Impact Factor: 9.9 ISSN-L: 2544-980X

AXBOROTNI MUHOFAZA QILISHNING MAQSAD VA ASOSLARI

Ernazarov Alisher Ergashevich [1]

Boliqulov G‘iyos Samariddin o‘g‘li[2]

Shirinov Nurbek Oydin o‘g‘li[3]

Annotatsiya: *Axborot xavfsizligi zamonaviy axborot jamiyatining muhim jihati hisoblanadi. Axborot xavfsizligining maqsadi ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashdir. Maxfiylik deganda, ma'lumotlar faqat ular uchun mo'ljallangan foydalanuvchilar uchun ochiq bo'lishi va tegishli ruxsatnomalarsiz uchinchi shaxslarga ochiq bo'lmasligi kerakligini anglatadi.*

Kalit so’zlar: *axborot xavfsizligi,doimiy,maqsad,,maxfiylik,mavjudlik,yaxlitlik*

Axborot xavfsizligi zamonaviy axborot jamiyatining muhim jihati hisoblanadi. Axborot xavfsizligining maqsadi ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashdir. Maxfiylik deganda, ma'lumotlar faqat ular uchun mo'ljallangan foydalanuvchilar uchun ochiq bo'lishi va tegishli ruxsatnomalarsiz uchinchi shaxslarga ochiq bo'lmasligi kerakligini anglatadi.

Butunlik ma'lumotlarning noto'g'ri yoki noqonuniy ravishda o'zgartirilmasligini va har doim haqiqat va to'liqligini ta'minlaydi.

Mavjudlik ma'lumotlar foydalanuvchilar uchun kerakli vaqtda va joyda muammosiz yoki kechikishlarsiz mavjud bo'lishi kerakligini anglatadi.

Axborot xavfsizligining kontseptual asosi quyidagi tamoyillarni o'z ichiga oladi:

1. Eng kam imtiyozlar printsipi: foydalanuvchilarga ruxsatsiz kirish yoki foydalanish ehtimolini minimallashtirish uchun ma'lumotlarga kirish uchun faqat zarur huquqlar berilishi kerak.

2. Standart himoya qilish printsipi: Axborot sukut bo'yicha himoyalangan bo'lishi kerak, ya'ni tegishli ruxsat olinmaguncha unga kirish cheklangan bo'lishi kerak.

3. Vazifalarni ajratish printsipi (Majburiyatlarni ajratish): Axborotdan zararli foydalanish ehtimolini oldini olish uchun axborot bilan bog'liq turli vazifalar va operatsiyalar turli shaxslar o'rtasida taqsimlanishi kerak.

4. Murakkablik printsipi: Xavfsizlik mexanizmlari va protseduralari ularni chetlab o'tish yoki buzish ehtimolini minimallashtirish uchun etarlicha murakkab bo'lishi kerak.

5. Uzluksiz himoya qilish printsipi: xavfsizlikni buzish ehtimolini bartaraf etish yoki minimallashtirish uchun axborotni himoya qilish doimiy va doimiy bo'lishi kerak.

6. Aniqlash va javob berish printsipi: Axborot xavfsizligi tizimlari potentsial xavfsizlik hodisalarini aniqlash va ularning ta'sirini minimallashtirish uchun ularga javob berish imkoniyatiga ega bo'lishi kerak.

---

[1] SamISI.

[2] *Kattaqo‘rg‘on servis texnikumi Tabiiy va gumanitar, axborot texnologiyalari kafdrasi mudiri.*

[3] *Kattaqo‘rg‘on servis texnikumi Tabiiy va gumanitar, axborot texnologiyalari kafdrasi o‘qituvchisi.*

Bu tamoyillarning barchasi axborot xavfsizligining kontseptual asosini tashkil etadi va axborot xavfsizligi tizimlarini ishlab chiqish va joriy etishda foydalaniladi.

Axborot xavfsizligi (IS) - bu axborot tizimining holati, unda uchinchi tomon aralashishi va shikastlanishi juda kam seziladi. Ma'lumot xavfsizligi shuningdek, axborotni ochish yoki apparat va dasturiy ta'minotni himoya qilish modullariga ta'sir qilish bilan bog'liq xavflarni boshqarishni ham nazarda tutadi.

Tashkilotda qayta ishlanadigan ma'lumotlarning xavfsizligi - bu kompaniya ichidagi axborot muhitini himoya qilish muammolarini hal etishga qaratilgan harakatlar majmui. Shu bilan birga, ma'lumot vakolatli shaxslar uchun foydalanish va jadal rivojlanish bilan cheklanmasligi kerak.

1. Doimiy. Hujumchi istagan paytda uni qiziqtirgan ma'lumotlarni himoya qilish modullarini chetlab o'tishga harakat qilishi mumkin.

2. Maqsad. Ma'lumotlar tashkilot yoki ma'lumotlar egasi tomonidan belgilangan muayyan maqsadlar uchun himoyalangan bo'lishi kerak.

3. Rejalashtirilgan. Himoyalashning barcha usullari maxfiy ma'lumotlarni himoya qilishni tartibga soluvchi davlat standartlari, qonun va qoidalarga muvofiq bo'lishi kerak.

