pasaytirish va mustaqil ravishda o'rganish imkonini beradi. Interaktiv yondashuvning asosiy xususiyatlari quyidagilardir:

1. O'quvchi va o'qituvchi orasidagi bog'lanish: Interaktiv yondashuv ta'lim jarayonida o'quvchilar bilan o'qituvchilar arasida samarali aloqa tuziladi. Oliy darajali sohada ishlaydigan mutaxassislar, talabalarning talabalik barcha bosqichlarini kuzatib boradigan shaxslar bo'ladi.

2. Mustaqil ishlash imkoniyati: Interaktiv yondashuv jarayonida har bir talaba mustaqil ravishda darslarga kirishi mumkin. Oliy darajali mutaxassislar tomonidan tayyorlangan dars materiallari, videolar, testlar va boshqa interaktiv vositalar orqali talabalarning o'ziga xos yo'l-yo'lakni rivojlantirishi kuzatib boriladi.

3. Yangi texnologiyalardan foydalanish: Interaktiv yondashuvning bir xususiyati yangi texnologiyalardan foydalanishdir. Internet, kompyuterlar, smartfonlar, interaktiv darsliklar va boshqa texnologik vositalar yordamida o'quvchilar bilimlarni o'rganishadi.

4. Real va virtual kommunikatsiya imkoniyati: Interaktiv yondashuv jarayonida talabalar haqida ma'lumot oluvchi interaktiv platformalar, chat tizimlari va video-konferensiyalar orqali o'qituvchilar bilimni baholaydi va talabalarga maslahat beradi. Bu usulda o'quvchi va o'qituvchi o'rtasidagi kommunikatsiya "real" (haqiqiy) dunyodagi ko'rinishda ham amalga oshirilishi mumkin.

5. O'zlashtirish: Interaktiv yondashuv jarayonida talabalar amaliyotga to'sqinlik sifatida texnik vazifalarni bajaradilar. Bunday vazifalar orqali talabalarning teorik bilimlarini amaliyotga aylantirish maqsadga muvofiq ravishda amalga oshiriladi.

Interaktiv yondashuvning afzalliklari quyidagilardir:

- Talabalarga mustaqil ishlash va o'rganish imkonini beradi.
- Oliy darajali mutaxassislar bilan bog'lanish muhim xususiyatlardan biridir.
- Texnologiyalardan samarali foydalaniladi.
- Real va virtual kommunikatsiya imkoniyati mavjud.
- O'quvchilar amaliyotga to'sqinlik sifatida texnik vazifalarni bajarish imkoniyatiga ega bo'ladi.

Interaktiv yondashuv asosida boshlang'ich ta’limda aloqadorlikni takomillashtirish uchun bir necha yordamchi usullar mavjud.

1. Video darslar: O'qituvchi o'z darsini video formatida olib berishi mumkin. Bu, o'quvchilar uchun boshqa vazifalar bilan birga, matnlar va tushunchalarni qo'llab-quvvatlashda qulaylik yaratadi.

2. Veb-saytlar va ilovalar: O'qituvchi o'quvchilar uchun ma'lumotlar, amaliy mashg'ulotlar va sinovlar taqdim etish uchun interaktiv veb-saytlardan va ilovalardan foydalanishi mumkin. Bu usul o'quvchilarni boshqarishni osonlashtiradi va ularning o'ziga xos davr ko'rinishida ta’lim olmasini ta'minlaydi.

3. Online vazifalar: O’qituvchi interaktiv yondashuvni takomillashtirish uchun online vazifalarni berishi mumkin. Bu vazifalar o’quvchilar bilan aloqada bo’lgan

masalalar ustiga ishlashga imkon beradi va ularning mustaqil ravishda fikrlash va muhokama qilish qobiliyatini rivojlantiradi.

4. Veb-konferensiyalar: O’qituvchi interaktiv yondashuvni takomillashtirish uchun online veb-konferensiyalar tashkil etishi mumkin. Bu konferensiyalarda o’quvchilar o’qituvchiga savollar berish, masalalar haqida gapirish va boshqa talabalar bilan fikrlash imkoniyatiga ega bo’ladi.

5. Forumlar va chatlar: O’qituvchi o'quvchilar uchun veb-forumlar yoki chat platformalarini tashkil etishi mumkin. Bu yerlarda o’quvchilar mavzular haqida gaplashishi, fikrlashishi va maslahat so'rashishi mumkin.

Interaktiv yondashuvning muhim afzalliklari aloqadorlikni takomillashtirishga imkon beradi. O'quvchilarning ko'nikmalari, tushunchalari va umumiy tushunarliqliklari kuchayib boradi. Shuningdek, interaktiv yondashuv o'quvchilarni mustaqil ravishda fikrlash, muhokama qilish va ijodiy yondashuv qobiliyatini rivojlantiradi.

