Shu nuqtayi nazardan, ekopedagogik kompetensiyalarni rivojlantirish metodikasining samaradorligi metodlarning alohida qo‘llanilishidan ko‘ra, ularning o‘zaro integratsiyasiga bog‘liq. Nazariy bilimlar interaktiv metodlar orqali faollashtirilishi, amaliy topshiriqlar orqali mustahkamlanishi, loyiha va tadqiqot faoliyati orqali rivojlantirilishi hamda refleksiya orqali baholanishi maqsadga muvofiqdir.

Xulosa va takliflar. Bo‘lajak boshlang‘ich ta’lim o‘qituvchilarida ekopedagogik kompetensiyalarni rivojlantirish metodikasi mazmunini takomillashtirishda kompetensiyaviy, faoliyatga yo‘naltirilgan, interaktiv va integrativ yondashuvlardan foydalanish muhim metodik asos bo‘lib xizmat qiladi.

Tadqiqot materiallarini tizimlashtirish asosida ekopedagogik ta’lim metodlari uch guruhga: nazariy-ekologik bilimlarni shakllantiruvchi, amaliy-ekopedagogik faoliyatni rivojlantiruvchi hamda ijodiy, kommunikativ va refleksiv faoliyatni rivojlantiruvchi metodlarga ajratildi.

Muammoli ta’lim, keys-stadi, loyiha, aqliy hujum, klaster, munozara, SWOT tahlil, STEAM, kichik guruhlarda ishlash va boshqa interaktiv metodlarning integratsiyalashgan holda qo‘llanilishi talabalarning ekologik bilimlarini amaliy faoliyat bilan bog‘lashga imkon beradi.

Raqamli pedagogik vositalar – multimedia, elektron ta’lim resurslari, virtual ekologik laboratoriyalar, interaktiv testlar va raqamli platformalar ekopedagogik ta’limning zamonaviy axborot muhitini shakllantirishga xizmat qiladi.

Umuman, takomillashtirilgan metodik modelda bilim → amaliy faoliyat → ijodiy izlanish → hamkorlik → refleksiya uzviyligining ta’minlanishi bo‘lajak boshlang‘ich ta’lim o‘qituvchilarida ekologik bilim, qadriyat, amaliy ko‘nikma, ekologik madaniyat va kasbiy mas’uliyatni kompleks rivojlantirish imkonini beradi.

Tadqiqot natijalariga asoslanib, quyidagi takliflarni ilgari surish mumkin:

– boshlang‘ich ta’lim yo‘nalishidagi fanlar mazmuniga ekologik va ekopedagogik mazmundagi amaliy topshiriqlarni tizimli kiritish;

–ekologik keyslar, loyihalar va muammoli vaziyatlar bankini yaratish;

–STEAM va raqamli texnologiyalar asosida ekologik mazmundagi integrativ topshiriqlarni ishlab chiqish;

–talabalarning ekologik faoliyatini elektron portfolio va refleksiv topshiriqlar asosida baholash;

– oliy pedagogik ta’lim muassasalarida ekoklub, ekologik loyiha va volontyorlik faoliyatlarini rivojlantirish;

–bo‘lajak boshlang‘ich ta’lim o‘qituvchilarining ekopedagogik kompetensiyalarini rivojlantirishga qaratilgan metodik qo‘llanmalar va elektron ta’lim resurslarini yaratish.

Foydalanilgan adabiyotlar ro‘yxati:

(1). O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning Taraqqiyot strategiyasi to‘g‘risida”gi PF-60-farmoni.

(2). O‘zbekiston Respublikasi Prezidentining “2030-yilgacha bo‘lgan davrda O‘zbekiston Respublikasining atrof-muhitni muhofaza qilish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-5863-farmoni. Toshkent, 2019.

(3). O‘zbekiston Respublikasi Vazirlar Mahkamasining “Uzluksiz ma’naviy tarbiya konsepsiyasini tasdiqlash va uni amalga oshirish chora-tadbirlari to‘g‘risida”gi 1059-qarori. 2019-yil 31-dekabr.

(4). O‘zbekiston Respublikasining “Ta’lim to‘g‘risida”gi qonuni. O‘RQ-637. Toshkent, 2020.

