AXBOROT XAVFSIZLIGI VA KIBER TAHDIDLAR: DOLZARB MUAMMOLAR VA YECHIMLAR

Axmedova Nilufar Farxodovna
Qarshi davlat texnika universiteti Kompyuter tizimlarining texnik va dasturiy ta’minoti kafedrasi dotsenti
Abilov Arslon Alisher o‘g‘li
Qarshi davlat texnika universiteti Telekommunikatsiya texnologiyalari yo’nalishi 1-bosqich talabasi

Annotatsiya: *Mazkur maqolada zamonaviy jamiyatda axborot xavfsizligini ta’minlash masalalari, kiber tahdidlarning turlari hamda ularning ijtimoiy-iqtisodiy hayotga ta’siri tahlil qilinadi. Muallif foydalanuvchilar, tashkilotlar va davlatlarning axborot himoyasi sohasidagi dolzarb muammolarini ko‘rsatib, ularga amaliy yechimlar taklif etadi.*

Kalit so‘zlar: *axborot xavfsizligi, kiber tahdid, kiber jinoyat, ma’lumotlarni himoya qilish, raqamli xavfsizlik, kiber madaniyat.*

XXI asr — bu raqamli inqilob asridir. Hozirgi kunda insoniyat hayotining deyarli barcha jabhalari internet va axborot texnologiyalariga bog‘langan. Elektron hukumat tizimlari, onlayn to‘lovlar, raqamli ta’lim va tibbiyot xizmatlari, hatto shaxsiy muloqot ham internet orqali amalga oshirilmoqda. Shu sababli, axborot xavfsizligini ta’minlash masalasi nafaqat texnik, balki milliy xavfsizlikning muhim tarkibiy qismi sifatida qaralmoqda.

O‘zbekiston Respublikasida raqamli transformatsiya jarayonlarining kengayishi, axborot-kommunikatsiya texnologiyalarining barcha sohalarga chuqur kirib borishi va kiber tahdidlarning murakkablashib borayotgani sharoitida kiber xavfsizlikni ta’minlash davlat siyosatining ustuvor yo‘nalishlaridan biriga aylandi. Shu munosabat bilan axborot makonini huquqiy tartibga soluvchi, kiber xavfsizlikning institutsional va tashkiliy asoslarini belgilab beruvchi “Kiberxavfsizlik to‘g‘risida”gi Qonunning qabul qilinishi muhim tarixiy voqea bo‘ldi. Mazkur hujjatning qabul qilinishi bosqichma-bosqich quyidagi tartibda amalga oshirilgan:

2022-yil 25-fevral — O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi tomonidan Qonun loyihasi ko‘rib chiqilib, ma’qullangan;

2022-yil 17-mart — Qonun O‘zbekiston Respublikasi Oliy Majlisi Senati tomonidan tasdiqlangan;

2022-yil 17-iyul — Qonun rasmiy tarzda kuchga kirgan va Respublika hududida majburiy ijro etilishi belgilangan.

Qonunning kuchga kirishi mamlakatda kiber xavfsizlikning huquqiy asoslarini mustahkamlab, axborot tizimlari, ma’lumotlar bazalari, telekommunikatsiya tarmoqlari hamda raqamli xizmatlarning himoyasini ta’minlashga qaratilgan kompleks mexanizmlarni joriy etdi. Ushbu hujjat davlat organlari, korxonalar, tashkilotlar va fuqarolarning kiber makondagi huquq va majburiyatlarini aniq belgilab, kiber tahdidlarning oldini olish, ularni aniqlash va bartaraf etish bo‘yicha yagona tizimli yondashuvni shakllantirdi.

Bundan tashqari, Qonun kiber insidentlarga munosabat bildirish tartibini, axborot xavfsizligi sohasida mas’ul organlarning vakolatlarini, shuningdek, shaxsiy ma’lumotlar

xavfsizligini ta’minlash bo‘yicha talablarni yanada kuchaytirdi. Kiber makonda yuzaga keladigan hujumlar, firibgarliklar, zararli dasturiy ta’minotlardan foydalanish holatlariga nisbatan javobgarlik choralari to‘liq huquqiy asosga ega bo‘ldi.

Umuman olganda, “Kiberxavfsizlik to‘g‘risida”gi Qonunning 2022-yilda qabul qilinishi O‘zbekiston Respublikasida axborot xavfsizligi bo‘yicha milliy siyosatni sifat jihatidan yangi bosqichga ko‘tardi. Mazkur normativ-huquqiy hujjat kiber makon barqarorligi, davlat va jamiyat manfaatlarini himoya qilish, shaxsiy ma’lumotlar daxlsizligini kafolatlash hamda xalqaro standartlarga mos kiber xavfsizlik infratuzilmasini shakllantirishda muhim omil bo‘lib xizmat qilmoqda.

Axborot xavfsizligi — bu foydalanuvchi yoki tashkilot ma’lumotlarining maxfiyligi, butunligi va mavjudligini ta’minlash jarayonidir. Ammo raqamli texnologiyalar rivojlanib borar ekan, u bilan bir qatorda kiber jinoyatlar ham ortmoqda. Har yili dunyo bo‘yicha milliardlab dollar miqdorida zarar yetkazadigan kiber hujumlar sodir etilmoqda.

1. Kiber tahdidlarning turlari va ularning oqibatlari. Kiber tahdidlar turli shaklda namoyon bo‘ladi:

Phishing (firibgarlik xabarlari) – foydalanuvchilarning login va parollarini o‘g‘irlashga qaratilgan xat yoki havolalar orqali amalga oshiriladi.

