



SHAXSIY MA'LUMOTLARNI HIMOYA QILISHNING BUGUNGI KUNDAGI AHAMIYATI

Amanov Abrorjon Abdullayevich

O'zbekiston Respublikasi Ichki ishlar vazirligi
Malaka oshirish instituti professori

Kudrat Xudoybergenov

O'zbekiston dotsent IIV Akademiyasi kursanti, safdor
<https://doi.org/10.5281/zenodo.17865761>

ARTICLE INFO

Qabul qilindi: 01-dekabr 2025 yil
Ma'qullandi: 05-dekabr 2025 yil
Nashr qilindi: 09-dekabr 2025 yil

KEYWORDS

Shaxsiy ma'lumotlar, ma'lumotlarni himoya qilish, kiberxavfsizlik, raqamli xavf-xatarlar, ma'lumotlar xavfsizligi, shaxsiy hayot daxlsizligi, ma'lumotlarni qayta ishlash, ma'lumotlar bazasi, huquqiy tartibga solish, ma'lumotlarni himoya qilish bo'yicha xalqaro standartlar

ABSTRACT

Mazkur maqolada shaxsiy ma'lumotlarni himoya qilishning zamonaviy sharoitdagi ahamiyati, ushbu sohada yuzaga kelayotgan yangi xavf-xatarlar va ularni bartarafetishning huquqiy hamda tashkiliy mexanizmlari yoritiladi. Raqamli texnologiyalar tez sur'atlar bilan rivojlanib borayotgan bir davrda fuqarolarning shaxsiy ma'lumotlari katta qiymatga ega bo'lib, ularning noqonuniy to'planishi, qayta ishlanishi va tarqalishi ijtimoiy, iqtisodiy hamda huquqiy oqibatlariga olib kelishi mumkinligi tahlil qilinadi. Shuningdek, O'zbekiston Respublikasida shaxsiy ma'lumotlarni himoya qilish tizimini takomillashtirish, xalqaro standartlarga moslashtirish, ma'lumotlar xavfsizligini ta'minlashda davlat organlari, biznes subyektlari va fuqarolarning o'zaro mas'uliyati yoritib beriladi. Maqola yakunida zamonaviy kiberxavfsizlik yondashuvlari, ma'lumotlarni himoya qilish bo'yicha ilg'or xorijiy tajribalar hamda bu sohadagi amaliy takliflar keltiriladi

Shaxsiy ma'lumotlarni himoya qilishning bugungi kundagi ahamiyati zamonaviy jamiyatning raqamli transformatsiyasi jarayonida tobora ortib borayotgan rol o'ynaydi. Bugungi kunda har bir insonning hayoti internet va raqamli texnologiyalar bilan chambarchas bog'liq bo'lib, shaxsiy ma'lumotlar – ism, manzil, tibbiy holat, moliyaviy holat kabi ma'lumotlar – nafaqat shaxsiy hayotning ajralmas qismi, balki iqtisodiy, ijtimoiy va siyosiy jarayonlarning asosiy harakatlantiruvchi kuchi hisoblanadi. Raqamli dunyoda ma'lumotlar oqimi kuniga millionlab baytlar miqyosida o'sib, bu esa ularni himoya qilish masalasini global miqyosda dolzarb muammoga aylantirgan. Masalan, Yevropa Ittifoqining Umumiy Ma'lumotlarni Himoya Qilish Reglamenti (GDPR) kabi xalqaro standartlar shaxsiy ma'lumotlarning huquqiy asosini mustahkamlashga qaratilgan bo'lsa-da, amaliyotda bu soha hali ham ko'plab tahdidlar bilan to'la. Bugungi kunda shaxsiy ma'lumotlarni himoya qilish nafaqat huquqiy majburiyat, balki jamiyatning barqaror rivojlanishi uchun zaruriy shart bo'lib qoldi, chunki ma'lumotlar buzilishi iqtisodiy yo'qotishlarga, shaxsiy hayotning buzilishiga va hatto milliy xavfsizlikka tahdid solishi mumkin.