(5). O‘zbekiston Respublikasi Prezidentining “Ekologiya va atrof-muhitni muhofaza qilish sohasida davlat boshqaruvi tizimini takomillashtirish to‘g‘risida”gi PF-5024-farmoni. Toshkent, 2017.

(6). O‘zbekiston Respublikasi Prezidentining “O‘zbekiston–2030” strategiyasini “Atrof-muhitni asrash va yashil iqtisodiyot” yilida amalga oshirishga oid davlat dasturi to‘g‘risida”gi PF-16-farmoni. Toshkent, 2025.

(7). Nishonboyeva M.G. Biologiya darslarida ekologik tarbiya. Toshkent, “O‘qituvchi”, 1992, 104-bet.

(8). Ayubova I.X. Texnika oliy ta’lim muassasalari talabalarida ekologik xavfsizlik madaniyatini shakllantirish tizimlari. Pedagogika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi, Toshkent, 2019, 149-bet.

Tillayev Azamat Ibragimovich (O‘zbekiston Milliy universiteti dotsenti, PhD; tillayev1@mail.ru)

KRIPTOGRAFIYA FANINING “KRIPTOGRAFIYANING MATEMATIK ASOSLARI” BO‘LIMI UCHUN MULTIMEDIALI DASTURIY TA’MINOT ISHLAB CHIQISH VA UNDAN FOYDALANISHNI TASHKIL ETISH

Annotatsiya. *Maqolada kriptografiya fanining “Kriptografiyaning matematik asoslari” bo‘limi uchun multimediali dasturiy ta’minotni ishlab chiqish va undan o‘quv jarayonida foydalanishni tashkil etish masalalari yoritilgan. Dasturiy ta’minot ADDIE modeli asosida loyihalangan bo‘lib, nazariy, animat-*

sion, virtual laboratoriya, nazorat va yordamchi modullardan iborat. Multimedia dizaynining kognitiv tamoyillari, modul arifmetikasi, Evklid algoritmi va modul bo'yicha darajaga ko'tarish mavzularini visuallashtirish yondashuvlari, dasturdan auditoriya, laboratoriya, mustaqil va masofaviy ta'limda foydalanish shakllari hamda samaradorlikni baholash tajribasining dizayni asoslab berilgan.

Kalit so'zlar: *kriptografiya, sonlar nazariyasi, modul arifmetikasi, Evklid algoritmi, Eyler funksiyasi, multimediali dasturiy ta'minot, animatsiya, virtual laboratoriya, ADDIE.*

Тиллаев Азамат Ибрагимович (доцент Национального университета Узбекистана, PhD; tillayev1@mail.ru)

РАЗРАБОТКА МУЛЬТИМЕДИЙНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАЗДЕЛА «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ» ДИСЦИПЛИНЫ «КРИПТОГРАФИЯ» И ОРГАНИЗАЦИЯ ЕГО ИСПОЛЬЗОВАНИЯ

Аннотация. *В статье рассмотрены вопросы разработки мультимедийного программного обеспечения для раздела «Математические основы криптографии» дисциплины «Криптография» и организации его использования в учебном процессе. Программное обеспечение спроектировано на основе модели ADDIE и включает теоретический, анимационный, лабораторный, контрольный и справочный модули. Обоснованы принципы мультимедийного дизайна, подходы к визуализации модулярной арифметики, алгоритма Евклида и возведения в степень по модулю, формы использования программы и дизайн педагогического эксперимента.*

Ключевые слова: *криптография, теория чисел, модулярная арифметика, алгоритм Евклида, мультимедийное программное обеспечение, виртуальная лаборатория, ADDIE.*

Tillayev Azamat Ibragimovich (Associate Professor of the National University of Uzbekistan, PhD; tillayev1@mail.ru)

DEVELOPMENT OF MULTIMEDIA SOFTWARE FOR THE "MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY" SECTION OF THE "CRYPTOGRAPHY" COURSE AND ORGANIZATION OF ITS USE IN THE EDUCATIONAL PROCESS

Annotation. *The article addresses the development of multimedia software for the "Mathematical Foundations of Cryptography" section of the Cryptography course and the organization of its use in teaching. The software is designed according to the ADDIE model and consists of theory, animation, virtual laboratory, assessment and reference modules. Multimedia design principles, approaches to visualizing modular arithmetic, the Euclidean algorithm and modular exponentiation, forms of classroom and distance use, and the design of a pedagogical experiment are substantiated.*

