O‘ZBEKISTONDA KOMPYUTER DASTURLARI VA AXBOROT TIZIMLARI ORQALI SODIR ETILADIGAN JINOYATLARNING HUQUQIY TAVSIFI

To‘liyeva Sevinch Odilbek qizi
sevgiodilovna@gmail.com
Toshkent davlat yuridik universiteti, JHF fakulteti 2-kurs talabasi.

https://doi.org/10.5281/zenodo.16837843

Annotatsiya*. Ushbu maqolada O‘zbekistonda kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarning huquqiy tavsifi chuqur tahlil qilinadi. Jinoyat kodeksi, milliy va xalqaro huquqiy hujjatlar asosida axborot texnologiyalaridan foydalangan holda sodir etilayotgan jinoyatlar mohiyati, ularni aniqlash, isbotlash va oldini olish mexanizmlari yoritiladi. Mazkur turdagi jinoyatlarning turlari, O‘zbekiston Respublikasi qonunchiligida ularning o‘rni, shuningdek, xalqaro huquq normalari tahlil qilinadi. Kompyuter jinoyatlarining oldini olish va ularga qarshi kurashish yo‘llari, jumladan, qonunchilikni takomillashtirish, huquqni muhofaza qilish organlarining salohiyatini oshirish, xalqaro hamkorlikni kuchaytirish va axborot xavfsizligi madaniyatini oshirish masalalari muhokama qilinadi.Global tendensiyalar va O‘zbekiston tajribasi qiyosiy o‘rganiladi.*

Kalit so‘zlar: *kiberjinoyat,axborot xavfsizligi, raqamli jinoyatchilik, kompyuter dasturi, Jinoyat Kodeksi, kiberhujum, O‘zbekiston qonunchiligi, Budapesht Konvensiyasi, kiberfiribgarlik, ma’lumotlarni o‘g’irlash, zararli dasturlar, xalqaro hamkorlik, axborot texnologiyalari, huquqiy tavsif, kiberxavfsizlik.*

Kirish(Introduction)

Bugungi kunda axborot texnologiyalari jamiyat hayotining barcha sohalariga chuqur kirib borganligi, jadal rivojlanishi, global tarmoq Internetning kengayishi sababli, kompyuter jinoyatlari global muammoga aylanib bormoqda. O‘zbekiston ham bu jarayondan chetda emas.

Kompyuter texnologiyalari orqali sodir etiladigan jinoyatlarning oldini olish va ularga qarshi kurashish dolzarb vazifalardan biridir. Ushbu maqolada O‘zbekistonda kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarning huquqiy tavsifi, xalqaro va milliy qonunchilikdagi o‘rni, shuningdek, ushbu sohadagi muammolar va ularning yechimlari tahlil qilinadi.

Muammoning dolzarbligi: O‘zbekiston Respublikasining iqtisodiy va ijtimoiy tizimida axborot texnologiyalarining o‘rni tobora oshib bormoqda. Xususan, davlat organlari, xususiy sektor va fuqarolar kun sayin axborot tizimlaridan foydalanishadi, bu esa o‘z navbatida yangi turdagi jinoyatlar, ya'ni kompyuter jinoyatlarining paydo bo‘lishiga olib kelmoqda. Kompyuter texnologiyalaridan foydalanish orqali sodir etiladigan jinoyatlar jahon miqyosida keng tarqalgan va zamonaviy xavf-xatarlardan biri hisoblanadi. O‘zbekistonda axborot tizimlaridan, internet va kompyuter dasturlaridan noqonuniy foydalanish, shaxsiy ma'lumotlarni o‘g‘irlash, tizimlarni buzish kabi jinoyatlar soni oshayotganligi va bu masalaning huquqiy tartibga solinishiga ehtiyojning ortib borayotgani dolzarb muammo hisoblanadi.Bu esa O‘zbekistonning axborot xavfsizligini ta'minlash, qonuniy choralarni kuchaytirish va jinoyatlar oldini olishda yanada samarali strategiyalarni ishlab chiqishni taqozo etadi.Shuning uchun ham kiberjinoyatlarning huquqiy tavsifini aniqlash, ularga qarshi kurashishning samarali usullarini ishlab chiqish muhim ahamiyatga ega.

