“DEEPFAKE (SUN'IY QIYOFA VA OVOZ) TEXNOLOGIYALARI ORQALI SODIR ETILADIGAN KIBERFIRIBGARLIKLARNI JINOIY-HUQUQIY KVALIFIKATSIYA QILISH MUAMMOLARI”

Umurzakova Nargisa Muxtarovna
Ilmiy rahbar: Toshkent Davlat Agrar Universiteti ‘’Huquqshunoslik’’kafedrasi dotsenti [Mobil:+998990129077.E-mail: nargisau71@gmail.com]
Meliboyeva Farida Murodilla qizi
Toshkent Davlat Agrar Universiteti ‘’Agroiqtisodiyot, logistika va xizmatlar’ fakulteti Yurisprudensiya yo’nalishi 2-kurs talabasi. [Mobil:+998889051305.E-mail: meliboyevafarida004@gmail.com]
Parmonqulova Umida Toxir qizi
Toshkent Davlat Agrar Universiteti “Agroiqtisodiyot, logistika va xizmatlar” fakulteti Yurisprudensiya yo‘nalishi 2-bosqich talabasi [Mobil:+998930462245. E-mail: umidaparmonqulova@gmail.com
https://doi.org/10.5281/zenodo.20371973

Annotatsiya: Maqolada sun’iy intellekt va Deepfake yordamida sodir etiladigan kiberfirgarlikni jinoiy-huquqiy baholash muammolari yoritilgan. O‘zbekiston Jinoyat kodeksining 168-moddasi generativ texnologiyalar xavfini to‘liq qamrab olmasligi xalqaro tajriba asosida tahlil qilingan. Tadqiqot yakunida Jinoyat kodeksiga yangi og‘irlashtiruvchi belgi kiritish, majburiy markirovka uchun ma’muriy jazo belgilash va raqamli dalillarni ekspertiza qilish algoritmi bo‘yicha aniq qonunchilik takliflari ilgari surilgan.

Kalit so‘zlar: Sun’iy intellekt, Deepfake, Kiberfirgarlik, Jinoyat kodeksi, Elektron dalil.

Zamonaviy axborot-kommunikatsiya texnologiyalari, axborot xavfsizligi tizimlari va generativ sun’iy intellekt (SI) modellarining global miqyosda jadal integratsiyalashuvi ijtimoiy munosabatlarni raqamlashtirish bilan bir qatorda, kiberjinoyatchilikning mutloq transformatsiyalashgan prinsiplarini yuzaga keltirmoqda. Bugungi kunda global raqamli makonda hamda O‘zbekiston Respublikasining milliy kiber-muhitida chuqur o‘rganuvchi neyrotarmoqlar (Deep Learning) hamda generativ-musobaqalashuvchi tarmoqlar (GAN – Generative Adversarial Networks) yordamida insonning tashqi ko‘rinishi, yuz mimikalari va akustik (ovozli) biometrik ma’lumotlarini real vaqt rejimida yuqori aniqlikda o‘zgartirish yoki soxtalashtirish imkonini beruvchi “Deepfake” (dizaynlashtirilgan soxtalik) texnologiyalari keng ommalashmoqda. Ushbu texnologik yutuqlar multimedia kontentlarini yaratish, kinoindustriya va virtual reallik sohalarida ijobiy funksiyalarga ega bo‘lsa-da, kiberjinoyatchilik subyektlari qo‘lida shaxsning raqamli identifikasiyasini o‘g‘irlash, konfidensial axborotlarni qo‘lga kiritish va fuqarolarning mulkiy huquqlariga tajovuz qilishning destruktiv quroliga aylanib ulgurdi[1].Aynan ijtimoiy muhandislik (social engineering) va fishing usullarini Deepfake texnologiyalari bilan o‘zaro uyg‘unlashtirgan holda, yirik tadbirkorlik subyektlari hamda davlat organlari rahbarlarining yoki fuqarolarning yaqin qarindoshlarining ovozi va video-tasvirini sun’iy intellekt yordamida skanerlab, sintez qilish orqali bank plastik kartalaridan mablag‘larni o‘zlashtirish, virtual hisobraqamlarni bo‘shatish yoki to‘g‘ridan-to‘g‘ri pul o‘tkazmalarini

