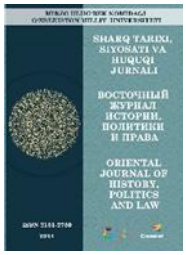
DOI: https://doi.org/10.37547/supsci-ojhpl-06-11-37 Pages: 430-442

Oriental Journal of History, Politics and Law

ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW

journal homepage:
https://www.supportscience.uz/index.php/ojhpl



MECHANISMS FOR INTRODUCING ARTIFICIAL INTELLIGENCE TECHNOLOGIES INTO THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Abbosjon Olimov
Investigator, Investigation Department, Department of Internal Affairs of Chilonzor District
Independent researcher, University of Public Security of the Republic of Uzbekistan
E-mail: abrorolimov048@gmail.com
Tashkent, Uzbekistan

ABOUT ARTICLE

Key words: artificial intelligence, law enforcement, legal regulation, high-risk systems, personal data, biometric identification, human oversight, algorithmic accountability, digital transformation.

Received: 09.11.2026
Accepted: 10.11.2026
Published: 11.11.2026

Abstract: The article examines the legal and institutional mechanisms for introducing artificial intelligence (AI) technologies into the activities of law enforcement agencies. Using formal-legal, comparative-legal and systemic methods, the study analyses the national legal framework of Uzbekistan – the AI Development Strategy until 2030, Presidential Decree PF-189, Resolution PQ-155 on the digital transformation of internal affairs bodies, the Law "On Personal Data" and the new Article 7¹ of the Law "On Informatization" – alongside the EU Artificial Intelligence Act, Directive (EU) 2016/680, the Council of Europe Framework Convention and UNESCO and OECD instruments. AI applications in law enforcement are classified into three risk groups according to their impact on individual rights. A four-level introduction model is proposed (legal basis, institutional structure, technical requirements, human and judicial oversight), together with a matrix of safeguards for each level and the stages of a system's life cycle. Proposals are formulated for further improving national legislation, including a sectoral regulation on the use of AI by internal affairs bodies, mandatory human rights impact assessment and audit logging.

SUN'IY INTELLEKT TEXNOLOGIYALARINI HUQUQNI MUHOFAZA QILUVCHI ORGANLAR FAOLIYATIGA JORIY ETISH MEXANIZMLARI

Abbosjon Olimov
Chilonzor tumani IIO FMB Tergov bo‘limi tergovchisi;
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti mustaqil izlanuvchisi
E-mail: abrorolimov048@gmail.com
Toshkent, O‘zbekiston

MAQOLA HAQIDA

Kalit so‘zlar: sun’iy intellekt, huquqni muhofaza qilish, huquqiy tartibga solish, yuqori xavfli tizimlar, shaxsga doir ma’lumotlar, biometrik identifikatsiya, inson nazorati, algoritmik javobgarlik, raqamli transformatsiya.

Annotatsiya: Maqolada sun’iy intellekt (SI) texnologiyalarini huquqni muhofaza qiluvchi organlar faoliyatiga joriy etishning huquqiy va institutsional mexanizmlari tadqiq etiladi. Formal-huquqiy, qiyosiy-huquqiy va tizimli tahlil usullari asosida O‘zbekistonning milliy huquqiy bazasi – Sun’iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi, PF-189-son Farmon, ichki ishlar organlarini raqamli transformatsiya qilishga oid PQ-155-son qaror, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun hamda “Axborotlashtirish to‘g‘risida”gi Qonunning yangi 7¹-moddasi – Yevropa Ittifoqining Sun’iy intellekt to‘g‘risidagi akti, 2016/680-son Direktivasi, Yevropa Kengashi doiraviy konvensiyasi, UNESCO va OECD hujjatlari bilan qiyosan tahlil qilingan. SI qo‘llanishlari shaxs huquqlariga ta’sir darajasiga ko‘ra uch xavf guruhiga ajratilgan. Normativ asos, institutsional tuzilma, texnik talablar hamda inson va sud nazoratidan iborat to‘rt darajali joriy etish modeli va har bir daraja hamda tizim hayotiy sikli bosqichlari uchun kafolatlar matritsasi taklif etilgan. Milliy qonunchilikni yanada takomillashtirish, jumladan ichki ishlar organlarida SI dan foydalanish bo‘yicha sohaviy nizom, inson huquqlariga ta’sirni majburiy baholash va audit jurnalini yuritishga oid takliflar ishlab chiqilgan.

МЕХАНИЗМЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аббосжон Олимов
Следователь следственного отдела УКД ОВД Чиланзарского района
Самостоятельный соискатель Университета общественной безопасности Республики Узбекистан
E-mail: abrorolimov048@gmail.com
Ташкент, Узбекистан

О СТАТЬЕ

Ключевые слова: искусственный интеллект, правоохранительная деятельность, правовое регулирование, системы высокого риска, персональные данные, биометрическая идентификация, человеческий контроль, алгоритмическая ответственность, цифровая трансформация.

