ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 2 / UIF:8.2 / MODERNSCIENCE.UZ

“DEEPFAKE” ТЕХНОЛОГИЯЛАРИ ВОСИТАСИДА СОДИР ЭТИЛАЁТГАН КИБЕРЖИНОЯТЛАР: ЎЗБЕКИСТОН ШАРОИТИДАГИ ТАҲДИДЛАР, ҲУҚУҚИЙ МУАММОЛАР ВА ОЛДИНИ ОЛИШ ЧОРАЛАРИ

Choriyev Ulug‘bek Jalol o‘g‘li
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti
ilmiy xodimi, kapitan.

https://doi.org/10.5281/zenodo.18619615

Аннотация. *Мазкур мақолада deepfake технологиялари воситасида содир этилаётган кибержиноятларнинг Ўзбекистон шароитидаги кўриниши, уларнинг ҳуқуқий баҳоланиши ва олдини олиш чоралари содда тилда таҳлил қилинган. Deepfake — сунъий интеллект ёрдамида яратиладиган сохта видео, аудио ва тасвир контент бўлиб, у одамларни алдаш, фирибгарлик қилиш ва обрў тўкиш мақсадларида кенг қўлланилмоқда.*

Тадқиқот натижалари шуни кўрсатадики, Ўзбекистонда deepfake орқали амалга ошириладиган жиноятлар — молиявий фирибгарлик, шахсни қалбакилаштириш, шантаж ва сохта янгиликлар тарқатиш — йилдан-йилга кўпайиб бормоқда. Мақолада мавжуд ҳуқуқий базанинг етишмовчиликлари кўрсатилган ва амалий тавсиялар берилган.

Калит сўзлар: *deepfake, кибержиноят, сунъий интеллект, молиявий фирибгарлик, шахсни қалбакилаштириш, шантаж, Ўзбекистон, ҳуқуқий тартибга солиш, ижтимоий тармоқлар, медиа саводхонлик.*

Аннотация. *В данной статье простым языком проанализированы киберпреступления, совершаемые с помощью технологий deepfake в условиях Узбекистана, их правовая оценка и меры предотвращения. Deepfake — это поддельный видео-, аудио- и графический контент, создаваемый с помощью искусственного интеллекта, который широко используется в целях обмана, мошенничества и дискредитации. Результаты исследования показывают, что преступления с использованием deepfake в Узбекистане — финансовое мошенничество, подделка личности, шантаж и распространение фейковых новостей — растут из года в год. В статье показаны недостатки существующей правовой базы и даны практические рекомендации.*

Ключевые слова: *deepfake, киберпреступность, искусственный интеллект, финансовое мошенничество, подделка личности, шантаж, Узбекистан, правовое регулирование, социальные сети, медиаграмотность.*

Abstract. *This article analyzes cybercrimes committed using deepfake technologies in Uzbekistan, their legal assessment, and prevention measures in simple language. Deepfake is fake video, audio, and image content created using artificial intelligence, widely used for deception, fraud, and defamation. Research results show that deepfake-related crimes in Uzbekistan — financial fraud, identity forgery, blackmail, and dissemination of fake news — are increasing year by year. The article identifies gaps in the existing legal framework and provides practical recommendations.*

Keywords: *deepfake, cybercrime, artificial intelligence, financial fraud, identity forgery, blackmail, Uzbekistan, legal regulation, social networks, media literacy.*

ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 2 / UIF:8.2 / MODERNSCIENCE.UZ

КИРИШ

Тасаввур қилинг: Сизнинг таниш-билишингиз видео юборди, унда яқин қариндошингиз сиздан шошилинч равишда пул ўтказишни сўрамоқда. Овози, юзи, ҳаракатлари — ҳаммаси ўша одамники. Лекин аслида бу видеони компьютер дастури яратган ва қариндошингиз бундан умуман бехабар. Бу — deepfake технологияси орқали амалга ошириладиган фирибгарликнинг бир мисоли.

