LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

O‘ZBEKISTONDA AXBOROT XAVFSIZLIGI VA MANIPULYATIV TAHDIDLARNING HOZIRGI HOLATI: TAHLIL VA ISTIQBOLLAR

Malikboyeva Odina
Jahon iqtisodiyoti va diplomatiya universiteti ‘‘Davlat boshqaruvi’’ yo‘nalishi magistranti

Annotatsiya. *Mazkur maqolada O‘zbekiston Respublikasida axborot xavfsizligini ta’minlashning huquqiy-institutsional asoslari, raqamli transformatsiya sharoitida yuzaga kelayotgan manipulyativ axborot tahdidlarining tipologiyasi va zamonaviy shakllari ko‘rsatib berilgan. Shuningdek, ijtimoiy tarmoqlar, sun’iy intellekt vositalari va transchegaraviy axborot oqimlari orqali amalga oshiriladigan dezinformatsiya, ijtimoiy muhandislik va psixologik ta’sir ko‘rsatish usullari yetarlicha tahlil qilinib, ularga qarshi kurashishning huquqiy, institutsional va ta’lim-tarbiyaviy mexanizmlariga asoslangan. Tadqiqot natijalari asosida milliy axborot xavfsizligi tizimini takomillashtirish bo‘yicha ilmiy-amaliy tavsiyalar ishlab chiqilgan.*

Kalit so‘zlar: *axborot xavfsizligi, kiberxavfsizlik, manipulyativ tahdidlar, dezinformatsiya, ijtimoiy muhandislik, gibrid tahdidlar, raqamli savodxonlik, milliy xavfsizlik.*

Zamonaviy jamiyat rivojlanishining o‘ziga xos xususiyati axborot-kommunikatsiya texnologiyalarining barcha ijtimoiy-iqtisodiy jarayonlarga chuqur singib borishi bilan belgilanadi. Mazkur jarayon bir tomondan, davlat boshqaruvi, iqtisodiyot va fuqarolik jamiyati institutlarining samaradorligini oshirishga xizmat qilsa, ikkinchi tomondan, yangi turdagi tahdidlar xususan, ijtimoiy ong va qaror qabul qilish jarayonlariga yashirin ta’sir ko‘rsatishga qaratilgan manipulyativ axborot tahdidlarining yuzaga kelishiga sabab bo‘lmoqda. Shuningdek, O‘zbekiston Respublikasida so‘nggi yillarda kiberxavfsizlik va axborot xavfsizligi

Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

sohasida izchil huquqiy islohotlar amalga oshirilmoqda. Xususan, “Kiberxavfsizlik to‘g‘risida”gi qonun qabul qilingan bo‘lib, muhim axborot infratuzilmasi obyektlarini himoya qilish tizimi joriy etilgan, shuningdek maxsus vakolatli davlat organi sifatida “Kiberxavfsizlik markazi” davlat unitar korxonasi faoliyat yuritmoqda. Shunga qaramay, dezinformatsiya, deepfake texnologiyalari, botlar tarmog‘i va ijtimoiy muhandislik usullari orqali amalga oshiriladigan manipulyativ ta’sirlarga qarshi kurashishning kompleks ilmiy-metodologik asoslari yetarli darajada ishlab chiqilmagan, bu esa mazkur tadqiqotning dolzarbligini belgilaydi.

Mazkur maqolaning asosiy maqsadi – O‘zbekistonda axborot xavfsizligini ta’minlashning mavjud huquqiy-institutsional mexanizmlarini tahlil qilish, manipulyativ axborot tahdidlarining zamonaviy shakllarini tizimlashtirish hamda ularga qarshi kurashish bo‘yicha ilmiy asoslangan tavsiyalar ishlab chiqishdan iborat.

Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi:

1) axborot xavfsizligi va manipulyativ tahdidlar tushunchalarining nazariy-huquqiy mazmunini ochib berish;

2) O‘zbekiston Respublikasining amaldagi qonunchiligi va institutsional tizimini tahlil qilish;

3) manipulyativ axborot tahdidlarining zamonaviy tipologiyasini ishlab chiqish;

4) mavjud muammolarni aniqlash va ularni bartaraf etish yo‘llari bo‘yicha tavsiyalar shakllantirish.

Tadqiqot obyekti – O‘zbekiston Respublikasida axborot xavfsizligini ta’minlash tizimi bo‘lsa, predmeti – ushbu tizim doirasida manipulyativ axborot

tahdidlarining yuzaga kelish sabablari, shakllari va ularga qarshi kurashish mexanizmlaridir.

