DOI: https://doi.org/10.5281/zenodo.11245256

ISO/IEC 27001:2005 VA ISO/IEC 17799:2005 STANDARTLARI. “AXBOROT TEXNOLOGIYALARI. XAVFSIZLIKNI TA’MINLASH METODLARI. AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMLARI.”

Ramazonova Madina Shavkatovna
Ilmiy rahbar

Tojimuratov Shuxratbek Dilmurodjon o‘g‘li
Mirzayev Bekzod Toxirboy o‘g‘li
Babajanov Jaloliddin Umidjon o‘g‘li
Toshkent axborot texnologiyalar universiteti talabalari
abdujabbor.madina.1989@gmail.com

Annotatsiya: *Axborot xavfsizligi tashkilotning qo‘shimcha qiymat beradigan eng muhim resurslaridan biri bo‘lib, uni himoya qilish zarurati tug‘iladi. ISO 27001 standarti axborot xavfsizligini boshqarish tizimini (AXBT) ishlab chiqish va joriy etish bo‘yicha talablarga muvofiq jarayonlarni belgilaydi. Ushbu tizim axborot aktivlarining konfidensialligi, butunligi va foydalanuvchanligini ta’minlashni nazarda tutadi. ISO 27001 korxona uchun xavfsizlik siyosati va risklarni boshqarish jarayonini hujjatlashtirish, monitoring qilish va takomillashtirish imkonini beradi. Standart, shuningdek, ISO 9001 va ISO 14001 kabi boshqa menejment tizimlari bilan integratsiyalashgan. ISO/IEC 27002 esa axborot xavfsizligini boshqarish bo‘yicha batafsil ko‘rsatmalarni beradi. Mazkur hujjatda ISO 27001 va ISO 27002 standartlari asosida axborot xavfsizligini boshqarish tizimini joriy etish bosqichlari va tashkilotlar uchun muhim jihatlar bayon etilgan*

Kalit so‘zlar: *Axborot xavfsizligi, ISO 27001, Axborot xavfsizligini boshqarish tizimi, Konfidensiallik, Butunlik, Foydalanuvchanlik, Risklarni boshqarish, Xavfsizlik siyosati, Sertifikatlash*

Axborot - bu tashkilotga qo‘shimcha qiymat beradigan eng muhim biznes resurslaridan biri va natijada uni himoya qilish zarurati tug‘iladi. Axborot xavfsizligining zaif tomonlari moliyaviy yo‘qotishlarga olib kelishi va biznes operatsiyalariga zarar yetkazishi mumkin. Shu sababli, bizning davrimizda axborot

xavfsizligini boshqarish tizimini ishlab chiqish va uni tashkilotda joriy etish masalasi kontseptual hisoblanadi.

ISO 27001 standartiga asosan axborot xavfsizligi quyidagicha ta’riflanadi: “axborotning konfidensialligi, butunligi va foydalanuvchanligini saqlash; bundan tashqari, haqiqiylik, mualliflikdan bosh tortmaslik va ishonchlilik kabi boshqa xususiyatlar ham kiritilishi mumkin”.

Konfidensiallik - ma’lumotlarni faqat tegishli vakolatga ega bo‘lganlar (vakolatli foydalanuvchilar) foydalanishini ta’minlash;

Butunlik - ma’lumotlarning aniqligi va to‘liqligini, shuningdek uni qayta ishlash usullarini ta’minlash;

Foydalanuvchanlik - kerak bo‘lganda (talab bo‘yicha) vakolatli foydalanuvchilarning ma’lumotlarga kirishini ta’minlash.

ISO 27001:2005 sertifikatlashtirish uchun majburiy bo‘lgan axborot xavfsizligini boshqarish tizimiga qo‘yiladigan talablar ro‘yxati hisoblanadi, ISO 17799:2005 esa axborot xavfsizligi risklarini kamaytirish uchun tashkilot tanlagan boshqaruv vositalarini loyihalashda foydalanish mumkin bo‘lgan ko‘rsatmalarni namoyon qiladi.

