OLIY TA'LIM TALABALARIDA RAQAMLI AXBOROT XAVFSIZLIGI MADANIYATINI SHAKLLANTIRISH METODIKASINI TAKOMILLASHTIRISH

Abdalova Mexriniso Baxramovna
URDPI O'qituvchisi
https://doi.org/10.5281/zenodo.22913115

Annotatsiya: Mazkur maqolada oliy ta'lim talabalarida raqamli axborot xavfsizligi madaniyatini shakllantirish metodikasini takomillashtirish masalalari yoritilgan. Raqamli texnologiyalarning ta'lim, kommunikatsiya va kundalik hayotga chuqur kirib borishi talabalar tomonidan shaxsiy ma'lumotlar, elektron hisoblar, ta'lim resurslari va boshqa raqamli axborotlardan xavfsiz foydalanish ko'nikmalarini rivojlantirishni taqozo etmoqda. Tadqiqotda raqamli axborot xavfsizligi madaniyatining motivatsion-qadriyatli, kognitiv, operatsion-amaliy, kommunikativ-axloqiy va refleksiv komponentlari aniqlashtirilgan. Talabalarda xavfsiz raqamli xulq-atvorni shakllantirishga yo'naltirilgan "Anglash – Aniqlash – Himoyalash – Nazorat qilish – Refleksiya" metodik modeli taklif etilgan. Shuningdek, phishing xabarlarini aniqlash, kuchli parol yaratish, shaxsiy ma'lumotlarni himoyalash, xavfsiz havolani aniqlash, raqamli izni boshqarish va kiberhigiyena bo'yicha amaliy metodlardan foydalanish imkoniyatlari asoslangan.

Kalit so'zlar: raqamli axborot xavfsizligi, axborot madaniyati, kiberhigiyena, raqamli savodxonlik, phishing, shaxsiy ma'lumotlar, raqamli iz, internet xavfsizligi, oliy ta'lim, talabalar.

Kirish

Raqamlashtirish jarayonlarining jadallashuvi natijasida oliy ta'lim talabalarining kundalik faoliyati elektron ta'lim platformalari, ijtimoiy tarmoqlar, messenjerlar, elektron pochta, bulutli xizmatlar va boshqa raqamli vositalar bilan bevosita bog'lanmoqda.

Bunday sharoitda talabaning raqamli texnologiyalardan foydalanish qobiliyati bilan bir qatorda ulardan xavfsiz foydalanish madaniyati ham muhim ahamiyat kasb etadi.

Raqamli muhitdagi xavfsizlik faqat texnik himoya vositalaridan foydalanish bilan cheklanmaydi. Foydalanuvchining o'z xatti-harakatlarini nazorat qilishi, shaxsiy ma'lumotlarni ehtiyotkorlik bilan taqdim etishi, shubhali havolalarni ochmasligi, hisoblarini himoyalashi va raqamli izini anglab yetishi ham xavfsizlikning muhim tarkibiy qismlaridir.

Shu nuqtayi nazardan, oliy ta'lim jarayonida raqamli axborot xavfsizligi madaniyatini shakllantirishga yo'naltirilgan pedagogik metodikani takomillashtirish dolzarb pedagogik vazifalardan biridir.

Raqamli axborot xavfsizligi madaniyati tushunchasi

Raqamli axborot xavfsizligi madaniyati — shaxsning raqamli muhitda axborotni xavfsiz qabul qilish, saqlash, uzatish va undan foydalanish, shaxsiy ma'lumotlarini himoyalash hamda xavfsizlikka tahdid tug'diruvchi vaziyatlarda ongli va mas'uliyatli harakat qilishga tayyorligini ifodalovchi bilim, ko'nikma, qadriyat va xulq-atvorlar tizimidir.

Mazkur tushuncha quyidagi elementlarni qamrab oladi:

raqamli xavflarni anglash;

shaxsiy ma'lumotlarni himoyalash;

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

akkauntlarni xavfsiz boshqarish;
parol xavfsizligi;
phishingni aniqlash;
xavfsiz internet xulq-atvori;
raqamli izni boshqarish;
axborot almashinuvi etikasi;
xavfsizlikka oid refleksiya.
Talabalarga tahdid soluvchi asosiy raqamli xavflar

