ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME -10

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 10

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

AXBOROT TIZIMLARIDA MA'LUMOTLAR MAXFIYLIGINI TA'MINLASHDA FEDERATIV O'QITISH (FEDERATED LEARNING) YONDASHUVINING SAMARADORLIGI NAZARIY TAHLIL VA QIYOSIY BAHOLASH

G'ofurova Muxlisa G'ulom qizi
Toshkent ijtimoiy innovatsiya universiteti Iqtisodiyot va pedagogika fakulteti
Axborot tizimlari va texnologiyalari yo'nalishi 2-bosqich talabasi
E-mail: muxlisagofurova@gmail.com
Tel: +998-90-358-21-04

Annotatsiya. Zamonaviy axborot tizimlarida ma'lumotlar hajmining jadal o'sishi bilan birga shaxsiy ma'lumotlarni himoya qilish muammosi tobora dolzarb tus olmoqda. Markazlashtirilgan mashinaviy o'qitish modellari xom ma'lumotlarni yagona serverga to'plashni talab qilib, GDPR kabi xalqaro me'yoriy talablar bilan ziddiyat keltirib chiqaradi. Federativ o'qitish (Federated Learning, FL) — ma'lumotlarni mahalliy qurilmalarda saqlab, faqat model parametrlarini almashinish orqali umumiy model shakllantiruvchi taqsimlangan o'qitish paradigmasi — ushbu muammoning zamonaviy va ilmiy asoslangan yechimi sifatida qaralmoqda. Ushbu maqolada FL ning nazariy asoslari, asosiy algoritmik mexanizmlari (FedAvg, FedProx, Differensial maxfiylik) va amaliy tatbiq natijalari tizimli adabiyotlar sharhi hamda qiyosiy tahlil metodlari yordamida IMRAD uslubida o'rganilgan. Tadqiqot natijalari shuni ko'rsatadiki, FL yondashuvi model aniqligini 92-96% darajada saqlab, GDPR talablariga to'liq muvofiqlikni ta'minlaydi. FedProx algoritmi non-IID muhitlarda FedAvg ga nisbatan 22% gacha ustunlikni namoyish etadi. Kommunikatsiya xarajatlari, non-IID muammo va xavfsizlik tahdidlari hali hal etilmagan cheklovlar bo'lib qolmoqda.

Kalit so'zlar: federativ o'qitish, ma'lumotlar maxfiyligi, axborot tizimlari, FedAvg, FedProx, differensial maxfiylik, taqsimlangan mashinaviy o'qitish, GDPR, ma'lumotlar minimalligi, kiberxavfsizlik, sun'iy intellekt.

Abstract. With the rapid growth of data volumes in modern information systems, the problem of protecting personal data is becoming increasingly critical. Centralized machine learning models require raw data to be collected on a single server, creating conflicts with international regulatory standards such as GDPR. Federated Learning (FL) — a distributed training paradigm that keeps data on local devices and shares only model parameters to build a global model — is considered a modern and scientifically grounded solution to this problem. This paper examines the theoretical foundations of FL, its core algorithmic mechanisms (FedAvg, FedProx, Differential Privacy) and practical application results through systematic literature review and comparative analysis in IMRAD

format. Results demonstrate that the FL approach maintains model accuracy at 92-96% while ensuring full GDPR compliance. FedProx shows up to 22% superiority over FedAvg in non-IID environments. Communication costs, the non-IID problem, and security threats remain unresolved limitations.

Keywords: federated learning, data privacy, information systems, FedAvg, FedProx, differential privacy, distributed machine learning, GDPR, data minimization, cybersecurity, artificial intelligence.

Аннотация. С быстрым ростом объёмов данных в современных информационных системах проблема защиты персональных данных становится всё более актуальной. Модели централизованного машинного обучения требуют сбора исходных данных на едином сервере, что вступает в противоречие с международными нормативными стандартами, такими как GDPR. Федеративное обучение (Federated Learning, FL) — парадигма распределённого обучения, при которой данные остаются на локальных устройствах, а для формирования глобальной модели передаются лишь параметры модели — рассматривается как современное и научно обоснованное решение данной проблемы. В статье в формате IMRAD изучаются теоретические основы FL, ключевые алгоритмические механизмы (FedAvg, FedProx, дифференциальная приватность) и результаты практического применения. Подход FL обеспечивает точность модели 92-96%, полностью соответствуя требованиям GDPR. FedProx демонстрирует преимущество до 22% над FedAvg в условиях non-IID.

