



AXBOROT XAVFSIZLIGINI TA'MINLASH USULLARI

Respublika musiqa va san'at texnikumi

*Informatika fani o'qituvchisi **Namozova Lubat Baxrilloevna***

Annotatsiya: Axborot xavfsizligini ta'minlash bugungi kunning eng dolzarb masalalaridan biri hisoblanadi. Axborot texnologiyalari rivojlanishi bilan birga, turli sohalarda ishlatiladigan axborot resurslari, foydalanuvchi ma'lumotlari hamda xavf ostida qolayotgan axborot tizimlarini himoya qilish istagi va ehtiyoji paydo bo'ldi. Ammaviy informatsiyalashtirish jarayonlari natijasida jamiyat hayotida axborotning ahamiyati ortib bormoqda. Axborotning zamonaviy jamiyatdagi roli shunchalik kuchaymoqdaki, uni himoyalash va saqlash yo'llarini to'g'ri belgilash har bir tashkilot, idora va shaxs uchun muhim ahamiyatga ega bo'lib qolmoqda.

Kalit so'zlar: Axborot xavfsizligi, himoya choralar, autentifikatsiya, shifrlash, tarmoqlar xavfsizligi, monitoring, audit, zaxiralash, konfidensiallik, foydalanuvchi xavfsizligi.

Axborot xavfsizligini ta'minlashga oid tizimli chora-tadbirlar ishlab chiqilishi nafaqat axborot texnologiyalari mutaxassislari, balki rahbarlar va foydalanuvchilarning ham e'tiborida bo'lishi zarur. Axborot tizimini himoya qilish uchun bo'layotgan tahdid va xatarlarga munosib javob bera olish, zamonaviy mezonlar asosida, axborot xavfsizligini ta'minlashni talab qiladi. Bu borada birinchi navbatda, axborot resurslari qiymatini va ular uchun mavjud xavflarni to'g'ri baholash lozim. Axborot tizimi bilan ishlovchi tashkilot xodimlari ma'lumotlar asosiy boylik hisoblanishini tushunib yetishi va undan to'g'ri foydalanish bo'yicha aniq yo'riqnomalarga ega bo'lishlari muhim. Axborot xavfsizligini ta'minlashning eng asosiy maqsadi – axborot resurslari yaxlitligini, konfidensialligini va mavjudligini himoya qilishdan iborat. Yaxlitlik, ya'ni axborotning xatosiz, original va talab darajasida buzilmasdan saqlanishi, konfidensiallik esa, axborotdan faqat



ruxsat etilgan shaxslarning foydalanishini ta'minlash, mavjudlik esa, axborotga ehtiyoj tug'ilganda unga darhol murojaat qilish imkoniyatini kafolatlashdan iboratdir [1].

Axborot xavfsizligini ta'minlash usullari turli bosqichlardan iborat bo'lib, har bir bosqichda o'ziga xos vazifalar, nazorat va monitoring ishlari olib boriladi. Avvalo, axborot xavfsizligini huquqiy asoslarda ta'minlash zarur. Bu sohada davlat va xalqaro darajada qabul qilingan qonun, normativ hujjatlar, me'yoriy aktlar asosida, axborot resurslarini himoyalash bo'yicha umumiy qoidalar va majburiyatlar belgilanadi. Ichki tashkilot qoidalari, axborot xavfsizligi siyosati va foydalanuvchilarning behaviour kodeksi ham amalda muhim rol o'ynaydi. Bunday hujjatlar har bir foydalanuvchiga o'z vazifalari va javobgarligini aniq tushuntirib beradi. Axborot xavfsizligini tashkil etishning texnik usullari, eng avvalo, axborot resurslariga ruxsatsiz kirishni cheklash tizimlarini joriy etish orqali amalga oshiriladi. Bunda foydalanuvchilarning autentifikatsiya va avtorizatsiya jarayonlari asosida, axborotga kirish huquqlari taqsimlanadi. Autentifikatsiya yordamida foydalanuvchi kimligini isbotlashi, avtorizatsiya esa unga qanday axborotga ruxsat berilganini aniqlab beradi. Bu usullar parol, tokenlar, biometrik ko'rsatkichlar, yuzni aniqlash, barmoq izi orqali amalga oshiriladi. Shuningdek, kriptografik usullardan keng foydalaniladi. Bu usullar axborotni shifrlash orqali maxfiylik darajasini oshiradi. Oddiy matndagi axborot maxsus algoritmlar yordamida shifrlanadi va faqat shifrdan ochish kalitiga ega bo'lgan shaxslar uni qayta tiklash imkoniyatiga ega bo'ladi. Kriptografik vositalardan foydalangan holda ma'lumotlarni uzatish, saqlash va qayta ishlash jarayonlarida xavfsizlik yanada mustahkamlanadi. Xususan, elektron pochta orqali yuboriladigan axborotlarning kriptolanmagan shaklda uzatilishi turli kiberhujumlarga sabab bo'lishi mumkin. Shu bois, zamonaviy axborot tizimlarida har bir ma'lumot almashinuvi shifrlash yordamida amalga oshiriladi [2].



