DEEPFAKE TEXNOLOGIYALARI: HUQUQIY JAVOBGARLIK VA KIBERXAVFSIZLIK MUAMMOLARI

Abdazimov Saidaminxo‘ja Zoirxo‘ja o‘g‘li
O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi o‘qituvchisi;

Annotatsiya: *Ushbu maqolada sun’iy intellekt asosida yaratilayotgan deepfake texnologiyalarining huquqiy tavsifi, ularning kiberxavfsizlikka va shaxs huquqlariga keltirayotgan tahdidlari hamda dunyo davlatlarining ushbu sohadagi qonunchilik tajribasi tahlil etiladi. Maqolada GAN texnologiyasining ishlash mexanizmi, deepfake yordamida amalga oshirilayotgan jinoyat turlari va ularni isbotlashdagi huquqiy muammolar ko‘rib chiqiladi. AQSh, Xitoy, Yevropa Ittifoqi va Buyuk Britaniyaning maxsus qonunchilik choralari qiyosiy tahlil qilinadi.*

Kalit so‘zlar: *deepfake, sun’iy intellekt, GAN texnologiyasi, kiberxavfsizlik, huquqiy javobgarlik, raqamli firibgarlik, ovozni sintez qilish, disinformatsiya.*

Аннотация: *В данной статье анализируются правовая характеристика технологий дипфейк, создаваемых на основе искусственного интеллекта, угрозы, которые они представляют для кибербезопасности и прав личности, а также законодательный опыт мирового сообщества в данной области. В статье рассматриваются механизм работы технологии GAN, виды преступлений, совершаемых с использованием дипфейк, и правовые проблемы их доказывания. Проводится сравнительный анализ специальных законодательных мер США, Китая, Европейского союза и Великобритании.*

Ключевые слова: *дипфейк, искусственный интеллект, технология GAN, кибербезопасность, правовая ответственность, цифровое мошенничество, синтез голоса, дезинформация.*

Abstract:*This article analyzes the legal characterization of deepfake technologies developed on the basis of artificial intelligence, the threats they pose to cybersecurity and individual rights, and the legislative experience of world states in this field. The article examines the operating mechanism of GAN technology, the types of crimes committed using deepfakes, and the legal challenges of proving them. A comparative analysis is conducted of the special legislative measures adopted by the United States, China, the European Union, and the United Kingdom.*

Keywords: *deepfake, artificial intelligence, GAN technology, cybersecurity, legal liability, digital fraud, voice synthesis, disinformation.*

KIRISH

Raqamli texnologiyalarning jadal rivojlanishi bilan birga yangi avlod kibertahdidlari ham paydo bo‘lmoqda. Ularning eng xavflisi — “deepfake” texnologiyasi bo‘lib, u sun’iy intellekt yordamida shaxsning yuzini, ovozini va harakatlarini ishonchli

tarzda soxtalashtirish imkonini beradi. “Deep” (chuqur o‘rganish) va “fake” (soxta) so‘zlarining qo‘shilmasidan hosil bo‘lgan bu atama 2017 yilda Reddit platformasida paydo bo‘lgan bo‘lsa-da, bugungi kunda u global miqyosdagi huquqiy va ijtimoiy muammoga aylangan.

Ommaviy axborot vositalarida siyosatchilar, biznesmenlar va oddiy fuqarolar nomidan uydirma bayonotlar tarqatish, firibgarlik, shantaj va obro‘ga zarar yetkazish maqsadlarida deepfake texnologiyasidan foydalanish holatlari yildan-yilga ko‘payib bormoqda. Sensity AI tadqiqot kompaniyasining ma‘lumotlariga ko‘ra, internetdagi deepfake videolar soni 2019 yildan 2023 yilga qadar 9 barobar oshgan. Ushbu hodisa nafaqat kiberxavfsizlik, balki sud-huquq tizimi, shaxsiy hayot daxlsizligi va ommaviy axborotning ishonchliligi uchun ham jiddiy muammo tug‘dirmoqda.

