O‘ZBEKISTONDA ELEKTRON TO‘LOV TIZIMLARI ORQALI SODIR ETILADIGAN FIRIBGARLIKLARNING HUQUQIY TAVSIFI

Buriyeva Mohina Muxiddin qizi
Toshkent davlat yuridik universiteti
Jinoiy odil sudlov fakulteti 2-kurs “B” potok talabasi.
mohinaburiyeva1501@gmail.com
https://doi.org/10.5281/zenodo.16837497

Annotatsiya. *Ushbu tadqiqot zamonaviy raqamli dunyoda elektron to‘lov tizimi orqali sodir etilayotgan firibgarlikning huquqiy tavsifiga bag‘ishlangan. Maqolada kiberjinoyat tushunchasi, kiberfiribgarlik va ularning turlari, kriminalistik elementlari, uni oldini olishga qaratilgan chora-tadbirlar, qabul qilingan milliy qonunchilik hujjatlari hamda xalqaro standartlar tahlil qilingan. Shuningdek, maqolada kibermakonda yuzaga keladigan muammomalar tizimli, huquqiy, ilmiy-amaliy tahlil qilingan.*

Kalit so‘zlar: *Kibermakon, kiberjinoyat, kiberxavfsizlik, elektron to‘lov tizimlari, kiberfiribgarlik, kriminalistik elementlar, raqamlashtirish, ma’lumotlar xavfsizligi.*

KIRISH

Zamonaviy, raqamli texnologiyalar asrida yashar ekanmiz, bugungi kunda raqamlashtirish jarayoni shiddat bilan rivojlanib, deyarli barcha sohalarga kirib bormoqda.

Jumladan ilm-fan, ishlab chiqarish, xizmat ko‘rsatish shuningdek, davlat boshqaruv sohasiga ham sezilarli darajada muaayyan o‘zgarishlarga sabab bo‘lmoqda. Hattoki, pensiya, nafaqa, oylik maosh olish, turli xil kommunal to‘lovlar, soliq va kundalik faoliyatda barcha to‘lovlarni amalga oshirishda, elektron to‘lov tizimi orqali hech qanday qiyinchiliklarsiz to‘lov qilish imkoniyati vujudga keldi. Natijada, naqd to‘lovlarisiz moliyaviy hisob-kitoblarni amalga oshirish bugungi kunda eng samarali usul bo‘lib qolmoqda. Elektron to‘lovlar qanchalik mukammal ko‘rinmasin uning bir necha kamchiliklari va nuqsonlari bo‘lishi tabiiy, albatta.

Jumladan, elektron to‘lovlar insoniyat hayotini yengillashtirgan bo‘lsa-da, kiberjinoyatchilikning eng muhim turlaridan bo‘lgan kiberfiribgarlikning ham rivojlanishiga imkoniyat yaratdi. Bugungi kunda kompyuter texnologiyalari va elektron qurilmalar orqali sodir etilayotgan ushbu firibgarlik kundan kunga ko‘payib bormoqda. Ma’lumki, ko‘plab dunyo mamlakatlarida ushbu kiberjinoyatchilikni oldini olishga qaratilgan mukammal tizim ishlab chiqilmagan. Bu esa jabrlanuvchilar sonining oshishiga va ko‘plab kiberjinoyatchilik ishlarini ochilmay qolishiga sabab bo‘lmoqda. Biz elektron to‘lov tizmi orqali sodir etilayotgan firibgarlik turlari, unng kriminalistik elementlarini tahlil qilgan holda, ushbu kiberfiribgarlikning oldini olishga qaratilga bir necha takliflar berishga harakat qilamiz.

METODOLOGIYA

Ushbu maqolada biz **birinchidan,** raqamlashtirish jarayoni jadal rivojlanishi uchun elektron to‘lov tizimini keng targ‘ib qilinishi, uning bugungi kundagi ahamiyati, u orqali yartilayotgan imkoniyatlar va qulayliklar haqida ekspertlarning tadqiqotlar orqali tahlil qildik.