Keywords: *cryptography, number theory, modular arithmetic, Euclidean algorithm, multimedia software, virtual laboratory, ADDIE.*

Kirish. O'zbekiston Respublikasi Prezidentining 2019-yil 8-oktabrdagi PF-5847-farmoni bilan tasdiqlangan Oliy ta'lim tizimini 2030-yilgacha rivojlantirish konsepsiyasi hamda 2020-yil 5-oktabrdagi PF-6079-farmoni bilan tasdiqlangan "Raqamli O'zbekiston–2030" strategiyasi o'quv jarayoniga raqamli ta'lim resurslarini joriy etishni ustuvor vazifa sifatida belgilaydi [1,2]. Zamonaviy kriptografik tizimlarning kriptobardoshliligi to'liq matematik asoslarga tayanadi. RSA algoritmi butun sonlarni tub ko'paytuvchilarga ajratish murakkabligiga, Diffi–Xellman kalit almashish protokoli diskret logarifmlash masalasining murakkabligiga asoslangan [5]. O'zbekiston Respublikasining O'z DSt 1092:2009 (elektron raqamli imzo) va O'zDSt 1105:2009 (ma'lumotlarni shifrlash algoritmi) davlat standartlari ham modul arifmetikasi va chekli maydonlar nazariyasini qo'llaydi. Shu sababli "Kriptografiyaning matematik asoslari" bo'limi kriptografiya kursining tayanch qismi hisoblanadi.

Amaliyotda ushbu bo'limni o'qitish bir qator qiyinchiliklarga duch keladi. Birinchidan, sonlar nazariyasi tushunchalari (taqqoslamalar, qoldiqlar halqasi, multiplikativ guruh, chekli maydon) abstrakt xarakterga ega va talabalar ularni kriptografik algoritmlar bilan bog'lashda qiynaladi. Ikkinchidan, kriptografiyada ishlatiladigan sonlar yuzlab xonali bo'lib, ular bilan qo'lda hisoblash imkonsiz, kichik sonlardagi misollar esa algoritmlarning samaradorligi haqida to'g'ri tasavvur bermaydi. Uchinchidan, Evklidning kengaytirilgan algoritmi yoki Xitoy qoldiqlar teoremasi kabi ko'p bosqichli protseduralarni doskada tushuntirishda talabalar oraliq natijalar orasidagi bog'lanishni yo'qotadi. Multimediali dasturiy ta'minot matn, grafika, animatsiya, video va interaktiv hisoblash vositalarini yagona muhitda birlashtirib, bu qiyinchiliklarni bartaraf etish imkonini beradi [9].

Adabiyotlar tahlili va metodologiya. Kriptografiyaning matematik asoslari N.Koblitsning sonlar nazariyasi va kriptografiyaga bag‘ishlangan kursida, A.Menezes va hammualliflarning amaliy kriptografiya bo‘yicha qo‘llanmasida, shuningdek V.Stallings hamda K.Paar va Y.Pelsl darsliklarida tizimli bayon etilgan. Ushbu manbalarda modul arifmetikasi, Evklid algoritmi, Eyler funksiyasi, Ferma va Eyler teoremalari, Xitoy qoldiqlar teoremasi, tublik testlari va chekli maydonlar kriptografik algoritmlarning zaruriy nazariy asosi sifatida qaraladi. Tublikni ehtimoliy tekshirish algoritmlari G.Miller va M.Rabin ishlarida asoslangan [5,6].

Multimediali o‘quv resurslarini loyihalashning nazariy asosini R.Mayerning multimediali o‘rganishning kognitiv nazariyasi tashkil etadi. Unga ko‘ra, inson axborotni ko‘rish va eshitish kanallari orqali alohida qayta ishlaydi, har bir kanalning sig‘imi esa cheklangan. J.Svellerning kognitiv yuklama nazariyasi o‘quv materialining ortiqcha elementlari ishchi xotirani band qilib, o‘rganishni qiyinlashtirishini ko‘rsatadi [3,4].

