UO‘K 342.738

O‘zbekistonda raqamli xizmatlar, shaxsga doir ma’lumotlar va kiberxavfsizlik

Digital Services, Personal Data and Cybersecurity in Uzbekistan

Nazarov Abdulloh Iqboljon o‘g‘li

Toshkent davlat yuridik universiteti talabasi

Annotatsiya

Elektron davlat xizmatida fuqaro taqdim etgan ma’lumot qanday maqsadda ishlatilishi va uni kim ko‘rishi xizmatning o‘ziday muhim. Maqolada O‘zbekiston qonunchiligidagi ishlov berish asoslari, rozilik, ma’lumot subyektining huquqlari va ma’lumotlarni mamlakat hududida saqlash talablari tahlil qilinadi. Yevropa Ittifoqining GDPR reglamenti bilan qisqa qiyos beriladi. Elektron ariza va soxta bank xabari haqidagi ikki shartli misol orqali zarur bo‘lmagan ma’lumot so‘ralishi xavfi va tasdiqlash kodining aldov yo‘li bilan qo‘lga kiritilishi ko‘rib chiqiladi. Xizmat shaklidagi majburiy maydonlarni qayta ko‘rib chiqish, xodimlarning kirish vakolatlarini vazifasiga mos belgilash va soxta xabarlarni aniqlash bo‘yicha amaliy mashg‘ulotlar o‘tkazish taklif etiladi.

Kalit so‘zlar. elektron davlat xizmatlari, shaxsga doir ma’lumotlar, rozilik, ma’lumotlarni mahalliy saqlash, kiberxavfsizlik, fishing.

Abstract

This article examines the legal grounds for processing personal data in Uzbekistan, the role of consent, data subject rights and local storage requirements. It compares selected provisions with the EU General Data Protection Regulation. Two hypothetical scenarios, an online public service application and a fake bank message, illustrate the risk of asking for unnecessary data and the risk of obtaining a verification code through deception. The article proposes reviewing mandatory fields in online forms, limiting staff access according to their duties and using practical exercises to teach people how to recognise fraudulent messages.

Keywords. digital public services, personal data, consent, data localisation, cybersecurity, phishing.

Аннотация

В статье рассматриваются основания обработки персональных данных в Узбекистане, роль согласия, права субъекта данных и требования к хранению отдельных категорий данных на территории страны. Отдельные положения сопоставляются с Общим регламентом ЕС по защите данных. На двух условных примерах, электронной заявки на государственную услугу и поддельного сообщения от банка, показаны риски запроса сведений, не нужных для оказания услуги, и получения кода подтверждения путём обмана. Предлагается пересмотреть обязательные поля электронных форм, разграничить доступ сотрудников по их обязанностям и проводить практические занятия по распознаванию мошеннических сообщений.

Ключевые слова. электронные государственные услуги, персональные данные, согласие, локализация данных, кибербезопасность, фишинг.

1. Kirish

Elektron arizani to‘ldirayotgan fuqaro nega telefon raqamini kiritishi kerakligini har doim ham bilavermaydi. Raqam ariza holati haqida xabar berish uchun kerak bo‘lishi mumkin. Shu raqamdan boshqa maqsadda foydalanilsa, fuqaro dastlab bergan ma’lumot qayerga va nima uchun uzatilganini bilishga haqli. Konstitutsiyaning 31-moddasi shaxsga doir ma’lumotlar himoyasini kafolatlaydi. U insonga noto‘g‘ri ma’lumotni tuzatishni, qonunga xilof yig‘ilgan yoki huquqiy asosi qolmagan ma’lumotni esa yo‘q qilishni talab etish huquqini ham beradi [1].

Masalaning ko‘lami haqida Markaziy bank ma’lumotlari tasavvur beradi. 2024-yilda bank kartalari bilan bog‘liq firibgarlik yuzasidan Markaziy bankka 301 ta ariza va 159 ta qo‘ng‘iroq kelib tushgan [6]. Bu ikki ko‘rsatkich murojaat kanallari bo‘yicha hisoblangan. Ulardan mamlakatdagi jami firibgarlik hodisalari sonini yoki ularning qanchasi aynan fishing bilan bog‘liqligini aniqlab bo‘lmaydi.