Axborot xavfsizligi va manipulyativ tahdidlar muammosi xalqaro ilmiy adabiyotda kiberxavfsizlik, strategik kommunikatsiya va gibrid urushlar nazariyasi doirasida keng yoritilgan bo‘lib, xorijiy va mahalliy tadqiqotchilarning ishlarida axborot xavfsizligining texnik, huquqiy va ijtimoiy-psixologik jihatlari o‘rganilgan. Xalqaro tashkilotlar – Xalqaro telekommunikatsiya ittifoqi (ITU), Yevropa Ittifoqining kiberxavfsizlik agentligi (ENISA) kabi tuzilmalarning hisobotlari milliy kiberxavfsizlik strategiyalarini shakllantirishda uslubiy asos sifatida qo‘llaniladi. Mahalliy huquqshunoslik va axborot texnologiyalari sohasidagi tadqiqotlarda esa asosiy e’tibor huquqiy tartibga solish va institutsional rivojlanish masalalariga qaratilgan.

Tadqiqotda umumilmiy (tahlil va sintez, induksiya va deduksiya, tizimli yondashuv) hamda maxsus-huquqiy (qiyosiy-huquqiy, formal-yuridik, kontent-tahlil) metodlardan foydalanilgan. Normativ-huquqiy manba sifatida O‘zbekiston Respublikasining amaldagi qonunlari, Prezident farmonlari va qarorlari, shuningdek tarmoq idoralarining rasmiy statistik va tahliliy materiallari o‘rganilgan.

O‘zbekiston Respublikasida axborot xavfsizligi sohasidagi huquqiy baza so‘nggi besh-olti yil ichida sezilarli darajada takomillashtirildi. 2022-yil 15-aprelda qabul qilingan O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonun ushbu sohadagi asosiy tizimlashtiruvchi normativ hujjat bo‘lib, davlat organlari va tashkilotlarning kiberxavfsizlikni ta’minlash borasidagi huquq va majburiyatlarini, muhim axborot infratuzilmasi obyektlarini himoya qilish tartibini, shuningdek sohadagi kadrlar salohiyatini rivojlantirish mexanizmlarini belgilaydi. Mazkur

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

qonunni amalga oshirish maqsadida bir qator ijrochi hujjatlar qabul qilingan: Prezidentning 2020-yil 15-iyundagi PF-6007-son Farmoni axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etishga, PQ-4751-son qarori esa kiberxavfsizlikni ta’minlash tizimini takomillashtirishga qaratilgan. 2023-yil 31-maydagi PQ-167-son qaror muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini yanada rivojlantirishni nazarda tutadi. Bundan tashqari, 2023-yil sentabr oyida muhim axborot infratuzilmasi obyektlarining kiberxavfsizlik darajasini baholash tartibi belgilangan alohida nizom tasdiqlangan. Institutsional jihatdan sohani muvofiqlashtiruvchi asosiy organ vakolatli davlat organi ishchi organi sifatida faoliyat yurituvchi “Kiberxavfsizlik markazi” davlat unitar korxonasi hisoblanadi. Ushbu tuzilma muhim axborot infratuzilmasi obyektlarini baholash, monitoring qilish va kiberhodisalarga tezkor javob berish funksiyalarini bajaradi. 2024-yil 20-sentabrda qabul qilingan O‘RQ-964-son Qonun bilan kredit tashkilotlari va elektron hukumat tizimida axborot xavfsizligini kuchaytirish, shuningdek axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan huquqbuzarliklarning oldini olish bo‘yicha qo‘shimcha normalar joriy etildi. Jumladan, to‘lov tizimlari operatorlarining xavfsizlik rejimi buzilishi holatlari to‘g‘risida Markaziy bankka zudlik bilan xabar berish majburiyati mustahkamlandi.

Kadrlar tayyorlash yo‘nalishida ham muhim qadamlar qo‘yilgan: kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha alohida davlat dasturi qabul qilingan, oliy ta’lim muassasalarida axborot xavfsizligi, kiberxavfsizlik injiniringi va kriptografiya yo‘nalishlari bo‘yicha yuqori malakali mutaxassislar tayyorlash tizimi yo‘lga qo‘yilgan, shuningdek axborot xavfsizligi bo‘yicha kasbiy standart ishlab chiqilgan. Shunga qaramay, mavjud huquqiy baza

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

asosan texnik va infratuzilmaviy kiberxavfsizlikka qaratilgan bo‘lib, ijtimoiy ong darajasida namoyon bo‘ladigan manipulyativ-psixologik tahdidlarni – dezinformatsiya, deepfake kontent va ijtimoiy muhandislikni tartibga solishga qaratilgan maxsus mexanizmlar hali yetarlicha shakllanmagan. Bu holat qonunchilikni yanada takomillashtirish zaruratini keltirib chiqaradi.