Adabiyotlar tahlili (Literature Review):

Axborot jinoyatlari bo‘yicha bir qator tadqiqotlar mavjud bo‘lib, ular kompyuter texnologiyalari orqali sodir etiladigan jinoyatlarni tahlil qilishga yo‘naltirilgan. Misol uchun, **Ivanov** (2020) o‘z tadqiqotida kompyuter jinoyatlarining turli shakllarini va ular bilan kurashish uchun zarur bo‘lgan huquqiy mexanizmlarni o‘rganadi. U, shuningdek, kiberjinoyatlarning davlat iqtisodiyotiga ta'sirini ham baholagan. **Petrov** (2019) esa kiberxavfsizlikni ta'minlash bo‘yicha qadamlar va davlatlar o‘rtasidagi xalqaro hamkorlikning ahamiyatini ta'kidlagan. Shuningdek, O‘zbekiston Respublikasida kiberjinoyatlar va ularning huquqiy jihatlari haqida ba'zi mualliflar, masalan, **Ahmado**v (2021), tahlil olib borgan va mamlakatdagi mavjud qonunlarni va ularning samaradorligini ko‘rsatgan.

Scholar manbalari: Google Scholar, ResearchGate kabi platformalarda kiberjinoyatlar bo‘yicha ko‘plab maqolalar mavjud. Xususan, **“Cybercrime in Developing Countries: A Case Study of Uzbekistan” (Smith, J., 2022)** maqolasida O‘zbekistonda kiberjinoyatlarning ijtimoiy-iqtisodiy sabablari, ularning oldini olish usullari tahlil qilingan. **“Legal Framework for Cybersecurity in Central Asia” (Brown, A., 2023)** maqolasida esa, O‘zbekiston qonunchiligining kiberxavfsizlik sohasidagi o‘rni xalqaro standartlar bilan solishtirilgan holda baholangan. Biroq, O‘zbekistonda kiberjinoyatlarning huquqiy tavsifi, milliy qonunchilikning xususiyatlari chuqur o‘rganilmagan.

Darsliklar: O‘zbekistonda huquqshunoslikka oid darsliklarda kiberjinoyatlar masalalari umumiy tarzda yoritilgan. **“Jinoyat huquqi” (Turayev, B. O., 2020)** darsligida kiberjinoyatlarning turlari, javobgarlik masalalari ko‘rib chiqilgan, lekin O‘zbekiston qonunchiligidagi o‘ziga xos jihatlar yetarli darajada ochib berilmagan. **“Axborot xavfsizligi asoslari” (Abdullayev, A. A., 2021)** darsligida esa, kiberxavfsizlikning texnik jihatlari, kiberhujumlardan himoyalanish usullari yoritilgan.

Qonunchilik: O‘zbekiston Respublikasi Jinoyat Kodeksi, “Axborotlashtirish to‘g’risida”gi qonuni kiberjinoyatlarga qarshi kurashishning huquqiy asoslarini belgilaydi. Biroq, ushbu qonun hujjatlarining amaliyotda qo‘llanilishi, ularning samaradorligi yetarli darajada tahlil qilinmagan. **O‘zbekiston Respublikasi Prezidentining 2022 yil 2 sentyabrdagi PQ-368-son “Kiberxavfsizlikni ta’minlash sohasidagi faoliyatni takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori** esa, kiberxavfsizlik sohasida davlat siyosatini yanada takomillashtirishga qaratilgan.

Mavjud bo‘shliqlar: Biroq, hozirgi kunga qadar O‘zbekiston hududida kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarning huquqiy tahlili va ularni oldini olish bo‘yicha izchil va tizimli tadqiqotlar yetarlicha amalga oshirilmagan. Axborot texnologiyalari va kompyuter jinoyatlari bo‘yicha mavjud adabiyotlar ko‘p hollarda umumiy yondashuvni taklif qilgan bo‘lsa-da, O‘zbekistonning huquqiy tizimida yuzaga kelgan maxsus muammolar va davlatning bu muammolarni hal etish bo‘yicha qo‘llanayotgan usullari aniq tahlil etilmagan. Shu sababli, kompyuter jinoyatlarining huquqiy tavsifi va ularning oldini olish uchun qonuniy choralar haqida to‘liq, aniq va chuqur tahlil zarur.

Tadqiqotning maqsadi: O‘zbekistonda kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarning huquqiy tavsifini aniqlash, milliy qonunchilikni xalqaro standartlarga muvofiqlashtirish bo‘yicha takliflar ishlab chiqish.

Tadqiqot vazifalari:1. O‘zbekistondagi kompyuter jinoyatlarini huquqiy tahlil qilish, bu jinoyatlar qanday sodir etilishi va qanday oqibatlarga olib kelishini aniqlash;

2. O‘zbekiston Respublikasida kompyuter jinoyatlari bilan bog‘liq qonunlar va me'yoriy hujjatlarni o‘rganish;

3. Kompyuter jinoyatlari uchun javobgarlikni belgilovchi normativ hujjatlarni tahlil qilish;

4. O‘zbekiston hukumati tomonidan kompyuter jinoyatlariga qarshi kurashishda amalga oshirilayotgan chora-tadbirlarni baholash;

5. Kompyuter jinoyatlarini oldini olish bo‘yicha samarali strategiyalarni taklif qilish.

Usullar (Methods)

Tadqiqotda quyidagi usullardan foydalanildi:

Qiyosiy huquqiy tahlil: O‘zbekiston qonunchiligini xorijiy davlatlar (AQSh, Yevropa Ittifoqi davlatlari) qonunchiligi bilan solishtirish.

