SCIENCE HUB REVIEW
2026
Volume 1
Issue 5
www.sciencehubreview.uz
ILMIY ELEKTRON JURNAL

KIBERXAVFSIZLIK VA MUHIM AXBOROT INFRATUZILMASINI HIMOYA QILISHNING HUQUQIY ASOSLARI

Davlatov Ag‘abek Misir o‘g‘li

Toshkent davlat yuridik universiteti magistranti, Sport huquqi yo‘nalishi

Annotatsiya

Mazkur tezisda kiberxavfsizlik va muhim axborot infratuzilmasini himoya qilishning huquqiy asoslari milliy qonunchilik hamda xalqaro standartlar bilan qiyosiy tahlil qilinadi. Muhim axborot infratuzilmasi tushunchasi, uning subyektlari zimmasidagi majburiyatlar, shaxsga doir ma’lumotlarni himoya qilish, kiberhodisalar haqida xabar berish va javobgarlik masalalariga e’tibor qaratiladi. Yevropa Ittifoqining NIS 2 direktivasi, NIST Cybersecurity Framework 2.0 va ISO/IEC 27001:2022 standarti tajribasi o‘rganilib, O‘zbekiston qonunchiligidagi mavjud bo‘shliqlar aniqlanadi hamda milliy tartibga solish tizimini takomillashtirishga doir takliflar asoslantiriladi.

Kalit so‘zlar

kiberxavfsizlik, muhim axborot infratuzilmasi, kiberhodisa, shaxsga doir ma’lumotlar, risklarni boshqarish, ta’minot zanjiri, NIS 2, ISO/IEC 27001, huquqiy javobgarlik.

Kirish

Raqamli transformatsiya sharoitida davlat boshqaruvi, bank-moliya, energetika, transport, sog‘liqni saqlash va aloqa tizimlari o‘zaro bog‘langan yagona axborot muhitiga aylanmoqda. Bunday tizimlar xizmatlar samaradorligini oshirsa-da, ularning ishdan chiqishi yoki noqonuniy egallanishi jiddiy ijtimoiy-iqtisodiy oqibatlarga olib kelishi mumkin. Elektr ta’minoti dispetcherlik tizimiga hujum ishlab chiqarishni to‘xtatishi, bank to‘lov infratuzilmasidagi uzilish fuqarolarning mablag‘lardan foydalanishiga to‘sqinlik qilishi, shifoxona axborot tizimining bloklanishi esa bemorlar hayotiga xavf tug‘dirishi mumkin.

Shu bois kiberxavfsizlik faqat texnik mutaxassislar vazifasi bilan cheklanmaydi. U davlatning konstitutsiyaviy majburiyatlari, inson huquqlari, iqtisodiy barqarorlik, milliy xavfsizlik va tashkilotlarning yuridik javobgarligi bilan chambarchas bog‘liqdir. Mazkur

munosabatlarni tartibga soluvchi asosiy maxsus hujjat O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni hisoblanadi. Tadqiqotda normativ-huquqiy tahlil, qiyosiy-huquqiy yondashuv va vaziyatli tahlil usullaridan foydalanildi.

Kiberxavfsizlik va muhim axborot infratuzilmasi tushunchasi

Kiberxavfsizlik axborot tizimlari, tarmoqlar va resurslarni kiberhujumlar hamda boshqa kiberxavflardan himoya qilishga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik va kriptografik choralar majmuasidir. O‘RQ-764-son Qonun kiberhimoyani hodisalarning oldini olish, hujumlarni aniqlash va ularga qarshi choralar ko‘rish, oqibatlarni bartaraf etish hamda tizimlar barqarorligini tiklash bilan bog‘laydi. Muhim axborot infratuzilmasi esa strategik va ijtimoiy-iqtisodiy ahamiyatga ega avtomatlashtirilgan boshqaruv tizimlari, axborot tizimlari, resurslar, tarmoqlar va texnologik jarayonlar majmuasini anglatadi.

Mazkur obyektlarning ahamiyati faqat ma’lumotlar maxfiyligida emas, balki ularning yaxlitligi va xizmatlarning uzluksizligida ham namoyon bo‘ladi. Axborot xavfsizligining klassik modeli maxfiylik, yaxlitlik va mavjudlik maqsadlarini ajratadi. J. Saltzer va M. Schroeder eng kam vakolat berish, himoya mexanizmlarini sodda saqlash va xavfsizlikni tizimni loyihalash bosqichidayoq hisobga olish tamoyillarini asoslagan. R. Anderson esa xavfsizlikni insonlar, texnologiya, iqtisodiy rag‘batlar va tashkiliy jarayonlar o‘zaro ta’sir qiladigan yaxlit tizim sifatida tahlil qiladi. Bu qarashlar huquqiy talablarni texnik va tashkiliy boshqaruv bilan uyg‘unlashtirish zarurligini ko‘rsatadi.

