ILMIY AXBOROTNI HOMOYA QILISHDA KIBERXAVFSIZLIK TAMOYILLARINING O’RNI

Mamalatifov Amirjon Farruxovich
Sharof Rashidov nomidagi Samarqand Davlat Universiteti Sun’iy Intellekt va Raqamli Texnologiyalar fakulteti Axborot tizimlari va texnologiyalari yo‘nalishi 105-guruh talabasi
M.A.Axrorova
Ilmiy rahbar: PhD
https://doi.org/10.5281/zenodo.17657027

ARTICLE INFO

Qabul qilindi: 10-noyabr 2025 yil
Ma’qullandi: 15- noyabr 2025 yil
Nashr qilindi: 20- noyabr 2025 yil

KEY WORDS

Kiberxavfsizlik, ilmiy axborot, axborotni himoya qilish, akademik yozuv, maxfiylik, butunlik, mavjudlik, plagiat, axborot madaniyati, akademik halollik, kiber gigiyena, sun’iy intellekt, axborot texnologiyalari, ilmiy tadqiqotlar xavfsizligi, raqamli muhit.

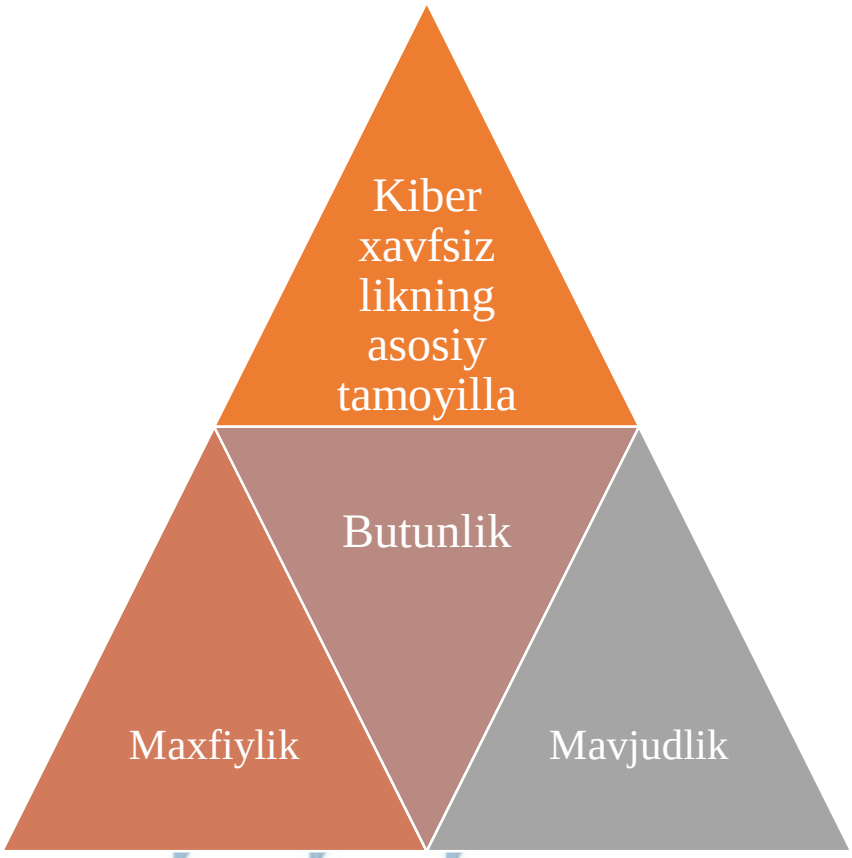
ABSTRACT

Ushbu maqolada ilmiy axborotni himoya qilish jarayomida kiberxavfsizlik tamoyillarining o’rni va ahamiyati yoritilgan. Raqamli texnologiyalar tez sur’atlarda rivojlanayotgan bugungi kunda ilmiy ma’lumotlarning maxfiyligi, butunligi va ishonchliligini taminlash muhim masalalardan biridir. Maqolada kiberxavfsizlikning asosiy tamoyillari – maxfiylik, butunlik va mavjudlik – ilmiy faoliyatda qanday qo’llanilishi tahlil qilinadi. Shuningdek, akademik muhitda ma’lumot o’g’irlanishining oldini olishda kiberxavfsizlik choralarining ahamiyati muhokama etiladi. Tadqiqot natijalariga ko’ra, ilmiy axborotni himoya qilish madaniyatini rivojlantirish akademik halollikni mustahkamlash va ilmiy tadqiqotlar sifatini oshirishga xizmat qiladi..