2020-yil 5-oktabrdagi PF-6079-son Farmon bilan tasdiqlangan «Raqamli O‘zbekiston — 2030» strategiyasi elektron davlat xizmatlarini rivojlantirish uchun dasturiy asos yaratgan [4]. 2026-yil 10-martdagi PF-38-son Farmon kiberxavfsizlik strategiyasi va kiberjinoyatchilikning oldini olish masalalariga bag‘ishlangan [5]. Bu ikki hujjatni birga o‘qiganda xizmatning ommalashuvi bilan birga uni xavfsiz ishlatish va hodisaga javob berish tartibi ham oldindan rejalashtirilishi kerakligi ko‘rinadi.

2. Tadqiqot maqsadi va usullari

Maqsad elektron xizmatda ma’lumot yig‘ish, undan foydalanish va uni saqlashga doir talablarni amaliy vaziyatlar orqali tushuntirishdir. Normativ-huquqiy tahlilda Konstitutsiya, O‘RQ-547 va O‘RQ-764-son

qonunlarning tegishli moddalari koʻrib chiqildi. Qiyosiy-huquqiy usul orqali Oʻzbekiston normalari GDPRning ishlov berish maqsadi, rozilik, maʼlumot hajmi va subyekt huquqlariga oid qoidalari bilan solishtirildi. Markaziy bank eʼlon qilgan koʻrsatkichlar mavzuning amaliy ahamiyatini yoritish uchun ishlatildi. Elektron ariza va bank xabari muallif tuzgan shartli vaziyatlardir. Tadqiqotda mustaqil soʻrov yoki texnik audit oʻtkazilmadi.

3. Adabiyotlar sharhi

Mahalliy adabiyotlarda shaxsga doir maʼlumotlar himoyasi turli darajada oʻrganilgan. Rajabov raqamli muhitdagi huquqiy himoya masalalarini kiberxavfsizlik va savodxonlik bilan bogʻlaydi [8]. Xusanova masalani mehnat munosabatlari doirasida koʻrib, maʼlumotga kirish va uni uchinchi shaxsga uzatishda paydo boʻladigan xavflarga eʼtibor qaratadi [9]. Bu mulohaza davlat xizmatiga ham taalluqli. Masalan, arizaga oid ayrim maʼlumotlar murojaatni koʻrib chiquvchi xodimga kerak boʻlsa, boshqa boʻlimga ularni koʻrish vakolatini berish zarurati alohida asoslanadi. Bahodirov esa transchegaraviy axborot oqimi va milliy infratuzilma masalasini raqamli suverenitet doirasida tahlil qiladi [10]. Uning yondashuvi maʼlumot qayerda saqlanishi haqidagi savolning kengroq huquqiy sabablarini tushuntiradi.

Solove maxfiylikka doir zararlarni maʼlumot yigʻish, unga ishlov berish va uni tarqatish kabi bosqichlar boʻyicha ajratadi [11]. Nissenbaum uchun maʼlumotning kimga va qaysi sharoitda berilgani muhim [12]. Shu nuqtai nazardan, ariza holati haqida xabar yuborish uchun olingan raqamdan reklama xabarlarini tarqatishda foydalanish maʼlumotning dastlabki vazifasini oʻzgartiradi. Acquisti, Brandimarte va Loewenstein foydalanuvchilar maʼlumot ulashishning oqibatini oldindan toʻliq baholay olmasligini koʻrsatadi [13]. Acquisti, Taylor va Wagman esa shaxsiy maʼlumot ulashishning foyda va xarajatlarini iqtisodiy adabiyotlar asosida koʻrib chiqadi [14]. Mazkur ishlar xizmat shaklida rozilik tugmasi bilan birga tushunarli izoh ham boʻlishi kerakligini asoslashga yordam beradi. Cavoukian, Taylor va Abramsning maxfiylikni loyihalash bosqichidan hisobga olish haqidagi yondashuvi bu fikrni tashkilot masʼuliyati bilan bogʻlaydi [15].

