Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN (Print) 2616-7174. ISSN (Online) 2663-2500

ЖАҢА МЕДИА / НОВЫЕ МЕДИА / NEW MEDIA

ХҒТАР 070.1:004.932.2
Шолу мақала

https://doi.org/10.32523/2616-7174-2026-156-3-168-181

Синтетикалық медиа форензикасының даму бағыттары (Қазақстан мысалында)

Н.Ж. Кошкенов*[1], И.У. Салиев[2], Б. Тогтарбай*[3]

[1,2,3]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

*(E-mail: *[1]koshkenov_nzh_2@enu.kz, [2]islam_1407@mail.ru, [3]beibit.toktarbai78@gmail.com)*

Аңдатпа. Бұл мақалада генеративті жасанды интеллект (ЖИ) технологияларының қарқынды дамуы салдарынан туындаған жаңа ақпараттық сын-қатерлер мен оларды анықтауға арналған заманауи форензикалық әдіс-тәсілдерге шолу жасалады. Қазіргі машиналық оқыту алгоритмдерінің эволюциясы шынайы контент пен жасанды медиа арасындағы айырмашылықты адам көзіне көрінбейтін деңгейге жеткізе бастады. Атап айтқанда, мақалада дипфейктер банктердің KYC (Know Your Customer – «клиентті тану») хаттамаларын бұзудағы қаржылық алаяқтық схемалары мен саяси манипуляцияларының зиянды әлеуеті талданады. Зерттеу жұмысында FaceForensics++ сияқты халықаралық бенчмарктерді қолдану тәжірибесі де сараланады, конволюциялық нейрондық желілерді (CNN) пайдаланған кеңістіктік талдаудан бастап дискретті косинустық түрлендіруге (DCT) негізделген жиілік аналитикасына, физиологиялық биометрия (rPPG) мен аудиовизуалды фонетикалық сәйкессіздікті бағалаудың инновациялық әдістеріне дейінгі озық тәсілдер де қарастырылады. Мақалада Қазақстан ақпараттық кеңістігіндегі синтетикалық медианың таралуы, қазақ-орыс екітілді ортада пайда болатын фонетикалық артефактілер мен «Жасанды интеллект туралы» жаңа заңдағы құқықтық мәселелер зерделенеді. Қорытындылай келе, шетелдік детекторларды пассивті импорттаудан бас тартып, локализацияланған ұлттық деректер жинақтарын құруға, тәуелсіз алгоритмдік медиа-аудит институтын қалыптастыруға және фактчекинг үдерісіне заманауи форензика құралдарын кіріктіруге стратегиялық көшудің қажеттілігі негізделеді.

Түйін сөздер: синтетикалық медиа форензика, дипфейк, жасанды интеллект, ақпараттық қауіпсіздік, rPPG, CNN, Қазақстан.

Түсті: 31.08.2026; Мақұлданды: 27.09.2026; Онлайн қолжетімді: 30. 09. 2026

***хат-хабар авторы**

Кіріспе

Соңғы бес жыл ішінде машиналық оқыту алгоритмдері түбегейлі трансформацияға ұшырады. Алғашында тек медиа контентті талдау мен жіктеу үшін ғана қолданылған құралдар қазір гипершынайы суреттер, бейнежазбалар мен аудиожазбаларды дербес жасай алатын қуатты генеративтік жүйелерге айналды. Бұл технологиялық серпілістің негізінде есептеу қуаттылығының артуы мен орасан зор деректер массивтері жатыр, олар өз кезегінде цифрлық шындық туралы ұғымды түбірімен өзгерткен жасанды интеллекттің екі фундаменталды архитектурасының дамуына жол ашты.

Біріншісі – генеративті-жауласушы нейрондық желілер (Generative Adversarial Networks, GAN). Бұл архитектураның негізінде бір-бірімен үздіксіз бәсекелесетін екі нейрондық алгоритм – генератор мен дискриминатор жатыр. Генератор синтетикалық деректерді үздіксіз жасап, оларды нақты үлгілерге барынша ұқсатуға тырысады. Өз кезегінде, дискриминатор ұсынылған контентті талдап, оның жасанды немесе шынайы екенін ажырату міндетін атқарады. Осындай антагонистік оқыту үдерісі барысында екі модель де бірін-бірі жетілдіреді: генератор адам қабылдауы мен қарапайым алгоритмдер жалғанды шындықтан ажырата алмайтындай деңгейге жеткенге дейін гипершынайы контент (дипфейк) генерациялауды жалғастырады (Goodfellow et al., 2014).

Ал екіншісі бұдан жаңарақ архитектура саналатын Midjourney, DALL-E және басқа да заманауи бейне генераторлар платформаларында кеңінен қолданылатын диффузиялық модельдер. Бұл модельдер Марков тізбегіне негізделген термодинамикалық диффузия процесін имитациялайды. Яғни, олар алдымен оқу деректеріне біртіндеп гауссиандық шуыл қосып, оны толық деструкциялайды, содан кейін күрделі нейрондық желіні кері шуылды жою процесіне үйрету арқылы жұмыс істейді. Бұл бастапқы статикалық шуылдан жоғары сапалы, семантикалық тұрғыдан мінсіз медиа контентті синтездеуге мүмкіндік береді.

Осы технологиялық жетістіктер шығармашылық индустриялар, кинематограф, жарнама және бейне ойындар үшін айтарлықтай зор әлеует бергенімен, ақпараттық тұтастыққа бұрын-соңды болмаған қауіп-қатер төндіруде (Verdoliva, 2020). Дүниежүзілік экономикалық форумның жаһандық тәуекелдер жөніндегі сараптамаларында жасанды интеллект тудырған дезинформация мен мисинформация ең басты стратегиялық қауіптердің қатарына енгізілген. Желіде еркін қолжетімді, ашық бастапқы коды бар бағдарламалық пакеттер бағдарламалау немесе бейнемонтаж дағдылары жоқ кез келген адамға манипуляцияланған медиа активтерін жасауға мүмкіндік береді.

