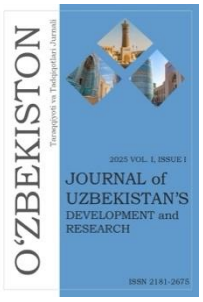

Journal of Uzbekistan's Development and Research (JUDR)

Journal home page: https://ijournal.uz/index.php/judr

# O'ZBEKISTON AXBOROT XAVFSIZLIGI SOHASIDAGI HUQUQIY TARTIBOTNING ZAMONAVIY MUAMMOLARI VA XALQARO AMALIYOT ASOSIDA TAKLIFLAR

Akramova Sabrina[1]

*Toshkent davlat yuridik universiteti*

KEYWORDS

axborot xavfsizligi, kiberjinoyat, shaxsiy ma'lumotlar, davlat siri, xalqaro tajriba, qonunchilik tahlili.

ABSTRACT

Maqolada O'zbekiston Respublikasining axborot xavfsizligi sohasidagi amaldagi qonunchilik holati xalqaro standartlar va ilg'or xorijiy tajriba asosida tahlil qilinadi. Muhim infratuzilma, shaxsiy ma'lumotlar, davlat sirlarini muhofaza qilish hamda kiberjinoyatlarga qarshi kurash yo'nalishlarida mavjud bo'shliqlar aniqlanib, Yevropa Ittifoqi, AQSh va Janubiy Koreya qonunchiligi bilan taqqoslanadi. Qonun hujjatlarining aniq mexanizmlarga ega emasligi, sud nazorati va xavflarni boshqarish tizimlarining yetishmasligi milliy qonunchilikni takomillashtirish zaruratini ko'rsatadi. Taklif etilayotgan huquqiy yechimlar milliy sharoitga moslashtirilgan va xalqaro tajriba bilan uyg'unlashtirilgan holda asoslab beriladi.

2181-2675/© 2025 in XALQARO TADQIQOT LLC.
DOI: **10.5281/zenodo.16617075**


## Kirish

O'zbekiston Respublikasi so'nggi yillarda axborot xavfsizligini ta'minlash borasida muhim huquqiy tashabbuslarni amalga oshirdi. Xususan, 2019-yilda qabul qilingan "Shaxsiy ma'lumotlar to'g'risida"gi qonun hamda 2022-yilda kuchga kirgan "Kiberxavfsizlik to'g'risida"gi qonun mamlakatning raqamli xavfsizlikni mustahkamlash va axborot makonini huquqiy jihatdan tartibga solishga qaratilgan strategik yo'nalishini ifodalaydi. Shu bilan birga, Yevropa Ittifoqi, AQSh va Janubiy Koreya kabi ilg'or huquqiy-amaliy tajribaga ega davlatlar qonunchiligi bilan solishtirma tahlil O'zbekiston normativ-huquqiy bazasida hali ham tizimli takomillashtirishni talab etuvchi jihatlar mavjudligini ko'rsatmoqda.

Hozirgi kunda O'zbekistonda "Kiberxavfsizlik to'g'risida"gi qonun mavjud bo'lsa-da,

[1] Toshkent davlat yuridik universiteti Magistratura va sirtqi ta`lim fakulteti Ommaviy axborot vositalari yo`nalishi magistranti

muhim axborot infratuzilmasini himoya qilishni maxsus tartibga soluvchi alohida va keng qamrovli qonun hujjatlari mavjud emas. Bu esa energetika, transport, moliya va sog‘liqni saqlash kabi hayotiy muhim sektorlarning kiberxavfsizligini ta‘minlashda aniq mexanizmlar va majburiyatlarning yetishmasligiga olib kelishi mumkin.

