AXBOROTLARNI HIMOYA QILISHNING TASHKILIY, HUQUQIY VA TEXNIK USULLARI

Muallif:
Andijon shahar 2-son texnikumi
Informatika va axborot fani o‘qituvchisi
Zakirova Nafisa Saidikramovna

Annotatsiya

Mazkur ilmiy maqolada axborot xavfsizligini ta’minlashning tashkiliy, huquqiy va texnik usullari keng yoritilgan. Axborot texnologiyalarining rivojlanishi natijasida ma’lumotlarni himoya qilish dolzarb masalaga aylanganligi, turli kiberxavf va tahdidlarning oldini olishda zamonaviy himoya vositalarining ahamiyati tahlil qilingan. Shuningdek, korxona va ta’lim muassasalarida axborot xavfsizligini ta’minlashning amaliy jihatlari hamda real hayotiy misollar keltirilgan. Axborotlarni himoyalashda huquqiy me’yorlar, tashkiliy choralar va texnik vositalarning o‘zaro uyg‘un holda qo‘llanishi muhim ekanligi asoslab berilgan.

Kirish

Bugungi globallashuv va raqamlashtirish davrida axborot eng muhim resurslardan biriga aylandi. Davlat boshqaruvi, bank tizimi, ta’lim, sog‘liqni saqlash hamda ishlab chiqarish sohalarining barchasi axborot texnologiyalariga bog‘liq holda faoliyat yuritmoqda. Shu sababli axborotni himoya qilish masalasi strategik ahamiyat kasb etmoqda.

Axborot xavfsizligi deganda axborotning maxfiyligi, yaxlitligi va foydalanish imkoniyatining saqlanishi tushuniladi. Axborotga noqonuniy kirish, uni o‘zgartirish yoki yo‘q qilish katta iqtisodiy va ma’naviy zarar keltirib chiqarishi mumkin. Shu

bois axborotni himoyalashning samarali tizimini yaratish har bir tashkilot va davlatning ustuvor vazifasidir.

Hozirgi vaqtda axborotlarni himoya qilishning uch asosiy yo‘nalishi mavjud:

1. Tashkiliy usullar
2. Huquqiy usullar
3. Texnik usullar

Ushbu maqolada mazkur yo‘nalishlarning mohiyati, afzalliklari va qo‘llanilish mexanizmlari yoritib beradi.

Kalit so‘zlar

Axborot xavfsizligi, kiberxavfsizlik, axborotni himoyalash, tashkiliy usullar, huquqiy himoya, texnik himoya, autentifikatsiya, shifrlash, biometrik himoya, antivirus, firewall, ma’lumotlar bazasi. yoritiladi.

Axborotni himoyalashning tashkiliy usullari

Tashkiliy himoya usullari axborot xavfsizligini ta’minlashda inson omili bilan bog‘liq jarayonlarni boshqarishga qaratilgan. Bu usullar maxsus qoidalar, ichki tartiblar va nazorat tizimlari orqali amalga oshiriladi.

1. Xodimlar faoliyatini nazorat qilish

Ko‘plab axborot xavfsizligi muammolari aynan xodimlarning ehtiyotsizligi sababli yuzaga keladi. Masalan, oddiy parolni boshqa shaxsga aytib qo‘yish yoki zararli faylni ochish orqali tizimga virus kirib kelishi mumkin.

Shu sababli tashkilotlarda:

- maxfiy axborot bilan ishlash qoidalari;
- parol siyosati;
- xizmat kompyuterlaridan foydalanish tartibi ishlab chiqiladi.

Misol:

Bank tizimida ishlovchi xodimlarga har 30 kunda parolni almashtirish talabi qo‘yiladi. Bu ruxsatsiz kirish ehtimolini kamaytiradi.

2. Axborot xavfsizligi bo‘yicha treninglar

Xodimlarni muntazam o‘qitish muhim hisoblanadi. Chunki zamonaviy kiberjinoyatchilar ko‘pincha “ijtimoiy muhandislik” usulidan foydalanadi.

Misol:

Firibgar elektron pochta orqali “Siz yutuq yutdingiz” degan xabar yuboradi va foydalanuvchidan login-parolini kiritishni so‘raydi. O‘qitilgan xodim bunday xabarlarga ishonmaydi.