Синтетикалық контенттің зиянды әлеуеті қазіргі таңда бірқатар стратегиялық бағытта көрініс тауып отыр. Мысалы, саяси аренада ол сайлау науқандары кезінде қоғамдық пікірді манипуляциялауға, электоратты адастыруға және саяси қайраткерлерді дискредитациялауға бағытталған ақпараттық операциялар үшін қолданылады. Немесе айталық, қаржы және корпоративтік секторда да дипфейктер ауқымды экономикалық алаяқтықтың негізгі құралына айналып отыр. Атап айтқанда, киберқылмыскерлер банктер мен қаржы институттарының клиенттерін қашықтан биометриялық сәйкестендіруіне арналған KYC (Know Your Customer – «клиентті тану») хаттамаларын бұзып өту үшін нақты уақыт режиміндегі синтетикалық бейнелер мен дауыстарды сәтті қолдануда. Сонымен қатар, бұл генеративтік технологиялар жеке тұлғаларды бопсалау, қорқыту және психологиялық манипуляцияға құрылған күрделі әлеуметтік инжиниринг схемаларында да кеңінен пайдаланылуда.

Осы қиындықтарға төтеп беру үшін бүгінгі таңда халықаралық ортада синтетикалық медиа форензикасы (Synthetic Media Forensics) деген атаумен танымал болып келе жатқан жаңа ғылыми бағыт қалыптасуда. Қолмен өңделген пиксельдердің ізіне түсумен немесе файлдардың метадеректерін тексерумен шектелетін дәстүрлі цифрлық криминалистикадан айырмашылығы, заманауи форензика терең оқыту алгоритмдерінің контентті синтездеу барысында қалдыратын математикалық, статистикалық және биофизикалық артефактілерін анықтауға негізделген. Бұл сала қазіргі уақытта үздіксіз технологиялық тежеріс сипатына ие болып отыр. Осы генеративтік модельдердің әрбір жаңа буыны бұрынғы анықтау алгоритмдерін айналып өтуді үйренген сайын, форензика ғылымы да спектральды талдау, физиологиялық биометрия және кросс-модальды (аудио-визуалды) диссонансты зерттеу сияқты жаңа, аса күрделі аналитикалық тәсілдерді ойлап табуға мәжбүр болуда.

Материалдар мен әдістер

Зерттеу барысында синтетикалық медиа форензикасының негізгі бағыттарын анықтау үшін кеңістіктік, жиілік, биофизикалық және фонетикалық ауытқуларды кешенді талдау әдістері қолданылды. Зерттеу дизайны технологиялық аудит, лингвистикалық сараптама және салыстырмалы-құқықтық талдауды біріктіретін пәнаралық тәсілге негізделген.

1. Технологиялық және алгоритмдік талдау әдістері. Алгоритмдік манипуляцияларды анықтау тәсілдерін бағалау мақсатында келесі форензикалық бағыттар сарапталды:

* Кеңістіктік талдау. Пиксель деңгейіндегі микроскопиялық ақауларды (бұлыңғырлану, қабаттасу шекаралары, тері текстурасындағы аномалиялар) анықтау үшін Xception және ResNet сияқты конволюциялық нейрондық желілердің (CNN) архитектуралары зерттелді.

* Жиілік спектрін талдау. Генеративті модельдердің апсемплинг (upsampling) процесі кезінде қалдыратын периодты жасанды шуылдарын тіркеу үшін дискретті косинустық түрлендіру (DCT) әдістері қолданылды. Бұл әдіс күшті сығымдалған бейнелерден де математикалық артефактілерді бөліп алуға мүмкіндік береді.

* Физиологиялық биометрия. Қашықтан фотоплетизмография (rPPG) технологиясы арқылы бейнежазбадағы адам бетінің терісіндегі көзбен көру мүмкін емес микро-түстік өзгерістерді өлшеу әлеуеті талданды. Бұл тәсіл жүрек соғысы сигналын оқып, генерацияланған медиадағы уақыттық және биофизикалық сәйкессіздіктерді дәл анықтайды.

2. Деректер базасы және кросс-датасеттік валидация. Халықаралық тәжірибені және анықтау жүйелерінің тиімділігін бағалау үшін синтетикалық медиа форензикасындағы ең танымал үш автоматты тестілеу эталонының (бенчмарктерінің) құрылымына салыстырмалы шолу жасалды (Кесте 1). Бұл базалар детекторлардың «кросс-датасеттік жалпылау», яғни бір базадан үйренгенін екінші базада қолдану мәселесін айқындау үшін негіз болды.

Кесте 1. Синтетикалық медиа форензикадағы негізгі халықаралық деректер базаларының (бенчмарктердің) салыстырмалы сипаттамасы

Датасет атауы	Бейне-лер саны (жуықтап)	Жасалу ортасы және специфи-кациясы	Қолданылған манипу-ляция әдістері

FaceForensics++	5 000	Зертханалық жағдай, жоғары сапалы, біркелкі камера ракурсы мен жарық.	FaceSwap, Deepfakes, Face2Face, NeuralTextures
Celeb-DF	5 600+	Нақты әлемге жақындатылған (in-the-wild), танымал адамдардың бейнелері.	Жетілдірілген дипфейк генерациясы (жақсартылған бет маскалары мен түстер).
DFDC (Deepfake Detection Challenge)	100 000+	Ауқымды, аса күрделі жағдайлар, әртүрлі жарық, кедергілер мен камера бұрыштары.	8-ден астам түрлі генеративті алгоритмдер мен өңдеу әдістері.

3. Лингвомәдени және құқықтық сараптама. Қазақстандық контексті зерделеу барысында ұлттық ақпарат аренасының лингвомәдени ерекшеліктері, атап айтқанда қазақ тілінің фонетикалық заңдылықтары мен екітілді ортаның спецификасы талданды. Қазақ тіліне тән спецификалық фонемалардың мысалы, қатаң және ұяң дауыссыздардың аудиовизуалды артикуляциясы мен виземалар (ерін қимылы) арасындағы сәйкессіздіктерді анықтау тетіктері қарастырылды.

Сонымен қатар, нормативтік базаны зерттеу мақсатында салыстырмалы-құқықтық және құрылымдық-функционалдық талдау әдістері қолданылды. Қаржылық алаяқтық пен киберқылмыстың нақты эмпирикалық мысалдары негізінде Қазақстан Республикасының Қылмыстық кодексінің, «Масс-медиа туралы» заңының, сондай-ақ жаңадан қабылданған «Жасанды интеллект туралы» заңының нормаларына құқықтық баға беріліп, ұлттық заңнамадағы олқылықтар анықталды.