Ikkinchidan, kibermakonda sodir etilayotgan kiberjinoyatchilikning cheksiz tabiati, turlari va uni sodir etishda ilg‘or texnologiyalar ya’ni elektron qurilmalardan foydalishning o‘ziga xos xususiyatlari, kiberjinoyatchilkka oid statistika ma’lumotlori ko‘plab ilmiy tadqiqotlar va rasmiy saytlardan olingan ma’lumotlar asosida tahlil qilishga harakat qildik.

Uchinchidan, kiberjinoyatning bir turi sifatida kiberfiribgarlik tushunchasi va uning an’anaviy firibgarlik jinoyati bilan farqli va o‘xshash jihatlari, kiberfiribgarlikning bir necha

turlarini milliy qonunchilik normalari va ekspertlar tomonidan tayyorlangan ilmiy maqolalarni tahlil qilib ko‘rib chiqdik.

To‘rtinchidan, kiberxavfsizlik tushunchasiga, shuningdek, kiberxavfsizlikning bugungi zamonaviy axborot texnologiyalari rivojlangan kibermakonda shaxs, jamiyat va davlat manfaatlarida ta’minlashda tutgan ahamiyatini O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi qonun va xalqaro huquqiy hujjatlar asosida tahlil amalga oshirdik.

Beshinchidan, elektron to‘lov tizimi orqali sodir etilayotgan kompyuter firibgarligini oldini olishga qaratilgan shaxsiy takliflar taqdim etishga harakat qildik.

NATIJA

Endilikda kiberjinoyat aslida nima ekanligini turli qarashlar bilan tahlil qilib o‘tamiz.

Kiberjinoyatchilik - axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi [1] . Kibermakon deganda, axborot texnologiyalari orqali yaratiladigan muhitni tushunishimiz mumkin.

Shuningdek, **L.Bo‘ronovning fikricha**, “Kiberjinoyatchilik tushunchasi axborot-kommunikatsiya texnologiyalari sohasidagi ko‘plab turdagi jinoyatlarni o‘zida birlashtirgan.

Virtual taqrmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, mualliflik huquqini buzish, kredit kartochkalari raqami va bank rekvizitlarini o‘g‘irlash hamda boshqa turli huquqbuzarliklar shular jumlasidandir”[2].

Yuqoridagi fikr mulohazalar asosida aytishimiz mumkinki, kiberjinoyat raqamli dunyoda sodir etilib, kompyuter, telefon yoki boshqa elektron qurilmalar orqali amalga oshiriladi. Hamda elektron tizimlarni buzib kirish, pul va shaxsiy ma’lumotlarni qo‘lga kiritish ularni o‘zgartirish yoki butkul o‘chirib tashlashni o‘z ichiga oladi. Kiberjinoyatchilikning turlariga quyidagilarni misol sifatida aytishimiz mumkin:

Shaxsiy ma’lumotlarni o‘g‘irlash - internet foydalanuvchilarining shaxsiy va moliyaviy ma'lumotlarini o'g'irlash uchun ishlatiladigan turli xil hujumlar, masalan, phishing (soxta xat yoki saytlar orqali), viruslar va zararli dasturlar.

Kiberfiribgarlik – kiberjinoyatchilar tomonidan bank tizimlariga yoki shaxslarning moliyaviy hisob raqamlariga soxta veb-saytlar oqali kirib moliyaviy zarar keltiradi. Ushbu kiberjinoyatchilik turini keyingi o‘rinlarda batafsil tahlil qilamiz.

Kiberjinoyatchilikning eng muhim turlaridan biri bo‘lgan **kiberfiribgarlik** tushunchasini tahlil qilar ekanmiz, avvalo firibgarlik nima ekanligini bilib olishimiz darkor. **O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasiga muvofiq, firibgarlik,** ya’ni aldash yoki ishonchni suiiste’mol qilish yo‘li bilan o‘zganing mulkini yoki o‘zganing mulkiga bo‘lgan huquqni qo‘lga kiritishdir[3].

