmoqlarni tiklash, CERT va CSIRT guruhlari faoliyatining muhim qismidir. Tizimlar zarar ko‘rgan taqdirda, ularni qayta tiklash va himoya qilish uchun zaruriy choralarni ko‘rish, shuningdek, xavfsizlikning yuqori darajasini ta’minlash uchun kerakli chora-tadbirlarni amalga oshirish kerak bo‘ladi. Shuningdek, tizimni tiklashdan oldin hujumlar haqida to‘liq axborot yig‘ish va huquqiy holatni tekshirish zarur bo‘ladi.

✓ **Xavfsizlikni doimiy monitoring qilish**. Tezkor javob berish guruhlari kiberhujumlarning oldini olish va xavfsizlikni yaxshilash bo‘yicha monitoringni amalga oshirib turadilar. Bu guruhlar tarmoqlarda doimiy ravishda xavfsizlikni nazorat qilish, tarmoqda yuzaga kelgan potentsial xavf-xatarlarni aniqlash va ularga tezkor javob berishni ta’minlaydilar. Xavfsizlikni monitoring qilish, kiberxavfsizlik siyosatlarining samarali ishlashini ta’minlash va kiberhujumlarni oldini olish uchun muhim vosita hisoblanadi.

Tezkor javob berish guruhlarining xalqaro hamkorlikdagi o‘rni

✓ **Global tarmoqda kooperatsiyaning kuchayishi**. Kiberjinoyatlar, global xususiyatga ega bo‘lgani uchun, CERT va CSIRT guruhlari o‘rtasida xalqaro hamkorlikni rivojlantirish zarur. Bunday hamkorlik nafaqat jinoyatchilarga qarshi kurashishda, balki kiberxavfsizlikni mustahkamlashda ham yordam beradi. Axborot almashish, global darajadagi xavfsizlik tarmoqlarini kuchaytirish va kiberhujumlarning oldini olish uchun zarur bo‘lgan barcha texnik va inson resurslarini birlashtirishda samarali vositadir.

✓ **Interpol va Europol bilan hamkorlik**. Interpol va Europol kabi xalqaro tashkilotlar, CERT va CSIRT guruhlari bilan yaqindan hamkorlik qilib, kiberhujumlarning oldini olish va bartaraf etishda muhim rol o‘ynaydi. Axborot almashish va qo‘llab-quvvatlash jarayonlarida ushbu tashkilotlar, CERT va CSIRT guruhlari bilan birgalikda operatsiyalarni amalga oshirish, jinoyatchilarga qarshi samarali choralarni ko‘rish va zarur axborotni taqdim etishda ishtirok etadilar.

✓ **Xalqaro axborot tizimlarining o‘zaro aloqalari**
Xalqaro miqyosda axborot tizimlari va ma’lumot almashish tarmoqlari

oʻrtasidagi oʻzaro aloqalar, CERT va CSIRT guruhlari oʻrtasidagi hamkorlikni kuchaytiradi. Xalqaro axborot almashish tarmoqlari orqali, turli davlatlar va tashkilotlar oʻrtasida kiberhujumlar boʻyicha real vaqt rejimida axborot almashish amalga oshiriladi, bu esa xavfsizlikni mustahkamlashga yordam beradi.

Xulosa qilib aytganda, Tezkor javob berish guruhlari (CERT, CSIRT) kiberjinoyatlarga qarshi kurashishda muhim rol oʻynaydi. Ularning faoliyati, kiberhujumlarning oldini olish, xavfsizlikni yaxshilash va tizimlarni tiklashni oʻz ichiga oladi. Bu guruhlar nafaqat milliy, balki xalqaro darajada hamkorlik qilish orqali kiberxavfsizlikni ta’minlashga yordam beradi. Shuningdek, xalqaro hamkorlikni kuchaytirish, global miqyosda kiberjinoyatlarga qarshi samarali kurashish uchun zarur vosita boʻlib xizmat qiladi. CERT va CSIRT guruhlari oʻrtasidagi hamkorlik, kiberhujumlarni tezda aniqlash va bartaraf etishda eng samarali usul hisoblanadi.

Birgalikdagi tergovlar va operatsiyalar. Kiberjinoyatlar bilan kurashish dunyo miqyosida samarali boʻlishi uchun davlatlar va xalqaro tashkilotlar oʻrtasida mustahkam huquqni muhofaza qiluvchi organlararo hamkorlik zarur. Xususan, kiberjinoyatlarning murakkabligi, tezkorlik bilan tarqalishi va chegaralararo xarakterga ega boʻlishi tufayli, bunday jinoyatlarni aniqlash, tergov qilish va jinoyatchilarni javobgarlikka tortish uchun oʻzaro hamkorlikda birgalikda tergovlar va operatsiyalarni olib borish juda muhimdir.

Birgalikdagi tergovlar va operatsiyalar — bu huquqni muhofaza qiluvchi organlar, masalan, politsiya, maxsus xizmatlar, prokuratura va boshqa tegishli tashkilotlar oʻrtasidagi oʻzaro hamkorlikni ifodalaydi. Bu jarayonlar, nafaqat milliy darajada, balki xalqaro miqyosda ham amalga oshiriladi, chunki kiberjinoyatlar koʻpincha bir nechta davlatning hududida sodir boʻladi va davlatlarning milliy chegaralarini buzadi. Shunday qilib, kiberjinoyatlar bilan bogʻliq tergov va operatsiyalar bir davlat hududida qolmay, balki global hamkorlikni talab qiladi.

Birgalikdagi tergovlar: tavsif va zaruriyati. Birgalikdagi tergovlar — bu bir yoki bir nechta davlatning huquqni muhofaza qiluvchi organlari tomonidan, xalqaro miqyosda yoki chet eldagi jinoyatlarni tergov qilish uchun hamkorlikda olib boriladigan jarayondir. Kiberjinoyatlar koʻp hollarda bir davlatdan boshqa davlatga oʻtish, tarmoqlardan foydalanish va xalqaro axborot tizimlaridan foydalanish orqali amalga oshiriladi. Shuning uchun,

kiberjinoyatlar bilan kurashishdagi eng samarali usul – bu davlatlar o‘rtasidagi hamkorlik orqali birgalikda tergov olib borishdir.

Birgalikdagi tergovlar quyidagi afzalliklarga ega:

- **Xalqaro darajada kiberjinoyatchilarni qidirish va ushlash**. Kiberjinoyatlar ko‘pincha tezkor va murakkab xarakterga ega bo‘lib, ularning tergovini milliy hududlar bilan cheklab bo‘lmaydi. Birgalikdagi tergovlar orqali davlatlar kiberjinoyatchilarni qidirish, aniqlash va ularni ushlashda o‘zaro yordam ko‘rsatadi. Bu o‘z navbatida, jinoyatchilarning yirik kiberhujumlar tashkil qilish imkoniyatini kamaytiradi.
- **Axborot almashish va tahlil qilish**. Kiberjinoyatchilar ko‘pincha boshqa davlatlarning tarmoqlaridan foydalanadilar. Shuning uchun, tergovchilarning malakali axborot almashish tizimi orqali kiberjinoyatchilar haqidagi axborotni tezda tarqatish imkoniyati yaratadi. Kiberhujumlar va zararli dasturlarning tarqalishini oldini olish uchun har bir davlat o‘z hududida mavjud barcha zarur axborotni o‘zaro almashishi kerak.
- **Resurslar va malakali xodimlar birlashishi**. Milliy tergov organlarining imkoniyatlari doimiy ravishda yangi texnologiyalar va usullarga moslashishga ehtiyoj sezadi. Birgalikdagi tergovlar natijasida davlatlar o‘zaro texnik resurslarni, ekspertiza va malakali xodimlarni birlashtiradi. Bu kiberhujumlarni aniqlash va ularni tahlil qilishda katta yordam beradi.
- **Huquqiy muammolarni bartaraf etish**. Kiberjinoyatlar ko‘pincha bir nechta davlatlarning huquqiy tizimlariga ta’sir qiladi, shuning uchun bunday jinoyatlarni tergov qilishda huquqiy muammolar yuzaga kelishi mumkin. Birgalikdagi tergovlar, ko‘p hollarda, xalqaro huquqni qo‘llash orqali ushbu muammolarni hal etishga yordam beradi. Masalan, ekstraditsiya, huquqiy yordam va axborot almashish protokollari xalqaro darajadagi tergovlarga ko‘maklashadi.

Birgalikdagi operatsiyalar: tavsif va zaruriyati. Kiberjinoyatlarga qarshi operatsiyalar bir necha davlatlarning huquqni muhofaza qiluvchi organlari tomonidan birgalikda amalga oshiriladi. Bu operatsiyalarni amalga oshirishda maxsus vositalar, texnologiyalar va ko‘p hollarda xodimlar birlashadi. Kiberjinoyatlarni aniqlash, ularni to‘xtatish va jinoyatchilarni jazolash maqsadida xalqaro darajadagi operatsiyalarni tashkil etish zarur.

Birgalikdagi operatsiyalar quyidagi usullar orqali amalga oshiriladi:

- **Xalqaro konferentsiyalar va seminarlar**. Xalqaro darajadagi kiberxavfsizlik bo‘yicha konferentsiyalar, seminarlar va ishchi guruhlar orqali

davlatlar o‘zaro hamkorlikni kuchaytirishadi. Bunday tadbirlar orqali huquqni muhofaza qiluvchi organlar bir-birlariga o‘z tajriba va bilimlarini almashish, kelajakda birgalikdagi operatsiyalarni qanday o‘tkazish bo‘yicha muhim maslahatlar berish imkoniyatiga ega bo‘ladilar.

- **Kiberhujumlarni oldini olish operatsiyalari**. Kiberhujumlarni oldini olish uchun bir nechta davlatlarning huquqni muhofaza qiluvchi organlari tomonidan oldindan rejalashtirilgan operatsiyalar amalga oshiriladi. Masalan, kiberhujumlar haqida olingan malumotlarga asoslanib, xavfli tarmoq faoliyatlari to‘xtatilib, zararli dasturlar va tarmoqlarni blokirovka qilish amalga oshiriladi.
- **Real vaqt rejimida operatsiyalar**. Kiberhujumlar real vaqt rejimida amalga oshirilganda, huquqni muhofaza qiluvchi organlar birgalikda tezkor harakat qilishlari kerak. Shu sababli, operatsiyalar ko‘pincha real vaqt rejimida amalga oshiriladi. Bir davlat tomonidan aniqlangan xavfli tarmoq faoliyatini boshqa davlatlar bilan tezkor hamkorlikda bartaraf etish imkoniyati mavjud.
- **Xalqaro huquqni muhofaza qilish agentliklari bilan hamkorlik**. Kiberjinoyatlarni tergov qilish va operatsiyalarni amalga oshirishda xalqaro huquqni muhofaza qilish agentliklari, masalan, Interpol, Europol va BMT kabi tashkilotlar bilan hamkorlik zarur. Ular ko‘pincha global kiberhujumlarni bartaraf etishda muhim rol o‘ynaydilar.

Xulosa qilib aytganda, Birgalikdagi tergovlar va operatsiyalar kiberjinoyatlarga qarshi samarali kurashishda, xususan, transchegaraviy jinoyatlar bilan bog‘liq holatlarda muhim rol o‘ynaydi. Ular, davlatlar o‘rtasidagi o‘zaro hamkorlikni kuchaytirib, jinoyatchilarning yashirish va qochish imkoniyatlarini kamaytiradi. Bunday hamkorlik, nafaqat milliy, balki xalqaro darajadagi xavfsizlikni ta’minlashda, kiberjinoyatchilarga qarshi kurashishda juda samarali vosita hisoblanadi. Tezkor va samarali javob berish, zaruriy texnik vositalarni birlashtirish, axborot almashish va huquqiy yordam ko‘rsatish — bularning barchasi kiberjinoyatlarga qarshi xalqaro hamkorlikni mustahkamlashda muhim omillardir.

3.4. O‘zbekistonda kiberjinoyatga qarshi chora-tadbirlar

Kiberjinoyatlar bugungi kunda global xavf-xatarni tashkil etadigan va davlatlar uchun jiddiy tahdidlardan biri bo‘lib qolmoqda. O‘zbekistonda ham kiberjinoyatlarning tobora ortib borayotgan xavfi, raqamli texnologiyalar va internet tarmog‘ining keng tarqalishi, shu bilan birga, bu sohada huquqiy va

texnik imkoniyatlarning oshishi kiberjinoyatlarning oldini olish, ularni bartaraf etish va jinoyatchilarni javobgarlikka tortish boʻyicha yangi yondashuvlarni talab etadi.

Oʻzbekistonda kiberjinoyatlar bilan kurashish davlatning maqsadli siyosati va qonun hujjatlari bilan belgilangan boʻlib, bu sohada bir qancha chora-tadbirlar amalga oshirilmoqda. Kiberjinoyatlarning oldini olish va ularga qarshi kurashish sohasida hukumat tomonidan qonunchilikni takomillashtirish, zamonaviy texnologiyalarni joriy etish, huquqni muhofaza qiluvchi organlar va boshqa tashkilotlarning oʻzaro hamkorligini kuchaytirish, shuningdek, xalqaro hamkorlikni rivojlantirish zarurati tobora ortib bormoqda.

Kiberjinoyatlar nafaqat axborot tizimlarining buzilishi va shaxsiy ma’lumotlarning oʻgʻirlanishi, balki iqtisodiy, ijtimoiy va siyosiy jarayonlarga ham tahdid soladi. Oʻzbekiston bu muammolarni hal qilishda oʻzining milliy xavfsizlikni ta’minlash va kiberhujumlarga qarshi kurashish siyosatining samaradorligini oshirishga qaratilgan bir qancha tashabbuslarni amalga oshirmoqda.

Ushbu bobda Oʻzbekistonda kiberjinoyatga qarshi amalga oshirilayotgan chora-tadbirlar, shu jumladan, normativ-huquqiy bazaning takomillashtirilishi, axborot xavfsizligini ta’minlash boʻyicha tashkiliy va texnik choralar, huquqni muhofaza qiluvchi organlar oʻrtasidagi hamkorlik va xalqaro hamkorlikning ahamiyati keng yoritiladi. Bu yondashuvlar nafaqat kiberjinoyatlarning oldini olish, balki ularga qarshi kurashishda mamlakatning xalqaro miqyosdagi oʻrni va huquqiy doirasini kengaytirishga imkon beradi.

Milliy qonunchilik bazasining tahlili. Oʻzbekiston Respublikasi axborot texnologiyalarining tez rivojlanishi, internet va raqamli tizimlarning keng tarqalishi bilan birga kiberjinoyatlar va axborot xavfsizligini ta’minlash muammosiga e’tiborini kuchaytirmoqda. Kiberjinoyatlar nafaqat iqtisodiy yoki texnik zarar keltirish, balki ijtimoiy barqarorlik va milliy xavfsizlikka ham tahdid solmoqda. Shu boisdan, davlat kiberjinoyatlar bilan kurashish, axborot xavfsizligini ta’minlash va fuqarolarning raqamli huquqlarini himoya qilish boʻyicha tizimli chora-tadbirlarni amalga oshirmoqda.

Oʻzbekistonda kiberjinoyatlarni samarali nazorat qilish va ularni jinoyat deb e’tirof etish uchun yuridik asosni yaratishda milliy qonunchilikni rivojlantirishga alohida e’tibor qaratilmoqda. Ushbu qonunchilik bazasi xalqaro me’yorlarga va standartlarga muvofiqlashtirilgan holda, kiberjinoyatlarga qarshi kurashishda samarali mexanizmlarni taqdim etadi.

O‘zbekistonning kiberjinoyatlarga qarshi qonunchilikka yondashuvi. O‘zbekiston Respublikasining kiberjinoyatlar bo‘yicha qonunchilik bazasining rivojlanishi va takomillashishi ko‘plab qonun va hujjatlar bilan bog‘liq. 2019-yilda "Axborot texnologiyalari va kommunikatsiyalari sohasida kiberxavfsizlikni ta’minlash" bo‘yicha tegishli qonunlar qabul qilindi. Ushbu qonun kiberjinoyatlarni aniqlash, ular bilan kurashish, huquqni muhofaza qiluvchi organlarga tegishli vakolatlar berish, va samarali javobgarlikni ta’minlashga yo‘naltirilgan.

Kiberjinoyatlar bo‘yicha maxsus qonunlar va normativ hujjatlar. Kiberjinoyatlarni jinoyat deb e’tirof etishda maxsus qonunlar va normativ hujjatlar muhim rol o‘ynaydi. O‘zbekistonning 2009-yilda qabul qilingan "Kompyuter jinoyatlari" to‘g‘risidagi qonuni, ayniqsa, bu sohadagi huquqiy asoslarni belgilashda muhim ahamiyatga ega. Ushbu qonun kiberjinoyatlarni huquqiy tahlil qilish, ma’lumotlar o‘g‘irligi, tizimlarga noqonuniy kirish va boshqa kiberxavfsizlikka doir huquqbuzarliklarni aniqlashni maqsad qilib qo‘yadi.

2016-yilda qabul qilingan "Axborot resurslari va axborot tizimlarini himoya qilish to‘g‘risidagi" qonun, axborot xavfsizligini ta’minlash uchun zarur bo‘lgan yuridik asoslarni mustahkamlashga yordam berdi. Bu qonun, shuningdek, axborot tizimlarini himoya qilishda davlatning, shuningdek, xususiy sektorning mas’uliyatini aniqlashga qaratilgan.

Kiberjinoyatlar bo‘yicha jazolar va huquqiy mexanizmlar. Kiberjinoyatlarni jinoyat deb e’tirof etish va ularni javobgarlikka tortish uchun belgilangan jazo choralariga ham alohida e’tibor qaratish zarur. O‘zbekiston Respublikasining Jinoyat kodeksida kiberjinoyatlarning turli xil ko‘rinishlariga javobgarlik belgilangan bo‘lib, bunda kompyuter tizimlariga noqonuniy kirish, ma’lumotlarni o‘g‘irlash, zararli dasturlarni tarqatish va boshqa kiberjinoyatlar uchun belgilangan jazolar keltirilgan. Bu jazo choralariga nafaqat jinoiy javobgarlik, balki ba’zi hollarda ma’muriy javobgarlik va iqtisodiy jarimalar ham qo‘llaniladi.

Qonunchilikdagi yana bir muhim jihat, kiberjinoyatlar va kiberxavfsizlikka oid normativ hujjatlarning milliy darajada emas, balki xalqaro miqyosda ham moslashishi zaruratini hisobga olishdir. O‘zbekistonning kiberjinoyatlarni jinoyat deb e’tirof etishdagi yurisdiktsiyasi va huquqiy normativlari, shu jumladan, xalqaro konvensiyalar va bitimlar bilan birgalikda, kiberxavfsizlikni ta’minlash uchun huquqiy asos yaratadi.

Xalqaro hamkorlik va qonunlararo muvofiqlik. O‘zbekistonning kiberjinoyatlarni oldini olish va bartaraf etishdagi yondashuvlarida xalqaro hamkorlik muhim ahamiyatga ega. Mamlakat 2001-yilda imzolangan Budapest konvensiyasiga qo‘shilish orqali, kiberjinoyatlar bilan kurashishda xalqaro standartlarga muvofiqlikni ta’minlashga intilmoqda. Budapest konvensiyasi, ayniqsa, ma’lumotlarni o‘g‘irlash, kompyuter tizimlariga noqonuniy kirish va zararli dasturlarni tarqatish kabi jinoyatlar bilan bog‘liq muammolarga qarshi xalqaro huquqiy choralarni belgilaydi. O‘zbekiston o‘z qonunchiligini ushbu konvensiyaning qoidalari va prinsiplariga moslashtiradi, bu esa mamlakatning kiberxavfsizlikni ta’minlash sohasidagi yuridik doirasini mustahkamlaydi.

Xulosa qilib aytganda, O‘zbekiston Respublikasining kiberjinoyatlar bo‘yicha qonunchilik bazasi axborot xavfsizligini ta’minlash, kiberjinoyatlar bilan kurashish va zamonaviy axborot texnologiyalariga asoslangan jinoyatlarni oldini olishga qaratilgan keng qamrovli chora-tadbirlarni o‘z ichiga oladi. Milliy qonunchilik bazasining tahlili shuni ko‘rsatadiki, mamlakatda kiberjinoyatlarga qarshi samarali yuridik mexanizmlar mavjud, ammo bu sohada xalqaro hamkorlikni kuchaytirish, qonunchilikni yanada takomillashtirish va texnik muhitni rivojlantirish zarurati mavjud. O‘zbekiston kiberjinoyatlarga qarshi kurashish bo‘yicha xalqaro me’yorlarga mos ravishda qonun chiqarish va amaliy choralarni qo‘llashda o‘z o‘rnini mustahkamlashga intilmoqda.

Elektron hukumat va raqamli xavfsizlik siyosati. Zamonaviy dunyoda kiberjinoyatlar va axborot texnologiyalariga asoslangan huquqbuzarliklar bilan kurashish davlat siyosatining ajralmas qismi bo‘lib qolmoqda. O‘zbekistonda ham, raqamli texnologiyalarning keng tarqalishi, shu bilan birga, axborot tizimlariga bo‘lgan talabning ortishi kiberjinoyatlar bilan bog‘liq xavflarni keltirib chiqarmoqda. Elektron hukumatni rivojlantirish va raqamli xavfsizlik siyosatini ta’minlash, ayniqsa, davlatning kiberjinoyatlarni oldini olish va ularga qarshi kurashishdagi muvaffaqiyatini belgilaydi.

Elektron hukumat: davlat xizmatlarining raqamli tizimi. Elektron hukumat O‘zbekiston Respublikasida 2000-yillarning boshlarida shakllanib, davlat xizmatlarini yanada ochiq, samarali va tezkor tarzda taqdim etishning asosiy mexanizmiga aylangan. O‘zbekiston hukumati axborot texnologiyalaridan foydalanish orqali jamiyatdagi ijtimoiy va iqtisodiy jarayonlarni zamonaviylashtirishni maqsad qilgan. Shuningdek, davlat

organlarining raqamli tizimlarda ishlashiga asoslangan xizmatlar fuqarolar va tadbirkorlar uchun qulaylik yaratmoqda. Lekin bu raqamli transformatsiyalar bir qator xavf-xatarlarni, shu jumladan, kiberjinoyatlarni keltirib chiqarishi mumkin.

Elektron hukumat tizimi davlatning markazlashtirilgan va tarqatilgan axborot tizimlariga asoslanadi, bu tizimlarga noqonuniy kirish yoki axborot o‘g‘irliklari kabi jinoyatlarni oldini olishni ta’minlash uchun yuqori darajadagi xavfsizlikni ta’minlash zarur. O‘zbekistonning axborot tizimlarida xavfsizlikni ta’minlashga qaratilgan bir qator qonunchilik hujjatlari va normativ talablar mavjud. Xususan, 2019-yilda qabul qilingan "Axborot resurslari va axborot tizimlarini himoya qilish to‘g‘risidagi" qonun bu sohadagi asosiy huquqiy me’yorni tashkil qiladi.

Raqamli xavfsizlik siyosati: milliy xavfsizlikni ta’minlash. Raqamli xavfsizlik siyosati, aslida, axborot va axborot texnologiyalarining himoya qilinishi, kiberhujumlar va kiberjinoyatlarning oldini olish uchun zarur bo‘lgan harakatlar tizimidir. O‘zbekiston hukumatining raqamli xavfsizlikka doir siyosati, milliy xavfsizlikning ajralmas bir qismi sifatida qaraladi. Bu siyosat, asosan, kiberjinoyatlarga qarshi kurashish, davlat axborot tizimlarining himoyasini mustahkamlash va fuqarolarning shaxsiy ma’lumotlarini himoya qilishga qaratilgan.