Elektron o‘quv resurslarini ishlab chiqishda ADDIE modeli (tahlil, loyihalash, ishlab chiqish, joriy etish, baholash) keng qo‘llaniladi. Dasturiy ta’minot sifatini baholash uchun ISO/IEC 25010 xalqaro standartidagi sifat modeli, elektron o‘quv kurslarini LMS platformalariga integratsiya qilish uchun esa SCORM spetsifikatsiyasi asos bo‘lib xizmat qiladi. Kriptografiyani o‘qitishda CrypTool va SageMath kabi vositalar qo‘llaniladi, biroq ular o‘zbek tilidagi o‘quv mazmuni bilan integratsiyalashmagan va o‘quv mashg‘ulotining metodik tuzilmasini hisobga olmaydi. Mazkur holat o‘zbek tilida, bo‘lim dasturiga to‘liq mos, multimedia dizayni tamoyillariga asoslangan dasturiy ta’minot ishlab chiqish zaruratini ko‘rsatadi [10,11].

Dasturiy ta’minot ADDIE modeli asosida ishlab chiqildi. Tahlil bosqichida fan dasturi, talabalarning dastlabki tayyorgarligi va tipik xatolari o‘rganildi. Loyihalash bosqichida bo‘lim mazmuni o‘quv modullariga ajratildi va har bir mavzu uchun multimedia elementlari tanlandi. Ishlab chiqish bosqichida dasturiy ta’minot HTML5 va JavaScript texnologiyalari asosida yaratildi. Joriy etish va baholash bosqichlarida dastur o‘quv jarayonida sinovdan o‘tkazildi [7].

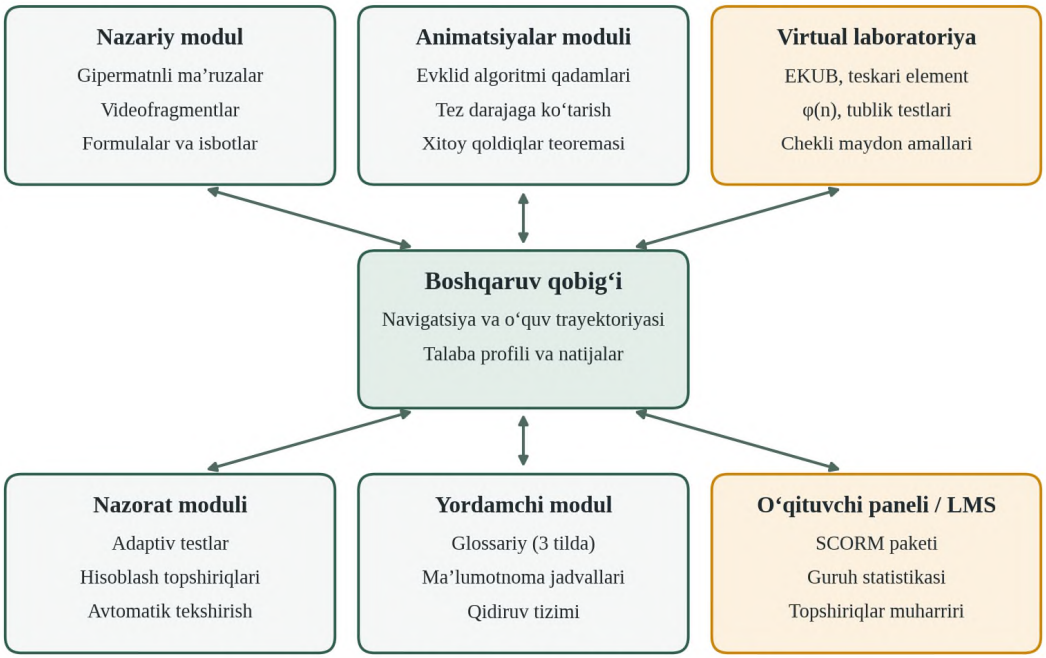
Natijalar va muhokama. Bo‘lim mazmuni va multimedia elementlarini tanlash. Bo‘lim mazmuni yetti mavzuga ajratildi. Har bir mavzu uchun uning tabiatiga mos multimedia elementi tanlandi: bosqichli protseduralar animatsiya, sonli qonuniyatlar interaktiv kalkulator va jadvallar, ehtimoliy jarayonlar esa simulatsiya orqali ifodalandi (1-jadval).