Dhamija, Tygar va Hearst tadqiqotida foydalanuvchilar qalbaki sahifani baholashda uning tashqi koʻrinishiga ham tayanishi koʻrsatilgan [16]. Sheng va hammualliflar fishingga moyillik hamda oʻquv aralashuvlarining taʼsirini tajriba orqali oʻrgangan [17]. Kumaraguru va hammualliflar esa soxta xabarni tanib olish boʻyicha oʻqitishni odatiy ish muhitiga yaqin sharoitda sinagan [18]. Ushbu ishlar asosida mashgʻulotda talabalardan xavfsizlik qoidasini yoddan aytish bilan birga, xabarni qaysi rasmiy kanal orqali tekshirishini amalda koʻrsatish ham soʻralishi mumkin.

4. Huquqiy tahlil

Ishlov berishning asosi, maqsadi va fuqaroning huquqlari

O‘RQ-547-son Qonunning 18-moddasida ishlov berishga yo‘l qo‘yiladigan asoslar belgilangan. Subyektning roziligi shulardan biri. Masalan, qonunchilik operatorga ma’lum vazifani yuklagan bo‘lsa va bu vazifani bajarish uchun ma’lumotga ishlov berish zarur bo‘lsa, ishlov berish qonuniy majburiyatga asoslanishi mumkin. Rozilik asos qilib olinganida 21-modda uning olinganini tasdiqlash mumkin bo‘lgan shaklda berish va chaqirib olish tartibini belgilaydi [2].

19-modda ishlov berish maqsadini ma’lumot yig‘ish paytida bildirilgan maqsad bilan bog‘laydi. Maqsad o‘zgarsa, shu modda yangi maqsad bo‘yicha rozilik olishni talab qiladi. 31-modda esa operatorga o‘z vazifasi uchun zarur va yetarli ma’lumotlar tarkibini tasdiqlash majburiyatini yuklaydi [2]. Masalan, faqat ariza holatini bildirishga xizmat qiladigan telefon raqamini majburiy maydonga aylantirishdan oldin xabarni shaxsiy kabinetga yuborish orqali ham shu maqsadga erishish mumkinligi ko‘rib chiqiladi.

22 va 30-moddalar fuqaroga o‘z ma’lumotlariga ishlov berilishi haqida axborot olish imkonini beradi. 30-moddaga muvofiq fuqaro huquqlarini himoya qilish uchun vakolatli organga yoki sudga murojaat qilishi mumkin. 31-modda operatorning noto‘g‘ri ma’lumotni tuzatish va qonunda ko‘rsatilgan hollarda ishlovni vaqtincha to‘xtatish yoki ma’lumotni yo‘q qilishga oid majburiyatlarini belgilaydi [2]. Elektron xizmatda bu huquqlardan foydalanish uchun murojaat shakli yoki aloqa manzili ariza sahifasida ko‘rinib turishi maqsadga muvofiq.

Ma’lumotlarni O‘zbekiston hududida saqlash

O‘RQ-547-son Qonunning 27¹-moddasi 2026-yil 26-martdagi O‘RQ-1125-son Qonun bilan yangi tahrirda bayon qilingan. Unga ko‘ra, biometrik va genetik ma’lumotlar, shuningdek, O‘zbekistonda faoliyat yurituvchi telekommunikatsiya operatorlaridagi ularning xizmatlaridan foydalanuvchi jismoniy shaxslarning ma’lumotlari mamlakat hududida saqlanishi shart. 20-modda shu toifadagi bazalarni davlat reyestrida ro‘yxatdan o‘tkazishni talab qiladi [2].

Qolgan ma’lumotlarni chet elda saqlash va ularga ishlov berish uchun 27¹-moddadagi shartlardan biri bajarilishi kerak. Bular tegishli davlatning teng himoya darajasiga ega deb tan olinishi, operatorning vakolatli organ talablariga mos standart shartnomaviy shartlar yoki majburiy korporativ qoidalarni qabul qilib, ularga rioya qilishi yoxud vakolatli organ tasdiqlagan ro‘yxatdagi xalqaro standartlarga rioya etishini qamrab oladi [2]. Masalan, elektron arizada telefon raqami so‘ralishi o‘z-o‘zidan ushbu xizmatni telekommunikatsiya operatoriga aylantirmaydi. Saqlash talabini

aniqlash uchun ma’lumotning turi, uni kim saqlayotgani va ishlov berish sharoiti tekshiriladi.