Нәтижелер

Алгоритмдік манипуляцияларды анықтауға арналған заманауи тәсілдерді талдау синтетикалық медиа форензикасы қиылысатын бірнеше вектор арқылы дамып келе жатқанын көрсетеді. Зерттеушілер мен криминалистер жалған контентті әшкерелеу үшін кеңістіктік, жиілік, биофизикалық және фонетикалық ауытқуларды кешенді түрде пайдаланады.

Кеңістіктік және жиілік аналитикасы жайлы айтар болсақ, форензиканың тарихи тұрғыда алғашқы әрі ең танымал құралдарына суреттерді пиксель деңгейінде талдайтын конволюциялық нейрондық желілерге (CNN) негізделген тәсілдер жататыны белгілі (Verdoliva, 2020). Әсіресе FaceSwap немесе Face2Face сияқты әдістерді дипфейк жасау процесіндеқолданғанкездекадрдыңкеңістіктіктұтастығыбұзыладыдептұжырымдайды Рөслер және басқа да зерттеушілер (Rössler et al., 2019). Олар бұл бағытта XceptionNet архитектурасына негізделген жүйелер ең жоғары нәтиже көрсететінін дәлелдей алды. Озық форензикалық конвейерлерде бүкіл кадр емес, заманауи бет трекері қолданылады. Жүйе бет аймағын қамтып, қабаттасу шекарасын ұстау үшін консервативті кадрлаумен (аймақты 1,3 есе ұлғайтып) жіктеу үшін нормаланған фрагментті XceptionNet желісіне береді. Зерттеулер мұндай автоматтандырылған жүйелердің адам қабылдауының мүмкіндіктерінен едәуір асып түсетінін көрсетеді. Яғни, бейнематериалдың сапасы (қысылуы) төмендеген кезде адамдардың дипфейкті визуалды анықтау қабілеті 58,73%-ға дейін құлайды, ал CNN детекторлары жоғары дәлдікті сақтайды.

Алайда, Раза және т.б. пікірінше, кеңістіктік әдістерде «жалпылау алшақтығы» тәрізді айтарлықтай осалдық бар. Конволюциялық желілер жаттығу кезінде қолданылған деректер жинағының (датасеттің) ерекше артефактілерін жаттап алуға бейім. Эмпирикалық деректер бойынша, модельдерді бұрын-соңды белгісіз деректер жинақтарында тестілеген кезде CNN архитектураларының өнімділігі орта есеппен 15%-дан астамға, ал трансформер архитектураларында 11,33%-ға төмендейді (Raza et al., 2026). Бұл заманауи анықтау жүйелері жасандылықтың іргелі семантикалық сипаттарын емес, нақты деректер жинағының спецификалық сығымдалу артефактілерін ғана үйренетінін растайды.

Пиксельдік талдаудың осы шектеулерін жеңу үшін криминалистер сигналдарды өңдеу теориясы мен жиілік спектрін талдауға жүгіне бастады. Зерттеулер генеративті-жауласушы желілермен (GAN) жасалған суреттер адам көзіне мүлде кемшіліксіз болып көрінсе де, жиілік саласында анық жасанды із қалдыратынын растайды (Giudice, Guarnera and Battiato, 2021). Жоғары ажыратымдылықты кескін жасау үшін нейрондық желілер апсемплинг операцияларын пайдаланады, бұл синтезделетін медиаға табиғи фотографияларда жоқ периодты жоғары жиілікті артефактілер енгізеді. Осы іздерді анықтау үшін дискретті косинустық түрлендіру (DCT) қолданылады, ол тіпті күшті бейне сығымдау кезінде де өзінің математикалық тұрақтылығын сақтай алады.

Ал биофизикалық маркерлер мен аудиовизуалды диссонансқа келер болсақ, қазіргі кезде синтетикалық медиа форензикасындағы ең инновациялық бағыттардың бірі – биологиялық және физиологиялық маркерлерді пайдалану. Оның негізінде қашықтан фотоплетизмография (Remote Photoplethysmography немесе rPPG) технологиясы жатыр (Seibold et al., 2025). Шынайы бейнежазбаларда адам ағзасындағы пульс (жүрек соғысы) сигналы субъектінің бетінде ырғақты микро-түстік өзгерістер түрінде көрінеді. Дипфейк жасау процесі бұл кеңістіктік-уақыттық үйлесімділікті бұзады. Заманауи форензикалық жүйелер уақыттық трансформерлер арқылы осы физиологиялық ауытқуларды талдап, алгоритмдік араласуды дәл анықтайды (Wu et al., 2024; Hernandez-Ortega et al., 2020).

Соңғы жылдары дауысты клондау және мәтінді сөйлету генерациясын ерінді синхрондау манипуляциясына интеграциялау үрдісі жиі байқалуда. Форензикада бұған қарсы фонемалар (дыбыстар) мен виземалар (олардың визуалды артикуляциясы) арасындағы сәйкессіздікті анықтау әдістері қолданылады. Генеративтік модельдер ауыз-бет артикуляцияның қатаң биомеханикалық шектеулерін толық сақтамайтындықтан, кадрлар арасында «уақыттық ерін дірілі» пайда болады (Liu et al., 2024). Сонымен қатар, синтезделген сөйлеуде шынайы адам дауысымен салыстырғанда үзілістер (паузалар) арасындағы уақыт артады. Бұл акустикалық сипаттамалар үзіліс ұзақтығы мен жиілігі арқылы әшкереленеді (Kulangareth et al., 2024). Бұған қоса, синтезделген аудиоконтентті спектрограммалық талдау барысында мел-жиіліктік кепстральды коэффициенттерді (MFCC) алу ерекше форензикалық маңызға ие. Адамның дауыс шығару аппаратының табиғи биомеханикалық резонансын толық эмуляциялай алмайтын мәтінді сөйлету (TTS) модельдері акустикалық деңгейде елеусіз математикалық аномалиялар қалдырады. Кепстральды талдау дыбыс толқынының іргелі жиіліктік сипаттамаларын бөліп алу арқылы осы жасанды микро-резонанстарды дәл анықтап береді.