3. Ruxsat darajalarini belgilash

Har bir foydalanuvchi o‘z lavozimiga mos axborotdan foydalanishi kerak.

Misol:

Maktabda:

- direktor barcha ma’lumotlarga kirish huquqiga ega;
- o‘qituvchi faqat o‘z guruhiga tegishli ma’lumotlarni ko‘ra oladi;
- talaba esa faqat o‘z reytingini ko‘ra oladi.

Bu usul ortiqcha axborot tarqalishining oldini oladi.

4. Zaxira nusxalar yaratish

Muhim ma’lumotlarning doimiy “backup” nusxasi olinadi.

Misol:

Universitet serveridagi talabalar bazasi har kuni avtomatik ravishda boshqa serverga saqlanadi. Agar asosiy server ishdan chiqsa, ma’lumotlar tiklanadi.

Tashkiliy usullar texnik vositalar bilan birgalikda qo‘llanilgandagina samarali natija beradi.

Axborotni himoyalashning huquqiy usullari

Huquqiy himoya davlat tomonidan qabul qilingan qonunlar va me’yoriy hujjatlar orqali amalga oshiriladi. Bu usullar axborot xavfsizligini ta’minlashning huquqiy asosini tashkil etadi.

1. O‘zbekiston Respublikasining qonunlari

O‘zbekistonda axborot xavfsizligini tartibga soluvchi bir qator qonunlar mavjud:

- “Axborotlashtirish to‘g‘risida”gi Qonun;
- “Davlat sirlarini saqlash to‘g‘risida”gi Qonun;
- “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun;
- “Elektron hukumat to‘g‘risida”gi Qonun.

Mazkur hujjatlar axborotdan foydalanish, uni saqlash va himoya qilishning huquqiy me’yorlarini belgilaydi.

2. Mualliflik huquqini himoya qilish

Dasturiy ta’minot, elektron kitoblar va ilmiy ishlardan noqonuniy foydalanish qonun bilan taqiqlanadi.

Misol:

Biror dasturiy mahsulotni litsenziyasiz ko‘paytirish mualliflik huquqining buzilishi hisoblanadi.

3. Kiberjinoyatlarga qarshi javobgarlik

Kompyuter tizimlariga noqonuniy kirish, virus tarqatish yoki ma’lumotlarni o‘g‘irlash jinoyat deb hisoblanadi.

Misol:

Bank kartalaridan noqonuniy pul yechib olish bilan shug‘ullangan shaxslar jinoiy javobgarlikka tortiladi.

4. Elektron raqamli imzo

Elektron hujjatlarning haqiqiyligini tasdiqlash uchun ERI (Elektron raqamli imzo) qo‘llaniladi.

Misol:

Soliq hisobotlari elektron tarzda yuborilganda ERI orqali tasdiqlanadi. Bu hujjatning qalbakilashtirilmaganini ko‘rsatadi.

Huquqiy himoya usullari jamiyatda axborot xavfsizligi madaniyatini shakllantirishga xizmat qiladi.

Axborotni himoyalashning texnik usullari

Texnik himoya usullari apparat va dasturiy vositalar orqali amalga oshiriladi. Hozirgi davrda eng samarali himoya aynan texnologik vositalar yordamida ta’minlanmoqda.

1. Antivirus dasturlari

Viruslar kompyuter tizimiga zarar yetkazuvchi dasturlardir. Antiviruslar ularni aniqlaydi va yo‘q qiladi.

Misol:

Kaspersky Anti-Virus yoki ESET NOD32 dasturlari zararli fayllarni aniqlab tizimni himoya qiladi.

2. Firewall (tarmoqlararo ekran)

Firewall kompyuter tarmog‘iga kiruvchi va chiquvchi trafikni nazorat qiladi.

Misol:

Korxona tarmog‘iga noma’lum IP manzildan kirishga urinish firewall tomonidan bloklanadi.

3. Kriptografik himoya

Kriptografiya axborotni shifrlash orqali himoya qiladi.

Misol:

Telegram messenjeridagi yozishmalar maxsus algoritmlar yordamida shifrlanadi. Shu sababli uchinchi shaxslar xabar mazmunini o‘qiy olmaydi.