Аннотация: В статье исследуются правовые и институциональные механизмы внедрения технологий искусственного интеллекта (ИИ) в деятельность правоохранительных органов. На основе формально-юридического, сравнительно-правового и системного методов проанализирована национальная правовая база Узбекистана – Стратегия развития технологий ИИ до 2030 года, Указ УП-189, постановление ПП-155 о цифровой трансформации органов внутренних дел, Закон «О персональных данных» и новая статья 7¹ Закона «Об информатизации» – в сопоставлении с Актом ЕС об искусственном интеллекте, Директивой (ЕС) 2016/680, Рамочной конвенцией Совета Европы, документами ЮНЕСКО и ОЭСР. Сферы применения ИИ в правоохранительной деятельности распределены на три группы риска по степени воздействия на права личности. Предложена четырёхуровневая модель внедрения (нормативная основа, институциональная структура, технические требования, человеческий и судебный контроль) и матрица гарантий для каждого уровня и этапов жизненного цикла системы. Сформулированы предложения по дальнейшему совершенствованию национального законодательства, включая отраслевое положение об использовании ИИ органами внутренних дел, обязательную оценку воздействия на права человека и ведение журнала аудита.

Kirish. Sun’iy intellekt (SI) texnologiyalari huquqni muhofaza qiluvchi organlarning kundalik faoliyatiga tobora chuqurroq kirib bormoqda. Xorijiy amaliyotda ular jinoyat sodir etilishi ehtimoli yuqori bo‘lgan hududlarni bashoratlash, video yozuvlarni avtomatik tahlil qilish, shaxsni yuz tasviri yoki ovozi orqali aniqlash hamda katta hajmdagi tergov materiallarini saralash uchun qo‘llanilmoqda [1; 2]. Bu texnologiyalar tergov tezligini oshirish, inson resurslarini samarali taqsimlash va jinoyatlarning oldini olish imkonini beradi. Shu bilan birga, ular inson huquqlari uchun yangi turdagi xavflarni ham yuzaga keltiradi: algoritmdagi xato yoki tarixiy nomutanosiblikni o‘zida aks ettirgan ma’lumotlarda o‘qitilgan model begunoh shaxsni tergov doirasiga tortishi, uning harakatlanish erkinligi va shaxsiy hayot daxlsizligini asossiz cheklashi mumkin [1; 3; 4].

Shu sababli SI ni huquqni muhofaza qilish sohasiga joriy etishni faqat texnik yoki tashkiliy loyiha sifatida ko‘rib chiqish yetarli emas. Majburlov vakolatiga ega davlat organi qo‘llaydigan algoritm oddiy boshqaruv vositasidan farq qiladi, chunki uning natijasi ushlab turish, tintuv, kuzatuv yoki ayblov e’lon qilish kabi shaxs huquqlarini bevosita cheklovchi harakatlarga asos bo‘lishi mumkin. Demak, texnologiya joriy etilishidan avval javobgarlik subyektlari, nazorat tartibi va huquqiy himoya vositalari aniq belgilab olinishi lozim [4].

O‘zbekistonda bu yo‘nalishdagi davlat siyosati so‘nggi yillarda izchil shakllanmoqda. Sun’iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi O‘zbekiston Respublikasi Prezidentining 2024-yil 14-oktabrdagi PQ-358-son qarori bilan tasdiqlangan [5], 2025-yil 22-oktabrdagi PF-189-son Farmon esa sohani yanada rivojlantirish va davlat boshqaruvida SI ni joriy etishga qaratilgan qo‘shimcha chora-tadbirlarni belgilagan [6]. Huquqni muhofaza qilish sohasi uchun ayniqsa muhim hujjat – Prezidentning 2025-yil 30-apreldagi “Ichki ishlar organlari tizimini raqamli transformatsiya qilish bo‘yicha kompleks chora-tadbirlar to‘g‘risida”gi PQ-155-son qarori bo‘lib, u bilan ichki ishlar organlari faoliyatiga SI texnologiyalarini tatbiq etish konsepsiyasi tasdiqlangan [7]. 2026-yil 21-yanvardagi O‘RQ-1115-son Qonun bilan esa “Axborotlashtirish to‘g‘risida”gi Qonunga “sun’iy intellekt” tushunchasi va SI dan foydalanishga oid maxsus 7^1-modda kiritildi [8]. Ushbu hujjatlar sohaning strategik va umumiy huquqiy asosini yaratdi. Endilikda navbatdagi vazifa – umumiy normalarni huquqni muhofaza qilish faoliyatining o‘ziga xos xususiyatlariga moslab aniqlashtirish, ya’ni qaysi tizimlardan qanday maqsadda, qanday kafolatlar bilan foydalanish mumkinligini belgilashdan iborat. Aynan shu masala tadqiqot mavzusining dolzarbligini belgilaydi.

Maqolaning maqsadi SI ni huquqni muhofaza qiluvchi organlar faoliyatiga joriy etishning huquqiy va institutsional mexanizmlarini aniqlash hamda har bir bosqichda zarur bo‘lgan huquqiy kafolatlarni asoslashdan iborat. Ushbu maqsaddan kelib chiqib, tadqiqot quyidagi savollarga javob izlaydi: birinchidan, huquqni muhofaza qilish sohasidagi SI qo‘llanishlarini qanday mezon asosida tasniflash mumkin; ikkinchidan, joriy etish jarayoni qanday darajalardan iborat va har bir darajada qanday kafolatlar talab etiladi; uchinchidan, O‘zbekiston qonunchiligi ushbu talablarga qay darajada javob beradi va uni qaysi yo‘nalishlarda takomillashtirish maqsadga muvofiq?