Xavf turi	Mazmuni	Talabada shakllantiriladigan ko'nikma
Phishing	Soxta xabar yoki havola orqali ma'lumot olishga urinish	Shubhali xabarni aniqlash
Zaif parol	Oson taxmin qilinadigan paroldan foydalanish	Kuchli autentifikatsiya
Soxta akkaunt	Boshqa shaxs yoki tashkilot nomidan foydalanish	Profilni tekshirish
Zararli havola	Qurilma yoki ma'lumotlarga xavf tug'diruvchi havola	Havolani tekshirish
Shaxsiy ma'lumotlarni oshkor qilish	Keraksiz ma'lumotlarni internetda tarqatish	Maxfiylikni boshqarish
Raqamli iz	Internetdagi faoliyatdan qoladigan ma'lumotlar	Raqamli izni nazorat qilish
Ijtimoiy muhandislik	Ishonch yoki psixologik ta'sir orqali ma'lumot olish	Manipulyativ muloqotni aniqlash

Raqamli axborot xavfsizligi madaniyatining komponentlari
1. Motivatsion-qadriyatli komponent
Talabada raqamli xavfsizlikka mas'uliyatli munosabat shakllanadi.
U:
shaxsiy ma'lumotlarning qiymatini;
xavfsizlik qoidalariga rioya qilish zaruratini;
raqamli mas'uliyatni
anglaydi.
2. Kognitiv komponent
Talaba raqamli xavfsizlik tushunchalari va asosiy xavf turlarini biladi.
3. Operatsion-amaliy komponent
Talaba xavfsizlik choralarini amalda qo'llay oladi.
Masalan:
kuchli parol yaratish;
ikki bosqichli himoyani qo'llash;
shubhali havolani tekshirish;
maxfiylik sozlamalarini boshqarish.

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

4. Kommunikativ-axloqiy komponent

Talaba raqamli muhitda boshqa shaxslarning ma'lumotlari va huquqlariga hurmat bilan munosabatda bo'ladi.

5. Refleksiv komponent

Talaba o'zining raqamli xatti-harakatlarini muntazam tahlil qiladi.

Metodik model

Talabalarda raqamli axborot xavfsizligi madaniyatini shakllantirish uchun quyidagi model taklif etiladi:

ANGLASH
↓
Raqamli xavfni tushunish
↓
ANIQLASH
↓
Xavfli vaziyat va tahdid belgilarini aniqlash
↓
HIMOYALASH
↓
Tegishli xavfsizlik choralarini qo'llash
↓
NAZORAT QILISH
↓
O'z raqamli faoliyatini monitoring qilish
↓
REFLEKSIYA
↓
Xatolarni tahlil qilish va xavfsiz xulq-atvorni takomillashtirish
↓
NATIJA

Raqamli axborot xavfsizligi madaniyatiga ega talaba

Metodikani amalga oshirish bosqichlari

Birinchi bosqich — xavfni anglash

Talabalarga real hayotga yaqin vaziyatlar taqdim etiladi.

Masalan:

"Sizga universitet nomidan elektron xat keldi. Unda akkauntingiz bloklanishi va uni faollashtirish uchun havolaga kirishingiz kerakligi yozilgan."

Talabadan:

"Siz qanday harakat qilasiz?"

degan savol so'raladi.

Bu orqali talabaning dastlabki xavfsizlik xulq-atvori aniqlanadi.

Ikkinchi bosqich — xavfni aniqlash

Talabalar phishing xabarlarining belgilarini aniqlaydilar:

shoshilinch harakat qilishga undash;

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

shubhali manzil;
noma'lum yuboruvchi;
g'ayritabiiy havola;
ortiqcha shaxsiy ma'lumot so'rash;
tahdid yoki bosim ohangi.
Uchinchi bosqich — himoyalanish
Talabalarga xavfsizlik choralarini amaliy bajarish topshiriladi.
Masalan:
"Xavfsiz akkaunt" laboratoriyasi
Talaba:
Kuchli parol tamoyillarini aniqlaydi.
Ikki bosqichli autentifikatsiya tushunchasini o'rganadi.
Maxfiylik sozlamalarini tahlil qiladi.
Keraksiz ochiq ma'lumotlarni aniqlaydi.
To'rtinchi bosqich — raqamli izni nazorat qilish
Talabalar internetdagi o'zlari haqida mavjud bo'lishi mumkin bo'lgan ma'lumotlarni tahlil qiladilar.
Ularga quyidagi savollar beriladi:
Internetda men haqimda qanday ma'lumotlar mavjud?
Qaysi ma'lumotlar ommaga ochiq?
Qaysi ma'lumotlarni ulashish zarur emas?
Raqamli faoliyatim kelajakda qanday ko'rinishi mumkin?
Beshinchi bosqich — refleksiya
Mashg'ulot yakunida talabalar:
"Men bugun qanday xavfni aniqlashni o'rgandim?"
"Qaysi raqamli odatimni o'zgartirishim kerak?"
"Kelgusida qanday xavfsizlik qoidalariga amal qilaman?"
savollariga javob beradilar.
Samarali pedagogik metodlar
"Phishing detektivi"
Talabalarga bir nechta elektron xabar namunalari beriladi.
Ular xabarlarni:
xavfsiz;
shubhali;
xavfli
kategoriyalariga ajratadilar.
Har bir qaror dalil bilan asoslanadi.
"Xavfsiz havola"
Talabaga turli havolalar taqdim etiladi.
U havolaning:
domenini;
yozilish shaklini;
kontekstini;
yuboruvchisini