Kiberxavfsizlik talablari

O‘RQ-764-son Qonunning 14-moddasi davlat organlari va tashkilotlarining kiberxavfsizlik bo‘yicha huquq va majburiyatlarini belgilaydi. 15-modda davlat organlari va tashkilotlari hamda muhim axborot infratuzilmasi obyektlari tizimlarida zaxira nusxalarini yaratish va kamida oxirgi uch oylik nusxalarni saqlashni nazarda tutadi. 16-modda kiberxavfsizlik subyektlariga ma’lumotlarning noqonuniy tarqalishi yoki tizimga ruxsatsiz kirishning oldini olish, hodisa aniqlanganda choralar ko‘rish va vakolatli organni xabardor qilish majburiyatlarini yuklaydi [3]. Xizmatda bu qoidalar kirish vakolatlarini xodimning vazifasiga mos belgilash, tizimni zaxira nusxadan tiklashni sinab ko‘rish va hodisa haqida kim xabar berishini oldindan aniqlash orqali amalga tatbiq etiladi.

GDPR bilan qisqa qiyos

GDPRning 5-moddasi ma’lumotlarni aniq maqsad uchun va shu maqsadga yetarli hajmda yig‘ishni talab qiladi. 6-modda ishlov berishning qonuniy asoslarini, 7-modda rozilik shartlarini belgilaydi. 15–17-moddalarda ma’lumotdan xabardor bo‘lish va unga kirish, uni tuzatish hamda belgilangan hollarda o‘chirish huquqlari yoritilgan [7]. O‘zbekiston qonunchiligida shunga yaqin talablar O‘RQ-547-son Qonunning 18, 19, 21, 22, 30 va 31-moddalarida ifodalangan. Saqlash masalasida esa O‘zbekiston qonuni ayrim toifalar uchun mamlakat ichida saqlashni talab qiladi. GDPRning V bobi uchinchi mamlakatga uzatish shartlari va kafolatlarini belgilaydi [2, 7].

5. Shartli vaziyatlar va muhokama

Elektron arizada telefon raqami

Fuqaro ma’lumotnoma olish uchun elektron ariza topshiradi. Natija shaxsiy kabinetga yuboriladi, lekin shakl telefon raqamini ham majburiy so‘raydi. Agar SMS faqat qo‘shimcha qulaylik yaratish uchun ishlatilsa, maydonni ixtiyoriy qilish mumkin. Xizmat qoidalariga ko‘ra raqam haqiqatan zarur bo‘lsa, shaklda uning vazifasi tushuntiriladi. Raqamni ko‘rish vakolati shu ishga aloqador xodimlarga beriladi. Fuqaro raqamini yangilash yoki xatoni bildirish yo‘lini ham shu sahifadan topa olishi kerak [2].

Bank nomidan yuborilgan soxta xabar

Talabaga hisob bloklanishi haqida xabar keladi. Xabarda havolani ochib, tasdiqlash kodini kiritish so‘raladi. Talaba havolani ishlatmasdan bankning rasmiy ilovasini o‘zi ochib, bildirishnomalarni tekshirishi yoki bankning rasmiy aloqa raqamiga murojaat qilishi mumkin. Mashg‘ulotda

shu qarorning sababi ham muhokama qilinadi. Xabardagi shoshiltirish va kod talab qilinishi uni mustaqil kanal orqali tekshirish uchun yetarli sababdir. Tashkilot uchun esa bunday xabarlar haqida mijoz qayerga tezkor murojaat qilishi mumkinligini aniq koʻrsatish muhim [16–18].

Birinchi vaziyatda xavf xizmat shakli tuzilayotganda paydo boʻladi. Ikkinchisida esa foydalanuvchi tashqaridan kelgan xabarni baholashi kerak. Shu sabab elektron arizada soʻraladigan maʼlumotlar tarkibini tekshirish va fuqaroga shubhali xabarni tekshirishning sodda yoʻlini koʻrsatish bir-birini toʻldiradi. Keltirilgan statistika ushbu choralarning samaradorligini oʻlchashga asos bermaydi. Buning uchun xizmatlar kesimida alohida kuzatuv yoki tajriba zarur boʻladi.