Ключевые слова: федеративное обучение, конфиденциальность данных, информационные системы, FedAvg, FedProx, дифференциальная приватность, распределённое машинное обучение, GDPR, минимизация данных, кибербезопасность, искусственный интеллект.

KIRISH.

Raqamli transformatsiya jadal rivojlanayotgan hozirgi sharoitda axborot tizimlarida ma’lumotlar maxfiyligini ta’minlash tobora murakkablashib bormoqda. Sun’iy intellekt texnologiyalarining keng tarqalishi esa kiberxavfsizlik muammolarini yanada dolzarb qilmoqda. Bir tomondan, shaxsiy ma’lumotlarga bo‘lgan talab yil sayin oshib bormoqda — 2023-yil holatiga ko‘ra, kuniga 2,5 kvintillion bayt ma’lumot ishlab chiqilmoqda [1]. Ikkinchi tomondan, GDPR kabi qat’iy qonunchilik normalari ma’lumotlarni markaziy serverga to‘plash imkoniyatini keskin cheklamoqda.

Markazlashtirilgan mashinaviy o‘qitish (Centralized Machine Learning) paradigmasida modelni o‘qitish uchun barcha xom ma’lumotlarni yagona serverga uzatish talab etiladi. Bu esa GDPR ning 5(1)(c)-moddasidagi ma’lumotlar minimalligi printsipi bilan bevosita ziddiyat keltirib chiqaradi [2].

ISSN 3030-3907

GDPR joriy etilganidan beri, 2026-yil yanvar holatiga ko‘ra, Yevropada jami 7,1 milliard yevrodan ortiq jarima undirilgan [3]. 2023-yilda sog‘liqni saqlash sohasida 133 million dan ortiq tibbiy yozuv ma’lumotlar buzilishi natijasida oshkor bo‘ldi [4].

Federativ o‘qitish (Federated Learning, FL) — 2017-yilda McMahan va boshq. tomonidan taklif etilgan [5] — xom ma’lumotlarni uzatmasdan, faqat model parametrlarini serverga yuborish orqali umumiy model shakllantiradigan paradigmadir. Bu yondashuv «ma’lumotlar qurolchasi» (data silos) muammosini bartaraf etib, maxfiy ma’lumotlarni mahalliy qurilmalarda saqlab qolgan holda mashinaviy o‘qitishni amalga oshirish imkonini beradi [6]. O‘zbekistonda ham «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun (2019, O‘RQ-547) axborot tizimlarida shaxsiy ma’lumotlarni himoya qilishga qat’iy talablar qo‘ymoqda [7].

Mazkur maqolaning maqsadi — axborot tizimlarida ma’lumotlar maxfiyligini ta’minlashda federativ o‘qitish yondashuvining nazariy asoslarini o‘rganish, asosiy algoritmik mexanizmlarini (FedAvg, FedProx, differensial maxfiylik) qiyosiy tahlil qilish, amaliy tatbiq natijalarini baholab, ushbu texnologiyaning samaradorligi va cheklovlarini ilmiy jihatdan asoslash hamda O‘zbekiston axborot tizimlari uchun amaliy tavsiyalar ishlab chiqishdan iborat.

ADABIYOTLAR TAHLILI VA METODOLOGIYA.

FL sohasidagi ilmiy tadqiqotlar 2017-yildan beri jadal rivojlanib kelmoqda. Sun’iy intellekt va kiberxavfsizlik sohasidagi mutaxassislar FL ni ma’lumotlarni himoya qilishning eng istiqbolli usullaridan biri sifatida e’tirof etmoqda. McMahan va boshq. (2017) ning asosiy maqolasi [5] FL paradigmasini rasmiy taqdim etib, FedAvg algoritmini ishlab chiqdi — bu keyingi barcha tadqiqotlar uchun poydevor bo‘ldi. Maqola Google Scholar da 10 000 dan ortiq iqtibosga ega.

Li va boshq. (2020) [6] FL tizimlarini to‘liq ko‘rib chiqib, ma’lumotlarning geterogenligi (non-IID muammo), kommunikatsiya samaradorligi va maxfiylik himoyasi kabi asosiy cheklovlarni batafsil tahlil qildi. Xuddi shu yili Li va boshq. FedProx algoritmini taklif etib [8], non-IID muhitlarda FedAvg ga nisbatan 22% gacha aniqlik ustunligini eksperimental isbotladi.

