KORXONA AXBOROT TIZIMLARINI BOSHQARISHDA AXBOROT XAVFSIZLIGI PARAMETRLARINING USTIVORLIGI

Islamova Dildora Sultanovna
Muhammad al-Xorazmiy nomidagi, TATU Qarshi filiali assistenti

Rivojlanishni o‘z oldiga maqsad qilib qo‘ygan har qanday korxona yoki tashkilotning bugungi kundagi asosiy maqsadi, axborotlarga bo‘lgan ehtiyojini aniqlashdan tortib, axborotlardan foydalanishgacha bo‘lgan tizim ishining ketma-ketligini belgilash eng muhim masala sanaladi. Bu o‘rinda gap, korxonada hal etiluvchi masalalarni turlarga ajratish, axborotlarni olish, qayta ishlash va foydalanish davriyligini belgilash, keladigan va chiqadigan hujjatlarni standartlash, axborotlarni qayta ishlash tartibini standartlash hamda korxona axborot tizimlarini boshqarish jarayonlarida korxona maxfiy sirlarini ham xavfsizlik parametlari asosida muntazam himoyalab borishni ko‘zda tutadi. Korxonaning axborot xavfsizligi boshqarish tizimini yaratishda ISO/IEC 27001 standart qoidalari talablariga javob berishi va sertifikatiga egalik huquqining mavjudligi tashkilotlarda axborot xavfsizligini ta’minlash uchun yagona ustivor ko’rsatkich hisoblanadi. Ushbu sertifikat bo‘yicha axborot xavfsizligi mexanizmini yo‘lga qo‘ygan tashkilotlarga hamkorlar va boshqa manfaatdor tomonlarning ishonchi oshadi, bu tashkilot xalqaro miqyosda tan olinishida bir turtki vazifasini o‘taydi. Yana bir muhim tomoni kompaniyaning yirik davlat shartnomalarida ishtirok etish imkoniyatlari ham kengayadi [1].

ISO/IEC 27001 — bu Xalqaro standartlashtirish tashkiloti va Xalqaro elektrotexnika komissiyasi tomonidan birgalikda ishlab chiqilgan xalqaro axborot xavfsizligi standartidir. Sertifikat axborot xavfsizligini boshqarish tizimini (AXBT) yaratish, ishlab chiqish va ta’minlash uchun axborot xavfsizligi sohasidagi talablarni o‘z ichiga oladi.

ISO/IEC 27001 dunyoda eng mashhur standartlardan biri bo‘lib, axborot xavfsizligini boshqarish tizimlari (AXBT) talablariga javob beradi. Axborot xavfsizligini boshqarish tizimlari nima degani? AXBT – bu kompaniyadagi maxfiy ma’lumotlarni xavfsiz bo‘lishi uchun boshqarishning tizimli yondashuvidir. Ushbu mexanizm kichik, o‘rta va yirik korxonalarga axborot xavfsizligini ta’minlashda yordam beradi va quyidagilarni tizim himoyasining asosiy xavfsizlik paramertlari deb baholaydi [2]:

· tizimlarga ruxsatsiz kirishdan (IDS) himoya qilish;
· shu jumladan tashkilot xodimlarining ruxsatsiz kirishidan ichki himoya;

E-Global Congress
Open Access | Peer Reviewed | Conference

· avtorizatsiya va autentifikatsiya;
· ma'lumotlarni uzatish kanallarini himoya qilish, yaxlitligini ta'minlash;
· mijozlar bilan ma'lumot almashishda ma'lumotlarning dolzarbligini ta'minlash;
· elektron hujjat aylanishi;
· axborot xavfsizligi hodisalarini boshqarish;
· biznesning uzluksizligini boshqarish;
· axborot xavfsizligi tizimining ichki va tashqi auditi.

Axborot xavfsizligi - bu axborotni biznesning uzluksizligini ta'minlash, biznes xavflarini minimumga keltirish va investitsiyalarni qaytarishni hamda biznes imkoniyatlarini maksimal oshirish masqsadida tahdidlarning keng spektridan muhofaza qilish demakdir. Shunday ekan tashkilotda hujjatlashtirilgan AXBT tashkilotning butun ish faoliyati va to‘qnash keladigan xatarlariga muvofiq ishlab chiqilishi, joriy etilishi, ekspluatatsiya qilinishi, monitoringini yuritishi, tahlil qilinishi, saqlab turishi va uzluksiz takomillashtirilishi kerak. Axborot xavfsizligiga dasturiy ta'minotning siyosatlari, metodlari, protseduralari, tashkiliy tuzilmalari va dasturiy ta'minot funksiyalari tomonidan taqdim etilishi mumkin bo‘lgan axborot xavfsizligini boshqarish bo‘yicha tadbirlarning tegishli kompleksini amalga oshirish yo‘li bilan erishiladi. Ko‘rsatilgan tadbirlar tashkilotning axborot xavfsizligi maqsadlariga erishishini ta'minlashi kerak[3].

Axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida hisoblangan axborot xavfsizligini boshqarish bo‘yicha tadbirlar quyidagilarni o‘z ichiga oladi:

a) axborot xavfsizligi siyosatini hujjatlashtirish;
b) axborot xavfsizligini ta'minlash bo‘yicha majburiyatlarni taqsimlash;
c) axborot xavfsizligi qoidalariga o‘qitish;
d) ilovalardagi axborotga to‘g‘ri ishlov berish;
e) texnik zaifliklarni boshqarish strategiyasi;
f) tashkilotning uzluksiz ishini boshqarish:
g) axborot xavfsizligi insidentlari va takomillashtirishlarini boshqarish.

Sanab o‘tilgan tadbirlarni ko‘pgina tashkilotlar va axborot muhiti uchun qo‘llasa bo‘ladi. Ushbu standartda keltirilgan barcha tadbirlar muhim hisoblansa ham, qandaydir choraning o‘rinli bo‘lishi tashkilot to‘qnash keladigan muayyan xavflar nuqtai nazaridan belgilanishi kerak. Demak, yuqorida ta'riflangan yondashish axborot xavfsizligini ta'minlash bo‘yicha tadbirlarni joriy qilish uchun tayanch nuqta bo‘lib hisoblanishiga qaramay, u xavflarni baholashga

E-Global Congress
Open Access | Peer Reviewed | Conference

asoslangan axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlashning samarali usuli hisoblanadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Abdullayev M.K. “Korxona axborot tizimlarinini boshqarish jarayonlarini algoritmlashtirish” “Iqtisodiyot va innovatsion texnologiyalar” ilmiy elektron jurnali. № 6, noyabr-dekabr, 2019 yil.
2. ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Требования».
3. O’z Dst ISO/IEC 27005:2013 «Информационные технологии. Методы обеспечения безопасности. Управления рисками информационной безопасности».

E-Global Congress
Open Access | Peer Reviewed | Conference