1-jadval

Bo‘lim mavzulari va ularga mos multimedia elementlari

Mavzu	Asosiy tushunchalar	Multimedia elementi
Modul arifmetikasi	Taqqoslamalar, qoldiqlar halqasi $\mathbb{Z}_n$	“Soat siferblati” animatsiyasi, modul kalkulatori
EKUB va Evklid algoritmi	Bo‘linish, Bezu munosabati, teskari element	Qadamli animatsiya, jadval generatori
Eyler funksiyasi, Ferma va Eyler teoremalari	$\varphi(n)$, multiplikativ guruh $\mathbb{Z}_n^*$	Guruh jadvali vizualizatsiyasi, tajriba kalkulatori
Xitoy qoldiqlar teoremasi	Taqqoslamalar tizimi	Bosqichli yechuvchi, animatsiya
Modul bo‘yicha darajaga ko‘tarish	Kvadratga oshirish va ko‘paytirish usuli	Bitlar bo‘yicha qadamli animatsiya, grafik
Tublik testlari	Ferma testi, Miller–Rabin testi	Ehtimoliy simulyatsiya, statistika grafigi
Chekli maydonlar	GF(p), GF(2^n), ko‘phadlar arifmetikasi	Qo‘shish va ko‘paytirish jadvallari

2. **Dasturiy ta’minotning tuzilmasi.** Dasturiy ta’minot boshqaruv qobig‘i va unga ulangan oltita moduldan iborat (1-rasm). Boshqaruv qobig‘i navigatsiyani, talabaning o‘quv trayektoriyasini va natijalarini saqlashni ta’minlaydi. Nazariy modul gipermatnli ma’ruzalar, qisqa videofragmentlar, formulalar va isbotlarni o‘z ichiga oladi. Animatsiyalar moduli algoritmlarni bosqichma-bosqich ko‘rsatadi, virtual laboratoriya esa talabaga ixtiyoriy kattalikdagi sonlar bilan mustaqil hisoblash o‘tkazish imkonini beradi.



1-rasm. Multimediali dasturiy ta'minotning tuzilmasi.

Nazorat moduli adaptiv testlar va hisoblash topshiriqlarini avtomatik tekshiradi: hisoblash topshiriqlarida har bir talabaga tasodifiy parametrlar asosida alohida variant generatsiya qilinadi. Yordamchi modul o'zbek, rus va ingliz tillaridagi atamalar glossariysini va ma'lumotnoma jadvallarini o'z ichiga oladi. Dastur brauzerda internet aloqasisiz ishlaydi, SCORM paketi ko'rinishida esa Moodle kabi LMS platformalariga joylashtiriladi. Katta sonlar bilan aniq hisoblash JavaScript tilining ixtiyoriy aniqlikdagi BigInt tipi yordamida amalga oshirilgan [8].

3. Matematik mazmunni vizuallashtirish. Dasturda har bir mavzu formal ta'rif, animatsiyali misol va interaktiv tajriba ketma-ketligida bayon qilinadi. Modul arifmetikasining asosiy tushunchasi – taqqoslama:

$$a \equiv b \pmod{n} \iff n \mid (a - b). \tag{1}$$

Evklid algoritmi $r_{i+1} = r_{i-1} \bmod r_i$ rekurrent munosabati asosida ishlaydi, uning kengaytirilgan varianti esa Bezu munosabatini qanoatlantiruvchi koeffitsiyentlarni topadi:

$$a \cdot s + b \cdot t = EKUB(a, b). \tag{2}$$

Agar EKUB $(a, n) = 1$ bo'lsa, (2) dan a ning n modul bo'yicha teskarisi $a^{-1} \equiv t \pmod{n}$ kelib chiqadi. Dasturda kengaytirilgan Evklid algoritmi jadval ko'rinishida animatsiya qilinadi: har bir qadamda yangi qator paydo bo'ladi va hisoblashda qatnashgan kataklar rang bilan ajratiladi. 2-jadvalda RSA algoritmining o'quv adabiyotlarida keng qo'llaniladigan misoli uchun $e = 17$ ning $\varphi(n) = 3120$ modul bo'yicha teskarisini topish jarayoni keltirilgan.

