HIMOYALANGAN AXBOROT TIZIMLARIDA FUNKSIONAL TALABLAR. HIMOYA AUDITI, IDENTIFIKATSIYA VA AUTENTIFIKATSIYA

Muallif: ***Ro‘ziqulova Fotima***
Samarqand davlat universiteti Urgut filiali,
Biznesni boshqarish va tabiiy fanlar
fakulteti, 3-bosqich talabasi
fotimaruzikulova04@gmail.com
Ilmiy rahbar: ***Suyarov Akram***
Samarqand iqtisodiyot va servis instituti, dotsent
akramsuyarov@mail.ru

Annotatsiya

Ushbu maqolada himoyalangan axborot tizimlarida funksional talablar, himoya auditi, identifikatsiya va autentifikatsiya tizimlarining ahamiyati, ishlash prinsiplari va ularga qo‘yiladigan talablar yoritilgan. Axborot xavfsizligini ta’minlashda ushbu komponentlarning har biri muhim rol o‘ynaydi. Maqolada texnik jihatlar, normativ talablar, amaliy tajribalar va tavsiyalar asosida mavzu chuqur tahlil qilinadi.

Kalit so‘zlar: *axborot tizimi, funksional talablar, himoya auditi, identifikatsiya, autentifikatsiya, xavfsizlik siyosati.*

1. Kirish

Axborot texnologiyalari keng rivojlangan hozirgi davrda axborotni himoyalash masalasi dolzarb bo‘lib qolmoqda. Tashkilot va korxonalarning axborot resurslari raqamli muhitga o‘tishi bilan birga ularni himoya qilish zarurati ham oshmoqda. Ayniqsa, himoyalangan axborot tizimlari uchun funksional talablarni to‘g‘ri belgilash va ularni amalda ta’minlash muhim ahamiyat kasb etadi. Ushbu maqolada axborot tizimlaridagi funksional xavfsizlik talablarining asosiy komponentlari — himoya auditi, identifikatsiya va autentifikatsiya jarayonlari yoritiladi.

2. Asosiy qism

2.1. Himoyalangan axborot tizimlarida funksional talablar

Funksional xavfsizlik talablar — bu axborot tizimida xavfsizlikni ta’minlash uchun qanday vazifalar bajarilishi kerakligini ko‘rsatadigan texnik va tashkiliy talablar yig‘indisidir. Bular quyidagilarni o‘z ichiga oladi:

- Kirishni nazorat qilish (Access Control)
- Ma’lumotlarni shifrlash va shifrdan chiqarish
- Xodimlar faoliyatini monitoring qilish
- Ma’lumotlar bazasining yaxlitligi va izchilligini ta’minlash
- Foydalanuvchi harakatlarini qayd etish va nazorat qilish

Barcha funksional talablar ISO/IEC 27001 va O‘zbekiston Respublikasi qonunchiligi asosida ishlab chiqilishi lozim.

2.2. Himoya auditi

Himoya auditi — bu axborot tizimidagi xavfsizlik holatini doimiy ravishda nazorat qilish va baholash vositasi bo‘lib, quyidagi maqsadlarga xizmat qiladi:

- Tizimdagi ruxsatsiz kirish harakatlarini aniqlash
- Foydalanuvchi faoliyatining hujjatlashtirilgan yozuvlarini yuritish
- Xavfsizlik siyosatiga rioya qilinayotganini tekshirish
- Xavfsizlik bo‘yicha muammolar va zaifliklarni aniqlash

Audit quyidagi komponentlarni o‘z ichiga oladi:

Audit komponenti	**Tavsifi**
Audit jurnallari	Har bir harakat yozib boriladi
Real vaqtli monitoring	Tizim harakatlari onlayn kuzatib boriladi
Xavfsizlik tahlili	Anomaliyalar va hujumlar aniqlanadi
Hisobotlar	Rivojlanish holati va muammolar yoritiladi

2.3. Identifikatsiya va autentifikatsiya

Identifikatsiya — bu foydalanuvchining kimligini aniqlash jarayoni. **Autentifikatsiya** esa — bu foydalanuvchining da’vo qilinayotgan shaxs ekanini tasdiqlash jarayoni hisoblanadi. Bu ikki jarayon birgalikda ishlaydi va xavfsizlikning birinchi darajali to‘sig‘ini tashkil etadi.

Identifikatsiya vositalari:

- Login, ID raqamlar
- Biometrik ko‘rsatkichlar (barmoq izi, ko‘z to‘r pardasi)

Autentifikatsiya usullari:

- Parol orqali
- Bir martalik kodlar orqali (OTP)
- Token yoki smart-karta yordamida
- Biometrik autentifikatsiya

Zamonaviy tizimlar ko‘p bosqichli autentifikatsiyani (Multi-Factor Authentication) qo‘llaydi. Bu usulda bir nechta xavfsizlik omillari (parol + SMS + barmoq izi) birgalikda ishlatiladi.

2.4. Tavsiyalar va amaliy yondashuvlar

Axborot xavfsizligini ta’minlashda quyidagilar muhim hisoblanadi:

- Har bir foydalanuvchiga o‘ziga xos identifikator berilishi
- Audit tizimining uzluksiz ishlashini ta’minlash
- Autentifikatsiya uchun kuchli parol siyosatini ishlab chiqish
- Autentifikatsiya jarayonini foydalanuvchi uchun qulay va tez amalga oshirish
- Xavfsizlik siyosatini va foydalanuvchi huquqlarini doimiy yangilab borish

3. Xulosa

Himoyalangan axborot tizimlarida funksional talablar, jumladan himoya auditi, identifikatsiya va autentifikatsiya jarayonlari tizim xavfsizligini ta’minlashda muhim o‘rin egallaydi. Har bir elementning o‘zaro uyg‘un ishlashi orqali foydalanuvchilarning axborotga ruxsatli kirishi va ruxsatsiz kirishga qarshi ishonchli himoya yaratiladi. Zamonaviy texnologiyalar asosida ishlab chiqilgan, talablar asosida mustahkamlangan xavfsizlik tizimi tashkilotning axborot aktivlarini ishonchli himoya qiladi.

Foydalanilgan adabiyotlar

1. Qodirov M. (2020). Axborot xavfsizligi asoslari. Toshkent: "Fan va texnologiya".
2. Karimov R. (2021). Kompyuter tizimlari va xavfsizlik. Samarqand: SamDU nashriyoti.
3. Xasanov B. (2019). Axborot tizimlarida identifikatsiya va autentifikatsiya. Toshkent: TATU nashriyoti.
4. ISO/IEC 27001:2022. Axborot xavfsizligi boshqaruv tizimi standartlari.
5. Stallings W. (2017). Network Security Essentials. Pearson Education.
6. Tanenbaum A. (2015). Modern Operating Systems. Pearson Education.
7. Xolboyev A. (2023). Dasturiy xavfsizlik va himoyalangan tizimlar. Urganch: Ixtisoslashgan nashriyot.