Tadqiqotning ilmiy yangiligi quyidagilarda namoyon bo‘ladi: huquqni muhofaza qilish sohasidagi SI qo‘llanishlarining shaxs huquqlariga ta’sir darajasiga asoslangan uch guruhli tasnifi taklif etildi; joriy etishning to‘rt darajali modeli ishlab chiqildi va u tizim hayotiy siklining bosqichlari bilan bog‘langan kafolatlar matritsasi shaklida aniqlashtirildi; “Axborotlashtirish to‘g‘risida”gi Qonunning yangi 7^1-moddasi huquqni muhofaza qilish faoliyati kontekstida ilk bor tahlil qilinib, uni amalga oshirish mexanizmlari asoslandi.

Adabiyotlar sharhi. Mavzuga oid ilmiy adabiyotlarni shartli ravishda uch yo‘nalishga ajratish mumkin: bashoratli politsiya faoliyatining ijtimoiy oqibatlarini o‘rganuvchi tadqiqotlar, algoritmik noxolislikni aniq misollarda ko‘rsatgan ishlar hamda huquqiy tartibga solish va etik tamoyillarga bag‘ishlangan manbalar.

Birinchi yo‘nalishda bashoratli tahlilning tarixiy ma’lumotlarga tayanishi asosiy muammo sifatida ko‘riladi. A.G. Ferguson bunday tizimlar o‘tmishdagi amaliyotdagi nomutanosibliklarni yangi texnologik shaklda qayta ishlab chiqarishi mumkinligini ko‘rsatadi [1]. S. Brayne Los-Anjeles politsiya departamentidagi kuzatuvlari asosida katta ma’lumotlar xodimning mustaqil qaror qabul qilish imkoniyatini qanday o‘zgartirishi va kuzatuv doirasini qanday kengaytirishini o‘rganadi [2]. K. Lum va W. Isaac esa bashoratli modelni Oklend shahri ma’lumotlarida sinab, jarayonning o‘z-o‘zini kuchaytirishi xavfini qayd etadi: xodimlar ko‘proq yuborilgan hududda ko‘proq huquqbuzarlik qayd etiladi, bu esa keyingi bashoratda o‘sha hududni yana yuqori xavfli qilib ko‘rsatadi [3].

Ikkinchi yo‘nalishdagi tadqiqotlar bu xavflar nazariy taxmin emasligini tasdiqlaydi. J. Buolamwini va T. Gebru yuz tasviri asosida jinsni aniqlovchi tijorat tizimlarida teri rangi to‘q ayollar uchun xatolik darajasi 34,7 foizgacha yetgani, teri rangi och erkaklar uchun esa 0,8 foizdan oshmaganini ko‘rsatgan [9]. J. Angwin va hammualliflarining tahlilida AQShda qo‘llaniladigan COMPAS dasturi afroamerikalik ayblanuvchilarni boshqa ayblanuvchilarga nisbatan deyarli ikki baravar ko‘p hollarda noto‘g‘ri ravishda yuqori xavfli deb belgilagani aniqlangan [10]. V. Eubanks esa jamoat sektoridagi avtomatlashtirilgan tizimlar ijtimoiy jihatdan himoyaga muhtoj guruhlarga nomutanosib zarar yetkazishi mumkinligini yoritadi [11]. Bu natijalar algoritm aniqligini umumiy ko‘rsatkich bilan emas, balki turli guruhlar kesimida baholash zarurligini ko‘rsatadi.

Uchinchi yo‘nalish yuqoridagi xavflarga huquqiy javoblarni qamrab oladi. Yevropa Ittifoqining 2024/1689-son reglamenti (Sun’iy intellekt to‘g‘risidagi akt) huquqni muhofaza qilish maqsadida jamoat joylarida real vaqt rejimida masofaviy biometrik identifikatsiyadan foydalanishni asosan taqiqlaydi, istisnolarni esa sud yoki mustaqil ma’muriy organning oldindan beriladigan ruxsatiga bog‘laydi [12; 5-modda]. Reglament shaxsning jinoyat sodir etish ehtimolini faqat profilashtirish yoki uning shaxsiy xususiyatlari asosida baholashni taqiqlangan amaliyotlar qatoriga kiritgan, dalillarning ishonchliligini baholash va profilashtirish tizimlarini esa yuqori xavfli deb belgilagan [12; III-ilova, 6-band]. 2016/680-son Direktiva biometrik ma’lumotlarga ishlov berishni faqat qat’iy zarurat bo‘lganda va tegishli kafolatlar mavjud bo‘lganda ruxsat etadi hamda faqat avtomatlashtirilgan ishlov berishga asoslangan va shaxs uchun salbiy huquqiy oqibat keltiruvchi qarorlarni, qonunda kafolatlar nazarda tutilgan hollar bundan mustasno, taqiqlaydi [13; 10, 11-moddalar].

