LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

MA'LUMOTLAR SIZIB CHIQISHI UCHUN HUQUQIY JAVOBGARLIK: O'ZBEKISTON VA XORIJIY DAVLATLAR TAJRIBASI

Tojiyev Bekjon Isomiddin o'g'li,
Toshkent davlat yuridik universiteti
Ommaviy huquq fakulteti 2-kurs talabasi
bekjontojiyev1607@gmail.com

Annotatsiya: *Ushbu tadqiqot ma'lumotlar sizib chiqishi uchun huquqiy javobgarlik masalasiga bag'ishlangan. Unga ko'ra axborotlashgan jamiyat sharoitida shaxsga doir ma'lumotlar xavfsizligini ta'minlash va ularning sizib chiqishi (data breach) holatlarida huquqiy javobgarlikni belgilash masalalari tadqiq etiladi. Tadqiqot davomida O'zbekiston Respublikasining milliy qonunchiligi hamda Yevropa Ittifoqining GDPR (Ma'lumotlarni himoya qilish umumiy reglamenti) normalari hamda Amerika hamda Osiyo tajribalari asosida qiyosiy-huquqiy tahlil qilindi. Maqolada ma'lumotlar sizib chiqishi (data breach) tushunchasining huquqiy tabiati ochib berilgan hamda subyektlarning fuqarolik, ma'muriy va jinoiy javobgarligi chegaralari o'rganilgan. Olib borilgan tahlillar natijasida, milliy qonunchilikda ma'lumotlar sizib chiqqanligi haqida xabardor qilish mexanizmlari va zararni qoplash tizimidagi mavjud bo'shliqlar aniqlandi. Maqola so'ngida kiber-makonda shaxsiy ma'lumotlar daxlsizligini kafolatlash hamda javobgarlik choralarini takomillashtirish bo'yicha ilmiy-amaliy takliflar ilgari surilgan.*

Kalit so'zlar: *shaxsga doir ma'lumotlar, data breach, personal data ma'lumotlar sizib chiqishi, huquqiy javobgarlik, GDPR, CCPA, kiber huquq, raqamli xavfsizlik, ma'muriy jarima, jinoiy javobgarlik, fuqarolik javobgarligi, zararni qoplash, ma'naviy zarar, kiberjinoyatchilik, axborot tizimlari, kiber-tahdidlar, raqamli xavfsizlik*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL

Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

LEGAL LIABILITY FOR DATA BREACHS

Tojiyev Bekjon Isomiddin o‘g‘li,

2nd-year student at the Faculty of Public Law,

Tashkent State University of Law

bekjontojiyev1607@gmail.com

Abstract: *This research is dedicated to the issue of legal liability for data leaks. It examines the challenges of ensuring the security of personal data in the context of an information-driven society and the establishment of legal responsibility in cases of data breaches. The study conducts a comparative legal analysis based on the national legislation of the Republic of Uzbekistan, the European Union's General Data Protection Regulation (GDPR) standards, as well as American and Asian experiences. The article clarifies the legal nature of the "data breach" concept and investigates the boundaries of civil, administrative, and criminal liability for subjects involved. As a result of the analysis, existing gaps in national legislation regarding data breach notification mechanisms and the damage compensation system were identified. The article concludes by proposing scientific and practical recommendations for guaranteeing the inviolability of personal data in cyberspace and improving liability measures.*

Keywords: *personal data, data breach, legal liability, GDPR, CCPA, cyber law, digital security, administrative fine, criminal liability, civil liability, compensation for damages, moral damage, cybercrime, information systems, cyber threats, digital safety.*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА УТЕЧКУ ДАННЫХ

Тожиев Бекжон Исомиддинович,
Студент 2-го курса факультета публичного права
Ташкентский государственный юридический университет
bekjontojiyev1607@gmail.com

Аннотация: *Данное исследование посвящено вопросам юридической ответственности за утечку данных. В нем рассматриваются проблемы обеспечения безопасности персональных данных в условиях информационного общества и вопросы установления правовой ответственности в случаях их утечки (data breach). В ходе исследования был проведен сравнительно-правовой анализ на основе национального законодательства Республики Узбекистан, норм Общего регламента по защите данных Европейского Союза (GDPR), а также опыта стран Америки и Азии. В статье раскрыта правовая природа понятия «утечка данных» (data breach) и изучены границы гражданской, административной и уголовной ответственности субъектов. В результате проведенного анализа выявлены пробелы в национальном законодательстве в механизмах уведомления об утечке данных и в системе возмещения ущерба. В завершение статьи выдвинуты научно-практические предложения по обеспечению неприкосновенности персональных данных в киберпространстве и совершенствованию мер ответственности.*

Ключевые слова: *персональные данные, утечка данных, data breach, юридическая ответственность, GDPR, CCPA, киберправо, цифровая безопасность, административный штраф, уголовная ответственность, гражданская ответственность, возмещение ущерба, моральный вред,*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

киберпреступность, информационные системы, киберугрозы, цифровая безопасность.