Келесі халықаралық датасеттер және кросс-датасеттік валидация тәсіліне келер болсақ, бұндай анықтау алгоритмдерін оқытып-үйрету үшін орасан зор датасеттер (деректер базалары) талап етіледі. Мәселен, 2019 жылы жасалған FaceForensics++

эталоны синтетикалық медиа форензиканы стандарттауда маңызды қадам болды. Алайда Celeb-DF және DFDC сияқты әлемдік нақты деректер базаларын енгізу кросс-датасеттік жалпылау мәселесінің бар екенін көрсетіп берді. Бұл әмбебап анықтау алгоритмінің әлі күнге дейін жасалмағанын көрсетеді (Singh and Dhumane, 2025). Яғни, бүгінгі күні белгілі бір деректер базасында оқытылған нейрожелілер басқа жағдайда жасалған жаңа дипфейктерді жоғары дәлдікпен тани алмайды. Бұл олардың жалған контенттің іргелі табиғатын түсінбей, тек нақты бір датасетке ғана тән спецификалық артефактілерді механикалық түрде жаттап алуға бейім екенін білдіреді.

Ал отандық контекстке келер болсақ, ұлттық ақпарат аренасының өзіндік лингвомәдени және криминогендік ерекшеліктері жоқ емес. Мәселен, Қазақстанда мемлекет пен корпорациялар басшыларының, соның ішінде ҚР Президенті мен ірі банктердің топ-менеджерлерінің бейнелерін пайдаланған қаржылық шабуылдар айтарлықтай жиілеп кеткен (Қазақстан Ұлттық Банкі, 2025). Халықаралық тәжірибе көрсеткендей, мұндай дипфейктер жай ғана жалған ақпарат емес, қаржы институттарының клиентті қашықтан тануға арналған KYC хаттамаларын айналып өтуге арналған жоғары технологиялық әлеуметтік инжиниринг құралына айналып отыр (Incode, 2024). Адамды анықтау жүйелерін бұзу үшін киберқылмыскерлер нақты уақыт режимінде синтезделген бейнелерді сәтті қолдануда.

Қаржылық алаяқтық векторларын талдайтын болсақ, қаскүнемдердің банктердегі қашықтан биометриялық сәйкестендіру кезеңін бұзып өтуінің екі негізгі технологиялық сценарийі кездеседі. Біріншісі презентациялық шабуыл, яғни экранға шығарылған дипфейк бейнесін камераға тікелей көрсету. Екіншісі әрі анағұрлым қауіптісі инъекциялық шабуыл. Бұл жағдайда синтетикалық деректер ағыны виртуалды драйвер арқылы верификация жүйесіне тікелей енгізіліп, құрылғының физикалық сенсорын (камерасын) айналып өтеді. Қазіргі таңдағы «тірі адамды анықтау» (Liveness detection) жүйелерінің басым көпшілігі тек келіп түскен контенттің визуалды шынайылығын тексерумен шектеледі, ал инъекциялық шабуылдар контенттің қайнар көзін бұрмалайтындықтан, бұл екі бөлек технологиялық мәселе болып отыр (Ayosso, 2026).

Бұл қауіптің ауқымы халықаралық киберқауіпсіздік есептерінде нақты сандық көрсеткіштермен расталып отыр. Group-IB компаниясының «Weaponized AI» баяндамасына сәйкес, компанияның Fraud Protection тобы бір ғана қаржы институтына 2025 жылдың қаңтар-тамыз аралығында цифрлық KYC процесінде 8065 дипфейк алаяқтық әрекетін әшкерелеуге көмегін тигізген. Осы 8065 әрекет кезінде 5702 алаяқтық шот пен 88 нақты құрылғы анықталған. Құрылғылардың 83-і Android, ал 5-і iOS негізінде болған. (Group-IB, 2026). Өз кезегінде, iProov компаниясының деректеріне сүйенген талдау виртуалды камера арқылы жасалған шабуылдардың 2024 жылы 2665%-ға, ал бет ауыстыру (face-swap) инъекцияларының 2023 жылдың екінші жартысында алдыңғы кезеңмен салыстырғанда 704%-ға өскенін көрсетеді (Rajagopal, 2026). Шынайы өмірде де мұндай олқылықтардың ауыр зардаптары кездесіп отырады. Мысалы, Нидерланд полициясының ресми хабарламасына сәйкес, 2025 жылғы қарашада 34 жастағы амстердамдық ер адам жалған пәтер жалдау хабарландырулары арқылы құрбандардың жеке құжаттарын алып, AI негізіндегі бет манипуляциясы (дипфейк) арқылы банктің цифрлық сәйкестендіру процесін айналып өтіп, кемінде 46 банктік шот ашып, алаяқтық мақсатқа пайдаланған (Politie, 2025). Ескерту: осы мақала жазылған күні үкім әлі шыққан жоқ. Іс 2026 жылғы наурыз айында сот тарапынан толық тергелмеген деп танылып, қосымша тергеуге жіберілген.

Сондай-ақ, мемлекетаралық алауыздық тудыруға бағытталған сыртқы саяси провокациялар мен ақпараттық-психологиялық операциялар да көрініс табуда. Мысалы, 2025 жылы қыркүйек айында Ресей Федерациясы Сыртқы істер министрлігінің ресми өкілі Мария Захарованың бейнесі қолданылған дипфейк интернет желісінде пайда болған еді. Онда киберқылмыскерлер шынайы бейнекадрлардың артикуляциясын өзгертіп, синтезделген дауыс арқылы ҚР Президентінің БҰҰ Бас Ассамблеясындағы кездесулері туралы жалған пікір таратқаны айтылады (Министерство иностранных дел России, 2024). Тағы бір мысал ретінде Қазақстанның сол кездегі Сыртқы істер министрі Мұрат Нұртілеу мен бірқатар облыс әкімдерінің бейнелері пайдаланылып, олардың атынан шетелдік әскери науқандарды қолдайтын жалған мәлімдемелер генерацияланғанын да айтуға болады (Orda.kz, 2024). Бұл мысалдар дипфейк технологиясының жай ғана қаржылық алаяқтық емес, ұлттық қауіпсіздікке қатер төндіретін стратегиялық қаруға айналғанын көрсетеді.

Бір айта кетерлігі, отандық медиа форензиканың дамуына кедергі болатын ең маңызды ғылыми тосқауылдардың бірі – тілдік фактор және фонетикалық ерекшеліктер болып отыр. Халықаралық зерттеулердегі тәжірибелер аз ресурсты тілдерде тек ағылшын тіліне негізделген трансформерлердің тиімсіз болатыны дәлелденген еді (Owais et al., 2026). Қазақ тілінің лингвистикалық архитектурасы мен фонетикалық заңдылықтары отандық медиа аудит үшін бірегей кедергілер қалыптастыруда.