FOYDALANILGAN ADABIYOTLAR:

1. Aliyarovich, T. E. ., & Sayfiddinovich, X. R. . (2021). Forms and Methods of Innovative Approach through the use of Ethnopedagogy in the Development of Heury Capacity in Primary Schools. Journal of Ethics and Diversity in International Communication, 1(7), 16–22.

2. Jurayev, J. S. O. (2021). Abu Ali ibn Sinoning falsafiy qarashlarida axloq masalasi va uning bugungi kundagi ahamiyati. Oriental renaissance: Innovative, educational, natural and social sciences, 1(3), 11-14.

3. Abdinazarovna, S. G. (2020). THE REFLECTION FEATURES OF ABBREVIATIONS AND ACRONYMS OF THE ENGLISH, RUSSIAN AND UZBEK LANGUAGES. Тил, таълим, таржима” халқаро журнали, 2(1).

4. Mavlonova R., Rahmonqulova R. Boshlang’ich ta‘limning interaktivlashgan pedagogikasi. T., Ilm ziyo, - 2009. 49-bet.

5. Javohir Gaybullo og, Z., & Sayfiddinovich, X. R. (2021). Boshlang‘Ich Sinf O‘Qish Darslari Samaradorligini Oshirishda Qo‘Llaniladigan Interfaol Metodlar. Барқарорлик ва Етакчи Тадқиқотлар онлайн илмий журнали, 1(6), 93-104.

AXBOROTLARNI HIMOYALASHDA AES KRIPTOGRAFIK ALGORITMINING IMKONIYATLARI

Seytniyazov Davronbek Bayramovich *tayanch doktorant*
Atamuratova Shaxsanem Turdimuratovna *talaba*
Dauletmuratova Juldiz Ayapbergenovna *talaba*
Jumaniyazova Ulbosin Polatbay qizi *talaba*

Bugungi kunda axborotlashgan jamiyat jadal suratlar bilan shakllanib, axborotlar dunyosida davlat chegaralari degan tushuncha yo'qolib bormoqda. Global kompyuter tarmog'i jahon davlatlarining ijtimoiy-iqtisodiy, siyosiy, ma'naviy va madaniy hayotida alohida ahamiyat kasb etmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi bo'lib hisoblanadi. O'zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimini yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o'z ifodasini topdi. Bu borada O'zbekiston Respublikasining «Davlat sirlarini saqlash to'g'risida»gi, «Axborotlashtirish to'g'risida»gi va boshqa qonunlar qabul qilindi hamda amalda tatbiq etib kelinmoqda.

Axborot xavfsizligi - bu axborotning saqlanishi va himoya qilinishini ta'minlashga, shuningdek unga ruxsatsiz kirishning oldini olishga va uning egasiga zarar yetkazishga qaratilgan chora-tadbirlar majmuidir. Zamonaviy dunyoda ushbu mavzuning dolzarbligi shubhasizdir, chunki axborot texnologiyalari va kommunikatsiyalari odamlarning kundalik hayotida, shuningdek, korxonalar, tashkilotlar va davlatlar faoliyatida tobora muhim rol o'ynamoqda.

Hozirda axborotlarni himoyalashda eng keng qo'llaniladigan usullarning biri bu shifrlash bo'lib uni amalga oshirishda birnechta algoritmlardan foydalanilmoqda. Shu kabi algoritmlardan biri AES shifrlash algoritmi bo'lib hisoblanadi.

Kengaytirilgan shifrlash standarti (AES) algoritmi dunyodagi eng keng tarqalgan simmetrik ma'lumotlarni shifrlash algoritmlaridan biri bo'lib hisoblanadi. Bu algoritm 2001 yilda AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan va avvalgi shifrlash standarti DES algoritmini o'rniga foydalanish uchun taqdim etilgan.

AES axborotlarni uzatish yoki saqlashdan oldin ularni shifrlash orqali ma'lumotlarning maxfiyligi va yaxlitligini himoya qilish uchun ishlatiladi. U turli sohalarda, jumladan, axborot xavfsizligi, moliya, tibbiyot, hukumat va hatto shifrlangan flesh-disklar va Wi-Fi routerlar kabi iste'molchi ilovalarida keng qo'llaniladi.

AES bitni almashtirish va aralashtirish printsipi asosida ishlaydi. U 128-bitli ma'lumotlar bloklarini shifrlash uchun 128, 192 yoki 256-bitli kalitdan foydalanadi. AES bir nechta qadamlardan iborat bo'lib, ularning har birida quyidagi operatsiyalar amalga oshiriladi: