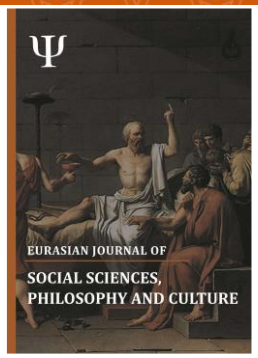
EURASIAN JOURNAL OF SOCIAL SCIENCES, PHILOSOPHY AND CULTURE
Innovative Academy Research Support Center
IF = 9.3 www.in-academy.uz/index.php/ejsspc



SYSTEMATIC MEASURES IMPLEMENTED USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE DETECTION OF CRIMES COMMITTED THROUGH DEEPFAKE TECHNOLOGY

Khudoyberdiyev Murodjon Akmal o‘g‘li
Academy of Law Enforcement Agencies of the Republic of Uzbekistan. 3rd-year student of the “Investigative Activity” program. Email: xudoyberdiyevm620@gmail.com
https://doi.org/10.5281/zenodo.18277858

ARTICLE INFO
Received: 12th January 2026
Accepted: 16th January 2026
Online: 17th January 2026
KEYWORDS
Deepfake, artificial intelligence, video authentication, DARPA MediFor, legal measures, deepfake detection, disinformation.

ABSTRACT
This article analyzes crimes committed through deepfake technology, methods for their detection, and approaches to countering the risks posed by such technologies. Based on international practices, including the experience of the United States and global law enforcement practices, the study examines the role of artificial intelligence, legal measures, and technological solutions in combating deepfake-related crimes. Particular attention is paid to the main methods of detecting deepfake content, technologies such as DARPA MediFor and Microsoft Video Authenticator, as well as the significance of regulatory and legal initiatives and international cooperation in addressing this issue.

DEEPFAKE TEXNOLOGIYASI ORQALI SODIR ETILADIGAN JINOYATLARNI FOSH ETISHDA SUN'IY INTELLEKT TEXNOLOGIYALARI YORDAMIDA AMALGA OSHIRILADIGAN TIZIMLI CHORALAR

Xudoyberdiyev Murodjon Akmal o‘g‘li
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi 3-kurs “Tergov faoliyati” yo‘nalishi talabasi
Email: xudoyberdiyevm620@gmail.com
https://doi.org/10.5281/zenodo.18277858

ARTICLE INFO
Received: 12th January 2026
Accepted: 16th January 2026
Online: 17th January 2026
KEYWORDS
Deepfake, sun'iy intellekt, video autentifikatsiya, DARPA MediFor, huquqiy chora-tadbirlar, deepfake aniqlash, dezinformatsiya.

ABSTRACT
Mazkur maqolada deepfake texnologiyasi orqali sodir etilgan jinohyatlarning fosh etilishi va uning yaratgan xavflarga qarshi kurashish usullari tahlil qilinadi. Xalqaro miqyosda, AQSh tajribasi va xalqaro amaliyot misollari asosida sun'iy intellekt, huquqiy chora-tadbirlar va texnologik yechimlar ko‘rib chiqiladi. Maqola deepfake kontentni aniqlashdagi asosiy metodlar, DARPA MediFor va Microsoft Video Authenticator kabi texnologiyalar, shuningdek, normativ-huquqiy tashabbuslar va xalqaro hamkorlikning o‘rni haqida so‘z yuritiladi.

Bugungi kunda axborot texnologiyalari rivojlanishi bilan deepfake kontentining tarqalishi sezilarli darajada ortib bormoqda. Bu texnologiya noto‘g‘ri ma’lumot tarqatish, siyosiy manipulyatsiyalar va shaxsiy ma’lumotlarni suiiste’mol qilish kabi xavflarni keltirib chiqaradi. Ushbu maqolada milliy va xalqaro tajribalar va xalqaro amaliyot misollari asosida deepfake texnologiyasini aniqlash va unga qarshi kurashish usullari tahlil qilinadi.