[1] Chesney R., Citron D. Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. – 2019. – Vol. 107. – P. 1753-1819

amalga oshirishga majburlash bilan bog‘liq kiberfirgarliklar soni geometrik progressiya asosida ortib bormoqda. Bunday ijtimoiy xavfli qilmishlar an’anaviy kiber-hujumlardan farqli o‘laroq, jabrlanuvchilarda mutloq vizual va auditorial ishonch (psixologik verifikasiya) uyg‘otishi sababli, subyektlarni chalg‘itish samaradorligi va yetkazilayotgan moddiy zararning ko‘lami nuqtai nazaridan jamiyat xavfsizligiga jiddiy tahdid solmoqda. O‘zbekiston Respublikasining milliy jinoiy qonunchilik tizimida kiber-makonda sodir etiladigan mulkiy va kompyuter tizimiga oid jinoyatlarga qarshi kurashishning huquqiy asoslari O‘zbekiston Respublikasining Jinoyat kodeksi (JK) normalari orqali tartibga solinadi. Xususan, milliy qonunchilikda ushbu qilmishlar JKning 168-moddasi (Firgarlik) va XX[1] bobi (Axborot texnologiyalari sohasidagi jinoyatlar) kesishmasida kvalifikatsiya qilinadi. JK 168-moddasi uchinchi qismining “g” bandida firgarlik qilmishi “axborot texnologiyalaridan foydalanib yoki ularni joriy etib” sodir etilganligi jinoiy javobgarlikni og‘irlashtiruvchi tarkibiy belgi sifatida mustahkamlangan[2]. Biroq, amaldagi jinoiy-huquqiy normalar tahlili shuni ko‘rsatadiki, qonun chiqaruvchi “axborot texnologiyalari” tushunchasi ostida asosan an’anaviy hisoblash texnikasi, fishing havolalari, ruxsatsiz ma’lumotlar bazasiga kirish yoki avtomatlashtirilgan to‘lov tizimlarini manipulyatsiya qilishni nazarda tutadi. Deepfake kabi generativ sun’iy intellekt vositalari yordamida inson qiyofasi va uning shaxsiy-subyektiv xususiyatlarini (ovoz va video) to‘liq kompyuter modellashtirish orqali sodir etiladigan kiberfirgarliklarning moddiy-huquqiy tabiati hamda obyektiv tomoni elementlari amaldagi qonunchilikda va O‘zbekiston Respublikasi Oliy sudi Plenumining 2017-yil 11-oktabrdagi “Firgarlik bo‘yicha sud amaliyoti to‘g‘risida”gi 35-sonli Qarorida to‘liq huquqiy bahosini topmagan[3]. Ushbu Plenum qarorining 4-bandida aldash tushunchasiga ta’rif berilgan bo‘lsa-da, u jismoniy dunyodagi munosabatlarga yoki oddiy matnli/hujjatli yolg‘onlarga qaratilgan bo‘lib, sun’iy sintez qilingan biometrik raqamli reallikni qamrab olmaydi. Xalqaro huquqiy makonda kiberjinoyatchilikka, shu jumladan generativ raqamli manipulyatsiyalarga qarshi kurashish bo‘yicha transchegaraviy va yurisdiksiyaviy hamkorlik mexanizmlari Yevropa Kengashining “Kiberjinoyatchilik to‘g‘risida”gi Budapesht Konvensiyasi (2001-y.)[4] prinsiplari hamda BMTning Kiberjinoyatchilikka qarshi maxsus qo‘mitasi tomonidan ishlab chiqilayotgan universal konvensiya loyihalari darajasida muvofiqlashtirilmoqda. Shuningdek, xalqaro tajribada raqamli xavfsizlikni ta’minlash maqsadida Yevropa Ittifoqining Sun’iy intellekt to‘g‘risidagi akti (EU AI Act, 2024-y.)[5] qabul qilinib, uning doirasida generativ SI modellaridan foydalangan html yaratilgan kontentlarni majburiy raqamli markirovka qilish (watermarking) va deepfake kontentlarini foydalanuvchiga majburiy ravishda ma’lum qilish majburiyati yuklatildi. Biroq, O‘zbekiston Respublikasi ushbu xalqaro konvensiyalarning to‘liq ishtirokchisi bo‘lmaganligi hamda milliy qonunchilikda generativ SI vositalarini jinoiy maqsadlarda qo‘llaganlik uchun maxsus kvalifikatsiya mezonlarining mavjud emasligi tergov va sud idoralari oldida bunday jinoyatlarni to‘g‘ri jinoiy-huquqiy baholash borasida kolliziyalarni yuzaga keltirmoqda.Sud-tergov amaliyotida va kriminalistikada vujudga kelayotgan asosiy muammo shundan iboratki,