Raqamli texnologiyalar tez sur’atlarda rivojlanayotgan davrda ilmiy axborotning xavfsizligi dolzarb masalalardan biriga aylandi. Ilmiy faoliyat jarayonida katta hajmda katta hajmda ma’lumotlar yaratiladi, qayta ishlanadi va saqlanadi. Ushbu ma’lumotlar ilmiy izlanishlarning asosiy poydevori hisoblanadi. Shuning uchun ilmiy axborotning maxfiyligi, butunligi va mavjudligini ta’minlash ilmiy jarayonning muhim shartidir. Kiberxavfsizlik tamoyillari ilmiy axborotni himoya qilishga xizmat qiladi. Maxfiylik axborotga faqat ruxsatt berilgan shaxslarning kirishini ta’minlasa, butunlik ma’lumotlarning o’zgarmagan holda saqlanishiga yordam beradi. Mavjudlik esa zarur paytda ma’lumotlarning foydalanishga tayyor bo’lishini anglatadi. Bu tamoyillarni to’g’ri qo’llash ilmiy tadqiqotlar sifatini oshiradi, ilmiy halollikni mustahkamlaydi va ilmiy natijalarning ishonchliligini kafolatlaydi.

1. Kiberxavfsizlik tamotillarining nazariy asoslari.

Kiberxavfsizlik uch asosiy tamoyilga tayanadi: maxfiylik, butunlik va mavjudlik. Bu tamoyillar har qanday axborotni himoya qilish tizimining poydevorini tashkil qiladi.



1.1. Maxfiylik

Maxfiylik – bu axborotga ruxsatsiz begona shaxslarning kirishiga yo’l qo’ymaslikdir. Ilmiy axborot ko’pincha muhim natijalar, kashfiyotlar, yangi texnologiyalar, tadqiqot metodlari va grant loyihalari bilan bog’liq bo’lgani uchun ularning maxfiyligini ta’minlash muhimdir. Maxfiylikni ta’minlashda zamonaviy shifrlash tizimlari, himoyalangan serverlar, kirish darajalari va ikki bosqichli autenfikatsiyani juda muhim o’rin tutadi.

Axborotning maxfiyligini buzish oqibatida:

- Ilmiy natijalar o’g’irlanishi;
- Plagiat holatlari oshishi;
- Ilmiy loyihalarning moliyaviy xavfi;
- Ilmiy kashfiyotlarning boshqa shaxslar tomonidan egallab olinishi mumkin.

1.2. Butunlik

Butunlik tamoyili ma’lumotlarning o’zgarmasligi, aniq saqlanishi va ruxsatsiz tahrir qilinmasligini anglatadi. Ilmiy tajribalar, statistik ma’lumotlar, laboratoriya natijalari va ilmiy dalillarning o’zgarishi natijasida tadqiqotning noto’g’ri xulosalarga olib kelishiga sabab bo’ladi. Shu bois ma’lumotlar butunligini himoya qilish juda muhimdir.

Buzilish xavflari:

- Zararli dasturlar orqali ma’lumotni o’zgartirish;
- Sever xatoliklari;
- Ruxsatsiz kirish;
- Texnik nosozlik.

1.3. Mavjudlik

Mavjudlik – bu ma’lumotlar har doim foydalanishga tayyor bo’lishi kerakligini bildiradi. Ilmiy jarayon uzluksiz bo’lishi uchun ma’lumotlarga istalgan vaqt kirish imkoniyati bo’lishi shart. Mavjudlikni buzish ilmiy ishlarga jiddiy to’sqinlik qiladi.

Mavjudlikka tahdidlar:

- DDoS hujumlar;
- Internet tarmog’idagi uzilishlar;
- Serverning ishdan chiqishi;
- Ma’lumotlar bazasining bloklanishi.