Maqolaning maqsadi deepfake texnologiyasining texnik mohiyatini huquqiy nuqtai nazardan tahlil etish, uning jinoyat turlari sifatidagi tavsifini aniqlash va xorijiy davlatlar tajribasi asosida O‘zbekiston qonunchiligi uchun tavsiyalar ishlab chiqishdan iborat.

DEEPFAKE TEXNOLOGIYASINING TEXNIK ASOSLARI VA TAHDID DARAJASI

Deepfake texnologiyasi asosini Generative Adversarial Network (GAN) — ya’ni raqobatdosh generativ tarmoq tashkil etadi. Bu arxitektura 2014 yilda Ian Goodfellow tomonidan taklif etilgan bo‘lib, u ikki neyron tarmoqdan iborat: generator (soxta kontent yaratuvchi) va diskriminator (soxta va haqiqiyni ajratuvchi). Ikkala tarmoq bir-biriga qarshi o‘qitilib, natijada generator shunchalik mukammal soxta kontent yaratadiki, diskriminator uni haqiqiydan farqlay olmay qoladi.

Deepfake texnologiyasi uch asosiy turga bo‘linadi. Birinchisi — yuz almashtiruv (face swap): mavjud video yoki rasmda bir shaxsning yuzi boshqasining yuzi bilan almashtiriladi. Ikkinchisi — ovoz sintezi (voice cloning): 3-5 daqiqalik ovoz namunasi asosida ixtiyoriy matnni o‘sha shaxsning ovozida gapirtirish mumkin bo‘lgan model yaratiladi. Uchinchisi — to‘liq sintez (full synthesis): kompyuter tomonidan to‘liq yaratilgan, haqiqatda mavjud bo‘lmagan shaxsning video va audio tasviri shakllantiriladi.

Deepfake ning tahdid darajasiga kelganda, World Economic Forum ning 2023 yilgi hisobotida deepfake texnologiyasi keyingi o‘n yillikdagi eng xavfli texnologik tahdidlar ro‘yxatida 3-o‘rinni egallagan. FBI ning 2022 yilgi ogohlantirishida deepfake orqali uyushtirilayotgan tadbirkorlik elektron pochta firibgarligi (Business Email Compromise) holatlari 2019 yilga nisbatan 65 foizga oshgani qayd etilgan. Shuningdek, Europol ning 2022 yilgi tahlilida deepfake texnologiyasi yo‘l qo‘ygan 96 foiz hollarda jabrlanuvchi ayollar bo‘lgani va ularning aksariyatida shantaj maqsadlari ko‘zlangani aniqlangan.

HUQUQIY JAVOBGARLIK: KIM JAVOBGAR?

Deepfake texnologiyasi bilan bog‘liq jinoyatlarda huquqiy javobgarlikni belgilash an’anaviy huquq normalari doirasida bir qator qiyinchiliklarni keltirib chiqaradi. Javobgarlik masalasi uch toifada ko‘rib chiqiladi.

Yaratuvchining javobgarligi. Deepfake yaratuvchi shaxs, qoida tariqasida, asosiy javobgar hisoblanadi. Biroq anonim identifikatsiya muammosi tufayli yaratuvchini aniqlash koʻpincha qiyin. Bundan tashqari, bir qator mamlakatlar qonunchiligida deepfake ni yaratishning oʻzi (tarqatmasdan) jinoyat sifatida belgilanmagan, bu esa huquqiy boʻshliq hosil qiladi.

Tarqatuvchining javobgarligi. Deepfake kontentni ongli ravishda tarqatgan shaxs ham javobgarlikka tortilishi mumkin. AQSh va Yevropa huquqida “knowingly distribute” (ongli tarqatish) tamoyili asosida bunday shaxslarni jinoiy ta’qib qilish imkoniyati mavjud. Biroq anonim tarqatish platformalarida bu ham qiyin kechadi.

