TELEKOMMUNIKATSIYA SOHASIDA KIBERXAVFLARNI BOSHQARISHNING XORIJIY MODELLARI

ISLOMOV DILMUROD FAXRIDDIN O‘G‘LI
“O‘zbektelekom” AK Birinchi bo‘lim bosh mutaxassisi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti magistranti
+998990600060
e-mail: d.islomov@utc.uz

ANNOTATSIYA: *Ushbu ish telekommunikatsiya sohasida kiberxavflarni aniqlash, baholash va boshqarish bo‘yicha xorijiy mamlakatlarda qo‘llanilayotgan metod va strategiyalarni tahlil qiladi. Ishda kiberxavfning iqtisodiy va texnologik oqibatlari, turli mamlakatlarning standart va normativ hujjatlari, shuningdek xavflarni boshqarishning xalqaro tajribalari ko‘rib chiqiladi. Xorijiy modellarda kiberxavfni aniqlash uchun risklarni baholash tizimlari, monitoring vositalari, shuningdek kiberxavfsizlik siyosatini shakllantirish mexanizmlari o‘rganilgan. Ish telekommunikatsiya kompaniyalarida xavflarni minimallashtirish va iqtisodiy zararlarni kamaytirish bo‘yicha amaliy tavsiyalar beradi.*

Kalit so‘zlar: *kiberxavf, boshqaruv modeli, telekommunikatsiya, riskni baholash, xavfsizlik strategiyasi, monitoring tizimi, xalqaro standart, iqtisodiy zarar.*

Telekommunikatsiya sohasida kiberxavflar global darajada tobora ortib borayotgan tahdid sifatida e’tirof etilmoqda. Xorijiy mamlakatlar amaliyotida kiberxavfni boshqarish tizimlari yuqori texnologik infratuzilma, xavfsizlik protokollari va risklarni baholash mexanizmlariga asoslangan holda shakllantiriladi. Ushbu tizimlarning asosiy maqsadi axborot va

kommunikatsiya resurslarini himoya qilish, iqtisodiy zararlarni minimallashtirish va xizmatlarning uzluksizligini ta’minlashdir.

Xorijiy mamlakatlarda ishlab chiqilgan boshqaruv modellari odatda uch bosqichni o‘z ichiga oladi: xavflarni aniqlash va klassifikatsiyalash, monitoring va baholash, shuningdek xavfsizlik siyosatini amalga oshirish. Shuningdek, bu modellarda xalqaro standartlar va normativ-huquqiy hujjatlar asosida kompaniyalar va davlat organlari o‘rtasida hamkorlik muhim ahamiyatga ega.

Ushbu ishda telekommunikatsiya sohasida qo‘llanilayotgan xorijiy boshqaruv modellari tahlil qilinib, ularning samaradorligi, kuchli va zaif tomonlari aniqlanadi. Shuningdek, kiberxavflarning iqtisodiy oqibatlari va ularni boshqarish bo‘yicha amaliy tavsiyalar ishlab chiqiladi.

Telekommunikatsiya tarmoqlaridagi kiberxavflar global miqyosda butun dunyo davlatlari va korxonalar e’tibor markaziga aylangan. Axborot infratuzilmasining raqamlashtirilishi va onlayn xizmatlar kengaygan sari telekommunikatsiya tizimlariga bo‘lgan tahdidlar ham murakkablashib, ularning iqtisodiy salbiy oqibatlari sezilarli darajada ortmoqda. Shu sababli xorijiy mamlakatlarda kiberxavflarni boshqarish modellari tizimli, ilmiy asoslangan va global standartlarga muvofiq shakllantirilgan. Ushbu yondashuvlar nafaqat texnik himoya choralarini, balki strategik va iqtisodiy boshqaruv mexanizmlarini ham o‘z ichiga oladi.

O‘zbekiston Respublikasining amaldagi qonunchiligi bu jarayonni tartibga solish uchun asosiy huquqiy bazani yaratadi. Xususan, O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni telekommunikatsiya va axborot tarmoqlarida kiberxavfsizlikni hukumat siyosati darajasida tartibga soladi va kiberhujumlarga qarshi chora-tadbirlarni belgilaydi. Qonunda kiberxavfsizlik subyektlari uchun yuridik talablar qat’iy ko‘rsatilib, bu sohada milliy me’yorlar belgilangan. Qonun, shuningdek, kiberxavflarni aniqlash,

oldini olish va bartaraf etishga qaratilgan nazorat mexanizmlarini ham ta’minlaydi.