6. Xulosa va takliflar

Elektron davlat xizmatini qayta koʻrib chiqishda avvalo har bir majburiy maydon boʻyicha maʼlumot nima uchun kerakligi, unga ishlov berishning huquqiy asosi, uni kim koʻrishi va qancha vaqt saqlanishi aniqlanishi lozim. Fuqaroga beriladigan izohni bevosita ariza shakliga joylashtirish, tuzatish boʻyicha murojaatni esa shu sahifadan yuborish imkonini yaratish taklif etiladi.

Tashkilot ichida xodimning vazifasi oʻzgarganda maʼlumotga kirish vakolati ham qayta koʻrib chiqilishi kerak. Kiberxavfsizlik hodisasi yuz bersa, uni qayd etish, vakolatli organga xabar berish va xizmatni tiklash uchun masʼul shaxslar oldindan belgilanishi maqsadga muvofiq. Taʼlim muassasalarida esa talabalarga ikkita namunaviy bank xabarini solishtirish va shubhali xabarni rasmiy kanal orqali tekshirishni mashq qildirish mumkin.

Foydalanilgan manbalar

[1] Oʻzbekiston Respublikasi Konstitutsiyasi. 2023. 31-modda. Manba

[2] «Shaxsga doir maʼlumotlar toʻgʻrisida»gi Qonun. 02.07.2019, OʻRQ-547. Amaldagi tahrir. Manba

[3] «Kiberxavfsizlik toʻgʻrisida»gi Qonun. 15.04.2022, OʻRQ-764. Manba

[4] Prezidentning «Raqamli Oʻzbekiston — 2030» strategiyasini tasdiqlash toʻgʻrisidagi Farmoni. 05.10.2020, PF-6079. Manba

[5] Prezidentning Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish toʻgʻrisidagi Farmoni. 10.03.2026, PF-38. Manba

[6] Oʻzbekiston Respublikasi Markaziy banki. CERT-CBU axborot toʻplami. 2024-yilda bank kartalari bilan bogʻliq firibgarlik yuzasidan murojaatlar statistikasi. Manba

[7] European Parliament and Council. Regulation (EU) 2016/679 (GDPR). 2016. Manba

[8] Rajabov, O. Raqamli muhitda shaxsga doir ma’lumotlarni huquqiy himoya qilishning dolzarb masalalari. Tsentralnoaziatskiy jurnal akademicheskix issledovaniy, 3(11), 2025. doi.org/10.5281/zenodo.17549298

[9] Xusanova, S. Xodimlarning shaxsga doir ma’lumotlarini himoya qilishning ayrim xususiyatlari. Siyosatshunoslik, huquq va xalqaro munosabatlar jurnali, 4(6), 2025. Manba

[10] Bahodirov, Sh. Raqamli suverenitet tushunchasining nazariy-huquqiy mohiyati. Zamonaviy dunyoda ilm-fan va texnologiya, 5(16), 37–41, 2026. doi.org/10.70413/zdift-v05-i16-s49856

[11] Solove, D. J. A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3), 477–564, 2006. Manba

[12] Nissenbaum, H. Respecting Context to Protect Privacy: Why Meaning Matters. Science and Engineering Ethics, 24, 831–852, 2018. doi.org/10.1007/s11948-015-9674-9

[13] Acquisti, A., Brandimarte, L., Loewenstein, G. Privacy and Human Behavior in the Age of Information. Science, 347(6221), 509–514, 2015. doi.org/10.1126/science.aaa1465

[14] Acquisti, A., Taylor, C., Wagman, L. The Economics of Privacy. Journal of Economic Literature, 54(2), 442–492, 2016. doi.org/10.1257/jel.54.2.442

[15] Cavoukian, A., Taylor, S., Abrams, M. E. Privacy by Design: Essential for Organizational Accountability and Strong Business Practices. Identity in the Information Society, 3, 405–413, 2010. doi.org/10.1007/s12394-010-0053-z

[16] Dhamija, R., Tygar, J. D., Hearst, M. Why Phishing Works. CHI ’06, 581–590, 2006. doi.org/10.1145/1124772.1124861

[17] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., Downs, J. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. CHI ’10, 373–382, 2010. doi.org/10.1145/1753326.1753383

[18] Kumaraguru, P. va boshq. School of Phish: A Real-World Evaluation of Anti-Phishing Training. SOUPS ’09, 2009. doi.org/10.1145/1572532.1572536