Ushbu masalada xorijiy davlatlarning tajribasini ko‘radigan bo‘lsak, Yevropa Ittifoqining axborot xavfsizligi sohasidagi yangilangan NIS2 direktivasi[2] muhim va strategik ahamiyatga ega tashkilotlar zimmasiga kiberxavfsizlik bo‘yicha huquqiy majburiyatlar yuklaydi. Direktivada kiberxavf-xatarlarni boshqarish bo‘yicha qat’iy tashkiliy va texnik chora-tadbirlarni joriy etish, yuzaga kelgan muammolar haqida belgilangan muddatlarda hisobot taqdim etish (dastlabki ogohlantirish 24 soat ichida, batafsil xabar 72 soat ichida, yakuniy hisobot esa bir oy muddatda)[3] majburiyati ko‘zda tutilgan. Bundan tashqari, qonunbuzarliklar uchun jiddiy moliyaviy sanksiyalar belgilangan. Mazkur direktiva “barcha xavflarni qamrab oluvchi” yondashuvni asos qilib oladi; ya’ni, tashkilotlar nafaqat kiberhujumlar, balki texnik nosozliklar, tabiiy ofatlar yoki inson omilidan kelib chiqadigan uzilishlarga ham tayyor bo‘lishi talab etiladi[4].

Janubiy Koreyada amalda bo‘lgan “Axborot-kommunikatsiya infratuzilmasini himoya qilish to‘g‘risida”gi qonun davlat miqyosidagi axborot tizimlarining uzluksiz va xavfsiz faoliyat yuritishini ta’minlashga qaratilgan[5]. Qonun doirasida milliy xavfsizlik, mudofaa, jamoat tartibi, moliya, aloqa, transport va energetika kabi sohalarni qamrab oluvchi elektron infratuzilma subyektlari muhim ob’ektlar sifatida tasniflanadi. Mazkur qonun bu subyektlardan zaifliklarni aniqlash va baholash, ularga nisbatan oldini olish va tiklashga qaratilgan kompleks himoya choralarini ishlab chiqish va amaliyotga tatbiq etishni majburiy tarzda talab qiladi[6].

Bundan tashqari, O‘zbekiston Respublikasining 2019-yilda qabul qilingan “Shaxsiy ma’lumotlar to‘g‘risida”gi qonuni shaxsiy ma’lumotlarga ishlov berish jarayonini huquqiy jihatdan tartibga soluvchi asosiy normativ-huquqiy hujjat hisoblanadi[7]. Ushbu qonun ma’lumot subyektining roziligini asosiy qonuniy asos sifatida belgilaydi hamda shaxsiy ma’lumotlar bazalarining majburiy ro‘yxatdan o‘tkazilishini nazarda tutadi.

Shu bilan birga, ushbu qonunchilik hujjatida ma’lumotlar xavfsizligiga oid buzilishlar uchun javobgarlik choralari ko‘zda tutilgan bo‘lsa-da, ularning huquqiy mezonlari, jarima miqdorlari yetarli darajada aniqlashtirilmagan. Shuningdek, ma’lumot subyektlarining o‘z axborotlari ustidan nazoratini ta’minlovchi fundamental huquqlari, xususan,

[1] NIS 2 Directive. (n.d.). Www.nis-2-Directive.com. https://www.nis-2-directive.com/
[2] NIS2 Directive. (2025, February 24). CyberArk. https://www.cyberark.com/what-is/nis2-directive/
[3] Fowler, C. (2025, February 26). Navigating NIS2 Incident Reporting Obligations | RadarFirst. RadarFirst. https://www.radarfirst.com/blog/navigating-nis2-a-guide-to-incident-reporting-obligations/
[4] Statutes of the Republic of Korea. (n.d.). Elaw.klri.re.kr. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43

[5] Statutes of the Republic of Korea. (n.d.). Elaw.klri.re.kr. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43
[6] *O‘RQ-764-son 15.04.2022. Kiberxavfsizlik to‘g‘risida*. (n.d.). Lex.uz. https://lex.uz/uz/docs/-5960604

**“ma’lumotlarni ko‘chirish huquqi”, “unutilish huquqi”** kabi prinsiplarga oid tartibotlar qonunchilikda batafsil yoritilmagan.

Bundan tashqari, transchegaraviy ma’lumot uzatish jarayonlarini tartibga soluvchi huquqiy mexanizmlar hamda shaxsiy ma’lumotlarning sizib chiqishi (ma’lumotlar buzilishi) yuzasidan vakolatli organlarga yoki subyektlarga xabar berish muddatlariga oid qat’iy talablarning mavjud emasligi qonunchilikdagi muhim bo‘shliqlardan biridir.

