"KRIPTOGRAFIK USULLAR" FANINI O'QITISHDA NAZARIY VA AMALIYOT MASHG'ULOTLAR MUVOZANATINI TA'MINLASH: MUAMMOLAR VA PEDAGOGIK YECHIMLAR

Gaziyev Quyosh Azamatovich
Namangan davlat universiteti,
Raqamli ta'lim texnologiyalari kafedrasi katta o'qituvchisi
hilol200218@gmail.com
+99893 705 17 14, ORCID: 0009-0004-5428-7278

Annotatsiya*. Ushbu maqolada oliy ta'lim muassasalarida "Kriptografik usullar" fanini o'qitish jarayonida nazariya va amaliyot mashg'ulotlar o'rtasidagi muvozanatni ta'minlash masalasi tahlil qilinadi. Kriptografiya kabi murakkab va yuqori matematik asosga ega fanlarda nazariy tushunchalarning ko'pligi, laboratoriya mashg'ulotlari uchun texnik resurslarning yetishmasligi, talabalar tayyorgarlik darajasidagi farqlar hamda o'qituvchilarning amaliy kiberxavfsizlik tajribasi cheklanganligi asosiy muammolar sifatida ko'rsatiladi. Tadqiqot metodologiyasi sifatida pedagogik kuzatuv, so'rovnoma, o'quv natijalarini tahlil qilish va tajriba-sinov yondashuvlari qo'llanildi. Natijalar shuni ko'rsatadiki, modul asosidagi o'qitish, loyiha, muammoli vaziyatlar, simulyatsiya va laboratoriya mashg'ulotlarini minimal resurslar bilan tashkil etish usullari fan samaradorligini sezilarli oshiradi. Muhokama qismida mazkur yechimlarning didaktik va metodik afzalliklari hamda ularni O'zbekiston oliy ta'lim tizimiga moslashtirish imkoniyatlari asoslab beriladi.*

Kalit so'zlar*: kriptografik usullar, nazariya-amaliyot muvozanati, laboratoriya mashg'uloti, loyiha asosida o'qitish, kiberxavfsizlik, pedagogik yechimlar, kompetensiya.*

ОБЕСПЕЧЕНИЕ БАЛАНСА ТЕОРЕТИЧЕСКИХ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПРИ ПРЕПОДАВАНИИ ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ»: ПРОБЛЕМЫ И ПЕДАГОГИЧЕСКИЕ РЕШЕНИЯ

Аннотация. *В данной статье анализируется проблема обеспечения баланса между теоретическими и практическими занятиями в процессе преподавания дисциплины «Криптографические методы» в высших учебных заведениях. В качестве основных проблем выделяются: большое количество теоретических понятий в таких сложных и математически насыщенных дисциплинах, как криптография; недостаток технических ресурсов для проведения лабораторных занятий; различия в уровне подготовки студентов; а также ограниченный практический опыт преподавателей в области кибербезопасности. В качестве методологии исследования использовались педагогическое наблюдение, анкетирование, анализ учебных результатов и экспериментальные подходы. Результаты показывают, что модульное обучение, проектный подход, проблемно-ориентированное обучение, симуляции и*

организация лабораторных занятий с минимальными ресурсами значительно повышают эффективность обучения. В разделе обсуждения обосновываются дидактические и методические преимущества данных решений, а также возможности их адаптации к системе высшего образования Узбекистана.

Ключевые слова: *криптографические методы, баланс теории и практики, лабораторные занятия, проектное обучение, кибербезопасность, педагогические решения, компетенции.*

ENSURING THE BALANCE BETWEEN THEORETICAL AND PRACTICAL TRAINING IN TEACHING THE COURSE "CRYPTOGRAPHIC METHODS": PROBLEMS AND PEDAGOGICAL SOLUTIONS

Abstract. *This article analyzes the issue of ensuring a balance between theoretical and practical training in teaching the course "Cryptographic Methods" in higher education institutions. In complex and mathematically intensive disciplines such as cryptography, the abundance of theoretical concepts, the lack of technical resources for laboratory work, differences in students' prior knowledge, and the limited practical cybersecurity experience of instructors are identified as the main challenges. The research methodology includes pedagogical observation, surveys, analysis of learning outcomes, and experimental approaches. The results indicate that modular teaching, project-based learning, problem-based approaches, simulations, and organizing laboratory activities with minimal resources significantly enhance the effectiveness of the course. The discussion section substantiates the didactic and methodological advantages of these solutions, as well as their adaptability to the higher education system of Uzbekistan.*

Keywords: *cryptographic methods, theory-practice balance, laboratory training, project-based learning, cybersecurity, pedagogical solutions, competence.*