Platformalar javobgarligi. Kontent joylashtirilgan ijtimoiy tarmoqlar va video platformalar ham cheklangan javobgarlikka ega. AQShning CDA (Communications Decency Act Section 230) 230-moddasiga koʻra, platformalar uchinchi shaxslar tomonidan joylashtirilgan kontent uchun odatda javobgar hisoblanmaydi. Biroq YeIning Digital Services Act (2022) bu yondashuvni oʻzgartirdi va yirik platformalardan deepfake kontentni faol aniqlash va oʻchirish majburiyatini qoʻydi.

Jinoyat turlari sifatidagi tavsif. Deepfake yordamida sodir etiladigan asosiy jinoyatlar quyidagilardan iborat: raqamli firibgarlik — boshqa shaxs nomidan moliyaviy mablagʻ talab qilish; tuhmat va obroʻga zarar yetkazish — yolgʻon bayonotlar tarqatish; shantaj — deepfake kontentni tarqatish tahdidi orqali tovlamachilik; siyosiy manipulyatsiya — siyosatchilar nomidan uydirma bayonotlar tarqatish; davlat sirlarini oshkor qilish taqlidini misol qilib keltirishimiz mumkin.

Isbotlash muammosi. Deepfake ni sudda isbotlash kriminalistika fanining yangi va murakkab yoʻnalishi hisoblanadi. Raqamli izlar oʻchirilgan yoki manipulyatsiya qilingan hollarda ekspertiza qilish qiyinlashadi. Hozirda Microsoft, Adobe va Intel kabi kompaniyalar raqamli kontent autentifikatsiyasi (Content Authenticity Initiative — CAI) tizimlarini ishlab chiqmoqda, bu tizimlar kontent yaratilgan paytdanoq raqamli imzo bilan belgilash imkonini beradi.

XALQARO HUQUQIY TAJRIBA

Amerika Qoʻshma Shtatlari

AQSh deepfake ni tartibga solishda federal va shtat qonunchiligining kombinatsiyasidan foydalanadi. Federal darajada 2019 yilda qabul qilingan DEEPFAKES Accountability Act (DEFPA) deepfake kontent yaratuvchilarga uni tegishli ravishda belgilash (labeling) majburiyatini yukladi. Bundan tashqari, 2023 yilda Senat tomonidan taklif etilgan NO FAKES Act loyihasi shaxsning raqamli tasviridan uning roziligisiz foydalanishni federal jinoyat sifatida belgilashga qaratilgan.

Shtat darajasida Virjiniya (2019), Kaliforniya (2019), Teksos (2023) va Jorjiya (2023) shtatlari deepfake ga oid maxsus qonunlar qabul qildi. Xususan, Teksos qonuni saylov kampaniyalarida deepfakedan foydalanishni jinoyat deb belgilagan boʻlsa, Virjiniya qonuni yashirin yuz almashtiruvchi tasvirlarni tarqatish uchun 2500 dollar miqdorida jarimani nazarda tutadi.

Xitoy Xalq Respublikasi

Xitoy 2022 yil yanvarida dunyodagi birinchi maxsus deepfake qonuni — “Deep Synthesis” qoidalarini qabul qildi. Ushbu qoidalarga koʻra, deepfake kontent yaratuvchilar uni majburiy ravishda “AI tomonidan yaratilgan” deb belgilashi shart. Foydalanuvchilar oʻzining haqiqiy shaxsini roʻyxatdan oʻtkazishi va deepfake da qatnashgan shaxslarning roziligini olishi majburiy. Qoidalarni buzganlik uchun xizmat koʻrsatuvchi platformalar va kontent yaratuvchilarga jiddiy ma’muriy jarimalar belgilangan.

