



## TA'LIM MUASSASALARIDA AXBOROT XAVFSIZLIGINI TA'MINLASH MASALALARI

**Alijon Muhammadiyev Ulug'bekovich**

Shahrisabz davlat pedagogika instituti  
Matematika va informatika yo'nalishi talabasi

**Normurodova Sadoqat Xoliqulovna**

Shahrisabz davlat pedagogika instituti  
Matematika va ta'limda axborot texnologiyasi kafedrası katta o'qituvchi

Email: sadoqatnormurodova33@gmail.com

<https://orcid.org/0009-0009-1604-7456>

<https://doi.org/10.5281/zenodo.18016006>

### ARTICLE INFO

Qabul qilindi: 15-dekabr 2025 yil

Ma'qullandi: 18-dekabr 2025 yil

Nashr qilindi: 22-dekabr 2025 yil

### KEY WORDS

axborot xavfsizligi, ta'lim muassasasi, kiberxavfsizlik, ma'lumotlarni himoya qilish, raqamli savodxonlik, xavf va risklarni boshqarish.

### ABSTRACT

*Maqolada ta'lim muassasalarida axborot xavfsizligini ta'minlashning nazariy va amaliy masalalari tahlil qilingan. Axborot xavfsizligi ta'lim jarayonining uzluksizligi, ma'lumotlarning maxfiyligi va yaxlitligini ta'minlashga xizmat qiladi. Tadqiqotda axborot xavfsizligini boshqarishning tashkiliy, texnik, huquqiy va pedagogik chora-tadbirlari, shuningdek, xavf va risklarni boshqarish, xalqaro standartlar va favqulodda vaziyatlarga tayyorgarlik masalalari yoritilgan. Maqola natijalari ta'lim muassasalarida axborot xavfsizligini mustahkamlash va pedagogik jarayonni samarali tashkil etishda amaliy ahamiyatga ega.*

Zamonaviy ta'lim tizimining jadal raqamlashtirilishi ta'lim muassasalarida axborot-kommunikatsiya texnologiyalaridan keng foydalanishni taqozo etmoqda. Elektron hujjat aylanishi, masofaviy ta'lim platformalari, raqamli baholash tizimlari va ma'lumotlar bazalarining joriy etilishi ta'lim jarayonining samaradorligini oshirish bilan birga, axborot xavfsizligini ta'minlash masalasini ham dolzarb muammolardan biriga aylantirmoqda. Ta'lim muassasalarida axborot resurslarining himoyalanganligi o'quvchilar va xodimlarning shaxsiy ma'lumotlariga zarar yetkazilishi, ta'lim jarayonining uzilishi hamda axborot tizimlarining ishdan chiqishiga olib kelishi mumkin.

Axborot xavfsizligi — bu axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga qaratilgan tashkiliy, texnik va huquqiy chora-tadbirlar majmuasidir. Ta'lim muassasalarida axborot xavfsizligini ta'minlash nafaqat texnologik masala, balki pedagogik, boshqaruv va huquqiy jihatlarni ham o'z ichiga oladi. Xususan, ta'lim jarayoni ishtirokchilarida axborot xavfsizligi madaniyatini shakllantirish, raqamli savodxonlikni oshirish va mas'uliyatli foydalanish ko'nikmalarini rivojlantirish muhim ahamiyat kasb etadi.

Bugungi kunda kiberxavfsizlikka tahdidlarning ko'payishi, zararli dasturlar, fishing hujumlari hamda ma'lumotlarning noqonuniy tarqalishi ta'lim muassasalarida axborot xavfsizligini kompleks yondashuv asosida tashkil etishni talab etmoqda. Shu bois, axborot xavfsizligini ta'minlash mexanizmlarini takomillashtirish, zamonaviy himoya vositalarini joriy etish va me'yoriy-huquqiy bazani mustahkamlash masalalarini ilmiy jihatdan tahlil qilish dolzarb hisoblanadi.