Xalqaro tartibga solishning asosiy yo‘nalishlari

Xalqaro amaliyotda muhim infratuzilmani himoya qilish majburiy normalar va ixtiyoriy standartlar uyg‘unligiga asoslanadi. Yevropa Ittifoqining 2022-yil 14-dekabrdagi 2022/2555-son NIS 2 direktivasi kiberxavflarni boshqarish, rahbariyatning shaxsiy mas’uliyati, ta’minot zanjiri xavfsizligi va hodisalar haqida bosqichma-bosqich xabar berish talablarini kuchaytirdi. Ushbu yondashuvning o‘ziga xosligi shundaki, kiberxavfsizlik uchun javobgarlik IT bo‘limidan boshqaruv organlari darajasiga ko‘tariladi.

AQShda 2024-yilda qabul qilingan NIST Cybersecurity Framework 2.0 kiberxavflarni boshqarish (Govern), aniqlash (Identify), himoyalash (Protect), kuzatish (Detect), javob qaytarish (Respond) va tiklash (Recover) funksiyalari orqali tizimlashtiradi. ISO/IEC 27001:2022 standarti esa axborot xavfsizligini boshqarish tizimini yaratish, joriy etish va doimiy takomillashtirish talablarini belgilaydi. Mazkur hujjatlar yumshoq huquq xususiyatiga ega bo‘lsa-da, tashkilotlarning ichki siyosati va nazorat choralarini rejalashtirishda muhim mezon vazifasini bajaradi.

Qiyosiy tahlil shuni ko‘rsatadiki, Yevropa Ittifoqi modeli majburiy talablar va ma’muriy sanksiyalarga, AQSh modeli esa ko‘proq ixtiyoriy standartlar va davlat-xususiy sheriklikka tayanadi. B. Schneier ta’kidlaganidek, raqamli xavfsizlikni faqat texnik mexanizmlar bilan cheklab bo‘lmaydi: inson xulqi, ishonch va tashkiliy jarayonlar ham himoyaning tarkibiy qismidir. Demak, samarali tartibga solish qonuniy majburiyatlar, boshqaruv madaniyati va texnik nazoratni birlashtirishi lozim.

O‘zbekiston qonunchiligining holati va mavjud muammolar

O‘zbekistonda kiberxavfsizlikning huquqiy negizini O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonun, 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun hamda 2003-yil 11-dekabrdagi 560-II-son “Axborotlashtirish to‘g‘risida”gi Qonun tashkil etadi. O‘RQ-764-son Qonunda qonuniylik, kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi, yagona yondashuv va xalqaro hamkorlikka ochiqlik tamoyillari mustahkamlangan. Shuningdek, muhim axborot infratuzilmasi obyektlari uchun alohida himoya yo‘nalishlari va kiberxavfsizlik hodisalari haqida vakolatli organga xabar berish majburiyati belgilangan.

Kiberhodisalar ko‘pincha shaxsga doir ma’lumotlar bilan bog‘liq bo‘ladi. O‘RQ-547-son Qonun ma’lumotlarni qonuniy maqsadda qayta ishlash, ularning maxfiyligi va himoyalanganligini ta’minlash talablarini belgilaydi. Masalan, tibbiyot muassasasining elektron bazasidan bemorlarning tashxislari yoki genetik tahlil natijalari o‘g‘irlansa, bu faqat texnik nosozlik emas, balki fuqarolarning shaxsiy hayotiga daxl qiluvchi huquqbuzarlikdir. Davlat xizmatlari portalida ma’lumotlar bazasining noto‘g‘ri sozlanishi natijasida shaxsiy ma’lumotlarning ochiq internetda ko‘rinib qolishi ham shunday oqibatlarga olib keladi.

Biroq tahlil amaldagi qonunchilikda bir qator muammolar mavjudligini ko‘rsatadi. Birinchidan, muhim axborot infratuzilmasi subyektlari uchun tarmoqlar kesimidagi minimal xavfsizlik talablari va ularning bajarilishini tekshirish mezonlari yetarlicha aniq emas. Ikkinchidan, hodisalar haqida xabar berishning muddatlari, kanallari va dastlabki ma’lumotlar tarkibi amaliyot uchun to‘liq tushunarli tarzda belgilanmagan. Uchinchidan, Qonunda talablarni buzgan shaxslar qonunchilikda belgilangan tartibda javob berishi nazarda tutilgan bo‘lsa-da, rahbariyatning shaxsiy mas’uliyati va pudratchilar orqali yuzaga keladigan ta’minot zanjiri xavflari uchun javobgarlik alohida tartibga solinmagan.