KIRISH

Bugungi kunda insoniyat raqamli transformatsiya jarayonining markazida turibdi. Jamiyatning deyarli barcha sohalari — iqtisodiyotdan tortib davlat boshqaruvigacha — axborot tizimlariga integratsiya qilinishi natijasida “shaxsga doir ma’lumotlar” tushunchasi zamonaviy dunyoning eng qimmatli aktiviga aylandi. Biroq, texnologik taraqqiyot o‘z navbatida kiber-tahdidlarning ham keskin ortishiga sabab bo‘ldi. Xususan, ma’lumotlar sizib chiqishi (data breach) nafaqat jismoniy shaxslarning daxlsizlik huquqini buzmoqda, balki yirik korporatsiyalar va davlat institutlarining xavfsizligiga ham jiddiy xavf tug‘dirmoqda.

Tadqiqotning dolzarbligi shundaki, bugungi global raqamli transformatsiya davrida axborot eng qimmatli strategik resursga aylandi. Jamiyat hayotining barcha jabhalari, xususan, davlat boshqaruvi, moliya-bank tizimi va ijtimoiy xizmatlarning raqamli platformalarga ko‘chishi shaxsga doir ma'lumotlar xavfsizligini ta’minlash masalasini milliy xavfsizlik darajasiga ko‘tardi. Biroq, texnologik imkoniyatlar kengayishi bilan birga, kiber-makonda ma’lumotlar sizib chiqishi (data breach) bilan bog‘liq xavf-xatarlar ham keskin ortib bormoqda.

Xalqaro kiberxavfsizlik markazlari tahliliga ko‘ra, har yili dunyo miqyosida milliardlab shaxsiy ma'lumotlar noqonuniy ravishda ochiq tarmoqqa chiqib ketmoqda. Bu esa nafaqat inson huquqlari va shaxsiy daxlsizlikning buzilishiga, balki jiddiy moliyaviy yo‘qotishlar va jamiyatda raqamli tizimlarga bo‘lgan ishonchning pasayishiga olib kelmoqda. O‘zbekistonda ham raqamli iqtisodiyotni rivojlantirish ustuvor vazifa etib belgilangan bir davrda, shaxsga doir ma’lumotlar

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

sizib chiqishi uchun huquqiy javobgarlik mexanizmlarini takomillashtirish va qonunchilikdagi bo‘shliqlarni to‘ldirish har qachongidan ham dolzarb hisoblanadi.

Xalqaro tajriba shuni ko‘rsatadiki, Equifax, Yahoo yoki Facebook kabi gigant kompaniyalarda sodir bo‘lgan ma’lumotlar o‘g‘irlanishi holatlari huquqiy tartibga solishning qanchalik muhimligini isbotladi. Dunyo miqyosida Yevropa Ittifoqining GDPR va AQShning CCPA kabi qat’iy standartlari qabul qilinayotgan bir paytda, O‘zbekiston milliy qonunchiligida ham ushbu masalada javobgarlik mexanizmlarini takomillashtirish zarurati tug‘ilmoqda.

Ushbu tadqiqotning asosiy maqsadi shaxsga doir ma’lumotlar sizib chiqishi holatlarida huquqiy javobgarlikning nazariy va amaliy jihatlarini kompleks tahlil qilishdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilab olindi:

- "Ma'lumotlar sizib chiqishi" (data breach) tushunchasining huquqiy tabiatini xalqaro va milliy qonunchilik prizmasida ochib berish;
- Ma’lumotlar xavfsizligini ta’minlashda mas’ul subyektlarning fuqarolik, ma’muriy va jinoiy javobgarligi chegaralarini tadqiq etish;
- Yevropa Ittifoqining GDPR va AQShning CCPA kabi ilg'or xalqaro standartlarini milliy qonunchilikka implementatsiya qilish imkoniyatlarini o‘rganish;
- O‘zbekiston Respublikasining ma'lumotlarni himoya qilish sohasidagi qonunchiligini takomillashtirish bo‘yicha ilmiy-amaliy taklif va tavsiyalar ishlab chiqish.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Tadqiqot natijasida olingan ma’lumotlar ma’lumotlar sizib chiqishi bo‘yicha huquqiy javobgarlikni tahlil qilish bo‘yicha amaliy tavsiyalar berish imkonini beradi. Shuningdek, ushbu sohadagi ilmiy bilimlarni boyitishga xizmat qiladi.