Ta'lim muassasalarida axborot xavfsizligini ta'minlash zamonaviy raqamli ta'lim muhitining ajralmas qismi hisoblanadi. Bugungi kunda ta'lim jarayonida elektron ma'lumotlar bazalari, masofaviy ta'lim platformalari, raqamli baholash tizimlari va axborot-kommunikatsiya texnologiyalaridan keng foydalanilayotgani axborot xavfsizligiga bo'lgan talabni yanada kuchaytirmoqda. Ta'lim muassasalarida saqlanadigan axborotlar, xususan, o'quvchilar va xodimlarning shaxsiy ma'lumotlari, o'quv rejalari, baholash natijalari va moliyaviy hujjatlar turli kiberxavflarga duch kelishi mumkin.

Axborot xavfsizligi tushunchasi axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlash tamoyillariga asoslanadi. Maxfiylik axborotga faqat ruxsat etilgan shaxslar tomonidan kirishni nazarda tutsa, yaxlitlik axborotning ruxsatsiz o'zgartirilishidan himoyalanihini anglatadi. Mavjudlik esa axborot tizimlarining uzluksiz ishlashini va zarur vaqtda foydalanuvchilar uchun ochiq bo'lishini ta'minlashni talab etadi. Ushbu tamoyillarni ta'lim muassasalarida amalga oshirish axborot xavfsizligini ta'minlashning asosiy mezonlari hisoblanadi.

Ta'lim muassasalarida axborot xavfsizligiga tahdidlar ichki va tashqi omillar bilan bog'liq bo'lishi mumkin. Ichki tahdidlarga xodimlar va o'quvchilarning axborot xavfsizligi qoidalariga rioya qilmasligi, parollarning himoyasizligi, ruxsatsiz dasturlardan foydalanish kabi holatlar kiradi. Tashqi tahdidlar esa zararli dasturlar, fishing hujumlari, tarmoq hujumlari va ma'lumotlarni noqonuniy qo'lga kiritish bilan bog'liqdir. Ushbu tahdidlar ta'lim jarayonining uzilishiga, ma'lumotlarning yo'qolishiga yoki oshkor bo'lishiga olib kelishi mumkin.

Axborot xavfsizligini ta'minlashda tashkiliy chora-tadbirlar muhim ahamiyat kasb etadi. Ta'lim muassasalarida axborot xavfsizligi siyosatini ishlab chiqish, foydalanuvchilarning vakolatlarini aniq belgilash, axborot tizimlaridan foydalanish bo'yicha ichki me'yoriy hujjatlarni joriy etish zarur. Shuningdek, o'qituvchilar, xodimlar va o'quvchilar uchun axborot xavfsizligi bo'yicha muntazam trening va seminarlar tashkil etish axborot xavfsizligi madaniyatini shakllantirishga xizmat qiladi.

Texnik jihatdan axborot xavfsizligini ta'minlash zamonaviy himoya vositalaridan foydalanishni talab etadi. Antivirus dasturlari, tarmoq ekranlari (firewall), ma'lumotlarni shifrlash, autentifikatsiya va avtorizatsiya tizimlari axborot tizimlarini himoyalashda muhim rol o'ynaydi. Bundan tashqari, zaxira nusxalarini yaratish va favqulodda vaziyatlarda ma'lumotlarni tiklash mexanizmlarini yo'lga qo'yish ta'lim muassasalarida axborot resurslarining xavfsizligini ta'minlashda muhim omil hisoblanadi.

Axborot xavfsizligini ta'minlashning huquqiy jihatlari ham alohida e'tiborga loyiqdir. Ta'lim muassasalari milliy qonunchilik va me'yoriy-huquqiy hujjatlarga muvofiq ravishda shaxsiy ma'lumotlarni himoya qilish, axborot resurslaridan qonuniy foydalanishni ta'minlashi lozim. Bu borada mas'ul shaxslarning javobgarligini belgilash va axborot xavfsizligi talablariga rioya etilishini nazorat qilish muhim ahamiyatga ega.