Біріншіден, қазақ тіліндегі спецификалық увуляр (қ, ғ), веляр (ң) дауыссыздары мен еріндік (ө, ү, ұ) дауысты дыбыстарының транскрипциясы мен дыбысталуы ерекше биомеханикалық ротофасиалды қимылдарды талап етеді. Ағылшын тілінің датасеттерінде оқытылған ЖИ генераторлары осы күрделі артикуляциялық ауыс-түйістерді модельдеу кезінде кадрлар арасындағы «уақыттық ерін дірілі» эффектісін жасанды түрде тудырады. Екіншіден, қазақ тілі агглютинативті сипатқа ие және сингармонизм заңдылығына бағынады. Синтезделген сөйлеуде бұл үндестік заңдылықтары жиі бұзылып, интонациялық контурлар мен микро-паузалардың табиғи емес сәйкессіздігіне (акустикалық диссонансқа) алып келеді. Осы фундаменталды заңдылықтарды ескерсек, қазақ тілінің өзіндік фонетикалық ерекшеліктеріне бейімделген жергілікті датасеттердің болмауы салдарынан, шетелдік автоматтандырылған жасанды интеллект детекторлары қазақтілді дипфейктерді талдауда технологиялық дәрменсіздік танытуы әбден ықтимал.

Талқылау

Синтетикалық медианың қарқынды таралуы дәстүрлі құқықтық жүйелердің дайын еместігін айғақтады. Дегенмен, кейінгі жылдары бұл олқылықтың орнын толтыруға бағытталған әрекеттер де байқалуда. Қазақстан Республикасының Қылмыстық кодексінің қазіргі редакциясында жасанды интеллект немесе дипфейк терминдері тікелей аталмайды. Алаяқтық және жалған ақпарат тарату баптары бойынша құқық бұзушылықтар сараланғанымен, генеративті жасанды интеллектті қолдануды арнайы ауырлататын мән-жай ретінде қарастыру тетіктері әлі де жетілдіруді қажет етеді. Негізгі дәлелдемелік база мәселесі ретінде елде валидті форензикалық сараптама жүргізіп, сотқа синтетикалық медиаға қатысты бұлтартпас техникалық дәлелдер ұсына алатын тәуелсіз алгоритмдік медиа-аудит институтының әлі қалыптаспағанын айтуға болады.

Қалай дегенмен де, бүгінгі күні осы бағытта мемлекет тарапынан маңызды институционалдық шешімдер қабылдануда. Соның бір айғағы ретінде «Масс-медиа

туралы» Заңның (2024 жылғы 19 маусымдағы № 93-VIII) 14-бабына 2025 жылғы 17 қарашадағы № 231-VIII Заңмен енгізілген және 2026 жылы күшіне енген түзетулер шеңберінде жасанды интеллект құралдарын қолдану арқылы жасалған медиа өнімдерді міндетті түрде таңбалау қажеттігін атап өткен жөн (Қазақстан Республикасының Заңы, 2024). Сондай-ақ, «Жасанды интеллект туралы» Заңның (2025 жылғы 17 қараша, № 230-VIII) қабылдануы да Қазақстанды жасанды интеллекті заңнамалық түрде реттеген алғашқы Орталық Азия мемлекеттерінің біріне айналдырды. Дегенмен заңда дипфейк жасау немесе таратуды тікелей саралайтын қылмыстық-құқықтық норма көзделмеген – жасанды интеллект жүйелерінің келтірген зиянын өтеу жалпы азаматтық-құқықтық тәртіппен, Азаматтық кодексте айқындалған негізде жүзеге асырылады (Қазақстан Республикасының Заңы, 2025; Qazinform, 2025).

Халықаралық құқықтық тәжірибемен салыстырмалы талдау жасау ұлттық заңнаманың даму векторларын айқындауға мүмкіндік береді. Мәселен, Еуропалық Одақтың «Жасанды интеллект туралы актісі» (EU AI Act) тәуекелдерге негізделген тәсілді қолданады әрі 50-бабы аясында жүйе қолданушылары дипфейк-контенттің жасанды екенін немесе өзгертілгенін міндетті түрде ашып көрсетуі талап етіледі. Қазақстанның қазіргі бағыты азаматтық-құқықтық реттеу мен таңбалауға (ЕО моделіне жақын) сүйенгенімен, ұлттық қауіпсіздік пен қаржы жүйесіне төнетін қатерлердің артуы болашақта Қылмыстық кодекске «генеративті алгоритмдерді қолдана отырып жасалған қылмыс» деген арнайы саралаушы белгіні енгізуді қажет етеді деп пайымдайды авторлар.

Генеративтік ЖИ қауіптеріне кешенді қарсы тұру және Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету үшін бірқатар стратегиялық бастамаларды іске асыру маңызды. Бірінші кезекте, синтетикалық контенттің ұлттық датасетін жасау кезек күттірмейтін міндет. Қазақ тілінің фонетикасы мен артикуляциялық ерекшеліктерін, сондай-ақ аймақтың антропометриялық деректерін ескеретін ауқымды деректер базасы отандық зерттеу институттары үшін жергілікті нейрондық желі-детекторларын оқытудың берік іргетасы болмақ. Екіншіден, алгоритмдік медиа аудит институтын қалыптастыру жай ғана технологиялық емес, құқықтық қажеттілік. Ұсынылып отырған институттың мәртебесі сотқа ұсынылатын цифрлық дәлелдемелердің тізбегін сақтауды қамтамасыз етуі тиіс. Бұл дегеніміз, сот сараптамасы тек визуалды тексерумен шектелмей, DCT жиілік спектрін талдау, кепстральды коэффициенттерді алу және rPPG технологиясы сияқты математикалық негізделген әдістерге сүйенуі қажет. Аудит институты машиналық детекторлардың ықтималдық нәтижелерін криминалист-ғалымдардың шешімімен растайтын «адам және алгоритм» гибридті моделін енгізуі тиіс.

Үшіншіден, журналистердің біліктілігін арттыру және автоматтандырылған детекторларды интеграциялау үлкен рөл атқарады. Рөслер және басқа да зерттеушілер айтпақшы, адам көзінің дипфейкті анықтау мүмкіндігінің шектеулі екендігін ескере отырып, масс-медиа өкілдері мен фактчекерлер цифрлық форензиканың негізгі дағдыларын меңгеріп, өздерінің жұмыс процестеріне аудио және бейне қатарлары арасындағы рассинхронизацияны анықтай алатын заманауи детекторлардың жүйелерін интеграциялауы қажет.