Kiberfiribgarlik esa virtual dunyoda internet, telefon, kompyuter, elektron dastur va boshqa raqamli texnologiyalar asosida amalga oshirilib, an’anaviy firibgarlikdan farqli o‘laroq, aniq bir hudud yoki shaxs doirasida emas, balki butun dunyo bo‘ylab amalga oshirilib, ma’lum makonga ega emas. Ushbu kiberjinoyat turi bo‘yicha bir necha qarashlar mavjud.

[1] https://lex.uz/uz/docs/-5960604 “Kiberxavfsizlik to‘g‘risida” gi O‘zbekiston Respublikasi qonuni
[2] Кибержиноятчиликка қарши курашишда интернет-маданиятнинг аҳамияти | ICTNEWS Bo’ronov.L Kiberjinoyatchilikka qarshi kurashishda internet madaniyatining ahamiyati – 2018-y
[3] https://lex.uz/docs/-111453 O‘zbekiston Respublikasi Jinoyat kodeksi.

Xususan, **V.K.Barchukovning fikricha**, kiberfiribgarlik kompyuter firibgarligi bo‘lib, u ichki ma’lumotlardan foydalangan holda firibgarlik va ishonchni suiiste’mol qilish orqali o‘zganing mulkiga tajovuz qilishdir [4]. **D.A.Zikovaning fikricha,** kiberfiribgarlik jinoyati kompyuter texnologiyalari yordamida firibgarlik, ishonchni suiiste’mol qilish orqali o‘zga shaxsning pul mablag‘larini o‘zlashtirish, uning mulkiga zarar keltirish va ushbu mulkka ega bo‘lish hisoblanadi [5]. **M.A.Yefremova esa,** “kiberfiribgarlik” tushunchasini “kompyuter ma’lumoti orqali firibgarlik qilish” tushunchasi bilan bir xil ekanligini va ularning sinonim so‘zlar hisoblanishini ta’kidlaydi[6]. Demak, yuqoridagi olimlarning fikrlariga qo‘shilgan holda aytishimiz mumkinki, kiberfiribgarlik haqiqatan ham komyuter firibgarligi bilan o‘zaro bir xil tushuncha desak bo‘ladi. U asosan an’anaviy firibgarlik singari shaxsning mol-mulki yoki shaxsiy ma’lumotlarini uning ishonchini suiste’mol qilib, aldash yo‘li bilan tajovuz qilinib, faqatagina raqamli dunyoda kompyuter texnologiyalari orqali sodir etiladi.

Kiberfiribgarlik jinoyatining kriminalistik elementlari quyidagilardan iborat:

- Jinoyatning predmeti;
- Jinoyat sodir etish usuli
- Jinoyat shaxsi;
- Jinoyat izi va dalillar.

Kiberfiribgarlik jinoyatining predmeti – bu firibgar tomonidan qo‘lga kiritiladigan, uning qonunga xilof xatti-harakati natijasida zarar yetkaziladigan ashyolar, masalan: pul, moddiy qimmatliklar, shaxsiy ma’lumotlar va boshqalar bo‘lishi mumkin. Kiberfiribgarlikning turi bo‘lgan **Vishing onlayn firibgarligi** orqali jinoyatning predmetini tahlil qiladigan bo‘lsak, firibgarning asosiy e’tibori jabrlanuvchining bank kartalarida pul mablag‘larini o‘zlashtirishdan iborat bo‘ladi. Bu holatda bank kartalari to‘g‘ridan to‘g‘ri jinoyat predmeti bo‘la olmaydi, negaki, firibgarning maqsadi bank kartlarini o‘g‘irlashga emas, balki undagi pulni o‘g‘irlashdan iborat. Ya’ni bu jinoyatda jinoyat predmeti o‘zganing mol-mulki hisoblanadi.

Kompyuter texnologiyalar va boshqa elektron qurilmalar orqali kiberfiribgarlikning turli xil usullari sodir etilmoqda. Jumladan, elektron to‘lov tizmi orqali sodir etiladigan, ya’ni kompyuter firibgarligining bit necha turlarini ko‘rib chiqamiz.