Shuningdek, ta'lim muassasalarida axborot xavfsizligini ta'minlashda pedagogik yondashuv ham muhim o'rin tutadi. O'quvchilarda axborot savodxonligi, raqamli madaniyat va kiberxavfsizlik ko'nikmalarini shakllantirish ularning axborot resurslaridan ongli va xavfsiz foydalanishini ta'minlaydi. Bu esa nafaqat ta'lim muassasasining, balki jamiyatning umumiy axborot xavfsizligini mustahkamlashga xizmat qiladi.

Umuman olganda, ta'lim muassasalarida axborot xavfsizligini ta'minlash kompleks yondashuvni talab etuvchi muhim jarayon bo'lib, tashkiliy, texnik, huquqiy va pedagogik chora-

tadbirlarning uyg'unligi asosida samarali natijalarga erishish mumkin. Axborot xavfsizligining ta'minlanishi ta'lim jarayonining uzluksizligi, ta'lim sifati va ishtirokchilarning ishonchini mustahkamlashda muhim ahamiyat kasb etadi.

Axborot xavfsizligini ta'minlashda risklarni boshqarish yondashuvi muhim ahamiyat kasb etadi. Ta'lim muassasalarida mavjud axborot resurslari va axborot tizimlariga tahdidlarni aniqlash, ularning ehtimollik darajasi va keltirishi mumkin bo'lgan zararni baholash orqali xavfsizlik choralari rejalashtirish mumkin. Risklarni baholash asosida ustuvor himoya yo'nalishlarini belgilash axborot xavfsizligini ta'minlash jarayonining samaradorligini oshiradi.

Ta'lim muassasalarida axborot xavfsizligini boshqarish tizimini joriy etish zamonaviy talablar darajasida muhim hisoblanadi. Bunday tizim axborot xavfsizligi bo'yicha mas'ul shaxslarni tayinlash, xavfsizlik hodisalarini qayd etish va tahlil qilish, shuningdek, doimiy monitoringni amalga oshirishni o'z ichiga oladi. Axborot xavfsizligi insidentlariga tezkor javob berish mexanizmlarining mavjudligi ta'lim jarayonida yuzaga kelishi mumkin bo'lgan uzilishlarning oldini olishga xizmat qiladi.

Bulutli texnologiyalardan foydalanishning kengayishi ta'lim muassasalarida axborot xavfsizligiga nisbatan yangi yondashuvlarni talab etmoqda. Bulutli muhitda ma'lumotlarni saqlash va qayta ishlash qulayliklar bilan birga, ularni himoyalash masalasini ham dolzarb qiladi. Shu sababli, ma'lumotlarni shifrlash, foydalanuvchilarni ko'p bosqichli autentifikatsiyadan o'tkazish hamda xizmat ko'rsatuvchi provayderlarning xavfsizlik standartlariga muvofiqligini baholash muhim hisoblanadi.

Shuningdek, axborot xavfsizligini ta'minlashda inson omili alohida o'rin tutadi. Amaliyot shuni ko'rsatadiki, axborot xavfsizligi bilan bog'liq muammolarning aksariyati foydalanuvchilarning ehtiyotsizligi yoki yetarli bilimga ega emasligi natijasida yuzaga keladi. Shu bois, ta'lim muassasalarida xodimlar va o'quvchilar uchun muntazam ravishda axborot xavfsizligi bo'yicha o'quv mashg'ulotlari, amaliy seminarlar va tushuntirish ishlari olib borilishi zarur.

Axborot xavfsizligini ta'minlashda xalqaro tajribani o'rganish va joriy etish ham muhim ahamiyatga ega. ISO/IEC 27001 kabi xalqaro axborot xavfsizligi standartlaridan foydalanish ta'lim muassasalarida axborot xavfsizligini boshqarish tizimini takomillashtirishga yordam beradi. Ushbu standartlar asosida ishlab chiqilgan ichki siyosat va reglamentlar axborot resurslarining ishonchli himoyasini ta'minlashga xizmat qiladi.