ADABIYOTLAR TAHLILI

Ma’lumotlar sizib chiqishi uchun huquqiy javobgarlikni o‘rganishda ushbu sohadagi ilmiy maqolalar, kitoblar va milliy va xorijiy adabiyotlardan, shuningdek, milliy va xorijiy qonunchiliklardan foydalangan holda ushbu mavzuga oid nazariy asoslar o‘rganildi..Xususan, milliy qonunchilik asosida: O‘zbekiston Respublikasining 2019-yil 2-iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-son Qonuni, O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni, xorijiy qonunchilik asosida Yevropa Ittifoqining General Data Protection Regulation (GDPR) reglamenti, AQShda yagona federal qonun bo‘lmasa-da, shtatlar darajasidagi qonunlar (masalan, CCPA - California Consumer Privacy Act) va sohaviy qonunlar (HIPAA), shuningdek, xorijiy maqolalardan, Graham Greenleaf o‘zining *"Asian Data Privacy Laws"* (Oxford University Press) tadqiqotida Yaponiya, Janubiy Koreya va Xitoy qonunchiligidagi ma’lumotlarni himoya qilish tendensiyalarini qiyosiy tahlili , Daniel J. Solove o‘zining *"Understanding Privacy"* (Harvard University Press) va *"The Digital Person"* asarlarida ma’lumotlar sizib chiqishi natijasida yetkazilgan "nomoddiy zarar"ni (intangible harm) baholashning huquqiy muammolarini tadqiq etishga oid ilmiy maqolalar hamda ilmiy kitoblardan foydalanildi.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

NATIJALAR

Ma’lumotlar sizib chiqishi uchun huquqiy javobgarlik masalasiga oid ilmiy izlanishlari natijasida shuni o‘rgandikki, hozirgi kunda ma’lumotlar sizib chiqishi uchun huquqiy javobgarlik masalasini belgilash juda ham bahsli va munozarali bo‘lib bormoqda. Aslida ma’lumotlar sizib chiqishiga nimalar sabab bo‘lishi tadqiqot davomida aniqlangdi. Tadqiqot natijalariga ko‘ra ma’lumotlar sizib chiqishining 3 ta asosiy “yo‘lagi” mavjud bo‘lib ularning birin-ketinlikda tahlil qilib o‘tamiz.

Birinchisi, Kiber hujum natijasida ma’lumotlar sizib chiqishini ko‘rishimiz mumkin. Xalqaro huquq doirasida ham kiber jinoyatchilik mavjud bo‘lib bunda ma’lum bir davlat tomonidan boshqa davlatning axborot tizimlari yoki shunga o‘xshash ma’lumotlar bazasiga noqonuniy ravishda kirib olishadi hamda ushbu va shunga o‘xshash jinoyatlarni sodir etadi. Bu holat Xalqaro huquqda External Cyber Attacks[1] deb ataladi. Ibm.com sayti ma’lumotlari asosida tadqiqotlar olib borilgan hamda unga ko‘ra Kiber hujum orqali ham ma’lumotlar sizib chiqishi ya’ni data breach ning sodir etilishi keltirib o‘tilgan. Ma’lumotlar sizib chiqishining ushbu yo‘lagi tashkilotning axborot perimetridan tashqaridagi subyektlar tomonidan amalga oshiriladigan maqsadli g‘ayrihuquqiy harakatlar majmuidir. Masalan olib qaraylik bunda A davlat B davlatga urush e’lon qildi va bunda A davlat unga qurolli to‘qnashuv orqali emas, balki kiber hujum orqali davlatga zarba bermoqchi. Bunda aynan davlat data breachdan foydalanishi mumkin bo‘ladi. Bunda u A davlat fuqarolarini shaxsiy

[1] **External Cybersecurity** // ZeroFox Glossary. – URL: (murojaat sanasi: 04.04.2026).

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

ma’lumotlarni keng ommaga oshkora ko‘rinishda kelitirib qo‘yishi mumkin bo‘ladi. Buning natijaasida fuqarolarning davlat o‘z majburiyatini bajarmaganligi ya’ni shaxsiy ma’lumotlarni ishonchli tarzda himoya qilmaganligi uchun norozilik kayfiyati uyg‘onishiga sabab bo‘ladi.

Ikkinchisi, Inson omili bilan bog‘liq bo‘lgan yo‘lak ya’ni ehtiyotsizlik natijasida ma’lumotlar sizib chiqishi. Tadqiqot natijalari shuni tasdiqlaydiki, ma’lumotlar sizib chiqishi hodisalarining katta qismi (ayrim manbalarda 80% gacha) tashqi tajovuz natijasida emas, balki ma’lumotlar bilan bevosita ishlovchi xodimlarning ehtiyotsizligi oqibatida yuzaga keladi. Bunga shaxslarning ma’lumotlarini to‘g‘ri saqlay olmaganligi va axborot xavfsizligi madaniyatiga yetarli darajada rioya etmaganligi asosiy sabab bo‘ladi. Xususan, ehtiyotsizlik yo‘lagi orqali sodir bo‘ladigan sizib chiqishlar ko‘pincha qasddan qilingan jinoyat emas, balki subyektiv sustkashlik natijasida ushbu huquqbuzarlik kelib chiqadi . Ushbu jarayonning huquqiy-tashkiliy ildizlarini ncsc.gov.uk[2] saytidan quyidagi omillar bilan izohlanishini ko‘rish mumkin:

- Raqamli bilimning yetishmasligi natijasida ma’lumtolar sizib chiqishi. Bunda xodimlarning o‘z xizmat akkauntlari va parollarini himoyalanmagan holda qoldirishi, shaxsiy qurilmalardan (BYOD — Bring Your Own Device) korporativ tarmoqlarga nazoratsiz ulanishi hamda shubhali fishing havolalariga ishonuvchanlik bilan yondashishi ma’lumotlar xavfsizligiga "ichkaridan" darz ketkazadi.