Maxfiylik himoyasi yo‘nalishida Abadi va boshq. (2016) [9] differensial maxfiylik usulini mashinaviy o‘qitishga qo‘llashning matematik asosini ishlab chiqdi. Gosselin va boshq. (2025) [10] ACM Computing Surveys da FL ning maxfiylik hujumlari va mudofaa usullarini tizimli ko‘rib chiqdi.

Sog‘liqni saqlash sohasida Roth va boshq. (2020) [11] NVIDIA va ko‘p kasalxonalar hamkorligida mammografiya tasvirlarini tahlil qiluvchi federativ model ishlab chiqdi. Teo va boshq. (2024) [12] Cell Reports Medicine da nashr etgan tizimli sharhda 22 693 ta maqoladan 612 tasi tahlil qilindi — FL tadqiqotlarining faqat 5,2% i real tibbiy amaliyotda sinab ko‘rilganligi aniqlandi.

ISSN 3030-3907

Collins va Wang (2025) [14] ning so‘nggi review maqolasi FL ning asosiy texnik muammolarini jamlagan holda kelajakdagi tadqiqot yo‘nalishlarini belgilab berdi.

TADQIQOT METODOLOGIYASI.

Ushbu tadqiqot tizimli adabiyotlar sharhi (Systematic Literature Review, SLR) metodologiyasiga asoslanib, PRISMA ko‘rsatmalariga muvofiq amalga oshirildi [15]. Scopus, Web of Science, IEEE Xplore va ACM Digital Library bazalarida 2016-2025 yillar oralig‘ida qidiruv o‘tkazildi. Qo‘llanilgan metodlar: (1) algoritmik qiyosiy baholash — FedAvg, FedProx va DP-FL ni samaradorlik, non-IID bardoshliligi va xavfsizlik mezonlari bo‘yicha taqqoslash; (2) empirik natijalar sintezi — sog‘liqni saqlash va moliya sohasidagi haqiqiy tatbiq natijalari yig‘ma tahlili; (3) GDPR muvofiqlik tahlili. Yakuniy tahlilga 17 ta asosiy manba kiritildi.

NATIJALAR.

Federativ o‘qitish tizimi uchta asosiy komponentdan iborat: (1) Markaziy server (Global Aggregator) — mijozlardan kelgan model parametrlarini jamlab global modelni shakllantiradi; (2) Mijoz qurilmalar — mahalliy ma’lumotlarda lokal model o‘qitadi; (3) Xavfsiz kommunikatsiya protokoli — faqat model parametrlarini uzatadi [5, 6].

FL ning bir o‘qitish sikli to‘rtta bosqichdan iborat: birinchidan, server joriy global modelni tanlangan mijozlarga yuboradi; ikkinchidan, har bir mijoz mahalliy ma’lumotlarida SGD yordamida model o‘qitadi; uchinchidan, mijozlar faqat yangilangan parametrlarni serverga yuboradi; to‘rtinchidan, server barcha yangilanishlarni og‘irlikli o‘rtacha formula orqali birlashtirib yangi global model hosil qiladi [5].

FL ning uchta yetakchi algoritmi quyidagi jadvalda taqqoslanadi:

1-jadval.

FL algoritmlarining qiyosiy tahlili (adabiyotlar asosida tuzilgan)

Algoritm	Agregatsiya mexanizmi	Non-IID bardoshliligi	Model aniqligi	Asosiy afzalligi
FedAvg [5]	Og‘irlikli o‘rtacha	O‘rtacha	95-98% (IID)	Oddiy, samarali
FedProx [8]	Proksimal regularizatsiya	Yuqori	92-96% (non-IID)	Geterogen muhit
DP-FL [9]	Gauss shovqini	O‘rtacha	89-94%	Matematik kafolat
SCAFFOLD [16]	Dispersiya kamaytirish	Yuqori	93-97% (non-IID)	Tez konvergensiya

ISSN 3030-3907

FedAvg MNIST to‘plamida 99% aniqlikka atigi 18 ta kommunikatsiya turida erishdi [17]. FedProx esa non-IID muhitda FedAvg ga nisbatan 22% gacha aniqlik ustunligini ko‘rsatdi [8]. DP-FL esa matematikada belgilangan Gauss shovqinini qo‘shib, ε-δ differensial maxfiylik kafolatini beradi — shovqin darajasiga qarab model aniqligi 3-8% ga kamayishi mumkin [9].

Markazlashtirilgan ML va FL yondashuvlarining keng qiyosiy baholashi:

2-Jadval.