Ammo, umumiy ma’lumotlarni himoya qilish to‘g‘risidagi reglament (GDPR) Yevropa Ittifoqida shaxsiy ma’lumotlarni muhofaza qilishni fundamental huquq sifatida e’tirof etadi. Reglament ma’lumotlarga ishlov berish va transchegaraviy uzatish uchun qat’iy protseduralarni belgilaydi hamda subyektlarga keng ko‘lamli huquqlar — shu jumladan, ularni ko‘rish, tuzatish, o‘chirish va cheklash huquqlarini kafolatlaydi[8]. Axborot sizib chiqishi holatlarida 72 soat ichida vakolatli organlarga xabar berish[9] majburiyati joriy qilingan bo‘lib, reglament buzilgan taqdirda 20 million yevrogacha yoki kompaniya yillik aylanmasining 4 foizigacha jarima qo‘llanadi[10].

Janubiy Koreyaning PIPA qonuni ma’lumot subyektining ongli roziligiga asoslangan holda shaxsiy ma’lumotlarni himoya qiladi va transchegaraviy uzatish uchun qat’iy me’yorlarni belgilaydi[11]. Axborot buzilishi yuz bergan taqdirda regulyatorlar hamda jabrlanuvchilarga xabar berish qonuniy majburiyat sifatida belgilanadi. Qoidabuzarliklar uchun 30 million vongacha moliyaviy sanksiyalar nazarda tutilgan[12].

O‘zbekistonning “Kiberxavfsizlik to‘g‘risida”gi qonuni (2022) raqamli tahdidlarga qarshi kurashishda xalqaro hamkorlik zaruratini e’tirof etadi va milliy axborot makonini muhofaza qilishga qaratilgan umumiy tamoyillarni belgilaydi[13]. Biroq, Yevropa Ittifoqi direktivalari yoki Janubiy Koreyaning tegishli qonunchiligi bilan solishtirilganda, kiberjinoyatlarning aniq turlari, ularning kvalifikatsiyasi va jazolari bo‘yicha huquqiy mexanizmlar yetarli darajada ishlab chiqilmagan. Ayniqsa, yuridik shaxslarning kiberjinoyatlar uchun javobgarligi masalasi qonunda aniqlik bilan tartibga solinmagan bo‘lib, bu sohaga oid normativ bazani takomillashtirish zarurati mavjud.

Yevropa Ittifoqining axborot tizimlariga hujumlar to‘g‘risidagi 2013/40/EU direktiva kiberjinoyatlarni — jumladan, axborot tizimlariga noqonuniy kirish, ma’lumotlarni buzish yoki ushlab qolish, zararli dasturiy ta’minotdan (botnetlar) foydalanish kabi

7 European Commission. (2018). *Legal framework of EU data protection*. European Commission. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

8 Staff, I. (2025, January 27). *Cross-border PII data transfer basics and regulations*. InCountry. https://incountry.com/blog/cross-border-pii-data-transfer-basics-and-regulations/

9 Staff, I. (2025, January 27). *Cross-border PII data transfer basics and regulations*. InCountry. https://incountry.com/blog/cross-border-pii-data-transfer-basics-and-regulations/

10 *South Korea PIPA Compliance Services | VeraSafe*. (2025, March 7). VeraSafe. https://verasafe.com/advisory-and-audit/south-korea-pipa-compliance/

11 *Data Protection Guide Korea*. (2023). Multilaw.com. https://multilaw.com/Multilaw/Multilaw/Data_Protection_Laws_Guide/DataProtection_Guide_Korea.aspx

12 Melikulov To‘lqinjon Farxodovich. (2025). *Научный информационный бюллетень*, *7*(1), 154–159. https://inlibrary.uz/index.php/ifx/article/view/83609

holatlarni — jinoiy huquqbuzarlik sifatida belgilaydi[14]. Ushbu huquqiy hujjat yuridik shaxslarning javobgarligini ham ko‘zda tutadi va a’zo davlatlar o‘rtasida 24/7 aloqa nuqtalari orqali tezkor xalqaro hamkorlikni yo‘lga qo‘yishni rag‘batlantiradi[15].