M. Veale va F.Z. Borgesius xavf darajasiga asoslangan yondashuvning kuchli va zaif tomonlarini tahlil qilib, yuqori xavfli tizimlar muvofiqligini baholashning asosan standartlar va o‘zini o‘zi baholashga tayanishini uning zaif nuqtasi sifatida qayd etgan [14]. Etik tamoyillar darajasida UNESCO tavsiyasi [4], L. Floridi va hammualliflari taklif etgan besh tamoyil (foyda keltirish, zarar yetkazmaslik, avtonomiya, adolat va tushuntirib berilishi) [15] hamda OECD tavsiyasi [16] umumiy yo‘nalishni belgilaydi. Inson huquqlari va asosiy erkinliklarini himoya qilish to‘g‘risidagi konvensiyaning 6, 8 va 13-moddalari [17], shaxsga doir ma’lumotlarni avtomatlashtirilgan tarzda qayta ishlashda shaxslarni himoya qilish to‘g‘risidagi konvensiyani o‘zgartiruvchi protokol (108+) [18] hamda Yevropa Kengashining SI to‘g‘risidagi doiraviy konvensiyasi [19] huquqiy kafolatlar uchun qiyosiy mezon bo‘lib xizmat qiladi. NIST tomonidan ishlab chiqilgan xavflarni boshqarish asosi [20] va ISO/IEC 42001 standarti [21] esa texnik boshqaruvni tashkil etishda tayanch hisoblanadi.

Milliy qonunchilikka kelsak, O‘zbekistonda shaxsga doir ma’lumotlar bilan bog‘liq munosabatlar 2019-yil 2-iyuldagi O‘RQ-547-son Qonun bilan tartibga solinadi [22]. “Axborotlashtirish to‘g‘risida”gi Qonunning 7^1-moddasi esa SI asosida ishlaydigan axborot tizimlari insonning hayoti, sog‘lig‘i, erkinligi, sha’ni va qadr-qimmatiga putur yetkazmasligi shartligini hamda inson huquqi va erkinligiga aloqador yuridik ahamiyatga ega qarorlar qabul qilishda faqat bunday tizimlar xulosalariga tayanish mumkin emasligini mustahkamladi [8]. Adabiyotlar sharhi shuni ko‘rsatadiki, xorijiy ilmiy manbalarda SI bilan bog‘liq xavflar yetarlicha o‘rganilgan bo‘lsa-da, ularni milliy huquq tizimiga moslashtirilgan va huquqni muhofaza qilish faoliyatining o‘ziga xosligini hisobga olgan yaxlit joriy etish modeli hali ishlab chiqilmagan. Mazkur maqola shu bo‘shliqni to‘ldirishga qaratilgan.

Tadqiqot metodologiyasi. Tadqiqot nazariy-huquqiy xarakterga ega va uch guruh manbaga tayanadi: xalqaro hujjatlar va xorijiy ilmiy adabiyotlar; O‘zbekiston Respublikasining normativ-huquqiy hujjatlari (O‘RQ-547, O‘RQ-1115, PQ-358, PQ-155, PF-189); davlat organlarining rasmiy e’lonlari. Formal-huquqiy usul normalar mazmunini aniqlash, qiyosiy-huquqiy usul Yevropa Ittifoqi va Yevropa Kengashi yondashuvlarini milliy qonunchilik bilan solishtirish, tizimli tahlil esa joriy etish jarayonining alohida unsurlari o‘rtasidagi bog‘liqlikni ochib berish uchun qo‘llanildi. SI qo‘llanishlari shaxs huquqlariga ta’sir darajasi mezoni bo‘yicha tasniflandi, joriy etish modeli esa tizimning hayotiy sikli (loyihalash, sinov, ekspluatatsiya, audit) bosqichlari bilan qiyoslab aniqlashtirildi. Tadqiqotning cheklovi shundaki, unda empirik ma’lumotlar (tizimlar ishlashi natijalari, statistika) tahlil qilinmaydi: idoraviy tizimlarning texnik tavsiflari ochiq e’lon qilinmagani sababli tahlil normativ hujjatlar va rasmiy axborotlar bilan cheklangan.

Tahlil va natijalar. *SI qo‘llanishlarini xavf darajasiga ko‘ra tasniflash.* Joriy etish modelini qo‘llashdan oldin SI qo‘llanishlarini xavf darajasiga ko‘ra farqlash zarur, chunki har bir qo‘llanish uchun kafolatlar hajmi uning shaxs huquqlariga ta’siriga mutanosib bo‘lishi lozim. Ushbu mezon asosida qo‘llanishlarni uch guruhga ajratish mumkin (1-jadval).

1-jadval. Huquqni muhofaza qilish sohasidagi SI qo‘llanishlarining xavf darajasi bo‘yicha tasnifi (muallif taklifi)

Guruh	Qo‘llanish turlari	Asosiy xavf	Zarur huquqiy rejim
I. Qat’iy cheklanadigan (alohida ruxsat talab qilinadigan)	jamoat joylarida real vaqt rejimidagi masofaviy biometrik identifikatsiya; yuz tasvirlarini maqsadsiz yig‘ish orqali bazalar shakllantirish; faqat shaxsiy xususiyatlarga asoslangan jinoiy xavf bashorati	shaxsiy hayot daxlsizligi va harakatlanish erkinligiga keng ko‘lamli aralashuv	qonunda to‘liq ro‘yxat bilan belgilangan istisnolar; sud yoki mustaqil organning oldindan ruxsati; qat’iy muddat va hudud chegarasi
II. Yuqori xavfli	dalillarni baholash, xavf darajasini hisoblash, profilashtirish, ovoz va yuz bo‘yicha post-faktum identifikatsiya, tergov materiallarini tahliliy saralash	noxolislik, noto‘g‘ri gumon, aybsizlik prezumpsiyasining buzilishi	joriy etishdan oldin inson huquqlariga ta’sirni baholash; guruhlar kesimida sinov; inson tasdig‘i; audit jurnali; shikoyat qilish huquqi
III. Past xavfli	hujjatlarni tarjima qilish, murojaatlarni tasniflash, ma’muriy jarayonlarni avtomatlashtirish, statistik hisobotlar	axborot xavfsizligi, ma’lumotlar sizib chiqishi	umumiy shaffoflik va axborot xavfsizligi talablari; SI qo‘llanilganini belgilash

