AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY TAMOYILLARI VA USULLARI

Nusratillayev Madamin O‘ktam o‘g‘li, Razzoqov Ilhom Dovranovich

Qarshi davlat universiteti

nusratillayevmadamin@gmail.com

razzokov.id@qarshidu.uz

Annotatsiya. *Ushbu tezisda axborot xavfsizligini ta’minlashning zamonaviy tamoyillari va usullari qisqacha tahlil qilingan: axborotning maxfiyligi, butunligi va mavjudligini ifodalovchi CIA modeli, axborot xavfsizligini boshqarish tizimlari (ISMS), kiberxavfsizlik risklarini boshqarish, texnik himoya mexanizmlari, inson omili va xavfsizlik madaniyati, hamda Zero Trust arxitekturasi. Tahlil natijalari axborot xavfsizligining alohida texnik choralar majmuasidan tashkiliy, texnik va insoniy omillarni birlashtirgan, uzluksiz boshqariladigan tizimli jarayonga aylanib borayotganini ko‘rsatadi.*

Kalit so‘zlar: *axborot xavfsizligi, CIA modeli, ISO/IEC 27001, NIST Cybersecurity Framework, kiberxavfsizlik, risklarni boshqarish, Zero Trust, xavfsizlik madaniyati.*

Raqamli texnologiyalarning jadal rivojlanishi, elektron hukumat, raqamli bank xizmatlari va bulutli texnologiyalarning keng tarqalishi axborot resurslarining ahamiyatini sezilarli darajada oshirmoqda. Kiberhujumlar soni va murakkabligining ortishi esa axborot xavfsizligini zamonaviy boshqaruv tizimining ajralmas qismiga aylantirmoqda. An’anaviy yondashuvda xavfsizlik ko‘pincha faqat texnik vositalar orqali ta’minlangan, biroq zamonaviy tahdidlar ijtimoiy muhandislik, ichki tahdidlar va ko‘p bosqichli hujumlarni o‘z ichiga oladi. Bu esa kompleks yondashuvni talab qiladi. Shu sababli ISMS, risklarga asoslangan boshqaruv, Zero Trust arxitekturasi kabi yo‘nalishlar faol rivojlanmoqda. Tezisning maqsadi - axborot xavfsizligini ta’minlashning zamonaviy tamoyillari va usullarini tahlil

qilish hamda ularning tashkiliy xavfsizlik darajasiga ta’sirini baholashdan iborat.

Maxfiylik, butunlik va mavjudlik tamoyillarini o‘z ichiga olgan CIA modeli axborot resurslarini himoyalash talablarini aniqlashda asosiy konsepsiya hisoblanadi[1]. ISO/IEC 27001 standarti xavfsizlikni bir martalik tadbir emas, balki doimiy boshqariladigan jarayon sifatida tashkil etishning tizimli modelini beradi [2]. NIST Cybersecurity Framework 2.0 tashkilot faoliyatini boshqarish, tahdidlarni aniqlash, himoyalash, javob berish va tiklash jarayonlarini tizimlashtirishga yordam beradi [3]. Texnik himoya mexanizmlari - kriptografiya, autentifikatsiya, kirishni boshqarish va monitoring - NIST SP 800-53 kabi hujjatlarda tavsiflangan [7]. Texnik vositalar mavjud bo‘lishiga qaramay, xodimlarning ehtiyotsizligi yoki shubhali xabarlar bilan noto‘g‘ri ishlashi xavfsizlikka salbiy ta’sir ko‘rsatishi mumkin [4]. NIST SP 800-207 hujjatida Zero Trust arxitekturasi foydalanuvchi yoki qurilmaga tarmoqdagi joylashuvidan qat’iy nazar avtomatik ravishda ishonmaslik tamoyiliga asoslanishi ko‘rsatilgan [5]. Amaliy tendensiyalarni esa ENISA

va Verizon hisobotlari, huquqiy va boshqaruv asoslarini esa GDPR hamda COBIT kabi hujjatlar to‘ldiradi [6]. Tahlil shuni ko‘rsatadiki, zamonaviy axborot xavfsizligi texnik himoya, tashkiliy boshqaruv va inson omilini birlashtiruvchi kompleks tizim sifatida rivojlanmoqda.

Axborot xavfsizligining nazariy negizini CIA modeli tashkil etadi: maxfiylik - ma’lumotlarga faqat vakolatli shaxslarning kirishini ta’minlash; butunlik - ma’lumotlarni ruxsatsiz o‘zgartirishlardan himoyalash; mavjudlik - resurslarning zarur vaqtda foydalanish uchun mavjud bo‘lishini ta’minlash.

