SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

ICHKI ISHLAR ORGANLARIDA SHAXSGA DOIR MA'LUMOTLAR TO'G'RISIDAGI QONUNNI QO'LLASHNING AYRIM JIHATLARI

Madaliyev Azizbek Sherzodjon o'g'li

O‘zbekiston Respublikasi IIV Akademiyasi 3-kurs kursanti

Toshkent. sh

https://doi.org/10.5281/zenodo.20704843

Annotatsiya: Mazkur ilmiy maqolada ichki ishlar organlari (IIO) faoliyatida shaxsga doir ma'lumotlarni yig‘ish, qayta ishlash, saqlash va himoya qilish jarayonlarining huquqiy va amaliy jihatlari tahlil qilingan. Jinoyatlarni fosh etish hamda jamoat xavfsizligini ta'minlash zarurati bilan fuqarolarning shaxsiy hayot daxlsizligi o‘rtasidagi huquqiy muvozanatni ta'minlash muammolari ilmiy asoslangan. Amaliyotdagi ma'lumotlar sizib chiqishi (insider threats) xavfi, axborot tizimlariga vakolatsiz kirishning oldini olish va tizimli audit loglarni yuritish masalalari yoritilgan. Yevropa Ittifoqi (GDPR), AQSh (CJIS) va Janubiy Koreyaning ilg‘or xorij tajribasi qiyosiy o‘rganilib, O‘zbekiston Respublikasining milliy qonunchiligi va huquqni qo‘llash amaliyotini, xususan, raqamli xavfsizlik arxitekturasini takomillashtirish yuzasidan aniq ilmiy-amaliy takliflar ishlab chiqilgan.

Kalit so‘zlar: shaxsga doir ma'lumotlar, ichki ishlar organlari, shaxsiy hayot daxlsizligi, kiberxavfsizlik, raqamli izlar, GDPR, insayder tahdidlar, ma'lumotlar himoyasi, axborot xavfsizligi.

Аннотация: В данной научной статье анализируются правовые и практические аспекты процессов сбора, обработки, хранения и защиты персональных данных в деятельности органов внутренних дел (ОВД). Научно обоснованы проблемы обеспечения правового баланса между необходимостью раскрытия преступлений и обеспечением общественной безопасности, с одной стороны, и неприкосновенностью частной жизни граждан — с другой. Освещены практические риски утечки данных (insider threats), предотвращения

несанкционированного доступа к информационным системам и ведения системного аудита (audit logs). Изучен передовой зарубежный опыт Европейского Союза (GDPR), США (CJIS) и Южной Кореи, разработаны конкретные научно-практические предложения по совершенствованию национального законодательства и правоприменительной практики Республики Узбекистан, в частности архитектуры цифровой безопасности.

Ключевые слова: персональные данные, органы внутренних дел, неприкосновенность частной жизни, кибербезопасность, цифровые следы, GDPR, инсайдерские угрозы, защита данных, информационная безопасность.

Abstract: This scientific article analyzes the legal and practical aspects of the collection, processing, storage, and protection of personal data in the activities of internal affairs bodies (IAB). The problems of ensuring a legal balance between the need to solve crimes and ensure public security, on the one hand, and the privacy of citizens, on the other, are scientifically substantiated. Practical risks of data leakage (insider threats), prevention of unauthorized access to information systems, and the maintenance of systemic audit logs are highlighted. The advanced foreign experience of the European Union (GDPR), the USA (CJIS), and South Korea was comparatively studied, and specific scientific and practical proposals were developed for improving the national legislation and law enforcement practice of the Republic of Uzbekistan, particularly the digital security architecture.

Keywords: personal data, internal affairs bodies, privacy, cybersecurity, digital footprints, GDPR, insider threats, data protection, information security.

Raqamli texnologiyalar asrida shaxsga doir ma'lumotlar nafaqat inson huquqlarining ajralmas qismi, balki davlat boshqaruvi va huquqni muhofaza qilish organlari faoliyatining asosiy axborot resursiga aylandi. O‘zbekiston Respublikasining Konstitutsiyasi va "Shaxsga doir ma'lumotlar to‘g‘risida"gi Qonuniga asosan, har bir

shaxs o‘zining shaxsiy hayoti daxlsizligiga, shaxsiy va oilaviy sirlari himoya qilinishiga haqli.

