YANGI O'ZBEKISTONNING RAQAMLI TA'LIM MUHITIDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING USTUVOR YO'NALISHLARI

Mamadaliyeva Sug'diyona Ilxomjon qizi
Farg'ona ilg'or kasbiy mahorat texnikumi Informatika va axborot texnologiyalari fani katta o'qituvchisi
e-mail: ibrohimovasugdiyona98@gmail.com

Annotatsiya: Mazkur tezisda Yangi O'zbekistonda ta'lim tizimining raqamli transformatsiyasi sharoitida axborot xavfsizligini ta'minlashning ustuvor yo'nalishlari tahlil qilinadi. Raqamli ta'lim platformalarida shaxsiy ma'lumotlarni himoya qilish, kiberxavflarning oldini olish, foydalanuvchilarni identifikatsiyalash, axborot xavfsizligi madaniyatini shakllantirish hamda ta'lim muassasalarining kiberbarqarorligini oshirish masalalariga alohida e'tibor qaratiladi. Shuningdek, Estoniya, Finlandiya, Singapur va Janubiy Koreya tajribalari o'rganilib, ilg'or xalqaro amaliyotlarni O'zbekiston ta'lim tizimiga moslashtirish bo'yicha ilmiy-amaliy takliflar ishlab chiqiladi.

Kalit so'zlar: raqamli ta'lim, axborot xavfsizligi, kiberxavfsizlik, raqamli transformatsiya, shaxsiy ma'lumotlar, ta'lim platformalari, kiberxavfsizlik madaniyati, xalqaro tajriba.

Kirish: Bugungi globallashuv va raqamli transformatsiya sharoitida axborot-kommunikatsiya texnologiyalari ta'lim tizimining ajralmas tarkibiy qismiga aylanmoqda. Elektron ta'lim platformalari, masofaviy o'qitish tizimlari, elektron kundaliklar, raqamli kutubxonalar va bulutli texnologiyalarning keng qo'llanilishi ta'lim jarayonining samaradorligini oshirish bilan birga, axborot xavfsizligi bilan bog'liq yangi muammolarni ham yuzaga keltirmoqda.

Yangi O'zbekistonda ta'lim tizimini modernizatsiya qilish, raqamli xizmatlarni kengaytirish va zamonaviy texnologiyalarni o'quv jarayoniga joriy etish muhim vazifalardan hisoblanadi. Biroq ta'lim jarayonining raqamli muhitga ko'chishi faqat texnik infratuzilmani rivojlantirish bilan cheklanmasligi lozim. Ushbu jarayonda o'quvchilar, talabalar, pedagoglar va ta'lim muassasalariga tegishli axborotlarni ishonchli himoya qilish, ma'lumotlardan qonuniy foydalanishni ta'minlash va kiberxavflarga qarshi barqaror tizim yaratish ham muhim ahamiyat kasb etadi.

Asosiy qism: Raqamli ta'lim muhitida axborot xavfsizligi buzilishi shaxsiy ma'lumotlarning oshkor bo'lishi, foydalanuvchi hisoblarining egallab olinishi, o'quv materiallarining yo'qolishi, ta'lim xizmatlarining vaqtincha to'xtashi hamda soxta axborotlarning tarqalishiga olib kelishi mumkin. Shu sababli axborot xavfsizligini ta'minlash masalasi texnik muammo bo'lish bilan birga, tashkiliy, huquqiy va pedagogik ahamiyatga ham ega. Ushbu tezis davomida raqamli ta'lim muhitida axborot xavfsizligini ta'minlashning ustuvor yo'nalishlarini aniqlash, rivojlangan davlatlar tajribasini tahlil qilish va ularni O'zbekiston ta'lim tizimiga moslashtirish bo'yicha takliflar ishlab chiqishdan iborat. Xorijiy davlatlar tajribasi shuni ko'rsatadiki, raqamli ta'lim xavfsizligi alohida dastur yoki antivirus o'rnatish bilangina ta'minlanmaydi. Buning uchun yagona standartlar, aniq javobgarlik, xavfsiz raqamli infratuzilma va foydalanuvchilarning tegishli bilimlarini birlashtiruvchi tizimli yondashuv zarur.