2. Ilmiy Axborotga Tahditlar Va Raqamli Xavf- Xatarlar

Ilmiy axborotga tahdidlar tobora ortib bormoqda. Zamonaviy kiberhujumlar murakkablashib borayotgani sababli himoya tizimlarini takomillashtirish zarur.

2.1. Plagiat va ma’lumot o’g’irlanishi

Plagiat – bu ilmiy halollikning eng katta dushmanidir. Plagiat holarlari ayniqsa talabalik va ilmiy tadqiqot jarayonida jo’p uchraydi. Intellektual mulkni o’g’irlash ilmiy salohiyatga jiddiy zarar yetkazadi.

2.2. Fishing va zararli dasturlar

Fishing xabarlari orqali zararli fayllar yuborilib, foydalanuvchilarning shaxsiy ma’lumotlari, parollari, elektron pochta tizimlariga kirish huquqlari o’g’irlanadi. Ilmiy muassasalar uchun bu katta xavf hisoblanadi, chunki ular ko’plab maxfiy ma’lumotlarga ega.

2.3. Server va tizim hujumlari

Ilmiy tashkilotlar server kiberjinoyatchilar uchun muhim nishondir. Tadqiqot natijalarining yo’qolishi, serverning ishdan chiqishi yoki ma’lumotlarning o’chib ketishi ilmiy jarayonga jiddiy zarar yetkazadi.

2.4. Sun’iy intellektdan noto’g’ri foydalanish

Sun’iy intellekt xatolikka yo’l qo’ysa, noto’g’ri ilmiy natijalar paydo bo’lishi munkin. AI yordamida tayyorlangan matnlar ba’zan plagiatga o’xshash bo’lishi yoki tekshirilmagan ma’lumotlarga asoslangan ehtimoli bor.

3. Ilmiy Muassasalarda Kiberxavfsizlikni Ta’minlash Choralari

3.1. Kiber gigiyena

Har bir ilmiy xodim:

- Kuchli paroldan foydalanishi;
- Shubhali havolalardan qochishi;
- Muntazam ravishda tizimlarni yangilab borishi lozim

3.2. Ma’lumotlarni zaxiralash

Zaxira nusxalar (backup) ilmiy axborotning yo’qolishining oldini oladi. Bulutli texnologiyalar (cloud storage) bu jarayonda eng qulay vositalardan biridir.

3.3. Himoyalangan platformalardan foydalanish

Elsevier, Scopus, Web of Science kabi platformalar ilmiy ma’lumotlarni xavfsiz saqlaydi va himoya vositalari bilan ta’minlaydi.

3.4. Plagiat aniqlash tizimlari

Turnitin, Antiplagiat, PlagScan kabi dasturlar ilmiy halollikni nazorat qilishning samarali usullaridan biridir.

3.5. Axborot xavfsizligi siyosati

Har bir muassasa o’zining axborot xavfsizligini siyosatini ishlab chiqishi kerak:

- Xavfsizlik qoidalari;
- Ma;lumotlar almashinuvi protokollari;
- Parollar siyosati;
- Favqulodda vaziyat rejasi.

Ilmiy axborotni himoya qilish ilmiy jarayonning muhim tarkibiy qismidir. Maxfiylik, butunlik va mavjudlik tamoyillariga rioya qilish ilmiy faoliyatning samaradorligini oshiradi. Kiberxavfsizlikni ta’minlash bo’yicha choralar choralar ilmiy halollikni mustahkamlaydi, ma’lumotlar bilan ishlash madaniyatini rivojlantiradi va global ilmiy hamjamiyatda ishonchni oshiradi.

Foydalanilgan adabiyotlar:

1. Stallings, W. Network Security Essentials: Applications and Standards. Person, 2020.
2. Kurose, J. Ross, K.Computer Networking: A Top - Down Approach. Pearson, 2021.
3. Shay, W. Understanding Cybersecurity. Cengage Learning, 2019.
4. Pfleeger, C.Pfleeger, S. Margulies, J. Security in Computing. Pearson, 2015.
5. Kovacs, E.Cybersecurity for Information Professionals. CRC Press, 2022.
6. www.google.uz