[2] National Cyber Security Centre (NCSC). – URL: https://www.ncsc.gov.uk/ (murojaat sanasi: 04.04.2026).

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

- Kommunikativ xatoliklarning mavjud bo‘lishi orqali ma’lumotlar sizib chiqishi. Amaliyotda ko‘p uchraydigan holatlardan biri — maxfiy ma’lumotlar bazasini elektron pochta yoki messenjerlar orqali yuborishda qabul qiluvchi manzilini adashtirib yuborishdir. Bunday mexanik xatolar oqibatida minglab fuqarolarning shaxsga doir ma’lumotlari ochiq internet makoniga sizib chiqmoqda.
- Tizimli nazoratning zaifligi (Organizational Negligence)orqali data breach bo‘lishi. Tadqiqot shuni ko‘rsatadiki, inson omili tufayli yuzaga kelgan har qanday xatolik zamirida tashkilotning aybi ham mavjud. Ya’ni, operator tomonidan xodimlarga axborot xavfsizligi bo‘yicha tegishli treninglar o‘tkazilmaganligi va ma’lumotlarning chiqib ketishini to‘suvchi texnik filtrlar (DLP — Data Loss Prevention tizimlari) joriy etilmaganligi huquqiy javobgarlikning operator zimmasiga tushishiga sabab bo‘ladi.

Huquqiy nuqtayi nazardan, ehtiyotsizlik oqibatida yuzaga kelgan sizib chiqishlar subyektning ayb shakliga ko‘ra “bevaqtlik” yoki “sovuqqonlik” sifatida tavsiflanishi mumkin. Bu esa qonun ijodkorlari va huquqshunoslar oldiga faqatgina jazolash emas, balki tashkilotlarda axborot bilan ishlashning huquqiy mexanizmlarini va korporativ xavfsizlik standartlarini takomillashtirish vazifasini qo‘yadi

Uchinchisi bu ichki omil, ya’ni insayderlar orqasidan ma’lumotlar sizib chiqishi. Tadqiqot natijalari shuni ko‘rsatadiki, tashqi kiber-hujumlar va ehtiyotsizlikdan farqli o‘laroq, ichki omil bilan bog‘liq sizib chiqishlar qasddan sodir etilishi bilan ajralib turadi. Bu yo‘lak tashkilotning o‘z xodimlari yoki ma’lumotlarga qonuniy kirish huquqiga ega bo‘lgan shaxslar tomonidan amalga

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

oshiriladigan g‘ayrihuquqiy harakatlarni qamrab olishini ko‘rishimiz mumkin bo‘ladi.

Ma’lumotlar sizib chiqishining asosiy omillarini o‘rganganimizdan so‘ng, ushbu omillarga yechim berishda xalqaro standartlardan andoza olgan holatda yangi qonunchilik normalarini yaratishimizga to‘g‘ri keladi. Xalqaro standratlardan birin-ketinlikda tahlil qilib boramiz, Ma’lumotlar xavfsizligini ta’minlashda xalqaro hamjamiyat tomonidan ishlab chiqilgan huquqiy mexanizmlar uchta asosiy modelga bo‘linadi. Ushbu modellarning har biri javobgarlik subyektini belgilash va sanksiyalar qo‘llashda o‘ziga xos yondashuvga ega.

GDPR — bugungi kunda dunyodagi eng qat’iy va mukammal huquqiy hujjat bo‘lib, u "shaxsning ma’lumotlar ustidan nazorati" prinsipiga asoslanadi[3]. GDPR ga ko‘ra shaxsiy ma’lumotlarni saqlanishi, ularning sizib chiqishi oldini olish uchun bir-nechta prinsiplari keltirib o‘tilgan bo‘lib, birinchisi, 72 soatlik qoida. GDPRning 33-moddasiga binoan, ma’lumotlar sizib chiqqan taqdirda, operator bu haqda nazorat qiluvchi organni 72 soat ichida xabardor qilishi shart[4]. Ushbu majburiyatning buzilishi mustaqil huquqbuzarlik hisoblanadi. Bundan tashqari, Eksterritoriallik hammavjud bo‘lib, Reglament Yevropa Ittifoqi hududidan tashqarida joylashgan, biroq Yevropa fuqarolariga xizmat ko‘rsatuvchi har qanday kompaniyaga (masalan, Google, Meta, o‘zbekistonlik eksportyorlar)