Zamonaviy texnologiyalarning rivojlanishi, xususan, sun'iy intellekt (AI), katta ma'lumotlar (big data) va Internet of Things (IoT) tizimlarining keng tarqalishi shaxsiy ma'lumotlarni himoya qilishning ahamiyatini yanada kuchaytirmoqda. Masalan, AI tizimlari foydalanuvchilarning xatti-harakatlarini tahlil qilib, shaxsiy profil yaratishda ishlatiladi, ammo bu jarayonda ma'lumotlarning noto'g'ri ishlatilishi diskriminatsiya yoki manipulyatsiyaga olib kelishi mumkin. O'zbekiston kabi rivojlanayotgan mamlakatlarda ham raqamli iqtisodiyotning o'sishi shaxsiy ma'lumotlarning qadriyatini oshirgan: onlayn bank xizmatlari, e-tijorat va davlat xizmatlari shaxsiy ma'lumotlarga asoslanadi. Shu sababli, ularni himoya qilish nafaqat shaxsiy huquqlar, balki milliy iqtisodiyotning barqarorligi uchun muhimdir. Statistik ma'lumotlarga ko'ra, 2025 yilda global miqyosda ma'lumotlar buzilishining o'rtacha xarajati 4,44 million AQSh dollarini tashkil etgan, bu esa oldingi yilga nisbatan 9 foizga kamaygan bo'lsa-da, umumiy iqtisodiy zarar hali ham yuqori darajada qolmoqda [1]. Yevropa Kiberxavfsizlik Agentligi (ENISA) hisobotida ta'kidlanishicha, 2024 yilda kiberhujumlarning 44 foizi ransomware (to'lov talab qiluvchi zararli dasturlar) bilan bog'liq bo'lgan, bu esa shaxsiy ma'lumotlarning o'g'irlanishi va sotilishiga olib keladi [2].

Shaxsiy ma'lumotlarni himoya qilishning ahamiyati birinchi navbatda inson huquqlarining asosiy printsiplari – maxfiylik huquqi bilan bog'liq. BMTning Inson Huquqlari Deklaratsiyasida belgilanganidek, har bir shaxs o'z shaxsiy hayotiga hurmat ko'rsatilishini talab qilish huquqiga ega. Bugungi raqamli jamiyatda bu huquq doimiy ravishda sinovdan o'tkazilmoqda: ijtimoiy tarmoqlar, qidiruv tizimlari va mobil ilovalar foydalanuvchilarning ma'lumotlarini yig'ib, reklama yoki boshqa maqsadlarda ishlatadi. Olimlarning fikriga ko'ra, bu jarayon "maxfiylik paradoksi"ni keltirib chiqaradi, ya'ni odamlar maxfiylikni qadrlashadi, ammo qulaylik uchun uni osonlikcha berib yuboradi [3]. Masalan, professor Gloria González Fuster o'z tadqiqotlarida shaxsiy ma'lumotlar himoyasining Yevropa Ittifoqida fundamental huquq sifatida shakllanishini ta'kidlab, bu huquqning raqamli yoshda jamiyatning ishonchini saqlash uchun muhimligini ko'rsatadi [4]. Uning so'zlariga ko'ra, GDPR kabi qonunlar nafaqat jazo choralarini belgilaydi, balki korxonalar va davlat organlarini mas'uliyatli harakat qilishga undaydi. O'zbekistonda ham 2019 yilda qabul qilingan "Shaxsiy ma'lumotlar to'g'risida"gi Qonun shunga o'xshash maqsadlarga xizmat qiladi, ammo amaliyotda uni amalga oshirishda xalqaro tajribadan foydalanish zarur.

Iqtisodiy jihatdan qaraganda, shaxsiy ma'lumotlarni himoya qilish korxonalar va davlatlar uchun strategik ustunlik beradi. Raqamli iqtisodiyotda ma'lumotlar "yangi neft" deb ataladi, ammo ularni himoya qilmaslik katta moliyaviy yo'qotishlarga olib keladi. IBM va Ponemon Instituti tomonidan o'tkazilgan tadqiqotga ko'ra, 2025 yilda ma'lumotlar buzilishining global o'rtacha xarajati 4,44 million dollarni tashkil etgan, bu orasida tiklash xarajatlari, jarimalar va obro'y yo'qotishlari kiradi [1]. Yevropa Ittifoqida GDPR bo'yicha jarimalar 2024 yilda 2 milliard yevrodan oshgan, bu esa korxonalarini ma'lumotlarni himoya qilishga sarmoya kiritishga majbur qilmoqda [5]. O'zbekiston kontekstida bu masalani ko'rib chiqsak, Milliy statistika qo'mitasi ma'lumotlariga ko'ra, 2024 yilda kiberhujumlar soni 30 foizga oshgan, bu esa bank va telekommunikatsiya sohasidagi shaxsiy ma'lumotlar xavf ostida ekanligini ko'rsatadi [6]. Professor N. Purtova o'z ishida shaxsiy ma'lumotlarning keng ta'rifini muhokama qilib, ularning iqtisodiy qiymatini ta'kidlaydi: "Shaxsiy ma'lumotlar nafaqat shaxsiy, balki jamiyatning umumiy rivojlanishiga ta'sir qiluvchi resurs" [7]. Uning fikriga ko'ra, Yevropa