4. Biometrik himoya

Barmoq izi, yuzni aniqlash yoki ko‘z qorachig‘i orqali autentifikatsiya amalga oshiriladi.

Misol:

Zamonaviy smartfonlarda Face ID yoki Fingerprint tizimi mavjud.

5. Bulutli texnologiyalar xavfsizligi

Bulutli xizmatlardan foydalanishda ma’lumotlarni himoya qilish muhimdir.

Misol:

Google ning Google Drive xizmatida ikki bosqichli autentifikatsiya mavjud.

6. Zaxiralash va tiklash tizimlari

Serverlar uchun RAID texnologiyalari hamda avtomatik backup tizimlari qo‘llaniladi.

Misol:

Katta kompaniyalarda ma’lumotlar bir vaqtning o‘zida bir nechta serverlarda saqlanadi.

Texnik usullar doimiy ravishda takomillashtirib boriladi, chunki kiberxavflar ham rivojlanib bormoqda.

Axborot xavfsizligining zamonaviy muammolari

Bugungi kunda quyidagi tahdidlar keng tarqalgan:

- phishing hujumlari;
- ransomware viruslari;
- DDoS hujumlari;
- ma’lumotlar sizib chiqishi;
- ijtimoiy muhandislik.

Misol:

2024-yilda ko‘plab tashkilotlarda ransomware hujumlari sababli serverlar bloklanib, ma’lumotlarni qayta tiklash uchun katta mablag‘ talab qilingan.

Sun’iy intellekt texnologiyalarining rivojlanishi ham yangi xavflarni yuzaga keltirmoqda. Deepfake texnologiyalari orqali soxta audio va video materiallar tayyorlanmoqda.

Ta’lim tizimida axborot xavfsizligini ta’minlash

Ta’lim muassasalarida elektron jurnal, masofaviy ta’lim platformalari va onlayn test tizimlari qo‘llanilmoqda. Bu esa axborot xavfsizligiga alohida e’tibor talab qiladi.

Muhim choralar:

- talabalar ma’lumotlarini himoya qilish;
- platformalarda kuchli autentifikatsiya;
- o‘qituvchilarni kiberxavfsizlik bo‘yicha o‘qitish;
- elektron resurslarni zaxiralash.

Misol:

Onlayn dars platformasida foydalanuvchi paroli oddiy bo‘lsa, akkaunt buzilishi mumkin. Shu sababli murakkab parollar tavsiya etiladi.

Xulosa

Axborot xavfsizligi bugungi raqamli jamiyatning ajralmas qismiga aylandi. Axborotlarni himoya qilishning tashkiliy, huquqiy va texnik usullari bir-biri bilan uzviy bog‘liq holda qo‘llanilgandagina samarali natija beradi.

Tashkiliy usullar inson omilini nazorat qilishga xizmat qilsa, huquqiy usullar axborot xavfsizligining qonuniy asoslarini yaratadi. Texnik vositalar esa amaliy himoyani ta’minlaydi.

Kelajakda sun’iy intellekt, kvant texnologiyalari va bulutli tizimlarning rivojlanishi bilan axborot xavfsizligi masalalari yanada dolzarb bo‘lib boradi. Shu sababli har bir mutaxassis va foydalanuvchi axborot xavfsizligi madaniyatiga ega bo‘lishi zarur.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni.
2. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni.
3. S.K. G‘aniyev. “Axborot xavfsizligi”. Toshkent, 2017.
4. Bobojonov I.A. “Axborotni ruxsatsiz foydalanishdan himoyalash: huquqiy, tashkiliy va texnik yondashuvlar”.
5. Odilova S.A., Toshboltayev F.O‘. “Axborot xavfsizligi va shaxsiy ma’lumotlarni himoya qilish”.
6. Hayitov S.A. “Axborotlarni himoyalash metodologiyasi”.
7. Aripov M., Begalov B. “Axborot texnologiyalari”. Toshkent.

8. G‘ulomov S.S. “Informatika va axborot texnologiyalari”. Toshkent.
9. Makarova N.V. “Informatika”. Toshkent.
10. Internet manbalari va zamonaviy kiberxavfsizlik portallari.