Birinchi guruhga qo‘llanilishi qat’iy cheklanishi lozim bo‘lgan tizimlar kiradi. Masalan, Yevropa Ittifoqi reglamenti internet yoki kuzatuv kameralari yozuvlaridan yuz tasvirlarini maqsadsiz yig‘ish orqali yuzni tanib olish bazalarini yaratish yoki kengaytirishni taqiqlangan amaliyot deb hisoblaydi [12; 5-modda]. Milliy qonunchilik uchun bu yondashuvdan foydalanish chet el modelini mexanik ko‘chirishni emas, balki eng intruziv texnologiyalar uchun alohida ruxsat tartibini belgilashni anglatadi. Ikkinchi guruhga dalillarni baholash, xavf darajasini hisoblash va profilashtirish tizimlari kiradi; ular foydalanishga topshirilishidan oldin ekspertizadan o‘tishi kerak bo‘lgan yuqori xavfli tizimlardir. PQ-155-son qarorda rejalashtirilgan ovoz asosida shaxsni identifikatsiya qilish texnologiyalari [7] ham aynan shu guruhga mansub, chunki ovoz yuz tasviri singari biometrik ma’lumot hisoblanadi. Uchinchi guruhni esa shaxs huquqlariga bevosita ta’sir qilmaydigan qo‘llanishlar tashkil etadi; ularga nisbatan umumiy shaffoflik va axborot xavfsizligi talablari yetarli bo‘lishi mumkin. Tasnifning amaliy ahamiyati shundaki, u resurslarni eng ko‘p

nazorat talab qiladigan tizimlarga yo‘naltirish va past xavfli loyihalarni ortiqcha byurokratik talablardan ozod qilish imkonini beradi.

To‘rt darajali joriy etish modeli. Tahlil natijalari SI ni huquqni muhofaza qiluvchi organlar faoliyatiga joriy etishni o‘zaro bog‘liq to‘rt darajadan iborat model sifatida ko‘rish mumkinligini ko‘rsatdi. Birinchi daraja – normativ asos – nimaga ruxsat etilganini, ikkinchi daraja – institutsional tuzilma – tizimni kim tasdiqlashi va kim nazorat qilishini, uchinchi daraja – texnik talablar – qanday ma’lumot va algoritm ishlatilishini belgilaydi. To‘rtinchi daraja, ya’ni inson va sud nazorati, yakuniy qarorni kim qabul qilishini hamda shaxs uning ustidan qanday shikoyat qila olishini hal qiladi. Bu darajalar ketma-ket emas, balki birgalikda ishlaydi: normativ asos bo‘lmasa, nazorat amalda ishlamaydi, mustaqil nazorat bo‘lmasa esa eng puxta yozilgan norma ham to‘liq ijro etilmaydi.

Normativ asos. Birinchi daraja nuqtayi nazaridan asosiy talab qonuniylik tamoyilidan kelib chiqadi: shaxsiy hayotga har qanday aralashuv qonunga muvofiq bo‘lishi va qonuniy maqsadga mutanosib bo‘lishi kerak. Inson huquqlari va asosiy erkinliklarini himoya qilish to‘g‘risidagi konvensiyaning 8-moddasi talqinida bu talab qonunning shunchaki mavjud bo‘lishini emas, balki uning ochiq, aniq va oqibatlarini oldindan ko‘ra bilish mumkin bo‘lishini ham anglatadi [17; 8-modda]. O‘zbekistonda ushbu daraja bo‘yicha muhim qadamlar qo‘yildi: PQ-358 va PF-189 hujjatlari sohaning strategik yo‘nalishini [5; 6], PQ-155 ichki ishlar organlari uchun SI ni tatbiq etish konsepsiyasini [7], “Axborotlashtirish to‘g‘risida”gi Qonunning 7^1-moddasi esa SI dan foydalanishning umumiy huquqiy chegaralarini [8] belgiladi. Keyingi bosqichda ushbu umumiy normalarni idoraviy darajada aniqlashtirish maqsadga muvofiq: tizimdan foydalanish maqsadlari, foydalanilishi mumkin bo‘lmagan ma’lumot manbalari, ma’lumotlarni saqlash muddatlari va foydalanishga ruxsat beruvchi organ alohida normativ hujjatda aniq ko‘rsatilishi lozim.