[3] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119/1
[4] GDPR, Article 33: "Notification of a personal data breach to the supervisory authority"

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

nisbatan qo‘llaniladi[5]. Shu bilan birga yana bir choralardan biri , javobgarlik choralari yillik aylanmaning 4 foizigacha yoki 20 million yevrogacha bo‘lgan miqdorda belgilanganligi hisoblanadi[6] . Bu tashkilotlarni kiber-xavfsizlikka "xarajat" emas, balki "zaruriy investitsiya" sifatida qarashga majbur qiladi. GDPR normalari ma’lumotlar sizib chiqishi hamda ularning oldini olish, javobgarlik masalasini belgilashda asosiy standartlardan biri hisoblanadi.

GDPR xalqaro standartidan tashqari yana bir muhim xalqaro standart mavjuddir. Bu asosan Amerikada kuzatilivchi standart hisoblanadi. AQSHda yagona federal qonun mavjud emas, biroq Kaliforniya shtatining **CCPA** (California Consumer Privacy Act) qonuni GDPRga eng yaqin model hisoblanadi[7].

CCPA standartida ham bir qancha prinsiplar keltirilgan bo‘lib ulardan biri bu Iste’molchi huquqi prinsipi hisoblanadi. Bu model ko‘proq iqtisodiy zarar va iste’molchi huquqlariga yo‘naltirilgan. Ma’lumotlar sizib chiqqanda, iste’molchi statut zarari (statutory damages) talab qilish huquqiga ega, ya’ni u aniq moddiy zarar ko‘rganini isbotlashi shart emas — sizib chiqish faktining o‘zi kompensatsiya uchun asos bo‘ladi[8]. Shuningdek, Safe Harbor prinsipining inqirozi haqida ham gapirish lozim. AQSH tajribasi shuni ko‘rsatadiki, kompaniyalar "o‘z-o‘zini tartibga solish" (self-regulation) orqali xavfsizlikni ta’minlay olmaydi, shuning uchun davlat nazorati kuchaytirilmoqda[9].

[5] Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing. p. 22-25
[6] GDPR, Article 83: "General conditions for imposing administrative fines". Section 5.
[7] California Consumer Privacy Act of 2018 (CCPA). *California Civil Code*, Section 1798.100 - 1798.199.100
[8] Chassang, G. (2017). The European General Data Protection Regulation: Emergence of a personal data protection law 2.0. *Ecancermedicalscience*, 11, 708.
[9] Solove, D. J., & Hartzog, W. (2014). *The FTC and the New Common Law of Privacy*. Columbia Law Review, Vol. 114, No. 3.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

MUNOZARA

Dastlab ma’lumotlar qanday turlarga bo‘linadi, ma’lumotlar sizib chiqishi nima hamda ularga nisbatan qanday javobgarlik masalasini ham izohlab ketish zarur bo‘ladi. Ma'lumotlarning buzilishi - bu ruxsatsiz shaxslar shaxsiy ma'lumotlar (ijtimoiy ta'minot raqamlari, bank hisob raqamlari, sog'liqni saqlash ma'lumotlari) va korporativ ma'lumotlar (mijozlar yozuvlari, intellektual mulk, moliyaviy ma'lumotlar) kabi maxfiy yoki maxfiy ma'lumotlarga kirishlari mumkin bo‘lgan har qanday xavfsizlik hodisasi hisoblanadi. "Ma'lumotlarning buzilishi" va "buzish" atamalari ko‘pincha "kiberhujum" bilan bir-birining o‘rnida ishlatiladi. Biroq, barcha kiberhujumlar ham ma'lumotlarning buzilishi emas. Ma'lumotlarning buzilishi faqat kimdir ma'lumotlarga ruxsatsiz kirish huquqini qo‘lga kiritadigan xavfsizlik buzilishlarini o‘z ichiga oladi .

Masalan, veb-saytni qamrab oluvchi tarqatilgan xizmat ko‘rsatishdan bosh tortish (DDoS) hujumi ma'lumotlarning buzilishi emas. Kompaniyaning mijozlar ma'lumotlarini qulflaydigan va agar kompaniya to‘lov to‘lamasa, o‘g'irlangan ma'lumotlarni sizdirib yuborish bilan tahdid qiladigan ransomware hujumi ma'lumotlarning buzilishi hisoblanadi. Qattiq disklar, USB flesh-disklar yoki hatto maxfiy ma'lumotlarni o‘z ichiga olgan qog'oz fayllarning jismoniy o‘g'irlanishi ham ma'lumotlarning buzilishi hisoblanadi.