Dunyoga ma`lum va mashhur Microsoft kompaniyasi tomonidan 2020-yilda **Microsoft Video Authenticator** nomli deepfake texnologiyalariga qarshi kurash uchun mo`ljallangan, sun’iy intellekt yordamida tasvir va videolardagi manipulyatsiyalarni aniqlay oladigan dasturni ishlab chiqdi. Dastur tasvir yoki videoni tahlil qilib, uning sun’iy ravishda o‘zgartirilganligini foiz ko‘rinishida baholaydi. Videolar uchun har bir kadrni real vaqt rejimida tahlil qilish imkoniyatiga ega. Bu dastur Face Forensic++ va DeepFake Detection Challenge Dataset kabi jamoat ma’lumotlar to‘plamlaridan foydalangan holda yaratilgan. Ushbu to`plamlarga alohida to`xtaladigan bo`lsak :

FaceForensics++ – bu deepfake va boshqa yuz manipulyatsiyalarini aniqlash uchun yaratilgan dataset bo‘lib, Technical University of Munich va University of Naples Federico II tadqiqotchilari tomonidan ishlab chiqilgan. Unda 1,000 dan ortiq haqiqiy va soxtalashtirilgan videolar mavjud bo‘lib, deepfake, Face2Face, FaceSwap, NeuralTextures kabi texnologiyalar yordamida tahrirlangan tasvirlarni o‘z ichiga oladi. Bu dataset mashinani o‘qitish modellari uchun soxta va haqiqiy yuz ifodalarini farqlashga yordam beradi.

DeepFake Detection Challenge (DFDC) Dataset – Facebook, Microsoft, Amazon kabi yirik kompaniyalar hamkorligida yaratilgan ochiq dataset bo‘lib, unda 100,000 dan ortiq haqiqiy va soxtalashtirilgan videolar mavjud. Ushbu dataset deepfake texnologiyalari bilan yaratilgan tasvirlarni tahlil qilish va ilg‘or modellarni sinab ko‘rish uchun mo‘ljallangan.

M**icrosoft Video Authenticator** dasturning ishlash prinsipi shundaki, u tasvirlardagi nozik o‘zgarishlar, masalan, rang o‘zgarishlari yoki kulrang soyalarni aniqlaydi, bu esa inson ko‘zi bilan ko‘rish qiyin bo‘lgan manipulyatsiyalarni fosh etishga yordam beradi. biroq, Microsoft ushbu texnologiyani keng ommaga taqdim etmagan. Buning o‘rniga, u **Reality Defender 2020** tashabbusi orqali demokratik jarayonlarga aloqador tashkilotlarga, jumladan, yangiliklar agentliklari va siyosiy kampaniyalarga taqdim etilgan.

Shuni ham ta’kidlash joizki, Microsoft sun’iy intellekt texnologiyalarining noto‘g‘ri qo‘llanilishidan xavotirlanib, ba’zi AI vositalarini ommaga taqdim etishda ehtiyotkorlik bilan yondashmoqda. Masalan, kompaniya **VASA-1** deb nomlangan yangi AI texnologiyasini namoyish qilgan bo‘lsa-da, uning noto‘g‘ri qo‘llanilish ehtimolini inobatga olib, uni ommaga taqdim etishdan bosh tortgan .

Shuningdek, AQSh Mudofaa Ilg‘or Tadqiqot Loyihalari Agentligi (DARPA) tomonidan 2016-yilda ishga tushirilgan Media Forensics (MediFor) dasturi raqamli media, xususan, tasvir va videolarning ishonchliligini avtomatik baholash texnologiyalarini rivojlantirishga qaratilgan. Dasturning asosiy maqsadi — raqamli manipulyatsiyalarni aniqlash va ularning manbalarini topish orqali soxta

ma’lumotlarning tarqalishiga qarshi kurashish. MediFor dasturi tasvir va videolarning yaxlitligini uchta asosiy darajada tahlil qiladi: raqamli yaxlitlik (media fayllarining metama’lumotlari va raqamli izlarini tahlil qilish orqali ularning o‘zgartirilganligini aniqlash), jismoniy yaxlitlik (tasvirlardagi yorug‘lik, soyalar va geometriya kabi jismoniy xususiyatlarni tekshirish orqali noaniqliklarni aniqlash) va semantik yaxlitlik (media tarkibidagi mantiqiy va kontekstual nomuvofiqliklarni aniqlash). MediFor dasturi doirasida DARPA yetakchi tadqiqotchilar va tashkilotlar bilan hamkorlik qilib, raqamli media ishonchliligini avtomatik baholash uchun ilg‘or texnologiyalarni ishlab chiqdi. Ushbu texnologiyalar soxta media materiallarini aniqlash va ularning manbalarini topishda muhim ahamiyatga ega bo‘ldi.