Institutsional tuzilma. Normativ asos qanchalik puxta bo‘lmasin, uning ijrosi institutsional tuzilmaga bog‘liq. PQ-155-son qaror bilan Ichki ishlar vazirligi tarkibida Raqamli texnologiyalar va huquqiy statistika departamenti tashkil etildi [7], PF-189-son Farmon esa davlat organlarida SI loyihalarini joriy etishni muvofiqlashtirish tartibini belgiladi [6]. Bu SI joriy etishning boshqaruv markazini aniqlab berdi. Nazariy jihatdan muhim masala shundaki, nazoratning samaradorligi funksiyalarning taqsimlanishiga bog‘liq: agar bitta bo‘linma tizimni ishlab chiqsa, undan foydalansa va o‘zi baholasa, ichki nazorat yetarli mustaqillikka ega bo‘lmaydi. Shu bois ishlab chiqish, foydalanish va audit funksiyalarini turli subyektlarga yuklatish tavsiya etiladi; masalan, shaxsga doir ma’lumotlarni muhofaza qilish bo‘yicha vakolatli organ va prokuratura nazoratining roli aniq belgilanishi mumkin. Yevropa Kengashining doiraviy konvensiyasi ham SI tizimlarining butun hayotiy sikli davomida xavf va ta’sirni baholash tizimini yaratishni talab qiladi [19; 16-modda], bu esa nazoratning bir martalik emas, balki uzluksiz bo‘lishini taqozo etadi.

Texnik talablar. Uchinchi daraja ma’lumotlar va algoritmlar sifatiga taalluqli. Rasmiy xabarlarga ko‘ra, davlat organlari o‘z ma’lumotlar bazalarini yagona “Data-markaz”ga o‘tkazish vazifasini olgan [23]. Ma’lumotlarni markazlashtirish boshqaruvni soddalashtiradi va idoralararo hamkorlikni tezlashtiradi, biroq markazlashgan bazaning xavfsizligiga talab ham shunga mos ravishda oshadi. Shu sababli axborot xavfsizligi loyihaning keyingi bosqichi emas, balki uning ajralmas qismi sifatida rejalashtirilishi kerak. Adabiyotlar sharhida ko‘rsatilgan noxolislik xavfidan kelib chiqib, eng muhim texnik talablar ikkita: birinchidan, tizim xatoliklarini turli ijtimoiy guruhlar kesimida o‘lchash [9]; ikkinchidan, har bir so‘rov va qarorni keyingi audit uchun qayd etish [20; 21]. 2016/680-son Direktiva ham avtomatlashtirilgan ishlov berish tizimlarida ma’lumotlarni yig‘ish, ko‘rish, o‘zgartirish va uzatish harakatlarini jurnalda qayd etishni talab qiladi [13; 25-modda]. Bundan tashqari, biometrik ma’lumotlar shaxsga doir ma’lumotlarning alohida himoya talab qiladigan turi ekanini hisobga olib, yuz va ovoz namunalarini saqlash muddatlari va o‘chirish tartibi texnik reglamentlarda aks ettirilishi lozim [22].

Inson va sud nazorati. To‘rtinchi daraja qolgan uchtasining samaradorligini yakuniy tarzda ta’minlaydi. Agar xodim tizim natijasini tekshirmasdan tasdiqlasa, inson nazorati formal tus oladi: avtomatlashtirishga ortiqcha ishonish (automation bias) qaror sifatini pasaytiradi va javobgarlikni algoritm ortiga yashiradi. Milliy qonunchilik bu masalada aniq pozitsiyani egalladi: “Axborotlashtirish to‘g‘risida”gi Qonunning 7^1-moddasiga ko‘ra, inson huquqi va erkinligiga aloqador yuridik ahamiyatga ega qarorlarni qabul qilishda faqat SI asosida ishlaydigan tizimlar xulosalariga tayanish mumkin emas [8]. Ushbu norma huquqni muhofaza qilish faoliyati uchun alohida ahamiyatga ega, chunki tergov harakatlari va protsessual qarorlarning aksariyati aynan shu toifaga kiradi. Uni amalda ta’minlash uchun protsessual mexanizm zarur: xodim tizim natijasini rad etish huquqiga ega bo‘lishi, natijani mustaqil dalillar bilan tekshirishi va o‘z qarorini asoslab hujjatlashtirishi kerak. Qiyosiy misol sifatida Yevropa Ittifoqi reglamenti masofaviy biometrik identifikatsiya natijasi asosida biror harakat qilishdan oldin uni kamida ikki nafar vakolatli shaxs alohida tekshirib tasdiqlashini talab qiladi [12; 14-modda]. Shaxs esa o‘ziga nisbatan qabul qilingan qaror asosidagi ma’lumotlarni olish va bu qaror ustidan sudga shikoyat qilish huquqiga ega bo‘lishi lozim [13; 11-modda], [17; 6, 13-moddalar]. Real vaqt rejimidagi biometrik identifikatsiya kabi eng intruziv qo‘llanishlarda esa sud yoki mustaqil organning oldindan beriladigan ruxsati maqsadga muvofiq [12; 5-modda].

Modelning darajalari tizim hayotiy siklining turli bosqichlarida turlicha namoyon bo‘ladi. Shu sababli har bir daraja va bosqich uchun zarur kafolatlarni matritsa shaklida ifodalash amaliy jihatdan qulay (2-jadval).