2017-yilda O‘zbekiston Respublikasi Prezidentining "Raqamli iqtisodiyotni rivojlantirish va kiberxavfsizlikni ta’minlash to‘g‘risidagi" farmoni kiberjinoyatlarning oldini olish va milliy xavfsizlikni ta’minlashda katta ahamiyat kasb etadi. Farmon doirasida hukumatning barcha organlari va idoralari o‘rtasida axborot xavfsizligini ta’minlashga yo‘naltirilgan bir qator strategik chora-tadbirlar ishlab chiqildi. Bular orasida axborot xavfsizligi bo‘yicha texnik infratuzilma va yuridik bazaning mustahkamlash, davlat va xususiy sektordagi barcha tizimlarda xavfsizlikni ta’minlash masalalari mavjud.

Raqamli xavfsizlikka doir qonunlar va normativ hujjatlar. O‘zbekistonda raqamli xavfsizlikni ta’minlashda muhim ahamiyatga ega bo‘lgan qonun va normativ hujjatlar ishlab chiqilgan. Ushbu qonunlar kiberjinoyatlar va axborot tizimlarining xavfsizligi bilan bog‘liq har qanday huquqbuzarliklarga qarshi samarali choralarni ko‘rishga yo‘naltirilgan. Kiberjinoyatlar bilan kurashish uchun huquqni muhofaza qiluvchi organlar, xususan, Ichki ishlar vazirligi va Milliy xavfsizlik xizmati o‘zaro hamkorlikda

ishlashadi va bu yuridik mexanizmlarni amalga oshirishda o‘zining alohida o‘rniga ega.

O‘zbekiston Respublikasining Jinoyat kodeksida kiberjinoyatlar uchun belgilangan jazo choralarining tahlili shuni ko‘rsatadiki, mamlakatda kiberjinoyatlarga qarshi kurashish tizimi samarali ishlamoqda. Bu tizim, ayniqsa, internet orqali amalga oshirilgan jinoyatlarni, shu jumladan, ma’lumotlarni o‘g‘irlash, zararli dasturlarni tarqatish va boshqa huquqbuzarliklarni aniqlash va jazolashga qaratilgan.

Kiberhujumlarga qarshi yangi texnologiyalar va xalqaro hamkorlik. Kiberhujumlar va kiberjinoyatlarga qarshi kurashishda ilg‘or texnologiyalarni joriy etishning muhimligi ortib bormoqda. O‘zbekiston bu borada sun’iy intellekt, katta ma’lumotlar (big data), blokcheyn texnologiyasi va kriptografiya kabi zamonaviy texnologiyalarni tadbiq etishga intilmoqda. Ushbu texnologiyalar nafaqat axborot tizimlarining xavfsizligini ta’minlash, balki davlatning raqamli transformatsiyasini qo‘llab-quvvatlashda ham o‘z o‘rnini topadi.

Xalqaro hamkorlikning ahamiyati ham beqiyos. O‘zbekiston o‘zining xalqaro hamkorligini kuchaytirishga, xususan, kiberxavfsizlikka doir xalqaro konvensiyalar va bitimlarga qo‘shilish, kiberjinoyatlar bilan kurashish bo‘yicha xalqaro tashkilotlar bilan yaqindan ishlashga intilmoqda. Bu jarayon kiberjinoyatlarga qarshi global kurashda O‘zbekistonning roli va o‘rnini mustahkamlashga yordam beradi.

Xulosa qilib aytganda, Elektron hukumat va raqamli xavfsizlik siyosati O‘zbekistonda kiberjinoyatlarga qarshi kurashish va axborot xavfsizligini ta’minlash sohasida muhim qadamlardir. Davlatning raqamli tizimlarida xavfsizlikni ta’minlash, kiberjinoyatlar bilan kurashish va ularni oldini olish uchun amalga oshirilayotgan yuridik va texnik choralar mamlakatning global miqyosda raqamli xavfsizlikni ta’minlashdagi ishtirokini mustahkamlashga xizmat qiladi. Kiberjinoyatlar va axborot xavfsizligi sohasida xalqaro hamkorlik va ilg‘or texnologiyalarni joriy etish O‘zbekistonning xavfsiz raqamli infratuzilmasini rivojlantirishda muhim o‘rin tutadi.

Ilmiy-tadqiqot institutlari va ta’lim muassasalari roli. O‘zbekiston Respublikasida kiberjinoyatlar bilan kurashish va axborot xavfsizligini ta’minlashga qaratilgan sa’y-harakatlar nafaqat davlat organlari tomonidan amalga oshiriladi, balki ilmiy-tadqiqot institutlari va ta’lim muassasalari ham bu jarayonda muhim o‘rin tutadi. Kiberjinoyatlarga qarshi samarali kurashish

nafaqat texnik vositalar va qonunchilikka asoslangan choralarda, balki xalqning kiberxavfsizlik boʻyicha bilimini oshirish va yangi avlod kiberxavfsizligini ta’minlovchi mutaxassislarni tayyorlashda ham oʻz ifodasini topadi. Shu boisdan, ilmiy-tadqiqot institutlari va ta’lim muassasalari kiberjinoyatlarni oldini olish va ularga qarshi kurashishda mustahkam va barqaror poydevor yaratishda katta rol oʻynaydi.

Ilmiy-tadqiqot institutlarining ahamiyati. Kiberjinoyatlarning murakkabligi va tez oʻzgarib turadigan xususiyatlari ilmiy-tadqiqot ishlarini olib borishning zarurligini ta’kidlaydi. Kiberjinoyatlar bilan kurashishda ilmiy-tadqiqot institutlari, universitetlar va axborot xavfsizligi sohasidagi mutaxassislar innovatsion usullarni ishlab chiqish, kiberhujumlarning yangi turlarini aniqlash va ularga qarshi samarali himoya tizimlarini yaratish boʻyicha izlanishlar olib bormoqdalar. Ushbu institutlar tomonidan ishlab chiqilgan ilmiy va texnologik yechimlar mamlakatning raqamli xavfsizligini mustahkamlashda muhim rol oʻynaydi.

Oʻzbekistonda kiberxavfsizlik boʻyicha ilmiy tadqiqotlar olib boriladigan asosiy institutlar – Axborot texnologiyalari universiteti, Oʻzbekiston Milliy universiteti va boshqa bir qator oliy ta’lim muassasalari boʻlib, ular oʻz faoliyatida zamonaviy xavfsizlik tizimlarini rivojlantirishga katta e’tibor qaratmoqda. Ular nafaqat kiberjinoyatlarni oldini olish boʻyicha ilmiy ishlanmalar, balki xalqaro tajribalar va zamonaviy xavfsizlik metodlarini oʻrganishga qaratilgan dasturlarni ham ishlab chiqmoqdalar.

Bundan tashqari, ilmiy-tadqiqot institutlari axborot xavfsizligi sohasida jahon miqyosida yetakchi boʻlgan xalqaro konferensiyalar va simpoziumlarga qatnashib, xalqaro hamkorlikni mustahkamlashda ham ishtirok etmoqdalar. Bu institutlar tomonidan ishlab chiqilgan texnologiyalar va ilmiy yechimlar Oʻzbekistonda kiberjinoyatlarning oldini olishda yangi yondashuvlar va yuridik chora-tadbirlarni takomillashtirishga yordam beradi.

Ta’lim muassasalarining roli. Ta’lim muassasalari, ayniqsa, kiberxavfsizlik sohasidagi mutaxassislarni tayyorlashda hal qiluvchi ahamiyatga ega. Oʻzbekistonda ta’lim muassasalarida axborot texnologiyalari va kiberxavfsizlik boʻyicha keng qamrovli dasturlar mavjud. Bu dasturlar talabalarga kiberjinoyatlar, axborot tizimlarini himoya qilish, zararli dasturlarni aniqlash va kiberxavfsizlikni ta’minlash boʻyicha zarur bilimlarni taqdim etadi.

O‘zbekiston Respublikasida axborot texnologiyalari sohasida mutaxassislar tayyorlash uchun bir qator ilmiy va ta’lim muassasalari faoliyat yuritadi. Masalan, O‘zbekiston Axborot texnologiyalari universiteti, Toshkent shahridagi boshqa oliy o‘quv yurtlari va texnik institutlarida kiberxavfsizlikka alohida e’tibor qaratilgan. Bu ta’lim muassasalari zamonaviy ilmiy yondashuvlarni o‘rgatish, talabalarga kiberjinoyatlarni oldini olish va axborot tizimlarining xavfsizligini ta’minlashni o‘rgatish, shuningdek, o‘zlarini bu sohada rivojlantirishga imkon yaratmoqda.

Shuningdek, ta’lim tizimida kiberxavfsizlikni o‘rgatish faqat oliy ta’lim bilan cheklanmaydi. Maktablarda ham axborot texnologiyalarini o‘rgatishning muhimligi oshmoqda. Kiberxavfsizlikni o‘rgatish, yosh avlodni raqamli xavfsizlik bo‘yicha bilim bilan ta’minlash, kelajakda ular kiberjinoyatlarni oldini olish va kiberxavfsizlikni ta’minlashda muhim rol o‘ynashini ta’minlaydi.

Ilmiy-tadqiqotlar va amaliyotdagi yondashuvlar. Kiberjinoyatlarga qarshi kurashishda ilmiy tadqiqotlar va amaliyotning uyg‘unlashuvi muhim ahamiyatga ega. O‘zbekistonning ilmiy-tadqiqot institutlari, ta’lim muassasalari va amaliyotda ishlayotgan kiberxavfsizlik mutaxassislari o‘rtasidagi hamkorlik kiberjinoyatlar bilan samarali kurashishning samarali mexanizmlarini ishlab chiqishda asosiy omil bo‘lib qoladi. O‘quv dasturlari va ilmiy ishlar, amaliy tajribalar bilan birgalikda kiberjinoyatlarni aniqlash, ularga qarshi kurashish va oldini olish uchun yangi yondashuvlarni ishlab chiqish zarur.

Xalqaro hamkorlik. Ilmiy-tadqiqot institutlari va ta’lim muassasalari o‘rtasidagi hamkorlikning yana bir muhim jihati xalqaro aloqalardir. O‘zbekistonning kiberxavfsizlik bo‘yicha xalqaro hamkorlikni rivojlantirishga bo‘lgan intilishi, ilmiy va ta’lim muassasalarining jahon miqyosida yirik universitetlar va ilmiy institutlar bilan tajriba almashish imkoniyatini yaratadi. Bu o‘z navbatida, kiberjinoyatlarga qarshi kurashish bo‘yicha yangi, ilg‘or texnologiyalar va ilmiy yondashuvlarni joriy etishga yordam beradi.

Xulosa qilib aytganda, Ilmiy-tadqiqot institutlari va ta’lim muassasalari kiberjinoyatlarga qarshi kurashish, axborot xavfsizligini ta’minlash va kiberxavfsizlik sohasida mutaxassislarni tayyorlashda muhim rol o‘ynaydi. O‘zbekistonning ilmiy va ta’lim tizimi kiberjinoyatlarni oldini olish va ularga samarali javob berishning asosiy poydevorini yaratadi. Bu institutlar nafaqat ilmiy ishlanmalar, balki amaliyotga tadbiq etiladigan yangi texnologiyalarni

yaratishda ham asosiy o‘rin tutadi. Kiberxavfsizlik sohasidagi ta’lim va ilmiy-tadqiqot ishlarining davom etishi, O‘zbekistonning raqamli xavfsizligini ta’minlashda muvaffaqiyatli bo‘lishi uchun zarurdir.

BOB BO‘YICHA UMUMIY XULOSALAR

Mazkur bobda kiberjinoyatlarga qarshi xalqaro hamkorlik tajribasi muhokama qilindi, unda kiberjinoyatlar bilan kurashishning global darajadagi yondashuvlari va amaliyotlari batafsil tahlil qilindi. Ushbu bobda kiberjinoyatlarni oldini olish va ularni samarali tarzda jazolashda xalqaro hamkorlikning ahamiyati, shu jumladan, huquqiy va amaliy choralar yoritildi.

- **Budapest konvensiyasi: mazmuni va huquqiy asoslari** bandida kiberjinoyatlarni oldini olish va ularni javobgarlikka tortish uchun xalqaro hamkorlikni ta’minlovchi muhim huquqiy hujjat – Budapest konvensiyasi va uning o‘rni ta’riflandi. Konvensiya, asosan, kiberjinoyatlarni global miqyosda tan olish, ularni jinoyat deb e’tirof etish va ularni tergov qilish, hamda elektron dalillarni himoya qilishga yo‘naltirilgan normativ hujjat sifatida katta ahamiyatga ega. Shuningdek, konvensiyaning a’zo davlatlar o‘rtasidagi hamkorlikni kuchaytirishdagi roli, yuridik va texnik jihatlari muhokama qilindi.
- **Xalqaro tashkilotlarning roli** bandi kiberjinoyatlarga qarshi kurashishda xalqaro tashkilotlarning o‘rni va funksiyalarini ochib berdi. Xalqaro tashkilotlar, masalan, BMT, INTERPOL, va Evropa Ittifoqi, kiberxavfsizlik bo‘yicha global siyosatlarni shakllantirishda, davlatlar o‘rtasidagi hamkorlikni mustahkamlashda va kiberjinoyatlar bilan kurashishda ko‘plab ijobiy natijalarga erishishda muhim rol o‘ynaydi. Bularning barchasi mamlakatlar o‘rtasida axborot almashish, texnologik yordam ko‘rsatish va umumiy xavfsizlik choralarini ishlab chiqishda yordam beradi.
- **Huquqni muhofaza qiluvchi organlararo hamkorlik** bandi, huquqni muhofaza qiluvchi organlararo hamkorlikning kiberjinoyatlarga qarshi kurashishda qanday ahamiyatga ega ekanligini tahlil etdi. Kiberjinoyatlarni aniqlash, tergov qilish va jazolash uchun davlatlarning huquqni muhofaza qiluvchi organlari o‘rtasida samarali va tezkor hamkorlik zarur. Ushbu hamkorlik, nafaqat kiberjinoyatlar bilan bog‘liq muammolarni hal etishda, balki elektron jinoyatlarni jinoyatga aylantirishdagi yuridik me’yorlarni birlashtirishda ham muhim rol o‘ynaydi.

➢ **O‘zbekistonda kiberjinoyatga qarshi chora-tadbirlar** bandi O‘zbekistonda kiberjinoyatlar bilan kurashish uchun amalga oshirilayotgan chora-tadbirlar, qonunchilik va texnologik tadbirlarni batafsil yoritdi. O‘zbekistonning raqamli xavfsizlik siyosati, elektron hukumatni rivojlantirish va axborot texnologiyalarini xavfsizligini ta’minlashdagi faoliyatlari mamlakatning kiberjinoyatlarga qarshi kurashishda erishayotgan muvaffaqiyatlarini ko‘rsatadi. Shuningdek, kiberjinoyatlarga qarshi kurashish uchun davlat va xususiy sektorlarga o‘rnatilgan huquqiy va texnik mexanizmlar haqida so‘z yuritildi.

Xulosa qilib aytganda, Kiberjinoyatlar global muammo sifatida davlatlar va xalqaro tashkilotlarni hamkorlikka chaqirmoqda. Ushbu bobda kiberjinoyatlarga qarshi kurashish uchun xalqaro hamkorlikning qanday shakllari mavjudligi, global yondashuvlar, xalqaro huquqiy asoslar va o‘zaro amaliy hamkorlik masalalari muhokama qilindi. Budapest konvensiyasi va xalqaro tashkilotlar o‘rtasidagi hamkorlik, shuningdek, O‘zbekistonning kiberxavfsizlik va kiberjinoyatlarga qarshi kurashishda amalga oshirayotgan yuridik va texnik chora-tadbirlari, davlatlar o‘rtasidagi hamkorlikni kuchaytirish va umumiy xavfsizlikni ta’minlashda muhim o‘rin tutadi. Kiberjinoyatlar bilan kurashishda xalqaro hamkorlik, har bir davlatning milliy xavfsizligini ta’minlashning muhim komponenti sifatida xizmat qiladi.

IV BOB. KIBERJINOYATLARNI HUQUQIY JIHATDAN TAN OLISHDAGI ISTIQBOLLAR

Kiberjinoyatlar zamonaviy dunyoda tobora ko‘proq e’tibor qaratilayotgan, jamiyatning barcha sohalariga ta’sir ko‘rsatuvchi xavfli fenomenaga aylangan. Raqamli texnologiyalar va internetning rivojlanishi kiberjinoyatlarning yangi turlari, ularning turlari va amalga oshirish usullarining o‘zgarishini yuzaga keltirdi. Buning natijasida, kiberjinoyatlar an’anaviy jinoyatlar bilan solishtirganda, ko‘plab yangi yuridik muammolarni keltirib chiqarmoqda. Shunday qilib, kiberjinoyatlarni huquqiy jihatdan tan olish, ularni to‘g‘ri klassifikatsiya qilish va jinoyat sifatida e’tirof etish masalalari o‘ta muhim va dolzarb bo‘lib qolmoqda.

Ushbu bobda kiberjinoyatlarni huquqiy jihatdan tan olish va jinoyat deb e’tirof etish masalalari ilmiy jihatdan o‘rganiladi. Bu o‘rganish jarayonida kiberjinoyatlarning jahon miqyosida ta’sir doirasi, huquqiy klassifikatsiyasi va ularning huquqiy maqomini belgilashga oid istiqbollar tahlil qilinadi.

Shuningdek, xalqaro huquq tizimining kiberjinoyatlarni tan olishdagi roli, mavjud me’yorlar va normativ hujjatlarning samaradorligi, shu jumladan, zamonaviy huquqiy tizimlarga kiberjinoyatlarni o‘z ichiga olish bo‘yicha yangilanishlar va takliflar ko‘rib chiqiladi.

Kiberjinoyatlarni tan olishda yuzaga kelayotgan muammolarni hal qilishda xalqaro hamkorlik, milliy qonunchilik tizimlarining rivojlanishi va texnologik o‘zgarishlarning ta’siri katta ahamiyatga ega. Kiberjinoyatlarni jinoyat sifatida tan olishda yuridik jihatlarning o‘zgarishi va yangi normativ hujjatlarning yaratish ehtiyoji o‘ta muhimdir. Ushbu bobda kiberjinoyatlarning huquqiy klassifikatsiyasi, ularni jinoyat sifatida e’tirof etishning istiqbollari va yuzaga kelayotgan yuridik muammolarni hal qilishda o‘zgaruvchan dunyoviy sharoitlarni hisobga olish zarurligi ko‘rsatib o‘tiladi.

Shunday qilib, kiberjinoyatlarni huquqiy jihatdan tan olishning istiqbollarini ko‘rib chiqish, nafaqat jahon miqyosidagi xavfsizlikni ta’minlash, balki huquqni muhofaza qilish tizimining samaradorligini oshirishda ham muhim o‘rin tutadi.

4.1. Raqamli suverenitet va ziddiyatlar

Raqamli suverenitet, dunyo miqyosida davlatlarning o‘z hududlarida axborot oqimlarini nazorat qilish, raqamli infratuzilma va ma’lumotlarni boshqarish imkoniyatiga ega bo‘lishini ifodalaydi. Bugungi kunda, axborot texnologiyalarining rivojlanishi va internetning global tarmoq sifatida kengayishi, davlatlarning o‘z milliy qiziqishlarini himoya qilish uchun raqamli suverenitetni ta’minlash zaruriyatini keltirib chiqarmoqda. Bu jarayon, kiberjinoyatlar va raqamli tahdidlarning oshib borishi bilan yanada murakkablashmoqda, chunki zamonaviy raqamli infratuzilma va global tarmoqdagi jarayonlar ko‘plab huquqiy va siyosiy ziddiyatlarni keltirib chiqaradi.

Raqamli suverenitet va uning doirasida yuzaga keladigan ziddiyatlar xalqaro huquq, davlatlararo hamkorlik va milliy qonunchilik tizimlari o‘rtasidagi muvozanatni ta’minlashga qaratilgan ko‘plab savollarni ko‘ndalang qo‘yadi. Har bir davlat o‘z hududidagi axborot xavfsizligini ta’minlash uchun raqamli suverenitetni qo‘llashga intiladi, biroq global tarmoqlar orqali ma’lumotlarning erkin harakati bu jarayonni murakkablashtiradi. Bu shuningdek, davlatlarning o‘ziga xos siyosatlarini

amalga oshirish uchun raqamli suverenitetni qo‘llashni ta’minlashda jiddiy qiyinchiliklarga olib keladi.

Raqamli suverenitet bilan bog‘liq ziddiyatlar ko‘plab aspektlarni o‘z ichiga oladi. Birinchidan, davlatlar o‘rtasida raqamli infratuzilma va ma’lumotlar oqimi masalalarida turli yondashuvlar mavjud. Masalan, ba’zi davlatlar internetni erkin boshqarish va uning tarkibini cheklashni maqsad qilsa, boshqalari erkin axborot almashinuvi va raqamli huquqlarning himoyasini qo‘llab-quvvatlaydi. Ikkinchidan, global axborot xavfsizligi va kiberjinoyatlar bilan kurashishda xalqaro hamkorlikning ahamiyati ortsa-da, raqamli suverenitetni ta’minlashdagi farqlar davlatlar o‘rtasida xavf va manfaatlar bo‘yicha ziddiyatlarni keltirib chiqaradi.

Ushbu bo‘limda raqamli suverenitetning mohiyati va uning xalqaro huquqdagi o‘rni, shuningdek, raqamli suverenitetga asoslangan ziddiyatlarning xalqarolararo huquqiy va siyosiy aspektlari ko‘rib chiqiladi. Bu jarayonlarda yuzaga kelayotgan muammolarni hal qilishda turli davlatlarning qiziqishlari va xavfsizlik talablarini muvozanatlashtirishning o‘ta muhim ahamiyati mavjud. Raqamli suverenitetning kelajakdagi rivojlanishi va uning xalqaro hamkorlikka ta’siri, kiberjinoyatlar va global xavfsizlik masalalariga nisbatan qanday o‘zgarishlar keltirib chiqarishi muhim o‘rganish predmetiga aylanadi.

Davlatlararo “kiberurush”lar va ularning huquqiy talqini. Raqamli suverenitet va kiberxavfsizlik muammolarining o‘sib borishi bilan davlatlar o‘rtasida yangi turdagi ziddiyatlar, xususan, kiberurushlar (cyber warfare) o‘rtaga chiqdi. Kiberurush, odatda, bir davlat tomonidan boshqa bir davlatning raqamli infratuzilmasiga zarar yetkazish, muhim tizimlarni buzish yoki axborot xavfsizligini buzish maqsadida amalga oshirilgan hujum sifatida ta’riflanadi. Bu turdagi hujumlar, an’anaviy qurolli urushlar bilan solishtirilganda, ko‘plab afzalliklarga ega bo‘lishi mumkin, chunki ular ko‘p holatlarda an’anaviy huquqiy normalar bilan qamrab olinmaydi va kiberhujumlarning qiyinligini hisobga olib, ularning xalqaro huquqiy talqinini belgilash muammoli bo‘ladi.

Kiberurushlar yoki kiberhujumlar xalqaro huquq doirasida ko‘plab murakkab masalalarni keltirib chiqaradi. Ushbu hujumlar xalqaro jinoyat huquqining mavjud normalari bilan qanday tartibga solinishini aniqlash hozirda hal qilinishi zarur bo‘lgan muammo hisoblanadi. Kiberurushlar ko‘pincha davlatlararo huquqiy masalalar, masalan, davlatlararo yurisdiksiya,

suverenitet va o‘zaro hurmat masalalarini chuqurroq o‘rganishni talab qiladi. Davlatlararo kiberurushlar jiddiy xavf tug‘diradi, chunki ular iqtisodiy tizimlarni, muhim infratuzilmalarni va fuqarolarni nishonga olish imkoniyatiga ega.