Virus va zararli dasturlar (malware, trojan) – kompyuter tizimiga kirib, ma’lumotlarni yo‘qotadi yoki ularni noqonuniy nusxalaydi.

DDoS hujumlar – serverlarni haddan tashqari yuklash orqali ularning ishlashini to‘xtatadi.

Ransomware – ma’lumotlarni shifrlab, ularni ochish uchun to‘lov talab qiluvchi dastur.

Bunday hujumlar nafaqat shaxsiy foydalanuvchilarga, balki davlat idoralariga, banklarga va korxonalarga ham jiddiy zarar yetkazadi. Masalan,

2021-yilda “Colonial Pipeline” kompaniyasiga qilingan kiber hujum natijasida AQShda bir necha kun davomida yoqilg‘i yetkazib berish tizimi ishdan chiqqan.

2. O‘zbekiston sharoitida axborot xavfsizligining dolzarbligi. O‘zbekiston ham raqamli transformatsiya bosqichida. “Raqamli O‘zbekiston – 2030” dasturi doirasida barcha sohalarda elektron xizmatlar joriy etilmoqda. Biroq bu jarayon bilan birga axborot xavfsizligi masalasi ham dolzarb muammoga aylangan. Ba’zi tashkilotlarda himoya tizimlari eskirgan, ma’lumotlar shifrlanmagan holda saqlanadi.

Fuqarolarning axborot madaniyati yetarli emasligi ham xavf omillaridan biridir. Masalan, foydalanuvchilarning katta qismi bir xil paroldan bir necha tarmoqda foydalanadi yoki shubhali havolalarni ochadi.

Kiber jinoyatlar haqida xabardorlik pastligi sababli ayrim holatlarda fuqarolar o‘z ma’lumotlarini o‘zlari oshkor etib qo‘yadilar. Shu bois, axborot xavfsizligi bo‘yicha ommaviy savodxonlikni oshirish dolzarb vazifaga aylanmoqda.

Texnik himoya vositalarining eskiligi – ayrim muassasalarda himoya dasturlari muntazam yangilanmaydi.

Mutaxassislar yetishmasligi – kiber xavfsizlik bo‘yicha malakali kadrlar soni kam.

Huquqiy bo‘shliqlar – kiber jinoyatlarni tergov qilish mexanizmlari hali to‘liq shakllanmagan.

Xalqaro hamkorlikning sustligi – ko‘plab jinoyatlar transchegaraviy xarakterga ega bo‘lib, ular bilan kurashish uchun xalqaro tajriba zarur.

4. Yechimlar va takliflar. Birinchidan, axborot xavfsizligi madaniyatini oshirish maqsadida maktab va oliy ta’lim tizimlarida maxsus kurslar, amaliy mashg‘ulotlar yo‘lga qo‘yilishi kerak. Ikkinchidan, davlat va xususiy sektor zamonaviy himoya vositalaridan foydalanishi lozim: antivirus dasturlari, ma’lumotlarni shifrlash, zaxira nusxalarini saqlash tizimlari. Uchinchidan, kiber xavfsizlik mutaxassislarini tayyorlash uchun alohida o‘quv markazlar tashkil etish zarur. To‘rtinchidan, qonunchilikni kuchaytirish va xalqaro hamkorlikni rivojlantirish kiber jinoyatlarga qarshi kurashni samarali qiladi

Shuningdek, ommaviy axborot vositalarida va ijtimoiy tarmoqlarda foydalanuvchilarga xavfsizlik bo‘yicha amaliy tavsiyalar berish muhimdir.

Xulosa o’rnida shuni ta’kidlash lozimki, axborot xavfsizligi – bu har bir inson, tashkilot va davlatning umumiy mas’uliyatidir. Kiber tahdidlarga qarshi kurash faqat texnologik emas, balki ma’naviy va huquqiy yondashuvni ham talab etadi.

Agar har bir foydalanuvchi o‘z shaxsiy ma’lumotlariga ehtiyotkorlik bilan yondashsa, tashkilotlar himoya tizimlarini muntazam yangilasa, va davlat bu yo‘nalishda qat’iy siyosat yuritsa — o‘shanda raqamli xavfsizlik barqaror bo‘ladi.

Zero, raqamli taraqqiyotning kafolati — xavfsiz, ishonchli va barqaror axborot muhitidir

Foydalanilgan adabiyotlar:

1. “Kiber xavfsizlik to‘g‘risidagi” qonun , kodeks 2022y

2. No’monov Sh., Doliyev G. — “Axborot xavfsizligi va internet madaniyati: tushunchasi va muammolari” — 2023y.

3. Toshpolatova I., Panjiyev O. — “Kiber xavfsizlikda shaxsiy ma’lumotlar himoyasi” — 27 May 2025y.

4. Kadirova D.I., Abdulxoshimov J.O. — “Rivojlangan raqamli texnologiyalar davrida shaxsiy ma’lumotlarning ahamiyati va xavfsizligi” — 15 Dec 2024y.

5. Ibragimova M.K. — “Kiberxavfsizlik, ma’lumotlarni himoya qilish” 2 Apr 2023y

6. Mirzaakbarov D.D., Alijonova B.V. — “Kiberxavfsizlik. Raqamli dunyoda himoyalanish usullari” — 14 Apr 2025y.

7. Karimov I.M., Turg’unov N.A. — “Axborot Xavfsizligi Asoslari”— 2016 y