Markazlashtirilgan ML va FL yondashuvlarining qiyosiy baholashi

Ko‘rsatkich	Markazlashtirilgan ML	Federativ o‘qitish (FL)	Manba
Model aniqligi	95-98%	92-96%	[5, 8, 14]
Ma’lumotlar maxfiyligi	Past	Yuqori	[5, 9]
GDPR muvofiqligi	Cheklangan	To‘liq	[2, 10]
Kommunikatsiya xarajati	Past	O‘rtacha-yuqori	[6]
Non-IID bardoshliligi	Yuqori	O‘rtacha (FedProx: yuqori)	[8]
Xavfsizlik tahdidi	Markaziy (yuqori)	Taqsimlangan (past)	[10]

MUHOKAMA

GDPR muvofiqligi va amaliy tatbiq natijalari

Adabiyotlar tahlili shuni ko‘rsatdiki, FL yondashuvi GDPR talablariga markazlashtirilgan ML ga nisbatan sezilarli darajada yaxshiroq muvofiq keladi. Kiberxavfsizlik nuqtai nazaridan ham FL taqsimlangan arxitekturasi tufayli markaziy hujum nuqtasini bartaraf etadi. FL da xom ma’lumotlar hech qachon mahalliy qurilmadan tashqariga chiqmasligi GDPR ning ma’lumotlar minimalligi, maqsad cheklanishi va saqlash cheklovi printsiplarini bir vaqtda qondiradi [10].

Sog‘liqni saqlash sohasida NVIDIA va ko‘p kasalxonalar hamkorligidagi tadqiqot [11] federativ model bitta kasalxona ma’lumotlariga asoslangan modelga nisbatan yaxshiroq umumlashish qobiliyatini ko‘rsatdi. Teo va boshq. (2024) [12] ning sharhida FL tadqiqotlarining faqat 5,2% i real klinik amaliyotda sinab ko‘rilganligi katta tadqiqot salohiyatini ko‘rsatadi.

Moliya sohasida firibgarlikni aniqlash sohalarida FL modellari markazlashtirilgan modelga yaqin aniqlikda ishlashi, biroq banklararo ma’lumot almashinuvini talab qilmasligi aniqlangan. Collins va Wang (2025) [14]

ISSN 3030-3907

ma’lumotlariga ko‘ra, FL bozori 2020-yildagi 107 million dollardan 2025-yilga 538 million dollarga yetishi prognoz qilinmoqda.

Asosiy cheklovlar tahlili

Li va boshq. (2020) [6] va Collins va Wang (2025) [14] asosida FL ning to‘rtta asosiy cheklovi aniqlandi:

1. Non-IID muammo: mijozlar ma’lumotlari statistik jihatdan farqlanganda global modelning konvergensiyasi sekinlashadi. Bu muammo amaliyotdagi FL tizimlarining 70% dan ortig‘ida uchraydi [6];

2. Kommunikatsiya xarajati: har bir o‘qitish turida millionlab model parametrlarini uzatish katta tarmoq o‘tkazuvchanligini talab qiladi;

3. Xavfsizlik tahdidlari: model zaharlanishi (model poisoning) va gradient inversiya hujumlari FL tizimlarini tahdid ostida qoldirmoqda [10];

4. Tizimli geterogenligi: turli hisoblash quvvatiga ega qurilmalar tufayli o‘qitish jarayoni sekinlashishi mumkin.

O‘zbekiston axborot tizimlari uchun FL ni joriy etish yo‘l xaritasi:

3-jadval.

O‘zbekiston axborot tizimlari uchun FL ni joriy etish yo‘l xaritasi

Bosqich	Muddat	Asosiy chora	FL integratsiyasi
1. Tayyorlov	0-6 oy	Ma’lumot inventarizatsiyasi, audit	FL arxitekturasini tanlash
2. Pilot	6-18 oy	Sog‘liqni saqlash pilot loyiha	FedAvg yoki FedProx tatbiq
3. Kengaytirish	18-36 oy	Davlat tizimlariga tarqatish	DP-FL, maxfiylik audit
4. Integratsiya	36+ oy	Milliy standartlar ishlab chiqish	Blockchain + FL, XAI

XULOSA VA TAKLIFLAR.

