



ICHKI ISHLAR ORGANLARI FAOLIYATIDA DEEPPAKE TEXNOLOGIYALARI ORQALI SODIR ETILADIGAN KIBERJINOYATLARGA QARSHI KURASHISH VA ULARNING OLDINI OLISH MEXANIZMLARI

Ibragimov Jahongir Alisher o'g'li

O'zbekiston Respublikasi Ichki ishlar vazirligi
Akademiyasi 120-guruh kursanti

Annotatsiya

Mazkur maqolada sun'iy intellektga asoslangan "Deepfake" texnologiyalarining rivojlanishi va ularning kiberxavfsizlikka tahdidi tahlil qilingan. Ichki ishlar organlari tomonidan ushbu turdagi jinoyatlarni aniqlash, tergov qilish va oldini olishdagi mavjud muammolar hamda yechimlar o'rganilgan. Maqolada huquqiy bazani takomillashtirish, texnik ta'minotni kuchaytirish va aholining raqamli savodxonligini oshirish bo'yicha takliflar ishlab chiqilgan.

Kalit so'zlar

Deepfake, kiberjinoyat, ichki ishlar organlari, sun'iy intellekt, raqamli kriminalistika, ijtimoiy muhandislik, axborot xavfsizligi.

Механизмы борьбы с киберпреступлениями, совершаемыми с использованием технологий deepfake, и их предупреждения в деятельности органов внутренних дел

Аннотация. В данной статье проанализированы развитие технологий «Deepfake», основанных на искусственном интеллекте, и их угроза для кибербезопасности. Изучены существующие проблемы и пути их решения в деятельности органов внутренних дел по выявлению, расследованию и предотвращению преступлений данного вида. В статье разработаны предложения по совершенствованию правовой базы, усилению технического обеспечения и повышению цифровой грамотности населения.

Mechanisms for combating and preventing cybercrimes committed using deepfake technologies in the activities of internal affairs bodies

Ключевые слова: Deepfake (дипфейк), киберпреступление, органы внутренних дел, искусственный интеллект, цифровая криминалистика, социальная инженерия, информационная безопасность.

Abstract. This article analyzes the development of Artificial Intelligence-based "Deepfake" technologies and their threats to cybersecurity. The existing challenges and solutions regarding the detection, investigation, and prevention of this type of crime by internal affairs bodies are examined. The article develops proposals for improving the legal framework, strengthening technical support, and increasing the digital literacy of the population.

Keywords: Deepfake, cybercrime, internal affairs bodies, artificial intelligence, digital forensics, social engineering, information security.

XXI asrda raqamli texnologiyalarning jadal rivojlanishi insoniyatga keng imkoniyatlar yaratish bilan birga, yangi turdagi tahdidlarni ham yuzaga keltirmoqda. Bugungi kunda sun'iy intellekt (SI) va neyron tarmoqlar asosida ishlaydigan **Deepfake** (inglizcha "deep learning" — chuqur o'rganish va "fake" — soxta) texnologiyasi kiberjinoyatchilikning eng xavfli qurollaridan biriga aylanib bormoqda.

O'zbekiston Respublikasida raqamli iqtisodiyot va elektron hukumat tizimining rivojlanishi fonida shaxsga doir ma'lumotlarning daxlsizligini ta'minlash va kiberfiribgarlikka qarshi kurashish Ichki ishlar organlari (IIO) oldida turgan dolzarb vazifalardan hisoblanadi. Bu borada Prezidentimiz Sh.M. Mirziyoyev ta'kidlaganidek: "Axborot texnologiyalari rivojlangani sari, kiberxavfsizlikni ta'minlash masalasi milliy xavfsizlikning ajralmas qismiga aylanib bormoqda"¹.

Deepfake – bu insonning tashqi ko'rinishi, ovozi va harakatlarini sun'iy intellekt yordamida manipulyatsiya qilib, haqiqatga o'xshash soxta audio yoki video kontent yaratish jarayonidir. Ushbu texnologiya asosan Generativ Raqobatdosh Tarmoqlar asosida ishlaydi.