Telekommunikatsiya sohasida kiberxavflarni boshqarishning xorijiy modellari ko‘pincha xavfni boshqarish (risk management) tamoyili atrofida shakllanadi. Masalan, xalqaro miqyosda tan olingan NIST Cybersecurity Framework (AQSh Milliy Standartlar va Texnologiya Instituti modeli) xavfni boshqarishning beshta asosiy funktsiyasini belgilaydi aniqlash, himoya qilish, aniqlash (detect), javob berish va tiklash (recover). Bu yondashuv telekommunikatsiya infratuzilmasidagi tahdidlarni tizimli aniqlash, ularni iqtisodiy jihatdan baholash va rejalashtirilgan chora-tadbirlar orqali yo‘qotishlarni minimallashtirishga xizmat qiladi.

Shuningdek, xalqaro standartlar qatorida ISO/IEC 27001 axborot xavfsizligi boshqaruv tizimi modeli mavjud bo‘lib, u kompaniya ichida xavfsizlik siyosati, resurslar boshqaruvi, texnik va tashkiliy choralarni birlashtiradi. Bu standartning telekommunikatsiya kompaniyalarida tatbiqi ularning raqamli xizmatlar infratuzilmasining mustahkamligini ta’minlashga xizmat qiladi va iqtisodiy yo‘qotishlar ehtimolini kamaytiradi.

Xorijiy tajribada ko‘plab davlatlarda ITU-T standartlari (masalan, X.1205 kabi tavsiyalar) telekommunikatsiya infratuzilmasidagi kibertahdidlarni tasniflash, ularni aniqlash va tasvirlash uchun texnik yondashuvlarni belgilaydi. Ushbu standartlar telekommunikatsiya operatorlariga global xavfsizlik yondashuvlarini o‘z faoliyatiga integratsiyalash imkonini beradi, shu bilan birga raqamli xizmatlarning uzluksizligi va ishonchliligini ta’minlaydi.

Xalqaro tajribada yana bir muhim yondashuv bu ”Zero Trust Architecture” (nol ishonch arxitekturasi), unda foydalanuvchi va qurilmalar uchun default bo‘yicha ishonch belgilanmaydi, har bir kirish va harakat maxsus tekshiriladi. Ushbu yondashuv telekommunikatsiya tizimlarida juda muhim, chunki u ichki hamda tashqi tahdidlarni aniqlash va oldini olishni kuchaytiradi.

O‘zbekiston qonunchiligi va xalqaro modellarning uyg‘unligi telekommunikatsiya tizimlari uchun samarali kiberxavf boshqaruvi tizimini yaratishga xizmat qiladi. Milliy qonunchilik axborot tizimlarini himoya qilish bo‘yicha huquqiy mexanizmlarni beradi, xalqaro standartlar esa texnik va boshqaruv yondashuvlari uchun global me’yorlarni ta’minlaydi. Xorijiy modellarning tatbiqi telekommunikatsiya subyektlarida kiberxavflarni aniqlash va ularga qarshi chora ko‘rishning yuqori samaradorligini ta’minlab, iqtisodiy zararlarni sezilarli darajada kamaytirishga yordam beradi.

Jarayon bosqichi	Amaliy faoliyat	Texnik va boshqaruv vositalari	Natija va iqtisodiy ta’sir
Xavfni aniqlash	Telekom operatori tarmog‘idagi barcha faol xizmatlarni, foydalanuvchi qurilmalarini va server infratuzilmasini kuzatadi	NIST Risk Assessment metodikasi, log monitoring, ITU-T tavsiyalari	Potentsial kiberxavflar aniqlanadi, ularning iqtisodiy salbiy oqibatlari hisoblanadi
Tahdidlarni tasniflash	Aniqlangan xavflarni turkumlash, jiddiyligi va ta’sir doirasini belgilash	ISO/IEC 27001 xavfsizlik standartlari, xavf matritsasi	Kiberhujum ehtimoli va moliyaviy yo‘qotishlar aniqlanadi, resurslarni maqsadli yo‘naltirish mumkin
Oldini olish va himoya qilish	Tarmoqlarda xavfsizlik protokollarini joriy etish, foydalanuvchi autentifikatsiyasi va kirish nazoratini tashkil qilish	Zero Trust Architecture, firewall, antivirus va intrusion detection tizimlari	Kiberhujumlarning oldini olish orqali moliyaviy yo‘qotishlar kamayadi, xizmatlarning uzluksizligi ta’minlanadi