Kiberurushlarning huquqiy talqini. Kiberurushlar va ularning huquqiy maqomi haqidagi muhokamalar xalqaro huquqda haligacha aniq va yagona bir qarorga kelinmagan. Bunda asosan quyidagi masalalar muhim rol o‘ynaydi:

✓ **Raqamli hujumlarning sinflanishi**: Kiberurushni xalqaro huquq doirasida aniq belgilash juda muhimdir. Ayniqsa, qanday hujumlar, qaysi sharoitda, urush deb tan olinishi kerakligi haqida aniq talqinlar mavjud emas. Hozirda kiberhujumlar o‘zining tabiatiga ko‘ra an’anaviy urushlardan farq qiladi, chunki ular odatda bevosita inson qurbonlarisiz amalga oshiriladi. Shunday bo‘lsa-da, kiberhujumlarning iqtisodiy va siyosiy ta’sirlari bir xil darajada xavfli bo‘lishi mumkin. Bunday hujumlar uchun xalqaro jinoiy huquq doirasida urush jinoyatlari yoki huquqbuzarliklarining qaysi turi qo‘llanilishi kerakligi muhokama qilinadi.

✓ **Xalqaro konvensiyalar va kiberurush**: Xalqaro huquq konvensiyalari, masalan, 1949 yilgi Jeneva konvensiyalari va boshqa urush qonunlari, an’anaviy urushlarga tegishli bo‘lgan muqaddas va umumiy me’yorlarga asoslanadi. Biroq, bu konvensiyalar kiberhujumlarni qanday talqin qilishni ko‘rsatmaydi. Bu holat kiberurushlarga nisbatan yangi xalqaro huquqiy me’yorlarni ishlab chiqish zaruratini keltirib chiqarmoqda. Shu nuqtai nazardan, kiberurushlarning xalqaro huquq doirasidagi tan olinishi va ularni o‘rganish uchun yangi talqinlar, normativ va huquqiy mexanizmlar zarurdir.

✓ **O‘zaro xavf-xatarni hisobga olish**: Davlatlar o‘rtasidagi kiberurushlar ko‘pincha bir tomonning huquqiy va siyosiy huquqlariga tahdid solish sifatida ko‘riladi. Bunday hujumlar ko‘plab mamlakatlarning iqtisodiy xavfsizligini va milliy suverenitetini jiddiy ravishda tahdid qiladi. Shu sababli, kiberurushlarning xalqaro huquq doirasida tartibga solinishi va boshqa davlatlar tomonidan aniqlanishi zarur bo‘ladi. Bunga misol tariqasida, kiberhujumlarning xalqaro diplomatik reaktsiyalari, muayyan qat’iy choralar ko‘rish yoki milliy xavfsizlikni ta’minlash uchun harbiy reaksiyalar ko‘rsatilishi mumkin.

✓ **Kiberhujumlarning ta’sirining kengligi**: An’anaviy urushlarda aksariyat hollarda fuqarolar, infratuzilma va hayotiy tizimlar nishonga olinadi, bu esa to‘g‘ridan-to‘g‘ri urush jinoyatlariga sabab bo‘ladi. Kiberhujumlar esa,

axborot tizimlarini buzish, elektron tarmoq orqali ma’lumotlarni o‘g‘irlik qilish, yoki davlatni iqtisodiy jihatdan zaiflashtirish maqsadida amalga oshirilishi mumkin. Kiberurushlar insonlarning hayotiga to‘g‘ridan-to‘g‘ri tahdid solmasada, uzoq muddatli ijtimoiy va iqtisodiy oqibatlar keltirib chiqaradi.

Xulosa qilib aytganda, Davlatlararo kiberurushlarning huquqiy talqini zamonaviy xalqaro huquqdagi eng katta muammolardan biriga aylanmoqda. Bu jarayonda kiberhujumlar bilan bog‘liq xalqaro qonunchilikni ishlab chiqish, ular uchun aniq qoidalar belgilash, hamda kiberurushlarni huquqiy jihatdan belgilash zarurati ortmoqda. Shu bilan birga, raqamli suverenitetning mustahkamlanishi va davlatlarning o‘z hududlarida axborot xavfsizligini ta’minlash uchun turli yondashuvlarni qo‘llashda, kiberurushlarning global xavfini boshqarishning muhimligini anglash zarurdir.

Internetni nazorat qilish va senzura masalalari. Raqamli suverenitet masalalari davlatlar va xalqaro tashkilotlar o‘rtasida ko‘plab ziddiyatlarga sabab bo‘lmoqda. Xususan, internetni nazorat qilish va senzura qilishning davlatlararo yondashuvlari o‘rtasidagi farqlar, raqamli suverenitetga asoslangan siyosatlarni ishlab chiqishda muhim rol o‘ynaydi. Internet, global tarmoq sifatida, barcha davlatlar uchun erkin muloqot va axborot almashish imkoniyatlarini taqdim etadi. Biroq, internetni nazorat qilish masalasi nafaqat milliy xavfsizlikni ta’minlash, balki axborot erkinligini himoya qilish va fuqarolarni xolis axborotdan xabardor qilish o‘rtasidagi muvozanatni saqlashda muhimdir.

Internetni nazorat qilish va uning suverenitetga ta’siri. Internetni nazorat qilish, asosan davlatlarning axborot xavfsizligi va milliy suverenitetni ta’minlash uchun amalga oshiriladi. Ba’zi davlatlar internetni erkinlik va ochiqlik mezonlari bilan cheklab, o‘z hududlaridagi raqamli muhitni qat’iy nazorat qilishni afzal ko‘rishadi. Bunday holatlarda davlatlar internet tarmog‘ini o‘z milliy manfaatlariga mos ravishda boshqarishga, foydalanuvchilar faoliyatini cheklashga va ma’lumotlarni tahlil qilishga urinadilar. Shu bilan birga, internetning global xarakteri sababli, bunday siyosatlar ko‘pincha xalqaro huquq va inson huquqlariga zid bo‘lishi mumkin. Bu, o‘z navbatida, global axborot oqimining erkinligini cheklaydi va davlatlar o‘rtasidagi raqamli bo‘hronlarni keltirib chiqaradi.

Raqamli suverenitetning asosiy muammosi, internetni nazorat qilish va unga bo‘lgan siyosiy yondashuvlar o‘rtasidagi ziddiyatda yotadi. Internetni

to‘liq erkinlashtirish bilan uni davlatlar tomonidan nazorat qilish o‘rtasidagi o‘zaro ziddiyatning rivojlanishi, barcha davlatlar uchun yangi xalqaro muammolarni yuzaga keltiradi. Xalqaro huquq doirasida, internetga erkin kirish huquqi bilan davlatning axborot xavfsizligi va suverenitetini himoya qilish o‘rtasidagi muvozanatni saqlashga intilish zarur.

Senzura: erkinlik va xavfsizlik o‘rtasidagi nozik chiziq. Internetda senzura qilish, asosan, davlatlar tomonidan o‘z fuqarolarining axborot oqimlarini nazorat qilish va cheklashni anglatadi. Senzura, odatda, milliy xavfsizlikni ta’minlash, terrorizmga qarshi kurashish yoki ijtimoiy tartibsizliklarni oldini olish kabi maqsadlar bilan bog‘lanadi. Biroq, axborot erkinligi va internetda erkin muloqot qilish huquqi jahon miqyosida keng e’tirof etilgan huquqlardandir. Shu sababli, davlatlar internetda axborotlarni senzura qilishni amalga oshirishda, inson huquqlarini himoya qilish, erkin fikrlarni ifodalash va demokratik qadriyatlarni saqlash masalalarini ham inobatga olishlari zarur.

Internetda senzura qilishning yanada murakkab tomonlaridan biri — bu milliy va xalqaro nuqtai nazarlar o‘rtasidagi ziddiyatdir. Ba’zi davlatlar, masalan, internetni to‘liq nazorat qilib, o‘z fuqarolariga tashqi axborot oqimlarini cheklashga harakat qiladilar. Bu holatda, ularning yondashuvi, asosan, milliy xavfsizlikni ta’minlashga qaratilgan bo‘lsa-da, bu erkin muloqotga, yangiliklarni tarqatishga va haqiqiy axborotdan foydalanuvchilarning xabardor bo‘lishiga to‘sqinlik qiladi.

Bundan tashqari, internetdagi senzura davlatlarning xalqaro imidjiga ham ta’sir ko‘rsatadi. Ko‘plab xalqaro tashkilotlar va inson huquqlari tashkilotlari, internetda senzura qilishni erkinlikni cheklash sifatida qoralashadi. Shu sababli, ba’zi davlatlar internetni to‘liq nazorat qilishni amalga oshirishda yirik iqtisodiy, diplomatik va siyosiy bosimlarga duch kelishadi.

Xalqaro yondashuvlar va raqamli suverenitetni mustahkamlash. Raqamli suverenitet va internetni nazorat qilish o‘rtasidagi muvozanatni saqlash uchun bir qator xalqaro yondashuvlar ishlab chiqilgan. Internetning global tabiati, davlatlarning o‘z hududida internetni nazorat qilish siyosatlarini amalga oshirishda qanday cheklovlarga duch kelishlarini ko‘rsatadi. Biroq, raqamli suverenitetni ta’minlash va internetda axborot erkinligini saqlash masalalari, xalqaro hamjamiyat tomonidan birgalikda hal qilinishi kerak bo‘lgan muhim masaladir.

Xalqaro tashkilotlar, xususan, BMT, Xalqaro telekommunikatsiya ittifoqi (ITU) va Yevropa Ittifoqi kabi tashkilotlar, internetni nazorat qilish va senzura qilish masalalariga doir turli yondashuvlarni ishlab chiqmoqdalar. Shu bilan birga, internetning global xarakterini hisobga olgan holda, davlatlar oʻrtasida kelishuvlar va me'yorlar ishlab chiqish, internetni erkin va xavfsiz tutishning asosiy omillaridan biri boʻlishi kerak.

Xulosa qilib aytganda, Internetni nazorat qilish va senzura masalalari, raqamli suverenitet bilan bogʻliq boʻlib, davlatlar oʻrtasidagi ziddiyatlarni kuchaytiradi. Xalqaro huquq doirasida internetni nazorat qilish va senzura qilishni ta'minlash uchun aniq va umumjahon qoidalari zarur. Shu bilan birga, internetning erkinligini saqlash, axborot erkinligi va xavfsizlik oʻrtasida nozik muvozanatni saqlash uchun xalqaro hamkorlik va hamjihatlik zarur boʻladi. Bunday yondashuvlar nafaqat davlatlarning oʻzaro manfaatlarini inobatga olish, balki global raqamli xavfsizlikni ta'minlash uchun ham muhimdir.

Global axborot maydonida siyosiy manfaatlar toʻqnashuvi. Global axborot maydoni, ayniqsa internetning kundan-kunga kengayib borayotgan roli, siyosiy manfaatlar toʻqnashuvi uchun yangi va dolzarb maydon yaratmoqda. Raqamli suverenitet va axborot erkinligi oʻrtasidagi ziddiyatlar, koʻplab davlatlarning axborot siyosatlari va raqamli infratuzilmalarga boʻlgan yondashuvlariga sezilarli ta'sir koʻrsatmoqda. Raqamli suverenitet, bir tomondan, davlatlarning oʻz hududidagi axborot oqimlarini nazorat qilish huquqini anglatadi, ikkinchi tomondan esa, internetning global tabiatini hisobga olgan holda, xalqaro hamkorlikni ta'minlash zaruratini koʻrsatadi.

Siyosiy manfaatlar toʻqnashuvi global axborot maydonida oʻzining ifodasini ayniqsa ikki sohada aniq koʻrsatadi: davlatlar oʻrtasidagi axborot xavfsizligi va raqamli infratuzilma nazorati. Axborot xavfsizligi, milliy suverenitet va milliy xavfsizlikni ta'minlashda davlatlarning turli siyosiy yondashuvlarini yaratadi. Shu bilan birga, davlatlar oʻrtasidagi raqamli infratuzilmaning nazorati va axborot erkinligi oʻrtasidagi kurash, siyosiy manfaatlar toʻqnashuvining markazida turadi. Xalqaro hamjamiyatda kiberxavfsizlik va internetning global tartibi haqida turli siyosiy qarashlar mavjud boʻlib, ular global axborot maydonida yangi ziddiyatlarni keltirib chiqaradi.

Global axborot siyosatidagi davlatlarning yondashuvlari. Har bir davlat oʻzining milliy manfaatlarini saqlash va kuchaytirish uchun axborot oqimlarini nazorat qilishni xohlaydi. Shu sababli, ba'zi davlatlar, masalan,

Xitoy, Rossiya va Turkiya, internetni o‘z hududida to‘liq nazorat qilishni va xususiy ma’lumotlarni filtrlaydi. Xitoyning "Great Firewall" siyosati, Rossiyaning o‘z internet infratuzilmasini kuchaytirishga qaratilgan siyosatlari va boshqa davlatlarning axborot nazorati, raqamli suverenitetni ta’minlashda davlatlar o‘rtasida yanada keskin qarama-qarshiliklarni keltirib chiqaradi. Bu siyosatlar, o‘z navbatida, internetning ochiqligiga va axborot erkinligi prinsiplariga qarshi turadi.

Shuningdek, ba’zi davlatlar global axborot maydonida o‘zlarining siyosiy maqsadlariga erishish uchun axborot manipulyatsiyasi yoki "xibrid urushlar" metodlarini qo‘llashadi. Masalan, davlatlar o‘rtasidagi diplomatik, iqtisodiy va siyosiy ziddiyatlar ko‘pincha raqamli maydonda, xususan, "fake news" (yolg‘on axborot) tarqatish, xakerlik hujumlari, ma’lumotlarni o‘g‘irlash va ommaviy axborot vositalarini manipulyatsiya qilish orqali o‘z ifodasini topadi. Bunday holatlar, o‘z navbatida, axborot erkinligi va suverenitetni ta’minlashdagi muammolarni keltirib chiqaradi.

Global raqamli iqtisodiyot va siyosiy manfaatlar. Global raqamli iqtisodiyotda axborot texnologiyalarining va raqamli infratuzilmalarning roli har qachongidan ko‘ra kattalashmoqda. Axborot texnologiyalari va raqamli tarmoqlar global iqtisodiyotda muhim o‘rin egallaganligi sababli, davlatlar axborot oqimlarini nazorat qilish orqali iqtisodiy raqobatni boshqarishga intilishadi. Masalan, global texnologik gigantlar, ayniqsa, AQShning texnologiya kompaniyalari, boshqa davlatlar uchun iqtisodiy va siyosiy muammolarni keltirib chiqaradi. Bunday kompaniyalar va ularning texnologiyalari, o‘z navbatida, axborot va ma’lumotlarga bo‘lgan global nazoratni kuchaytiradi, bu esa raqamli suverenitetni saqlashni xohlaydigan davlatlar uchun xavf tug‘diradi.

Davlatlar o‘rtasidagi siyosiy manfaatlar to‘qnashuvi nafaqat axborot xavfsizligini, balki iqtisodiy manfaatlarni ham o‘z ichiga oladi. Ba’zi davlatlar o‘z iqtisodiy tizimlarini raqamli texnologiyalar asosida qayta qurishga intilishadi, bu esa raqamli maydondagi suverenitetni mustahkamlashga xizmat qiladi. Shu bilan birga, raqamli iqtisodiyotning global tabiatini hisobga olgan holda, davlatlar o‘rtasida iqtisodiy va siyosiy ziddiyatlar yanada kuchayadi, chunki texnologik yutuqlar va axborot nazorati raqamli raqobatning markazida turadi.

Internetning global tartibi va siyosiy qaramlik. Internetning global xarakteri, davlatlarning o‘z hududlaridagi internetni to‘liq nazorat qilish va

suverenitetni ta’minlashni istashlari bilan qarama-qarshi keladi. Global internet va axborot tarmoqlarining ochiqligi, turli davlatlar o‘rtasida axborot oqimlarining erkinligini ta’minlashni talab qiladi. Biroq, axborot va ma’lumotlarning global almashinuvi, siyosiy qarashlar va milliy manfaatlar o‘rtasidagi to‘qnashuvni keltirib chiqaradi. Xalqaro hamjamiyatda erkin axborot almashinuvi va axborot erkinligi prinsiplariga sodiq qolish zarurati mavjud bo‘lsa-da, davlatlar o‘rtasidagi siyosiy qarashlar va manfaatlar bu prinsiplarni amalga oshirishni qiyinlashtiradi.

Yuqoridagi omillar, global axborot maydonidagi siyosiy manfaatlar to‘qnashuvi, raqamli suverenitetni mustahkamlash va internetning global tartibini yaratishda muhim rol o‘ynaydi. Bunda, bir tomondan, davlatlar o‘z hududida raqamli infratuzilmani nazorat qilishni afzal ko‘rishsa, boshqa tomondan, global axborot erkinligi va ko‘p tomonlama hamkorlikni ta’minlash zarurati muhim hisoblanadi. Shu bois, global axborot maydonida siyosiy manfaatlar to‘qnashuvi kelajakda xalqaro huquq va diplomatik munosabatlarda yangi qiyinchiliklar yaratadi, chunki har bir davlatning raqamli suvereniteti va axborot erkinligini saqlash istagi o‘zaro ziddiyatli bo‘lishi mumkin.

Xulosa qilib aytganda, Global axborot maydonida siyosiy manfaatlar to‘qnashuvi raqamli suverenitetning markaziy masalalaridan biriga aylanmoqda. Davlatlar o‘rtasida internet va axborot oqimlarini nazorat qilishga bo‘lgan turlicha yondashuvlar, xalqaro hamkorlik va axborot erkinligi o‘rtasidagi muvozanatni saqlashda katta muammolarni keltirib chiqaradi. Bu holatda, global axborot maydonida siyosiy manfaatlarning ziddiyatini bartaraf etish uchun xalqaro kelishuvlar va hamkorlikni kuchaytirish zarur.

4.2. Yagona xalqaro normativ hujjat ishlab chiqish ehtiyoji

Kiberjinoyatlar global miqyosda o‘sib borayotgan xavf-xatarlar sifatida, xalqaro huquq va davlatlar o‘rtasidagi hamkorlikni yangi va murakkab bosqichga olib chiqmoqda. Internetning global xarakteri, raqamli infratuzilmaning doimiy rivojlanishi va texnologiyalarning tezkor rivojlanishi, kiberjinoyatlarning oldini olish va ularni jazolash borasidagi mavjud me’yorlarning samaradorligini cheklamoqda. Shu bois, xalqaro miqyosda yagona normativ hujjat ishlab chiqish ehtiyoji tobora oshmoqda.

Kiberjinoyatlar o‘z tabiatiga ko‘ra davlatlararo chegara bilmasdan, har bir mamlakatning ichki huquqiy tizimidan tashqarida yuzaga keladi. Bu esa,

kiberjinoyatlar bilan kurashishda global hamkorlikni ta’minlashni zaruriyatga aylantiradi. Afsuski, hozirgi kunda kiberjinoyatlarga qarshi kurashish uchun xalqaro huquqiy asoslar, norma va mexanizmlar yetarli darajada rivojlanmagan. Kiberjinoyatlar bo‘yicha bir nechta xalqaro hujjatlar mavjud bo‘lsa-da, ularning ko‘plari alohida mamlakatlar yoki mintaqalarga qaratilgan, va ular o‘rtasida yondashuvlar farq qiladi. Masalan, Budapesht Konvensiyasi, 2001-yilda imzolangan bo‘lib, u faqat ma’lum bir mamlakatlar guruhini qamrab oladi va ko‘plab davlatlar tomonidan imzolanmagan.

Xalqaro miqyosda yagona normativ hujjat ishlab chiqish, kiberjinoyatlarga qarshi kurashishning samaradorligini oshirish va har bir davlatning o‘ziga xos yondashuvlarini birlashtirishga xizmat qiladi. Yagona normativ hujjat nafaqat kiberjinoyatlarni ta’riflash, balki ularni jazolash, tergov qilish va sudda qaror chiqarish bo‘yicha bir xil prinsiplarga asoslanish imkonini yaratadi. Bu hujjat, davlatlararo hamkorlikni mustahkamlash va bir-birining yurisdiktsiyalariga qarshi kiberjinoyatlar sodir etilayotganda hamkorlikni tartibga solishga yordam beradi.

Xalqaro huquq doirasida yagona normativ hujjat ishlab chiqish, kiberjinoyatlarning kompleks xususiyatlari, turli yurisdiktsiyalardagi farqliliklar va global xavfsizlik siyosati bilan bog‘liq muammolarni hal qilishda muhim qadam bo‘ladi. Bunday hujjat, kiberjinoyatlar bilan bog‘liq normativ asoslarni birlashtirishi, ularning o‘zaro huquqiy tan olinishini ta’minlash va xalqaro jinoyat huquqini yangilashga xizmat qiladi. Bu esa, o‘z navbatida, kiberjinoyatlarni jinoyat sifatida tan olishda samarali, izchil va adolatli yondashuvni ta’minlashga yordam beradi.

Shu sababli, bugungi kunda kiberjinoyatlarni global miqyosda yagona normativ asosda tartibga solish zarurati bejizga keltirilmagan. Ayni paytda, kiberjinoyatlar bo‘yicha yagona huquqiy asos yaratish uchun xalqaro hamkorlik va diplomatik tashabbuslar ko‘proq ahamiyat kasb etmoqda.

Yagona ta’rif va klassifikatsiya zarurati. Kiberjinoyatlar har tomonlama murakkab va dinamik xususiyatlarga ega bo‘lib, ularning ko‘pligi, turli shakllari va zamonaviy texnologiyalarning tez rivojlanishi ularni to‘g‘ri ta’riflash va klassifikatsiya qilishni juda qiyinlashtiradi. Bugungi kunda kiberjinoyatlarni ta’riflash va tasniflash bo‘yicha xalqaro miqyosda yagona yondashuv yo‘q. Har bir mamlakatning o‘zining huquqiy tizimi, madaniyati va iqtisodiy sharoitlariga ko‘ra, kiberjinoyatlarning o‘ziga xos ta’rifi va tasnifi shakllanadi. Shu sababli, kiberjinoyatlarni yagona ta’rif va klassifikatsiya

asosida tan olish, ularning xalqaro huquqiy doirada to‘g‘ri baholanishi va muvofiqligi uchun zarurdir.

Kiberjinoyatlar: global miqyosda noaniqliklar va farqlar. Afsuski, bugungi kunda ko‘plab mamlakatlarda kiberjinoyatlar faqatgina ba’zi an’anaviy jinoyatlar (masalan, firibgarlik, o‘g‘irlik) yoki axborot xavfsizligiga zarar yetkazish (masalan, zararli dasturlar, tarmoq hujumlari) bilan bog‘liq deb qaraladi. Bunday tasniflar kiberjinoyatlarning o‘ziga xos xususiyatlarini e’tiborga olmagan holda, turli xil huquqiy tizimlarda turli xil yondashuvlarga olib keladi. Masalan, ba’zi davlatlarda kiberjinoyatlarni faqat zararli dasturlarni tarqatish yoki kompyuter tizimlariga noqonuniy kirish sifatida tasniflash mumkin, boshqalari esa bu jinoyatlarni faqat axborot tizimlariga hujum qilish sifatida ko‘radilar. Bunday holat, kiberjinoyatlarni xalqaro miqyosda aniqlash, ularni jinoyat sifatida tan olish va jazolashda katta qiyinchiliklar yaratadi.