Deepfake нима? Оддий қилиб айтганда, deepfake — бу сунъий интеллект (компьютер дастурлари) ёрдамида яратиладиган сохта видео, аудио ёки расм. Бу технология ёрдамида исталган одамнинг юзини бошқа одамнинг юзига алмаштириш, овозини кўчириш ёки ҳеч қачон айтмаган сўзларни айтаётгандек кўрсатиш мумкин. "Deepfake" сўзи инглизча "deep learning" (чуқур ўқитиш) ва "fake" (сохта) сўзларидан олинган.

Бу технология нега хавфли? Чунки замонавий deepfake шу даражада сифатли яратиладики, уни ҳақиқий видеодан оддий кўз билан ажратиш деярли мумкин эмас. “Sumsub” компаниясининг 2025 йилги маълумотларига кўра, жаҳон бўйича deepfake фирибгарлик ҳолатлари бир йилда 10 баробар кўпайган. Жаҳон миқёсида deepfake жиноятлари келтираётган зарар йилига 40 миллиард доллардан ошиши башорат қилинмоқда.

Ўзбекистонда ҳам deepfake воситасида содир этилаётган жиноятлар тобора кўпайиб бормоқда. “Telegram”, “Instagram” ва “TikTok” каби ижтимоий тармоқлар орқали таниқли шахсларнинг сохта видеолари тарқатилмоқда, банк мижозлари видеоқўнғироқ орқали алданмоқда, одамлар сохта видеолар ёрдамида шантаж қилинмоқда. Бироқ, мамлакатимизда бу жиноятларни тартибга солувчи махсус қонунлар ҳали етарли эмас.

Deepfake яратиш жараёнини содда тилда тушунтирадиган бўлсак, уни расмга тушириш аппарати (фотоаппарат) ихтиро қилинишига қиёслаш мумкин. Фотоаппарат ҳақиқатни тасвирлайди, deepfake эса ҳақиқат "кўринишидаги" ёлғонни яратади.

Deepfake яратишнинг асосий усули — бу тизим иккита компьютер дастуридан иборат: биринчиси, сохта расм ёки видео яратишга ҳаракат қилади; иккинчиси, яратилган расмни ҳақиқий расмдан ажратишга ҳаракат қилади. Бу иккала дастур ўзаро "мусобақа" қилади — "сохтачи" тобора яхшироқ сохталик яратишни, "текширувчи" эса тобора яхшироқ аниқлашни ўрганади. Натижада, минглаб "мусобақа" турларидан кейин "сохтачи" шундай сифатли контент яратадики, уни "текширувчи" ҳам ажрата олмайди.

Бугунги кунда deepfake яратишнинг бир нечта тури мавжуд:

Юз алмаштириш (Face Swap). Бир одамнинг юзини бошқа одамнинг юзига алмаштириш. Масалан, фирибгар банк директорининг юзини ўз видеосига қўяди ва худди директор гапираётгандек видео яратади. “DeepFaceLab” дастури — энг кенг тарқалган юз алмаштириш воситаси бўлиб, барча deepfake видеоларнинг тахминан 95 фоизи шу дастур ёрдамида яратилган.

Овоз клонлаш (Voice Cloning). Атиги 3-10 сонияли овоз намунаси асосида исталган одамнинг овозини такрорлаш. “Microsoft” компаниясининг “VALL-E” дастури 3 сонияли овоз ёзувидан шахснинг овозини, оҳангини ва интонациясини такрорлай олади. Бу технология телефон орқали фирибгарлик қилишда айниқса хавфли.

Лабни синхронлаш (Lip Sync). Аудио ёзув асосида видеодаги одамнинг лаб ҳаракатларини автоматик ўзгартириш. Натижада, одам ҳақиқатда айтмаган сўзларни айтаётгандек кўринади.

Реал вақтда deepfake. Энг хавфлиси — видеокўнғироқ давомида реал вақтда юзни алмаштириш. Фирибгар Zoom ёки видеокўнғироқда бошқа одамнинг юзида гаплашади. Бу технология 2024 йилда Гонконгда 25,6 миллион долларлик фирибгарликда ишлатилган — фирибгарлар видеоконференцияда бир вақтда бир неча компания раҳбарларининг сохта тасвирларини яратган.