Jinoyatchilar Deepfake texnologiyasidan quyidagi maqsadlarda foydalanmoqdalar:

1) Moliyaviy firibgarlik: Kompaniya rahbarlari yoki yaqin qarindoshlarning ovozini soxtalashtirish orqali pul mablag'larini o'tkazishni so'rash (vishing).

2) Obro'sizlantirish va shantaj: Jamoat arboblari yoki oddiy fuqarolarning soxta intim yoki kompromat videolarini tarqatish bilan qo'rqitish.

3) Dezinformatsiya: Davlat organlari nomidan soxta bayonotlar tarqatish orqali ijtimoiy-siyosiy barqarorlikka putur yetkazish.

Tahlillar shuni ko'rsatadiki, 2025-yilga kelib Deepfake texnologiyasidan foydalangan holda sodir etilgan firibgarlik urinishlari so'nggi uch yil ichida 21 barobarga (2137 foizga) oshgan, 2025-yilning birinchi choragidayoq qayd etilgan insidentlar soni esa 2024-yilning umumiy ko'rsatkichidan 19 foizga yuqori bo'lgan².

Aholining Deepfake hujumlariga ishonuvchanligi sabablarining viktimalogik tahlili.

Kiberjinoyatchilarning muvaffaqiyati faqatgina Deepfake texnologiyasining takomillashuvi bilan emas, balki inson psixologiyasidagi zaif nuqtalardan ustalik bilan foydalanishi bilan izohlanadi. Kriminalistik va psixologik tadqiqotlar shuni ko'rsatadiki, aholining ushbu turdagi firibgarlik qurboniga aylanishi quyidagi omillar bilan bog'liq:

1. "Ko'z bilan ko'rish orali ishonish" fenomeni. Inson miyasi ming yillar davomida ko'rish va eshitish organlari orqali olingan ma'lumotni "mutlaq haqiqat" deb qabul qilishga moslashgan. Neyrobiologik tadqiqotlarga ko'ra, insonda vizual axborotni qayta ishlash jarayoni mantiqiy tahlildan ko'ra tezroq yuz beradi. Deepfake

¹ "Qani natija?" Shavkat Mirziyoyev kiberjinoyatchilikka qarshi kurashish ishlarini tanqid qildi // elektron manbaa: <https://daryo.uz/2026/01/27/qani-natija-shavkat-mirziyoyev-kiberjinoyatchilikka-qarshi-kurashish-ishlarini-tanqid-qildi/>

² Keepnet Labs. Deepfake Statistics & Trends 2025: Growth, Risks, and Future Insights [Elektron resurs]. – URL: <https://keepnetlabs.com/blog/deepfake-statistics-and-trends>

texnologiyasi aynan shu biologik zaiflikni nishonga oladi. Video yoki ovozli xabar kelganda, miya avtomatik ravishda “Bu mening tanishim” degan signalni beradi va tanqidiy fikrlash mexanizmi bloklanadi³.

2. Hissiy manipulyatsiya va shoshilinchlik effekti Deepfake orqali sodir etiladigan jinoyatlarda ko‘pincha “Hissiy shok” usuli qo‘llaniladi. Masalan, “rahbar”ning ovozi bilan zudlik bilan pul o‘tkazish buyurilganda yoki “farzand”ning yig‘lab yordam so‘ragan videosi ko‘rsatiladi. Bu holatda insonning mantiqiy fikrlash qobiliyati pasayib, hissiy qaror qabul qilishga o‘tadi. Kiberxavfsizlik bo‘yicha ekspert K. Mitnik ta’kidlaganidek: “Texnologiya qanchalik kuchli bo‘lmasin, insonning ishonchi va qo‘rquvi har doim tizimning eng zaif bo‘g‘ini bo‘lib qoladi”⁴.