[2] O‘zbekiston Respublikasining Jinoyat kodeksi. Lex.uz — Jinoyat kodeksi rasmiy matni (168-modda, XX[1]-bob).
[3] O‘zbekiston Respublikasi Oliy sudi Plenumining Qarori. Firgarlik bo‘yicha sud amaliyoti to‘g‘risida (11.10.2017 yildagi 35-son). Lex.uz — 35-sonli Plenum qarori.
[4] Council of Europe. Convention on Cybercrime (Budapest, 2001). Yevropa Kengashining Kiberjinoyat konvensiyasi rasmiy hujjati
[5] European Parliament. Artificial Intelligence Act (EU AI Act, 2024). Yevroparlament — EI Sun’iy intellekt akti rasmiy platformasi

Deepfake yordamida sodir etilgan firgarlikda jinoyat tarkibining obyektiv tomonidagi “aldash” mezonini an’anaviy normalar bilan isbotlash metodologiyasi mavjud emas. Bu yerda jabrlanuvchini chalg‘itish obyekti real shaxsning o‘zi emas, balki uning raqamli “kloni” (avatar) bo‘lib, bu holat jinoyat huquqi doktrinasidagi an’anaviy aldash tushunchasini kengaytirilgan shaklda tizimlashtirishni taqozo etadi. Bundan tashqari, O‘zbekiston Respublikasi Jinoyat-protsessual kodeksining (JPK)[6] normalari, xususan JPKning 81-moddasi (Dalillarning turlari) va 95-moddasi (Dalillarni baholash) doirasida raqamli dalillarni to‘plash, taqdim etish va ularning maqbulligini ta’minlash tartibi belgilangan bo‘lsa-da, sud muhokamasida Deepfake materiallarini elektron dalil sifatida tan olish, ularning haqiqiyligini va neyrotarmoqlar orqali generatsiya qilinganligini JPKning 172-moddasiga asosan sud-fonoskopik va kompyuter-texnikaviy ekspertizalari yordamida xatosiz isbotlashning protsessual algoritmi va metodik bazasi mukammal emas.

Ushbu ilmiy maqolaning fundamental maqsadi — O‘zbekiston Respublikasi jinoyat va jinoyat-protsessual huquqi qonunchiligi, iqtisodiy va kiber-jinoyatlarni tergov qilish milliy tajribasi hamda xorijiy ilg‘or standartlar tahlili asosida Deepfake texnologiyalari yordamida sodir etiladigan kiberfirgarliklarning o‘ziga xos jinoiy-huquqiy tabiatini aniqlashdan iborat. Shuningdek, ushbu qilmishlarni to‘g‘ri kvalifikatsiya qilish mezonlarini ishlab chiqish hamda Jinoyat kodeksining 168-moddasiga sun’iy intellekt modellari va raqamli identifikasiya manipulyatsiyalarini jinoiy javobgarlikka tortishga qaratilgan maxsus kvalifikatsiya belgilarini (yangi bandlarini) joriy etish bo‘yicha ilmiy-amaliy tavsiyalar to‘plamini shakllantirish tadqiqotning bosh obyekti hisoblanadi.