Қорытынды

Синтетикалық медиа форензика жаһандық және ұлттық ақпараттық қауіпсіздікті

қамтамасыз етудегі маңызды қорғаныс шебіне айналуда. Жүргізілген талдау генеративті жасанды интеллект эволюциясының қарапайым визуалды иллюзия жасаудан адамның биомеханикалық және физиологиялық параметрлерін терең алгоритмдік эмуляциялауға көшкенін көрсетеді. Ғылыми қауымдастық бұған қарсы тұру үшін кеңістіктік CNN-детекторлар, DCT жиілік аналитикасы, қашықтан фотоплетизмография (rPPG) жүйелері және фонетика-визуалды диссонансты анықтау желілері сияқты форензикалық құралдардың мықты арсеналын жасап шығарды. Алайда осы әдістердің ешқайсысы кросс-датасеттік жалпылау мәселесі мен генерация алгоритмдерінің үздіксіз бейімделуіне байланысты абсолютті шешім емес.

Қазақстан Республикасының контексінде бұл жаһандық технологиялық қауіп айқын жергілікті сипат алады. Жасанды интеллект технологияларын корпоративтік және инвестициялық алаяқтық схемаларда пайдалану, жоғары мемлекеттік қайраткерлердің бейнесін пайдаланған геосаяси дезинформация әрекеттері, сондай-ақ қазақ тілінің фонетикалық ерекшелігі отандық медиа кеңістігінің синтетикалық контентке қарсы тұруда әлі де осал екенін дәлелдеді.

Отандық журналистика, ақпараттық технология секторы мен құқық қорғау жүйесі үшін шетелдік бағдарламалық шешімдерді пассивті импорттау жеткіліксіз. Тәжірибелі журналистер мен фактчекерлер үшін CNN, DCT немесе rPPG сияқты күрделі технологиялардың практикалық мәні де айқын. Олар жалаң көзбен байқалмайтын пиксельдік бұрмаланулар мен биофизикалық сәйкессіздіктерді дәл табатын, редакциялық верификация хаттамаларына міндетті түрде кіріктірілуі тиіс күнделікті жұмыс құралына айналуы қажет.

Сонымен қатар, стратегиялық басымдылыққа ие болу үшін қазақ морфологиясы мен артикуляциясын ескере отырып ұлттық датасеттер жинап, сот инстанцияларына валидті дәлелдер ұсына алатын тәуелсіз техникалық медиа аудит институтын қалыптастыру және құқықтық базаны одан әрі жетілдіру қажет. Жасанды интеллект арқылы жасалған контентті міндетті түрде таңбалау талаптарымен қоса, жаңа «Масс-медиа туралы» және «Жасанды интеллект туралы» заңдардың қабылдануы заңнаманың мызғымас нормативтік іргетасын қалайды. Цифрлық форензика саласындағы іргелі және қолданбалы зерттеулерді одан әрі дамыту Қазақстан Республикасының ақпараттық тұтастығын қорғауды ғана емес, тұтас Орталық Азия аймағы үшін цифрлық қауіпсіздіктің озық стандарттарын қалыптастыруды да қамтамасыз етеді.

Авторлардың қосқан үлесі:

Кошкенов Н.Ж. – бақылау және ұсыныс беру, мақсат-міндетті анықтау, негізгі бөлімді жазу, жалпы ғылыми аппаратты басқару.

Салиев И.У. – әдебиетпен жұмыс, негізгі бөлімді жазу, материалдарды жинау.

Тогтарбай Б. – хат-хабар авторы, деректерді сұрыптау, редакциялау, мақаланың журнал талаптарына техникалық дәлдігін қадағалау.

Әдебиеттер тізімі

Ayosso, S. (2026) How deepfakes bypass liveness checks in real identity verification systems. DuckDuckGoose AI. Available at: https://www.duckduckgoose.ai/blog/how-deepfakes-bypass-liveness-checks-in-real-identity-verification-systems (Accessed: 8 September 2026).

Giudice, O., Guarnera, L. and Battiato, S. (2021) «Fighting Deepfakes by Detecting GAN DCT Anomalies», Journal of Imaging, 7(8), b. 128.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y. (2014) «Generative Adversarial Nets», Advances in Neural Information Processing Systems, 27, b. 2672–2680.

Group-IB (2026) Weaponized AI: Inside the Criminal Ecosystem Fueling the Fifth Wave of Cybercrime. Available at: https://www.group-ib.com/resources/research-hub/weaponized-ai/ (Accessed: 8 September 2026).

Hernandez-Ortega, J., Tolosana, R., Fierrez, J. and Morales, A. (2020) «DeepFakesON-Phys: DeepFakes Detection based on Heart Rate Estimation», arXiv:2010.00400.

Incode (2024) «Top 5 Cases of AI Deepfake Fraud From 2024 Exposed».

Kulangareth, N., Kaufman, J., Oreskovic, J. and Fossat, Y. (2024) «Investigation of Deepfake Voice Detection Using Speech Pause Patterns: Algorithm Development and Validation», JMIR Biomedical Engineering, 9, e56245.

Liu, W., She, T., Liu, J., Li, B., Yao, D., Liang, Z. and Wang, R. (2024) «Lips Are Lying: Spotting the Temporal Inconsistency between Audio and Visual in Lip-Syncing DeepFakes», Advances in Neural Information Processing Systems (NeurIPS), 37.

Министерство иностранных дел России (2024) «Об очередном целенаправленном вбросе дипфейка». [Онлайн]. Қолжетімді: https://mid.ru/2048364/?lang=en (Қаралған күні: 24 маусым 2026).

Orda.kz (2024) «Kazakhstan: Public Figures Targeted in Deepfake Videos Promoting Russian Military Campaign». [Онлайн]. Қолжетімді: https://en.orda.kz/kazakhstan-public-figures-targeted-in-deepfake-videos-promoting-russian-military-campaign-7079/ (Қаралған күні: 24 маусым 2026).

Қазақстан Республикасының Заңы (2024) «Масс-медиа туралы» Заңы, 2024 жылғы 19 маусымдағы № 93-VIII (2025 жылғы 17 қарашадағы № 231-VIII Заңымен енгізілген 14-бап, 7-тармаққа өзгеріспен).

Қазақстан Республикасының Заңы (2025) «Жасанды интеллект туралы» Заңы, 2025 жылғы 17 қарашадағы № 230-VIII.