MediFor dasturining muvaffaqiyatlaridan so‘ng, DARPA 2021-yilda Semantic Forensics (SemaFor) dasturini ishga tushirdi. SemaFor dasturi MediFor tomonidan yaratilgan texnologiyalarni yanada rivojlantirib, sun’iy va manipulyatsiyalangan media materiallarini avtomatik aniqlash, ularning manbalarini aniqlash va xususiyatlarini tavsiflashga qaratilgan. Bu dastur, shuningdek, matn, audio, tasvir va video kabi turli formatdagi soxta materiallarni aniqlash uchun ilg‘or texnologiyalarni ishlab chiqishga yo‘naltirilgan. DARPAning MediFor dasturi raqamli media ishonchliligini ta’minlash va soxta materiallarning tarqalishiga qarshi kurashishda muhim qadam bo‘ldi. Ushbu dastur orqali ishlab chiqilgan texnologiyalar hozirgi kunda ham soxta media materiallarini aniqlash va ularning manbalarini topishda keng qo‘llanilmoqda.

Xitoy hukumati esa deepfake texnologiyasidan noqonuniy foydalanishning oldini olish uchun 2023-yil 10-yanvardan boshlab yangi tartib-qoidalarni kuchga kiritdi. Ushbu qoidalar Xitoy Kiberxavfsizlik Administratsiyasi (CAC), Madaniyat va turizm vazirligi hamda Radio va televideniye boshqarmasi tomonidan ishlab chiqilgan. Ularning maqsadi deepfake texnologiyasi orqali noto‘g‘ri yoki zararli kontent tarqalishini oldini olish va sun’iy intellekt asosida yaratilgan vizual va ovozli materiallarni tartibga solishdan iborat.

Yangi qoidalarga ko‘ra, deepfake kontentini ishlab chiqaruvchilar va tarqatuvchilar o‘z mahsulotlariga maxsus raqamli suv belgisi qo‘shishlari shart. Bu belgilar foydalanuvchilarga video yoki tasvirning sun’iy ravishda o‘zgartirilganligini ko‘rsatadi. Agar biror shaxsning yuzi, ovozi yoki harakatlari deepfake texnologiyasi orqali qayta yaratilsa, ushbu shaxsning oldindan roziligi olinishi kerak. Rozilik olinmagan taqdirda, bunday materiallar noqonuniy deb hisoblanadi va ularni yaratgan yoki tarqatgan shaxslarga qarshi choralar ko‘riladi.

Xitoy hukumati deepfake texnologiyasining ijtimoiy axborot tarqatish jarayoniga ta’sirini kamaytirish maqsadida, agar ushbu texnologiyadan yangiliklar yoki muhim ijtimoiy xabarlarni tarqatishda foydalanilsa, faqat davlat tomonidan tasdiqlangan manbalar asosida material tayyorlashni talab qiladi. Boshqacha qilib aytganda, deepfake yordamida yaratilgan xabarlar ishonchli axborot manbalaridan olingan bo‘lishi lozim. Shu bilan birga, zo‘ravonlik, terrorizm yoki jinoyatchilikni targ‘ib qiluvchi deepfake materiallarini yaratish va tarqatish qat’iyan taqiqlangan. Ushbu talablar buzilgan taqdirda, material egalariga nisbatan qattiq chora ko‘riladi.

Buyuk Britaniyada deepfake texnologiyasiga qarshi kurashish maqsadida 2023-yilda Onlayn Xavfsizlik Qonuni (Online Safety Act) qabul qilingan. Ushbu qonun sun’iy

intellekt yordamida yaratilgan materiallarning noqonuniy ishlatilishini cheklashga qaratilgan. Mazkur qonunning asosiy maqsadi odamlarni onlayn tahqirlash, shaxsiy huquqlarining buzilishi, firibgarlik va noto‘g‘ri axborot tarqalishidan himoya qilishdan iborat. Buyuk Britaniya qonuniga muvofiq, agar deepfake texnologiyasi orqali kimningdir obro‘siga putur yetkazadigan yoki ularning shaxsiy hayotiga tajovuz qiladigan material tayyorlansa, bunday harakatlar jinoyat deb baholanadi. Xususan, deepfake yordamida shaxsning ruxsatisiz tayyorlangan jinsiy yoki shaxsiy mazmundagi tasvirlar tarqatilgan taqdirda, aybdorlarga nisbatan jinoiy javobgarlik qo‘llaniladi. 2024-yilda ushbu qonunga kiritilgan qo‘shimchalarga ko‘ra, deepfake texnologiyasidan foydalanib, kimnidir qo‘rqitish, tuhmat qilish yoki tahqirlashga uringan shaxslar ham jinoiy javobgarlikka tortilishi mumkin.