ISO 27001 korxona uchun axborot xavfsizligini boshqarishning samarali tizimini yaratish, qo‘llash, ko‘rib chiqish, monitoring qilish va qo‘llab-quvvatlash imkonini beradigan jarayonlarni belgilaydi; tashkilotning mavjud biznes risklari kontekstida hujjatlashtirilgan axborot xavfsizligini boshqarish tizimini ishlab chiqish, joriy etish, ishlatish, monitoring qilish, tahlil qilish, qo‘llab-quvvatlash va takomillashtirishga qo‘yiladigan talablarni belgilaydi.

ISO 27001 standartiga asoslangan axborot xavfsizligini boshqarish tizimi (11.1-rasm) quyidagilarga imkon beradi:

- axborot aktivlarining aksariyat qismini kompaniya rahbariyati uchun tushunarli qilish;
- mavjud biznes jarayonlariga asosiy xavfsizlik tahdidlarini aniqlash;
- risklarni hisoblash va kompaniyaning biznes maqsadlari asosida qarorlar qabul qilish;
- kritik vaziyatlarda samarali tizim boshqaruvini ta’minlash;
- xavfsizlik siyosatini amalga oshirish jarayonini kuzatish (axborot xavfsizligi tizimining zaif tomonlarini topish va tuzatish);
- shaxsiy mas’uliyatni aniq belgilash;
- xavfsizlik tizimini qo‘llab-quvvatlash xarajatlarini kamaytirish va optimallashtirishga erishish;
- xavfsizlik quyi tizimini biznes jarayonlariga integratsiyalashuviga va ISO 9001:2000 bilan integratsiyalashuviga yordam berish;

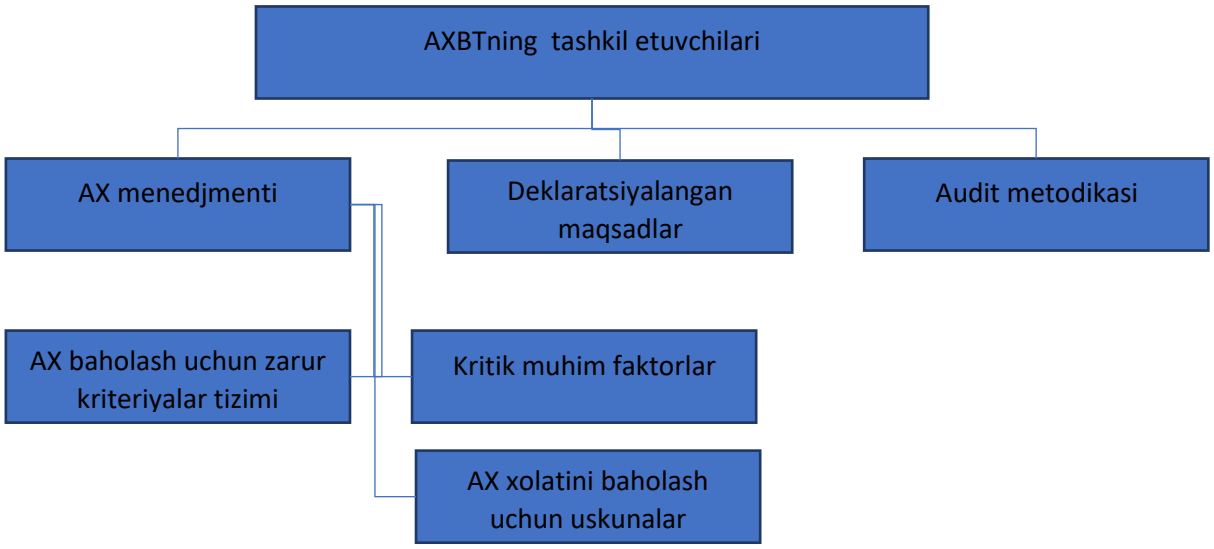
– mijozlar, hamkorlar va biznes egalariga axborot xavfsizligiga bog‘liqlikni namoyish etish;

– xalqaro e’tirofga ega bo‘lish va kompaniyaning ichki bozorda ham, tashqi bozorda ham obro‘sini oshirish;

– standartga rioya qilish orqali biznesning qonun oldida shaffofligi va tozaligini ta’kidlash.