Қазақстан Ұлттық Банкі (2025) «Ұлттық Банк жасанды интеллектті пайдалану арқылы жасалатын жаңа алаяқтық схемалар туралы ескертеді». [Электронды ресурс]. Қолжетімді: https://nationalbank.kz/kz/news/informacionnye-soobshcheniya/17903 (Қаралған күні: 24 маусым 2026).

Owais, M. et al. (2026) «Deepfake audio detection in low-resource languages: A case study of Urdu», IEEE Access.

Politie (2025) Oplichter aangehouden die met behulp van deepfake tientallen bankrekeningen opende en misbruikte. Available at: https://www.politie.nl/nieuws/2025/december/17/05-oplichter-aangehouden-die-met-behulp-van-deepfake-tientallen-bankrekeningen-opende-en-misbruikte.html (Accessed: 8 September 2026).

Qazinform (2025) «Kazakhstan to introduce regulations to tackle deepfakes».

Rajagopal, S.K. (2026) How deepfake injection attacks bypass liveness detection. Signzy. Available at: https://www.signzy.com/blogs/liveness-detection-bypass-deepfake-injection (Accessed: 8 September 2026).

Raza, A., Basit, A., Amin, A., Arfeen, Z.A., Masud, M.I., Fayyaz, U. and Jumani, T.A. (2026) «A Comprehensive Review of Deepfake Detection Techniques: From Traditional Machine Learning

to Advanced Deep Learning Architectures», AI, 7(2), 68. DOI: 10.3390/ai7020068.

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J. and Nießner, M. (2019) «FaceForensics++: Learning to Detect Manipulated Facial Images», Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), b. 1–11.

Seibold, C., Wisotzky, E.L., Beckmann, A., Kossack, B., Hilsmann, A. and Eisert, P. (2025) «High-quality deepfakes have a heart!», Frontiers in Imaging, 4, 1504551.

Singh, S. and Dhumane, A. (2025) «Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges», MethodsX, 15, 103632.

Verdoliva, L. (2020) «Media Forensics and DeepFakes: An Overview», IEEE Journal of Selected Topics in Signal Processing, 14(5), b. 910–932.

Wu, J., Zhu, Y., Jiang, X., Liu, Y. and Lin, J. (2024) «Local attention and long-distance interaction of rPPG for deepfake detection», The Visual Computer, 40, b. 1083–1094.

N.Zh. Koshkenov[1] I.U. Saliyev[2] B. Togtarbay*[3]

[1,2,3]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Synthetic Media Forensics and Directions for Development (The Case of Kazakhstan)

Abstract. This article reviews the new information challenges arising from the rapid development of generative artificial intelligence (AI) technologies and the modern forensic methods used to detect them. The current evolution of machine learning algorithms has begun to reduce the distinction between authentic content and synthetic media to a level imperceptible to the human eye. Specifically, the article analyzes the malicious potential of deepfakes in financial fraud schemes—such as bypassing banks' KYC (Know Your Customer) protocols—and in political manipulations. The research also examines the experience of applying international benchmarks like FaceForensics++, exploring advanced verification approaches ranging from spatial analysis using convolutional neural networks (CNNs) and frequency analytics based on the discrete cosine transform (DCT), to physiological biometrics (rPPG) and innovative methods for evaluating audiovisual phonetic discrepancies. The paper investigates the proliferation of synthetic media in Kazakhstan's information space, phonetic artifacts emerging in a bilingual Kazakh-Russian environment (temporal lip jitter in the articulation of uvular and velar consonants), and legal gaps in the new Law "On Artificial Intelligence". In conclusion, the study substantiates the strategic necessity of transitioning away from the passive importation of foreign detectors toward creating localized national datasets, establishing an independent institute for algorithmic media audit, and integrating modern forensic tools into the fact-checking process.

Keywords: synthetic media forensics, deepfake, artificial intelligence, information security, rPPG, CNN, Kazakhstan.

References

Ayosso, S. (2026) How deepfakes bypass liveness checks in real identity verification systems. DuckDuckGoose AI. Available at: https://www.duckduckgoose.ai/blog/how-deepfakes-bypass-liveness-checks-in-real-identity-verification-systems (Accessed: 8 September 2026).

Giudice, O., Guarnera, L. and Battiato, S. (2021) «Fighting Deepfakes by Detecting GAN DCT Anomalies», Journal of Imaging, 7(8), p. 128.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y. (2014) «Generative Adversarial Nets», Advances in Neural Information Processing Systems, 27, pp. 2672–2680.

Group-IB (2026) Weaponized AI: Inside the Criminal Ecosystem Fueling the Fifth Wave of Cybercrime. Available at: https://www.group-ib.com/resources/research-hub/weaponized-ai/ (Accessed: 8 September 2026).

Hernandez-Ortega, J., Tolosana, R., Fierrez, J. and Morales, A. (2020) «DeepFakesON-Phys: DeepFakes Detection based on Heart Rate Estimation», arXiv:2010.00400.

Incode (2024) «Top 5 Cases of AI Deepfake Fraud From 2024 Exposed».

Kulangareth, N., Kaufman, J., Oreskovic, J. and Fossat, Y. (2024) «Investigation of Deepfake Voice Detection Using Speech Pause Patterns: Algorithm Development and Validation», JMIR Biomedical Engineering, 9, e56245.

Liu, W., She, T., Liu, J., Li, B., Yao, D., Liang, Z. and Wang, R. (2024) «Lips Are Lying: Spotting the Temporal Inconsistency between Audio and Visual in Lip-Syncing DeepFakes», Advances in Neural Information Processing Systems (NeurIPS), 37.

Ministerstvo inostrannykh del Rossii (2024) «Ob ocherednom tselenapravlennom vbrose dipfeika» [On another targeted deepfake release]. [online] Available at: https://mid.ru/2048364/?lang=en (Accessed: 24 June 2026). [in Russian]

Orda.kz (2024) «Kazakhstan: Public Figures Targeted in Deepfake Videos Promoting Russian Military Campaign». [online] Available at: https://en.orda.kz/kazakhstan-public-figures-targeted-in-deepfake-videos-promoting-russian-military-campaign-7079/ (Accessed: 24 June 2026).

Owais, M. et al. (2026) «Deepfake audio detection in low-resource languages: A case study of Urdu», IEEE Access.