IBMning 2025-yilgi ma'lumotlar buzilishining narxi haqidagi hisobotiga ko‘ra, ma'lumotlar buzilishining global o‘rtacha qiymati 4,44 million AQSh dollarini tashkil etadi. Har qanday hajmdagi va turdagi tashkilotlar buzilishlarga moyil bo‘lsa-da, bu buzilishlarning jiddiyligi va ularni bartaraf etish xarajatlari har

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

xil bo‘lishi mumkin[10]. Masalan, Qo‘shma Shtatlarda ma'lumotlarning buzilishining o‘rtacha qiymati 10,22 million AQSh dollarini tashkil etadi, bu Hindistondagi buzilish qiymatidan (2,51 million AQSh dollari) taxminan 4 baravar ko‘p. Buzilish oqibatlari, ayniqsa, sog'liqni saqlash, moliya va davlat sektori kabi yuqori darajada tartibga solingan sohalardagi tashkilotlar uchun jiddiy bo‘lib, bu yerda katta jarimalar va jarimalar xarajatlarni oshirishi mumkin. Masalan, IBM hisobotiga ko‘ra, 2025-yilda sog'liqni saqlash ma'lumotlarining buzilishining o‘rtacha qiymati 7,42 million AQSh dollarini tashkil etadi, bu ketma-ket 14-yil davomida sohalar orasida eng yuqori o‘rtacha buzilish qiymati hisoblanadi. Ma'lumotlarning o‘g'irlanishi bilan bog'liq xarajatlar bir nechta omillarga bog'liq bo‘lib, IBM hisobotida to‘rtta asosiy omillar qayd etilgan: yo‘qolgan biznes, aniqlash va kuchayish, buzilishdan keyingi javob va xabarnoma.

Ma'lumotlar buzilishi natijasida biznes, daromad va mijozlarning yo‘qotilishi tashkilotlarga o‘rtacha 1,38 million AQSh dollariga tushadi. Ma'lumotlar buzilishini aniqlash va uni kuchaytirish narxi yanada yuqori bo‘lib, 1,47 million AQSh dollarini tashkil etadi. Ma'lumotlar buzilishidan keyingi xarajatlar, jumladan, jarimalar, kelishuvlar, yuridik to‘lovlar, zarar ko‘rgan mijozlarga bepul kredit monitoringini taqdim etish va shunga o‘xshash xarajatlar, o‘rtacha ma'lumotlar buzilishi qurboniga 1,20 million AQSh dollariga tushdi.

AQShning 2022-yilgi Muhim infratuzilma uchun kiber-hodisalar haqida xabar berish to‘g'risidagi qonuni (CIRCIA) milliy xavfsizlik, moliya va boshqa belgilangan sohalardagi tashkilotlardan shaxsiy ma'lumotlar yoki biznes operatsiyalariga ta'sir qiluvchi kiberxavfsizlik hodisalari haqida 72 soat ichida

[10] Cost of a Data Breach Report 2025 // IBM Security. – URL: https://www.ibm.com/reports/data-breach (murojaat sanasi: 04.04.2026).

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Ichki xavfsizlik departamentiga xabar berishni talab qiladi[11].

AQShning Sog‘liqni saqlash sug‘urtasining ko‘chmaligi va hisobdorligi to‘g‘risidagi qonuniga (HIPAA) bo‘ysunadigan tashkilotlari, agar himoyalangan sog‘liqni saqlash ma’lumotlari oshkor qilingan bo‘lsa, AQSh Sog‘liqni saqlash va aholini ijtimoiy himoya qilish vazirligiga, ta’sirlangan shaxslarga va ba’zan ommaviy axborot vositalariga xabar berishlari shart. AQShning barcha 50 shtatida ham o‘zlarining ma'lumotlarning buzilishi haqida xabar berish qonunlari mavjud.

Umumiy ma'lumotlarni himoya qilish to‘g'risidagi Nizom (GDPR) Yevropa Ittifoqi fuqarolari bilan biznes yuritayotgan kompaniyalardan qonunbuzarliklar haqida 72 soat ichida rasmiylarga xabar berishni talab qiladi.

Tadqiqot natijasida aynan ma’lumotlar sizib chiqishi bo‘yicha bir nechta real keyslar ham mavjud bo‘lib ulardan eng muhimlarini tahlil qilib ketish lozim bo‘ladi.

TJX keysi

2007-yilda TJ Maxx va Marshalls chakana savdo do‘konlarining bosh kompaniyasi bo‘lgan TJX Corporation kompaniyasining buzilishi o‘sha paytda AQSh tarixidagi eng yirik va eng qimmat iste'molchi ma'lumotlarining buzilishi bo‘lgan. Taxminan 94 million mijozning ma'lumotlarining maxfiyligi buzilgan va kompaniya 256 million AQSh dollaridan ortiq moliyaviy zarar ko‘rgan.

Xakerlar ikkita do‘konning simsiz tarmoqlariga trafik tahlilchilari o‘rnatish orqali ma'lumotlarga kirish huquqiga ega bo‘lishdi. Sniffers xakerlarga do‘konning

[11] Regulation (EU) 2016/679 (General Data Protection Regulation) // OJ L 119, 04.05.2016; Art. 33.

kassa apparatlaridan orqa tizimlarga uzatilayotgan ma'lumotlarni qo‘lga kiritish imkonini berdi[12].