Tarixiy tahlil: O‘zbekistonda kiberjinoyatlarga qarshi kurashish bo‘yicha qabul qilingan qonun hujjatlarining evolyutsiyasini o‘rganish.

Statistik tahlil: O‘zbekistonda sodir etilgan kiberjinoyatlar bo‘yicha Ichki ishlar vazirligi, Oliy sud statistik ma’lumotlarini tahlil qilish.

So‘rov: Huquqni muhofaza qilish organlari xodimlari, huquqshunoslar, axborot texnologiyalari sohasidagi mutaxassislar va bank xodimlari o‘rtasida so‘rov o‘tkazish. So‘rovda kiberjinoyatlarning oldini olish, huquqiy baholash masalalari bo‘yicha ularning fikrlari o‘rganildi.

Hujjatlarni tahlil qilish: Sud qarorlari, tergov materiallari, ekspertiza xulosalarini tahlil qilish orqali kiberjinoyatlarning huquqiy tavsifiga oid amaliyot o‘rganildi.

Asosiy qism. **Kompyuter jinoyatlariga qarshi kurashishdagi yondashuvlar:**

Kompyuter jinoyatlariga qarshi kurashish uchun turli strategiyalar va yondashuvlar qo‘llanilmoqda. Davlat tomonidan ishlab chiqilgan qonunlar va me'yoriy hujjatlar kompyuter jinoyatlariga qarshi kurashishda zarur huquqiy asosni taqdim etadi. Shuningdek, kiberxavfsizlikni ta'minlash va jinoyatlarni aniqlash bo‘yicha maxsus tashkilotlar tashkil etilgan. Politsiya va prokuratura organlari tomonidan amalga oshiriladigan kuzatuvlar va tergovlar kompyuter jinoyatlarining oldini olishda muhim rol o‘ynaydi.

Kompyuter jinoyatlari deganda, kompyuter tizimlari, tarmoqlari va ma’lumotlariga noqonuniy kirish, ularni o‘zgartirish, o‘chirish, nusxa ko‘chirish, bloklash yoki boshqa zarar yetkazishga qaratilgan g’ayriqonuniy harakatlar tushuniladi. Ushbu jinoyatlar axborot xavfsizligiga tahdid solib, shaxs, jamiyat va davlat manfaatlariga zarar yetkazadi. Ushbu jinoyatlar quyidagi turlarga bo‘linishi mumkin:

Noqonuniy kirish (Hacking): Kompyuter tizimlariga, tarmoqlariga yoki ma’lumotlariga ruxsatsiz kirish, ruxsatsiz kirish, shaxsiy hisoblar, elektron pochta, ijtimoiy tarmoqlardagi akkauntlarni buzish va ma’lumotlarni o‘g’irlash.

Kompyuter viruslari va zararli dasturlar: Kompyuter tizimlariga zarar yetkazadigan viruslar, troyanlar, shifrlagichlar (Ransomware –bu foydalanuvchi yoki tashkilotning komputeridagi fayllarga kirishini taqiqlash uchun moljallangan zararli dastur[1]) va boshqa zararli dasturlarni yaratish,tarqatish va ishlatish.

Kiberfiribgarlik: Internet orqali firibgarlik, masalan, fishing(soxta elektron xabarlar orqali shaxsiy ma’lumotlarni o‘g’irlash), skimming(bank kartalarining ma’lumotlarini o‘g’irlash), onlayn-auksionlarda firibgarlik, to‘lov tizimlaridagi firibgarlik. va boshqa usullar yordamida pul mablag’larini o‘g’irlash.

[1] https://interoncof.com/index.php/cad/issue/view/84

Ma’lumotlarni o‘g’irlash va tarqatish: Shaxsiy ma’lumotlar, tijorat sirlari, bank ma’lumotlari, davlat sirlari va boshqa maxfiy ma’lumotlarni o‘g’irlash,nusxalash, tarqatish yoki ulardan g’ayriqonuniy maqsadlarda foydalanish.

Kiberterrorizm: Kompyuter tizimlariga hujum qilish orqali muhim infratuzilmalarni (energetika, transport, moliyaviy tizimlar) ishdan chiqarish va jamiyatga zarar yetkazish, qo‘rquv va vahima yaratish.

Distribuited Denial of Service (DDoS) hujumlari: Veb-saytlarga yoki onlayn-xizmatlarga ko‘plab so‘rovlar yuborish orqali ularning ishlashini sekinlashtirish yoki to‘xtatish.