Fishing

Bank kartalari bilan bog‘liq firibgarlik jinoyatini sodir etish usullaridan biri bu **“fishing”** ya’ni “baliq ovi” usulidir. Bunda IT texnologiya sohasida yetarli bilim va ko‘nikmalarga ega firibgarlar tomonidan foydalanuvchining ishonchiga kirib, bank kartasiga doir maxfiy ma’lumotlari egallanadi [7]. Ushbu jinoyatning sodir etishning o‘ziga xos xususiyati shundan iboratki, xakerlar masofadan turib ijtimoiy tarmoqlar va turli xil veb-sahifalardan foydalanuvchining akkauntiga, elektron pochtasiga yoki aloqa vositasiga turli xil ko‘rinishdagi SMS xabarnoma yuboradi. Masalan, firibgar tashkilot, biror bir xizmat nomidan shuningdek, yaqin insonlar nomidan turli soxta xabarlarni yuboradi, u odatda biror bir havola bo‘lishi mumkin. Foydalanuvchi esa ushbu havolaga kirish orqali firibgarlar tomonidan tayyorlangan soxta saytga kiradi.

[4] Барчуков В.К. Терминология мошенничества в сфере компьютерной информации. – М.: Пробелы в российском законодательстве. № 4. 2017 г. – С. 163-165.

[5] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. дис. … канд. юрид. наук. Владимир, 2002. – 211 с.

[6] Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. – С. 19 21.

[7] Shazzo S.K. Sposobi soversheniya moshennichestva v otnoshenii grajdan [Methods of committing fraud against citizens]. Vestnik Adigeyskogo gosudarstvennogo universiteta. Seriya 1: Yurisprudentsiya. 2008. № 2. S. 5.

Agar login va parol so‘ralgan bo‘lsa uni kiritish orqali maxfiy ma‘lumotlar o‘g‘irlanadi.

Bugungi kunda soxta saytlar yaratish fishing kiberfiribgarligining eng zamonaviy uslubidan biriga aylanib qoldi. U haqiqiy saytlar bilan deyarli o‘xshash bo‘lganligi tufayli uni farqalash uchun diqqatliroq bo‘lish bilan birgalikda, maxsus ko‘nikma va bilim ham zarur.

Vishing

Hozirgi kunda yurtimizda yeng ko‘p kuzatilayotgan firibgarlik usulidan yana biri bu **vishing** onlayn firibgarligidir. Firibgarlikning bu usulida firibgarlar o‘z “o‘ljalarini” telefon orqali qo‘lga kiritishadi. Vishing so‘zi ingliz tilidan ya’ni, “voice” ovoz va “fishing” baliq ovi so‘zlarining jamlanmasidan hosil bo‘lgan[8]. Ushbu kiberfiribgarlikda firibgar o‘zini mansabdor shaxs sifatida, ya’ni bank xodimi, soliq inspektori, IIV xodimi va boshqa tashkilot xodimi sifatida tanishtirib, shaxsiy ma’lumotlarni misol uchun, Pin-kod, parol, SMS orqali kelgan tasdiqlash kodini so‘raydi. Uni bilib olish orqali akkauntga kirib hisob raqamdagi pullarni yechib olishi mumkin.

Meros firibgarligi

Ushbu firibgarlik ham kibermakonda tez-tez uchraydigan kiberfiribgarligi bo‘lib, bunda firibgar tomonidan jabrlanuvchiga chet eldagi qarindoshidan katta miqdordagi meros qolganligi haqida xabar qilinib, tayyorlangan soxta hujjatlar orqali uning ishonchiga kirishga harakat qiladi, hamda jabrlanuvchiga merosni rasmiylashtirish uchun to‘lov qilishni talab qiladi. Jabrlanuvchi tomonidan to‘lov amalga oshirilganidan so‘ng firibgar yo‘qolib qoladi. Ushbu firibgarlikni aniq bir misol bilan tushuntirib o‘tadigan bo‘lsak, Komil Sindarovning “Qabohat girdobi” asarida meros firibgarligiga oid jinoyat ishi ko‘rilgan. Unga ko‘ra, Halima ismli shaxs xorijlik firibgarning nayrangiga uchraydi. Firibgar A ning familiyasi “Isoqova” va otasining ismi “Isroilovna” dan foydalanib, Indoneziyada vafot etgan yirik tadbirkor Isroil Isakovning “yagona merosxo‘ri” sifatida ko‘rsatishni taklif qiladi. Halima bu taklifga ishonib, pasport nusxasi va zarur hujjatlarni yuboradi. Bir necha kundan so‘ng, merosga ega bo‘lganligi haqida soxta guvohnomani oladi va bojxona xarajatlari uchun o‘ttiz uch ming dollar so‘raladi. Shundan so‘ng kelishilgan pulni Halima o‘tkazib bergan va firibgarning telefoni, electron manzili taqa-taq o‘chgan. Bu meros firibgarligiga yaqqol misol bo‘la oladi.