Janubiy Koreya “Axborot-kommunikatsiya tarmoqlaridan foydalanishni rag‘batlantirish va axborotni himoya qilish to‘g‘risida”gi qonun kiberjinoyatlarning asosiy shakllarini — ruxsatsiz kirish, zararli dasturlarni tarqatish, axboriy maxfiylikni buzish yoki oshkor qilish — jinoyat deb baholaydi[16]. Qonunda ushbu huquqbuzarliklar uchun aniq jazo choralariga, jumladan, ozodlikdan mahrum qilish yoki jarimalarga oid normativ tartiblar belgilangan.

**Xulosa**

O‘zbekiston axborot xavfsizligi sohasida mustahkam huquqiy asos yaratish yo‘lida izchil taraqqiyot yo‘lidan bormoqda. So‘nggi yillarda qabul qilingan qonun hujjatlari, ayniqsa “Kiberxavfsizlik to‘g‘risida”gi qonun, shuningdek, muhim axborot infratuzilmasini himoya qilishga doir Prezident qarorlari va strategik dasturlar, raqamli tahdidlarga qarshi tizimli yondashuv shakllanayotganini ko‘rsatadi.

Shu bilan birga, axborot xavfsizligini ta’minlashdagi institutsional infratuzilmaning kengayishi va sohaga ixtisoslashgan organlarning shakllanishi O‘zbekiston tomonidan raqamli xavfsizlikni strategik ustuvor yo‘nalish sifatida tan olinganining isboti hisoblanadi. Bu, o‘z navbatida, davlatning nafaqat texnik yoki texnologik, balki huquqiy va institutsional darajadagi tayyorgarligini kuchaytirishga xizmat qilmoqda.

Biroq xalqaro tajribadan kelib chiqiladigan bo‘lsa, axborot xavfsizligi sohasidagi ilg‘or amaliyotlar – xususan, Yevropa Ittifoqi, AQSh, Janubiy Koreya va Singapurda qo‘llanilayotgan mexanizmlar – milliy tizimni yanada mukammallashtirish uchun muhim manba bo‘lib xizmat qilishi mumkin. Ayniqsa, muhim axborot infratuzilmasini hujumlardan himoya qilish, xavfsizlik va inson huquqlari o‘rtasida muvozanatni ta’minlash, kiberjinoyatlarga qarshi samarali mexanizmlarni ishlab chiqish borasidagi yondashuvlar milliy qonunchilikda ham inobatga olinishi lozim.

Yuqorida sanab o‘tilgan muammolarga yechim sifatida quyidagilarni taklif qilish mumkin: Brinchidan, muammoga taklif sifatida O‘zbekiston Respublikasida muhim axborot infratuzilmasini huquqiy jihatdan alohida tartibga soluvchi, ushbu obyektlarning aniqlanish mezonlarini, ularning operatorlari zimmasidagi xavfsizlik choralarini, xavf baholash tartibini va kiberinsidentlar haqida o‘z vaqtida xabar berish majburiyatlarini belgilab beruvchi maxsus qonun hujjati ishlab chiqilishi maqsadga muvofiqdir. Bunday

[13] *Directive 2013/40 - Attacks against information systems - EU monitor*. (n.d.). Www.eumonitor.eu. https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vjcf5614azjn

[14] *European Union’s Directive on Attacks Against Information Systems - (Comparative Criminal Justice Systems) - Vocab, Definition, Explanations | Fiveable*. (2025). Fiveable.me. https://library.fiveable.me/key-terms/comparative-criminal-justice-systems/european-unions-directive-on-attacks-against-information-systems

[15] *Korea*. (2019). Cybercrimelaw.net. https://www.cybercrimelaw.net/Korea.html

yondashuv Yevropa Ittifoqining NIS2 direktivasi hamda Janubiy Koreya qonunchiligidagi konseptual asoslar bilan uyg‘unlashgan bo‘lishi mumkin.

Ikkinchidan, “Shaxsiy ma’lumotlar to‘g‘risida”gi qonunni quyidagilar bilan takomillashtirish kerak:

Ma’lumotlar subyektlarining huquqlarini kengaytirish, masalan, ma’lumotlarni ko’chirish (data portability) va unutilish (right to be forgotten) huquqlarini aniq belgilash.