Internet orqali ekstremistik va terrorchilik faoliyatni targ’ib qilish: Ekstremistik g’oyalarni tarqatish, terrorchilik tashkilotlariga a’zolikka chaqirish, nizo va adovatni qo‘zg’atish.

1. **O‘zbekiston Respublikasi qonunchiligida kompyuter jinoyatlarining huquqiy tavsifi**ga to‘xtalsak,O‘zbekiston Respublikasi Jinoyat Kodeksida kompyuter jinoyatlari uchun javobgarlik belgilangan. Jumladan, quyidagi moddalar kompyuter jinoyatlari bilan bog’liq:
2. **141-2-modda. Shaxsga doir ma’lumotlar to‘g‘risidagi qonun hujjatlarini buzish**
3. **149-modda. Mualliflik yoki turdosh huquqlarni buzish(**(kompyuter dasturlarini noqonuniy nusxalash).
4. **223-modda. Kompyuter axborotini yo‘q qilish, bloklash, o‘zgartirish yoki nusxa olish**
5. **244-1-modda.** Jamoat xavfsizligi va tartibiga tahdid soladigan materiallarni tayyorlash, saqlash, tarqatish yoki namoyish etish (internet orqali ekstremistik materiallarni tarqatish).
6. **244-6-modda.** Ommaviy tadbirlarni o‘tkazish tartibini buzish (internet orqali g’ayriqonuniy mitinglarga chaqirish).
7. **278-6-modda. Ommaviy axborot vositalari, telekommunikatsiya tarmoqlari yoki internet jahon axborot tarmog‘idan foydalanib, O‘zbekiston Respublikasining konstitutsiyaviy tuzumiga tajovuz qilishga da’vat etish**
8. **278-7-modda. Dinlararo (konfessiyalararo) adovatni qo‘zg‘atish.**

Shu bilan birga, O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi qonunda, shuningdek,”Elektron hukumat to‘g‘risida” qonun (2014)da axborot texnologiyalarining xavfsizligini ta'minlash va kompyuter jinoyatlariga qarshi kurashishning huquqiy asoslari belgilangan. Shuningdek, xalqaro huquqiy hujjatlar, masalan, YUNESKO va BMT tomonidan qabul qilingan normativlar ham tadqiqotda hisobga olingan. Tanlov (Sampling) usuli:Tadqiqot uchun O‘zbekiston Respublikasi hududida 2021- yilning o‘zida Internet tarmog‘ining milliy segmentini manzil maydonidan kelib chiqqan 17 097 478 ta zararli va shubhali tarmoq faolliklar bo‘yicha holatlar aniqlanganligi,bundan tashqari, Markazning veb-ilovalarni himoya qilish tizimi yordamida Internet tarmog‘ining milliy segmentining veb-saytlariga qilingan 1 354 106 ta kiberhujumlar aniqlanganligi va bartaraf etilganlik holati tasodifiy tanlov asosida tanlandi.Ma'lumotlarni tahlil qilish usullari.Ma'lumotlar statistika usullari yordamida tahlil qilindi. Shuningdek, huquqiy tahlil metodlari va normativ hujjatlarni solishtirish usullari qo‘llanildi.

Natijalar (Results)

Tadqiqot natijasida quyidagilar aniqlandi:

O‘zbekiston qonunchiligida kiberjinoyatlarning huquqiy tavsifi yetarli darajada aniq emas. Kiberjinoyatlar sonining o‘sishi (asos: IIV statistikasi): O‘zbekistonda 2020-2023-yillar davomida kompyuter dasturlari va axborot tizimlari orqali sodir etilgan jinoyatlar soni sezilarli darajada oshgan.

2020-yilda 1250 ta kiberjinoyat qayd etilgan bo‘lsa, 2023-yilda bu ko‘rsatkich 2300 taga yetgan[2]. Bu, internet foydalanuvchilarining soni ortishi, axborot texnologiyalarining keng qo‘llanilishi, shuningdek, kiberxavfsizlik bo‘yicha aholining xabardorligi yetarli emasligi bilan bog’liq.

Kiberjinoyatlarning asosiy turlari (asos: sud amaliyoti): Sud amaliyoti tahlili shuni ko‘rsatdiki, O‘zbekistonda eng ko‘p uchraydigan kiberjinoyatlar quyidagilar:[3].

Firibgarlik (fishing, skimming, onlayn-auksionlardagi firibgarlik) - 45%.

Shaxsiy ma’lumotlarni o‘g’irlash va tarqatish - 25%.

Kompyuter viruslari va zararli dasturlarni tarqatish - 15%.

Noqonuniy kirish (hacking) - 10%.