Ta'lim muassasalarida axborot xavfsizligini ta'minlashning muhim yo'nalishlaridan biri sifatida favqulodda vaziyatlarga tayyorgarlik masalasi ham ko'rib chiqilishi lozim. Texnik nosozliklar, kiberhujumlar yoki tabiiy ofatlar natijasida axborot tizimlarining ishdan chiqishi ehtimolini inobatga olgan holda zaxira nusxalarini yaratish, axborotlarni tezkor tiklash rejalari va uzluksizlik strategiyalarini ishlab chiqish ta'lim jarayonining barqarorligini ta'minlaydi.

Shu tariqa, ta'lim muassasalarida axborot xavfsizligini ta'minlash faqat texnik muammo bo'lib qolmay, balki boshqaruv, pedagogik va huquqiy jihatlarini qamrab oluvchi murakkab tizim sifatida namoyon bo'ladi. Ushbu yondashuv asosida olib borilgan faoliyat ta'lim muassasalarida raqamli muhitning ishonchliligi va barqarorligini ta'minlashga xizmat qiladi.

### **Xulosa**

Ta'lim muassasalarida axborot xavfsizligini ta'minlash bugungi raqamli ta'lim muhitida dolzarb va strategik ahamiyatga ega muammo sifatida namoyon bo'lmoqda. Tadqiqot natijalari shuni ko'rsatdiki, ta'lim jarayonida elektron platformalar, ma'lumotlar bazalari va masofaviy

ta'lim tizimlaridan keng foydalanish nafaqat ta'lim sifatini oshirish imkonini beradi, balki axborot xavfsizligiga doimiy e'tibor qaratishni talab qiladi.

Axborot xavfsizligini ta'minlashning samarali mexanizmi tashkiliy, texnik, huquqiy va pedagogik chora-tadbirlarning uyg'unligiga bog'liq. Tashkiliy jihatdan siyosat va qoidalar ishlab chiqish, mas'ul shaxslarni belgilash, muntazam monitoring va xodimlar hamda o'quvchilarni malaka oshirish muhim ahamiyat kasb etadi. Texnik jihatdan antivirus dasturlari, tarmoq ekranlari, shifrlash va zaxira nusxalari kabi vositalar ta'lim muassasalari axborot resurslarini himoya qiladi. Huquqiy jihatdan shaxsiy ma'lumotlarni himoya qilish va me'yoriy-huquqiy hujjatlarga rioya qilish talab etiladi, pedagogik jihatdan esa foydalanuvchilarni raqamli savodxonlik va axborot xavfsizligi ko'nikmalari bilan ta'minlash zarur.

Shuningdek, xavf va risklarni boshqarish, xalqaro standartlarni joriy etish hamda favqulodda vaziyatlarga tayyorgarlik ko'rish ta'lim muassasalarida axborot xavfsizligini mustahkamlashga xizmat qiladi. Shu bilan birga, axborot xavfsizligi bo'yicha kompleks yondashuvning tatbiqi ta'lim jarayonining uzluksizligi, sifatining oshishi va o'quvchilar hamda xodimlarning ishonchini mustahkamlashga yordam beradi.

#### Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Prezidentining ta'lim tizimini rivojlantirish bo'yicha farmonlari va qarorlari. – Toshkent.
2. Inoyatov U.I. Axborot xavfsizligi va ta'lim muassasalari boshqaruvi. – Toshkent: Fan, 2021.
3. Karimov A.T. Ta'lim muassasalarida raqamli texnologiyalar va kiberxavfsizlik. – Toshkent: O'qituvchi, 2020.
4. ISO/IEC 27001:2013. Information Security Management Systems — Requirements. – Geneva: ISO, 2013.
5. Andreev A.V. Kiberbezopasnost v obrazovatelnykh uchrezhdeniyakh. – Moskva: Nauka, 2019.
6. UNESCO. ICT in Education and Cybersecurity Guidelines. – Paris, 2018.
7. OECD. Digital Education Strategies and Security Measures. – Paris, 2019.