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

tahlil qiladi.
"Raqamli izim"
Talaba o'zining raqamli xulq-atvorini tahlil qiladi.
Bu metod shaxsiy ma'lumotlarni ehtiyotkorlik bilan ulashish va raqamli reputatsiyani boshqarishga xizmat qiladi.
"Xavfsizlik eksperti"
Guruhdagi bir talaba "ekspert" rolini bajaradi.
Boshqa talabalar unga turli vaziyatlarni taqdim etadi:
"Telefoningizga noma'lum havola keldi."
"Ijtimoiy tarmoqdagi tanishingiz pul so'radi."
"Elektron pochta orqali parolingizni yuborish so'raldi."
"Ekspert" vaziyat bo'yicha xavfsiz harakat algoritmini ishlab chiqadi.
"5 qadamli raqamli xavfsizlik" algoritmi
Talabalarga quyidagi universal algoritmni o'rgatish mumkin:
1. TO'XTANG
Shubhali xabar yoki havola kelganda darhol harakat qilmang.
2. TEKSHIRING
Yuboruvchi va manbani tekshiring.
3. TAQQOSLANG
Ma'lumotni mustaqil manba bilan solishtiring.
4. HIMOYALANG
Shaxsiy ma'lumot, parol yoki maxfiy kodlarni bermang.
5. XULOSA QILING
Xavfsiz yoki xavfli ekanini aniqlang.
Ushbu algoritm:
TO'XTANG → TEKSHIRING → TAQQOSLANG → HIMOYALANG → XULOSA QILING
ko'rinishida yodda saqlash uchun qulay metodik vosita bo'lib xizmat qiladi.
Tajriba-sinov ishlarini tashkil etish
Metodikani amaliyotda sinovdan o'tkazish uch bosqichda tashkil etilishi mumkin.
Aniqlovchi bosqich
Talabalarning dastlabki raqamli xavfsizlik madaniyati aniqlanadi.
Baholash mezonlari:
xavfni aniqlash;
phishingni tanish;
shaxsiy ma'lumotlarni himoyalash;
xavfsiz parol tamoyillarini bilish;
raqamli izni anglash;
xavfsiz xulq-atvor.
Shakllantiruvchi bosqich
Talabalar bilan amaliy mashg'ulotlar tashkil etiladi:
phishing detektivi;
xavfsiz havola;
raqamli izim;