Internet do‘konlar bilan bog‘liq firibgarlik – ba’zi firibgarlar qalbaki, sifatsiz tovarlar yoki maxsulotlar savdosi bilan shug‘ullanib xaridorlarni chuv tushursa, boshqalari maxsulot uchun oldindan qisman yoki to‘liq to‘lov qilishni talab qiladi[9]. To‘lov amalga oshirilgandan so‘ng ko‘pgina hollarda tovar yetkazib berilmaydi. Bizga ma’lumki, bugungi kunda internet do‘konlari kundan kunga ko‘payib bormoqda. Ushbu kiberfiribgarlikni yaqinda sodir bo‘lgan keys orqali tahlil qilishga harakat qilamiz.

Farg‘ona viloyatida yashovchi fuqaro A.Sh. o‘zining bank kartasidan 700.000 so‘m miqdoridagi pul mablag‘lari noma’lum shaxs tomonidan o‘zlashtirilgani bo‘yicha IIOga murojaat qilgan. Bu haqda Ichki ishlar vazirligi TQD Kiberxavfsizlik markazi xabar beradi. Ma’lumotlarga ko‘ra, X.S ismli shaxs “OLX” onlayn internet do‘koniga “Aser” rusumli noutbukni arzon narxlarda sotilishi yuzasidan yolg‘on ma’lumotlar bilan e’lon qilgan. Buni ko‘rgan A.SH ismli shaxs telefon orqali X.S bilan o‘zaro kelishib, oldindan 700.000(yeti yuz ming) miqdorda pul to‘lovini “Avans” sifatida o‘tkazishga rozi bo‘ladi.

[8] Табак И.С. Мошенничество с банковскими картами / И.С. Табак // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40.

[9] Kozodaeva O. N., Obidennova A. S. Sposobi soversheniya moshennichestva sispol`zovaniem bankovskix kart [Ways to commit fraud using bank cards]. Uchenie zapiski Tambovskogo otdeleniya RoSMU. S. 52.

Shundan so‘ng X.S ismli shaxs “Avans” sifatidagi pul to‘lovini qabul qilib olib, tovarni yetkazib bermaydi. Yozishmalarni ham butkul o‘chirib, A.SH ismli shaxsninng telefon raqamini qora ro‘yxatga solib qo‘yadi.

Internet-tilanchilik – soxta xayriya jamg‘armalari

Firibgarlar tomonidan internet sahifalarida va turli xil ijtimoiy tarmqolarda kasallikkka chalingan yoxud og‘ir ahvoldagi shaxslarning fotosuratlarini tarqatilib, shaxslardan xayr-ehson qilishlarini so‘rab murojaat qilishadi. Ya’ni insonlarga psixologik ta’sir qilgan holda ularning ishonchiga kirishni uddalashadi. Bunday hollarda odatda rasmi joylangan shaxslar ular uchun pul mablag‘lari jamg‘arilayotganligidan bexabar bo‘lishadi.

Jinoyat shaxsiga doir ma’lumot

Ushbu kriminalistik jinoyat elementida jinoyat shaxsiga doir ma’lumotlar o‘rganiladi.