YeI deepfake ni tartibga solishda bir necha me’yoriy hujjatdan foydalanadi. EU AI Act (2024) yuqori xavfli SI tizimlari roʻyxatiga deepfake generatorlarini kiritdi va ularni majburiy roʻyxatdan oʻtkazish hamda shaffoflik talablariga boʻysundirdi. Digital Services Act (2022) yirik platformalardan deepfake kontentni tizimli monitoring qilish va foydalanuvchilarni xabardor qilishni talab qiladi. GDPR esa shaxs tasviridan uning roziligisiz foydalanishni shaxsiy ma’lumotlarni qayta ishlash qoidalarini buzish deb belgilaydi.

Amaliyotda Germaniyada 2021 yilda siyosiy deepfake tarqatgan shaxs 2 yil shartli qamoq jazosiga hukm qilingan. Fransiyada 2022 yilda deepfake orqali firibgarlik amalga oshirgan guruh 3,5 million evro miqdorida zarar etkazgan va guruh a’zolari 5 yilgacha qamoq jazosiga tortilgan.

Buyuk Britaniya

Buyuk Britaniya 2023 yilda Online Safety Act qonunini qabul qilib, unda rozilik olinmagan soxta tasvirlarni tarqatishni jinoiy javobgarlikka tortadigan alohida modda kiritdi. 2024 yilda esa Criminal Justice Bill loyihasida deepfake yaratishning oʻzini (tarqatmasdan ham) jinoyat sifatida belgilash taklif etildi — bu dunyodagi eng qat’iy yondashuv hisoblanadi.

OʻZBEKISTONDA HUQUQIY BOʻSHLIQ VA TAVSIYALAR

Oʻzbekiston amaldagi qonunchiligida deepfake atamasiga va u bilan bogʻliq jinoyatlarga oid maxsus me’yorlar mavjud emas. Biroq deepfake yordamida sodir etilgan jinoyatlarga qisman qoʻllanilishi mumkin boʻlgan bir qator normalar mavjud. Jinoyat kodeksining 168-moddasi (firibgarlik), 139-moddasi (tuhmat)

va 189-moddasi (kompyuter tizimlariga noqonuniy kirish) ushbu toifadagi jinoyatlarga cheklangan tarzda qoʻllanilishi mumkin boʻlsa-da, ular deepfake ning oʻziga xos xususiyatlarini toʻliq qamrab olmaydi.

Oʻzbekistonda deepfake tahdidining dolzarbligi. 2023 yilda Oʻzbekistonda bir necha yirik firibgarlik holatlari qayd etilgan boʻlib, ularda shaxslarning ovozi va tasviri soxtalashtirilgan.

Xususan, bank xodimlari nomidan uydirma qoʻngʻiroqlar uyushtirish va ijtimoiy tarmoqlarda siyosiy shaxslar nomidan soxta videolar tarqatish holatlari davlat organlari tomonidan qayd etilgan. Bu esa Oʻzbekistonda ham deepfake muammosi amaliy ahamiyat kasb etayotganidan dalolat beradi.

Huquqiy boʻshliqni bartaraf etish boʻyicha tavsiyalar. Birinchidan, Jinoyat kodeksiga “Raqamli kontent soxtalashtirish” deb nomlanuvchi alohida modda kiritish

maqsadga muvofiq. Ushbu modda deepfake yaratish, tarqatish va undan noqonuniy maqsadlarda foydalanishni alohida jinoyat turi sifatida belgilashi lozim. Ikkinchidan, “Sun’iy intellekt asosida yaratilgan kontent” belgisini majburiy qiluvchi me’yoriy hujjat ishlab chiqish zarur. Uchinchidan, Raqamli texnologiyalar vazirligi tarkibida deepfake kontentni aniqlash va monitoring qiluvchi maxsus bo‘lim tashkil etish taklif etiladi. To‘rtinchidan, YeIning GDPR tajribasidan kelib chiqib, shaxs tasviridan va ovozidan uning roziligisiz tijorat yoki boshqa maqsadlarda foydalanishni qonuniy tartibga solish lozim.