Standartda kompyuterlar va kompyuter tarmoqlarini boshqarish vositalari bilan bir qatorda xavfsizlik siyosatini ishlab chiqish, xodimlar bilan ishlash (yollash, o‘qitish, ishdan bo‘shatish), ishlab chiqarish jarayonining uzluksizligini ta’minlash va qonunchilik talablariga katta e’tibor berilgan.

AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMI



11.1-rasm. AX boshqarish tizimi

Ushbu standartning talablari umumiy xususiyatga ega va keng doiradagi tashkilotlar - kichik, o‘rta va yirik - tijorat va sanoat bozorlari: moliya va sug‘urta, telekommunikatsiya, kommunal xizmatlar, chakana savdo va ishlab chiqarish tarmoqlari, turli xil xizmat ko‘rsatish sohalari, transport sektori, davlat idoralari va boshqalar tomonidan qo‘llanilishi mumkin..

ISO 27001 standarti ISO 9001:2000 va ISO 14001:2004 sifat menejmenti tizimi standartlari bilan uyg‘unlashtirilgan va ularning asosiy tamoyillariga asoslanadi. Bundan tashqari, ISO 9001 majburiy tartiblari ISO 27001 tomonidan ham talab qilinadi. ISO 27001 talablari uchun hujjatlar tuzilishi ISO 9001ga o‘xshaydi. ISO 27001 talab qiladigan hujjatlarning aksariyati allaqachon ishlab chiqilgan va ulardan ISO 9001 doirasida foydalanilmoqda. Shunday qilib, agar tashkilotda, masalan, ISO 9001 yoki ISO 14001 ga muvofiq boshqaruv tizimi allaqachon mavjud bo‘lsa, u holda ISO 27001 standarti talablariga muvofiqligini ta’minlash afzalroqdir, sababi mavjud

tizimlar, bu korxonaning ichki xarajatlarini va joriy etish va sertifikatlash xarajatlarini sezilarli darajada kamaytiradi.

ISO 27001:2005 standarti axborot xavfsizligini boshqarish tizimini rasmiy sertifikatlashni ta’minlaydi.

Standartga muvofiqlik sertifikati biznes hamkorlar, investorlar va mijozlarga kompaniyaning axborot xavfsizligi yuqori darajada o‘rnatilganligini va axborot xavfsizligini samarali boshqarish yo‘lga qo‘yilganligini aniq ko‘rsatish imkonini beradi.

Axborot xavfsizligini boshqarish tizimini ishlab chiqish va joriy etish bosqichlari. Axborot xavfsizligini boshqarish tizimini ishlab chiqishning quyidagi asosiy bosqichlarini ajratib ko‘rsatish mumkin :

- aktivlar inventarizatsiyasi ;
- aktivlarni turkumlash ;
- axborot tizimini himoyalnganligini baholash;
- axborot risklarini baholash;
- axborot risklarini qayta ishlash (shu jumladan qimmatli aktivlarni himoya qilish bo‘yicha aniq chora-tadbirlarni aniqlash);
- tanlangan riskni davolash choralarini joriy qilish;
- tanlangan chora-tadbirlarning amalga oshirilishi va samaradorligini monitoring qilish;
- axborot xavfsizligini boshqarish tizimida kompaniya boshqaruvining roli.

Axborot xavfsizligini boshqarish tizimining samarali ishlashining asosiy shartlaridan biri kompaniya rahbariyatining axborot xavfsizligini boshqarish jarayoniga jalb etilishi hisoblanadi. Barcha xodimlar tushunishlari kerakki, birinchidan, axborot xavfsizligi bo‘yicha barcha tadbirlar rahbariyat tomonidan boshlanadi va amalga oshirilishi majburiydir, ikkinchidan, kompaniya rahbariyati axborot xavfsizligini boshqarish tizimining ishlashini shaxsan nazorat qiladi, uchinchidan, boshqaruvning o‘zi axborotni xavfsizligini ta’minlash uchun kompaniyaning barcha xodimlari kabi bir xil qoidalarga amal qiladi.