Ya’ni jinoyat shaxsi uning individual xususiyatlari, umumiy fazilatlari, kasbiy va intellektual darajasi o‘rganiladi. Masalan, ular kompyuter texnologiyalari sohasida chuqur bilim va tajribaga ega mutaxassislar yoki shunchaki havaskorlar ham bo‘lishi mumkin. Biz ularni kiberjinoyat doirasida **“Xaker”** deb ataymiz. Uning ikki turini chuqurroq tahlil qilishga harkat qilamiz. **Birinchisi, fisher** odamlarni aldab, ularning ishonchiga kirish orqali bank karta raqamlari va boshqa shaxsiy ma’lumotlarni qo‘lga kiritadigan firibgar. Ular asosan o‘zlarini bank xodimlari yoki muayyan mansabdor shaxs sifatida tanishtirib, kiberfiribgarlik bo‘yicha chuqur bilim va tajribaga ega shaxslar bo‘lishadi. **Ikkinchisi, karderlar** bo‘lib ular asosan bank karta raqamlari haqida ma’lumotlarni to‘plash, o‘g‘irlash bilan shug‘illanuvchi shaxslar bo‘lib, aniqroq aytadigan bo‘lsak, ular ko‘pgina hollarda ofitsiant yoki sotuvchi bo‘lib faoliyat olib borishadi. Ular mijozlarning bamk kartalari haqidagi ma’lumotlarni ularga sezdirmasdan bilib olishadi va ushbu ma’lumotlarni o‘zlarining jinoiy faoliyatini amalga oshirishda foydalanishadi.

Jinoyat izlari

Sodir etilgan kiberfiribgarlik jinoyatini tezda ochish va aniqlash uchun jinoyat izlari va dalillar muhim ahamiyat kasb etadi.

Kriminalistik adabiyotlarda “virtual” yoki “raqamli” izlar tushunchasi borasida turli xil qarashlar mavjud. Xususan, V.A.Agibalov, V.A.Mesheryakovlar virtual iz bu kompyuter tizimi orqali raqamli moddiy tashuvchida qayd qilingan real (fizik) jarayonni tasvirlovchi yoki ushbu jarayonning raqamli shakldagi rasmiy (matematik) modelidir, ya’ni jinoyat bilan bog‘liq bo‘lgan kompyuter tizimining boshqa harakatlari natijasi deyishadi[10].

V.A. Mesheryakov izlarning uchinchi guruhi sifatida virtual izlarni kiritish kerakligini ta’kidlaydi. Uning fikricha, virtual izlar binar ko‘rinishda namoyon bo‘lib, faqatgina dasturiy vositalarni ishlatuvchi qurilmalar hamda axborotni o‘ziga qabul qilishga yaroqli bo‘lgan raqamli qurilmalarda qoladi[11]

Yuqoridagi fikrlar asosida xulosa qiladigan bo‘lsak, virtual iz ko‘z bilan ko‘rib, qo‘l bilan ushlab bo‘lmaydigan raqamli muhitdagi nomodddiy izlardir. U asosan firibgarning niyati yoki uslubi haqida ma’lumot beradi. Virtual iz esa kompyuter texnologiyalarida yoki elektron qurilamlarda qoldirilgan aniq va isbotlangan moddiy ko‘rinishga ega bo‘ladi.

Bugungi kunda kiber jinoyatchilar tomonidan sodir etilayotgan jinoyatlar davlat va uning fuqarolari yoki boshqa shaxslarning xavfsizligiga putur yetkazmoqda.

[10] Агибалов В.А., Мещеряков В.А. Природа и сущность виртуальных следов, «Воронежские криминалистические чтения», Выпуск 12, Воронеж, 2010. С. 17-19.

[11] Meshcheryakov V.A. Prestupleniya v sfere kompyuternoy informatsii: osnovi teorii praktiki rassledovaniya. – Voronij, 2002.

Tadqiqot natijasida kiberjinoyatchilik va kiberfribgarlik sohasida statistika ma'lumotlari tahlil qilinib, quyidagi ma'lumotlar olindi.