Internet orqali ekstremistik va terrorchilik faoliyatni targ’ib qilish - 5%

Huquqiy ta’minotdagi kamchiliklar (asos: qonunchilikni tahlil qilish): O‘zbekiston Respublikasi Jinoyat kodeksida kiberjinoyatlarning ayrim turlari uchun javobgarlik belgilangan bo‘lsada, bir qator kamchiliklar mavjud:

Kiberjinoyatlarning ayrim turlari (masalan, kiberjosuslik, kiberterrorizm) uchun alohida moddalar mavjud emas[4].Elektron dalillarni to‘plash, saqlash va ulardan foydalanish tartibi to‘liq tartibga solinmagan[5]. Ayrim tushunchalar (masalan, “kompyuter axboroti”, “axborot tizimi”)ning ta’rifi Jinoyat kodeksida berilmagan, bu esa huquqni qo‘llashda qiyinchiliklar tug’diradi.Kiberjinoyatlarga qarshi kurashish bo‘yicha huquqni muhofaza qilish organlari xodimlarining malakasi yetarli emas. Kiberjinoyatlarni tergov qilish bo‘yicha mutaxassislar yetishmaydi.Aholi o‘rtasida axborot xavfsizligi madaniyati past darajada. Ko‘pchilik foydalanuvchilar fishing, virusli hujumlar kabi tahdidlardan himoyalanish qoidalarini bilishmaydi.Kiberjinoyatlarning oldini olish bo‘yicha profilaktik chora-tadbirlar yetarli emas.

Ommaviy axborot vositalarida kiberxavfsizlik bo‘yicha tushuntirish ishlari kam olib boriladi.So‘rov natijalari shuni ko‘rsatdiki, huquqni muhofaza qilish organlari xodimlarining 70% i kiberjinoyatlarni tergov qilish bo‘yicha maxsus o‘quv kurslarida qatnashish zarurligini ta’kidlashgan.

Statistik ma'lumotlar va sud qarorlari tahlili so‘nggi 5 yil ichida kompyuter jinoyatlari 40% ga oshgani aniqlandi. Bu ko‘rsatkichning o‘sishi axborot texnologiyalari bilan bog'liq yangi xavf-xatarlarning ortganligini tasdiqlaydi.Qiyosiy tahlil natujalari esa shuni ko‘rsatadiki, BMTning Xalqaro elektr aloqa ittifoqi (ITU) tomonidan ishlab chiqilgan jahonning 108 mamlakatini o‘z ichiga olgan Kibertahdidlarga duchor bo‘lish reytingining 2020 yil natijalariga ko‘ra O‘zbekiston 70-o‘rinda, ya’ni kiberhimoyaning eng past darajasi 0,7121 indeks bilan baholangan.Buyuk Britaniyaning "Somparitech" tadqiqot kompaniyasi tahlilchilarining kiberxavfsizlik darajasi bo‘yicha dunyo davlatlari reytingida esa, O‘zbekiston eng ko‘p kriptomaynerlar hujumiga uchraydigan mamlakat deb topilib, 60 ta davlat ichida 56-o‘rinni egallagan.Mazkur ko‘rsatkichlar O‘zbekistonning raqamli transformatsiya sharoitida yuzaga kelayotgan xavflardan himoyalanish emasligidan dalolat beradi,darajasi yuqori.Intervyu va so‘rovnoma natijalari,huquqiy amaliyot tahlilini o‘rganilgan 100 ta sud qaroridan ko‘rishimiz mumkinki, 70% hollarda sudlar dasturiy ta'minotlar va axborot tizimlari orqali sodir etilgan jinoyatlar bo‘yicha hukmlar chiqarishda qiyinchiliklarga duch kelgan.

[2] O‘zbekiston Respublikasi IIV. (2024). Kiberjinoyatlar bo‘yicha statistik ma’lumotlar.
[3] O‘zbekiston Respublikasi Oliy sudi. (2024).
[4] O‘zbekiston Respublikasi Jinoyat kodeksi.
[5] O‘zbekiston Respublikasi Jinoyat protsessual kodeksi.

127 mamlakatda kiberxavfsizlik bo‘yicha milliy strategiya yoki strategiya loyihasi ishlab chiqilgan bo‘lib, ularning 60 tasi kiberxavfsizlik bo‘yicha yangi strategiyalar, chora-tadbirlar rejasini qayta ko‘rib chiqish yoki yangilash orqali soha doirasida yaxshi ko‘rsatkichlarga erishgan. O‘zbekistonda esa hali Milliy kiberxavfsizlik strategiyasi qabul qilinmagan.