Ta’rifning yagona va universal asosga ega bo‘lishi. Kiberjinoyatlar bo‘yicha yagona ta’rifni ishlab chiqish, bu jinoyatlar turli mamlakatlarda qanday tasniflanishini aniq belgilash va ularga qarshi samarali kurashish uchun zarur. Yagona ta’rif, bir tomondan, jinoyatlarni tan olish va jazolashni birlashtirish, boshqa tomondan esa, kiberjinoyatlar haqidagi statistik ma’lumotlarni to‘plash va solishtirishni yengillashtiradi. Ta’rifda kiberjinoyatlarning xususiyatlari aniq belgilab, ularga to‘g‘ri va adolatli huquqiy choralar ko‘rish uchun umumiy me’yorlar yaratiladi.

Shu bilan birga, yagona ta’rif faqatgina terminologik aniqlikni ta’minlab qolmay, balki kiberjinoyatlarning barcha shakllarini va usullarini o‘z ichiga olishga imkon yaratadi. Yagona ta’rif nafaqat mavjud jinoyatlarni, balki yangi turdagi, ilg‘or texnologiyalar bilan amalga oshirilgan jinoyatlarni ham o‘z ichiga oladi. Bu, kiberjinoyatlarni tahlil qilish va ular bilan kurashishda yangi yondashuvlarni ishlab chiqishga imkon beradi.

Klassifikatsiya tizimining ahamiyati. Yagona klassifikatsiya tizimi kiberjinoyatlarni ularning xususiyatlariga qarab aniq guruhlashga imkon beradi. Bu tizim, masalan, zararli dasturlar, xakerlik hujumlari, firibgarlik, o‘g‘irlik, axborotni manipulyatsiya qilish va boshqa ko‘plab jinoyatlarni o‘z ichiga oladi. Klassifikatsiya tizimi kiberjinoyatlarni ularning darajasi va ta’siriga qarab tasniflash imkonini yaratadi. Shuningdek, bu tizim, jinoyatchilarni aniqlash va ularga nisbatan huquqiy choralar ko‘rishda davlatlar o‘rtasida hamkorlikni yanada samarali qilishga yordam beradi.

Xalqaro hamkorlik va yagona normativ hujjat ehtiyoji. Kiberjinoyatlarni yagona ta’rif va klassifikatsiya asosida tan olish, xalqaro miqyosda hamkorlikni mustahkamlashga yordam beradi. Bu esa, o‘z navbatida, kiberjinoyatlarga qarshi kurashish uchun yagona xalqaro normativ hujjat ishlab chiqish ehtiyojini yanada oshiradi. Yagona ta’rif va klassifikatsiya kiberjinoyatlarning xalqaro huquq doirasida birlashtirilishi va kelajakda ularni samarali jazolashni ta’minlash uchun zarurdir. Hozirgi kunda xalqaro huquqiy doirada yagona ta’rif va klassifikatsiya asosida to‘liq normativ tizim ishlab chiqilmaganligi, kiberjinoyatlar bilan bog‘liq huquqiy tartibga solishdagi qator muammolarni keltirib chiqarmoqda.

Shu nuqtai nazardan, yagona ta’rif va klassifikatsiya tizimining ishlab chiqilishi, kiberjinoyatlarga qarshi global kurashni samarali tashkil etish va bu jinoyatlar bilan bog‘liq huquqiy hamkorlikni takomillashtirishda muhim qadam bo‘lib xizmat qiladi. Bu tizimning muvaffaqiyatli ishlashi, kiberjinoyatlarni tan olishda bir xillikni ta’minlash va ularni samarali jazolashning yagona xalqaro asoslarini yaratadi.

Ko‘p tomonlama xalqaro hujjatlar tashabbuslari. Ko‘p tomonlama xalqaro hujjatlar tashabbuslari kiberjinoyatlarga qarshi kurashishda muhim va zarur bosqichlardan biri hisoblanadi. Bugungi kunda kiberjinoyatlarning oldini olish va ularga qarshi kurashishda yagona, universal huquqiy tizimning yetishmasligi kiberxavfsizlik va axborot xavfsizligini ta’minlashda jiddiy to‘siqlarni yuzaga keltiradi. Shunday qilib, ko‘p tomonlama xalqaro hujjatlar tashabbuslari kiberjinoyatlarga qarshi kurashishda eng samarali usul sifatida, barcha mamlakatlarni yagona normativ doirada birlashtirishga imkon beradi.

Birinchi va eng mashhur ko‘p tomonlama xalqaro hujjat, 2001 yilda Yevropada qabul qilingan Budapesht Konvensiyasidir. Ushbu konvensiya kiberjinoyatlar bilan kurashishda ko‘plab mamlakatlar tomonidan qabul qilingan asosiy hujjat bo‘lib, davlatlar o‘rtasidagi hamkorlikni tartibga solish, kiberjinoyatlar sodir etilgan taqdirda jinoyatchilarni jazolashni muvofiqlashtirishga qaratilgan. Budapesht Konvensiyasi, kiberjinoyatlarni tan olish va ularga nisbatan davlatlar o‘rtasida umumiy standartlarni joriy qilish bo‘yicha yirik tashabbusdir. Biroq, bu konvensiya barcha davlatlar tomonidan imzolanmagan va ba’zi davlatlar bu hujjatga qo‘shilmagan. Shu sababli, ko‘p tomonlama yana boshqa tashabbuslarni ishlab chiqish ehtiyoji yuzaga kelmoqda.

Shuningdek, BMTning kiberjinoyatlarga qarshi kurashishda o‘zining rolini oshirishga intilayotgan tashabbuslari ham mavjud. 2018 yilda BMTning Kiberxavfsizlik bo‘yicha xalqaro tuzilmalari tomonidan qabul qilingan "Kiberjinoyatlarni oldini olish bo‘yicha global strategiya" hujjati ham xalqaro miqyosda kiberjinoyatlarni tartibga solishda eng muhim tashabbuslardan biri bo‘ldi. Ushbu hujjat, BMTning barcha a’zo davlatlarini kiberxavfsizlik sohasida o‘zaro hamkorlikni kuchaytirishga va yagona strategiyalarni ishlab chiqishga chaqiradi.

Ko‘p tomonlama tashabbuslar, ayniqsa kiberjinoyatlar bilan kurashishda, davlatlar o‘rtasidagi yondashuvlarni birlashtirish uchun juda muhimdir. Shu bilan birga, hozirgi kunda mavjud ko‘plab xalqaro hujjatlar, asosan, axborot texnologiyalari va kiberjinoyatlar sohasidagi faqat ayrim jihatlarni qamrab oladi. Ushbu holat davlatlar o‘rtasidagi bir xil yondashuvni shakllantirishda muammolarni keltirib chiqaradi. Bundan kelib chiqib, yagona xalqaro normativ hujjat ishlab chiqish va uni barcha davlatlar tomonidan qabul qilish, kiberjinoyatlarni jinoyat sifatida tan olishdagi umumiy yondashuvni ta’minlashga yordam beradi.

Ko‘p tomonlama xalqaro hujjatlar tashabbuslarini muvaffaqiyatli amalga oshirish uchun, barcha mamlakatlar o‘rtasida siyosiy ixtiloflar va iqtisodiy manfaatlar bilan bog‘liq to‘siqlarni yengib o‘tish zarur. Yagona xalqaro huquqiy tizimni yaratish, barcha davlatlar o‘rtasida huquqiy yondashuvlarning izchilligini ta’minlash, hamkorlikni kuchaytirish va samarali kurashish mexanizmlarini joriy etish uchun imkon yaratadi.

Milliy qonunlarning xalqaro huquq bilan uyg‘unligi. Global miqyosda kiberjinoyatlar tobora ko‘proq tarqalib bormoqda, bu esa xalqaro huquqning samarali ishlashini ta’minlash va milliy qonunlar bilan uyg‘unlikni saqlash zaruratini keltirib chiqarmoqda. Kiberjinoyatlar va kiberxavfsizlik sohasidagi normalar va yondashuvlar o‘rtasidagi tafovutlar ko‘p hollarda global hamkorlikni kuchaytirishda va jinoyatlarni jazolashda samarali mexanizmlar yaratishda qiyinchiliklar yuzaga keltiradi. Shu nuqtai nazardan, milliy qonunlarning xalqaro huquq bilan uyg‘unligi bugungi kunda kiberjinoyatlarni bartaraf etish va ularning oldini olishda zaruriy shartdir.

Milliy qonunlar va xalqaro huquqning o‘zaro ta’siri. Xalqaro huquq, davlatlar o‘rtasidagi o‘zaro munosabatlarni tartibga soluvchi normativ tizim bo‘lib, uni tuzish va amal qilishda barcha davlatlarning manfaatlari inobatga olinadi. Kiberjinoyatlar bilan bog‘liq vaziyatlarda, milliy qonunlar va xalqaro

huquq o‘rtasidagi uyg‘unlik davlatlarning kiberjinoyatlarga qarshi kurashishda qanday yondashuvni tanlashiga, axborot xavfsizligini ta’minlashdagi strategiyalarini ishlab chiqishga va kiberjinoyatchilarni javobgarlikka tortishga ta’sir qiladi.

Milliy qonunlar xalqaro huquqdan kelib chiqqan normalar va standartlarga muvofiq ishlab chiqilishi lozim. Agar milliy qonunlar xalqaro huquqga to‘g‘ri kelmasa, bu nafaqat ikki tomonlama muammolarni keltirib chiqaradi, balki davlatlar o‘rtasida jinoyatchilarni ekstraditsiya qilish, tergov o‘tkazish, va kiberjinoyatlar bo‘yicha ma’lumot almashishda jiddiy to‘siqlar yaratadi. Masalan, Budapesht Konvensiyasida kiberjinoyatlar bilan bog‘liq umumiy ta’riflar, jazolar va protseduralar belgilangan bo‘lsa-da, har bir davlat ushbu normativalarni o‘z qonunlariga mos ravishda qabul qilishda farqlanadi, bu esa o‘z navbatida, xalqaro hamkorlikni cheklaydi.

Milliy qonunlarning xalqaro konvensiyalar bilan mosligi. Xalqaro kiberxavfsizlik tizimida davlatlarning milliy qonunlari global me’yorlarga moslashishi va xalqaro huquq bilan uyg‘un bo‘lishi zarur. Milliy qonunlar, xalqaro konvensiyalar va bitimlarga asoslangan holda, kiberjinoyatlarga qarshi kurashishda yagona yondashuvni ta’minlashga xizmat qiladi. Shuningdek, davlatlarning axborot xavfsizligi va kiberjinoyatlar bo‘yicha o‘z qonunlarini xalqaro normativlarga moslashtirish, global xavfsizlikni oshirishda va kiberjinoyatlarga qarshi samarali choralar ko‘rishda muhim omil hisoblanadi.

Budapesht Konvensiyasi o‘zida kiberjinoyatlarga qarshi kurashishning yagona standartlarini ishlab chiqgan bo‘lsa-da, bu normativ hujjat barcha davlatlar tomonidan qabul qilinmagan va har bir davlat o‘z qonunlarini shunga moslashtirishda erkinlikka ega. Bu holat ko‘plab davlatlar o‘rtasida kiberjinoyatlar bilan kurashishdagi farqliliklarni keltirib chiqaradi. Shu sababli, kiberxavfsizlik bo‘yicha normativlar va milliy qonunlarni o‘zaro uyg‘unlashtirish, kiberjinoyatlar sohasidagi xalqaro hamkorlikni kuchaytirish va samarali jazolash mexanizmlarini ta’minlashda muhim rol o‘ynaydi.

Milliy qonunlarning xalqaro hamkorlikka ta’siri. Kiberjinoyatlar global miqyosda keng tarqalgan bo‘lgani sababli, davlatlar o‘rtasida ma’lumot almashish, tergovlar olib borish, va jinoyatchilarni jazolashda xalqaro hamkorlikni amalga oshirish zarurati yuzaga kelmoqda. Milliy qonunlar xalqaro huquq bilan uyg‘un bo‘lishi, bu hamkorlikni soddalashtiradi va davlatlar o‘rtasida to‘siqlarsiz hamkorlik o‘rnatishga imkon beradi. Shu bilan birga, davlatlarning axborot almashish, kiberjinoyatlar bo‘yicha ma’lumotlar

yig‘ish va jinoyatchilarni jazolash jarayonlarida umumiy protseduralarga rioya qilishi, xalqaro huquqning samarali ishlashini ta’minlaydi.

Milliy qonunlar xalqaro me’yorlarga moslashtirilganda, davlatlar o‘rtasida kiberjinoyatlarni tergov qilish va jazolash jarayonlari tezlashadi. Misol uchun, ekstraditsiya so‘rovlarida, ma’lumotlarni yig‘ish va ulashish, bir xil yuridik protseduralarga asoslanib amalga oshirilishi mumkin. Shu bilan birga, davlatlarning kiberjinoyatlarni tergov qilishdagi o‘zaro hamkorlikni kuchaytirish va xatarlarni bartaraf etish bo‘yicha bitta tizimga asoslangan yondashuvni ishlab chiqish zarur.

Milliy qonunlarning global kiberxavfsizlik tizimidagi roli. Kiberjinoyatlar bilan kurashishdagi muvaffaqiyat ko‘p jihatdan davlatlarning milliy qonunlarining samarali va xalqaro huquqga mosligi bilan belgilanadi. Milliy qonunlarni global kiberxavfsizlik tizimiga moslashtirish, kiberjinoyatlarga qarshi kurashishda davlatlar o‘rtasidagi koordinatsiyani kuchaytirishga imkon beradi. Shuningdek, global xavfsizlik tizimining samarali ishlashi uchun milliy qonunlarni xalqaro normativlar bilan moslashtirish va integratsiya qilish zarur.

Kiberjinoyatlarga qarshi kurashishda yagona normativ hujjat ishlab chiqish va milliy qonunlarni xalqaro huquq bilan uyg‘unlashtirish, kiberjinoyatlarning oldini olishda, axborot xavfsizligini ta’minlashda va kiberjinoyatlarni jazolashda davlatlar o‘rtasidagi bir xillikni ta’minlaydi. Bu esa, o‘z navbatida, xalqaro hamkorlikni kuchaytiradi va kiberxavfsizlik sohasidagi o‘zaro ishonchni mustahkamlaydi.

Xulosa qilib aytganda, Milliy qonunlarning xalqaro huquq bilan uyg‘unligi kiberjinoyatlarni bartaraf etishda va ularni jinoyat sifatida tan olishdagi umumiy yondashuvni yaratishda muhim omil hisoblanadi. Bunda xalqaro konvensiyalar va normativ hujjatlar asosida davlatlar o‘rtasida o‘zaro kelishuvlar va hamkorlikni ta’minlash zarur. Milliy qonunlarni xalqaro huquqning umumiy tamoyillariga moslashtirish, kiberjinoyatlarga qarshi kurashishda samarali mexanizmlar yaratish va davlatlar o‘rtasidagi muammolarni bartaraf etishda asosiy vositaga aylanadi.

4.3. Sun’iy intellekt va avtomatlashtirilgan jinoyatlar xavfi

Bugungi kunda texnologiyaning rivojlanishi kiberjinoyatlarning yangi, avvalgidan ancha murakkab shakllarini yaratishga olib kelmoqda. Ayniqsa, sun’iy intellekt (SI) va avtomatlashtirilgan tizimlar kiberjinoyatchilikni yangi

bir bosqichga olib chiqmoqda. Kiberjinoyatlar faqatgina insonlarning bevosita ishtirokini talab qilmasdan, balki avtomatlashtirilgan tizimlar va algoritmlar yordamida amalga oshirilayotgan murakkab huquqbuzarliklarga ham aylanishi mumkin. Shunday qilib, sun’iy intellekt va avtomatlashtirilgan tizimlarning kiberjinoyatlarda qo‘llanilishi huquqiy, axborot xavfsizligi va etik masalalarda yangi chaqiriqlarni keltirib chiqarmoqda.

Sun’iy intellekt va avtomatlashtirishning rivojlanishi kiberjinoyatlarni yanada murakkablashtirmoqda. Masalan, avtomatik tizimlar yordamida noqonuniy ma’lumotlar almashish, kiberxavfsizlikni buzish, bank tizimlarida firibgarliklar va boshqa jinoyatlarni amalga oshirish mumkin. Bunda, sun’iy intellekt algoritmlari o‘z-o‘zini o‘rgatish va insonni aldagan holda huquqbuzarliklar qilishga yordam berishi mumkin. Shu sababli, bu kabi texnologiyalarning kiberjinoyat sohasida paydo bo‘lishi davlatlarning kiberxavfsizlik va huquqni muhofaza qilish tizimlariga yangicha yondashuvni talab qiladi.

Sun’iy intellekt va kiberjinoyatlarning evolyutsiyasi. Sun’iy intellektning kiberjinoyatlarda qo‘llanishi texnologiyaning bir qismi sifatida yanada kengayib bormoqda. Boshqacha aytganda, sun’iy intellekt tizimlari, o‘z-o‘zini rivojlantiruvchi algoritmlar orqali, kiberjinoyatlar uchun yangi imkoniyatlar yaratmoqda. Avtomatlashtirilgan tizimlar yordamida, masalan, firibgarlik, hakerlik hujumlari, maxfiy ma’lumotlarga noqonuniy kirish va boshqa jinoyatlar tezkor va samarali tarzda amalga oshirilishi mumkin. Bu jarayonlar esa davlatlar o‘rtasidagi hamkorlik va kiberxavfsizlikni ta’minlashda yangi muammolarni keltirib chiqaradi.

Avtomatlashtirilgan jinoyatlar: xavf va tahdidlar. Avtomatlashtirilgan jinoyatlar - bu inson qatnashmasdan faqatgina algoritmlar va avtomatlashtirilgan tizimlar yordamida amalga oshiriladigan huquqbuzarliklardir. Ushbu jinoyatlar, odatda, ma’lumotlar bazalariga noqonuniy kirish, shaxsiy ma’lumotlarni o‘g‘irlash, tarmoq orqali firibgarliklar qilish kabi amallarni o‘z ichiga oladi. Sun’iy intellekt va avtomatlashtirilgan tizimlarning rivojlanishi natijasida, kiberjinoyatlar yanada tezkor, samarali va ko‘proq miqyosda sodir bo‘lishi mumkin.

Misol uchun, sun’iy intellekt yordamida amalga oshiriladigan phishing hujumlari yanada murakkablashadi. Bu hujumlar avvalgi xakerlik usullariga qaraganda yanada yaxshilangan va avtomatlashtirilgan bo‘ladi. Sun’iy intellekt tizimlari yordamida, kiberjinoyatchilar tezda ko‘plab odamlarni

aldaydi va shaxsiy ma’lumotlarni o‘g‘irlaydi, buning natijasida katta moliyaviy zararlar keltiriladi. Shuningdek, sun’iy intellektni ishlatgan holda kiberxavfsizlik tizimlarini, masalan, tarmoq himoyasi yoki foydalanuvchi identifikatsiyasi tizimlarini aldaydigan yangi avlod dasturlar yaratilishi mumkin.

Huquqiy muammolar va normativ tartibga solish. Sun’iy intellekt va avtomatlashtirilgan tizimlarning kiberjinoyatlar sohasidagi qo‘llanilishi, birinchi navbatda, huquqiy tartibga solishning samaradorligini ta’minlashni talab qiladi. Avtomatlashtirilgan tizimlar yordamida amalga oshiriladigan jinoyatlar odamning bevosita ishtirokini talab etmaganligi sababli, mavjud huquqiy tizimlar ko‘pincha bu kabi jinoyatlar uchun samarali jazolarni ta’minlashda qiyinchiliklarga duch keladi. Shuningdek, sun’iy intellekt yordamida amalga oshirilgan jinoyatlar uchun javobgarlikni belgilash, kim javobgar ekanligini aniqlash va bu kabi jinoyatlarga nisbatan huquqiy mexanizmlar ishlab chiqish muhim ahamiyatga ega.

Bugungi kunda sun’iy intellektni jinoyatga jalb qilish yoki uni jinoyat sifatida e’tirof etish masalasi har bir mamlakatning ichki qonunchiligiga va xalqaro huquq tamoyillariga ta’sir ko‘rsatmoqda. Shuning uchun xalqaro normativ hujjatlar va milliy qonunlarni ishlab chiqishda sun’iy intellekt va avtomatlashtirilgan tizimlar asosida kiberjinoyatlar uchun yangi qoidalar va yondashuvlarni ishlab chiqish zarur.

Xulosa qilib aytganda, Sun’iy intellekt va avtomatlashtirilgan tizimlarning kiberjinoyatlarda qo‘llanilishi global kiberxavfsizlik va huquqni muhofaza qilish tizimlariga yangi chaqiriqlarni keltirib chiqarmoqda. Ushbu texnologiyalar orqali jinoyatlar yanada murakkablashadi va ularga qarshi kurashishda yangi yondashuvlarni talab qiladi. Shu sababli, sun’iy intellekt va avtomatlashtirilgan tizimlar bilan bog‘liq kiberjinoyatlarga nisbatan huquqiy normativlarni ishlab chiqish va joriy qilish, kiberxavfsizlikni ta’minlashda muhim omilga aylanadi. Shuningdek, xalqaro hamkorlik, axborot almashish va huquqiy mexanizmlar orqali bunday jinoyatlarga qarshi samarali choralar ko‘rish zarurati kuchaymoqda.

AI yordamida sodir etilayotgan kiberjinoyatlar. Sun’iy intellekt (AI) va avtomatlashtirilgan tizimlarning rivojlanishi kiberjinoyatchilikni yangi va yanada murakkab shakllarga olib kelmoqda. AI texnologiyalarining kiberjinoyatlarda qo‘llanilishi avvalgi jinoyat usullariga nisbatan o‘zgacha xavf-xatarlar yaratmoqda. Ushbu texnologiyalar nafaqat jinoyatlarni yanada

tezkor va samarali qilish imkonini beradi, balki jinoyatlarni amalga oshirishda inson aralashuvini minimallashtiradi. Bu esa o‘z navbatida, huquqni muhofaza qilish tizimlarini yangi chaqiriqlarga duchor qiladi va kiberjinoyatchilikni nazorat qilishni murakkablashtiradi.

Sun’iy intellektning kiberjinoyatlarda qo‘llanilishi. AI texnologiyalari yordamida amalga oshiriladigan kiberjinoyatlar odatda ikki asosiy yo‘nalishda sodir etiladi: avtomatlashtirilgan hujumlar va sun’iy intellektga asoslangan firibgarliklar. Avtomatlashtirilgan hujumlar ko‘plab kompyuter tizimlarini bir vaqtning o‘zida maqsad qilib, kiberhujumlarni amalga oshirishga imkon yaratadi. AI texnologiyalari yordamida jinoiy xatti-harakatlar murakkablashib, yanada tezkor va samarali bo‘lib, ularni aniqlash va oldini olishni qiyinlashtiradi.

Misollar:

- **Phishing hujumlari:** Sun’iy intellekt yordamida kiberjinoyatchilar o‘zlarini ishonchli manba sifatida taqdim etib, foydalanuvchilarning shaxsiy ma’lumotlarini o‘g‘irlaydigan murakkab phishing hujumlarini amalga oshirishi mumkin. AI tizimlari xatolarni minimallashtirishi va maqsadli foydalanuvchi guruhlarini aniqlashda katta yordam beradi, shu bilan birga, hakerlar foydalanuvchilarning onlayn xatti-harakatlarini o‘rganib, ularning xohish-istaklarini tushunish va optimallashtirishga imkon yaratadi.
- **Automated Malware (zararli dasturlar):** Sun’iy intellekt yordamida zararlangan tizimlar o‘z-o‘zidan tarqalishi yoki odam aralashuvisiz yangi zararlangan tizimlarni topishi mumkin. AI tizimlari yangi xatarlarni aniqlash va yangi zararli dasturlarni yaratishda juda samarali. Avtomatik ravishda o‘zini o‘zgartiradigan yoki yangilaydigan zararlovchi dasturlar sun’iy intellekt yordamida yaratilib, kiberhujumlarni yanada samarali va xavfli qilishga olib keladi.

