



## AXBOROT XAVFSIZLIGINI TA'MINLASHNING ASOSIY VAZIFALARI VA DARAJALARI

Davlatov Ramazon Abdumo'min o'g'li

*TerDU Matematika va informatika yo'nalishi talabasi*

**Annotatsiya:** Jamiyatning jadal sur'atlarda axborotlashtirilishi sababli axborot xavfsizligi muammosi nihoyatda dolzarb va doimo shunday bo'lib qoladi. Ushbu maqolada axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo'ladigan tahdidlar, kriptologiya maqsadlari va uning qarama-qarshi ikki yo'nalishi ya'ni kriptografiya va kriptotahlil yo'nalishlari haqida batafsil ma'lumotlar berilib o'tilgan. Axborotlarni ishonchli himoyalash masalalari ko'rib o'tildi.

**Kalit so'zlar:** Axborot xavfsizligi, konfidensiallik, yaxlitlik, indentifikatsiya, autentifikatsiya, vakolat berish, foydalanishni nozoratlash, mulklik huquqi, sertifikatatsiya, imzo, voz kechmaslik, sanasini yozish, olganligiga tilxat berish, bekor qilish, anonimlik.

Kompyuter texnikasi va axborot tizimlarining iqtisodda, boshqarishda, aloqada, ilmiy tadqiqotlarda, ta'limda, xizmat ko'rsatish sohasida, tijoratda, moliya va inson faoliyatining boshqa sohalarida qo'llashining rivoji axborotlashtirish va umuman, jamiyat rivojini belgilovchi yo'nalish hisoblanadi. Kompyuter texnikasining qo'llanilishi evaziga erishuvchi samara axborot ishlanishi ko'lamining oshishi bilan ortib boradi. Ushbu texnikaning qo'llanish sohalarini va ko'lamini uning ishlashining ishonchliligi va barqarorligi muomalari bilan bir qatorda unda aylanuvchi axborot xavfsizligini ta'minlash muammosini tug'diradi.

Axborotni muhofaza qilish masalalari bilan kriptologiya (kriptos-maxiy, logos-ilm) fani shug'ullanadi. Kriptologiya maqsadlari o'zaro qarama-qarshi ikkita yo'nalishga ega bo'lgan- kriptografiya va kriptotahlil yo'nalishlariga ajraladi.

Kriptografiyaning ochiq ma'lumotlarni shifrlash masalalarining matematik uslublari bilan shug'ullanishi to'g'risida yuqorida aytib o'tildi.

Kriptotahlil esa shifrlash uslubi (kaliti yoki algoritmi) ni bilmagan holda shifrlangan ma'lumotni asl holatini (mos keluvchi ochiq ma'lumotni) topish masalalarini yechish bilan shug'ullanadi.

Hozirgi zamon kriptografiyasi quyidagi bo'limlarni o'z ichiga oladi:

- Simmetrik kriptotizimlar.
- Ochiq uslubga yoki yana boshqacha aytganda ochiq kalitlar algoritimiga asoslangan kriptotizimlar.
- Eliktron raqamli imzo kriptografik tizimlari.
- Kriptotizimlar uchun kriptobardoshlik kalitlarini ishlab chiqish va ulardan foydalanishni boshqarish.

Tadqiqot materiallari va metodologiyasi.

Axborot xavfsizligini ta'minlash muntazam va kompleks xarakterga ega ko'p qirrali faoliyatni amalga oshirishni ko'zda tutadi. Uni amalga oshirishda axborot xavfsizligidan



manfaatdor taraflar oldida qo'yiladigan vazifalarga alohida e'tibor berish zarur. Ushbu turli-tuman vazifalarni bir necha quyidagi asosiy guruhlariga ajratish mumkin:

1. Axborotdan foydalanishni ta'minlash, ya'ni maqbul vaqt mobaynida axborot xizmatini olish hamda axborotni olishda ruhsatsiz taqiqlanishni bartaraf etish;

2. Axborot yaxlitligini ta'minlash, ya'ni axborotning ruhsatsiz modifikatsiyalanishini yoki buzilishini bartaraf etish;

3. Axborot konfidensialligini ta'minlash, ya'ni axborotdan ruhsatsiz tanishishni bartaraf etish.

Axborot xavfsizligi – mamlakat madaniy mulkining, xo'jalik sub'ektlari va fuqorolar intellektual mulkining, davlat va kasbiy sirga maxsus ma'lumotlarning ishonchli himoyalanganligi holati.

Odatda, bir-biridan axborat xavsizligining huquqiy, texnik, moliyaviy, tashkiliy va boshqa resursli ta'minot bilan farqlanuvchi axborat xavsizligi sub'ektlarining quyidagi to'rtta kategoriyasi ajratiladi:

- butun bir davlat;
- davlat tashkilotlari;
- tijorat tuzilmalari;
- alohida fuqoralar.

Yuqorida keltirilgan axborot xavsizligini ta'minlashdagi asosiy vazifalar qamrab olgan quyidagi keng spektrli masalalarni ko'rib chiqish joiz hisoblanadi:

- konfidensiallik;
- yaxlitlik;
- indentifikatsiya;
- autentifikatsiya;
- vakolat berish;
- foydalanishni nozoratlash;
- mulklik huquqi;
- sertifikatsiya;
- imzo;
- voz kechmaslik;
- sanasini yozish;
- olganligiga tilxat berish;
- bekor qilish;
- anonimlik.

Yuqorida keltirilgan vazifalar mavjud axborot dunyosi ehtiyojiga asosan tavsiflangan. Vaqt o'tishi bilan ba'zi vazifalar o'z dolzarbligini yo'qotishi va aksincha, yechimini kutuvchi yangi vazifalar paydo bo'lishi mumkin.

**Xulosa** qilib shuni aytish mumkinki, axborotlarni saqlash va uzatish tizimlari bir tomondan takomillashib murakkablashgan va ikkinchi tomondan axborotlardan foydalanuvchilar uchun keng qulayliklar vujudga kelgan davrda, axborotlarni maqsadli boshqarishning qator muhim masalalari kelib chiqadi. Bunday masalalar qatoriga katta



hajimdagi axborotlarning tez va sifatli uzatish hamda qabul qilish axborotlarni ishonchligini ta'minlash, axborotlar tizimida axborotlarni begona shaxslardan (keng ma'noda) muhofaza qilish kabi ko'plab boshqa masalalar kiradi.

#### FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. S. K. Ganiyev, M. M. Karimov, K.A. Tashev. Axborot xavfsizligi. T. , 2017 yil.
2. S. S. Qosimov. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi.
3. M. Aripov, B. Begalov, U. Begimqulov, M. Mamarajabov. Axborot texnologiyalari. T. 2009 yil.