Amaldagi O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi uchinchi qismi “g” bandida firgarlik qilmishi “axborot texnologiyalaridan foydalanib yoki ularni joriy etib” sodir etilganligi kvalifikatsiya belgisi (jinoiy javobgarlikni og‘irlashtiruvchi holat) sifatida mustahkamlangan. Biroq, milliy qonunchilik mantiqida va an’anaviy jinoiy-huquqiy doktrinada “axborot texnologiyalari” tushunchasi ostida jinoyatni sodir etishda passiv qurol yoki vosita vazifasini bajaruvchi texnik tizimlar (kompyuter texnikasi, smartfon, telekommunikatsiya tarmoqlari yoki bank to‘lov tizimlari) tushuniladi. Deepfake yoki generativ sun’iy intellekt (SI) modellari esa passiv vosita doirasidan chiqib, inson omilisiz kontentni intellektual manipulyatsiya qiluvchi, mustaqil kontent sintez qiluvchi (yaratuvchi) va algoritmlar asosida chalg‘ituvchi faol tizim hisoblanadi.Ayni paytda, milliy jinoiy qonunchilikda o‘zga shaxsning biometrik ma’lumotlarini (ovoz chastotalari, yuz biometriyasi va qiyofasini) sun’iy intellekt neyrotarmoqlari yordamida ruxsatsiz egallash hamda generatsiya qilish, ya’ni “raqamli shaxs o‘g‘riligi” (Digital Identity Theft) jinoyat tarkibining alohida obyektiv tomoni elementi yoki mustaqil jinoyat sifatida kvalifikatsiya qilinmaydi. Sud-tergov amaliyotida Deepfake texnologiyalarini qo‘llash orqali jabrlanuvchining vizual va auditorial ongini to‘liq chalg‘itib sodir etilgan yuqori texnologik kiber-jinoyatlar oddiy matnli fishing ssenariylari yoki ijtimoiy muhandislikning an’anaviy shakllari bilan bir xil huquqiy mezonlar asosida jazolanmoqda. Vaholanki, generativ sun’iy intellekt yordamida yaratilgan raqamli yolg‘onning inson psixikasiga ta’sir ko‘rsatish va uni ruhan manipulyatsiya qilish (chalg‘itish) kuchi, ijtimoiy xavflilik darajasi hamda yetkaziladigan moddiy va ma’naviy zararning ko‘lami an’anaviy firgarlik shakllaridan bir necha barobar yuqoridir. Bu holat JK 168-moddasining joriy kiber-

[6] O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. Lex.uz — JPK rasmiy matni (81, 95, 172-moddalar).

mezonlarini differensiyalash va generativ SI ishtirokidagi qilmishlar uchun alohida jinoiy-huquqiy baho berish tizimini yaratish zaruriyatini asoslaydi.

Yevropa Ittifoqining Sun'iy intellekt to'g'risidagi akti (EU AI Act, 2024) to'g'ridan-to'g'ri jinoyat-huquqiy xarakterga ega bo'lmasa-da, kiberjinoyatlarning oldini olish va axborot xavfsizligini ta'minlashda tizimli moddiy-huquqiy filtr vazifasini bajaradi []. Mazkur hujjat SI tizimlarini yuzaga keltiradigan xavf darajasiga ko'ra to'rtta guruhga ajratadi va Deepfake texnologiyalarini "Maxsus shaffoflik riski" (Specific transparency risk) to'plamiga kiritadi. 2026-yilga kelib to'liq majburiy kuchga ega bo'lgan ushbu Aktning 52-moddasi talablariga muvofiq, generativ SI tizimlaridan foydalanuvchilar audio, video yoki foto kontentning sun'iy ravishda yaratilgani yoki intellektual manipulyatsiya qilinganligini (Deepfake ekanligini) foydalanuvchiga ochiq, aniq va tushunarli tarzda ko'rsatishi, ya'ni majburiy raqamli markirovka (watermarking) qo'llashi shart.O'zbekiston qonunchiligidagi farq va o'ziga xos kolliziya shunda ko'rinadiki, garchi respublikamizda 2026-yil 21-janvardan boshlab sun'iy intellekt texnologiyalarini huquqiy tartibga solishga qaratilgan fundamental O'RQ-1115-sonli Qonun kuchga kirgan va unda SI mahsulotlarini markirovka qilish prinsiplari belgilangan bo'lsa-da, ushbu preventiv tizim to'liq ishlamaslik xavfi ostida turibdi. Negaki, milliy qonunchilikda, xususan, Ma'muriy javobgarlik to'g'risidagi kodeksda (MJTK) yoki Fuqarolik kodeksida generativ kontentlarni majburiy markirovka qilish talablarini buzganlik uchun qat'iy sanksiyalar va huquqiy javobgarlik mexanizmlari hali mukammal darajada shakllantirilmagan. Natijada, ushbu qoida amaliyotda deklarativ xarakterda qolib, har qanday shaxs ruxsatsiz biometrik nusxa (Deepfake) yaratishda davom etmoqda. Bunday huquqiy bo'shliq oqibatida profilaktik (ma'muriy-huquqiy) to'siq real kuchga ega bo'lmayapti va qilmish faqat pul o'zlashtirilib, ijtimoiy xavfli oqibat yuz berganidan keyingina JKning 168-moddasi (Firgarlik) bilan jinoyat sifatida tergov qilinmoqda. Bu esa kiberjinoyatlarning oldini olish bosqichida huquqiy mexanizmlarning samarasizligini ko'rsatadi.