Sun’iy intellekt yordamida amalga oshiriladigan firibgarliklar. Sun’iy intellekt yordamida amalga oshiriladigan firibgarliklar, odatda, raqamli tizimlarni buzish va moliyaviy zararlarni keltirib chiqarish maqsadida sodir etiladi. AI tizimlari yordamida amalga oshiriladigan firibgarliklar nafaqat tez-tez amalga oshiriladi, balki ular ancha murakkab va tasodifiy elementlarni o‘z ichiga oladi. Sun’iy intellekt, shuningdek, huquqni muhofaza qiluvchi organlar tomonidan aniqlanishi va tekshirilishi qiyin bo‘lgan yangi turdagi jinoyatlarni yaratadi.

Misollar:

- **Foydalanuvchi profilingi va manipulyatsiya:** AI tizimlari yordamida kiberjinoyatchilar ijtimoiy tarmoqlar va boshqa onlayn platformalardan foydalanuvchilarning shaxsiy ma’lumotlarini yig‘ib, ularni aldagan holda manipulyatsiya qilishlari mumkin. Sun’iy intellekt, foydalanuvchilarning odatlari, xatti-harakatlari va afzalliklarini tahlil qilish orqali, ularga qarshi hujumlar rejalashtirishi mumkin. Bu jarayon nafaqat foydalanuvchilarga, balki keng miqyosda axborot xavfsizligiga ham tahdid soladi.
- **Qaror qabul qilish tizimlariga ta’sir qilish:** AI yordamida qaror qabul qilish tizimlari (masalan, kredit kartalari, sug‘urta kompaniyalarining qaror qabul qilish tizimlari)ni aldagan holda moliyaviy firibgarliklar amalga oshirilishi mumkin. Kiberjinoyatchilar sun’iy intellektni o‘z foydasiga ishlatib, tizimning ishonchli faoliyatini buzib, firibgarliklarni amalga oshirishi mumkin.

Sun’iy intellekt yordamida zararli amallarni avtomatlashtirish. AI tizimlari nafaqat jinoyatlarni amalga oshirishni osonlashtiradi, balki bu jarayonni avtomatlashtiradi. Hozirgi kunda zararli dasturlar va hakerlik hujumlarini avtomatlashtirish uchun sun’iy intellektdan foydalanish avvalgi hujum usullariga nisbatan yanada yuqori samaradorlikka erishish imkonini yaratadi. Bu, o‘z navbatida, kiberjinoyatchilar uchun yangi imkoniyatlarni ochadi.

Misollar:

- **Botnet’lar yordamida hujumlar:** Sun’iy intellekt yordamida avtomatik ravishda hujumlar tashkil qiluvchi botnet’lar yaratilishi mumkin. Bu tizimlar internet orqali butun dunyodagi bir qator tizimlarni boshqarib, maqsadli serverlar yoki tizimlarga to‘sqinlik qiladi yoki ularga zarar yetkazadi. AI yordamida bu botnet’lar o‘z-o‘zini yangilaydi va o‘zgartiradi, bu esa ularni aniqlashni qiyinlashtiradi.
- **Avtomatlashtirilgan tarmoq hujumlari:** AI yordamida kiberjinoyatchilar, avvalgi xatolardan o‘rganib, tarmoq tizimlariga hujum qilishni avtomatlashtirishi mumkin. Bu tizimlar o‘z-o‘zini optimallashtirib, qaysi tizimlar eng zaif ekanligini aniqlab, ularga hujum qilishga imkon yaratadi. Bu jarayon kiberhujumchilarning samaradorligini oshiradi va huquqni muhofaza qiluvchi organlarga bunday hujumlarni aniqlashni yanada qiyinlashtiradi.

Huquqiy muammolar va xavf-xatarlarni boshqarish. Sun’iy intellekt yordamida amalga oshirilayotgan kiberjinoyatlar nafaqat texnologik, balki huquqiy masalalarni ham keltirib chiqaradi. Bunday jinoyatlarni aniqlash va ularni oldini olish uchun, avvalo, AI tizimlari va avtomatlashtirilgan tizimlarning huquqiy maqomini belgilash zarur. AI tizimlarini jinoyatga jalb qilish, mas’uliyatni aniqlash va bu kabi jinoyatlarni ta’qib qilish uchun yangi normativ va qonuniy asoslar yaratish talab etiladi. Xalqaro hamkorlik va davlatlarning kiberxavfsizlik sohasidagi qonunlarni birlashtirish muhim ahamiyatga ega.

Xulosa qilib aytganda, AI yordamida sodir etilayotgan kiberjinoyatlar texnologiyaning rivojlanishi bilan parallel ravishda yanada kengaymoqda. Sun’iy intellektning kiberjinoyatchilikka qo‘llanilishi murakkablikni, samaradorlikni va xavfni oshiradi. Shuning uchun, bu turdagi jinoyatlarga qarshi kurashishda yangicha yondashuvlar va texnologik, huquqiy, axborot xavfsizligi choralarini ishlab chiqish zarur. Kiberxavfsizlikni ta’minlash va sun’iy intellektga asoslangan jinoyatlarni oldini olishda xalqaro hamkorlik, normativ hujjatlarni ishlab chiqish va texnologik yangilanishlar muhim rol o‘ynaydi.

Mas’uliyatni aniqlashdagi murakkablik. Sun’iy intellekt (SI) va avtomatlashtirilgan tizimlarning kiberjinoyatlarda qo‘llanilishi yangi huquqiy, axborot xavfsizligi va etik masalalarni keltirib chiqarmoqda. Ushbu texnologiyalar yordamida sodir etilgan jinoyatlar uchun mas’uliyatni aniqlashda bir qator murakkabliklar paydo bo‘ladi. Odatda, jinoyatlar sodir etilganida, javobgarlik insonlarga yuklanadi, lekin sun’iy intellekt va avtomatlashtirilgan tizimlar orqali amalga oshirilgan jinoyatlar holatida mas’uliyatni aniqlashda aniq qonuniy me’yorlar va amaliyotlar mavjud emas. Bu esa, kiberjinoyatlarni ta’qib qilish va oldini olishda samaradorlikni pasaytiradi.

Sun’iy intellektning o‘z-o‘zini rivojlantirishi va insonning rolini aniqlash. Sun’iy intellekt tizimlari har o‘z-o‘zini rivojlantirish va o‘rganish jarayoniga asoslangan. Ular dasturlangan algoritmlar yordamida ma’lum bir maqsadga erishish uchun o‘z-o‘zini takomillashtirish va yangi xatti-harakatlarni yaratish qobiliyatiga ega. Bunday tizimlar insonning bevosita aralashuvi yoki boshqaruvi bo‘lmagan holda ishlashi mumkin. Natijada, sun’iy intellekt tomonidan sodir etilgan jinoyatlar holatida, kimning javobgar ekanligini aniqlashda katta qiyinchiliklar yuzaga keladi.

Masalan, agar biror jinoyat sodir etilsa, va bu jinoyatning amalga oshirilishida sun’iy intellekt tizimi asosiy rol o‘ynagan bo‘lsa, lekin insonning aralashuvi bo‘lmagan bo‘lsa, bu holatda jinoyat uchun kim javobgar bo‘lishi kerakligi masalasi hal etilishi lozim. Agar sun’iy intellektning qarorlari va xatti-harakatlari natijasida jinoyat sodir bo‘lsa, tizimning yaratuvchisi yoki ishlovchisi javobgar bo‘lishi kerakmi, yoki tizimni ishlab chiqishda ishtirok etgan jismoniy yoki yuridik shaxslar javobgar bo‘ladi?

Avtomatlashtirilgan tizimlar va ularning kiberjinoyatdagi roli. Avtomatlashtirilgan tizimlar yordamida jinoyatlar amalga oshirilishi mumkin bo‘lsa-da, bu tizimlar faqat dasturlangan algoritmlar va kodga asoslanadi. Avtomatlashtirilgan tizimlarning barcha harakatlari inson tomonidan dasturlangan bo‘lib, bu tizimlar insonning bevosita aralashuvisiz ishlaydi. Agar avtomatlashtirilgan tizim orqali kiberjinoyat sodir etilsa, mas’uliyatni aniqlashda murakkabliklar yuzaga keladi. Ushbu holatda, mas’uliyat tizimni ishlab chiqqan dasturchilarga, tizimni o‘rnatgan tashkilotga yoki tizimni boshqarish bo‘yicha mas’ul bo‘lgan shaxslarga yuklanishi kerakmi?

Misollar:

- **Avtomatlashtirilgan botnet hujumlari:** Agar avtomatik ravishda bir nechta botlar orqali biror tarmoqka hujum qilinsa, bu holda botlar o‘z-o‘zidan zarar yetkazish imkoniga ega bo‘ladi. Bu yerda kiberjinoyatchilikni sodir etgan dasturchi yoki tizim yaratuvchisi javobgar bo‘lishi mumkinmi, yoki hujumni amalga oshirgan har bir botning ishlashiga mas’ul bo‘lgan shaxs yoki tashkilot javobgar bo‘lishi kerakmi?
- **Zararlangan tizimlar orqali firibgarlik:** Sun’iy intellekt yordamida zararli tizimlar yaratish va ularni avtomatlashtirish orqali firibgarlik amalga oshirilishi mumkin. Agar avtomatlashtirilgan tizim tomonidan firibgarlik amalga oshirilsa, mas’uliyatni kiberjinoyatchilarga yoki tizimlarni ishlab chiqqan va ularni tasdiqlagan shaxslarga belgilashda huquqiy asoslar yetishmasligi muammosi kelib chiqadi.

Normativ hujjatlarda bo‘shliq va ular o‘rtasidagi tafovut. Sun’iy intellekt va avtomatlashtirilgan tizimlarning jinoyatlar sohasidagi mas’uliyatini aniqlashda, amaldagi xalqaro huquqiy normativ hujjatlar ko‘pincha yetarli emas. Xalqaro huquq, ko‘plab holatlarda, jinoyatni sodir etgan aniq shaxslarni aniqlashda keng imkoniyatlarga ega bo‘lmaydi. Ko‘plab davlatlar o‘z ichki qonunlarida kiberjinoyatlar bilan bog‘liq aniq mas’uliyatni belgilashda muayyan huquqiy bo‘shliqlarni qoldirgan. Bu, ayniqsa, sun’iy

intellekt tizimlari yoki avtomatlashtirilgan qurilmalar orqali amalga oshirilgan jinoyatlar holatida aniq koʻrsatmalarni taqdim etmaydi.

Shuningdek, xalqaro qonunchilik tizimlari, masalan, **Budapesht konvensiyasi** kabi normativ hujjatlar ham bu kabi yangi xavf-xatarlarni qamrab olishda yetarlicha moslashmagan. Ushbu konvensiya kiberjinoyatlarning umumiy shakllarini taʼriflagan boʻlsa-da, sunʼiy intellekt va avtomatlashtirilgan tizimlarning kiberjinoyatlardagi roli haqida aniq meʼyorlar koʻrsatilmagan. Shu bilan birga, sunʼiy intellekt tizimlarining kiberjinoyatchilikda qanday rol oʻynashini va masʼuliyatni kimga yuklashni belgilash uchun xalqaro normativ meʼyorlarni yangilash zarurati mavjud.

Sunʼiy intellekt va avtomatlashtirilgan jinoyatlar uchun masʼuliyatni aniqlashdagi amaliy qiyinchiliklar. Jinoyatlarni aniqlashda sunʼiy intellekt va avtomatlashtirilgan tizimlarning yordamida amalga oshirilgan jinoyatlarning aniqlanishi, koʻpincha, anʼanaviy usullar bilan taqqoslaganda murakkabroq boʻladi. Sunʼiy intellekt tizimlari odatda oʻz qarorlarini mustaqil ravishda qabul qiladi va ularga insonning bevosita aralashuvi minimaldir. Bu holatlarda jinoyatning sodir boʻlganligini aniqlash va uni huquqiy meʼyorlar doirasida tahlil qilish, masʼuliyatni aniqlashni qiyinlashtiradi. Dastur yaratuvchisi, tizim ishlab chiqaruvchisi yoki boshqaruv tizimi masʼuliyatini belgilash uchun mavjud qonuniy mexanizmlar yetersiz boʻlib qolmoqda.

Bundan tashqari, masʼuliyatni aniqlashda, jinoyatni sodir etgan "shaxs" yoki "subyekt"ni aniqlash ham yangi muammolarni keltirib chiqaradi. Kiberjinoyatlar, odatda, virtual muhitda amalga oshiriladi, bu esa jinoyatchini aniq aniqlashni yanada qiyinlashtiradi. Sunʼiy intellektning oʻz-oʻzini oʻrgatish qobiliyati va uning ish faoliyati insondan mustaqil tarzda amalga oshirilayotganligi sababli, masʼuliyatni kimga yuklashni aniqlashda aniq bir qonuniy yondashuvni ishlab chiqish zarurati yuzaga keladi.

Xulosa qilib aytganda, Sunʼiy intellekt va avtomatlashtirilgan tizimlarning kiberjinoyatlarda qoʻllanilishi masʼuliyatni aniqlashda yangi huquqiy qiyinchiliklarni keltirib chiqaradi. Bu tizimlar oʻz-oʻzini rivojlantirganligi sababli, jinoyatlarni sodir etgan shaxslarni aniqlashda aniq qonuniy asoslar mavjud emas. Shu sababli, sunʼiy intellekt va avtomatlashtirilgan tizimlar orqali sodir etilgan jinoyatlar uchun masʼuliyatni aniqlashda xalqaro va milliy qonunchilikni yangilash zarur. Bu masʼuliyatni aniqlashda zamonaviy texnologiyalarni hisobga olgan holda yangi

yondashuvlarni ishlab chiqish, axborot xavfsizligini ta’minlash va kiberjinoyatchilikka qarshi samarali kurashishni ta’minlash uchun muhimdir.

AI texnologiyalari uchun nazorat mexanizmlari. Sun’iy intellekt (SI) texnologiyalari kiberjinoyatlar sohasida yangi xavf-xatarlar yaratish bilan birga, ularni oldini olish va nazorat qilish uchun samarali mexanizmlar ishlab chiqish zaruratini taqdim etadi. AI texnologiyalarining rivojlanishi va ularning avtomatlashtirilgan tizimlar yordamida keng qo‘llanilishi, yasalgan tizimlarning mustaqil va ba’zida kutilmagan xatti-harakatlar qilishiga olib keladi. Bu esa, nafaqat texnologiyalarning huquqiy, balki etik masalalarga ham doir muammolarni keltirib chiqaradi. Bunday tizimlar orqali amalga oshirilgan jinoyatlarni oldini olish va ularni nazorat qilish uchun aniq, mustahkam va global miqyosda amal qiluvchi nazorat mexanizmlarini ishlab chiqish zarur.

Sun’iy intellekt texnologiyalarining rivojlanishi va xavflar. Sun’iy intellekt texnologiyalarining kundan-kunga rivojlanishi, ular orqali sodir bo‘lishi mumkin bo‘lgan jinoyatlar sonini oshirishga olib kelmoqda. AI tizimlari, masalan, o‘z-o‘zini o‘rganish algoritmlaridan foydalanib, kutilmagan va noaniq xatti-harakatlar qilishlari mumkin. Ushbu tizimlar ba’zida ma’lum bir maqsadga erishish uchun inson istagi va axborot xavfsizligi mezonlariga qarshi harakat qilishi mumkin. AI texnologiyalarining kiberjinoyatlar sohasida qo‘llanilishi, ularning manipulyatsiyasi va avtonom xatti-harakatlari natijasida xatarlilikka olib kelishi mumkin. Shuning uchun, sun’iy intellekt texnologiyalarini joriy etishdan oldin, ular uchun kuchli nazorat mexanizmlarini ishlab chiqish zarurati seziladi.

AI texnologiyalariga nisbatan nazorat mexanizmlarining zarurati. AI texnologiyalarining rivojlanishi bilan bog‘liq birinchi muammo – bu tizimlarning insondan mustaqil ishlash qobiliyati va uning kutilmagan natijalari. Bunday texnologiyalarni nazorat qilish uchun bir nechta asosiy mexanizmlar zarur:

a) Axborot xavfsizligi va qonuniy me’yorlar. AI texnologiyalarining ishlashiga ta’sir etuvchi qonuniy me’yorlarni ishlab chiqish zarurati mavjud. Shu bilan birga, sun’iy intellektning faoliyatini boshqaruvchi xalqaro huquqiy asoslar ham ishlab chiqilishi kerak. Bunday mexanizmlar axborot xavfsizligini ta’minlash va kiberjinoyatlar oldini olishga yordam beradi. Qonunchilik, sun’iy intellekt tizimlarining qanday ishlashini va ular orqali sodir etilgan jinoyatlar uchun javobgarlikni aniqlashni belgilashga qaratilgan bo‘lishi lozim.

Misol tariqasida, **Avropa Ittifoqining GDPR (General Data Protection Regulation)** qonuni, ma’lumotlarni himoya qilish sohasida ko‘rsatilgan qat’iy qonuniy talablar, shuningdek, sun’iy intellektga oid qonunlar ishlab chiqilishini ko‘rsatadi. Bu kabi qonunlar, sun’iy intellekt tizimlarining o‘zgarishini va ularning kiberjinoyatlarga aloqasini nazorat qilishda asos bo‘lishi mumkin.

b) Shaffoflik va auditi. Sun’iy intellekt tizimlarining ishlash jarayonida shaffoflik va audit mexanizmlari muhim ahamiyatga ega. AI tizimlarining qanday ishlashini va ulardan qaysi maqsadlarda foydalanilishini tushunish uchun tizimlarning ochiqligi zarur. Tizimlar ishlayotgan algoritmlarning to‘liq tekshiruvidan o‘tkazilishi, foydalanuvchilar va davlat organlari uchun tizimlarni tahlil qilish imkoniyatini yaratadi.

AI tizimlarini ishlab chiqqan tashkilotlar tomonidan amalga oshirilgan audit va baholash jarayonlari orqali, tizimlar o‘rganilishi va huquqiy nuqtai nazardan xavfli xatti-harakatlar va kiberjinoyatlarga olib kelishi mumkin bo‘lgan xatoliklar aniqlanishi mumkin. Audit jarayonlari, sun’iy intellekt tizimlarining qonunlarga mosligini ta’minlash, ular orqali sodir etilgan jinoyatlar uchun javobgarlikni aniqlashda yordam beradi.

c) AI tizimlarini nazorat qilish uchun mustahkam xususiy sektor va davlat hamkorligi. Sun’iy intellekt tizimlarini nazorat qilish uchun xususiy sektor va davlat organlari o‘rtasida hamkorlik zarur. Xususiy sektor tomonidan ishlab chiqilgan tizimlar va davlat tomonidan taqdim etiladigan xavfsizlik standartlari o‘rtasidagi hamkorlik sun’iy intellektni boshqarishda samarali mexanizm yaratadi. Ayniqsa, global miqyosda, mamlakatlar o‘rtasidagi qonunchilikni uyg‘unlashtirish va bir-birini to‘ldiruvchi xavfsizlik mexanizmlarini yaratish juda muhimdir.

d) Sun’iy intellektning etik masalalari va ijtimoiy javobgarlik. Sun’iy intellekt tizimlari, shuningdek, etik masalalarni keltirib chiqaradi. Tizimlarning insonlar va jamiyatga qanday ta’sir qilishi va ular qanday ijtimoiy mas’uliyatni yuklashi kerakligini aniq belgilash zarur. AI tizimlari avtomatlashtirilgan qarorlar qabul qilishda inson aralashuvi minimal bo‘lgan holatlarda, tizimlar orqali amalga oshirilgan qarorlarning etikasini baholash masalasi murakkablashadi. Shu sababli, har bir AI tizimi uchun etik kodekslar va standartlar ishlab chiqilishi lozim.

Sun’iy intellekt tizimlari uchun global miqyosda nazorat mexanizmlarining integratsiyasi. Sun’iy intellekt texnologiyalarining global

miqyosda keng tarqalishi, ularning xalqaro darajada nazorat qilinishi kerakligini ko‘rsatadi. Shu nuqtai nazardan, xalqaro tashkilotlar, jumladan, **BMT**, **Evropa Ittifoqi** va boshqa global hamkorlik institutlari tomonidan sun’iy intellekt texnologiyalariga oid umumiy xavfsizlik va nazorat standartlari ishlab chiqilishi zarur.

Yangi texnologiyalarni va sun’iy intellektni boshqarishda xalqaro kelishuvlar, nazorat qilish va xavfsizlikni ta’minlash uchun yagona integratsiyalashgan tizimlarni yaratish zarur. Bunday tizimlar global miqyosda AI tizimlarining xavf-xatarlarini minimallashtirishga, kiberjinoyatlarning oldini olishga va foydalanuvchilarning huquqlarini himoya qilishga qaratilgan bo‘lishi kerak.

Xulosa qilib aytganda, Sun’iy intellekt texnologiyalarining kiberjinoyatlarda qo‘llanilishi va ularga qarshi samarali kurashish uchun kuchli nazorat mexanizmlari zarur. Buning uchun, sun’iy intellekt tizimlarining xavfsiz ishlashini ta’minlash, etik nuqtai nazardan mas’uliyatni aniqlash va texnologiyalarni boshqarishning xalqaro va milliy darajadagi standartlarini ishlab chiqish lozim. Xususiy sektor va davlat organlari o‘rtasidagi hamkorlik, audit, shaffoflik, etik kodekslar va global miqyosdagi integratsiyalashgan tizimlar sun’iy intellekt texnologiyalarining xavf-xatarlarini nazorat qilish va kiberjinoyatlar oldini olishda muhim omil bo‘ladi.

4.4. Inson huquqlari va axborot xavfsizligi muvozanati

Inson huquqlari va axborot xavfsizligi o‘rtasidagi muvozanatni ta’minlash bugungi kunda xalqaro huquq va davlatlar siyosatida eng dolzarb masalalardan biriga aylangan. XXI asrning axborot texnologiyalari davrida, kiberjinoyatlar va raqamli tahdidlar doimo yangi xavflarni keltirib chiqarmoqda. Shu bilan birga, bu texnologiyalarning huquqiy va etik ta’sirini baholash, ayniqsa, inson huquqlarini himoya qilish va axborot xavfsizligini ta’minlashda paydo bo‘layotgan masalalarni hal qilish juda muhimdir.

Kiberxavfsizlik va axborot xavfsizligi sohasida davlatlarning o‘zaro hamkorligi ortib borayotgan bir vaqtda, inson huquqlari hamon ajralmas prinsip sifatida e’tiborda qoladi. Insonlarning shaxsiy hayotini himoya qilish, so‘z erkinligi, ma’lumotlarni himoya qilish, xususiy hayotni buzmasdan davlat xavfsizligini ta’minlash kabi muhim masalalar kiberxavfsizlikni ta’minlash jarayonida alohida o‘ringa ega. Biroq, ba’zida bu ikki soha o‘rtasidagi muvozanatni topish murakkablashadi, chunki axborot xavfsizligini ta’minlash

va kiberjinoyatlar bilan kurashishda amalga oshirilgan choralar inson huquqlarini cheklashga olib kelishi mumkin.