XULOSA

Deepfake texnologiyasi bugungi kunda huquq, kiberxavfsizlik va ommaviy axborot sohalari kesishmasida yotuvchi eng murakkab muammolardan biriga aylangan. Ushbu texnologiyaning GAN asosidagi ishlash mexanizmi uni an’anaviy kriminalistik usullar bilan aniqlashni qiyinlashtiradi, huquqiy jihatdan esa yaratuvchi, tarqatuvchi va platformalar o‘rtasidagi javobgarlik taqsimoti aniq tartibga solinmagan.

Xorijiy davlatlar tajribasi shuni ko‘rsatmoqdaki, faqat texnik choralar yoki faqat qonuniy tartibga solish yetarli emas — samarali kurash uchun ikkala yondashuv birgalikda qo‘llanilishi zarur. O‘zbekiston uchun ushbu sohada alohida qonunchilik normalarini ishlab chiqish, raqamli kontent autentifikatsiyasi tizimlarini joriy etish va xalqaro hamkorlikni kuchaytirish — bu uchta yo‘nalish ustuvor vazifa bo‘lib qolmoqda. Raqamli iqtisodiyot va axborot xavfsizligi sohasida olib borilayotgan islohotlar doirasida deepfake muammosiga ham alohida e‘tibor qaratish davr talabiga aylangan.

FOYDALANILGAN ADABIYOTLAR:

1. Umarov Sh.A., Abduqodirov A.. Axborot xavfsizligi tizimlarini intellektuallashtirish masalalari. Al-Farg’oniy avlodlari, 15(3), 45–60.2024

2. Kenjaboyev O. T., Allanazarov, A. Sh.. Axborot tizimi xavfsizligi. Toshkent: Uzsmart. 2013

3. Turdimatov, M.M., Sadirova X.X.. Axborotni himoyalashda chetlab o‘tishning mumkin bo‘lgan ehtimollik holatini baholash usullari. Cybersecurity Journal, 27(2), 112–130.2023

4. Umarov Sh. A., Sun’iy intellekt asosida tahdidlarni aniqlash. Farg‘ona: Fan va texnologiya. 2019

5. Muxtarov F. M., Toshpulatov S. M.. Sun’iy intellekt vositalarini ta’limni nazorat qilish va baholashda qo‘llash. Information Systems Review, 19(4), 78–95.2023

6. Khabibullayevich, M. R., & Khatamovich, D. M. (2025). Modern intellectual systems: status, functions, technologies and development tendencies. American Journal Of Applied Science And Technology, 5(02), 52-55.

7. Li, Bingcheng, Dingkang Li, and Mingyuan Zhu. “Application analysis of data encryption technology”. Applied and Computational Engineering 50, no. 1 (March 25, 2024): 199–205. http://dx.doi.org/10.54254/2755-2721/50/20241502.

8. Abdullayev A., Qosimova U., Axborot xavfsizligi asoslari. Uslubiy qoʻllanma. Studylib.net. 2009.

9. Toshpulatov Sh. M.. Blockchain va Zero Trust Security modeli. Samarqand: Innovatsion texnologiyalar nashriyoti. 2022

10. Abdazimov, S., & Djamatov, M (2026). Biometric authentication: modern methods of ensuring information security. Научный Фокус, 3(34), 222-230.

11. Abdazimov, S., & Djamatov, M. (2026). Simmetrik kriptotizimlarda oʻrniga qoʻyish algoritmlarining qiyosiy tahlili va amaliy ahamiyati. Научный Фокус, 3(34), 231-237.

12. Abdazimov, S., (2022). Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2(5), 109-115.

13. Мирзаева, М. Б., & Абдазимов, С. З. (2022). Использование технологий искусственного интеллекта в сфере высшего образования.

14. Abdazimov, S., & Djamatov, M (2026). Zamonaviy axborot xavfsizligi tizimlarini loyiihalash: ai va iot yondashuvlari asosida. Научный Фокус, 3(34), 313-321.