AQSh huquq tizimida Deepfake texnologiyalari orqali sodir etiladigan kiberfirgarliklarga va shaxs qiyofasini ruxsatsiz manipulyatsiya qilishga qarshi jinoiy hamda fuqarolik sanksiyalari ixtisoslashgan federal qonunlar bilan tartibga solinadi. Xususan, federal firgarlik qonunlari (Wire Fraud Statute — 18 U.S.C. § 1343) bilan bir qatorda, 2025-yilda qabul qilinib, 2026-yil may oyidan boshlab to'liq majburiy ijroga qaratilgan "TAKE IT DOWN Act" (S. 146) federal qonuni bu boradagi huquqiy mexanizmlarni o'zaro integratsiya qildi. AQSh federal qonunchilik andozalariga ko'ra, kiber-tovlamachilik yoki firgarlik maqsadi bo'lmagan taqdirda ham, generativ SI yordamida manipulyatsiya qilingan multimedia kontentida qonuniy talab qilingan o'chirib bo'lmaydigan raqamli belgi (Irreversible Digital Watermark) yoki "Deepfake material" degan maxsus ogohlantirish yozuvi majburiy ko'rsatilmasa, subyektlar to'g'ridan-to'g'ri federal jinoiy javobgarlikka tortiladi va 3 yildan 5 yilgacha ozodlikdan mahrum etilishi yoki yirik fuqarolik-huquqiy jarimalarga (har bir qoidabuzarlik uchun 53,000 AQSh dollarigacha) duchor qilinadi. O'zbekiston qonunchiligidagi farq va jiddiy huquqiy bo'shliq (lacuna) shunda ko'rinadiki, garchi respublikamizda 2026-yil 21-yanvardan boshlab sun'iy intellekt texnologiyalaridan foydalanishning umumiy prinsiplarini belgilovchi O'RQ-1115-sonli Qonun kuchga kirgan bo'lsa-da, u jinoiy sanksiyalar tizimini to'liq qamrab olmagan. Amaldagi O'zbekiston Respublikasi Jinoyat kodeksining XX^1-bobida (Axborot texnologiyalari sohasidagi jinoyatlar) faqatgina begona kompyuter tizimiga ruxsatsiz kirish (JK 278^1-modda) yoki zararli dasturlar yaratish (JK 278^4-modda) kabi texnik qilmishlar jazolanadi. Biroq, deepfake

yaratuvchi ochiq neyrotarmoqlar, ochiq algoritmlar yoki botlardan foydalanganlik to‘g‘ridan-to‘g‘ri jinoiy taqiqlarga kirmaydi. Ya’ni, kiberjinoyatchi o‘zga tizimni jismonan yoki virtual buzib kirmasdan, ochiq generativ dasturlar orqali o‘zga shaxsning ovozi va yuz qiyofasini klonlashtirsa va bu orqali firgarlik sodir etsa, XX[1]-bob moddalari prosessual jihatdan ishlamaydi va qilmish faqat JKning 168-moddasi (Firgarlik) doirasida kvalifikatsiya qilinadi. Bu esa raqamli shaxs o‘g‘riligining ijtimoiy xavflilik darajasini amaldagi jinoiy jazolash tizimida to‘liq aks ettirish imkonini bermaydi.