Inson huquqlarining muhofazasi va kiberjinoyatlar. Inson huquqlari, ayniqsa, so‘z erkinligi, shaxsiy hayotni himoya qilish, va ma’lumotlarning xavfsizligi kiberxavfsizlikni ta’minlashda markaziy o‘ringa ega bo‘lib, global miqyosda ijtimoiy, siyosiy va iqtisodiy jarayonlarga ta’sir ko‘rsatadi. Biroq, kiberjinoyatlar va axborot tahdidlari, ayniqsa davlatlar o‘rtasidagi onlayn xatarlar kuchaygan sari, ushbu huquqlarni himoya qilishni yanada qiyinlashtirmoqda. Kiberjinoyatchilikning o‘ziga xos xususiyatlari, global miqyosda tezkor va anonim tarzda amalga oshirilishi, shuningdek, shaxsiy ma’lumotlarga zarar yetkazishi yoki ularni o‘g‘irlash orqali insonlarning huquqlarini buzishi mumkin. Shu sababli, kiberjinoyatlarga qarshi kurashishda davlatlar o‘rtasida mavjud hamkorlik va milliy huquqiy tizimlar ko‘plab murakkab huquqiy, axborot xavfsizligi va etik masalalarni hal qilishga majbur qilmoqda.

Axborot xavfsizligi va davlat xavfsizligi masalalari. Davlatlarning axborot xavfsizligini ta’minlash zarurati jahonning ko‘plab mintaqalarida o‘sib bormoqda. Kiberterrorizm, ma’lumotlar buzilishi, yoki davlat rahbarlarini nishonga olgan kiberhujumlar kabi tahdidlar davlat xavfsizligini ta’minlashdagi asosiy masalalarga aylanmoqda. Shuningdek, davlatlar o‘rtasida raqamli chegaralar, internetda erkinlik va ma’lumotlarni saqlashga oid nizolar ham kiberxavfsizlikni mustahkamlash uchun zarur bo‘lgan normativ hujjatlarni ishlab chiqishni talab qilmoqda. Shu bilan birga, davlatlar o‘z xalqining xavfsizligini ta’minlashda axborot nazoratini joriy etish va kiberjinoyatlarni tergov qilishda xalqaro huquqni inobatga olgan holda operatsiyalarni amalga oshiradi.

Biroq, axborot xavfsizligini ta’minlashda davlatlarning kuch ishlatishi ba’zan inson huquqlarining buzilishiga olib keladi. Masalan, internetni kuzatish yoki foydalanuvchilar faoliyatini monitoring qilish, ba’zi hollarda shaxsiy hayotni himoya qilish huquqiga zid bo‘lishi mumkin. Shu sababli, davlatlar axborot xavfsizligini ta’minlashda huquqiy nazoratni amalga oshirishda tenglik, adolat va shaffoflikni ta’minlashga harakat qilishi lozim.

Inson huquqlari va axborot xavfsizligi o‘rtasidagi muvozanat. Inson huquqlari va axborot xavfsizligi o‘rtasidagi muvozanatni ta’minlashda, bir tomondan, kiberjinoyatlarga qarshi kurashish va davlat xavfsizligini ta’minlash uchun zarur choralar ko‘rilsa, boshqa tomondan, shaxsiy

ma’lumotlarning maxfiyligi, so‘z erkinligi, axborot olish erkinligi kabi huquqlarni himoya qilish zarur. Buning uchun xalqaro huquq va milliy qonunchilik tizimlarida quyidagi muhim tamoyillarni inobatga olish kerak:

- ✓ **Proportsionallik tamoyili** – axborot xavfsizligini ta’minlash uchun amalga oshirilgan choralarning inson huquqlariga zarar yetkazmasligini ta’minlash lozim. Har bir chorani amalga oshirishda uning zarar va foydasi to‘liq tahlil qilinishi kerak.
- ✓ **Shaffoflik** – kiberxavfsizlikni ta’minlash uchun amalga oshirilayotgan davlatning harakatlari va qonunlar shaffof bo‘lishi kerak. Insonlarning o‘z huquqlari to‘g‘risida to‘liq ma’lumotga ega bo‘lishi va davlat organlari tomonidan amalga oshirilgan harakatlarning me’yorlariga rioya qilinishi kerak.
- ✓ **Tenglik va adolat** – kiberjinoyatlarga qarshi kurashishda inson huquqlarini himoya qilish jarayonida tenglikni ta’minlash muhimdir. Inson huquqlarining himoyasi barcha shaxslar uchun bir xil bo‘lishi lozim.
- ✓ **Xususiy hayotni hurmat qilish** – davlatlar axborot xavfsizligini ta’minlashda xususiy hayotni himoya qilishni ustuvor vazifa sifatida ko‘rishi zarur. Kiberxavfsizlikka oid tadbirlar, xususan, ma’lumotlarni to‘plash va monitoring qilishda shaxsiy hayotni buzmaslik kerak.

Xulosa qilib aytganda, Inson huquqlari va axborot xavfsizligi o‘rtasidagi muvozanatni ta’minlash dolzarb global masala bo‘lib qolmoqda. Kiberjinoyatlar va axborot tahdidlari milliy va xalqaro miqyosda xavf tug‘dirmoqda. Biroq, axborot xavfsizligini ta’minlashda davlatlar tomonidan amalga oshirilayotgan choralarning, inson huquqlariga zarar yetkazmasdan, samarali bo‘lishi zarur. Buning uchun, davlatlar o‘rtasida hamkorlikni mustahkamlash, axborot xavfsizligini ta’minlashda inson huquqlariga hurmat ko‘rsatish va axborot olish, so‘z erkinligi kabi huquqlarni himoya qilish masalalari muhimdir. Yagona xalqaro yondashuv va normativ hujjatlarni ishlab chiqish orqali, axborot xavfsizligi va inson huquqlari o‘rtasidagi to‘g‘ri muvozanatni ta’minlash mumkin bo‘ladi.

Shaxsiy hayot daxlsizligini ta’minlash. Shaxsiy hayot daxlsizligi – bu har bir shaxsning o‘zining shaxsiy ma’lumotlari, hayoti, va faoliyati haqida boshqalar tomonidan noto‘g‘ri yoki noqonuniy aralashuvlarga qarshi huquqi sifatida, inson huquqlarining asosiy tamoyillaridan biridir. Bugungi kunda kiberxavfsizlik va axborot texnologiyalari jadal rivojlanayotgan davrda, shaxsiy hayot daxlsizligini ta’minlash masalasi yanada dolzarb ahamiyat kasb

etmoqda. Internetning va raqamli texnologiyalarni keng qo‘llashning tarqalishi, xususiy ma’lumotlar bilan manipulyatsiya qilishni, internet orqali shaxsiy axborotlarga kirish imkoniyatlarini oshirdi va shu bilan birga, bu sohada huquqiy himoya choralarini kuchaytirishni zaruriy holga keltirdi.

Shaxsiy hayot daxlsizligi ta’minlanishi, avvalo, shaxsning o‘zini himoya qilish va o‘zining maxfiy axborotlari bilan bog‘liq risklardan xoli bo‘lish imkoniyatiga ega bo‘lishidir. Bunda davlatlarning axborot xavfsizligi va kiberjinoyatlarga qarshi kurashishda amalga oshirilayotgan harakatlari, shaxsiy ma’lumotlarning muhofazasi masalasiga bevosita ta’sir ko‘rsatadi. Kiberjinoyatlarning tez rivojlanishi va raqamli tizimlar orqali shaxsiy axborotlarga noqonuniy kirish holatlari, davlatlarni axborot xavfsizligini ta’minlashga va shaxsiy hayot daxlsizligini himoya qilishga majbur qilmoqda.

Shaxsiy hayot va raqamli ma’lumotlarning himoyasi. Shaxsiy ma’lumotlar – bu insonning o‘ziga xos xususiyatlarini aniqlashga imkon beruvchi axborotlar bo‘lib, ular o‘z ichiga shaxsning ism-familiyasi, manzili, telefon raqami, tibbiy holati, moliyaviy va boshqa nozik ma’lumotlarni oladi. Internet va raqamli texnologiyalar yordamida shaxsiy ma’lumotlarning yig‘ilishi va saqlanishi, shuningdek, ularning xavfsizligi masalalari hozirgi kunda jiddiy huquqiy muammolarga aylangan.

Ko‘plab davlatlar, xususan, Yevropa Ittifoqi, shaxsiy ma’lumotlarni himoya qilishda global standartlarni belgilash uchun qonunchiliklarni kuchaytirdi. Yevropa Ittifoqida, masalan, 2018 yil 25 maydan kuchga kirgan **Umumiy ma’lumotlarni himoya qonuni (GDPR)**, shaxsiy ma’lumotlarning himoyasini ta’minlash va shu bilan birga shaxsning maxfiyligini himoya qilishga qaratilgan huquqiy mexanizmdir. Ushbu qonun, nafaqat Yevropa hududidagi davlatlar uchun, balki boshqa mamlakatlar uchun ham, shaxsiy ma’lumotlarni yig‘ish, saqlash, ishlatish va ularni qayta ishlashning qat’iy normalarini belgilaydi.

GDPRda, shaxsiy ma’lumotlarni yig‘ish va ishlatishdan oldin shaxsning roziligini olish, ma’lumotlarni himoya qilish va o‘zgarishlarga qarshi tizimlarni yaratish kabi masalalar qat’iy belgilangan. Ushbu normativ hujjat shaxsiy hayot daxlsizligini ta’minlashda muhim qadam hisoblanadi, chunki u xalqaro darajada shaxsiy ma’lumotlarning himoya qilinishini ta’minlashga qaratilgan.

Kiberxavfsizlik va shaxsiy hayot daxlsizligi. Kiberxavfsizlikning asosiy maqsadi – axborot tizimlarining himoya qilinishini ta’minlash va

ma’lumotlarning xavfsizligini kafolatlashdir. Biroq, kiberjinoyatlar va raqamli tahdidlar tufayli, shaxsiy hayot daxlsizligi ta’minlashda bir qator huquqiy va texnik muammolar paydo bo‘lmoqda. Internetda shaxsiy axborotlar, internet tranzaktsiyalari, telefon aloqalari va boshqa elektron ma’lumotlar turli shakllarda saqlanmoqda va ularga oson kirish mumkin. Shu sababli, kiberjinoyatchilar uchun bu ma’lumotlarga noqonuniy kirish imkoniyatlari mavjud bo‘lib, ular noqonuniy usullar bilan shaxsiy axborotlarni o‘g‘irlashi yoki buzishi mumkin.

Axborot xavfsizligi va shaxsiy hayot daxlsizligi o‘rtasida o‘zaro bog‘liqlik mavjud. Kiberjinoyatlar, masalan, shaxsiy ma’lumotlarni o‘g‘irlash yoki undan foydalangan holda firibgarlik qilish, shaxsning maxfiylik huquqini buzadi. Bunday holatlarda, davlatlar kiberxavfsizlikni ta’minlash bilan birga, shu ma’lumotlarni qanday himoya qilishni ham o‘rganishlari zarur. Internetda shaxsiy axborotlarning o‘g‘irlanishi, maxfiy axborotlarga noqonuniy kirish, va axborotlarni buzish kabi tahdidlar, davlatlarni shaxsiy hayotni himoya qilishga qaratilgan qonunlarni ishlab chiqishga undaydi.

Shaxsiy hayot daxlsizligini ta’minlashda texnologik vositalar ham muhim rol o‘ynaydi. Misol uchun, kriptografiya, ma’lumotlarni shifrlash va boshqa xavfsizlik choralarini qo‘llash shaxsiy ma’lumotlarni himoya qilishda samarali vositalardan biridir. Kriptografiya ma’lumotlarning sir saqlanishini ta’minlash uchun zarur vositadir, chunki u ma’lumotlarni shifrlab, faqat ruxsat etilgan shaxslar tomonidan ochilishini kafolatlaydi.

Shaxsiy hayotni himoya qilishdagi davlatlararo mas’uliyat. Shaxsiy hayot daxlsizligini ta’minlashda davlatlarning o‘zaro hamkorligi va global yondashuvi muhim ahamiyatga ega. Bunda davlatlar, shaxsiy ma’lumotlarni himoya qilishda umumiy xalqaro standartlarga amal qilishlari lozim. Xalqaro hamkorlik, kiberjinoyatlar va shaxsiy ma’lumotlarga noqonuniy kirish holatlariga qarshi kurashishda samarali bo‘lishi mumkin. Ayniqsa, shaxsiy ma’lumotlarni o‘g‘irlash, noto‘g‘ri ishlatish yoki o‘chirish kabi tahdidlarga qarshi xalqaro darajada ko‘rib chiqilayotgan qonunlar va normativ hujjatlar, davlatlar o‘rtasidagi hamkorlikni rivojlantirishga xizmat qiladi.

Bundan tashqari, davlatlarning milliy qonunlari va xalqaro huquq normalari o‘rtasidagi uyg‘unlik, shaxsiy hayotni himoya qilishda samarali mexanizm yaratadi. Milliy qonunlarning xalqaro huquq bilan uyg‘unligi, shaxsiy hayot daxlsizligini ta’minlashda nafaqat ichki, balki xalqaro miqyosda ham huquqiy xavfsizlikni yaratishga imkon beradi.

Xulosa qilib aytganda, Shaxsiy hayot daxlsizligi – bu inson huquqlarining ajralmas qismidir, va uni ta’minlash bugungi kunda global muammo sifatida qabul qilinmoqda. Kiberjinoyatlar va axborot xavfsizligi sohasidagi tahdidlar, shaxsiy hayotni himoya qilishda huquqiy, texnologik va siyosiy choralarni talab qiladi. Davlatlar, shaxsiy axborotlarni himoya qilish va kiberjinoyatlarni oldini olish uchun samarali normativ hujjatlar ishlab chiqishi, texnologik yechimlarni qo‘llashi, hamda xalqaro hamkorlikni mustahkamlashi zarur. Shaxsiy hayotni himoya qilish va axborot xavfsizligini ta’minlash o‘rtasidagi muvozanatni topish, inson huquqlarini hurmat qilishning eng muhim tamoyillaridan biri hisoblanadi.

Davlat xavfsizligi va tsenzura chegaralari. Bugungi kunda global miqyosda kiberxavfsizlik va axborot texnologiyalarining rivojlanishi shaxsiy huquqlar va erkinliklar, xususan, axborotga erkin kirish huquqi, shaxsiy hayotni himoya qilish va inson huquqlarining boshqa jihatlari bilan bog‘liq muammolarni keltirib chiqarmoqda. Davlat xavfsizligini ta’minlash va axborot xavfsizligini saqlash maqsadida amalga oshiriladigan choralar, ba’zan, inson huquqlari va erkinliklariga, ayniqsa, erkin axborot oqimini cheklashga olib kelishi mumkin. Bu muammo, ayniqsa, davlat xavfsizligini ta’minlashda axborotlar ustidan nazorat o‘rnatish, tsenzura va internetni cheklash masalalari bilan bog‘liq.

Davlat xavfsizligi va axborot xavfsizligini ta’minlashga qaratilgan tadbirlar, ko‘pincha, shaxsiy huquqlarga ta’sir qilishi mumkin. Xususan, bu huquqlar orasida erkin fikr bildirish, axborotga kirish va tarqatish huquqlari alohida ahamiyatga ega. Shuning uchun, davlat xavfsizligini ta’minlashga qaratilgan siyosatlar, erkinliklar va shaxsiy huquqlarni cheklamasdan amalga oshirilishi kerak. Shu bilan birga, kiberjinoyatlar, teraktlar va boshqa xavf-xatarlar, davlatlar uchun axborot xavfsizligini ta’minlashda muhim masala bo‘lib qolmoqda.

Tsenzura va davlat xavfsizligi. Tsenzura, yoki axborotning davlat tomonidan nazorat qilinishi, ayniqsa, internet va raqamli texnologiyalar sohasida muhim masalalardan biridir. Davlatlar ko‘pincha milliy xavfsizlikni himoya qilish va jamoat tartibini saqlashni maqsad qilib, axborotlarni nazorat qilish va cheklash choralarini ko‘rishadi. Internetda axborotning erkin tarqalishi, radikal g‘oyalar va terroristik tashkilotlar tomonidan ishlatilishi mumkin bo‘lgan bir vosita sifatida ko‘riladi. Shu sababli, ba’zi davlatlar o‘z

hududlarida internetni va axborot tizimlarini tsenzuraga olib, o‘z fuqarolarining axborotga kirish huquqini cheklashadi.

Agar davlat xavfsizligini ta’minlash maqsadida amalga oshiriladigan tsenzura, erkin axborot oqimini cheklasa yoki axborot erkinligini buzsa, bu inson huquqlarining poymol qilinishiga olib kelishi mumkin. Inson huquqlari bo‘yicha xalqaro standartlarga ko‘ra, axborot olish va erkin fikr bildirish har bir shaxsning fundamental huquqlaridan biridir. Shu sababli, davlatlar axborot xavfsizligini ta’minlashni, boshqa tomondan, erkin fikr va axborot tarqatish huquqini cheklamaslikka intilishlari zarur.

Tsenzuraning huquqiy chegaralari. Xalqaro huquq va inson huquqlari tamoyillariga muvofiq, tsenzura faqatgina ma’lum va qat’iy me’yorlar asosida amalga oshirilishi kerak. Tsenzura yoki axborotning davlat tomonidan nazorat qilinishi, inson huquqlariga salbiy ta’sir ko‘rsatmasligi uchun quyidagi huquqiy cheklovlar asosida amalga oshirilishi zarur:

- ✓ **Qonuniylik prinsipiga rioya qilish**: Axborotga nisbatan cheklovlar faqat qonun orqali amalga oshirilishi kerak. Boshqa so‘z bilan aytganda, tsenzura faqat belgilangan qonunlarga, jamiyatda mavjud bo‘lgan qoidalar va etik tamoyillarga asoslanishi zarur. Shu bilan birga, bu cheklovlar faqatgina o‘ta muhim xavflar va tahdidlar mavjud bo‘lganda, ya’ni, milliy xavfsizlikni ta’minlash uchun zarur bo‘lgan hollarda qo‘llanilishi mumkin.
- ✓ **Nazoratchilikning mustahkamligi**: Tsenzura siyosatini amalga oshiruvchi organlar fuqarolarning huquqlari va erkinliklariga zarar yetkazmaslik uchun qattiq nazorat ostida bo‘lishi zarur. Davlatlar axborot xavfsizligini ta’minlashda nazoratni amalga oshirgan tashkilotlarning mustahkamligi, shaffofligi va mas’uliyati kerak. Bunda fuqarolar o‘zining huquqlarini himoya qilish uchun qonuniy choralarni ko‘rish imkoniyatiga ega bo‘lishlari zarur.
- ✓ **O‘rta vaziyatlar va muvozanat**: Davlat xavfsizligini ta’minlash maqsadida amalga oshiriladigan tsenzura choralari, axborotning ochiqligi va erkinligini saqlashga intilish bilan muvozanatni topishi zarur. Shu sababli, faqatgina muhim va jiddiy tahdidlar yuzaga kelganda tsenzura choralarini qo‘llash mumkin. Boshqa hollarda esa axborotning erkin tarqatilishiga ruxsat berilishi kerak.
- ✓ **Xalqaro majburiyatlar va xalqaro huquq normativlari**: Davlatlar xalqaro majburiyatlarini inobatga olishlari kerak, chunki ular erkin fikr bildirish va axborot olish huquqiga zarar yetkazmaydigan tarzda xavfsizlik

choralarini amalga oshirishlari kerak. Bunday majburiyatlar, xususan, BMTning Inson Huquqlari bo‘yicha Umumjahon Deklaratsiyasi va boshqa xalqaro shartnomalarga asoslanadi.

Xulosa qilib aytganda, Davlat xavfsizligini ta’minlash va axborot xavfsizligini saqlashda, tsenzura va axborot ustidan nazoratning chegaralarini aniqlash katta huquqiy va siyosiy muammolarni keltirib chiqaradi. Tsenzura amalga oshirilgan hollarda, bu huquqiy va inson huquqlari bilan bog‘liq muvozanatni saqlash zarurati yuzaga keladi. Axborot erkinligi va shaxsiy huquqlarning buzilishiga olib kelmaydigan tarzda, davlat xavfsizligini ta’minlash uchun samarali mexanizmlar ishlab chiqish muhimdir. Shu bilan birga, davlatlar, xalqaro huquq va inson huquqlari tamoyillariga muvofiq ravishda, axborot ustidan nazoratni amalga oshirishi kerak, bu esa nafaqat xavfsizlikni ta’minlash, balki fuqarolarning erkinliklarini himoya qilishga ham xizmat qiladi.

Erkin axborot olish huquqi va xavfsizlikni muvofiqlashtirish. Inson huquqlari va axborot xavfsizligi o‘rtasidagi muvozanat, ayniqsa, kiberxavfsizlik sohasida dolzarb masala bo‘lib, shu bilan birga, zamonaviy jamiyatda erkin axborot olish huquqi va davlat xavfsizligini ta’minlash o‘rtasidagi o‘zaro bog‘lanishni anglatadi. Bu ikkala tamoyil o‘rtasidagi muvozanatni saqlash, bugungi global xavfsizlik muammolarini hisobga olgan holda, o‘ta murakkab va muhim vazifa hisoblanadi.

Erkin axborot olish huquqi. Erkin axborot olish huquqi har bir shaxsning fundamental huquqlaridan biri bo‘lib, bu huquq, nafaqat axborot manbalariga, balki shu axborotlarni erkin tarqatish va undan foydalanish imkoniyatini ham o‘z ichiga oladi. BMTning Inson Huquqlari bo‘yicha Umumjahon Deklaratsiyasining 19-moddasida erkin fikr bildirish va axborot olish huquqi asosiy huquqlardan biri sifatida tan olinadi. Bu huquq, fuqarolarning ijtimoiy, siyosiy va iqtisodiy hayotda faol ishtirok etishlarini ta’minlash uchun zarurdir.

Bugungi kunda axborot texnologiyalarining rivojlanishi, internet va raqamli platformalarning keng tarqalishi orqali, bu huquqning amalga oshirilishi yangi darajaga ko‘tarildi. Internet, axborot va bilimlarga erkin kirish uchun keng imkoniyatlarni yaratdi, shu bilan birga, jamiyatlar o‘rtasida axborotning tez va keng tarqalishini ta’minlaydi. Biroq, erkin axborot olish huquqining amalga oshirilishi, ko‘plab xavf-xatarlar bilan ham yuzma-yuz bo‘lishi mumkin.

Davlat xavfsizligi va axborot nazorati. Davlatlar, xavfsizlikni ta’minlash, terrorizmga qarshi kurashish, kiberxavfsizlikni mustahkamlash va boshqa milliy xavflarni kamaytirish maqsadida axborot oqimlarini nazorat qilishni amalga oshiradilar. Kiberjinoyatlar, xakerlik, axborotlar o‘g‘riligi va internet orqali amalga oshiriladigan boshqa turdagi jinoyatlar, davlatlar uchun axborot xavfsizligini ta’minlashda o‘ta jiddiy tahdidlardir. Bunday sharoitda, davlatlar axborot xavfsizligini ta’minlash uchun tsenzura yoki axborotlarni nazorat qilish choralarini qo‘llashlari mumkin.

Davlat xavfsizligini ta’minlashga qaratilgan axborot nazorati, ba’zan erkin axborot olish huquqini cheklashga olib keladi. Misol uchun, davlatlar internetda mavjud bo‘lgan radikal g‘oyalar, propagandani tarqatish, yoki terroristik guruhlar tomonidan qo‘llaniladigan axborotlarni nazorat qilish uchun internetni cheklash choralarini ko‘rishlari mumkin. Biroq, bunday cheklovlar, erkin axborot olish huquqining poymol qilinishiga olib kelishi mumkin.