2-jadval

Kengaytirilgan Evklid algoritmi: $17^{-1} \bmod 3120$ ni hisoblash

i	r_i	q_i	s_i	t_i
0	3120	–	1	0
1	17	183	0	1
2	9	1	1	−183
3	8	1	−1	184
4	1	8	2	−367

Jadvaldan $3120 \cdot 2 + 17 \cdot (-367) = 1$ ekani kelib chiqadi, demak, $17^{-1} \equiv -367 \equiv 2753 \pmod{3120}$. Talaba virtual laboratoriyada $17 \cdot 2753 = 46801 = 15 \cdot 3120 + 1$ tengligini tekshirib, natijaning to'g'riligiga ishonch hosil qiladi.

Eyler funksiyasi va Eyler teoremasi RSA algoritmining to'g'riligini asoslaydi:

$$\varphi(n) = n \cdot \prod_{p \mid n} (1 - 1/p), \quad a^{\varphi(n)} \equiv 1 \pmod{n}, \quad EKUB(a, n) = 1. \tag{3}$$

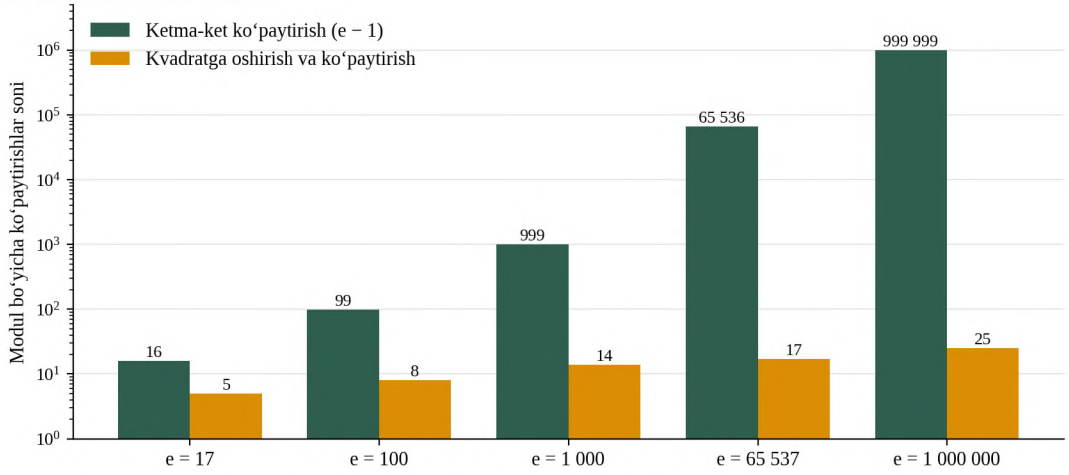
Xitoy qoldiqlar teoremasi o‘zaro tub modullar bo‘yicha taqqoslamalar tizimining yagona yechimini beradi:

$$x \equiv \Sigma\, a_i M_i y_i \ (mod\ M), \quad M = \prod m_i, \quad M_i = M/m_i, \quad y_i \equiv M_i^{-1} \ (mod\ m_i). \tag{4}$$

Modul bo‘yicha darajaga ko‘tarish mavzusida algoritmlar samaradorligini vizual taqqoslash muhim didaktik ahamiyatga ega. Daraja ko‘rsatkichi ikkilik ko‘rinishda $e = \Sigma\, e_i \cdot 2^i$ yozilsa, kvadratga oshirish va ko‘paytirish usulida ko‘paytirishlar soni quyidagiga teng:

$$N(e) = (\lfloor \log_2 e \rfloor) + (w(e) - 1), \tag{5}$$

bu yerda $w(e)$ – e ning ikkilik yozuvidagi birlar soni. Ketma-ket ko‘paytirishda esa $e - 1$ ta ko‘paytirish talab etiladi. 2-rasmda turli daraja ko‘rsatkichlari uchun (5) formula bo‘yicha hisoblangan qiymatlar keltirilgan. Masalan, RSA da keng qo‘llaniladigan $e = 65537$ uchun tez usul 17 ta ko‘paytirishni talab qiladi, ketma-ket usul esa 65536 tani.



2-rasm. Modul bo‘yicha darajaga ko‘tarishda ko‘paytirishlar soni (logarifmik shkala).

4. Multimedia dizayn tamoyillarini amalga oshirish. Dasturiy ta’minot interfeysi va mazmuni R. Mayerning multimediali o‘rganish tamoyillari asosida loyihalandi (3-jadval). Ularning maqsadi – talabaning kognitiv yuklamasini kamaytirib, e’tiborini matematik mohiyatga qaratish.