2024-yil may oyida O‘zbekistonning "uz" domen veb-saytlariga **6,6 milliondan ortiq** kiberhujumlar amalga oshirildi. **2021-2023-yillarda** O‘zbekistonda kiberjinoyatlar soni **25 baravarga** oshgani sababli mamlakatning bu kabi tahdidlarga qarshi turish salohiyati kun mavzusi bo'lib qolmoqda.[12]

O‘tkazilgan tadqiqot asosida ko‘rishimiz mumkinki, o‘tkan yillar davomida birgina O‘zbekistonning poytaxti Toshkent shahrining o‘zida ham ko‘rsatkichlar yillar davomida oshib bormoqda. 2021-yilda Toshkentda axborot texnologiyalari yordamida 2281 ta kiberhujum uyushtirilgan. 2022-yilda esa bu kiberjinoyatchilik ko‘rsatkichi 4332 tani tashkil etadi. Bu ko‘rsatkich qariyb 2 barobar ko‘paygani ko‘rishimiz mumkin. Bu jinoyatlarning 3372 tasi yoki 82 foizi bank plastik kartalarini talon-taroj qilish bilan bog‘liq. Kiberjinoyatchilikdan Toshkent shahar aholisi 2022-yilda 45,2 mlrd zarar ko‘rgan.

MUHOKAMA

Demak, yuqorida biz tahlil qilgan ma'lumotlar guvohlik beradiki, kiberjinotchilik yildan yilga o‘sib bormoqda, ularning orasida kompyuter firibgarligi eng ko‘p sodir etilaotgan kibr jinoyat turi sifatida namoyon bo‘lmoqda. Uni oldini olishga qaratilgan bir necha chora-tadbirlar, qonun hujjatlari ishlab chiqilgan. Jumladan, O‘zbekiston Respublikasida kiberxavfsizlik choralarini ta'minlash maqasadida "Kiberxavfsizlik to‘g‘risida" gi qonun, "Shaxsga doir ma'lumotlar to‘g‘risida"gi qonun, "Elektron hukumat to‘g‘risida"gi qonun va boshqalar qabul qilingan. Shuningdek, xalqaro darajadagi hujjat sifatida 2001-yil qabul qilingan Budapesht konvensiyasini aytishimiz mumkin.

O‘zbekiston Respublikasining **"Kiberxavfsizlik to‘g‘risida"**gi qonunning 11-moddasiga muvofiq, O‘zbekiston Respublikasining Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi hisoblanadi. Mazkur organ zimmasiga kiberxavfsizlikni ta'minlash bo‘yicha bir qator vazifalar yuklatilgan. Jumladan, organning vakolat doirasiga kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqish, kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan davlat nazorati ustidan nazoratni amalga oshirish, kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni hamda tergov harakatlarini amalga oshirish va boshqa kabi vazifalar kiradi. Biz yuqorida sanab o‘tgan kiberhujumlar odatda shaxs, jamiyat va davlat manfaatlariga tahdid soladi. Shu o‘rinda O'zbekiston Respublikasini kiberxavfsizlik masalalari bo'yicha milliy qonunchiligini dunyoning rivojlangan davlatlaridan biri Rossiya qonunchiligi bilan taqqoslab o‘tmoqchimiz, birinchidan, O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi qonunida faqat shaxs, jamiyat, davlat manfaatlarini muhofaza qilishga qaratilmasdan, balki xalqaro hamkorlik masalalarini rivojlantirishga ham alohida e'tibor qaratilgan. Rossiya Federativ Respublikasining 2014-yilda qabul qilingan "Kiberjinoyatchilikka qarshi kurashish to‘g‘risida"gi qonunida, shuningdek, 2017-yilda qabul qilingan "Kiberxavfsizlikka oid Milliy strategiyada asosiy urg‘u ichki xavfsizlik va milliy manfaatlarga qaratilgan. Ya'ni Rossiya qonunchiligi xalqaro hamkorlikdan voz kechib bo‘lsa-da, kiberxavfsizlik bo‘yicha milliy manfaatlarni ustuvorligiga asoslanadi. O‘zbekiston Respublikasi esa asosan kiberxavfsizlik bo‘yicha milliy manfaatlar bilan bir qatorda xalqaro hamkorlikka ham alohida e'tibor beradi.