Муҳим нукта шуки, бугунги кунда deepfake яратиш учун махсус билимлар талаб қилинмайди. Мобил телефондаги бепул иловалар (“Reface”, “FaceApp”) орқали ҳар қандай одам бир неча дақиқада оддий deepfake яратиши мумкин. Мураккаб deepfake учун эса “YouTube” да юзлаб бепул дарслик мавжуд.

ЎЗБЕКИСТОНДА DEEPFAKE ВОСИТАСИДА СОДИР ЭТИЛАЁТГАН ЖИНОЯТЛАРНИНГ ТУРЛАРИ ВА МИСОЛЛАРИ

1. Молиявий фирибгарлик

Ўзбекистонда deepfake ёрдамида амалга ошириладиган молиявий фирибгарликнинг бир нечта кўриниши кузатилмоқда:

Таниқли шахслар номидан сохта видео тарқатиш. “Telegram” ва “Instagram”да таниқли бизнесменлар, блогерлар ёки давлат арбобларининг deepfake видеолари тарқатилиб, сохта инвестиция лойиҳаларига пул тикиш таклиф қилинади. Масалан, "Мен шу лойиҳага пул тикдим ва бир ойда 3 баробар кўпайтирдим" каби сохта гапириш видеоси яратилади.

Минглаб Ўзбекистон фуқаролари бу сохта видеоларга ишониб, пулларини йўқотган.

Банк ходими номидан видеокўнғироқ. Фирибгарлар банк ходимининг deepfake юз тасвирини ишлатиб, мижозларга видеокўнғироқ қилади. "Ҳисобингиздан шубҳали операция аниқланди, тасдиқлаш учун СМС кодни айтинг" дейишади. Мижоз видеода ҳақиқий банк ходимини "кўргани" учун ишониб, СМС кодни бериб юборади ва пулларини йўқотади.

Қариндош-уруғ номидан сохта видео юбориш. Фирибгарлар ижтимоий тармоқлардан топилган расм ва видеолар асосида қурбоннинг яқинининг deepfake видеосини яратиб, "шошилинч, менга 2 000 000 сўм ўтказ, кечқурун қайтараман" каби хабарлар юборади. Яқин одамнинг юзи ва овозини кўриб-эшитган қурбон тезда пул ўтказади.

2. Шахсни қалбакилаштириш

Ўзбекистонда рақамли хизматлар “Click”, “Payme”, “Uzum Bank”, “MyID” жадал ривожланмоқда. Бу платформаларнинг кўпчилиги фойдаланувчини аниқлаш учун юзни таниш (Face ID) тизимидан фойдаланади. Deepfake технологияси бу тизимларга жиддий таҳдид солади:

Биометрик тасдиқлашни алдаш. Фирибгар қурбоннинг расмлари асосида deepfake видео яратиб, MyID ёки банк иловасининг юзни таниш тизимини алдашга ҳаракат қилади.

Жаҳон тажрибасида deepfake тасвирлар юзни таниш тизимларининг 68 фоизини муваффақиятли алдагани аниқланган.

Бошқа шахс номидан кредит олиш. Фирибгар deepfake ёрдамида бошқа одамнинг шахсини сохталаштириб, унинг номидан банкдан кредит олиши ёки молиявий хизматлардан фойдаланиши мумкин. Бу ҳолда ҳақиқий шахс фақат қарз ундириш хабарномасини олганда воқеадан хабар топади.

3. Шахсларни обрўсизлантириш

Deepfake технологиясининг энг кўп ишлатиладиган ва энг хавфли йўналишларидан бири — шантаж. Жаҳон статистикасига кўра, барча deepfake видеоларнинг 96 фоизи ноқонуний контент ҳисобланади. Ўзбекистонда бу жиноятнинг қуйидаги кўринишлари кузатилмоқда:

Сохта видео яратиб шантаж қилиш. Фирибгар қурбоннинг ижтимоий тармоқлардаги расмларидан фойдаланиб, уни шарманда қиладиган сохта видео яратади ва видеони тарқатилмаслиги учун пул тўлашни айтиб шантаж қилади. Жабрланувчи ўзининг обрўсидан қўрқиб, пул тўлайди.