3-jadval

Multimedia dizayn tamoyillarining dasturda amalga oshirilishi

Tamoyil	Mazmuni	Dasturda amalga oshirilishi
Bo‘laklash	Murakkab materialni talaba boshqaradigan qismlarga ajratish	Animatsiya “Keyingi qadam” tugmasi bilan boshqariladi
Signallash	Muhim elementlarni ajratib ko‘rsatish	Joriy qadamdagi sonlar va formulalar rang bilan belgilanadi
Fazoviy yaqinlik	Matn va tasvirni yonma-yon joylashtirish	Izoh animatsiyaning bevosita yonida chiqadi
Modallik	Tasvirni og‘zaki izoh bilan birga berish	Videofragmentlar ovozli izoh bilan ta’minlangan
Ortiqchasiz bayon	Mavzuga aloqasiz elementlarni olib tashlash	Bezak elementlarisiz minimalistik interfeys

5. Dasturiy ta’minotdan foydalanishni tashkil etish. Dasturiy ta’minotdan o‘quv jarayonining to‘rt shaklida foydalanish ko‘zda tutilgan.

Ma’ruza mashg‘ulotida o‘qituvchi animatsiyalar moduli yordamida algoritmlarni bosqichma-bosqich namoyish etadi va har bir qadamdan oldin talabalarga keyingi natijani bashorat qilish savolini beradi. Amaliy va laboratoriya mashg‘ulotlarida talabalar virtual laboratoriyada individual variantlar bo‘yicha hisoblashlarni bajaradi va natijalarni qo‘lda bajarilgan hisoblar bilan solishtiradi. *Mustaqil ta’limda* nazariy modul va adaptiv testlar mavzuni takrorlash hamda o‘z-o‘zini nazorat qilish uchun ishlatiladi. *Masofaviy ta’limda* dastur SCORM paketi ko‘rinishida LMSga joylashtiriladi, o‘qituvchi esa guruh statistikasi asosida qiyin mavzularni aniqlaydi [9].

Natijalar multimedia dizayni tamoyillariga asoslangan o‘quv resurslarining samaradorligi haqidagi xalqaro tadqiqotlar xulosalariga mos keladi. Dasturning asosiy afzalligi – sonlar nazariyasining abstrakt tushunchalarini kriptografik algoritmlar bilan bevosita bog‘lashidir: talaba Evklid algoritmini alohida mashq

sifatida emas, balki RSA kalitini yaratishning zaruriy qadami sifatida o‘zlashtiradi. Virtual laboratoriyada katta sonlar bilan ishlash imkoniyati esa algoritmlarning hisoblash murakkabligi haqida aniq tasavvur shakllantiradi, 2-rasmda ko‘rsatilgan taqqoslash buning yaqqol misolidir. Shu bilan birga, dasturiy ta’minotdan foydalanishda ayrim cheklovlarni hisobga olish lozim. Animatsiyalarni passiv kuzatish talabaning faol fikrlashini almashtirmasligi kerak, shu sababli har bir animatsiya bashorat savollari va mustaqil hisoblash topshiriqlari bilan birga qo‘llaniladi. Shuningdek, talabalarning qo‘lda hisoblash ko‘nikmalarini saqlab qolish uchun nazorat ishlarining bir qismi dastursiz bajariladi. Tadqiqot ishi AL-9624115223-sonli “Kriptografiya” fani bo‘yicha elektron o‘quv qo‘llanma yaratish” mavzusidagi amaliy loyiha doirasida bajarildi.

Xulosa va tavsiyalar. Tadqiqot natijasida quyidagi xulosalarga kelindi. Birinchidan, “Kriptografiya”ning matematik asoslari” bo‘limini o‘qitishdagi asosiy qiyinchiliklar tushunchalarning abstraktligi, katta sonlar bilan qo‘lda hisoblashning imkonsizligi va ko‘p bosqichli protseduralarni idrok etishning murakkabligi bilan bog‘liq. Ikkinchidan, ADDIE modeli asosida ishlab chiqilgan, nazariy, animatsion, virtual laboratoriya, nazorat va yordamchi modullardan iborat multimediali dasturiy ta’minot bu qiyinchiliklarni bartaraf etish imkonini beradi. Uchinchidan, R.Mayerning multimedia dizayn tamoyillarini qo‘llash kognitiv yuklamani kamaytiradi, dasturdan ma’ruza, laboratoriya, mustaqil va masofaviy ta’limda tizimli foydalanish esa bo‘lim bo‘yicha o‘quv jarayonining uzluksizligini ta’minlaydi. Ishlab chiqilgan dasturiy ta’minot va metodikani kriptografiya fanining boshqa bo‘limlarini, shuningdek, diskret matematika va sonlar nazariyasi fanlarini o‘qitishda ham qo‘llash mumkin.