Huquqiy mezonlar va taqqoslash asoslari	**O‘zbekiston Respublikasi qonunchiligi**	**Yevropa Ittifoqi (EU AI Act)**	**AQSH federal tizimi (TAKE IT DOWN Act)**
Kiberfiribgarlikni jazolash asosi	JK 168-modda 3-qismi “g” bandi (Faqat passiv “axborot texnologiyalari” tushunchasi).	Jinoyat qonuni emas, axborot xavfsizligi filtri (Risk-management).	Wire Fraud Statute (18 U.S.C. § 1343) va raqamli manipulyatsiya sanksiyalari.
Deepfake tushunchasining mavjudligi	O‘RQ-1115-sonli Qonunda faqat umumiy “Sun’iy intellekt” ta’rifi bor, jinoiy belgi yo‘q	Mavjud (52-modda, “Maxsus shaffoflik riski” guruhiga kiritilgan)	Mavjud (Federal kiberjinoyat va raqamli shaxs o‘g‘riligi sifatida).
Majburiy markirovka (Watermatking)	Qonunda belgilangan, lekin MJTKda jazo sanksiyasi (jarima) yo‘q (Deklarativ)	Majburiy (Buzganlik uchun yirik global aylanma foizida jarimalar qo‘llaniladi)	Majburiy (Ogohlantirishsiz tarqatilsa, 3 yildan 5 yilgacha federal jinoiy jazo).
Raqamli platformalar javobgarligi	Platformalarga deepfayklarni o‘chirish bo‘yicha aniq prosessual majburiyat yuklanmagan.	Kontent tahlili va algoritmlar ustidan qat’iy jamoat auditi belgilangan.	Majburiy (Notice and takedown tizimi bo‘yicha o‘chirmasa, platforma jazolanadi).
Profilaktik (Preventiv) ta’siri	Past (Faqat oqibat yuz berganda, pul o‘g‘rilangach jinoyat ishi ochiladi).	Yuqori (Generatsiya bosqichida texnik to‘siqlar o‘rnatiladi).	Yuqori (Tijoriy maqsadsiz soxtalashtirish ham sanksiyaga sabab bo‘ladi).

Izoh: Muallif tomonidan xalqaro va milliy normativ-huquqiy hujjatlar asosida tizimlashtirilgan

Tadqiqot jarayonida O‘zbekiston Respublikasi Oliy sudi Plenumining 2017-yil 11-oktabrdagi “Firgarlik bo‘yicha sud amaliyoti to‘g‘risida”gi 35-sonli Qarorining 4 va 5-bandlarida mustahkamlangan “aldash” va “ishonchni suiiste’mol qilish” klassik tushunchalari tizimli-mantiqiy tahlildan o‘tkazildi. Amaldagi Plenum tushuntirishiga ko‘ra, aldash — haqiqatga to‘g‘ri

kelmaydigan yolg‘on ma’lumotlarni qasddan xabar qilish yoki haqiqiy faktlarni yashirish shaklida (jismoniy munosabatlarda) talqin qilingan. Tadqiqotda ushbu terminologiyalarning an’anaviy talqin doirasi generativ raqamli makon (sun’iy intellekt muhiti) prinsiplari bilan qiyoslandi. Natijada, subyektlar o‘rtasidagi an’anaviy “shaxslararo ishonch” mexanizmi o‘rnini sun’iy intellekt yordamida yaratilgan raqamli subyektiv shaxs o‘g‘riligi (Digital Identity Theft), ya’ni jabrlanuvchining yaqinlari yoki rahbarlarining biometrik nusxalariga (klonlariga) ishonish fenomeni egallayotgani aniqlandi. Ushbu mantiqiy silsila orqali Jinoyat kodeksi doktrinasidagi “aldash” tushunchasini faqat jismoniy yoki oddiy hujjatli yolg‘on emas, balki “raqamli reallikni manipulyatsiya qilish orqali aldash” elementi bilan kengaytirish zarurati ilmiy jihatdan asoslab berildi. Kiberfirgarliklarning real ko‘lami va kriminologik dinamikasini o‘rganish maqsadida O‘zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazining axborot byulletenlari, huquqni muhofaza qiluvchi organlarning ochiq sud-tergov ma’lumotlari hamda Kaspersky xalqaro kiber-tahliliy resurslarining global hisobotlari (Kaspersky Global Report) asosida so‘nggi yillarga oid empirik materiallar to‘plandi. To‘plangan statistik ma’lumotlarga induksiya va deduksiya prinsiplari qo‘llanildi. Xususan, dastlab alohida olingan real jinoyat keyslari va bank plastik kartalaridan mablag‘larni o‘g‘irlash sxemalari tahlil qilindi (induksiya). So‘ngra ushbu xususiy holatlardan kelib chiqib, generativ sun’iy intellekt (Deepfake) texnologiyalari rivojlanishi bilan kiberfirgarlik jinoyatlarining umumiy o‘sish tendensiyasi, latentlik (yashirinlik) darajasi va jabrlanuvchilarning yosh toifalari bo‘yicha kriminologik xususiyatlari umumiy qonuniyat ko‘rinishida shakllantirildi (deduksiya). Bu esa milliy qonunchilikni zudlik bilan takomillashtirish zaruriyatini raqamli ko‘rsatkichlar bilan isbotlash imkonini berdi.