Kanadada deepfake texnologiyasining xavflarini kamaytirish maqsadida 2019-yilda Kanada Aloqa Xavfsizligi Tashkiloti maxsus hisobot e’lon qilgan edi. Ushbu hisobotda deepfake texnologiyasi orqali soxta axborot tarqatish xavfi va uning demokratik jarayonlarga salbiy ta’siri haqida so‘z yuritilgan. Bu masala ayniqsa saylov jarayonlarida muhim bo‘lib, firibgarlar sun’iy intellekt yordamida siyosatchilar yoki taniqli shaxslarning so‘zlarini manipulyatsiya qilib, noto‘g‘ri axborot tarqatishi mumkinligi ta’kidlangan. Shuningdek, hukumat 2024-yilda Onlayn Zararlar To‘g‘risidagi Qonunni (Online Harms Act) ishlab chiqdi. Mazkur qonunning asosiy maqsadi onlayn platformalar orqali zararli kontent tarqatilishining oldini olishdan iborat. Ushbu qonun jinoyat kodeksiga o‘zgartirishlar kiritishni ham nazarda tutadi. Ya’ni, deepfake texnologiyasidan foydalangan holda kimningdir shaxsiyatiga putur yetkazish, noto‘g‘ri axborot tarqatish yoki firibgarlik qilish holatlariga qat’iy huquqiy baho beriladi va bunday harakatlar uchun jinoiy javobgarlik joriy qilinadi.

Hindistonda deepfake texnologiyasiga qarshi kurash borasida hukumat juda qat’iy yondashuvni qo‘llaydi. 2023-yil noyabr oyida Hindiston Axborot Texnologiyalari Vazirligi ijtimoiy media platformalaridan deepfake kontentini tezkor ravishda aniqlash va olib tashlashni talab qiluvchi maxsus tavsiyalar berdi. Vazir Ashvini Vaishnav deepfake tahdidlariga qarshi kurashish maqsadida ijtimoiy tarmoqlarga nisbatan qat’iy talablar qo‘ygan. Bunda, agar ijtimoiy media platformalari deepfake kontentini o‘z vaqtida olib tashlamasa, ularning Hindiston hududida ishlashiga to‘sqinlik qilinishi yoki ularga qattiq jazo qo‘llanilishi mumkinligi ta`kidlangan.

Yevropa Ittifoqida deepfake texnologiyasini tartibga solish uchun 2024-yilda Sun’iy Intellekt To‘g‘risidagi Qonun (AI Act) qabul qilingan. Ushbu qonun sun’iy intellekt tizimlarini xavf darajasiga qarab to‘rtta toifaga ajratadi: qabul qilib bo‘lmaydigan xavf, yuqori xavf, cheklangan xavf va minimal xavf. Bu xavflar orasida Deepfake texnologiyasi yuqori xavf toifasiga kiritilgan va uni ishlatish qat’iy qoidalar asosida amalga oshirilishi shartligi esa alohida keltirib o`tilgan.

Yangi qonunga ko‘ra, deepfake texnologiyasidan foydalangan holda tayyorlangan har qanday materialda ushbu kontent sun’iy intellekt yordamida yaratilganligi aniq ko‘rsatilishi kerak. Bundan tashqari, deepfake kontenti siyosiy yoki ijtimoiy manipulyatsiya maqsadida ishlatilgan taqdirda, bunday harakatlar noqonuniy deb baholanadi. Saylovoldi kampaniyalari yoki ommaviy axborot vositalari orqali noto‘g‘ri

deepfake ma’lumotlar tarqatgan shaxslar yoki tashkilotlar jinoiy javobgarlikka tortilishi mumkin.

O‘zbekistonda ham sun’iy intellekt texnologiyalarini tartibga solish va ularni nazorat qilish bo‘yicha muayyan huquqiy asoslar yaratilgan. Jumladan, 2021-yil 17-fevralda Prezidentning "Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlarni yaratish chora-tadbirlari to‘g‘risida"gi qarori qabul qilindi. Ushbu hujjat "Raqamli O‘zbekiston – 2030" strategiyasi doirasida sun’iy intellekt texnologiyalarini rivojlantirish, ularning xavf-xatarlarini kamaytirish va ularni tartibga solish masalalariga bag‘ishlangan.

Deepfake texnologiyasining rivojlanishi bilan birga, dunyoning turli mamlakatlari bu sohada qat’iy tartibga solish mexanizmlarini ishlab chiqmoqda. Ushbu mexanizmlar sun’iy intellekt texnologiyalaridan noto‘g‘ri maqsadlarda foydalanishning oldini olishga qaratilgan bo‘lib, ularning har biri milliy xavfsizlik, axborot ishonchliligi va shaxsiy huquqlarni himoya qilishni maqsad qilgan.