Estoniya tajribasi: xavfsiz raqamli infratuzilma va elektron identifikatsiya

Estoniya davlat boshqaruvi va raqamli xizmatlarni rivojlantirishda elektron identifikatsiya hamda tizimlar o'rtasida xavfsiz ma'lumot almashish mexanizmlariga katta e'tibor qaratgan. Mamlakatda X-tee

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

deb ataladigan ma'lumot almashish infratuzilmasi turli axborot tizimlari o'rtasidagi ma'lumot almashinuvini xavfsiz tashkil etishga xizmat qiladi. Ushbu tajribaning ta'lim tizimi uchun ahamiyati shundaki, ta'lim muassasalaridagi turli platformalar o'rtasida ma'lumot almashish jarayonida foydalanuvchilarni ishonchli identifikatsiyalash, kirish huquqlarini cheklash va axborot almashinuvi jarayonlarini qayd etish imkoniyatlarini rivojlantirish mumkin.

O'zbekiston uchun amaliy misol: ta'lim muassasasining elektron jurnaliga kirishda shaxsni ishonchli tasdiqlash, pedagog va o'quvchilarga ularning vazifasiga mos huquqlar berish, baholarni o'zgartirish kabi muhim amallarni elektron qayd etish tizimini takomillashtirish. unda Estoniya modelini aynan ko'chirish emas, balki uning xavfsiz ma'lumot almashish, raqamli identifikatsiya va tizimlararo hamkorlik tamoyillarini milliy sharoitga moslashtirish maqsadga muvofiq.

Finlandiya tajribasi: raqamli savodxonlik va xavfsiz ta'lim madaniyati

Finlandiya ta'lim tizimida raqamli kompetensiyalar, media savodxonlik va tanqidiy fikrlashni rivojlantirish muhim o'rin tutadi. Bunday yondashuv ta'lim oluvchilarning internetdagi axborotlarni baholashi, soxta xabarlarni farqlashi va raqamli xizmatlardan mas'uliyat bilan foydalanishiga yordam beradi. Axborot xavfsizligida inson omili muhim bo'lgani sababli, foydalanuvchilarga faqat texnik qoidalarni o'rgatish yetarli emas. Ular nima uchun shaxsiy ma'lumotlarni himoya qilish, parollarni oshkor etmaslik, shubhali havolalarni tekshirish va noma'lum fayllarni ochmaslik zarurligini ham tushunishlari kerak.

O'zbekiston uchun amaliy misol: umumta'lim maktablari, professional ta'lim muassasalari va oliy ta'lim tashkilotlarida "Raqamli xavfsizlik haftaligi"ni tashkil etish. Unda fishing xabarlarini aniqlash, kuchli parol yaratish, shaxsiy ma'lumotlarni himoya qilish va internetdagi axborotning ishonchliligini tekshirish bo'yicha amaliy mashg'ulotlar o'tkazish mumkin. Mazkur yondashuv axborot xavfsizligini faqat IT mutaxassislarining vazifasi sifatida emas, balki har bir ta'lim ishtirokchisining kundalik mas'uliyati sifatida shakllantirishga yordam beradi.

Singapur tajribasi: kiberxavfsizlikni tizimli boshqarish

Singapurda kiberxavfsizlikni rivojlantirishda davlat miqyosidagi strategiyalar, tashkilotlarning xavfsizlik mas'uliyati va aholining kiberxavfsizlik bo'yicha xabardorligini oshirishga alohida e'tibor beriladi. Singapur Kiberxavfsizlik agentligi — Cyber Security Agency of Singapore (CSA) — mamlakatning kiberxavfsizlik siyosatini rivojlantirishda muhim o'rin tutadi. Ta'lim muassasalari uchun ushbu tajribaning muhim jihati — xavflarni oldindan baholash, hodisalarni qayd etish, xavfsizlik bo'yicha mas'ullarni belgilash va kiberhodisalarga javob berish tartiblarini ishlab chiqishdir.

O'zbekiston uchun amaliy misol: har bir ta'lim muassasasida axborot xavfsizligi bo'yicha mas'ul shaxsni belgilash, kiberhodisa yuz berganda bajariladigan harakatlar algoritmini ishlab chiqish hamda muhim elektron ma'lumotlarning zaxira nusxalarini muntazam yaratish. Masalan, ta'lim platformasining hisobi buzilganida mas'ul xodim shubhali kirishni to'xtatishi, parollarni tiklash choralarini ko'rishi, tegishli jurnallarni saqlashi va zarur hollarda yuqori turuvchi tashkilotga xabar berishi lozim. Bunday tartiblar hodisaga tartibli va tezkor munosabat bildirish imkonini oshiradi.