Сиёсий ва ижтимоий шахсларнинг обрўсини тўкиш. Deepfake ёрдамида давлат хизматчилари, журналистлар ёки жамоат арбобларининг сохта видеолари яратилиб, уларнинг обрўсини тўкиш мақсадида тарқатилади. Бу ҳолатлар жамиятда ишончсизлик ва тарқоқлик уйғотади.

Кибербуллинг. Мактаб ўқувчилари ва ёшлар орасида deepfake иловалар ёрдамида тенгдошларининг сохта видеоларини яратиб, уларни масхара қилиш ҳолатлари кузатилмоқда.

Бу рақамли зўравонликнинг янги ва хавфли кўриниши бўлиб, қурбонларда жиддий руҳий оқибатларга олиб келиши мумкин.

4. Сохта янгиликлар ва дезинформация

Deepfake технологияси сохта янгиликлар *(fake news)* яратиш ва тарқатишда ҳам кенг қўлланилмоқда. Ўзбекистонда қуйидаги ҳолатлар кузатилган:

Давлат раҳбарлари номидан сохта баёнотлар. Deepfake ёрдамида давлат раҳбарлари ёки масъул шахсларнинг ҳеч қачон айтмаган гапларини "айтаётган" видеолар яратилиб тарқатилади. Бу жамиятда тўлқинланиш ва ваҳима уйғотиши мумкин.

Иқтисодий ваҳима тарқатиш. “Банклар ёпилади”, “валюта курси кескин ўзгаради” каби сохта хабарларни таниқли шахслар “тасдиқлаётган” deepfake видеолар яратилиб, аҳоли орасида ваҳима уйғотилади.

Ҳозирги кунда Ўзбекистон Республикасининг қонунчилигида “deepfake” тушунчаси расман белгиланмаган ва бу технология ёрдамида содир этилган жиноятларни тартибга солувчи махсус норма мавжуд эмас. Бироқ, мавжуд қонунчилик доирасида deepfake жиноятларни маълум даражада квалификация қилиш мумкин:

Жиноят кодексининг 168-моддаси (Фирибгарлик). Deepfake ёрдамида бошқа шахсларни алдаб молиявий зарар етказиш ҳолатлари мазкур модда бўйича квалификация қилиниши мумкин. Бироқ, модда матнида deepfake технологиясининг хусусиятлари кўрсатилмаган, бу эса исботлаш жараёнини қийинлаштиради.

Жиноят кодексининг 278-моддаси (Компьютер маълумотларидан рухсатсиз фойдаланиш). Deepfake яратиш учун бошқа шахснинг расм ва видеоларини рухсатсиз ишлатиш ҳолатларига мазкур модда қўлланилиши мумкин.

ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 2 / UIF:8.2 / MODERNSCIENCE.UZ

Фуқаролик кодексининг 100-моддаси (Шахснинг шаъни ва қадр-қимматини ҳимоя қилиш). Deepfake контент орқали шахснинг обрўсига путур етказилганда қурбон фуқаролик даъво қўзғатиши мумкин.

“Шахсга доир маълумотлар тўғрисида”ги Қонунда шахсий расм ва видеоларни рухсатсиз ишлатиш бу қонун доирасида баҳоланиши мумкин, бироқ deepfake контекстида махсус механизмлар кўрсатилмаган.

Хорижий тажриба. Бир қатор мамлакатлар deepfake жиноятларни тартибга солиш бўйича махсус қонунлар қабул қилган:

АҚШда “DEEPFAKES Accountability Act” қабул қилинган бўлиб, deepfake контентни мажбурий белгилаш талаби ўрнатилган; Хитойда 2023 йилдан бошлаб "чуқур синтез" (deep synthesis) технологияларини тартибга солувчи қоидалар кучга кирган; Европа Иттифоқида доирасида deepfake контентни белгилаш мажбурий этилган; Жанубий Кореяда deepfake порнографик контент яратиш ва тарқатиш учун 5 йилгача озодликдан маҳрум қилиш жазоси белгиланган.