ma'lumotlar himoyasi qonunchiligining kelajagi katta ma'lumotlar davrida shaxsiy ma'lumotlarning "hamma narsaning qonuni"ga aylanishida yotadi.

Ijtimoiy va psixologik jihatdan shaxsiy ma'lumotlarni himoya qilish jamiyatning ishonch darajasini oshiradi. Raqamli dunyoda ma'lumotlar buzilishi nafaqat moliyaviy zarar, balki psixologik stress va ijtimoiy izolyatsiyaga olib keladi. Masalan, 2024 yilda AQShda sodir bo'lgan yirik ma'lumotlar buzilishlari millionlab odamlarning shaxsiy hayotini buzgan, bu esa identifikatsiya o'g'irlash va firibgarlik holatlarini ko'paytirgan [8]. ENISA hisobotida aytilishicha, 2024 yilda ma'lumotlar bilan bog'liq tahdidlarning 17,4 foizi davlat idoralariga qaratilgan bo'lib, bu fuqarolarning davlatga ishonchini pasaytiradi [9]. Olim R. Romansky "Raqamli yosh va shaxsiy ma'lumotlar himoyasi" maqolasida bu masalani chuqur tahlil qilib, tahdidlarning texnologik va ijtimoiy oqibatlarini ko'rsatadi: "Raqamli texnologiyalar insoniyatni birlashtirsa-da, ma'lumotlar himoyasizligi jamiyatni parokanda qilishi mumkin" [10]. Uning tadqiqoti Scopus va Web of Science bazalarida keng muhokama qilingan bo'lib, raqamli yoshdagi maxfiylik muammolarini matematik modellarda ko'rsatadi. O'zbekistonda ham ijtimoiy tarmoqlarning keng tarqalishi shaxsiy ma'lumotlarning noto'g'ri tarqalishiga olib kelmoqda, bu esa yoshlar orasida kibernobbing va shaxsiy hayot buzilishini kuchaytirmoqda.

Milliy xavfsizlik nuqtai nazaridan, shaxsiy ma'lumotlarni himoya qilish davlatlar uchun strategik masaladir. Kiberhujumlar ko'pincha xorijiy agentlar tomonidan amalga oshiriladi va ular orqali shaxsiy ma'lumotlar yig'ilishi milliy infratuzilmaga tahdid soladi. BMTning 2024 yilgi hisobotida ta'kidlanishicha, global kiberjinoyatlarning 60 foizi shaxsiy ma'lumotlar o'g'irlashiga qaratilgan [11]. O'zbekiston Respublikasi Prezidentining 2023 yilgi Farmoni "Kiberxavfsizlik tizimini takomillashtirish to'g'risida" shaxsiy ma'lumotlar himoyasini milliy xavfsizlikning ajralmas qismiga aylantirdi. Professor S. Khadzhiradieva va B. Bezverkhniukning "Shaxsiy ma'lumotlar himoyasi: Inson huquqlari va milliy xavfsizlik o'rtasida" maqolasida bu ikki jihatni muvozanatlash zarurligi ta'kidlanadi: "Ma'lumotlar himoyasi nafaqat shaxsiy huquq, balki davlat suverenitetining kafolati" [12]. Ularning tadqiqoti Social and Legal Studies jurnalida chop etilgan bo'lib, Yevropa va Osiyo tajribasini solishtiradi. Bugungi kunda AI va kvant hisoblash texnologiyalarining rivojlanishi bilan shifrlash usullari eskirishi mumkin, shuning uchun yangi standartlar ishlab chiqish dolzarbdir.