2-jadval. SI tizimlarini joriy etishda kafolatlar matritsasi (muallif taklifi)

Model darajasi	Loyihalash va sinov	Ekspluatatsiya	Audit va qayta baholash
Normativ asos	foydalanish maqsadi va xavf guruhini hujjatda belgilash; huquqiy ekspertiza	faqat belgilangan maqsadda foydalanish; ma'lumot manbalari ro'yxatiga rioya	normaning zarurligi va mutanosibligini davriy qayta ko'rib chiqish
Institutsional tuzilma	ishlab chiquvchi, foydalanuvchi va auditorni ajratish; ichki tasdiqlash tartibi	foydalanishga ruxsat berilgan xodimlar doirasi; idoraviy nazorat	mustaqil audit, prokuror nazorati, vakolatli organga hisobot
Texnik talablar	ma'lumotlar sifati; guruhlar kesimida sinov; axborot xavfsizligi	har bir so'rovni jurnalga yozish; saqlash muddatlariga rioya	xatoliklar statistikasi tahlili; modelni yangilash yoki to'xtatish
Inson va sud nazorati	xodimlarni o'qitish; natijani tekshirish tartibini ishlab chiqish	inson tasdig'i; rad etish huquqi; qarorni asoslash	shikoyatlar tahlili; sud amaliyotini umumlashtirish

Muhokama. Taklif etilgan model xavfsizlik va shaxs huquqlari o'rtasidagi muvozanatni ta'minlashga xizmat qiladi. Jinoyatlarni tezroq ochish va oldini olish jamiyat xavfsizligiga bevosita foyda keltiradi, ammo kuzatuv vositalari qonun bilan aniq chegaralanmasa, fuqarolarning qonuniy faoliyatiga ham ta'sir ko'rsatishi mumkin. Ilmiy adabiyotda bu hodisa "sovutuvchi ta'sir" (chilling effect) deb ataladi: shaxs o'zini kuzatilayotganini bilgani uchun qonuniy xatti-harakatlardan ham o'zini tiyadi. Shu sababli kuzatuv hajmi va muddati qonun bilan cheklanishi, uning zarurligi va mutanosibligi esa muntazam ravishda qayta baholanib turishi kerak. Bu yondashuv SI texnologiyalaridan voz kechishni emas, aksincha, ularga jamoatchilik ishonchini mustahkamlash orqali barqaror joriy etishni nazarda tutadi.

Yevropa tajribasini qiyosiy mezon sifatida qo'llashda ehtiyotkorlik zarur. M. Veale va F.Z. Borgesius ta'kidlaganidek, xavfga asoslangan yondashuv standartlar va o'zini o'zi baholashga ortiqcha tayanganda samaradorligini yo'qotishi mumkin [14]. Shuning uchun milliy modelda tashqi, mustaqil audit unsuri alohida o'rin egallaydi. Shu bilan birga, O'zbekiston yondashuvining ustun jihati ham bor: 7^1-moddadagi faqat SI xulosasiga tayanish taqiqi barcha davlat organlariga nisbatan umumiy qoida sifatida qonun darajasida mustahkamlangan [8], bu esa sohaviy hujjatlar uchun mustahkam tayanch bo'lib xizmat qiladi. UNESCO tavsiyasida ham SI tizimlari inson javobgarligi va nazorati o'rnini bosa olmasligi alohida qayd etilgan [4].

Shuni ham qayd etish lozimki, sohaviy yondashuv boshqa tarmoqlarda ham shakllanmoqda: masalan, sudlar faoliyatiga SI texnologiyalarini joriy etishga oid alohida farmon qabul qilingan [24]. Bu huquqni muhofaza qilish organlari uchun ham shunga o'xshash, ya'ni faoliyatning o'ziga xosligini hisobga olgan alohida nizom ishlab chiqish imkoniyatini ko'rsatadi.

Tergov va sud faoliyatidagi SI qo‘llanishlarini muvofiqlashtirish ham muhim: dastlabki tergovda SI yordamida olingan ma’lumotlarning dalil sifatida maqbulligi va ularni sudda tekshirish tartibi Jinoyat-protsessual qonunchiligi doirasida alohida o‘rganilishi lozim. Bu masala tadqiqotning keyingi yo‘nalishi sifatida belgilanadi.

Xulosa. O‘tkazilgan tahlil SI ni huquqni muhofaza qiluvchi organlar faoliyatiga joriy etish texnik jarayondan ko‘ra ko‘proq huquqiy tartibga solishni talab qilishini ko‘rsatdi. Taklif etilgan to‘rt darajali model (normativ asos, institutsional tuzilma, texnik talablar, inson va sud nazorati) yaxlit holda ishlaydi: ulardan biri yetishmasa, qolganlari ham to‘liq samara bermaydi. O‘zbekistonda sohaning strategik asoslari (PQ-358, PF-189), ichki ishlar organlari uchun maxsus konsepsiya (PQ-155) va SI dan foydalanishning umumiy huquqiy chegaralari (“Axborotlashtirish to‘g‘risida”gi Qonunning 7^1-moddasi) belgilangan. Navbatdagi bosqichda ushbu normalarni huquqni muhofaza qilish faoliyatining o‘ziga xos xususiyatlariga moslab aniqlashtirish maqsadga muvofiq. Yuqoridagilardan kelib chiqib, quyidagi takliflar ilgari suriladi.