Korxona aktivlarini inventarizatsiya qilish. Avvalo, axborot xavfsizligi nuqtai nazaridan kompaniyaning qimmatli aktivi nima ekanligini aniqlash kerak. Axborot xavfsizligini boshqarish tizimining protseduralarini batafsil tavsiflovchi ISO 17799 standartiga quyidagi aktiv turlari belgilangan:

- axborot resurslari (ma’lumotlar bazalari va fayllar, shartnomalar va kelishuvlar, tizim hujjatlari, tadqiqot ma’lumotlari, hujjatlar, o‘quv materiallari va boshqalar);
- dasturiy ta’minot;
- moddiy boyliklar (kompyuter uskunalari, telekommunikatsiyalar va boshqalar);

– xizmatlar (telekommunikatsiya xizmatlari, hayot faoliyatini qo‘llab-quvvatlash tizimlari va boshqalar);

– kompaniya xodimlari, ularning malakasi va tajribasi;

– nomoddiy resurslar (kompaniyaning obro‘si va imiji).

Inventarizatsiya qilish kompaniyaning qimmatli aktivlari ro‘yxatini tuzishdan iborat.

Aktivlarning muhimligi uchta parametr asosida baholanadi: konfidensiallik, butunlik va foydalanuvchanlik, ya’ni aktivlarning konfidensialligi, butunligi va foydalanuvchanligi buzilgan taqdirda kompaniyaga yetkaziladigan zarar baholanishi kerak.

Aktivlarning muhimligini baholash pul birliklarida va darajalarda amalga oshirilishi mumkin.

Har bir ko‘rsatilgan aktivning muhimligini baholash tamoyillari:

– axborot aktivlari (yoki axborot turlari) ularni oshkor qilish natijasida kompaniyaga yetkazilgan zarar nuqtai nazaridan baholanadi;

– dasturiy ta’minot, moddiy resurslar va xizmatlar ularning foydalanuvchanligi yoki ishga yaroqliligi nuqtai nazaridan baholanadi;

– kompaniya xodimlari o‘qish va o‘zgartirish huquqiga ega bo‘lgan axborot resurslaridan foydalanish imkoniyatini hisobga olgan holda, konfidensiallik va butunlik nuqtai nazaridan baholanadi;

– kompaniyaning obro‘si axborot resurslari bilan bog‘liq holda baholanadi.

Axborot riskini baholash. Axborot riskini baholash aktivlarning kritikligi, shuningdek zaifliklarning yuzaga kelish ehtimoli haqidagi ma’lumotlarni hisobga olgan holda amalga oshiriladigan risklarni hisoblashdan iborat.

Risk darajasi maqbul deb hisoblansa, risklar qabul qilinadi, ya’ni kompaniya ushbu risklarga nisbatan hech qanday choralar ko‘rishni maqsadga muvofiq deb hisoblamaydi va zarar ko‘rishga tayyor bo‘ladi.

Risklarni boshqarish jarayoni birinchi navbatda qaysi risklarni qo‘shimcha qayta ishlashni talab qilishi va qaysi biri qabul qilinishi mumkinligini aniqlashni talab qiladi.

Risklarni baholash va davolash natijalariga ko‘ra, qo‘llash mumkinligi to‘g‘risidagi Bayonot ishlab chiqiladi**.** Sertifikatlashdan o‘tish uchun ushbu hujjatning mavjudligi talab qilinadi.

ISO 27001 standartining A ilovasida kompaniya tomonidan bajarilishi kerak bo‘lgan barcha xavfsizlik talablari keltirilgan. Shu sababli, qo‘llash mumkinligi to‘g‘risidagi Bayonot kompaniyaning axborot risklarini kamaytirish bo‘yicha yakuniy qaror hisoblanadi.

Hujjatlashtirilgan protseduralar. Standart barcha risklarni kamaytirish choralarini hujjatlashtirishni talab qiladi, yani axborot xavfsizligini samarali

boshqarish uchun ma’lum hujjatlar (yo‘riqnomalar, siyosatlar, qoidalar) bilan tasdiqlanadigan va ma’lum shaxslar tomonidan amalga oshiriladigan protseduralar bo‘lishi kerak. Shuningdek, har bir protsedura tegishli hujjatda aks ettirilishi kerak. Hujjatlashtirilgan protseduralar axborot xavfsizligini boshqarish tizimining majburiy elementi hisoblanadi. Shu sababli, boshqaruv tizimi doirasida axborot xavfsizligi sohasidagi barcha protseduralarni tavsiflovchi normativ hujjatlar bazasini ishlab chiqish zarur.