Ichki ishlar organlari davlat miqyosida shaxsga doir ma'lumotlarning eng yirik bazalariga (pasport tizimi, biometrik ma'lumotlar, jinoiy va ma'muriy huquqbuzarliklar hisobi, avtomototransport vositalari reestri va h.k.) ishlov beruvchi subyekt hisoblanadi. Bu holat IIO xodimlari zimmasiga ikki karra mas'uliyat yuklaydi: birinchidan, jinoyatchilikka qarshi kurashish uchun ushbu ma'lumotlardan tezkorlik bilan foydalanish; ikkinchidan, fuqarolarning ma'lumotlarini qonunga xilof ravishda tarqalishi, o‘zgartirilishi yoki yo‘q qilinishidan mutlaq himoya qilish. Amaliyotda bu ikki maqsad o‘rtasidagi qonuniy muvozanatni saqlash qator huquqiy va texkologik yechimlarni talab etmoqda.

IIO faoliyatida axborot bazalarining kengayishi bilan shaxsga doir ma'lumotlar to‘g‘risidagi qonunchilik talablarini buzish xavfi ham ortib boradi. Asosiy muammolarni quyidagicha guruhlash mumkin:

- **Vakolat doirasidan asossiz chiqish:** Ba'zi hollarda xodimlar tomonidan fuqarolar haqidagi maxfiy axborotni (yashash manzili, sudlanganligi, avtomobil ma'lumotlari) bevosita xizmat zaruratisiz — shaxsiy qiziqish, tanish-bilishchilik yoxud uchinchi shaxslarning iltimosiga ko‘ra elektron bazalardan izlash holatlari uchraydi.
- **Insayder tahdidlar (Insider threats):** Jinoyat olami vakillari, xususiy detektivlar yoxud firibgarlar IIO bazalaridagi ma'lumotlarga qonuniy ruxsati bor xodimlarni moddiy qiziqtirish orqali ma'lumotlarni noqonuniy qo‘lga kiritishga urinishadi. Xodimlarning axborot xavfsizligi bo‘yicha hushyorligining pastligi bu xavfni yanada oshiradi.
- **Idoralararo ma'lumot almashinuvidagi zaifliklar:** Turli davlat organlari (soliq, bojxona, sog‘liqni saqlash) o‘rtasida ochiq API va shlyuzlar orqali amalga oshiriladigan integratsiyada "Nol ishonch" (Zero Trust) tamoyilining to‘liq ishlamasligi ma'lumotlar sizib chiqishiga texnik zamin yaratishi mumkin.

Yuqoridagi xavflarni minimallashtirish uchun IIO yagona axborot tizimida zamonaviy nazorat vositalarini joriy etish shart:

- **Ro'lga asoslangan ruxsat tizimi (RBAC - Role-Based Access Control):** Xodimning unvoni va lavozimidan kelib chiqib, u faqat o‘zining ish yurituvidagi hudud yoki jinoyat ishi doirasidagina ma'lumotlarni ko‘ra olishi kerak. Masalan, tuman profilaktika inspektori respublika bo‘yicha barcha fuqarolarning pasport ma'lumotlariga cheklanmagan tarzda kira olmasligi qat'iy texnik filtrlanishi lozim.
- **Avtomatlashtirilgan audit loglar:** Tizimga kirib ma'lumot qidirgan har bir xodimning raqamli izi (qachon, kimni, qaysi IP-manzildan qidirdi) blokcheyn texnologiyasi asosida o‘chirilmaydigan qilib saqlanishi kerak. Shubhali va noodatiy faollik (masalan, tungi soat 3:00 da minglab fuqarolar bazasini yuklab olishga urinish) datchiklari avtomatik ravishda Kiberxavfsizlik markaziga signal yuborishi zarur.

Rivojlangan davlatlar huquqni muhofaza qiluvchi organlarida ma'lumotlar himoyasi qat'iy standartlar asosida ishlaydi:

- **Yevropa Ittifoqi (GDPR va Europol direktivalari):** Yevropada Politsiya va jinoiy odil sudlov sohasida ma'lumotlarni qayta ishlash bo‘yicha maxsus Direktiva (LED - Law Enforcement Directive) amal qiladi. Unga ko‘ra, politsiya departamentlarida majburiy tartibda **Data Protection Officer (DPO – Ma'lumotlarni himoya qilish ofitseri)** lavozimi joriy qilingan. Bu ofitser tergov ishlari bilan shug‘ullanmaydi, uning yagona vazifasi xodimlarning ma'lumotlar bazasidan qonuniy foydalanayotganini audit qilishdir.
- **Amerika Qo'shma Shtatlari (AQSh):** FQB (FBI) qoshidagi Jinoyat odil sudlovi axborot xizmatlari (CJIS - Criminal Justice Information Services) bazasiga kirish uchun xodimlar murakkab ko‘p bosqichli autentifikatsiyadan (MFA) o‘tadi. Agar politsiya ofitseri tizimdan xizmatdan tashqari maqsadda (hatto o‘z qarindoshini tekshirish uchun bo‘lsa ham) foydalansa, u federal qonunlarga asosan qat'iy jinoiy javobgarlikka tortiladi va darhol ishdan olinadi.