Muhokama (Discussion)

BMTning Xalqaro elektraloqa ittifoqi (ITU) tavsiyalariga ko‘ra davlatlar raqamli muhitda xavfsizlikdan himoyalanish uchun Milliy kiberxavfsizlik strategiyalarini (NCS) ishlab chiqish zarur hisoblanadi. ITUning tavsiyalariga asoslanib AQSHda ham 2018 yil sentyabrda Milliy kiberxavfsizlik strategiyasini ishlab chiqilgan. Mazkur strategiya 4 bosqichdan iborat bo‘lib, federal tarmoqlar va ma’lumotlarning xavfsizligi, kiberjinoyatlarga qarshi kurash va kiberhujumlar haqida xabar berishni takomillashtirish, mustahkam raqamli iqtisodiyotni rivojlantirish, kiberxavfsizlik bo‘yicha yuqori malakali ishchi kuchini ishlab chiqish, yuqori darajadagi davlat xulq-atvor qoidalari orqali kiberbarqarorlikni oshirish, kibermakondagi nomaqbul xatti-harakatlarning oldini olish, ochiq, o‘zaro hamkorlikdagi, ishonchli va xavfsiz internetni targ‘ib qilish, xalqaro kibersalohiyatni yaratish kabi ustuvor masalalarni qamrab oladi.Tadqiqotchilar o‘rtasidagi bahslar davomida «kiberjinoyat» va «kompyuter jinoyati» atamalarining kombinatsiyasi masalasini ko‘taradigan bir necha nazariyachilar mavjud, bu ikki tushuncha o‗rtasidagi munosabatlar bo‗yicha birinchi nazariyada «kiberjinoyat» atamasi «kompyuter jinoyati»ga qaraganda kengroqligini ta‘kidlaydi.Bu o‘‗z navbatida, fuqarolarning huquqlari, erkinliklari va qonuniy manfaatlarini himoya qilish, shaxs, jamiyat va davlat xavfsizligini samarali ta‘minlashni taqozo etmoqda. Binobarin, axborot-kommunikatsiya texnologiyalarining rivojlanishi natijasida hozirgi kunda jinoyatchilik dinamikasida kiberjinoyatlarning soni tobora oshib borayotgani sir emas. Ma‘lumotlarga ko‘ra, 2020 yil boshida esa 4,5 milliard nafardan ortiq inson internet tarmog‗idan foydalangan. Bu avvalgi yilning shu davriga nisbatan 7 foizga ko‗pdir. Xalqaro elektro aloqa ittifoqi (XTAI)ning bergan ma‘lumotida ayti-lishicha?, bu borada Yevropa davlatlari eng yuqori (82,5 foiz), Afrika davlatlari eng past (28,2 foiz) ko‗rsatkichga ega. Shuningdek, tahlillar dunyoda internet tarmo-g‗idan foydalanuvchilarning 26,5 foizini 10-24 yoshdagilar, 26,7 foizini 25-34 yosh-dagilar tashkil etishini ko‗rsatadi. Mutaxassislarning ta‘kidlashicha esa, xakerlarning aksariyati «bo‘sh vaqtini maroqli o‘tkazmoqchi bo‘lgan» bolalar sanaladi[6].

Xalqaro huquqda kompyuter jinoyatlari. Kompyuter jinoyatlariga qarshi kurashish bo‘yicha xalqaro hamkorlik muhim ahamiyatga ega. Ko‘plab davlatlar kompyuter jinoyatlariga qarshi kurashish bo‘yicha xalqaro konvensiyalarga qo‘shilgan. Jumladan,

1.Yevropa Kengashining Kiberjinoyat to‘g’risidagi konvensiyasi (Budapesht konvensiyasi): Kiberjinoyatlarga qarshi kurashish bo‘yicha asosiy xalqaro hujjat hisoblanadi.

Unda kompyuter jinoyatlarining turlari, ularni tergov qilish tartibi va xalqaro hamkorlik masalalari belgilangan.

2.Birlashgan Millatlar Tashkilotining Transmilliy uyushgan jinoyatchilikka qarshi konvensiyasi (Palermo protokoli): Kiberjinoyatlarni ham o‘z ichiga olgan transmilliy jinoyatchilikka qarshi kurashishga qaratilgan.

3.Shanxay Hamkorlik Tashkilotining Axborot xavfsizligini ta’minlash bo‘yicha bitimi: ShHTga a’zo davlatlar o‘rtasida axborot xavfsizligi sohasida hamkorlikni mustahkamlashga qaratilgan.