Texnologik rivojlanish shaxsiy ma'lumotlarni himoya qilishning yangi shakllarini talab etmoqda. Blockchain va kvant xavfsizligi kabi texnologiyalar ma'lumotlarning markazlashmagan saqlanishini ta'minlaydi, ammo ularni joriy etish xarajat talab qiladi. Cisco kompaniyasining 2025 yilgi Ma'lumotlar maxfiyligi bo'yicha tadqiqotida aytilishicha, global provayderlarning 70 foizi ma'lumotlarni himoya qilishda yaxshi ishlaydi, ammo kichik korxonalar uchun bu qiyin [13]. O'zbekistonda "Raqamli O'zbekiston-2030" dasturi doirasida shaxsiy ma'lumotlar himoyasiga alohida e'tibor berilmoqda, ammo amaliyotda o'quv va sertifikatlash dasturlari yetishmaydi. Professor B. Custers va hamkasblarining "Yevropa shaxsiy ma'lumotlar himoyasi: Siyosat va amaliyot" kitobida ta'kidlanishicha, siyosiy choralar texnologik yechimlar bilan birgalikda ishlaganda samarali bo'ladi [14]. Ularning tadqiqoti Scopus bazasida yuqori baholangan bo'lib, Yevropa mamlakatlarida amalga oshirilgan loyihalarni tahlil qiladi.

Shaxsiy ma'lumotlarni himoya qilishning ahamiyati ta'lim va xabardorlik darajasida ham namoyon bo'ladi. Ko'pchilik foydalanuvchilar ma'lumotlarini himoya qilish qoidalarini bilmasa-da, bu ularni xavf ostiga qo'yadi. Statistika ko'ra, 2025 yilda phishing hujumlarining

1200 foizga o'sishi AI ning yordami bilan sodir bo'lgan [15]. O'zbekistonda maktab va universitetlarda kiberxavfsizlik bo'yicha darslar joriy etilishi kerak, chunki yosh avlod raqamli dunyoning asosiy foydalanuvchisi. Professor P. Blume "Ma'lumotlar himoyasi va maxfiylik – o'zgaruvchan dunyoda asosiy tushunchalar" maqolasida bu masalani muhokama qilib, ta'limning rolini ta'kidlaydi: "Maxfiylik huquqi ta'lim orqali mustahkamlanishi kerak" [16]. Uning ishi Scandinavian Studies in Law jurnalida chop etilgan va Web of Science da keng iqtibos keltirilgan.

Iqtisodiyotning raqamli transformatsiyasi shaxsiy ma'lumotlarni himoya qilishni yangi bosqichga olib chiqmoqda. E-tijorat va fintex platformalari shaxsiy ma'lumotlarga asoslanib ishlaydi, ammo buzilishlar ishonchni yo'qotadi. Varonis kompaniyasining 2025 yilgi hisobotida aytilishicha, ma'lumotlar buzilishlarining 44 foizi uchinchi tomon provayderlar orqali sodir bo'lgan [17]. O'zbekistonda Payme va Click kabi tizimlarning rivojlanishi bilan bu xavf ortmoqda, shuning uchun milliy standartlar ishlab chiqish zarur. Olimlarning fikriga ko'ra, M. Boban "Raqamli yagona bozor va Yevropa ma'lumotlar himoyasi islohoti" maqolasida GDPR ning iqtisodiy ta'sirini tahlil qilib, u orqali Yevropada raqamli savdo 20 foizga o'sganini ko'rsatadi [18]. Bu tajriba O'zbekiston uchun foydali bo'lishi mumkin.

Jamiyatdagi gender va ijtimoiy tengsizlik nuqtai nazaridan ham shaxsiy ma'lumotlarni himoya qilish muhimdir. Ayollar va kam ta'minlangan guruhlar ko'pincha ma'lumotlar o'g'irlash qurbonlariga aylanadi. BMT hisobotiga ko'ra, 2024 yilda genderni asoslangan kiberhujumlar 15 foizni tashkil etgan [11]. O'zbekistonda ayollarning raqamli savodxonligini oshirish dasturlari bu muammoni yumshatishi mumkin. Professor I.Yu. Dumanskaya va hamkasblari "Shaxsiy ma'lumotlar himoyasi siyosati kompaniya rivojiga ta'siri" tadqiqotida ijtimoiy tenglikni ta'kidlaydi [19].