Equifax Keysi

2017-yilda xakerlar kredit hisobotlari agentligi Equifax’ning tizimga kirishiga yo‘l qo‘yishdi va 143 milliondan ortiq amerikaliklarning shaxsiy ma’lumotlariga kirishdi.

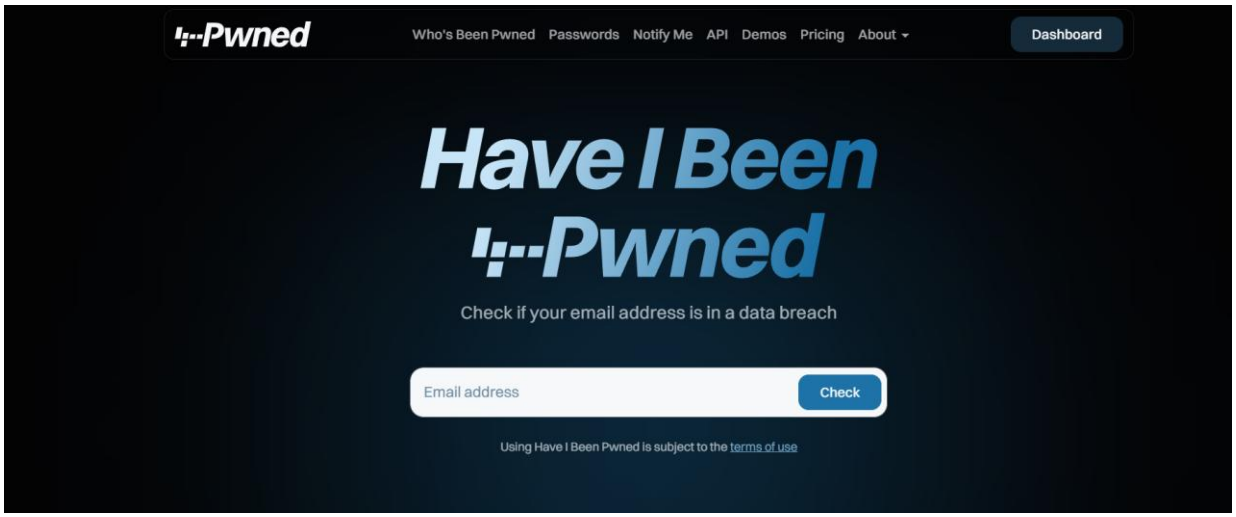
Xakerlar Equifax veb-saytidagi tuzatilmagan zaiflikdan foydalanib, tarmoqqa kirish huquqini qo‘lga kiritishdi. Keyin xakerlar ijtimoiy ta'minot raqamlari, haydovchilik guvohnomasi raqamlari va kredit karta raqamlarini topish uchun boshqa serverlarga o‘tishdi. Hujum Equifaxga hisob-kitoblar, jarimalar va buzilishlarni tuzatish bilan bog'liq boshqa xarajatlar o‘rtasida 1,4 milliard AQSh dollari miqdorida zarar yetkazdi[13].

Shuningdek , ma’lumotlar sizib chiqishi bo‘yicha platforma ishga tushirilgan bo‘lib tadqiqot davomida bu platforma haqida ham o‘rganildi. Raqamli xavfsizligingizni kuchaytirish uchun qaysi akkauntlar ta'sirlanganini bilish muhimdir. Bu vazifani siz xavfsizlik mutaxassislari tomonidan keng tavsiya etilgan bepul veb-sayt Have I Been Pwned da bajarishingiz mumkin. (" Pwn " atamasi kompyuter yoki dasturni buzish yoki nazoratni qo‘lga olish uchun xakerlik jargonidir.

[12] FTC v. The TJX Companies, Inc. (Agreement Containing Consent Order) // Federal Trade Commission. – 2008. – File No. 072 3055. – URL: https://www.ftc.gov/legal-library/browse/cases-proceedings/072-3055-tjx-companies-inc-matter (murojaat sanasi: 04.04.2026).
[13] Equifax Data Breach Settlement. // Federal Trade Commission. – 2019. – URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (murojaat sanasi: 04.04.2026).

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Avstraliyalik veb-xavfsizlik bo‘yicha maslahatchi Troy Hunt tomonidan yaratilgan sayt yuzlab buzilishlar va millionlab buzilgan akkauntlardan olingan ma'lumotlarni tahlil qiladi, bu ma'lumotlar ko‘pincha onlayn joylashtiriladi va jinoyatchilar tomonidan sotiladi. Sayt sizga elektron pochta manzili yoki telefon raqamini kiritish orqali sayt kuzatadigan ma'lumotlar buzilishlarida paydo bo‘lgan-bo‘lmaganligini aniqlash imkonini beradi. Keyin siz parollaringizni o‘zgartirishingiz va o‘zingizni himoya qilish uchun boshqa choralarni ko‘rishingiz mumkin[14].