Transchegaraviy ma’lumotlarni uzatish uchun “adekvatlik qarorlari” yoki “standart shartnoma shartlari” kabi aniq mexanizmlarni joriy etish[17].

Ma’lumotlar sizib chiqishi to‘g‘risida xabar berishning aniq muddatlarini (masalan, 72 soat ichida) va tartiblarini belgilash[18].

Qoidabuzarliklar uchun aniq va tabaqalashtirilgan ma’muriy jarimalarni, shuningdek, jinoiy javobgarlikni belgilash, bu EI va Janubiy Koreyadagi jarimalar miqdoriga yaqin bo‘lishi mumkin[19].

Uchinchidan,“Kiberxavfsizlik to‘g‘risida”gi qonunga quyidagi yo‘nalishlarda o‘zgartish va qo‘shimchalar kiritish maqsadga muvofiq: Kiberjinoyat turlarining batafsil va huquqiy jihatdan asoslangan tasnifini kiritish; Har bir jinoyat turi uchun aniq va differensial jazo choralari tizimini belgilash; Yuridik shaxslarning javobgarligini jinoiy va ma’muriy huquqiy doirada mustahkamlash.

Ushbu islohotlar kiberjinoyatlarga nisbatan huquqiy aniqlik va qat’iylikni oshiradi, shuningdek, xalqaro hamkorlik doirasida samarali integratsiyani ta’minlaydi.

Xorijiy mamlakatlarning ilg‘or tajribasini o‘rganish va ularni O‘zbekistonning huquqiy, iqtisodiy va texnologik sharoitlariga moslashtirish axborot xavfsizligi tizimini yanada takomillashtirishda strategik omil bo‘lib xizmat qiladi. Bu esa, o‘z navbatida, mamlakatning global kibermakondagi ishtirokini mustahkamlash va raqamli iqtisodiyotning barqaror rivojlanishini ta’minlashda muhim ahamiyat kasb etadi.

**Foydalanilgan adabiyotlar ro`yxati:**

1. O‘zbekiston Respublikasi qonunlari - Kiberxavfsizlik markazi. (n.d.). https://csec.uz/uz/docs/uzbekistan-laws/
2. O'RQ-764-son 25.02.2022. Kiberxavfsizlik to'g'risida. (n.d.). https://lex.uz/uz/docs/-5960604
3. O'RQ-547-son 02.07.2019. Shaxsga doir ma'lumotlar to'g'risida. (n.d.). https://lex.uz/docs/-4396419
4. What is NIS2 Directive? | CyberArk. (n.d.). https://www.cyberark.com/what-is/nis2-directive/

[16] Staff, I. (2025, January 27). *Cross-border PII data transfer basics and regulations*. InCountry. https://incountry.com/blog/cross-border-pii-data-transfer-basics-and-regulations/

[17] Fowler, C. (2025, February 26). *Navigating NIS2 Incident Reporting Obligations | RadarFirst*. RadarFirst. https://www.radarfirst.com/blog/navigating-nis2-a-guide-to-incident-reporting-obligations/

5. Directive 2013/40 - Attacks against information systems - EU monitor. (n.d.). https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vjcf5614azjn
6. Cross-border PII data transfer basics and regulations. (n.d.). https://incountry.com/blog/cross-border-pii-data-transfer-basics-and-regulations/
7. How to notify a data breach to your DPA? (n.d.). https://www.edpb.europa.eu/notify-data-breach_en
8. South Korea Personal Information Protection Act PIPA. (n.d.). https://www.breachrx.com/global-regulations-data-privacy-laws/south-korea-personal-information-act-2/
9. South Korea Information and Communications Infrastructure Protection Act mandatory security measures incident reporting. (n.d.). https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43
10. South Korea cybersecurity laws data protection critical infrastructure cybercrime state secrets. (n.d.). https://www.cybercrimelaw.net/Korea.html
11. EU GDPR critical infrastructure cybercrime state secrets legal framework. (n.d.). https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en
12. South Korea PIPA data breach notification cross-border data transfer consent. (n.d.). https://verasafe.com/advisory-and-audit/south-korea-pipa-compliance/