DEEPFAKE КОНТЕНТНИ АНИҚЛАШ ВА ЎЗИНИ ҲИМОЯ ҚИЛИШ УСУЛЛАРИ

1. Оддий одам deepfake ни қандай аниқлайди?

Ҳар бир инсон қуйидаги белгиларга эътибор бериб, deepfake контентни аниқлашга ҳаракат қилиши мумкин:

Кўзларга эътибор беринг. Deepfake видеоларда кўзлар кўпинча нотабиий кўринади: кўз равшанлиги (ёруғлик акси) иккала кўзда бир хил бўлмайди, кўз юмиб-очиш ҳаракати нотабиий тезликда бўлади, кўзнинг атрофидаги тери текстураси бузилган бўлиши мумкин.

Юз чегараларини текширинг. Deepfake видеоларда юз билан бош орасидаги чегарада — айниқса пешона, қулоқ ва бўйин атрофида нотабиийликлар кузатилиши мумкин: ранг фарқи, хиралик ёки ўткир чизиқлар.

Лаб ҳаракатларига эътибор беринг. Овоз билан лаб ҳаракатлари бир-бирига тўғри келадими? Deepfake видеоларда кўпинча лаб ва товуш бир-бирига тўлиқ мос келмайди.

Табиий ҳаракатларни кузатинг. Ҳақиқий одам гапираётганда бошини буради, қўл ҳаракатлари қилади, юз ифодалари табиий ўзгаради. Deepfake видеоларда бу ҳаракатлар кўпинча қотиб қолгандек кўринади.

Сифатга эътибор беринг. Видеонинг умумий сифатига қаранг юз атрофида хиралик, видеонинг кадрлар орасида “сакраш”лар, ёруғлик ва соялар нотабиий кўриниши deepfake белгиси бўлиши мумкин.

2. Техник аниқлаш воситалари

Замонавий технологиялар deepfake контентни автоматик аниқлашга ёрдам беради. “Microsoft Video Authenticator” — “Microsoft” компаниясининг бепул воситаси бўлиб, видео ва расмларнинг deepfake эканлигини фоиз кўрсаткичи билан аниқлайди.

“Deepware Scanner” — мобил илова бўлиб, видеоларни deepfake эканлигини текшириш имконини беради. “Intel Fake Catcher” — реал вақтда deepfake аниқлайдиган тизимлар ҳисобланади.

3. Ўзини ҳимоя қилиш қоидалари

Шахсий расм ва видеоларни ҳимоялаш. Ижтимоий тармоқлардаги ҳисобларнинг махфийлик созламаларини кучайтиринг — расм ва видеоларингиз фақат танишларингизга кўринсин. Юқори сифатли юз расмларини оммавий жойлашда чекланг. Deepfake яратиш учун фирибгарга сизнинг расмларингиз керак — расмларингиз қанча кам бўлса, хавф шунча паст бўлади.

Шубҳали видеоқўнғироқларга эҳтиёткорлик. Кутилмаган видеоқўнғироқ орқали пул ўтказиш сўралса — олдин тўхтаб ўйланг. Қўнғироқ қилган шахсга мустақил равишда — ўзингиз билган рақам орқали — қайта қўнғироқ қилиб текширинг. Видеоқўнғироқда ноодатий саволлар беринг — масалан, "кеча нима гаплашган эдик?" каби фақат ҳақиқий шахс билиши мумкин бўлган саволлар.

Молиявий операцияларда эҳтиёткорлик. Ҳеч қачон фақат видео ёки аудио қўнғироқ асосида катта миқдордаги пул ўтказманг. Ҳар доим иккинчи канал орқали тасдиқланг — масалан, юзма-юз учрашув ёки бошқа ишончли алоқа воситаси орқали.

Deepfake ҳақида хабардор бўлинг. Оила аъзоларингиз, айниқса кекса авлод ва болаларга deepfake хавфлари ҳақида тушунтиринг. "Кўрган нарсангизнинг ҳаммаси ҳам ҳақиқат эмас" — бу тамойилни ёдда тутинг.