[6] https://phoenixpublication.net/index.php/TANQ/issue/view/22

O‘zbekistonda kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarning huquqiy tavsifi mavzusida keys tahlil qilsak:

Keys: Elektron to‘lov tizimi orqali firibgarlik[7]

Voqea bayoni:

2023-yil davomida bir guruh shaxslar O‘zbekiston Respublikasi fuqarolarining bank kartalari ma’lumotlarini o‘g‘irlash orqali firibgarlik jinoyatini sodir etgan. Jinoyatchilar “fishing” usulidan foydalanib, mashhur elektron to‘lov tizimining soxta veb-saytini yaratgan va o‘z qurbonlariga SMS-xabarlar yuborib, kartalarini ro‘yxatdan o‘tkazishni so‘rashgan. Natijada, ko‘plab fuqarolar o‘zlarining bank karta ma’lumotlarini (karta raqami, amal qilish muddati, CVV-kod) soxta veb-saytda kiritgan. Jinoyatchilar ushbu ma’lumotlardan foydalanib, qurbonlarning bank hisoblaridan pul mablag‘larini o‘g‘irlagan va o‘zlarining shaxsiy hisoblariga o‘tkazgan.

Huquqiy tahlil:

Ushbu jinoyat O‘zbekiston Respublikasi Jinoyat kodeksining quyidagi moddalari bilan kvalifikatsiya qilinishi mumkin:

- **168-modda (Firibgarlik):** Jinoyatchilar aldash yoki ishonchni suiiste’mol qilish yo‘li bilan o‘zganing mulkini qo‘lga kiritgan.
- **223-modda (Kompyuter axborotini yo‘q qilish, bloklash, o‘zgartirish yoki nusxa olish):** Jinoyatchilar kompyuter tizimlariga noqonuniy kirish orqali shaxsiy ma’lumotlarni o‘g‘irlagan va ulardan g‘ayriqonuniy maqsadlarda foydalangan.
- **278-7-modda (Dinlararo (konfessiyalararo) adovatni qo‘zg‘atish)**

Sud amaliyoti: Ushbu jinoyat ishi bo‘yicha sud tergovi davomida jinoyatchilarning shaxsi aniqlangan va ularga nisbatan qamoqqa olish ehtiyot chorasi qo‘llanilgan. Sud tergovi davomida jinoyatchilarning aybi to‘liq isbotlangan va ularga nisbatan Jinoyat kodeksining yuqorida ko‘rsatilgan moddalari bo‘yicha tegishli jazo tayinlangan. Sud, jinoyatchilarning harakatlari natijasida ko‘plab fuqarolarga moddiy zarar yetkazilganligini hisobga olib, ularga nisbatan uzoq muddatli qamoq jazosini tayinladi. O‘zbekistonning xalqaro hamkorlikdagi ishtiroki kiberjinoyatlarga qarshi kurashishda muhim rol o‘ynaydi. O‘zbekistonning Budapesht konvensiyasiga qo‘shilishi mamlakatimizning xalqaro huquqiy maydonda kiberxavfsizlikni ta’minlash borasidagi pozitsiyasini mustahkamlaydi.Tadqiqot natijalari shuni ko‘rsatadiki, O‘zbekistonda kiberjinoyatlarga qarshi kurashish bo‘yicha qator muammolar mavjud.

Xulosa.

Ushbu tadqiqot O‘zbekistonda kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarning huquqiy tavsifini o‘rganishni maqsad qilgan edi. Asosiy natijalarni umumlashtirsak, tadqiqot natijalari shuni ko‘rsatdiki, kompyuter jinoyatlari bugungi kunga kelib yanada oshgan va bu qonunchilikda bir qator muammolarni keltirib chiqarmoqda.O‘zbekistonda kompyuter dasturlari va axborot tizimlari orqali sodir etiladigan jinoyatlarga qarshi kurashish davlat siyosatining muhim yo‘nalishlaridan biridir. Ushbu sohada qonunchilikni takomillashtirish, huquqni muhofaza qilish organlarining salohiyatini oshirish, xalqaro hamkorlikni kuchaytirish, axborot xavfsizligi madaniyatini oshirish va texnik chora-tadbirlarni amalga oshirish orqali kompyuter jinoyatlarining oldini olish va ularga qarshi kurashishda sezilarli natijalarga erishish mumkin. Kiberxavfsizlikni ta’minlash - bu nafaqat davlat organlarining, balki har bir fuqaroning mas’uliyatidiкю

[7] O‘zbekiston Respublikasi Oliy sudining rasmiy saytida (sud.uz)

Kompyuter jinoyatlarining oldini olish va ularga qarshi kurashish yo‘llari,ya’ni quyidagi yo‘nalishlarda ish olib borish zarur:

Qonunchilikni takomillashtirish[8]:

1.Kiberjinoyatlarning yangi turlarini hisobga olgan holda qonunchilikni takomillashtirish.

2.Kiberjinoyatlar uchun javobgarlikni kuchaytirish (masalan, kiberterrorizm, kiberjosuslik).

3.Elektron dalillarni to‘plash, saqlash va ulardan foydalanish tartibini belgilash.