Erkin axborot olish huquqi va xavfsizlik muvofiqlashtirilishi. Erkin axborot olish huquqi va xavfsizlikni ta’minlash o‘rtasidagi muvozanatni saqlash uchun quyidagi tamoyillarga asoslanish zarur:

- ✓ **Qonuniylik**: Davlatlar axborot xavfsizligini ta’minlash uchun amalga oshiradigan barcha choralari qonuniy asosga ega bo‘lishi kerak. Tsenzura va axborotga cheklovlar faqat davlatning xavfsizlik va tartibni saqlashdagi qonuniy huquqlariga asoslanishi lozim. Har qanday nazorat va cheklovlar aniq, ochiq-oshkora va asosli bo‘lishi kerak.
- ✓ **Muvozanatni ta’minlash**: Erkin axborot olish huquqi va davlat xavfsizligini ta’minlash o‘rtasidagi muvozanatni topish juda muhimdir. Bu, har ikki tamoyilga ham zarar yetkazmasdan amalga oshirilishi kerak. Davlat xavfsizligini ta’minlash uchun amalga oshirilgan choralar erkin axborot oqimini cheklamasligi, aksincha, muayyan xavflarni oldini olishni ta’minlashi zarur.
- ✓ **Xalqaro Majburiyatlar**: Erkin axborot olish huquqi va xavfsizlikni ta’minlash o‘rtasidagi muvozanat xalqaro huquq va inson huquqlari normativlariga ham muvofiq bo‘lishi kerak. BMTning Inson Huquqlari bo‘yicha Umumjahon Deklaratsiyasi, shuningdek, boshqa xalqaro shartnomalar, davlatlar uchun asosiy yo‘l-yo‘riq bo‘lib xizmat qilishi kerak. Xalqaro huquq doirasida, axborot xavfsizligini ta’minlashda erkinlik va xavfsizlikning uyg‘unligini saqlash zarurati tilga olinadi.

✓ **Shaxsiy Huquqlarni Himoya Qilish**: Xavfsizlikni ta’minlashga qaratilgan choralarning shaxsiy huquqlarni, ayniqsa, shaxsiy hayotni himoya qilishni poymol qilmasligi kerak. Davlat xavfsizligi uchun axborot nazoratini kuchaytirish jarayonida, shaxsiy huquqlar va maxfiylikka tahdidlar paydo bo‘lmasligi kerak. Shu bilan birga, shaxsiy huquqlarni cheklash faqatgina zarur bo‘lganda, ya’ni aniq va muhim xavflar mavjud bo‘lganda qo‘llanishi lozim.

Xulosa qilib aytganda, Erkin axborot olish huquqi va xavfsizlikni ta’minlash o‘rtasidagi muvozanatni topish, zamonaviy jamiyatda juda murakkab va dolzarb masala hisoblanadi. Davlatlar axborot xavfsizligini ta’minlash, ayniqsa, kiberjinoyatlar va terrorizmga qarshi kurashishda samarali choralar ko‘rishlari kerak, ammo bu jarayonda fuqarolarning erkin axborot olish huquqlarini cheklamaslikka intilishlari zarur. Muvozanatni saqlash uchun barcha choralarning qonuniy va xalqaro huquq standartlariga muvofiq bo‘lishi, shuningdek, shaxsiy huquqlarni himoya qilish va shaffoflikni ta’minlash juda muhimdir. Davlat xavfsizligini ta’minlash va erkin axborot olish huquqini saqlash, butun jamiyatning barqaror rivojlanishi uchun zarur tamoyillar hisoblanadi.

BOB BO‘YICHA UMUMIY XULOSALAR

Kiberjinoyatlar — zamonaviy jinoyatlar turidan biri bo‘lib, axborot texnologiyalarining rivojlanishi bilan kengayib, yanada murakkablashgan va global miqyosda ta’sir ko‘rsatgan. Kiberjinoyatlar, nafaqat individual shaxslar, balki davlatlar, iqtisodiy tizimlar va turli tashkilotlarga ham jiddiy tahdidlar keltiradi. Shu bois, ularni huquqiy jihatdan tan olish va ularga qarshi samarali kurashish davlatlar o‘rtasida hamkorlikni va xalqaro normativ hujjatlar ishlab chiqishni talab qiladi.

Kiberjinoyatlar va axborot texnologiyalarining tarqalishi, o‘zgaruvchan va tez sur’atlarda rivojlanayotgan dunyoda, huquqiy muammolarni samarali hal qilishni qiyinlashtirmoqda. Xususan, raqamli suverenitet, xalqaro normativlar, sun’iy intellekt va axborot xavfsizligi masalalari alohida muhokama qilinishi kerak. Ushbu bobda kiberjinoyatlarni tan olish va ular bilan kurashishda yuzaga kelayotgan asosiy istiqbollar tahlil qilinadi.

Raqamli suverenitet va ziddiyatlar. Raqamli suverenitet masalasi, xususan, davlatlarning o‘z hududida internet va axborot texnologiyalari ustidan nazoratni amalga oshirish istagi, bugungi kunda o‘ta dolzarb masalaga aylangan. Raqamli suverenitet, bir tomondan, davlatlarning axborot makonida

oʻzining mustaqil va erkin qarorlar qabul qilish huquqini anglatadi. Biroq, bu holatning xalqaro miqyosdagi ta’siri, koʻpincha ziddiyatlarga sabab boʻladi, chunki davlatlar oʻrtasidagi axborot va internet erkinligi, ba’zida milliy xavfsizlikni ta’minlashga qarshi chiqadigan holatlarga olib keladi. Shu nuqtai nazardan, raqamli suverenitetning qonuniy asoslari, davlatlarning xalqaro huquq bilan uygʻunligini saqlash masalalari, kiberjinoyatlar bilan kurashishdagi ziddiyatlar koʻrib chiqiladi.

Yagona xalqaro normativ hujjat ishlab chiqish ehtiyoji. Kiberjinoyatlar global miqyosda keng tarqalgan va ularning huquqiy jihatdan tan olinishi uchun yagona xalqaro normativ hujjatning mavjudligi zarur. Hozirda har bir davlat oʻz qonunlarini va qoidalarini ishlab chiqayotgan boʻlsada, kiberjinoyatlar va ularni jazolashning xalqaro koʻlamda yagona me’yorlar asosida amalga oshirilishi lozim. Bunday hujjat, kiberjinoyatlarning turli shakllarini aniq belgilash, jinoyatchilikni muhofaza qilish va davlatlar oʻrtasida hamkorlikni kuchaytirish uchun zarur. Yagona xalqaro hujjatni ishlab chiqish, kiberjinoyatlarni huquqiy jihatdan bir xil koʻrish va bunday jinoyatlarga qarshi kurashishda yanada samarali natijalarga erishish imkonini yaratadi.

Sun’iy intellekt va avtomatlashtirilgan jinoyatlar xavfi. Sun’iy intellekt (SI) va avtomatlashtirilgan texnologiyalar dunyoda tez sur’atlarda rivojlanmoqda. Ularning kiberjinoyatlar bilan bogʻliq xavf-xatarlari oʻziga xos va yangi huquqiy masalalarni keltirib chiqarmoqda. Sun’iy intellekt, ayniqsa, kiberjinoyatlar qilishda hamda jinoyatlarni oldini olishda oʻta muhim rol oʻynaydi. Biroq, SI orqali amalga oshirilgan jinoyatlar, mas’uliyatni aniqlashda, xavfsizlikni ta’minlashda va huquqni muhofaza qiluvchi organlar uchun murakkabliklar yaratadi. SI tizimlarining qarorlar qabul qilish jarayonlari shaffof emasligi, ular bilan bogʻliq jinoyatlar uchun mas’uliyatni aniqlashda murakkabliklarga olib keladi. Bunday xavflar va ularning huquqiy tartibga solinishi, sun’iy intellektning qonuniy va etik jihatlarini tahlil qilishni talab qiladi.

Inson huquqlari va axborot xavfsizligi muvozanati. Inson huquqlari va axborot xavfsizligi oʻrtasidagi muvozanat, kiberjinoyatlarga qarshi kurashishda asosiy masalalardan biri hisoblanadi. Axborot xavfsizligini ta’minlash uchun amalga oshiriladigan chora-tadbirlar, ba’zan shaxsiy huquqlarni cheklashga olib keladi. Internetda erkin axborot almashinuvi, fikr bildirish erkinligi va shaxsiy maxfiylik kabi huquqlar, xavfsizlikni ta’minlash

uchun cheklovlarga uchrashi mumkin. Biroq, inson huquqlarini himoya qilish va axborot xavfsizligini ta’minlash o‘rtasida to‘g‘ri muvozanatni topish zarur. Bu, davlatlar va xalqaro tashkilotlar tomonidan amalga oshiriladigan siyosatlar va huquqiy normativlar yordamida erishilishi mumkin.

Xulosa qilib aytganda, Kiberjinoyatlar va axborot xavfsizligi masalalari zamonaviy huquq tizimining muhim qismini tashkil qiladi. Raqamli suverenitet, yagona xalqaro normativ hujjatlarni ishlab chiqish, sun’iy intellekt va avtomatlashtirilgan jinoyatlar xavfi, inson huquqlari va axborot xavfsizligi muvozanati kabi masalalar, davlatlar o‘rtasidagi hamkorlikni kuchaytirish va xalqaro huquqni takomillashtirishga ehtiyojni keltirib chiqarmoqda. Bu masalalar, faqatgina xalqaro miqyosda muvofiqlashtirilgan va samarali huquqiy chora-tadbirlar orqali hal qilinishi mumkin.

XULOSA VA TAKLIFLAR

Zamonaviy axborot texnologiyalarining tez sur’atlarda rivojlanishi kiberjinoyatlar va ularga qarshi kurashishda yuzaga kelayotgan huquqiy muammolarni yanada murakkablashtirmoqda. Kiberjinoyatlar global miqyosda keng tarqalgan va har bir davlatni tahdid qilayotgan xavf bo‘lib, ayni paytda ularning huquqiy tan olinishi va jazolanishi, xalqaro hamkorlik va normativ hujjatlarning samarali ishlashi zaruriyatini tug‘diradi. Xalqaro kiberjinoyatlar va ularni jinoyat deb e’tirof etishdagi huquqiy muammolar, nafaqat milliy, balki xalqaro darajada ham jiddiy va dolzarb masalalarga aylangan.

Ushbu monografiyada kiberjinoyatlar sohasidagi huquqiy me’yorlar, xalqaro hamkorlik, raqamli suverenitet, va axborot xavfsizligi masalalari yoritilib, ular o‘rtasidagi muvozanatni ta’minlash yo‘llari ko‘rib chiqildi. Kiberjinoyatlarning yuridik tahlili, xususan, ularni jinoyat sifatida e’tirof etish, jinoyatni isbotlash va jazolashdagi qiyinchiliklar, shuningdek, kiberjinoyatlarga qarshi samarali choralar ko‘rishning muhimligi, bugungi kunda o‘ta dolzarb masalalardan biri hisoblanadi.

Shu bilan birga, xalqaro hamkorlik, xususan, Budapest Konvensiyasi va boshqa xalqaro normativ hujjatlar kiberjinoyatlarga qarshi kurashishda muhim o‘rin tutadi. Kiberjinoyatlarni samarali ravishda oldini olish va jazolash uchun milliy qonunlarning xalqaro huquq bilan uyg‘unligi zarur. Shuningdek, sun’iy intellekt va avtomatlashtirilgan jinoyatlar xavfi, erkin axborot olish huquqi va xavfsizlikni ta’minlash o‘rtasidagi muvozanatni saqlash kabi muammolar ham o‘z o‘rnida muhim ahamiyatga ega.

Monografiyaning yakuniy xulosasi sifatida, kiberjinoyatlar bilan kurashishda xalqaro hamkorlikni kuchaytirish, kiberjinoyatlarni global miqyosda yagona qonuniy me’yorlar asosida tan olish va sun’iy intellektning xavf-xatarlarini inobatga olgan holda yangi huquqiy normativlarni ishlab chiqish zarurati mavjudligini ta’kidlash lozim. Shu bilan birga, axborot xavfsizligini ta’minlashda davlatlarning ichki huquqiy tizimlarini va xalqaro huquqni uyg‘unlashtirish, shaxsiy huquqlarga zarar yetkazmasdan xavfsizlikni ta’minlash masalalariga alohida e’tibor qaratish zarur.

Takliflar

✓ **Xalqaro kiberjinoyatlarga qarshi yagona huquqiy me’yorlarni ishlab chiqish**: Kiberjinoyatlarni xalqaro darajada tan olish va ularga qarshi kurashishda yagona normativ hujjat ishlab chiqish zarur. Bunday hujjat, barcha

davlatlarga bir xil me’yorlarga amal qilish imkonini beradi va kiberjinoyatlarga qarshi global miqyosda samarali kurashish imkoniyatini yaratadi.

✓ **Milliy qonunlarni xalqaro huquq bilan uyg‘unlashtirish**: Har bir davlat kiberjinoyatlar bilan kurashishda xalqaro huquq bilan muvofiqlikni ta’minlash uchun o‘z qonunlarini yangilashi lozim. Bunda, milliy qonunlar, xalqaro me’yorlar bilan uyg‘unlashtirilishi kerak, bu esa kiberjinoyatlarni jazolashni yengillashtiradi.

✓ **Kiberxavfsizlik va sun’iy intellektning huquqiy tartibini takomillashtirish**: Sun’iy intellekt va avtomatlashtirilgan jinoyatlar xavfini kamaytirish uchun sun’iy intellekt texnologiyalarining yuridik jihatlarini chuqur tahlil qilish va ularga mos keladigan huquqiy me’yorlar ishlab chiqish lozim. Bu, kiberjinoyatlarning oldini olishda samarali tizim yaratishga yordam beradi.

✓ **Erkin axborot olish huquqi va xavfsizlik o‘rtasidagi muvozanatni saqlash**: Davlat xavfsizligini ta’minlash uchun axborot nazoratini kuchaytirishda shaxsiy huquqlar va erkinliklarni cheklamagan holda, to‘g‘ri muvozanatni topish zarur. Bu, fuqarolarni himoya qilish bilan birga, xavfsizlikni ta’minlashga imkon beradi.

✓ **Xalqaro hamkorlikni kuchaytirish**: Xalqaro tashkilotlar va davlatlar o‘rtasidagi hamkorlikni yanada kuchaytirish, kiberjinoyatlarga qarshi kurashishda yanada samarali tizim yaratishga yordam beradi. Xalqaro hamkorlik orqali, davlatlar o‘rtasida kiberjinoyatlarga qarshi birlashgan kurashning samaradorligini oshirish mumkin.

Ushbu takliflar, kiberjinoyatlar va ularni jazolashdagi huquqiy muammolarni hal etishda o‘zaro hamkorlikni rivojlantirish, global miqyosda samarali kurash tizimini yaratish va huquqiy jihatdan to‘g‘ri yechimlar ishlab chiqish imkonini yaratadi. Kiberjinoyatlarga qarshi kurashish, zamonaviy jamiyatda huquqiy tizimning eng muhim vazifalaridan biriga aylanganini hisobga olgan holda, huquqiy normativlar va xalqaro hamkorlikni yanada rivojlantirishga intilish zarurdir.

Tadqiqot natijalariga asoslangan umumiy xulosa va nazariy natijalar. Kiberjinoyatlar zamonaviy dunyoda eng dolzarb huquqiy masalalardan biriga aylangan. Ularning global miqyosda tez sur’atlarda rivojlanishi va bir vaqtning o‘zida har bir davlatning ichki xavfsizligi uchun tahdid solishi, kiberjinoyatlarni jinoyat sifatida tan olish, ular bilan samarali

kurashish va huquqiy normativlarni ishlab chiqish zaruratini taqozo etmoqda. Ushbu monografiyada kiberjinoyatlar bilan kurashishda yuzaga kelayotgan huquqiy muammolar va ularni xalqaro huquq doirasida tartibga solish, shuningdek, xalqaro hamkorlikni kuchaytirish va yangi normativ hujjatlarni ishlab chiqish masalalari koʻrib chiqildi.

Tadqiqot natijalariga koʻra, kiberjinoyatlar turlari va ularning ta’siri oʻta murakkab va keng miqyosli boʻlib, bu jinoyatlarni milliy darajada samarali jazolashning qiyinchiliklarini kuchaytiradi. Kiberjinoyatlar ba’zan an’anaviy jinoyatlar bilan solishtirganda yangi huquqiy masalalarni yuzaga keltiradi, masalan, elektron dalillarning ishonchliligi, internet orqali amalga oshirilgan jinoyatlarning hududiy chegaralarini aniqlashdagi qiyinchiliklar, va davlatlarning kiberjinoyatlarga qarshi kurashishda turlicha yondashuvlari. Kiberjinoyatlarni jinoyat sifatida tan olish va ularga qarshi kurashishda xalqaro hamkorlikning kuchayishi, ayniqsa, **Budapest Konvensiyasi** kabi xalqaro huquqiy hujjatlarning roli muhim ahamiyatga ega.

Tadqiqot davomida quyidagi asosiy nazariy natijalarga erishildi:

- **Kiberjinoyatlarning universal e’tirofi**: Kiberjinoyatlar bugungi kunda har bir davlatning ichki xavfsizligi uchun tahdid solishi va ularni jinoyat sifatida universal tan olish zarurati mavjud. Kiberjinoyatlarni global miqyosda yagona qonuniy asosda tan olish va jazolash usullari samarali kurash tizimini shakllantirishi mumkin. Bunday yondashuv davlatlar oʻrtasida huquqiy uygʻunlikni ta’minlaydi va kiberjinoyatlarga qarshi kurashishda samarali tizimni yaratadi.
- **Xalqaro hamkorlikning rivojlanishi**: Kiberjinoyatlar transmilliy xususiyatga ega boʻlgani uchun davlatlar oʻrtasida hamkorlikni kuchaytirish zarur. Xalqaro huquq doirasida hamkorlikni rivojlantirish, kiberjinoyatlarga qarshi birlashgan kurashni ta’minlashga yordam beradi. **Budapest Konvensiyasi** kabi hujjatlar kiberjinoyatlarga qarshi kurashishda davlatlar oʻrtasidagi hamkorlikni yanada mustahkamlashda muhim rol oʻynaydi.
- **Axborot xavfsizligi va inson huquqlari oʻrtasidagi muvozanat**: Kiberjinoyatlarga qarshi kurashishda, xavfsizlikni ta’minlash va inson huquqlarini himoya qilish oʻrtasidagi muvozanatni saqlash zarur. Davlat xavfsizligini ta’minlash, shaxsiy hayotni himoya qilish, va axborot xavfsizligi oʻrtasida toʻgʻri muvozanatni topish huquqiy tizimning asosiy vazifalaridan biridir.

- **Yagona xalqaro normativ hujjat ishlab chiqish ehtiyoji**: Kiberjinoyatlar bilan kurashish uchun yagona xalqaro normativ hujjat ishlab chiqish zarur. Bunday normativlar, davlatlar o‘rtasida huquqiy uyg‘unlikni ta’minlash va kiberjinoyatlarni jazolashda yagona yondashuvni yaratish imkonini beradi. Yagona xalqaro normativ hujjat kiberjinoyatlarga qarshi kurashishda davlatlar o‘rtasidagi hamkorlikni kuchaytiradi va jinoyatlarning oldini olishga yordam beradi.
- **Sun’iy intellekt va avtomatlashtirilgan jinoyatlar xavfi**: Yangi texnologiyalar, xususan, sun’iy intellekt va avtomatlashtirilgan tizimlar kiberjinoyatlarning yangi shakllarini yuzaga keltirmoqda. Bunday jinoyatlar bilan kurashishda mas’uliyatni aniqlash va qonuniy mexanizmlarni ishlab chiqish zarur. Sun’iy intellektga asoslangan jinoyatlarni jazolashda yangi yondashuvlar va huquqiy normativlar talab qilinadi.
- **Milliy qonunlar va xalqaro huquq o‘rtasidagi uyg‘unlik**: Milliy qonunlar va xalqaro huquq o‘rtasidagi uyg‘unlikni ta’minlash zarur. Kiberjinoyatlarga qarshi kurashishda davlatlar o‘rtasidagi huquqiy uyg‘unlikni saqlash, kiberjinoyatlarga qarshi kurashning samaradorligini oshiradi. Har bir davlat o‘z qonunlarini xalqaro huquq normalariga mos ravishda yangilashi kerak.

Ushbu tadqiqot natijalari, kiberjinoyatlarga qarshi samarali kurashish uchun xalqaro hamkorlik, yagona normativ hujjatlar, va yangi texnologiyalarni hisobga olgan holda huquqiy tizimlarni takomillashtirish zarurligini ko‘rsatadi. Kiberjinoyatlarga qarshi kurashishda yagona, hamkorlikka asoslangan huquqiy tizimlarni yaratish orqali global miqyosda xavfsizlikni ta’minlash va jinoyatlarni oldini olish mumkin.

Xalqaro va milliy darajada kiberjinoyatlarga qarshi kurashish bo‘yicha takliflar. Kiberjinoyatlar bugungi kunda butun dunyo bo‘ylab nafaqat jinoyatchilik, balki milliy xavfsizlik, iqtisodiy barqarorlik va shaxsiy huquqlarning poymol bo‘lishi nuqtai nazaridan ham jiddiy tahdidlarga sabab bo‘lmoqda. Ularning texnologik va transmilliy xususiyatlari tufayli kiberjinoyatlarni milliy doirada hal qilish imkoniyati cheklangan. Shuning uchun, kiberjinoyatlar bilan kurashishda xalqaro hamkorlikni kuchaytirish va milliy qonunlarni xalqaro standartlarga moslashtirish zarurati mavjud. Ushbu takliflar, kiberjinoyatlarga qarshi kurashishning samaradorligini oshirishga qaratilgan bo‘lib, quyidagilarni o‘z ichiga oladi:

✓ **Xalqaro hamkorlikni mustahkamlash va yagona normativ hujjatlarni ishlab chiqish**. Kiberjinoyatlarga qarshi kurashishda, xalqaro darajada yagona qonuniy me’yorlarning bo‘lishi zarur. Shu maqsadda, **Budapest Konvensiyasi** kabi xalqaro huquqiy hujjatlar asosida, kiberjinoyatlarni jinoyat sifatida tan olish va ularni jazolashda bir xil yondashuvni ta’minlaydigan yangi normativ hujjatlar ishlab chiqilishi lozim. Yagona xalqaro normativ tizim yaratish, kiberjinoyatlarni global miqyosda samarali jazolash imkonini beradi va davlatlar o‘rtasidagi huquqiy uyg‘unlikni ta’minlaydi. Bunda, har bir davlat kiberjinoyatlarga qarshi kurashish bo‘yicha xalqaro ko‘p tomonlama shartnomalar va konvensiyalarni ratifikatsiya qilish orqali o‘zining qonuniy majburiyatlarini oshirishi kerak.

✓ **Kiberxavfsizlikni ta’minlash uchun milliy qonunlarni yangilash va xalqaro huquq bilan uyg‘unlashtirish**. Kiberjinoyatlar bilan samarali kurashishda davlatlar o‘z milliy qonunlarini yangilash va xalqaro huquqning talablariga moslashtirish zarur. Bu, o‘z navbatida, kiberjinoyatlar bilan kurashishda huquqiy tizimning samaradorligini oshiradi. Milliy qonunlar va xalqaro huquq o‘rtasidagi uyg‘unlik, kiberjinoyatlarga qarshi kurashishda yagona yondashuvni yaratadi va jinoyatlarning o‘tkazilishini engillashtiradi. Shu maqsadda, har bir davlat kiberxavfsizlik va axborot xavfsizligi bo‘yicha o‘zining huquqiy bazasini rivojlantirib, tegishli qonunlarni mustahkamlash kerak.