Manipulyativ axborot tahdidlari deganda shaxs, ijtimoiy guruh yoki jamiyatning ongi, hissiyoti va qaror qabul qilish jarayoniga yashirin, ko‘pincha aldov yoki ishontirish usullari orqali maqsadli ta’sir ko‘rsatishga qaratilgan axborot ta’sirlari tushuniladi. Zamonaviy sharoitda ularning quyidagi asosiy shakllarini ajratish mumkin:

- Dezinformatsiya va soxta yangiliklar – ijtimoiy tarmoqlar va messenjerlar orqali tarqatiladigan, ataylab noto‘g‘ri yoki chalg‘ituvchi ma’lumotlar bo‘lib, ijtimoiy keskinlikni kuchaytirish yoki jamoatchilik fikrini boshqarish maqsadida qo‘llaniladi;
- Sun’iy intellekt asosidagi deepfake texnologiyalari – video va audio kontentni soxtalashtirish orqali real shaxslarning nomidan soxta bayonotlar yaratish imkonini beradi, bu esa an’anaviy tekshirish usullarining samaradorligini pasaytiradi;
- Ijtimoiy muhandislik va fishing hujumlari – foydalanuvchilarning ishonchidan foydalangan holda maxfiy ma’lumotlarni (parollar, moliyaviy rekvizitlar) egallashga qaratilgan psixologik manipulyatsiya usullari;
- Bot tarmoqlari va koordinatsiyalashgan noaniq xatti-harakatlar (CIB) – ijtimoiy tarmoqlarda sun’iy ravishda muayyan fikrni ustunlashtirish yoki muhokamani chalg‘itish maqsadida yaratiladigan avtomatlashtirilgan akkauntlar tizimi;

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

- Transchegaraviy gibrid ta’sir – milliy axborot maydonidan tashqarida joylashgan manbalar tomonidan davlat siyosati, ijtimoiy barqarorlik yoki milliy qadriyatlarga qaratilgan maqsadli axborot kampaniyalari.

Ushbu tahdidlarning umumiy xususiyati shundaki, ular ko‘pincha texnik jihatdan qonuniy vositalar (ijtimoiy tarmoq platformalari, messenjerlar, ochiq sun’iy intellekt xizmatlari) orqali amalga oshiriladi, bu esa ularni faqat texnik-huquqiy vositalar bilan cheklashni murakkablashtiradi va kompleks huquqiy, texnologik hamda ta’lim-tarbiyaviy yondashuvni talab qiladi.

O‘tkazilgan tahlil shuni ko‘rsatadiki, O‘zbekistonda axborot xavfsizligi tizimining institutsional asoslari izchil rivojlanmoqda, biroq manipulyativ tahdidlarga qarshi kurashish samaradorligini oshirish uchun bir qator yo‘nalishlarda takomillashtirish talab etiladi:

Birinchidan, huquqiy jihatdan dezinformatsiya va sun’iy intellekt yordamida yaratilgan soxta kontentning huquqiy maqomini aniq belgilovchi normalar hali to‘liq shakllanmagan. Bu ayniqsa, saylov jarayonlari, moliyaviy bozorlar va favqulodda vaziyatlar davrida yuzaga keladigan dezinformatsiya xavfini kuchaytiradi.

Ikkinchidan, institutsional jihatdan kiberxavfsizlik sohasidagi vakolatli organlar asosan texnik infratuzilmani himoya qilishga ixtisoslashgan bo‘lib, ijtimoiy tarmoqlardagi manipulyativ kontentni monitoring qilish va unga tezkor javob berish bo‘yicha maxsus mexanizmlarni fuqarolik jamiyati institutlari, ommaviy axborot vositalari va ta’lim tizimi bilan chambarchas bog‘liq holda yanada rivojlantirish zarurati mavjud.

Uchinchidan, kadrlar salohiyati borasida ijobiy siljishlarga qaramay (kriptologiya va kiberxavfsizlik yo‘nalishlari bo‘yicha ta’lim dasturlarining

kengaytirilishi), aholining, xususan yoshlarning, raqamli va media savodxonlik darajasini oshirish bo‘yicha tizimli, uzluksiz dasturlar yetarli emas. Aynan past media savodxonlik darajasi manipulyativ ta’sirlarga nisbatan zaiflikning asosiy omillaridan biri hisoblanadi.