Xulosa qilib aytganda, deepfake texnologiyalaridan foydalanishning huquqiy, texnologik va axloqiy jihatlarini aniq tartibga solish bugungi kunda dolzarb masaladir. Mazkur yo‘nalishda birinchi navbatda **O‘zbekiston Respublikasi jinoyat va ma’muriy qonunchiligiga aniq o‘zgartirishlar kiritish zarur**. Xususan, Jinoyat kodeksiga shaxsning ruxsatisiz sun’iy intellekt orqali yaratilgan soxta tasvir, ovoz yoki videolarni tayyorlash, tarqatish va undan manfaat ko‘zlab foydalanishni alohida jinoyat sifatida belgilovchi yangi modda kiritilishi maqsadga muvofiq. Shuningdek, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunda shaxsning yuzi, ovozi va tasviri alohida **biometrik ma’lumot** sifatida ko‘rsatilishi va deepfake orqali qayta ishlanishi faqat rozilik asosida ruxsat etilishi lozim. “Axborotlashtirish to‘g‘risida”gi Qonun va OAVga oid qonunlarda esa deepfake kontentida majburiy ravishda belgilalar (watermark) talabi joriy qilinishi zarur.

Deepfake texnologiyalarining xavf-xatarlarini kamaytirish jarayonida **idoralararo muvofiqlashtirilgan tizim** muhim rol o‘ynaydi. Bu borada Raqamli texnologiyalar vazirligi huzurida “Deepfake va Raqamli Manipulyatsiyalarni Aniqlash bo‘yicha Milliy Markaz” tashkil etilishi, uning faoliyati Huquqni muhofaza qilish organlari, AOKA hamda tegishli ilmiy-tadqiqot institutlari bilan uzviy hamkorlikda olib borilishi maqsadga muvofiq. Markazning asosiy vazifalariga sun’iy intellekt asosidagi forensika tizimlarini joriy qilish, deepfake kontentini real vaqt rejimida aniqlash, davlat organlariga ekspert xulosalari taqdim etish va texnik standartlarni ishlab chiqish kiradi.

Shuningdek, deepfake texnologiyalarining salbiy oqibatlarini kamaytirish uchun **ta’limiy va ilmiy yondashuv** ham shunchalik muhimdir. Oliy, o`rta va o`rta-maxsus ta’lim muassasalarida “Media xavfsizligi”, “AI etikasi” kabi fanlar joriy etilishi, o‘quvchi va talabalar o‘rtasida raqamli savodxonlikni oshirish bo‘yicha tizimli dasturlar ishlab chiqilishi zarur. Shu bilan birga, ommaviy axborot vositalari va blogerlar uchun deepfake kontentining belgilanmagan yoki manipulyativ shaklda tarqatilishiga oid professional standartlar ishlab chiqilishi ham dolzarbdir.

Binobarin, huquqiy normalarning aniq belgilanishi, texnik ekspertiza tizimlarining yaratlishi, idoralararo muvofiqlashtirish mexanizmlarining yo‘lga qo‘yilishi va jamoatchilikning media xabardorligini oshirish orqali deepfake texnologiyalarining

noqonuniy qo‘llanishining oldini olish mumkin. Mazkur yondashuvlar orqali mamlakatimizda global tajriba asosida mazkur sohada samarali va xavfsiz boshqaruv modelini shakllantirishi mumkin.

References:

1. Microsoft Corporation. Video Authenticator: A Tool for Deepfake Detection.
2. DARPA. MediFor Program: Media Forensics for Deepfake Detection.
3. AQSH Deepfake Accountability Act (2023).
4. Europol. Reports on Digital Media Manipulation.
5. Deeptrace Labs. Research on Deepfake Technologies.
6. Root-nation gadjetlar va texnologiyalarga bag‘ishlangan veb-sayt.
7. Unite.AI Sun'iy intellekt va uning qo'llanilishi haqida ma'lumot beruvchi platforma.
8. MPost.io – Texnologiyalar, startaplar va innovatsiyalar haqida yangiliklar va maqolalar chop etuvchi onlayn nashr.
9. www.lex.uz. (Milliy qonunchilik bazasi.)
10. Buzb.uz – O’zbekiston va jahon yangiliklarini yorituvchi onlayn nashr.
11. Kursiv.media – Markaziy Osiyo mintaqasidagi iqtisodiy va biznes yangiliklarini yorituvchi onlayn nashr.