✓ **Davlatlar o‘rtasidagi hamkorlikni kuchaytirish**. Kiberjinoyatlar transmilliy xarakterga ega bo‘lishi sababli, ularni milliy doirada hal qilish qiyinlashadi. Shuning uchun, davlatlar o‘rtasidagi huquqiy hamkorlikni mustahkamlash va jiddiy kiberjinoyatlarni aniqlash, tergov qilish va jazolash bo‘yicha birgalikda ishlash muhimdir. Xalqaro politsiya tashkilotlari, masalan, **Interpol**, va huquqni muhofaza qiluvchi boshqa tashkilotlar o‘rtasidagi hamkorlikni kuchaytirish, kiberjinoyatlar bilan kurashishda katta ahamiyatga ega bo‘ladi. Shuningdek, huquqni muhofaza qiluvchi organlar o‘rtasidagi axborot almashinuvi va texnik ko‘makni kengaytirish zarur.

✓ **Kiberjinoyatlarni oldini olish va ularning qurbonlarini himoya qilish**. Kiberjinoyatlarning oldini olish uchun samarali profilaktika dasturlarini ishlab chiqish zarur. Ushbu dasturlar, kiberjinoyatlarning turli shakllari haqida keng jamoatchilikni xabardor qilishni, ularning ta’sirini kamaytirishni va elektron qurilmalardan foydalanishning xavfsizligini oshirishni o‘z ichiga olishi kerak. Shuningdek, kiberjinoyatlar qurbonlarini himoya qilish uchun

zarur huquqiy chora-tadbirlarni ko‘rish lozim. Odamlarning shaxsiy ma’lumotlari va onlayn faoliyati ustidan noqonuniy nazoratni oldini olish, ularni himoya qilishga qaratilgan yangi yuridik mexanizmlar va texnologik yechimlar ishlab chiqilishi kerak.

✓ **Sun’iy intellekt va avtomatlashtirilgan tizimlar bilan bog‘liq huquqiy masalalarni tartibga solish**. Sun’iy intellekt va avtomatlashtirilgan tizimlarning kiberjinoyatlarda foydalanilishi yangi yuridik muammolarni keltirib chiqarmoqda. Bu texnologiyalar orqali amalga oshirilgan jinoyatlar uchun mas’uliyatni aniqlashda yangi yondashuvlar va huquqiy normativlar zarur. Sun’iy intellektning kiberjinoyatlar bilan bog‘liq yuridik aspektlarini aniqlash, shu jumladan, jinoyatlarni aniqlash, tergov qilish va jazolashda foydalaniladigan yangi texnologik vositalar, huquqiy tartibga solinishi lozim.

✓ **Axborot xavfsizligi va inson huquqlari o‘rtasidagi muvozanatni ta’minlash.** Kiberjinoyatlarga qarshi kurashishda axborot xavfsizligini ta’minlash muhim bo‘lishi bilan birga, shaxsiy huquqlarni cheklamaslikka alohida e’tibor qaratish lozim. Davlatlar axborot xavfsizligini ta’minlash uchun amalga oshirayotgan chora-tadbirlar, shaxsiy hayot daxlsizligini va fuqarolarning axborot olish huquqlarini cheklamagan holda amalga oshirilishi kerak. Shu maqsadda, kiberjinoyatlarga qarshi kurashishda shaxsiy huquqlarni himoya qilish bo‘yicha xalqaro standartlarga rioya etilishi zarur.

✓ **Kiberjinoyatlar bo‘yicha ta’lim va malaka oshirish dasturlarini yaratish.** Kiberjinoyatlar sohasida ixtisoslashgan mutaxassislarni tayyorlash, davlatlar o‘rtasida hamkorlikni rivojlantirish uchun zarur. Kiberjinoyatlarni tergov qilish, ularni tahlil qilish va jazolash bo‘yicha malakali mutaxassislarni tayyorlash, davlatlar o‘rtasida axborot va tajriba almashish imkoniyatlarini yaratadi. Xalqaro huquq va kiberxavfsizlik sohasidagi ta’lim dasturlarini kuchaytirish, yangi texnologiyalar bilan ishlashda huquqiy bilimlarni oshirish zarur.

Yuqoridagi takliflar, kiberjinoyatlarni samarali tarzda oldini olish va ularni jazolash uchun xalqaro va milliy darajada amalga oshirilishi lozim bo‘lgan chora-tadbirlarni aks ettiradi. Kiberjinoyatlarga qarshi kurashishda yuqori darajadagi hamkorlik, huquqiy tizimlarni yangilash, va yangi texnologiyalarni hisobga olgan holda normativ bazani takomillashtirish global xavfsizlikni ta’minlashda muhim ahamiyatga ega bo‘ladi.

Ilmiy va amaliy foydasi, tadqiqot doirasini kengaytirish istiqbollari. Kiberjinoyatlar bugungi kunda nafaqat huquqni muhofaza qilish organlari,

balki butun global jamoatchilikning diqqat markazida turadigan muhim huquqiy masala bo‘lib, uning ilmiy va amaliy ahamiyati ortib bormoqda. Ushbu monografiya kiberjinoyatlarni huquqiy jihatdan tan olish va ular bilan kurashishda yuzaga keladigan muammolarni tahlil qilishga qaratilgan bo‘lib, nafaqat ilmiy jihatdan yangi yondashuvlar va qarashlarni taklif qiladi, balki kiberjinoyatlarga qarshi kurashish uchun zarur bo‘lgan amaliy chora-tadbirlarni ham ishlab chiqadi.

Tadqiqotning ilmiy va amaliy foydalari quyidagi asosiy yo‘nalishlarda ko‘rsatilgan:

- **Ilmiy foydasi**. Monografiyaning ilmiy ahamiyati uning kiberjinoyatlarni huquqiy jihatdan tan olish, ularning transmilliy xususiyatlari, va kiberjinoyatlarga qarshi xalqaro hamkorlikni rivojlantirish masalalarini chuqur tahlil qilishda namoyon bo‘ladi. Tadqiqot, kiberjinoyatlar bilan kurashishda yuzaga keladigan huquqiy muammolarni o‘rganish orqali, huquqshunoslar va ilmiy tadqiqotchilar uchun yangi nazariy ma’lumotlar va konsepsiyalarni taklif etadi. Kiberjinoyatlar bilan bog‘liq mavjud huquqiy bo‘shliqlarni aniqlash va ular uchun samarali normativ yechimlarni ishlab chiqish, huquqshunoslik ilmiga yangi qadam qo‘yishga yordam beradi. Shu bilan birga, tadqiqotda kiberjinoyatlar bilan kurashishda xalqaro huquq, milliy qonunlar va global xavfsizlikni ta’minlash nuqtai nazaridan yangi ilmiy yondashuvlar keltirilgan.
- **Amaliy foydasi**. Kiberjinoyatlar bilan kurashish uchun yuridik tizimlar va huquqni muhofaza qiluvchi organlarga amaliy tavsiyalarni ishlab chiqish monografiyaning amaliy ahamiyatini tashkil etadi. Tadqiqot natijalari davlatlar o‘rtasida hamkorlikni kuchaytirish, xalqaro normativ hujjatlarni yangilash va kiberjinoyatlarning oldini olish bo‘yicha amaliy chora-tadbirlar ishlab chiqishda foydali bo‘ladi. Kiberjinoyatlar sohasidagi samarali qonuniy yondashuvlarni joriy etish va jinoyatlarni jazolashda xalqaro huquqni rivojlantirishda muhim ahamiyatga ega bo‘ladi. Shu bilan birga, ta’lim muassasalarida kiberjinoyatlar sohasidagi mutaxassislarni tayyorlash bo‘yicha amaliy dasturlarni ishlab chiqish, huquqiy va texnik bilimlarni kengaytirishga xizmat qiladi.
- **Tadqiqot doirasini kengaytirish istiqbollari**. Kiberjinoyatlar va ularga qarshi kurashish masalasi ilmiy tadqiqotlar doirasida doimiy ravishda yangilanib turadigan va kengayib borayotgan soha bo‘lib, uning kelajakda rivojlanishi quyidagi istiqbollarda ko‘rinadi:

✓ **Kiberjinoyatlar va sun’iy intellekt**: Sun’iy intellektning kiberjinoyatlarda foydalanilishi bilan bog‘liq yangi yuridik masalalar tadqiqot doirasiga kiritilishi kerak. Bu sohada yuridik mas’uliyatni aniqlash, avtomatlashtirilgan tizimlar orqali sodir etilgan jinoyatlarni jazolash, va texnologik yondashuvlarni ishlab chiqish kerak bo‘ladi.

✓ **Kiberxavfsizlik va inson huquqlari**: Axborot xavfsizligi va inson huquqlarining muvozanatini ta’minlash masalasi bo‘yicha yanada keng qamrovli tadqiqotlar olib borilishi lozim. Kiberjinoyatlarga qarshi kurashishda shaxsiy huquqlar va davlat xavfsizligini himoya qilish o‘rtasidagi muvozanatni topish zarur.

✓ **Global hamkorlikning rivojlanishi**: Kiberjinoyatlarga qarshi xalqaro hamkorlikni kuchaytirish, transmilliy jinoyatlar bilan kurashishning samaradorligini oshirishga qaratilgan yanada chuqurroq tadqiqotlar o‘tkazish zarur. Bu sohada xalqaro huquq, diplomatiya va milliy xavfsizlik sohalarini yanada chuqur o‘rganish imkoniyatlari mavjud.

✓ **Kiberjinoyatlar va moliyaviy jinoyatlar**: Kiberjinoyatlar bilan bog‘liq moliyaviy jinoyatlar, ayniqsa kriptovalyutalar va onlayn pul o‘tkazmalari orqali amalga oshiriladigan jinoyatlar bo‘yicha yangi yuridik normalarni ishlab chiqish ehtiyoji tug‘iladi.

Kiberjinoyatlar va ularga qarshi kurashish bo‘yicha tadqiqotlarning doirasini kengaytirish, huquqshunoslar va boshqa mutaxassislar uchun yangi yondashuvlar va yechimlarni taklif qilish, shu bilan birga, kiberjinoyatlar sohasida amaliy va ilmiy bilimlarni boyitishga yordam beradi. Tadqiqotlar, xalqaro va milliy huquqni rivojlantirish, texnologiyalarning tez rivojlanishini hisobga olgan holda, yuridik tizimlarning samaradorligini oshirishga xizmat qiladi. Bu esa kiberjinoyatlar bilan kurashishda yanada yaxshilangan yuridik mexanizmlarni yaratish imkonini beradi.

Foydalangan adabiyotlar ro‘yxati

1. Abdurakhmanov, F. (2018). Axborot xavfsizligi va huquqni muhofaza qilish tizimi. Toshkent: O‘zbekiston Davlat universiteti nashriyoti.
2. Abduvaliyev, N. (2016). O‘zbekiston Respublikasida kiberjinoyatlarni aniqlash va oldini olish. Toshkent: O‘zbekiston Yuridik akademiyasi.
3. Akbarov, D. (2018). Xalqaro hamkorlikda kiberjinoyatlar bilan kurashish: Tajribalar va kelajak. Toshkent: Huquqshunoslik markazi.
4. Akbarov, K. (2018). Kiberxavfsizlik va axborot tizimlarining rivojlanishi. Toshkent: O‘zbekiston texnologiya markazi.
5. Akhmedov, Z. (2019). Kiberjinoyatlar va xalqaro hamkorlik. Toshkent: O‘zbekiston Xalqaro munosabatlar universiteti.
6. Akramov, M. (2019). Xalqaro kiberjinoyatlar: Kelajakka qarab. Toshkent: O‘zbekiston ta’lim nashriyoti.
7. Anderson, R. (2017). Security Engineering: A Guide to Building Dependable Distributed Systems.
8. Baumer, C. (2018). Cybersecurity and International Cooperation in Law Enforcement.
9. Bodirov, A. (2018). Axborot xavfsizligi va kiberjinoyatlar. Toshkent: O‘zbekiston axborot texnologiyalari markazi.
10. Brenner, S. W. (2007). Cybercrime: Criminal Threats from Cyberspace.
11. Brenner, S. W. (2009). Cybercrime: A Crime of the Future?
12. Brenner, S. W., & Stuntz, A. (2013). Cybercrime: The New Frontier of Criminal Law.
13. Buchanan, B. (2018). Cybersecurity Law and Governance: A Global Perspective.
14. Chesney, R., & Citron, D. K. (2017). Defining Cybercrime and Cybersecurity Law.
15. Chisum, L., & Sorenson, E. (2014). Investigating Internet Crimes: An Introduction to Cybercrime.
16. Clark, J. (2016). The Law of Cybercrime.
17. Clough, J. (2017). Principles of Cybercrime.
18. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).

19. Davlat xavfsizligi va axborot texnologiyalari. (2018). Toshkent: O‘zbekiston Respublikasi Prezidenti huzuridagi Davlat xavfsizligi xizmatining nashriyoti.
20. Davronov, M. (2017). Kiberjinoyatlarning tahlili va ularning oldini olish. Toshkent: Yuridik maktabi.
21. Deibert, R. (2018). Access Denied: The Ethics of Cybersecurity and Digital Privacy.
22. Derrick, K. (2017). Rethinking Cybersecurity Law in the Age of Globalization.
23. Dunn Cavelty, M. (2014). Cyber-Security and Cyberwar: The Search for a Strategy.
24. Europol. (2019). Internet Organized Crime Threat Assessment (IOCTA).
25. Farxodov, A. (2019). Xalqaro huquqning kiberjinoyatlarga ta’siri. Toshkent: Yuridik ilmiy markazi.
26. Finkelstein, J. M. (2015). Internet Law: Cases and Problems.
27. G‘aniyev, N. (2018). Elektron jinoyatlar va xalqaro sud tizimi. Toshkent: O‘zbekiston huquqiy nashriyoti.
28. G‘ulomov, U. (2017). Kiberxavfsizlik va internet jinoyatlariga qarshi kurashish. Toshkent: O‘zbekiston Milliy universiteti.
29. Gibson, J. (2017). Understanding Cybercrime: A Global Perspective.
30. Goodman, S. (2019). International Law and the Fight Against Cybercrime.
31. Hackbarth, M. (2016). The Law of the Internet and Cybercrime.
32. Hasanov, U. (2019). Xalqaro hamkorlikda kiberjinoyatlarga qarshi kurashish. Toshkent: O‘zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi.
33. Heim, P. (2020). Global Cybersecurity: Challenges and Perspectives.
34. Hughes, D. (2019). Cybersecurity and the Protection of Privacy in the European Union.
35. Ibragimov, N. (2017). Kiberjinoyatlarning iqtisodiy oqibatlari. Toshkent: O‘zbekiston iqtisodiy universiteti.
36. Interpol. (2018). Cybercrime in the Age of Artificial Intelligence.
37. Ismoilov, D. (2017). Elektron jinoyatlar va ularning oldini olish. Toshkent: Yuridik fakulteti nashriyoti.

38. Jabborov, S. (2020). Kiberxavfsizlik sohasidagi xalqaro qonunlar. Toshkent: Huquqshunoslar nashriyoti.
39. Jordan, J. (2017). Privacy, Security, and Technology: The Legal Landscape.
40. Jumaniyozov, K. (2020). Axborot texnologiyalari va huquqni muhofaza qilish. Toshkent: O‘zbekiston Axborot texnologiyalari nashriyoti.
41. Kamilov, U. (2020). Kiberjinoyatlar va xalqaro yondashuvlar. Toshkent: O‘zbekiston huquqshunoslar ittifoqi.
42. Karimov, K. (2018). Xalqaro kiberjinoyatlarning rivojlanishi va unga qarshi kurash. Toshkent: Yuridik nashr.
43. Karimova, N. (2017). Kiberjinoyatlarni oldini olishda xalqaro hamkorlik. Toshkent: O‘zbekiston huquqiy universiteti.
44. Kaspersky, A. (2017). Cyber Crime: The Evolving Nature of Digital Threats.
45. Khayrullayev, A. (2020). Kiberjinoyatlarning huquqiy tahlili va ta’siri. Toshkent: O‘zbekiston Yuridik Akademiyasi.
46. Kowalski, E. (2016). Cybercrime: A Contemporary Overview.
47. Liu, W., & Wang, Y. (2018). Cybercrime and Cybersecurity: Chinese Approaches.
48. Maksudov, F. (2018). Axborot huquqi va kiberjinoyatlar. Toshkent: Yuridik huquqiy nashriyot.
49. Mansell, R. (2015). Cybercrime and Governance: Regulatory Challenges.
50. Martínez, J. (2019). Cybersecurity Law and Policy in the European Union.
51. Mavlonov, U. (2019). Kiberjinoyatlar va global xavfsizlik. Toshkent: O‘zbekiston jahon universiteti.
52. Meyer, T. (2019). The Global Impact of Cybercrime.
53. Miroshnichenko, S. (2015). Internet jinoyatlarini aniqlashda milliy qonunlarning roli. Toshkent: Yuridik universiteti nashriyoti.
54. Muhammadiev, T. (2017). Kiberjinoyatlar va ularga qarshi kurash: Xalqaro va milliy tajribalar. Toshkent: Yuqori O‘qish O‘rni.
55. Muhammedov, A. (2019). Internet jinoyatlari va ularga qarshi kurashish. Toshkent: O‘zbekiston ilmiy nashriyoti.
56. Muminov, I. (2017). O‘zbekistonda kiberjinoyatlar va ularga qarshi qonuniy choralar. Toshkent: Huquqshunoslik nashriyoti.

57. Oripov, A. (2019). Kiberjinoyatlar va ularning hukumatga ta’siri. Toshkent: Huquqiy tadqiqotlar markazi.

58. Qodirov, J. (2018). O‘zbekiston Respublikasida axborot texnologiyalari va kiberjinoyatlarni regulyatsiya qilish. Toshkent: O‘zbekiston davlat nashriyoti.

59. Qodirov, U. (2020). O‘zbekiston Respublikasi va kiberjinoyatlar. Toshkent: O‘zbekiston Yuridik akademiyasi.

60. Ravshanov, B. (2018). Xalqaro huquqda kiberjinoyatlar va internet xavfsizligi. Toshkent: O‘zbekiston milliy kutubxonasi.

61. Raxmatov, M. (2020). Kiberxavfsizlik va xalqaro hamkorlik: Yangi yondashuvlar. Toshkent: Axborot texnologiyalari.

62. Reed, C. (2019). Cybercrime and International Legal Enforcement.

63. Rizayev, A. (2019). Xalqaro huquq va kiberjinoyatlar. Toshkent: Yuridik universiteti nashriyoti.

64. Salomov, M. (2019). O‘zbekiston va Xalqaro kiberjinoyatlarga qarshi kurashish. Toshkent: Xalqaro huquqshunoslik.

65. Schneier, B. (2017). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.

66. Shadbolt, N. (2016). Artificial Intelligence and the Future of Cybersecurity.

67. Shayxov, O. (2019). Internet jinoyatlari va ularga qarshi qonuniy choralar. Toshkent: Huquqiy nashr.

68. Shodiev, F. (2016). Kiberxavfsizlik va huquqiy tartibot. Toshkent: O‘zbekiston davlat universiteti nashriyoti.

69. Shuxratov, S. (2020). O‘zbekistonda kiberjinoyatlarga qarshi chora-tadbirlar. Toshkent: Axborot texnologiyalari nashriyoti.

70. Singh, A. (2017). Cybercrime Legislation in India: Challenges and Solutions.

71. Smith, J. (2020). International Legal Frameworks on Cybercrime: A Critical Review.

72. Sodiqov, N. (2017). Xalqaro huquqdagi kiberjinoyatlar. Toshkent: O‘zbekiston yuridik institutlari.

73. Sommers, E. (2019). Digital Criminals: Trends, Prevention, and International Cooperation.

74. Stark, A. (2018). Understanding Cyberterrorism and its Impact on International Security.

75. Sullivan, J. (2016). The Ethics and Policy of Cybercrime Prevention.
76. Sultonov, F. (2017). Xalqaro kiberjinoyatlarni jinoyat deb e'tirof etishdagi huquqiy masalalar. Toshkent: O'zbekiston huquqshunoslik akademiyasi.
77. Swire, P., & Hemmings, J. (2017). The Role of International Law in Cybercrime.
78. Symantec. (2019). Internet Security Threat Report.
79. Sze, W. (2020). Cybercrime in Asia: Policies and Responses.
80. Taddeo, M., & Floridi, L. (2018). The Ethics of Cybercrime: Digital Crimes and their Legal Ramifications.
81. Toshmatov, M. (2017). Internet jinoyatlari va axborot xavfsizligi. Toshkent: Yuridik nashr.
82. Toshpulatov, D. (2020). Kiberjinoyatlarning huquqiy va iqtisodiy oqibatlari. Toshkent: Yuridik nashriyoti.
83. Tuerk, H. (2015). Cybercrime: Prevention, Detection, and Response.
84. Tursunov, J. (2016). O'zbekistonning axborot xavfsizligi sohasidagi qonuniy normativ hujjatlari. Toshkent: O'zbekiston Huquqiy instituti.
85. Tuychiyev, R. (2020). Kiberxavfsizlik va unga qarshi kurashishdagi xalqaro hamkorlik. Toshkent: O'zbekiston huquqshunoslik maktabi.
86. UNODC. (2020). Comprehensive Study on Cybercrime.
87. Weimann, G. (2019). Cyberterrorism: The New Face of War.
88. White, G. (2016). Digital Crime: The Intersection of Technology and Criminal Law.
89. Williams, P. (2015). Crime in the Digital Age: Cybercrime and its Regulation.
90. Woodward, D. (2018). The Evolution of Cybercrime and Law Enforcement's Response.
91. Xoliqov, E. (2019). O'zbekistonda kiberjinoyatlar va milliy yondashuvlar. Toshkent: O'zbekiston davlat universiteti.
92. Xudoyberganov, S. (2017). Kiberjinoyatlarning milliy va xalqaro jihatlari. Toshkent: O'zbekiston Respublikasi Milliy axborot texnologiyalari markazi.
93. Yates, J. (2020). Rethinking Cybercrime: Policy and Regulation.
94. Yusufov, J. (2018). Kiberjinoyatlar va ularning oldini olish choralari. Toshkent: O'zbekiston ilmiy-nashriyoti.

95. Yusupov, B. (2019). Raqamli xavfsizlik va axborot jinoyatlari. Toshkent: Yuridik axborot nashriyoti.

96. Yusupov, T. (2018). Internet jinoyatlari va ularni jazolash. Toshkent: Yuridik nashr.

97. Yusupova, R. (2019). Kiberjinoyatlarning huquqiy va iqtisodiy zararlari. Toshkent: O‘zbekiston iqtisodiy nashriyoti.

98. Zetter, K. (2016). Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon.

99. Ziyodullayev, A. (2020). Kiberjinoyatlar va ularning oldini olish: O‘zbekiston tajribasi. Toshkent: O‘zbekiston Yuridik Akademiyasi.

MUNDARIJA

ABDUMUTALOV BEHRUZBEK MA’RUFJONOVICH

****

XALQARO KIBERJINOYATLAR VA ULARNI JINOYAT DEB E’TIROF ETISHDAGI HUQUQIY MUAMMOLAR

MONOGRAFIYA

Muharrir: *N.Qo‘shbekov*
Dizayner: *R.Boboxonov*

****

Nashriyotga 2025-yil 23-yanvarda berildi.
Bosishga 2025-yil 29-yanvarda ruxsat etildi.
Bichimi: 84x108 1/16. Hajmi: 10,81 bosma taboq.
Times New Roman garniturasi ofset usulida chop etildi.
Buyurtma raqami: №7 Adadi: 70 dona.

“Al-Bilol” nashriyoti bosmaxonasida chop etildi.
Toshkent shahar Fayzilat ko‘chasi 34-uy