O‘zbekiston Respublikasi Oliy sudi Plenumining 2017-yil 11-oktabrdagi 35-sonli Qarorida firgarlikning asosi sifatida belgilangan “aldash” va “ishonchni suiiste’mol qilish” mezonlari bugungi kunda faqat subyektlararo (insonlararo) to‘g‘ridan-to‘g‘ri aloqalarga qaratilgan. Ammo Deepfake texnologiyalaridan foydalanilganda, jabrlanuvchi jismoniy shaxs tomonidan emas, balki sun’iy intellekt tomonidan mukammal generatsiya qilingan algoritmik reallik tomonidan aldanyapti. Bu holat jinoyat huquqi doktrinasidagi “aybni subyektiv baholash” prinsipiga yangicha yondashuvni talab etadi. Ayrim huquqshunos olimlar buni shunchaki “aldashning yangi vositasi” deb hisoblasalar-da, bizning tadqiqotimiz shuni ko‘rsatadiki, Deepfake oddiy passiv vosita (masalan, soxta hujjat) doirasidan chiqib, inson omilisiz chalg‘ituvchi faol tizimga aylangan. Shuning uchun, sud amaliyotida ushbu holatni oddiy firgarlik sifatida baholash jinoyatning ijtimoiy xavflilik darajasiga va adolat tamoyiliga to‘liq mos kelmaydi. Respublikamizda 2026-yil 21-janvardan kuchga kirgan O‘RQ-1115-sonli Qonun sun’iy intellekt tizimlarini tartibga solish yo‘lidagi birinchi tarixiy qadam bo‘ldi. Biroq, mazkur qonun tomonidan belgilangan generativ kontentlarni markirovka qilish (watermarking) majburiyati hozirgi kunda ko‘proq deklarativ xarakterga ega. Negaki, Ma’muriy javobgarlik to‘g‘risidagi kodeksda (MJTK) ushbu majburiyatni buzganlik uchun aniq jazo sanksiyalari mavjud emas. Natijada, kiberjinoyatchilar xorijiy va mahalliy ochiq neyrotarmoqlardan hech qanday huquqiy to‘siqsiz foydalanib, ruxsatsiz ovoz va video klonlarni yaratishda davom etmoqdalar. Biz taklif etgan MJTK 201^{12}-moddasi qonunchilikda aynan o‘sha bo‘shliqni (lacuna) yopishga va kiber-hujumlarni jinoiy bosqichga o‘tmasidanoq, ma’muriy-preventiv filtrlar orqali jilovlashga xizmat qiladi. Bu model Yevropa Ittifoqining Sun’iy intellekt to‘g‘risidagi akti (EU AI Act) 52-moddasida ko‘rsatilgan shaffoflik talablari bilan to‘liq garmonizatsiyalanadi.