Axborot xavfsizligini ta'minlashda doimiy monitoring va audit jarayonlari muhim ahamiyatga ega. Monitoring yordamida axborot tizimlari va tarmoqlarda yuzaga kelayotgan o'zgarishlar, kutilmagan hodisalar va funksiyalarning buzilishi, foydalanuvchi harakatlari va dasturiy ta'minot holati kuzatib boriladi. Texnologiyalar rivojlanib, yangidan-yangi tahdid va xatarlar vujudga kelmoqda, shu sababli tizimlarni doimiy ravishda tekshirib, zaif joylarni tez aniqlash va bartaraf etish zarurdir. Audit orqali esa, axborot xavfsizligi siyosatiga rioya etilayotganlik, xavfsizlik choralarining samaradorligi va tizimdagi zaifliklar o'rganiladi. Axborot xavfsizligini ta'minlashda tarmoq himoyasi usullaridan ham samarali foydalaniladi. Tarmoq xavfsizligi firewall, tarmoq segmentatsiyasi, virtual xususiy tarmoqlar (VPN), intruziyalarni aniqlash va oldini olish tizimlari yordamida ta'minlanadi. Firewall vositalari tarmoq bo'ylab kiruvchi va chiquvchi ma'lumotlarni to'sib, zararli trafikning oldini olishga xizmat qiladi. Segmentatsiya yordamida esa, tarmoqda bo'ladigan alohida bo'limlar ajratilib, bir bo'limdan boshqasiga noqonuniy o'tishlar cheklanadi. VPN texnologiyasi yordamida esa, ochiq tarmoqlarda xavfsiz ma'lumot uzatish imkoniyati paydo bo'ladi. Dasturiy ta'minotni muntazam yangilab borish, zaifliklarni bartaraf etishda, har xil ekspluatatsiyalar va viruslardan himoyalanişda muhim o'rin tutadi. Operatsion tizimlar, ishchi dasturlar va axborotlar bazasi dasturlari muntazam yangilanib, kriptografik himoya vositalari doimiy monitoring qilinadi. Kompyuter viruslari, Troyan dasturlari, spam, phishing kabi zararli dasturlar va usullardan himoyalaniş uchun antivirus va antimalware dasturlari o'rnatiladi va vaqt-vaqti bilan yangilanadi [3].

Axborot xavfsizligini ta'minlashda inson omili ham alohida rol o'ynaydi. Tahririy va xizmat axborotlarining maxfiy saqlanishi ko'p hollarda bevosita xodimlarning ogohlighi va ehtiyotiga bog'liq. Xodimlarning bilim va ko'nikmalarini oshirish, ular orasida faol targ'ibot va tashviqot ishlari olib borish, doimiy o'qitish va treninglar o'tkazish zarur. Axborotni muhofaza qilish qoidalari bo'yicha xodimlarning xabardorligi oshishi natijasida, tasodifiy yoki ataylab sodir qilinish



ehtimoli bor xatolar ancha kamayadi. Kiberxavflarni oldindan sezish va ularni bartaraf etish, xodimlarning hamkorligi asosida samaraliroq kechadi. Tashkilot va korxonalarda axborot xavfsizligini ta'minlash uchun ichki va tashqi tahdidlarni farqlash kerak. Ichki tahdidlar tashkilot doirasidagi xodimlar, ularning noto'g'ri harakatlari, beparvoliklari va dastlabki ma'lumotlarni himoya qilish choralari yetarli emasligi natijasida yuzaga keladi. Tashqi tahdidlar esa tashqi kiberhujumlar, raqib kompaniyalarning hakerlari yoki ruxsatsiz foydalanuvchilar tomonidan sodir etiladi. Har ikki turdagi xatarlar uchun alohida himoya strategiyalari ishlab chiqilishi lozim. Axborot xavfsizligini ta'minlashda axborotni zaxiralash tartib-qoidalari ham muhim ehtiyot choralaridan hisoblanadi. Muhim ma'lumotlarni muntazam zaxiralab borish, ularni saqlash uchun ishonchli tashqi qurilmalar yoki bulutli texnologiyalardan foydalanish, axborot yo'qolishi yoki zarar yetkazilishi ehtimolini kamaytiradi. Zaxira nusxalarini saqlash va tiklash amaliyoti IT infratuzilmasining uzluksiz faoliyat yuritishida hal qiluvchi rol o'ynaydi. Axborotni himoya qilishda yondashuvlar kompleks va ko'p bosqichli bo'lishi kerak. Faqat texnik yoki dasturiy vositalar bilan cheklanib qolmasdan, huquqiy, tashkiliy, ma'rifiy va insoniy omillarning uyg'unligi asosida kuchli zamonaviy axborot xavfsizligi siyosatini ishlab chiqish, uni doimiy takomillashtirib borish muhimdir [4].