Axborot xavfsizligini boshqarish bo‘yicha asosiy hujjatlar quyidagilardir:

- axborot xavfsizligini boshqarish siyosati;
- axborot xavfsizligi siyosati;
- metodikalar va ko‘rsatmalar;
- axborot xavfsizligini ta’minlash va uni boshqarishprotseduralari;
- fizik xavfsizlikni ta’minlash Reglamenti.

Kompaniya xodimlarini o‘qitish. Xodimlarni o‘qitish kunduzgi va sirtqi kurslar shaklida amalga oshirilishi mumkin, keyinchalik test sinovlari o‘tkaziladi, unda turli xil kurslar (foydalanuvchilar uchun ham, mutaxassislar uchun ham) o‘qitishning o‘yinli metodikalari va testlash kabilar taqdim etilishi mumkin bo‘lgan masofaviy ta’lim tizimidan foydalangan holda xodimlarni o‘qitishni tashkil etish tavsiya etiladi.

Asosiy qiyinchilik axborot xavfsizligini boshqarish tizimi protseduralarining samaradorligini tekshirishda bo‘lishi mumkin, ya’ni har bir protsedura uchun uning samaradorligi tekshiriladigan mezonlarni ishlab chiqish kerak va qo‘shimcha ravishda bunday mezonlar butun boshqaruv tizimi uchun ishlab chiqilishi kerak.

Axborot xavfsizligini boshqarish tizimining samaradorligini baholash mezonlari, masalan, axborot xavfsizligi hodisalari sonining o‘zgarishi, axborot xavfsizligi sohasidagi foydalanuvchilarning malakasi va boshqalar bo‘lishi mumkin.

Axborot xavfsizligini boshqarish tizimi protseduralarini joriy qilish. Protseduralarni joriy qilish, odatda, tegishli xodimlarni protsedurani bajarish qoidalari va muddatlari to‘g‘risida xabardor qilish, protseduraning bajarilishini muntazam ravishda nazorat qilish, shuningdek uning samaradorligini baholash, tuzatish va profilaktika choralarini joriy etish, ya’ni har bir protsedura uchun PDCA modelining butun siklini joriy qilishdan iborat.

ISO/IEC 27002:2013 xalqaro standarti.

2013 yilning kuzida axborot xavfsizligini boshqarish tizimlarining (AXBT) 2 ta xalqaro standarti nashr etildi. Bu ISO/IEC 27001:2013 standarti va ISO/IEC 27002:2013 standarti.

ISO/IEC 27002 “Information security, cybersecurity and privacy protection — Information security controls” (o‘zbekcha: Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni himoya qilish —Axborot xavfsizligini boshqarish

vositalari) - standarti ISO va IEC tomonidan 2013 yilda nashr etilgan va 2022 yilda yangi nashrda qayta nashr etilgan. 2007 yilgacha, bu standart ISO/IEC 17799 deb nomlangan. Standart 2000 yil da chop etilgan, Britaniya standarti BS 7799-1: 1999 ning to‘liq nusxasi hisoblangan ISO 17799 standarti asosida 2005 yilda ishlab chiqilgan.

ISO/IEC 27002:2013 xalqaro standarti mavjud risklarni hisobga olgan holda boshqaruv vositalarini tanlash, amalga oshirish va boshqarish kontekstida tashkilotlar tomonidan axborot xavfsizligini boshqarish tizimini ishlab chiqish va joriy etish bo‘yicha tavsiyalar beradi. U ISO / IEC 27001:2013 xalqaro standartiga nisbatan axborot xavfsizligini nazorat qilishni amalga oshirish bo‘yicha to‘liqroq tavsif va yo‘riqnomani taqdim etadi.

ISO/IEC 27000 standartlar seriyasi ichida ushbu standart quyidagicha nomalanadu: ISO / IEC 27002: 2013 - Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish bo‘yicha qoidalar to‘plami.