Xulosa. Generativ sun'iy intellekt va Deepfake texnologiyalarining raqamli makonda shiddat bilan ommalashishi an'anaviy kiberjinoyatchilik ko'rinishlarini mutloq yangi, tizimli va transformatsiyalashgan bosqichga olib chiqdi. O'tkazilgan ushbu ilmiy tadqiqot natijalari shuni ko'rsatadiki, amaldagi O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi tarkibidagi kiber-mezonlar generativ sun'iy intellekt (SI) modellarining faol algoritmik xavfini, ya'ni raqamli shaxs o'g'riligini (Digital Identity Theft) to'liq qamrab olishga ojizlik qilmoqda. Garchi respublikamizda sun'iy intellekt munosabatlarini tartibga solishga qaratilgan birinchi tizimli O'RQ-1115-sonli Qonun kuchga kirgan bo'lsa-da, unda belgilangan preventiv qoidalar jinoiy-huquqiy sanksiyalar bilan integratsiya qilinmaganligi sababli, amaliyotda yetarli darajada profilaktik to'siq vazifasini bajara olmayapti.

Tavsiyalar

- **Qonunchilikni modernizatsiya qilish**: JK 168-moddasi to'rtinchi qismiga generativ sun'iy intellekt va Deepfake texnologiyalari orqali sodir etiladigan kiberfirgarlik qilmishlari uchun maxsus og'irlashtiruvchi kvalifikatsiya belgisini (yangi "e" bandini) dispozitsiya va qat'iy jinoiy sanksiya (8 yildan 10 yilgacha ozodlikdan mahrum qilish) bilan birga joriy etish zarur.
- **Preventiv choralarni kuchaytirish:** Ma'muriy javobgarlik to'g'risidagi kodeksni (MJTK) sun'iy intellekt tomonidan yaratilgan multimedia materiallarini majburiy raqamli markirovka (watermarking) qilish talablarini buzganlik uchun sanksiyalarni nazarda tutuvchi yangi 201^{12}-modda bilan to'ldirish lozim. Bu chora Yevropa Ittifoqining EU AI Act qonunchilik andozalariga to'liq mos kelib, jinoyatlarni barvaqt oldini olishga xizmat qiladi.

Protsessual isbotlash bazasini yaratish: Deepfake materiallarini jinoyat protsessida maqbul dalil sifatida baholash uchun Jinoyat-protsessual kodeksining 81, 95 va 172-moddalari talablari doirasida uch bosqichli (fiksatsiya, kriminalistik neyro-deteksiya ekspertizasi va erkin prosessual baholash) algoritmik tizimni amaliyotga tatbiq etish lozim.

Foydalanilgan adabiyotlar:

1.O'zbekiston Respublikasining Jinoyat kodeksi. Lex.uz elektron milliy qonunchilik ma'lumotlari bazasi — Jinoyat kodeksi rasmiy matni (168, 278^1, 278^4-moddalar)
2.O'zbekiston Respublikasining Jinoyat-protsessual kodeksi. Lex.uz elektron milliy qonunchilik ma'lumotlari bazasi — JPK rasmiy matni (81, 95, 172-moddalar).
3.O'zbekiston Respublikasining Qonuni. Sun'iy intellektni qo'llash orqall yuzaga keladigan munosabatlarni tartibga solish munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga qo'shimcha va o'zgartirishlar kiritish to'g'risida (O'RQ-1115-son, 21-yanvar 2026-yil). Lex.uz rasmiy qonunchilik portali.
4.O'zbekiston Respublikasi Oliy sudi Plenumining Qarori. Firibgarlikka oid ishlar bo'yicha sud amaliyoti to'g'risida (2023-yil 23-iyundagi 17-sonli qaror — 2017-yilgi 35-sonli qaror o'rniga qabul qilingan yangi tahrir). Lex.uz — Oliy sud Plenumi rasmiy bazasi.
5.Yevropa Ittifoqi Parlamenti.Sun'iy intellekt to'g'risidagi akt (EU AI Act, 2024). European Parliament Artificial Intelligence Act Official Platform (Article 52 — Transparency obligations).
6.AQSh 119-Kongressi. Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act yoki TAKE IT DOWN Act (S. 146 / Pub. L. 119–12, 2025-yil qabul qilingan, 2026-yil may oyidan amalda). United States Congress Official Website.

7.O‘zbekiston Respublikasi Ichki ishlar vazirligi. Kiberxavfsizlik markazining axborot-tahliliy byulletenlari va statistik ma’lumotlari. Cyber102 rasmiy portali.