Ushbu tadqiqot sun’iy intellekt va kiberxavfsizlik sohasidagi zamonaviy muammolarni FL yondashuvi orqali hal etish imkoniyatlarini ko‘rsatib, quyidagi asosiy xulosalarga olib keldi:

1. FL yondashuvi model aniqligini 92-96% darajada saqlab, GDPR ning ma’lumotlar minimalligi, maqsad cheklanishi va saqlash cheklovi prinsiplarini bir vaqtda qondiradi. Markazlashtirilgan ML ga nisbatan maxfiylik kafolati ancha kuchliroq;

2. FedProx algoritmi non-IID muhitlarda FedAvg ga nisbatan 22% gacha yuqori aniqlik ta’minlab, geterogen tizimli muhitlar uchun eng samarali FL yechimi hisoblanadi;

ISSN 3030-3907

3. GDPR joriy etilganidan beri (2026-yil yanvar holatiga ko‘ra) 7,1 milliard yevrodan ortiq jarima undirilganligi axborot tizimlarida maxfiylikni ta'minlashning nafaqat etik, balki iqtisodiy zaruratini ham ko‘rsatadi;

4. Non-IID muammo, kommunikatsiya xarajatlari, xavfsizlik tahdidlari — FL ning hali to‘liq hal etilmagan asosiy cheklovlari bo‘lib qolmoqda.

O‘zbekiston axborot tizimlari uchun quyidagi takliflar beriladi:

5. Sog‘liqni saqlash va moliya sektorlarida pilot FL loyihalarini amalga oshirish;

6. O‘zDst milliy standartlariga FL talablarini kiritish;

7. «Raqamli O‘zbekiston — 2030» strategiyasi doirasida FL ni ustuvor axborot xavfsizligi texnologiyasi sifatida belgilash;

8. Oliy ta’lim muassasalarida FL bo‘yicha mutaxassislar tayyorlash dasturlarini kengaytirish.

FOYDALANILGAN ADABIYOTLAR

1. Statista Research Department. Volume of data/information created worldwide from 2010 to 2025. — Hamburg: Statista GmbH, 2023.
2. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). — Official Journal of the European Union, L 119, 2018. — P. 1-88.
3. Kiteworks. GDPR Fines Hit 7.1 Billion EUR: Data Privacy Enforcement Trends in 2026. [Online]. URL: https://www.kiteworks.com (murojaat: 2026-yil mart).
4. Duality Technologies. Federated Learning and Global Data Sovereignty Compliance. [Online]. URL: https://dualitytech.com/blog/federated-learning (murojaat: 2025).
5. McMahan H.B., Moore E., Ramage D., Hampson S., y Arcas B.A. Communication-efficient learning of deep networks from decentralized data // AISTATS. — PMLR 54, 2017. — P. 1273-1282.
6. Li T., Sahu A.K., Talwalkar A., Smith V. Federated learning: Challenges, methods, and future directions // IEEE Signal Processing Magazine. — 2020. — Vol. 37, No. 3. — P. 50-60.
7. O‘zbekiston Respublikasi. «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun, O‘RQ-547-son. — Toshkent, 2019.
9. Li T., Sahu A.K., Zaheer M. et al. Federated optimization in heterogeneous networks (FedProx) // MLSys. — 2020. — Vol. 2. — P. 429-450.
10. Abadi M., Chu A., Goodfellow I. et al. Deep learning with differential privacy // CCS'16. — ACM, 2016. — P. 308-318.
11. Gosselin R., Vieu L., Loukil F., Benoit A. The federation strikes back: A survey of federated learning privacy attacks, defenses, applications // ACM Computing Surveys. — 2025. DOI: 10.1145/3724113.

ISSN 3030-3907

12. Roth H.R., Chang K., Singh P. et al. Federated learning for breast density classification: A real-world implementation // DART, LNCS. — Vol. 12444. — Springer, 2020. — P. 181-191.
13. Teo Z.L., Jin L., Liu N. et al. Federated machine learning in healthcare: A systematic review // Cell Reports Medicine. — 2024. — Vol. 5, No. 2. DOI: 10.1016/j.xcrm.2024.101419.
14. Hagestedt I. et al. Toward a tipping point in federated learning in healthcare and life sciences // Patterns. — 2024. — Vol. 5, No. 11. — P. 101077.
15. Collins E., Wang M. Federated learning: A survey on privacy-preserving collaborative intelligence. arXiv:2504.17703. — Arizona State University, 2025.
16. Page M.J. et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews // BMJ. — 2021. — Vol. 372. — n71.
17. Karimireddy S.P. et al. SCAFFOLD: Stochastic controlled averaging for federated learning // ICML. — PMLR 119, 2020. — P. 5088-5099.
18. McMahan H.B., Ramage D. Federated learning: Collaborative machine learning without centralized training data // Google AI Blog. — 2017.