[12] https://daryo.uz/2024/08/27/ozbekistonda-kiberxavfsizlik-muammosi-hujumlar-soni-25-baravarga-oshdi

XULOSA

Ushbu tadqiqot yuzasidan umumiy xulosa qiladigan bo‘lsak, kompyuter texnologiyalari, raqamlashtirish jarayonlari yildan yilga rivojlanib borar ekan, kiberjinoyatlarning soni ham ortib bormoqda. Elektron to‘lov tizmi orqali to‘lovlarni amalga oshirish kundalik hayotimizning ajralmas qismiga aylanib ulgurdi. Bu esa shaxslarning mashaqqatli va halol mehnati bilan topgan pullarini firibgarlarga osongina o‘zlashtirib olish yo‘llarini topib, uni o‘zlariniki qilib olishni uddalashmoqda. Ayni damda statistika ma’lumotlariga ham e’tibor qaratadigan bo‘lsak, sodir etilayotgan kiberjinoyatning kata qismini kompyuter firibgarligini ko‘rishimiz mumkin. Bizning mamlakatimizda ham ushbu kiberjinoyatni oldini olishga qaratilgan qonunlar ishlab chiqilganligiga qaramasdan, ko‘pgina kiberjinoyatlar ochilmasdan qolib ketyapti, ya’ni jinoyatchilarni aniqlash tizmi yetarli darajada mukammal bo‘lmaganligi sababli ular jazodan qutilib qolmoqda. Aynan kiberfiribgarlikni oldini olishga qaratilgan bir necha takliflarni bermoqchiman. Jumladan;

1. Kiberfiribgarlik uchun javobgarlik choralarini kuchaytirish, ya’ni O‘zbekiston Respublikasi Jinoyat kodeksiga “Elektron to‘lov tizimi bilan bog‘liq jinoyat” yoki “Kiberfiribgarlik” nomi bilan alohida moddalarni kiritish zarur;
2. Barcha ta’lim muassalari, maktab, litsey, oliy ta’lim muassasalrida “Kiberxavfsizlik asoslari” fanini majburiy darslik sifatida o‘qitish;
3. IT-mutaxassislar, yuristlar va huquq tartibot organlari o‘rtasida kiberjinoyatchilikka qarshi kurashish uchun maxsus ishchi guruh tashkil etish;
4. Kiberjinoyatdan jabrlanganlar uchun maxsus onlayn platform tashkil etish.

Bibliografiya

1. O‘zbekiston Respublikasi Jinoyat kodeksi.
2. “Kiberxavfsizlik to‘g‘risida” gi O‘zbekiston Respublikasi qonuni
3. Барчуков В.К. Терминология мошенничества в сфере компьютерной информации. – М.: Пробелы в российском законодательстве. № 4. 2017 г. – С. 163-165.
4. Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. дис. … канд. юрид. наук. Владимир, 2002. – 211 с.
5. Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. – С. 19 21.
6. Shazzo S.K. Sposobi sovershenіya moshennichestva v otnoshenii grajdan [Methods of committing fraud against citizens]. Vestnik Adigeyskogo gosudarstvennogo universiteta. Seriya 1: Yurisprudentsiya. 2008. № 2. S. 5.
7. Табак И.С. Мошенничество с банковскими картами / И.С. Табак // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40.
8. Kozodaeva O. N., Obidennova A. S. Sposobi sovershenіya moshennichestva sispol`zovaniem bankovskix kart [Ways to commit fraud using bank cards]. Uchenie zapiski Tambovskogo otdeleniya RoSMU. S. 52.
9. Агибалов В.А., Мещеряков В.А. Природа и сущность виртуальных следов, «Воронежские криминалистические чтения», Выпуск 12, Воронеж, 2010. С. 17-19.
10. Meshcheryakov V.A. Prestupleniya v sfere kompyuternoy informatsii: osnovi teorii praktiki rassledovaniya. – Voronij, 2002

11. Кибержиноятчиликка қарши курашишда интернет-маданиятнинг аҳамияти | ICTNEWS Bo'ronov.L Kiberjinoyatchilikka qarshi kurashishda internet madaniyatining ahamiyati – 2018-y
12. https://daryo.uz/2024/08/27/ozbekistonda-kiberxavfsizlik-muammosi-hujumlar-soni-25-baravarga-oshdi