Milliy qonunchilikni takomillashtirish bo‘yicha takliflar

O‘tkazilgan qiyosiy tahlil asosida, avvalo, energetika, bank-moliya, sog‘liqni saqlash va transport sohalarining xususiyatlarini hisobga olgan holda muhim axborot infratuzilmasi subyektlari uchun xavfga asoslangan minimal kiberxavfsizlik talablari va tekshirish mezonlarini belgilash maqsadga muvofiq. Bunda talablar obyektning ahamiyati va xavf darajasiga mutanosib bo‘lishi ortiqcha ma’muriy yukning oldini oladi.

Ikkinchidan, kiberhodisalar haqida xabar berish tartibini NIS 2 direktivasi tajribasiga muvofiq bosqichma-bosqich modelda belgilash taklif etiladi: dastlabki ogohlantirish, batafsil xabar va yakuniy hisobot. Tezkor xabar berish aybni avtomatik tan olish emas, balki zararni kamaytirish va boshqa tizimlarni ogohlantirish vositasi ekanligi qonunda aniq ifodalanishi lozim.

Uchinchidan, rahbariyat nazoratini kuchaytirish zarur. Kiberxavfsizlik byudjeti, xavflar reyestri, mustaqil audit, xodimlar treningi va zaxira nusxalardan tiklash sinovlari boshqaruv organlari darajasida muntazam ko‘rib chiqilishi kerak. To‘rtinchidan, muhim infratuzilma subyektlarining pudratchilar bilan tuziladigan shartnomalarida xavfsizlik talablari, hodisa haqida tezkor xabar berish, auditga ko‘maklashish va dalillarni saqlash majburiyatlarini majburiy shart sifatida belgilash lozim.

Beshinchidan, davlat va xususiy sektor o‘rtasida tahdidlar haqida tezkor va xavfsiz axborot almashish mexanizmlarini rivojlantirish, bunda tijorat siri, shaxsga doir ma’lumotlar va davlat sirlarini himoya qilish kafolatlarini saqlash muhimdir. Oltinchidan, huquqshunoslar, IT mutaxassislari va rahbarlar uchun kiberhodisalarga javob berish bo‘yicha qo‘shma o‘quv mashg‘ulotlarini tashkil etish taklif etiladi. Ushbu takliflar

“O‘zbekiston — 2030” strategiyasi doirasidagi raqamli transformatsiya islohotlari bilan uyg‘un holda amalga oshirilishi maqsadga muvofiq.

Xulosa

Xulosa qilib aytganda, kiberxavfsizlik va muhim axborot infratuzilmasini himoya qilish davlat xavfsizligi, inson huquqlari va iqtisodiy barqarorlikning ajralmas qismidir. O‘zbekistonda ushbu sohaning asosiy huquqiy tayanchi “Kiberxavfsizlik to‘g‘risida”gi Qonun bo‘lib, shaxsga doir ma’lumotlar va axborotlashtirishga oid qonunlar uni to‘ldiradi. Shu bilan birga, samarali himoya faqat huquqiy hujjat yoki texnik vosita bilan ta’minlanmaydi: u xavflarni muntazam baholash, vakolatlarni cheklash, zaxira nusxalar, hodisaga javob berish, xodimlarni o‘qitish, pudratchilarni nazorat qilish va rahbariyat hisobdorligini o‘z ichiga olishi zarur. Minimal talablar va tekshirish mezonlarini joriy etish, xabar berish tartibini aniqlashtirish hamda NIST va ISO yondashuvlaridan metodik asos sifatida foydalanish milliy qonunchilikning xalqaro standartlarga yaqinlashishiga xizmat qiladi. Bunda tartibga solishning asosiy maqsadi tashkilotlarga ortiqcha yuk yaratish emas, balki xizmatlar barqarorligi va fuqarolar huquqlarini real himoya qiluvchi aniq, shaffof va prognoz qilinadigan huquqiy muhitni shakllantirishdan iborat.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni.

2. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni.

3. O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-son “Axborotlashtirish to‘g‘risida”gi Qonuni.

4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).

5. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, 2024.

6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.

7. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis: Wiley, 2020.

8. Schneier B. Secrets and Lies: Digital Security in a Networked World. New York: Wiley, 2000.

9. Saltzer J. H., Schroeder M. D. The Protection of Information in Computer Systems // Proceedings of the IEEE. 1975. Vol. 63, No. 9. P. 1278–1308.