3. Avtoritetga bo‘ysunish. O‘zbekiston mentalitetida kattalarga, rahbarlarga va davlat organlari vakillariga hurmat va so‘zsiz ishonch yuqori. Jinoyatchilar Deepfake yordamida vazirlik, bank yoki huquqni muhofaza qilish organlari rahbarlarining qiyofasidan foydalanganda, fuqarolarda “buyruqni muhokama qilmasdan bajarish” refleksi ishga tushadi. Bu psixologik omil korporativ firibgarliklarda katta rol o‘ynaydi.

4. Raqamli “filtrlar”ning yo‘qligi va axborot yuki. Zamonaviy axborot makonida inson har kuni gigabaytlab ma’lumot qabul qiladi. Axborot oqimining tezligi sababli, foydalanuvchilar kontentni chuqur tahlil qilmasdan, yuzaki iste’mol qilishga o‘rgangan. Ijtimoiy tarmoqlardagi “Lenta”ni tezkor varaqlash jarayonida foydalanuvchi Deepfake videodagi mayda nuqsonlarni (masalan, lab harakatidagi desinxronizatsiya yoki g‘ayritabiiy mimika) payqamay qoladi⁵.

5. Tasdiqlash moyilligi. Agar Deepfake orqali tarqatilayotgan soxta xabar insonning mavjud qarashlariga yoki qo‘rquvlariga mos kelsa (masalan, “Dollar kursi keskin oshib ketdi” yoki “Yangi jarimalar joriy etildi”), inson uni tekshirmasdan haqiqat deb qabul qilishga moyil bo‘ladi.

Deepfake texnologiyalari yordamida sodir etilayotgan jinoyatlarning latentlik darajasi yuqoriligi va transmilliy xususiyati IIO faoliyatida an’anaviy tergov usullaridan voz kechib, innovatsion mexanizmlarni qo‘llashni taqozo etadi. Mazkur mexanizmlarni to‘rt asosiy yo‘nalishga ajratish maqsadga muvofiq:

1. Kiberjinoyatlarga qarshi kurashish samaradorligini oshirish uchun IIO tizimida quyidagi tashkiliy o‘zgarishlarni amalga oshirish lozim:

Maxsus monitoring guruhlarini tashkil etish: IIO Tezkor-qidiruv departamenti huzurida ijtimoiy tarmoqlar va messenjerlarda tarqalayotgan shubhali media-kontentni real vaqt rejimida monitoring qiluvchi sun’iy intellektga asoslangan tahlil guruhlarini shakllantirish.

Xalqaro hamkorlik platformasi: Deepfake jinoyatlari ko‘pincha chet el serverlari orqali amalga oshirilishi sababli, Interpol va Yevropolning kiberjinoyatchilik

³ Kahneman, D. Thinking, Fast and Slow. – New York: Farrar, Straus and Giroux, 2011. – 499 p.

⁴ Mitnick, K., Simon, W. The Art of Deception: Controlling the Human Element of Security. – Indianapolis: Wiley, 2002. – 352 p.

⁵ Abdullayev, R.F. Raqamli jamiyatda axborot psixologik xavfsizlik muammolari // O‘zbekiston Milliy universiteti xabarlari. – 2023. – № 1. – B. 112-115

markazlari bilan tezkor axborot almashinuvi kanallarini kengaytirish. Bu jinoyatchining raqamli izini tezkor aniqlash imkonini beradi⁶.

2. Deepfake kontentni fosh etishda “Sun’iy intellektga qarshi sun’iy intellect” (AI vs AI) tamoyiliga asoslangan texnik vositalardan foydalanish hal qiluvchi ahamiyatga ega.

IIO Ekspert-kriminalistika markazlari faoliyatiga quyidagi texnologiyalarni joriy etish taklif etiladi:

Videodagi shaxsning yurak urishi natijasida yuz terisidagi mikroskopik rang o‘zgarishlarini (fotopletismografiya) tahlil qiluvchi – biometrik nomutanosiblik tahlili dasturiy ta’minotini joriy qilish. Deepfake videolarda bu tabiiy biologik signal mavjud bo‘lmaydi.