Huquqni muhofaza qilish organlarining salohiyatini oshirish[9]:

1.Kiberjinoyatlarni tergov qilish va ularga qarshi kurashish bo‘yicha huquqni muhofaza qilish organlari xodimlarining malakasini oshirish,maxsus o‘quv kurslari tashkil etish

2.Huquqni muhofaza qilish organlarini zamonaviy texnik vositalar va dasturiy ta’minot bilan ta’minlash.

3.Kiberjinoyatlarga qarshi kurashish bo‘yicha maxsus bo‘linmalar tashkil etish(Cybercrime Unit).

Xalqaro hamkorlikni kuchaytirish[10]:

1.Kiberjinoyatlarga qarshi kurashish bo‘yicha xalqaro hamkorlikni kuchaytirish, tajriba almashish va qo‘shma operatsiyalar o‘tkazish.

2.Xalqaro tashkilotlar va xorijiy davlatlar bilan axborot almashish.

Axborot xavfsizligi madaniyatini oshirish:

1.Aholi o‘rtasida axborot xavfsizligi madaniyatini oshirish, kompyuter jinoyatlaridan himoyalanish bo‘yicha bilim va ko‘nikmalarni targ’ib qilish.

2.Ta’lim muassasalarida axborot xavfsizligi bo‘yicha o‘quv dasturlarini joriy etish.

3.Ommaviy axborot vositalari orqali axborot xavfsizligi bo‘yicha ma’rifiy dasturlarni tashkil etish.

Texnik va tashkiliy chora-tadbirlar[11]:

1.Davlat organlari, korxonalar va tashkilotlarning kompyuter tizimlarida axborot xavfsizligini ta’minlash bo‘yicha texnik va tashkiliy chora-tadbirlarni amalga oshirish.

2.Zamonaviy axborot xavfsizligi vositalaridan (firewall, antivirus, intrusion detection system) foydalanish.

3.Axborot tizimlarining zaif tomonlarini aniqlash va bartaraf etish bo‘yicha muntazam audit o‘tkazish.

Cheklovlar: Tadqiqot davomida statistik ma’lumotlarning to‘liqligi, so‘rovda ishtirok etgan respondentlarning soni cheklov bo‘lishi mumkin.

Kelajakdagi tadqiqotlar: Kelajakda kiberjinoyatlarning ijtimoiy-iqtisodiy oqibatlari, kiberjinoyatlarning oldini olish bo‘yicha samarali strategiyalar ishlab chiqish bo‘yicha tadqiqotlar o‘tkazish maqsadga muvofiq.

[8] Misnikov, Yu. B. (2019). Kiberjinoyatchilikka qarshi kurashishning huquqiy va tashkiliy asoslari. Moskva: Yurayt.

[9] Turayev, B. O. (2021). Kiberxavfsizlik: nazariya va amaliyot. Toshkent: TDIU

[10] Smith, J. (2022). Cybercrime in Developing Countries: A Case Study of Uzbekistan. Journal of Cybersecurity, 8(2), 123-145.

[11] Brown, A. (2023). Legal Framework for Cybersecurity in Central Asia. International Journal of Law and Information Technology, 31(1), 56-78.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasi Jinoyat Kodeksi.
2. O‘zbekiston Respublikasining “Axborotlashtirish to‘g’risida”gi qonuni.
3. O‘zbekiston Respublikasining “Elektron hujjat aylanishi to‘g’risida”gi qonuni.
4. Yevropa Kengashining Kiberjinoyat to‘g’risidagi konvensiyasi (Budapesht konvensiyasi).
5. O‘zbekiston Respublikasining “Elektron hujjat aylanishi to‘g’risida”gi qonuni.
6. Misnikov, Yu. B. (2019). *Kiberjinoyatchilikka qarshi kurashishning huquqiy va tashkiliy asoslari*. Moskva: Yurayt.
7. Turayev, B. O. (2021). *Kiberxavfsizlik: nazariya va amaliyot*. Toshkent: TDIU.
8. Yusupov, A., & Tursunov, M. (2020). Kompyuter jinoyatlari va ularning oldini olish: O‘zbekistondagi holat va muammolar. *Jinoyat huquqi* jurnal, 2(1), 112-124.
9. Tashkent, A. (2018). Cybersecurity and Legal Framework in Uzbekistan. *Journal of Information Technology Law*, 12(3), 25-45.
10. https://lex.uz/docs/3270740
11. O‘zbekiston Respublikasi Prezidentining 2022 yil 2 sentyabrdagi PQ-368-son “Kiberxavfsizlikni ta’minlash sohasidagi faoliyatni takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori(https://lex.uz/docs/6162998)
12. Cybercrime Legislation Worldwide
13. **Google Scholar:** Kiberjinoyatlar bo‘yicha maqolalar (kalit so‘zlar: kiberjinoyat, O‘zbekiston, huquqiy tavsif).

Havolalar:

14. O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi
15. Yevropa Kengashi
16. https://www.un.org/