Consumer Reports odamlarni yillar davomida "Have I Been Pwned"ga yo‘naltirib kelmoqda va xavfsizlikni yaxshi biladigan iste'molchilar bundan oldin ham foydalangan bo‘lishlari mumkin.

Qonunchilikka takliflar

Ma’lumotlar sizib chiqishi uchun huquqiy javobgarlik masalasida xalqaro tajriba hamda standratlarga tayangan holatda O‘zbekistonda mavjud bo‘lgan bir nechta normalarga quyidagi takliflar kiritildi:

[14] https://www.consumerreports.org

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Birinchidan, jarimalar miqdorini "Differensiallash" va iqtisodiy drayverga aylantirish masalani hal qilish lozim. Hozirgi MJtK 46-2-moddasidagi jarimalar (BHMning 10 baravarigacha) yirik banklar yoki telekom kompaniyalari uchun juda kamlik qiladi va ularni tizimni himoya qilishga majburlamaydi.Taklif sifatida yuridik shaxslar (operatorlar) uchun jarimalarni ularning yillik aylanmasiga (oborotiga) foiz nisbatida belgilash (masalan, yillik tushumning 1% dan 4% gacha) lozim deb o‘ylaymiz.

Ikkinchidan, "Statut zarari" (Statutory Damages) tushunchasini kiritish ham zarur hisoblanadi. Fuqarolik kodeksi bo‘yicha ma’lumotlari sizib chiqqan shaxs o‘ziga yetgan aniq moddiy zararni isbotlashi juda qiyin (masalan, ma’lumot o‘g‘irlandi, lekin hali pul yechilmadi) hisoblanib, AQSHning CCPA tajribasiga tayangan holatda , fuqarolik qonunchiligiga shaxsga doir ma’lumotlar sizib chiqqan faktining o‘zi uchun bazaviy kompensatsiya miqdorini (isbot talab qilinmaydigan minimal summa) belgilash lozim.

Uchinchidan, "Ma’lumotlar himoyasi bo‘yicha inspektor" (DPO) lavozimini majburiylash lozim. Katta hajmdagi shaxsga doir ma’lumotlar bilan ishlovchi yuridik shaxslarda (masalan, 100 mingdan ortiq foydalanuvchisi borlar) alohida **Data Protection Officer (DPO)** lavozimini joriy etishni majburiy qilish. Sababi ushbu tizimni joriy qilish orqali ma’lumtolar sizib chiqishining insayder hamda ehtiyotsizlikdan ma’lumotlar sizib chiqishini oldini olish mumkin bo‘ladi.

XULOSA

Yuqoridagi tahlillardan kelib chiqib, O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuniga “Ma’lumotlar xavfsizligi insidenti haqida majburiy xabardor qilish” institutini kiritish hamda MJtKda

yuridik shaxslar uchun aylanma mablag‘dan kelib chiqadigan jarimalar tizimini joriy etish taklif qilinadi. Bu nafaqat jazo choralarini kuchaytiradi, balki raqamli iqtisodiyot sub’ektlarining ijtimoiy mas’uliyatini oshirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasining Qonuni. Shaxsga doir ma’lumotlar to‘g‘risida. – O‘RQ-547-son. – 2019-yil 2-iyul. // Qonunchilik ma’lumotlari milliy bazasi, 03.07.2019-y., 03/19/547/3363-son.
2. O‘zbekiston Respublikasining Qonuni. Kiberxavfsizlik to‘g‘risida. – O‘RQ-764-son. – 2022-yil 15-aprel. // Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022-y., 03/22/764/0315-son.
3. Regulation (EU) 2016/679 (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119.
4. Convention on Cybercrime (Budapest Convention) // Council of Europe. – ETS No. 185. – 2001.
5. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), 6 U.S.C. §§ 681–681g.
6. California Consumer Privacy Act (CCPA) // California Civil Code § 1798.100.
7. Cost of a Data Breach Report 2025 // IBM Security. – 2025. – URL: https://www.ibm.com/reports/data-breach (murojaat sanasi: 04.04.2026).
8. Verizon 2025 Data Breach Investigations Report (DBIR) // Verizon Enterprise Solutions. – 2025.
9. National Cyber Security Centre (NCSC) Official Portal. – UK Government. – URL: https://www.ncsc.gov.uk/.

Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

10. External Cybersecurity // ZeroFox Glossary. – URL: https://www.zerofox.com/glossary/external-cybersecurity/.
11. FTC v. The TJX Companies, Inc. (Agreement Containing Consent Order) // Federal Trade Commission. – 2008. – File No. 072 3055.
12. Equifax Data Breach Settlement // Federal Trade Commission (FTC). – 2019. – URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.
13. In re: Yahoo! Inc. Customer Data Security Breach Litigation // Northern District of California Case No. 16-MD-02752-LHK.