Axborot xavfsizligi tizimini joriy qilishda, har bir foydalanuvchi va mutasaddi shaxs tomonidan axborotga nisbatan javobgarlik va mas'uliyat bo'lishi zarur. Axborot resurslariga kirish tartibi qat'iy belgilanadi. Kirish huquqlari eng kamidan eng ko'pga qarab (minimumdan maksimumgacha) taqsimlanadi va ortiqcha imkoniyatlar o'chirib qo'yiladi. Barcha harakatlar tizim jurnaliga qayd qilinib boriladi, bu esa ehtimoliy buzilishlarni aniqlash va ularga tezkor javob berishda yordam beradi [5].

Xulosa:

Xulosa qilib aytganda, axborot xavfsizligini ta'minlash usullari zamonaviy jamiyat uchun alohida ahamiyat kasb etmoqda. Axborot resurslarini himoya qilishda



huquqiy, tashkiliy, texnik, dasturiy va insoniy omillarni uyg'unlashtirish, doimiy monitoring, audit va foydalanuvchi madaniyatini oshirish asosiy vazifa bo'lib qolaveradi. Axborot xavfsizligini ta'minlashda faqatgina modern usullar va zamonaviy texnologiyalarga tayanib qolmasdan, axborot bilan ishlovchi barcha insonlarni ogoh, e'tiborli va bilimli bo'lishlariga erishish lozim. Axborot xavfsizligi– kelajak taraqqiyoti va rivojlanishining muhim kafolatidir. Bu yo'lda uzluksiz izlanishlar, tajribalar va yangi yutuqlarga erishishga intilish zamin yaratadi. Axborot tsivilizatsiyasi davrida, axborot resurslarini himoyalash va ularni xavfsiz tarzda boshqarish, har bir inson va jamiyat uchun ustuvor vazifalardan bo'lib qoladi.

Foydalanilgan adabiyotlar:

1. Abduvaliyev, A.B. (2020). "Axborot xavfsizligini ta'minlashda kriptografik usullarning ahamiyati." Toshkent axborot texnologiyalari universiteti ilmiy jurnali, 3(2), 121-127.
2. Ahmedov, D.X. (2019). "Axborot tizimlarida xavfsizlik strategiyalari va tahdidlarni baholash." Zamonaviy axborot texnologiyalari, 4(6), 55-62.
3. Akhmedova, N.E. (2022). "Internet tarmoqlari xavfsizligi va uni himoyalash usullari." O'zbekiston axborot xavfsizligi jurnali, 8(1), 13-19.
4. Bobomurodov, I.B. (2018). "Dasturiy ta'minotda zaxira nusxalash va ma'lumotlarni tiklash usullari." Axborot texnologiyalari va kommunikatsiyalar, 5(4), 48-53.
5. Jo'rayev, B.X. (2019). "Axborotni shifrlashda zamonaviy usullardan foydalanish." Axborot xavfsizligi va ishonchli kommunikatsiyalar, 2(3), 74-82.
6. Karimov, S.R. (2017). "Axborot xavfsizligini oshirishning yangi yondashuvlari." Axborot texnologiyalari, 6(1), 91-97.
7. Matyoqubov, M.T. (2021). "Tashkilotlarda axborot xavfsizligi siyosati va boshqaruv tizimi." Zamonaviy tarmoqlar, 1(2), 35-41.
8. Mirzayeva, D.S. (2018). "Tahdidlarni aniqlash va axborot tizimlarini himoyalash texnologiyalari." Axborot va kompyuter injiniringi, 7(2), 58-66.