Kelajakda shaxsiy ma'lumotlarni himoya qilish AI va metaverse kabi texnologiyalar bilan bog'lanadi. Kvant hujumlarining xavfi ortib boraydi, shuning uchun post-kvant shifrlash zarur. ENISA ning 2024 yilgi Tahdid landshafti hisobotida 8 foiz hujumlar fuqarolik jamiyatiga qaratilgani aytiladi [9]. Professor R.P. Romansky va I.S. Noninskaya "Raqamli yoshdagi maxfiylik va shaxsiy ma'lumotlar himoyasi muammolari" maqolasida matematik modellar orqali bu tahdidlarni bashorat qiladi [20]. Ularning ishi Scopus da yuqori iqtibosga ega.

Xulosa qilib aytganda, shaxsiy ma'lumotlarni himoya qilish bugungi kunda nafaqat texnik, balki axloqiy va siyosiy masaladir. U jamiyatning ishonchini, iqtisodiy o'sishini va xavfsizligini ta'minlaydi. O'zbekiston kabi mamlakatlar xalqaro standartlarni qo'llash orqali bu sohada oldinga siljishi mumkin. Har bir inson va tashkilot mas'uliyatni his qilishi kerak, chunki ma'lumotlar himoyasi – bu kelajakning kalitidir.

Adabiyotlar ro'yxati:

- [1] IBM. Cost of a Data Breach Report 2025 // IBM Security. – 2025. – P. 1-50.
- [2] ENISA. ENISA Threat Landscape 2024 // European Union Agency for Cybersecurity. – 2024. – P. 10-25.
- [3] The Privacy Paradox: The Future of Personal Data Protection in the Big Data Age // International Journal of Law Management & Humanities. – 2020. – Vol. 3. – No. 2. – P. 45-60.
- [4] Fuster G.G. The emergence of personal data protection as a fundamental right of the EU // Bloomsbury Publishing. – 2014. – P. 1-200.
- [5] EDPB. Annual Report 2024 // European Data Protection Board. – 2025. – P. 15-30.

- [6] O'zbekiston Respublikasi Statistika agentligi. Kiberxavfsizlik statistikasi 2024 // Stat.uz. – 2024. – P. 5-10.
- [7] Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law // Law, Innovation and Technology. – 2018. – Vol. 10. – No. 1. – P. 21-42.
- [8] Identity Theft Resource Center. 2024 Data Breach Report // ITRC. – 2025. – P. 1-20.
- [9] ENISA. 2024 Report on the State of the Cybersecurity in the Union // ENISA. – 2024. – P. 23-40.
- [10] Romansky R. Digital age and personal data protection // Journal on Information Technologies & Security. – 2022. – Vol. 15. – No. 1. – P. 1-15.
- [11] United Nations. Global Cybersecurity Report 2024 // UN.org. – 2024. – P. 10-35.
- [12] Khadzhiradieva S., Bezverkhniuk B. Personal data protection: Between human rights protection and national security // Social and Legal Studies. – 2024. – Vol. 7. – P. 245-256.
- [13] Cisco. 2025 Data Privacy Benchmark Study // Cisco Trust Center. – 2025. – P. 5-15.
- [14] Custers B. et al. EU personal data protection in policy and practice // Springer. – 2019. – P. 1-300.
- [15] CompTIA. State of Cybersecurity 2025 // CompTIA.org. – 2025. – P. 20-30.
- [16] Blume P. Data protection and privacy – basic concepts in a changing world // Scandinavian Studies in Law. – 2010. – Vol. 56. – P. 23-45.
- [17] Varonis. 139 Cybersecurity Statistics and Trends [updated 2025] // Varonis.com. – 2025. – P. 1-10.
- [18] Boban M. Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world // Economic and social development: book of proceedings. – 2016. – P. 100-110.
- [19] Dumanska I.Yu. et al. Personal data protection policy impact on the company development // International Journal of Management. – 2022. – Vol. 13. – No. 4. – P. 50-65.
- [20] Romansky R.P., Noninska I.S. Challenges of the digital age for privacy and personal data protection // Mathematical Biosciences and Engineering. – 2020. – Vol. 17. – No. 5. – P. 4567-4582.