ISO/IEC 27002 quyidagilarni amalga oshirishni ko‘zlayotgan tashkilotlar tomonidan foydalanish uchun mo‘ljallangan:

1. ISO / IEC 27001 talablari asosida AXBT samarali ishlashi uchun boshqaruv vositalarini tanlash;

2. Axborot xavfsizligini nazorat qilishni amalga oshirish;

3. O‘zining axborot xavfsizligini boshqarish tamoyillarini ishlab chiqish.

Ushbu hujjatning maqsadlari uchun ISO / IEC 27000da keltirilgan atamalar va ta’riflar qo‘llaniladi.

Ushbu xalqaro standart axborot xavfsizligining 35 ta asosiy toifasini va 114 ta boshqaruv vositalaridan tarkib topgan 14 ta bo‘limni o‘z ichiga oladi, ularning ro‘yxati ISO / IEC 27001 standarti (A ilova)da keltirilgan. Bo‘limlar ketma-ketligi ularning ma’lum bir tashkilot uchun ahamiyatini bildirmaydi.

Standartning joriy versiyasi quyidagi asosiy bo‘limlardan iborat:

- Xavfsizlik siyosati.
- Axborot xavfsizligini tashkil etish.
- Resurslarni boshqarish.
- Inson resurslari xavfsizligi.
- Fizik va ekologik xavfsizlik.
- Kommunikatsiya va operatsiyalarni boshqarish.
- Foydalanishni boshqarish
- Axborot tizimlarini olish, ishlab chiqish va texnik xizmat ko‘rsatish.
- Axborot xavfsizligi insidentlarini boshqarish.
- Tashkilotning uzluksiz ishlashini boshqarish.
- Normativ talablarga muvofiqlik.

Shunday qilib, ushbu xalqaro standart qoidalari ISO/IEC 27001 talablariga muvofiq AXBTni joriy qiluvchi tashkilotlar tomonidan tegishli axborot xavfsizligi nazoratini tanlash va ularni individual biznes jarayonlariga qo‘llash uchun asos bo‘lib xizmat qilishi mumkin.

Bunday boshqaruv vositalari siyosatlar, jarayonlar, protseduralar, tashkiliy tuzilmalar va dasturiy ta’minot va apparat funktsiyalarini o‘z ichiga olishi mumkin. Xavfsizlikning aniq maqsadlari tashkilotning biznes maqsadlariga mos kelishini ta’minlash uchun ushbu boshqaruv elementlari yaratilishi, amalga oshirilishi, monitoring qilinishi, ko‘rib chiqilishi va kerak bo‘lganda takomillashtirilishi kerak.

ISO/IEC 27002:2013 standarti tashkilotlar unda va boshqa manbalarda keltirilgan boshqaruv vositalaridan foydalanishi mumkinligini ta’kidlaydi. Bundan tashqari, tashkilotlar zarur hollarda muayyan ehtiyojlarni qondirish uchun axborot xavfsizligini boshqarishning yangi vositalarini mustaqil ravishda ishlab chiqishi mumkin.

Juda muhim jihat shundaki, tashkilot o‘z nazorati va xavfsizlik talablarini tanlaydi. Ularni aniqlashning uchta manbasi mavjud:

1. Tashkilotning umumiy biznes strategiyasi va maqsadlarini hisobga olgan holda riskni baholash;

2. Qonun, me’yorlar, shartnoma yoki huquqiy hujjatlar asosida o‘rnatilgan talablar;

3. Axborotga ishlov berish, uni qayta ishlash, saqlash, uzatish va arxivlash tamoyillari, maqsadlari va biznes talablari.

Boshqaruv vositalarini tanlash, shuningdek, milliy va xalqaro qoidalarga muvofiq riskni qabul qilish darajasi, risklarni davolash variantlari va risklarni boshqarishga umumiy yondashuvni aniqlash asosida qabul qilingan tashkiliy qarorlarga bog‘liq.

Boshqarishning har bir asosiy toifasi uchun quyidagilar ko‘rsatilgan:

a) boshqaruv vazifasi, ya’ni u nimaga erishishga qaratilganligi;

b) belgilangan vazifani bajarish uchun qo‘llanilishi mumkin bo‘lgan bir yoki bir nechta boshqaruv elementlari.

Boshqaruvning tavsifi quyidagicha tuzilgan:

Amalga oshirish usuli. Boshqaruv muammosini hal qilishga qaratilgan muayyan amalga oshirish usulining tavsifi.