Politie (2025) Oplichter aangehouden die met behulp van deepfake tientallen bankrekeningen opende en misbruikte. Available at: https://www.politie.nl/nieuws/2025/december/17/05-oplichter-aangehouden-die-met-behulp-van-deepfake-tientallen-bankrekeningen-opende-en-misbruikte.html (Accessed: 8 September 2026).

Qazaqstan Respublikasynyng Zany (2024) «Mass-media turaly» Zany, 2024 zhylghy 19 mausymdaghy № 93-VIII (2025 zhylghy 17 qarashadaghy № 231-VIII Zanymen engizilgen 14-bap, 7-tarmaqqa ozgerispen) [On Mass Media: Law of the Republic of Kazakhstan No. 93-VIII of 19 June 2024, as amended by Law No. 231-VIII of 17 November 2025]. [in Kazakh]

Qazaqstan Respublikasynyng Zany (2025) «Zhasandy intellekt turaly» Zany, 2025 zhylghy 17 qarashadaghy № 230-VIII [On Artificial Intelligence: Law of the Republic of Kazakhstan No. 230-VIII of 17 November 2025]. [in Kazakh]

Qazaqstan Ulttyq Banki (2025) «Ulttyq Bank zhasandy intellektti paidalanu arqyly zhasalatyn zhana alayaqtyq skhemalar turaly eskertedi» [The National Bank warns about new fraud schemes created using artificial intelligence]. [online] Available at: https://nationalbank.kz/kz/news/informacionnye-soobshcheniya/17903 (Accessed: 24 June 2026). [in Kazakh]

Qazinform (2025) «Kazakhstan to introduce regulations to tackle deepfakes».

Rajagopal, S.K. (2026) How deepfake injection attacks bypass liveness detection. Signzy. Available at: https://www.signzy.com/blogs/liveness-detection-bypass-deepfake-injection (Accessed: 8 September 2026).

Raza, A., Basit, A., Amin, A., Arfeen, Z.A., Masud, M.I., Fayyaz, U. and Jumani, T.A. (2026) «A Comprehensive Review of Deepfake Detection Techniques: From Traditional Machine Learning to Advanced Deep Learning Architectures», AI, 7(2), 68. DOI: 10.3390/ai7020068.

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J. and Nießner, M. (2019) «FaceForensics++: Learning to Detect Manipulated Facial Images», Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), pp. 1–11.

Seibold, C., Wisotzky, E.L., Beckmann, A., Kossack, B., Hilsmann, A. and Eisert, P. (2025) «High-quality deepfakes have a heart!», Frontiers in Imaging, 4, 1504551.

Singh, S. and Dhumane, A. (2025) «Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges», MethodsX, 15, 103632.

Verdoliva, L. (2020) «Media Forensics and DeepFakes: An Overview», IEEE Journal of Selected Topics in Signal Processing, 14(5), pp. 910–932.

Wu, J., Zhu, Y., Jiang, X., Liu, Y. and Lin, J. (2024) «Local attention and long-distance interaction of rPPG for deepfake detection», The Visual Computer, 40, pp. 1083–1094.

Н. Ж. Кошкенов[1] И. У. Салиев[2] Б. Тогтарбай*[3]

[1,2,3]Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан

Форензика синтетических медиа и направления её развития (на примере Казахстана)

Аннотация. В данной статье представлен обзор новых информационных вызовов, возникших вследствие стремительного развития технологий генеративного искусственного интеллекта (ИИ), а также современных форензических методов их обнаружения. Текущая эволюция алгоритмов машинного обучения начала стирать грань между подлинным контентом и синтетическими медиа до уровня, незаметного для человеческого глаза. В частности, в статье анализируется вредоносный потенциал дипфейков в схемах финансового мошенничества, направленных на обход банковских протоколов KYC (Know Your Customer), и в политических манипуляциях. В исследовании также анализируется опыт применения международных эталонов тестирования, таких как FaceForensics++, и рассматриваются передовые подходы к верификации — от пространственного анализа с использованием сверточных нейронных сетей (CNN) и частотной аналитики на базе дискретного косинусного преобразования (DCT) до физиологической биометрии (rPPG) и инновационных методов оценки аудиовизуального фонетического несоответствия. В статье исследуются распространение синтетических медиа в информационном пространстве Казахстана, фонетические артефакты, возникающие в билингвальной казахско-русской среде (временное дрожание губ при артикуляции увулярных и велярных согласных), а также правовые пробелы в новом законе «Об искусственном интеллекте». В заключение обосновывается стратегическая необходимость отказа от пассивного импорта зарубежных детекторов в пользу создания локализованных национальных наборов данных (датасетов), формирования независимого института алгоритмического медиааудита и интеграции современных инструментов форензики в процесс фактчекинга.

Ключевые слова: форензика синтетических медиа, дипфейк, искусственный интеллект, информационная безопасность, rPPG, CNN, Казахстан.

Авторлар туралы мәлімет:

Кошкенов Н.Ж. – философия докторы (PhD), аға оқытушы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қажымұқан көшесі, 13, 010008, Астана, Қазақстан.

Салиев И.У. – докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қажымұқан көшесі, 13, 010008, Астана, Қазақстан.

Тогтарбай Б. – хат-хабар авторы, философия докторы (PhD), аға оқытушы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қажымұқан көшесі, 13, 010008, Астана, Қазақстан.

Information about the authors:

Koshkenov N. – Doctor of Philosophy (PhD), Senior Lecturer, L.N. Gumilyov Eurasian National University, 13 Kazhymukan St., 010008, Astana, Kazakhstan.

Saliyev I. – Doctoral student, L.N. Gumilyov Eurasian National University, 13 Kazhymukan St., 010008, Astana, Kazakhstan.

Togtarbay B. – corresponding author, Doctor of Philosophy (PhD), L.N. Gumilyov Eurasian National University, 13 Kazhymukan St., 010008, Astana, Kazakhstan.

Сведения об авторах:

Кошкенов Н.Ж. – PhD, старший преподаватель, Евразийский национальный университет имени Л.Н. Гумилева, ул. Кажымукана, 13, 010008, Астана, Казахстан.

Салиев И.У. – докторант, Евразийский национальный университет имени Л.Н. Гумилева, ул. Кажымукана, 13, 010008, Астана, Казахстан.

Тогтарбай Б. – автор для корреспонденции, PhD, старший преподаватель, Евразийский национальный университет имени Л.Н. Гумилева, ул. Кажымукана, 13, 010008, Астана, Казахстан.