- **Janubiy Koreya (PIPA):** Janubiy Koreya politsiyasida sun'iy intellektga asoslangan "Smart Access" monitoringi mavjud. Algoritm xodimning har kungi ish profilini tahlil qiladi. Agar ofitser o‘ziga xos bo‘lmagan toifadagi jinoyatchilar yoki o‘ta maxfiy arxiv hujjatlariga tez-tez murojaat qila boshlasa, tizim avtomatik ravishda uning hisobini vaqtincha bloklaydi hamda ichki tergov bo‘limiga xabar beradi.

"Shaxsga doir ma'lumotlar to‘g‘risida"gi Qonun talablarini Ichki ishlar organlari tizimida to‘laqonli va xavfsiz tatbiq etish maqsadida quyidagi ilmiy-amaliy takliflar ilgari suriladi:

Birinchidan, O‘zbekiston Respublikasi IIV axborot tizimlaridan qidiruv berish algoritmiga "Maqsadni majburiy asoslash" (Mandatory Justification) mexanizmini kiritish. Tizim orqali fuqaroning ma'lumotlarini olishdan oldin, xodim elektron maydonchaga o‘z ish yurituvidagi arizaning qayd raqamini, jinoyat ishi raqamini yoki qidiruv hujjatining asosini majburiy tarzda kiritishi kerak, aks holda tizim ma'lumot bermasligi lozim.

Ikkinchidan, Yevropa Ittifoqi tajribasi asosida, IIV Kiberxavfsizlik markazi hamda O‘z xavfsizligi xizmati tarkibida **"Ma'lumotlar himoyasi bo‘yicha ofitser" (DPO)** shtatini joriy etish. Ushbu xodimlar har oyda IIO bazalaridan foydalanish statistikasini raqamli auditdan o‘tkazib, xavf tug‘diruvchi xodimlarni barvaqt aniqlash bilan shug‘ullanishi kerak.

Uchinchidan, IIVning idoraviy intizomiy nizomlariga axborot xavfsizligi bo‘yicha qat'iy mezonlarni kiritish. Shaxsga doir ma'lumotlar to‘g‘risidagi qonunchilikni qasddan buzganlik, xizmat sirini tashkil etuvchi elektron axborotlarni begona shaxslarga berganlik (sotganlik) kabi holatlar uchun ichki ishlar organlaridan salbiy sabablarga ko‘ra bo‘shatish va jinoiy javobgarlikka tortish amaliyotini muqarrar qilish.

Xulosa qilib aytganda, axborot asrida fuqaroning shaxsiy ma'lumotlari uning mulkidek qadrlidir. Huquqni muhofaza qiluvchi organlar nafaqat jinoyatchilikka qarshi kurashish vositalariga, balki xalqning davlatga ishonchini belgilovchi eng xavfsiz va

shaffof axborot platformalariga ega bo‘lishi davlat taraqqiyoti va qonun ustuvorligining asosiy garovidir.

REFERENCES

1. O‘zbekiston Respublikasining Konstitutsiyasi. – Toshkent: "O‘zbekiston", 2023.
2. O‘zbekiston Respublikasining "Shaxsga doir ma'lumotlar to‘g‘risida"gi Qonuni. 02.07.2019 yildagi O‘RQ-547-son.
3. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni. 15.04.2022 yildagi O‘RQ-764-son.
4. Xudoyberdiyev A.A. "Ma’muriy ishlarni yuritish kafolatlari va huquqni qo‘llash amaliyoti". O‘quv qo‘llanma. – Toshkent: IIV Akademiyasi, 2024.
5. European Union. "General Data Protection Regulation (GDPR)" & "Law Enforcement Directive (LED)", Official Journal of the European Union, 2016.
6. Federal Bureau of Investigation (FBI). "Criminal Justice Information Services (CJIS) Security Policy". U.S. Department of Justice, 2023.
7. Park, S. "Artificial Intelligence and Privacy in South Korean Policing". Asian Journal of Criminology, 2022.