4. Faol. Operatsiyani qo'llab-quvvatlash va himoya tizimini takomillashtirish bo'yicha tadbirlar muntazam ravishda o'tkazilishi kerak.

5. Birlashtirilgan. Faqat shaxsiy himoya modullaridan yoki texnik vositalardan foydalanishga yo'l qo'yilmaydi. Himoyaning barcha turlarini to'liq qo'llash kerak, aks holda ishlab chiqilgan tizim ma'no va iqtisodiy asosdan mahrum bo'ladi.

6. Umumjahon. Himoya uskunalari kompaniyaning mavjud oqish yo'llariga muvofiq tanlanishi kerak.

7. Ishonchli. Himoyalashning barcha usullari ma'lumotlarni taqdim etish shaklidan qat'i nazar, buzg'unchi tomonidan himoyalangan ma'lumotlarning mumkin bo'lgan yo'llarini to'sib qo'yishi kerak.

DLP tizimi ham ushbu talablarga javob berishi kerak. Va uning imkoniyatlarini nazariy jihatdan emas, balki amalda baholash yaxshidir. Siz 30 kun davomida KIB SearchInform-ni bepul sinab ko'rishingiz mumkin.

Ushbu maqsadlarga erishish uchun autentifikatsiya, avtorizatsiya, shifrlash, xavfsizlik devorlari, antiviruslar, IDS/IPS va boshqalar kabi texnologiyalar va axborot xavfsizligi choralari qo'llaniladi. Shuningdek, axborot xavfsizligining muhim tarkibiy qismlari foydalanuvchilarni axborot xavfsizligi qoidalari haqida o'qitish va xabardor qilishdir.

Umuman olganda axborotni muhofaza qilishning maqsadini quyidagicha ifodalash mumkin:

– axborotni tarqab ketishi, o‘g‘irlanishi, buzilishi, qalbakilashtirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk ob’ekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;
– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfedensialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda sub’ektlarning huquqlarini ta’minlash.

Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi

mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan konsepsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– axborotni muhofaza qilish masalalarini hal etishga ixtisoslashtirilgan tashkilotlarning mavjudligi;

– ushbu muammoga oid etarlicha aniq ifodalangan qarashlar tizimi;

– etarlicha amaliy tajriba va boshqalar.

Biroq, xorijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendensiyasiga ega bo‘lib bormoqda. Axborotni muhofaza qilishning maqsadi ma'lumotlarning maxfiyligi, mavjudligi va yaxlitligini ta'minlashdan iborat.

Axborot xavfsizligining kontseptual asoslari quyidagi tamoyillarga asoslanadi:

1. Maxfiylik - faqat vakolatli shaxslarning ma'lumotlarga cheklangan kirishini ta'minlash. Ma'lumotlarga ruxsatsiz kirishni oldini olish uchun shifrlash, kirishni boshqarish vositalari, foydalanuvchi autentifikatsiyasi va boshqa choralarni o'z ichiga oladi.

2. Mavjudlik - ma'lumotlarning kerakli vaqtda mavjud bo'lishini va foydalanishga tayyorligini ta'minlash. Zaxiralash, ma'lumotlarni takrorlash, tizim ishonchliligi va xatolarga chidamliligini ta'minlash, shuningdek, mavjudlikni buzishga qaratilgan hujumlarning oldini olish va aniqlashni o'z ichiga oladi.

3. Yaxlitlik – axborot xavfsizligi va yaxlitligini ta’minlash. Ma'lumotlarning yaxlitligini tekshirish, raqamli imzolardan foydalanish, axborot o'zgarishlarini nazorat qilish va ruxsatsiz o'zgarishlardan himoya qilishni o'z ichiga oladi.

Foydalanilgan adabiyotlar:

1. *Эрназаров, А. Э., Джўраев, Н., Абороров, Ж., & Абдулла, Қ. (2023). Электрон Хукумат Тизимида Ахборот Хавфсизлигини Таъминлаш. Journal of Innovation in Education and Social Research, 1(4), 110-112.*
2. *Ergashevich, E. A. (2023). INTERNET TARMOG’I AXBOROT XURUJLARI. ИННОВАЦИИ В ПЕДАГОГИКЕ И ПСИХОЛОГИИ, 6(3).*
3. *Zuxra, X., & Ergashevich, E. A. E. A. (2023). AXBOROT TIZIMLARINING TURLARI: ASOSIY JIHATLARI VA QO'LLANILISHI. Synergy: Cross-Disciplinary Journal of Digital Investigation (2995-4827), 1(2), 1-4.*
4. *Ergashevich, E. A. (2023). USE OF SOCIAL NETWORKS IN THE EDUCATIONAL PROCESS. JOURNAL OF ECONOMY, TOURISM AND SERVICE, 2(11), 41-44.*
5. *Ergashevich, E. A. (2023). USE OF SOCIAL NETWORKS IN THE EDUCATIONAL PROCESS. JOURNAL OF ECONOMY, TOURISM AND SERVICE, 2(11), 41-44.*
6. *Ergashevich, E. A. (2023). Internet Tarmog ‘i Xizmat Turlarining Zamonaviy Tahlili. Journal of Innovation in Education and Social Research, 1(3), 174-176.*
7. *Ernazarov, A. Methodology for modern organization of training education and its implementation. 2020 International Journal of Advanced Science and Technology. 29(5), c. 1979-1982*