Foydalanish bo‘yicha tavsiyalar. Amalga oshirish usulini joriy qilish va belgilangan vazifani bajarish haqida batafsilroq ma’lumot beradi. Ushbu tavsiyalar barcha holatlarda to‘liq qo‘llanilmasligi yoki tegishli bo‘lmasligi va har qanday maxsus tashkiliy nazorat talablariga javob bermasligi mumkin.

Qo‘shimcha ma’lumot. Huquqiy masalalar yoki boshqa standartlarga havolalar kabi e’tiborga olinishi kerak bo‘lgan ma’lumotlarni o‘z ichiga oladi. Agar bunday ma’lumot nazorat uchun mavjud bo‘lmasa, tavsifning ushbu qismi olib tashlanadi.

XULOSA

Axborot xavfsizligi tashkilotlar uchun muhim biznes resursi bo‘lib, uni samarali boshqarish va himoya qilish zarurati mavjud. ISO 27001 standarti axborot xavfsizligini boshqarish tizimini ishlab chiqish va joriy etish bo‘yicha talablarni belgilaydi, bu tizim axborotning konfidensialligi, butunligi va foydalanuvchanligini ta’minlashga qaratilgan. Standart, shuningdek, mavjud biznes risklarini aniqlash, baholash va boshqarish uchun zarur jarayonlarni belgilaydi. ISO/IEC 27002 standarti esa axborot xavfsizligini boshqarish bo‘yicha batafsil ko‘rsatmalar va nazorat vositalarini taqdim etadi. Axborot xavfsizligini boshqarish tizimining samarali ishlashi uchun kompaniya rahbariyatining jalb etilishi va xodimlarning o‘qitilishi muhim ahamiyatga ega. ISO 27001 va ISO 27002 standartlariga muvofiq boshqaruv tizimining joriy etilishi tashkilotlarga xalqaro e’tirofga ega bo‘lish, biznes operatsiyalarini optimallashtirish va mijozlar va hamkorlar oldida ishonchlilikni oshirish imkonini beradi. Mazkur standartlarning qo‘llanilishi kompaniyalarga axborot xavfsizligi sohasida yuqori darajaga erishishga yordam beradi.

ADABIYOTLAR

1. O‘zbekiston Respublikasi Konstitutsiyasi.
2. O‘zbekiston Respublikasi Fuqarolik kodeksi. 01.03.1997. Qayta taxrirlangan versiyasi (21.04.2022y).
3. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. 16.04.2019 y.
4. O‘zbekiston Respublikasining «Axborot olish kafolatlari va erkinligi to‘g‘risida» Qonuni. 24.04.1997 y.
5. Yevropa Kengashining 1981 yil 28 yanvardagi “Shaxsiy ma’lumotlarni avtomatik qayta ishlash bo‘yicha jismoniy shaxslarni himoya qilish to‘g‘risida”gi konventsiyasi. Elektron resurs: lexdigital.ru/2012/052/ (Murojaat sanasi: 12.11.2015).
6. Yevropa Parlamenti va Kengashning 1996 yil 11 martdagi “Ma’lumotlar bazalarini huquqiy himoya qilish to‘g‘risida”gi 96/6/EC direktivasi. Elektron resurs
7. Yevropa Parlamentining 2001 yil 22 maydagi “Axborot jamiyatida mualliflik huquqi va turdosh huquqlarning ayrim jihatlarini uyg‘unlashtirish to‘g‘risida”gi 2001/29/EC direktivasi. Elektron resurs: http://www. wipo.int/wipolex/ru /text.jsp?file_id=126976 (Murojaat sanasi: 09.12.2015).
8. 2000 yil 8 iyundagi 2000/31/EC-sonli “Ichki bozorda axborot xizmatlarining ayrim huquqiy jihatlari to‘g‘risida”gi Yevropa Ittifoqi Direktivasi №2000/31/EC. Elektron resurs: http://www.wipo.int/wipolex/ru/text.jsp? file_id=181678 (Murojaat sanasi: 15.10.2015).
9. 1996 yil 20 dekabrdagi “BIMTning Mualliflik huquqi to‘g‘risida”gi Shartnomasi. - Jeneva: BIMT. – 2000. - № 226(R).