Janubiy Koreya tajribasi: raqamli ta'lim xizmatlari va ma'lumotlarni himoya qilish

Janubiy Koreya raqamli infratuzilma va texnologiyalarga asoslangan ta'lim xizmatlarini rivojlantirish bo'yicha ilg'or davlatlardan biri hisoblanadi. Mamlakat tajribasi raqamli xizmatlarni keng joriy etish bilan birga, shaxsiy ma'lumotlarni himoya qilish va axborot tizimlarining ishonchliligini ta'minlash zarurligini ko'rsatadi. Ta'lim tizimida o'quvchilar haqidagi ma'lumotlar, o'zlashtirish

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

natijalari va boshqa raqamli yozuvlar bilan ishlashda ma'lumotlarni yig'ish, saqlash, ulardan foydalanish va uzatish jarayonlari aniq tartibga solinishi lozim.

O'zbekiston uchun amaliy misol: elektron ta'lim platformalarida faqat zarur ma'lumotlarni yig'ish, foydalanuvchilarning shaxsiy ma'lumotlarini himoyalangan shaklda saqlash, ulardan foydalanish huquqini cheklash hamda ma'lumotlar bilan ishlash tartibini pedagoglar va o'quvchilarga tushuntirish. Bundan tashqari, platformalarni ishlab chiqish va joriy etish jarayonida xavfsizlik talablarini dastlabki bosqichdanoq hisobga olish lozim. Bu keyinchalik aniqlanadigan zaifliklarni bartaraf etish xarajatlari va xavflarini kamaytirishga yordam beradi.

Xalqaro tajribalar tahlili asosida O'zbekistonning raqamli ta'lim muhitida quyidagi ustuvor yo'nalishlarni rivojlantirish taklif etiladi.

Birinchi yo'nalish — yagona tashkiliy va me'yoriy talablarni takomillashtirish. Ta'lim muassasalarida axborot xavfsizligi siyosati, ma'lumotlardan foydalanish qoidalari, mas'ul shaxslarning vazifalari va kiberhodisalar haqida xabar berish tartiblari aniq belgilanishi zarur.

Ikkinchi yo'nalish — shaxsiy ma'lumotlarni himoya qilish. O'quvchi, talaba va pedagoglarning shaxsiy ma'lumotlari faqat belgilangan maqsadlarda qayta ishlanishi, ularga kirish huquqi cheklanishi va ma'lumotlarni saqlash muddatlari asoslantirilishi lozim.

Uchinchi yo'nalish — foydalanuvchilarni ishonchli identifikatsiyalash. Muhim ta'lim platformalarida ko'p omilli autentifikatsiyadan foydalanish, rollarga asoslangan kirish nazorati va muhim amallarni qayd etish mexanizmlarini joriy etish maqsadga muvofiq.

To'rtinchi yo'nalish — axborot xavfsizligi madaniyatini shakllantirish. Pedagoglar, o'quvchilar, talabalar va ma'muriy xodimlar uchun muntazam amaliy mashg'ulotlar tashkil etilishi kerak. Bunda fishingni aniqlash, parollarni himoyalash, zararli fayllardan ehtiyot bo'lish va sun'iy intellekt xizmatlaridan xavfsiz foydalanish masalalari qamrab olinishi lozim.

Beshinchi yo'nalish — kiberhodisalarning oldini olish va ularga tayyorlik. Axborot tizimlarini yangilash, zaifliklarni muntazam tekshirish, ma'lumotlarni zaxiralash va ularni tiklash bo'yicha mashqlar o'tkazish ta'lim muassasalarining barqarorligini oshiradi.

Oltinchi yo'nalish — raqamli ta'lim platformalarini xavfsizlik talablariga muvofiq rivojlantirish. Yangi platformalarni ishlab chiqishda xavfsizlikni loyihalash bosqichidan boshlab hisobga olish, tizimlarni mustaqil tekshirish va xizmat ko'rsatuvchi tashkilotlarning xavfsizlik majburiyatlarini belgilash zarur.

Yettinchi yo'nalish — sun'iy intellekt va bulutli xizmatlardan xavfsiz foydalanish. Ta'lim muassasalarida maxfiy ma'lumotlarni ruxsatsiz tashqi xizmatlarga joylashtirishning oldini oluvchi qoidalar ishlab chiqilishi, pedagog va o'quvchilarga ushbu xizmatlardan foydalanishning xavfsiz usullari o'rgatilishi lozim.