Jarayon bosqichi	Amaliy faoliyat	Texnik va boshqaruv vositalari	Natija va iqtisodiy ta’sir
Javob berish	Xavf yuzaga kelganda zudlik bilan chora ko‘rish, tizimni tiklash	Incident Response Plan, ISO/IEC 27035 bo‘yicha amaliyot	Xizmatlar tiklanadi, kiberhujum natijasida iqtisodiy zarar minimallashtiriladi
Monitoring va baholash	Har bir xavfsizlik chorasining samaradorligini doimiy nazorat qilish va tahlil qilish	SIEM tizimlari, audit tekshiruvlari, xalqaro standartlar bo‘yicha hisobot	Kiberxavfsizlikning samaradorligi baholanadi, keyingi investitsiya va strategiyalar aniqlanadi
Takomillashtirish	Xavfsizlik protokollarini yangilash, yangi texnologiyalarni joriy qilish	ISO/IEC 27001 yangilanishlari, AI va ML asosidagi xavf aniqlash tizimlari	Kiberxavfsizlikning barqarorligi oshadi, iqtisodiy zarar xavfi minimalga tushadi

Izoh: Jadval O‘zbekiston Respublikasi qonunchiligi va xalqaro standartlarga mos ravishda tayyorlandi. Har bir jarayon amaliy va iqtisodiy jihatdan telekommunikatsiya subyektlari uchun aniq foyda beradi. Xavflarni aniqlash va ularning oldini olishga qaratilgan choralar operatorlar uchun xizmatlarning uzluksizligi va moliyaviy barqarorlikni kafolatlaydi.

XULOSA

Telekommunikatsiya sohasida kiberxavflarni boshqarishning xorijiy modellari operatorlar va xizmat ko‘rsatuvchi tashkilotlar uchun zamonaviy xavfsizlikni ta’minlashda muhim o‘rin tutadi. Ushbu modellarda xavfni aniqlash, tasniflash, oldini olish, javob berish, monitoring va takomillashtirish jarayonlari tizimli va bosqichma-bosqich amalga oshiriladi.

Xorijiy tajribalar ko‘rsatadiki, xavfni aniqlash va tasniflashning ilmiy asoslangan metodlari iqtisodiy yo‘qotishlarni minimal darajada ushlab turadi,

investitsiya samaradorligini oshiradi va operatorning xizmat uzluksizligini kafolatlaydi. Oldini olish va himoya qilish choralarini joriy etish orqali kiberhujumlarning salbiy ta’siri kamayadi, moliyaviy va obro‘ risklari nazorat ostiga olinadi.

Javob berish va tizimni tiklash jarayonlari esa operatorning muhim aktivlarini himoya qiladi, xizmatlar uzluksizligini ta’minlaydi va ishonchlilikni oshiradi. Monitoring va baholash bosqichlari kiberxavfsizlik tizimining samaradorligini doimiy ravishda tahlil qilish imkonini yaratadi, shu bilan birga keyingi chora-tadbirlar va investitsion qarorlarni maqsadli qabul qilishni ta’minlaydi.

Shu bilan birga, xorijiy modellarda kiberxavfsizlikni boshqarish jarayonida texnologik va iqtisodiy komponentlar birgalikda qo‘llaniladi. Bu operatorlar uchun strategik ustunlikni ta’minlaydi, xatarlarni kamaytiradi va telekommunikatsiya xizmatlarining sifatini oshiradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. **O‘zbekiston Respublikasi Prezidenti qarori** “Axborot xavfsizligini ta’minlash chora-tadbirlari to‘g‘risida”, O‘zbekiston Respublikasi qonun hujjatlari, 2020 yil, 12 may.

2. **O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi** “Telekommunikatsiya sohasida kiberxavfsizlikni boshqarish tizimi bo‘yicha tavsiyalar”, Tashkent, 2021 yil, 8 sentabr.

3. **Lex.uz portali** “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash bo‘yicha qonun va me’yoriy hujjatlar to‘plami”, rasmiy elektron manba, 2022 yil, 3 fevral.

4. **O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori** “Telekommunikatsiya tarmoqlarida xavfsizlikni kuchaytirish va kiberxavflarga qarshi chora-tadbirlar to‘g‘risida”, Tashkent, 2019 yil, 25 oktyabr.