Tashkiliy darajada bu tamoyillar ISMS orqali amalga oshiriladi. ISO/IEC 27001 xavfsizlik siyosatini ishlab chiqish, risklarni baholash va nazorat choralarini doimiy monitoring qilishni o‘z ichiga olgan, Reja–Bajarish–Tekshirish–Yaxshilash (PDCA) siklini taklif etadi [2]. NIST Cybersecurity Framework 2.0 esa risklarni boshqarishni oltita funksiyaga ajratadi: Govern, Identify, Protect, Detect, Respond va Recover.

Texnik darajada bu funksiyalar kriptografiya, ko‘p faktorli autentifikatsiya,

kirishni boshqarish, tarmoq segmentatsiyasi, IDS/IPS va ma’lumotlarni zaxira nusxalash orqali amalga oshiriladi. Ularning samaradorligi esa yagona xavfsizlik arxitekturasi doirasida bir-birini to‘ldirishiga bog‘liq [7].

Texnik va tashkiliy choralar bilan bir qatorda, xodimlarni muntazam o‘qitish va xavfsizlik madaniyatini shakllantirish muhim ahamiyat kasb etadi [4]. Perimetrga asoslangan an’anaviy himoya endi yetarli emasligi sababli Zero Trust arxitekturasi taklif etiladi. Ushbu yondashuvda hech qanday foydalanuvchi yoki qurilmaga tarmoqdagi joylashuvidan qat’iy nazar avtomatik ravishda ishonilmaydi. Har bir so‘rov kirishga ruxsat berilishidan oldin tekshiriladi va minimal vakolat tamoyiliga asoslanadi.

Tahlil natijasida bir nechta asosiy tendensiya aniqlandi: texnik vositalardan tashkiliy boshqaruv tizimlariga (ISMS) o‘tish; xavfsizlikning risklarga asoslangan, moslashuvchan yondashuvga (NIST CSF) o‘tishi; perimetrga asoslangan himoyadan Zero Trust arxitekturasiga o‘tish; inson omili va xavfsizlik madaniyatining strategik ahamiyat kasb etishi; avtomatlashtirish va sun’iy intellektning tahdidlarni aniqlashda tobora ko‘proq qo‘llanilishi.

Bu tendensiyalar o‘zaro bog‘liq: ISMS doirasida belgilangan siyosat va risklarni baholash natijalari texnik nazorat choralarini tanlashga asos bo‘ladi, Zero Trust esa ushbu nazorat choralarini amalga oshirishning zamonaviy arxitekturaviy asosini taqdim etadi. Xodimlarning xavfsizlik bo‘yicha xabardorligi past bo‘lgan tashkilotlarda hatto eng ilg‘or texnik yechimlar ham ijtimoiy muhandislik hujumlari oldida ojiz qolishi mumkin.

Kelajakdagi axborot xavfsizligi tizimini quyidagi zanjir sifatida tasavvur qilish mumkin:

Risklarni baholash (ISMS) → texnik nazorat choralari → Zero Trust arxitekturasi → sun’iy intellekt asosidagi monitoring va avtomatlashtirilgan javob choralari.

Bunday integratsiya tahdidlarga tezroq javob berish imkonini bersada, malakali kadrlar va mos me’yoriy-huquqiy bazani talab qiladi.

Tadqiqot natijalari axborot xavfsizligining bir martalik texnik tadbirdan

tashkiliy boshqaruv, texnik himoya va inson omilini birlashtiruvchi uzluksiz jarayonga aylanib borayotganini ko‘rsatadi. CIA modeli nazariy asosni, ISO/IEC 27001 tashkiliy boshqaruvni, NIST Cybersecurity Framework risklarni boshqarish jarayonini tizimlashtiradi, Zero Trust arxitekturasi esa zamonaviy, tarqoq tarmoq muhitlariga mos yangi himoya yondashuvini taklif etadi.

Kiberhujumlarning murakkablashuvi va inson omilining barqaror ta’sir ko‘rsatishi xavfsizlikni faqat texnik emas, balki tashkiliy va strategik boshqaruv masalasi sifatida ko‘rib chiqishni taqozo etadi. Shu sababli xavfsizlik strategiyasini ishlab chiqishda texnik, tashkiliy va insoniy omillar muvozanati tarzda hisobga olinishi lozim.

ADABIYOTLAR RO‘YXATI

1. Whitman, M. E., Mattord, H. J. Principles of Information Security. 6th ed. Cengage Learning, 2018.

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

3. NIST. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024.

4. Verizon. Data Breach Investigations Report (DBIR). Verizon Business, 2023.

5. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020.

6. ENISA. Threat Landscape Report. European Union Agency for Cybersecurity.

7. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, 2020.