Rivojlangan davlatlar tajribasini samarali qo'llash uchun ularni to'liq ko'chirish emas, balki milliy qonunchilik, mavjud infratuzilma, moliyaviy imkoniyatlar va ta'lim muassasalarining ehtiyojlariga moslashtirish zarur.

Buning uchun uch bosqichli modelni taklif etish mumkin.

Birinchi bosqich — diagnostika va baholash. Ta'lim muassasasida mavjud axborot tizimlari, foydalanuvchi hisoblari, ma'lumotlarni saqlash tartibi va ehtimoliy xavflar inventarizatsiya qilinadi. Eng muhim axborot resurslari aniqlanib, xavflar darajasi baholanadi.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Ikkinchi bosqich — himoya mexanizmlarini joriy etish. Kuchli autentifikatsiya, kirish huquqlarini cheklash, dasturiy ta'minotni yangilash, zaxira nusxalarini yaratish, foydalanuvchilarni o'qitish va kiberhodisalarga javob berish tartiblari yo'lga qo'yiladi.

Uchinchi bosqich — monitoring va takomillashtirish. Xavfsizlik hodisalari tahlil qilinadi, tiklash mashqlari o'tkaziladi, aniqlangan kamchiliklar bartaraf etiladi va natijalar muntazam baholanadi.

Model samaradorligini baholashda aniqlangan zaifliklarni bartaraf etish muddati, zaxira nusxalarining tiklanish muvaffaqiyati, xavfsizlik mashg'ulotlaridagi ishtirok va foydalanuvchilarning fishingni aniqlash ko'nikmalari kabi ko'rsatkichlardan foydalanish mumkin. Mazkur modelni dastlab ayrim ta'lim muassasalarida sinovdan o'tkazib, natijalar asosida takomillashtirish va keyinchalik kengroq joriy etish maqsadga muvofiq.

Xulosa

Yangi O'zbekistonning raqamli ta'lim muhitida axborot xavfsizligini ta'minlash ta'lim sifatini oshirish, shaxsiy ma'lumotlarni himoya qilish va raqamli xizmatlarga bo'lgan ishonchni mustahkamlashning muhim shartidir. Bu jarayonda texnik himoya vositalarini joriy etish bilan bir qatorda, tashkiliy boshqaruv, huquqiy talablar va pedagogik yondashuvlar uyg'unligini ta'minlash zarur. Estoniyaning xavfsiz raqamli infratuzilma, Finlandiyaning raqamli va media savodxonlik, Singapurning kiberxavfsizlikni tizimli boshqarish hamda Janubiy Koreyaning raqamli ta'lim xizmatlarini rivojlantirish tajribalari O'zbekiston uchun muhim amaliy yo'nalishlarni belgilab beradi. Shu bilan birga, xorijiy tajribani joriy etishda milliy sharoit, amaldagi qonunchilik va ta'lim muassasalarining real imkoniyatlarini hisobga olish lozim.

Tadqiqot asosida ta'lim muassasalarida axborot xavfsizligi siyosatini takomillashtirish, foydalanuvchilarni ishonchli identifikatsiyalash, shaxsiy ma'lumotlarni himoyalash, muntazam kiberxavfsizlik mashg'ulotlarini tashkil etish va kiberhodisalarga tayyorlikni oshirish ustuvor vazifalar sifatida belgilanadi. Ushbu choralarning izchil amalga oshirilishi raqamli ta'lim muhitining xavfsizligi va barqarorligini mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasi. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun, O'RQ-547, 2019-yil 2-iyul.
2. O'zbekiston Respublikasi. "Kiberxavfsizlik to'g'risida"gi Qonun, O'RQ-764, 2022-yil 15-aprel.
3. 3. Mukhtarov, F. M. (2023). THE POWER OF CYBERSECURITY EDUCATION: DEFENDING AGAINST DIGITAL THREATS. GOLDEN BRAIN, 1(26), 63–66.
4. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. 2024.
5. Mukhtarov F. Applying the science of cyber security to the educational process of higher education //Евразийский журнал технологий и инноваций. – 2023. – Т. 1. – №. 9. – С. 72-78.
6. International Organization for Standardization. ISO/IEC 27001:2022 — Information Security Management Systems.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.