Birinchidan, ichki ishlar organlarida SI dan foydalanish tartibi to‘g‘risida sohaviy nizom qabul qilinishi maqsadga muvofiq; unda foydalanish maqsadlari, tizim turlari va ularning xavf guruhlari, ma’lumot manbalari, saqlash muddatlari hamda alohida ruxsat talab qilinadigan qo‘llanishlar aniq belgilanishi lozim.

Ikkinchidan, yuqori xavfli tizimlar foydalanishga topshirilishidan oldin ularning inson huquqlariga ta’sirini baholash majburiy tartibini joriy etish, baholash xulosalarining umumlashtirilgan natijalarini esa ma’lumotlar xavfsizligiga zarar yetkazmagan holda e’lon qilib borish tavsiya etiladi.

Uchinchidan, tizimni ishlab chiqish, undan foydalanish va uni audit qilish funksiyalari turli subyektlarga yuklatilishi, xatoliklar turli ijtimoiy guruhlar kesimida o‘lchanishi va har bir so‘rov hamda qaror audit jurnalida qayd etilishi lozim.

To‘rtinchidan, “Axborotlashtirish to‘g‘risida”gi Qonunning 7^1-moddasini amalga oshirish uchun protsessual mexanizm ishlab chiqilishi zarur: xodim tizim natijasini rad etish va buning asosini yozma ravishda ko‘rsatish huquqiga ega bo‘lishi, SI natijasi esa mustaqil dalillar bilan tasdiqlanmaguncha protsessual qarorning yagona asosi bo‘la olmasligi belgilanishi lozim.

Beshinchidan, fuqarolarning o‘zlariga nisbatan qo‘llanilgan avtomatlashtirilgan tahlil to‘g‘risida ma’lumot olish, o‘zlariga doir ma’lumotlarni tuzatish va tegishli qaror ustidan sudga shikoyat qilish huquqlarini kafolatlovchi tartib aniq belgilanishi maqsadga muvofiq.

Foydalanilgan adabiyotlar ro‘yxati:

1. Ferguson A.G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. – New York: NYU Press, 2017.

2. Brayne S. Predict and Surveil: Data, Discretion, and the Future of Policing. – New York: Oxford University Press, 2020.

3. Lum K., Isaac W. To Predict and Serve? // Significance. – 2016. – Vol. 13, № 5. – P. 14–19. – DOI: 10.1111/j.1740-9713.2016.00960.x

4. UNESCO. Recommendation on the Ethics of Artificial Intelligence. – Paris: UNESCO, 2021.

5. O‘zbekiston Respublikasi Prezidentining 2024-yil 14-oktabrdagi “Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PQ-358-son qarori. – URL: https://lex.uz/docs/-7158604

6. O‘zbekiston Respublikasi Prezidentining 2025-yil 22-oktabrdagi “Sun’iy intellekt texnologiyalarini yanada rivojlantirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida”gi PF-189-son Farmoni. – URL: https://lex.uz/docs/-7789403

7. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Ichki ishlar organlari tizimini raqamli transformatsiya qilish bo‘yicha kompleks chora-tadbirlar to‘g‘risida”gi PQ-155-son qarori. – URL: https://lex.uz/docs/7511360

8. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni (2026-yil 21-yanvardagi O‘RQ-1115-son Qonun bilan kiritilgan o‘zgartish va qo‘shimchalar bilan). – URL: https://lex.uz/acts/-83472

9. Buolamwini J., Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification // Proceedings of Machine Learning Research. – 2018. – Vol. 81. – P. 77–91.

10. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias // ProPublica. – 2016. – 23 May. – URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

11. Eubanks V. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. – New York: St. Martin’s Press, 2018.

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. – 2024. – L 2024/1689.

13. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences // Official Journal of the European Union. – 2016. – L 119. – P. 89–131.

14. Veale M., Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act // Computer Law Review International. – 2021. – Vol. 22, № 4. – P. 97–112. – DOI: 10.9785/cri-2021-220402

15. Floridi L., Cowls J., Beltrametti M. et al. AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations // Minds and Machines. – 2018. – Vol. 28. – P. 689–707. – DOI: 10.1007/s11023-018-9482-5

16. OECD. Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). – Paris: OECD, 2019.

17. Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5). – Rome, 1950.

18. Council of Europe. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). – Strasbourg, 2018.

19. Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). – Vilnius, 2024.

20. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. – Gaithersburg: NIST, 2023. – DOI: 10.6028/NIST.AI.100-1

21. ISO/IEC 42001:2023. Information technology – Artificial intelligence – Management system. – Geneva: ISO, 2023.

22. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-son Qonuni. – URL: https://lex.uz/docs/4396419

23. Sun’iy intellekt texnologiyalarini joriy qilish yangi bosqichga olib chiqiladi // O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. – URL: https://gov.uz/oz/news/view/94575

24. O‘zbekiston Respublikasi Prezidentining 2025-yil 23-avgustdagi “Sudlar faoliyatiga sun’iy intellekt texnologiyalarini joriy etish orqali odil sudlovga erishish darajasini oshirish hamda sud tizimining moddiy-texnik ta’minotini yaxshilashga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PF-140-son Farmoni. – URL: https://lex.uz/docs/-7696567