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

xavfsizlik eksperti;
case-study;
raqamli vaziyatlarni modellashtirish;
refleksiv kundalik.
Nazorat bosqichi
Talabalarning raqamli xavfsizlik bo'yicha bilim, ko'nikma va xulq-atvori qayta baholanadi.
Baholash darajalari
Past daraja
Talaba raqamli xavflarning ayrimlarini biladi, ammo amaliy vaziyatlarda xavfni mustaqil aniqlashda qiynaladi.
O'rta daraja
Talaba asosiy xavflarni aniqlay oladi va xavfsizlik choralarini qo'llaydi, ammo murakkab vaziyatlarda qo'shimcha ko'rsatmaga ehtiyoj sezadi.
Yuqori daraja
Talaba raqamli xavflarni mustaqil aniqlaydi, manbani tekshiradi, xavfsizlik choralarini to'g'ri tanlaydi, shaxsiy ma'lumotlarini himoya qiladi va o'zining raqamli xulq-atvorini refleksiv tahlil qila oladi.
Ilmiy yangilik
Tadqiqotning ilmiy yangiligi quyidagilarda namoyon bo'ladi:
Oliy ta'lim talabalarida raqamli axborot xavfsizligi madaniyatining motivatsion-qadriyatli, kognitiv, operatsion-amaliy, kommunikativ-axloqiy va refleksiv komponentlari tizimlashtiriladi.
"Anglash – Aniqlash – Himoyalash – Nazorat qilish – Refleksiya" metodik modeli ishlab chiqiladi.
Raqamli xavfsizlikni o'rgatishda real vaziyatlarni modellashtirish, case-study va amaliy laboratoriya topshiriqlarini integratsiyalash metodikasi taklif etiladi.
Talabalarning raqamli xavfsizlik madaniyatini baholash uchun xavfni aniqlash, xavfsiz qaror qabul qilish, amaliy himoyalanish va refleksiya mezonlari aniqlashtiriladi.
Talabalarning xavfsiz raqamli xulq-atvorini shakllantirish uchun "TO'XTANG – TEKSHIRING – TAQQOSLANG – HIMOYALANG – XULOSA QILING" algoritmi taklif etiladi.
Amaliy ahamiyati
Mazkur metodikadan oliy ta'lim muassasalarida:
raqamli pedagogika;
informatika;
axborot madaniyati;
tarbiyaviy ishlar;
media savodxonlik;
mustaqil ta'lim;
talabalar bilan profilaktik mashg'ulotlar
jarayonida foydalanish mumkin.
Metodika asosida "Raqamli xavfsizlik laboratoriyasi" nomli elektron ta'lim modulini ishlab chiqish ham mumkin.
Modul tarkibi:
Raqamli xavflar.
Phishing.

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

Akkaunt xavfsizligi.
Shaxsiy ma'lumotlarni himoyalash.
Xavfsiz havolalar.
Raqamli iz.
Ijtimoiy muhandislik.
Kiberhigiyena.
Amaliy vaziyatlar.
Yakuniy diagnostik test.
Xulosa

Oliy ta'lim talabalarida raqamli axborot xavfsizligi madaniyatini shakllantirish zamonaviy raqamli ta'lim muhitining muhim pedagogik vazifalaridan biridir. Talabaning raqamli texnologiyalardan foydalanish qobiliyati xavfsizlik ko'nikmalari bilan uyg'unlashgandagina uning raqamli kompetentligini to'laqonli rivojlantirish mumkin.

Taklif etilgan "Anglash – Aniqlash – Himoyalash – Nazorat qilish – Refleksiya" modeli talabaning xavfni nazariy jihatdan bilishidan boshlab, uni amaliy vaziyatda aniqlash, xavfsizlik choralarini qo'llash va o'z faoliyatini baholashgacha bo'lgan izchil pedagogik jarayonni ta'minlaydi.

Ayniqsa, phishing, soxta havolalar, shaxsiy ma'lumotlarni oshkor qilish, raqamli iz va ijtimoiy muhandislik bilan bog'liq vaziyatlarni amaliy mashg'ulotlarga kiritish talabalarning real raqamli muhitdagi xavfsiz xulq-atvorini rivojlantirish imkonini beradi.

Shunday qilib, oliy ta'limda raqamli axborot xavfsizligi madaniyatini bilim → aniqlash → amaliy himoyalanish → nazorat → refleksiya tamoyili asosida shakllantirish talabaning raqamli muhitdagi mas'uliyatli va xavfsiz faoliyatini ta'minlashga xizmat qiladi.

Foydalanilgan adabiyotlar:

1. UNESCO. Media and Information Literacy: Curriculum for Teachers. Paris: UNESCO.
2. UNESCO. Global Framework of Reference on Digital Literacy Skills. UNESCO Institute for Statistics.
3. Council of Europe. Digital Citizenship Education Handbook. Strasbourg.
4. European Commission. The Digital Competence Framework for Citizens: DigComp 2.2. Publications Office of the European Union, 2022.
5. OECD. Digital Security and Privacy in the Digital Economy. OECD Publishing.
6. NIST. Cybersecurity Framework. National Institute of Standards and Technology.
7. Livingstone S. Children and the Internet: Great Expectations, Challenging Realities. Polity Press.
8. Buckingham D. The Media Education Manifesto. Polity Press.
9. Hobbs R. Digital and Media Literacy: A Plan of Action. Aspen Institute.
10. UNESCO. Guidance for Generative AI in Education and Research. Paris: UNESCO.
11. Agar shu ketma-ketlikda davom ettirsak, 4-maqola uchun yanada boshqa yo'nalish sifatida: "Oliy ta'lim talabalarida tanqidiy fikrlash asosida soxta axborotni rad etish va qarshi dalil keltirish ko'nikmalarini rivojlantirish metodikasi" mavzusi mos keladi.

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