To‘rtinchidan, transchegaraviy xususiyatga ega bo‘lgan tahdidlarga qarshi kurashish milliy chegaralar doirasida cheklangan samaradorlikka ega bo‘lib, xalqaro va mintaqaviy hamkorlik mexanizmlarini jumladan, tajriba almashish, birgalikda monitoring va tezkor axborot almashinuvi tizimlarini kengaytirish talab etiladi.

1) “Kiberxavfsizlik to‘g‘risida”gi Qonunga sun’iy intellekt yordamida yaratilgan soxta audiovizual kontent (deepfake) va koordinatsiyalashgan dezinformatsiya kampaniyalariga oid tushunchalarni aniq belgilovchi qo‘shimcha va o‘zgartirishlar kiritish;

2) Davlat organlari, OAV va IT-kompaniyalar ishtirokida dezinformatsiyaga qarshi tezkor faktlarni tekshirish (fakt-cheking) tarmog‘ini institutsionallashtirish;

3) Umumta’lim va oliy ta’lim tizimida raqamli va media savodxonlikni uzluksiz shakllantiruvchi maxsus fanlar va modullarni joriy etish;

4) Davlat xizmatchilari va muhim infratuzilma xodimlari uchun ijtimoiy muhandislik va fishing hujumlariga qarshi turish bo‘yicha muntazam malaka oshirish tizimini yo‘lga qo‘yish;

5) Manipulyativ tahdidlar monitoringi va ularga javob berish bo‘yicha xalqaro tashkilotlar hamda qo‘shni davlatlar bilan institutsional hamkorlikni kengaytirish;

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

6) Fuqarolarning kiberhodisalar va dezinformatsiya holatlari to‘g‘risida xabar berishini soddalashtiruvchi yagona milliy platforma yaratish.

Xulosa

O‘tkazilgan tadqiqot natijalari shuni ko‘rsatadiki, O‘zbekiston Respublikasida axborot xavfsizligini ta’minlashning huquqiy-institutsional tizimi so‘nggi yillarda izchil rivojlantirilib, kiberxavfsizlik sohasidagi asosiy me’yoriy-huquqiy hujjatlar va vakolatli organlar faoliyati barqarorlashtirildi. Shu bilan birga, raqamli transformatsiya va sun’iy intellekt texnologiyalarining jadal rivojlanishi manipulyativ axborot tahdidlarining yangi, murakkab shakllarini keltirib chiqarmoqda, bu esa mavjud huquqiy va institutsional mexanizmlarni doimiy ravishda takomillashtirib borishni taqozo etadi. Dezinformatsiya, deepfake texnologiyalari, ijtimoiy muhandislik va koordinatsiyalashgan bot faoliyatiga qarshi samarali kurashish faqat texnik-huquqiy choralar bilan emas, balki jamiyatning raqamli savodxonligini oshirish, institutsional hamkorlikni mustahkamlash va xalqaro tajribani integratsiya qilish orqaligina ta’minlanishi mumkin. Ishlab chiqilgan tavsiyalar milliy axborot xavfsizligi tizimini yanada takomillashtirishga xizmat qilishi va mazkur yo‘nalishdagi keyingi ilmiy tadqiqotlar uchun asos bo‘lib xizmat qilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764-son, 2022-yil 15-aprel. // lex.uz.

2. O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasi axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish chora-tadbirlari to‘g‘risida”gi Farmoni, PF-6007-son, 2020-yil 15-iyun.

3. O‘zbekiston Respublikasi Prezidentining “O‘zbekistonda kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi Qarori, PQ-4751-son, 2020-yil 15-iyun.

4. O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori, PQ-167-son, 2023-yil 31-may.

5. O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risidagi Nizom, 2023-yil 22-sentabr, 3458-son.

6. O‘zbekiston Respublikasining “Kiberxavfsizlikni ta’minlash sohasidagi qonunchilik takomillashtirilishi munosabati bilan ayrim qonun hujjatlariga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi Qonuni, O‘RQ-964-son, 2024-yil 20-sentabr.

7. O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori, PQ-293-son, 2024-yil 15-avgust.

8. Axborot xavfsizligi bo‘yicha kasbiy standart. Milliy malaka tizimi materiallari. // mmtri.uz.

9. International Telecommunication Union (ITU). Global Cybersecurity Index — rasmiy hisobotlar materiallari.

Issue - 7(2026) / ISSN 3030-3052 Available at www.uznauka.uz

10. European Union Agency for Cybersecurity (ENISA). Threat Landscape — yillik tahliliy hisobotlar.