Foydalanilgan adabiyotlar ro‘yxati:

[1]. O‘zbekiston Respublikasi Prezidentining 2019-yil 8-oktabrdagi “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-5847-farmoni. www.lex.uz.

[2]. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi «Raqamli O‘zbekiston–2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-farmoni. www.lex.uz.

[3]. Mayer R.E. Multimedia Learning. 2nd ed. New York, Cambridge University Press, 2009, 304 p.

[4]. Branch R.M. Instructional Design: The ADDIE Approach. New York, Springer, 2009, 203 p.

[5]. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Pearson, 2017, 767 p.

[6]. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Springer, 2010, 372 p.

[7]. Tillayev A.I. Videoma’ruzalar tayyorlashning zamonaviy dasturiy vositalari yordamida o‘quv video materiallarini ishlab chiqish. “O‘zMU xabarlari”, 2025, 1-son/12, 206–209-betlar.

[8]. Tillayev A.I. Oliy ta’limda videoma’ruzalar tayyorlashning umumiy qoidalari. “Ilm sarchashmalari” UrDU ilmiy jurnali, 2025, 12-son/2, 138–141-betlar.

[9]. Azamat Tillaev. Development of An Electronic Training Manual on Cryptographic Methods Using Modern Multimedia and Artificial Intelligence Technologies. International Journal of Pedagogics, 6(05), USA, 2026, p. 463–466.

[10]. CrypTool: e-learning platform for cryptography and cryptanalysis [elektron resurs]. URL, https:/ /www. cryptool.org.

[11]. SageMath: open-source mathematics software system [Elektron resurs]. URL: https://www.sagemath. org.

Melliyeva Dilfuza O‘ralovna (Denov Tadbirkorlik va pedagogika instituti, Pedagogika fakulteti, “Boshlang‘ich ta’lim metodikasi” kafedrasi o‘qituvchisi; Email:d.meliyeva@.dtpi.uz;ORCID ID:0009-0005-7397-5233)

O‘QITUVCHINING O‘Z-O‘ZINI ANGLASHI, O‘QUV FAOLIYATINI REJALASHTIRISHI, MONITORING QILISHI VA BAHOLASH QOBILIYATLARINING KASBIY RIVOJLANISHDAGI O‘RNI

Annotatsiya. *Mazkur maqolada bo‘lajak boshlang‘ich sinf o‘qituvchilarining metakognitiv kompetensiyalarini rivojlantirishning nazariy-metodologik va amaliy asoslari yoritilgan. Tadqiqotda metakognitiv kompetensiyaning mazmuni, tarkibiy komponentlari hamda uni rivojlantirish imkoniyatlari kompetensiyaviy, fanlararo integrativ va refleksiv-faoliyatli yondashuvlar asosida tahlil qilingan. J.Flavell, G. Schraw va L.S.Vigotskiyning metakognitiv rivojlanish, kognitiv monitoring hamda rivojlantiruvchi ta’limga oid ilmiy qarashlari metodologik asos sifatida belgilangan. Tadqiqot jarayonida metakognitiv didaktik modullar, integrativ o‘quv klasterlari, fanlararo topshiriqlar, muammoli-amaliy vaziyatlar, refleksiv keyslar va o‘z-o‘zini baholash mexanizmlaridan foydalanish imkoniyatlari o‘rganilgan. Olingan natijalar mazkur metodik vositalarning bo‘lajak o‘qituvchilarda o‘z bilish faoliyatini rejalashtirish, monitoring qilish, boshqarish, baholash va refleksiv tahlil qilish ko‘nikmalarini rivojlantirishdagi ahamiyatini ko‘rsatgan. Tadqi-*