– Ovozli firibgarlikda (vishing) sintez qilingan ovozning chastota spektrogrammasini tahlil qilishga qaratilgan fonopskopik ekspertiza tayinlash. Sun’iy ovozlarda insonga xos bo‘lmagan “mikro-uzilishlar” va raqamli shovqinlar mavjudligini aniqlash.

3. Amaldagi qonunchilikni raqamli voqelikka moslashtirish jinoyatchilarni javobgarlikka tortishning asosi hisoblanadi:

– O‘zbekiston Respublikasi Jinoyat-protsessual kodeksiga raqamli ma’lumotlar, xususan, o‘zgartirilgan media-fayllarni dalil sifatida qabul qilish va ularni ekspertizadan o‘tkazishning aniq reglamentini kiritish.

– Shaxsning biometrik ma’lumotlaridan (yuzi, ovozi) uning roziligisiz foydalanganlik uchun alohida jinoiy javobgarlik belgilash. Yevropa Ittifoqining "Sun’iy intellekt to‘g‘risidagi qonuni" (AI Act) tajribasidan kelib chiqib, Deepfake yaratuvchilari o‘z mahsulotlariga maxsus “suv belgilari” (watermark) qo‘yish majburiyatini yuklash⁷.

4. Jinoyat sodir bo‘lgandan keyin uning oqibatlari bilan kurashishdan ko‘ra, uni oldini olish iqtisodiy va ijtimoiy jihatdan samaraliroqdir.

– Mahalla va ta’lim muassasalarida IIO inspektorlari tomonidan “Ijtimoiy muhandislikdan himoyalalanish” mavzusida master-klasslar o‘tkazish.

– Katta miqdordagi pul o‘tkazmalarida mijozning shaxsini biometrik identifikatsiya qilishda (FaceID) “jonlilikni tekshirish” (Liveness detection) texnologiyasini majburiy etib belgilash bo‘yicha Markaziy bank bilan hamkorlik qilish. Bu statik fotosurat yoki telefondan ko‘rsatilgan video orqali tizimni aldashning oldini oladi.

Фойдаланилган адабиётлар:

1. “Qani natija?” Shavkat Mirziyoyev kiberjinoyatchilikka qarshi kurashish ishlarini tanqid qildi // electron manbaa: <https://daryo.uz/2026/01/27/qani-natija-shavkat-mirziyoyev-kiberjinoyatchilikka-qarshi-kurashish-ishlarini-tanqid-qildi/>

⁶ Murodov, B.Sh. Kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlikning huquqiy jihatlari // O‘zbekiston Respublikasi IIV Akademiyasi Axborotnomasi. – 2022. – № 3. – B. 45-50.

⁷ European Commission. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. – Brussels, 2021. – COM(2021) 206 final.

2. Keepnet Labs. Deepfake Statistics & Trends 2025: Growth, Risks, and Future Insights [Elektron resurs]. – URL: <https://keepnetlabs.com/blog/deepfake-statistics-and-trends>

3. Kahneman, D. Thinking, Fast and Slow. – New York: Farrar, Straus and Giroux, 2011. – 499 p.

4. Mitnick, K., Simon, W. The Art of Deception: Controlling the Human Element of Security. – Indianapolis: Wiley, 2002. – 352 p.

5. Abdullayev, R.F. Raqamli jamiyatda axborot psixologik xavfsizlik muammolari // O‘zbekiston Milliy universiteti xabarлари. – 2023. – № 1. – B. 112-115

6. Murodov, B.Sh. Kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlikning huquqiy jihatlari // O‘zbekiston Respublikasi IIV Akademiyasi Axborotnomasi. – 2022. – № 3. – B. 45-50.

7. European Commission. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. – Brussels, 2021. – COM(2021) 206 final.