KIRISH

Raqamli transformatsiya jarayonlari kuchaygan sari axborot xavfsizligi masalalari barcha sohalarda ustuvor yo'nalishga aylanmoqda. Elektron hukumat, raqamli bank xizmatlari, elektron savdo, onlayn ta'lim, mobil to'lov tizimlari va bulutli xizmatlarning kengayishi kriptografiya fanining amaliy ahamiyatini keskin oshirdi. "Kriptografik usullar" fani axborot xavfsizligi, dasturiy injiniring, kompyuter injiniringi, telekommunikatsiya va raqamli iqtisodiyot yo'nalishlarida muhim tayanch fanlardan biri sifatida o'qitiladi. Shu bilan birga, kriptografiya o'z tabiatiga ko'ra ikki qatlamli: bir tomondan matematik nazariya (sonlar nazariyasi, modul arifmetika, algebraik tuzilmalar, ehtimollar nazariyasi), ikkinchi tomondan esa real

tizimlar va protokollar (PKI, TLS, raqamli imzo, kalitlarni boshqarish, parollarni xeshlash, autentifikatsiya) bilan bog‘liq.

Amaliyotdan ajralgan nazariya talabada “quruq formula” tasavvurini shakllantiradi, amaliyotga haddan tashqari urg‘u berish esa algoritmning ilmiy asosini tushunmasdan “tayyor kutubxona ishlatish” darajasida qolib ketish xavfini tug‘diradi. Shu sababli, kriptografiyani o‘qitishda nazariya va amaliyot muvozanatini topish – zamonaviy pedagogik va metodik vazifalardan biridir. Bu masala xalqaro adabiyotlarda ham “kriptografiya fanini kompetensiyaga asoslangan o‘qitish”, “amaliy mashg‘ulotlar orqali o‘qitish”, “real loyihalar orqali o‘rganadigan ta’lim” kabi yo‘nalishlarda muhokama qilinadi (Stallings, 2017; Katz & Lindell, 2020; Schneyer, 2015).

Ushbu maqolada oliy ta’limda “Kriptografik usullar” fanini o‘qitish tajribasi asosida muammolar aniqlanib, ularni bartaraf etish uchun modul asosidagi integratsiyalashgan (nazariya + laboratoriya + loyiha) model taklif etiladi.

ADABIYOTLAR TAXLILI

Oliy ta’limda “Kriptografik usullar” fanini o‘qitishda nazariya va amaliyot muvozanatini ta’minlash soha mutaxasislari tomonidan dolzarb yo‘nalish sifatida ko‘rib chiqilmoqda. Kriptografiya fanining murakkabligi, avvalo, uning ikki qatlamli kompetensiya talab qilishi bilan izohlanadi: bir tomondan matematik-nazariy asos (sonlar nazariyasi, modul arifmetika, algebra), ikkinchi tomondan esa real tizimlarda qo‘llash — implementatsiya, protokol tahlili, kalitlarni boshqarish, konfiguratsiya kabi amaliy ko‘nikmalar bilan bog‘liq. Shu sababli, kriptografiya ta’limida faqat nazariy yondashuv “quruq formula” darajasida qolish xavfini tug‘dirsa, faqat amaliy yondashuv esa algoritm mexanizmini tushunmasdan tayyor kutubxona ishlatish holatini kuchaytiradi.

Abdullayev va Hamidov (2018**)** “Kriptografiya va axborot xavfsizligi o‘qitish metodikasi” nomli maqolasida O‘zbekiston oliy ta’lim muassasalarida kriptografiya bo‘yicha o‘quv rejalari va laboratoriya mashg‘ulotlarini tashkil etishning amaliy aspektlarini tahlil qilgan. Mualliflar talabalar uchun modulli o‘qitish, laboratoriya mashqlarini bloklarga bo‘lish va real hayotiy masalalar asosida laboratoriya topshiriqlarini ishlab chiqishni taklif qiladi. Bu yondashuv nazariya va amaliyotni

bosqichma-bosqich uyg‘unlashtirishni maqsad qilgan. Islomova va Karimov (2022) pedagogik jurnalda nashr etilgan maqolalarida “simulyatsiya muhitida xavfsizlik protokollarini o‘rgatish” metodikasini taklif qiladi. Mualliflar Python va virtualizatsiya vositalaridan foydalanib, talabalarni real xavfsizlik tizimlarining xatti-harakatlarini sinab ko‘rishga yo‘naltiradi. Bu yondashuv G‘arb tadqiqotlaridagi “amaliy kiberxavfsizlik laboratoriyalari” yondashuvi bilan chambarchas bog‘liq.

O‘zbekiston olimlari tadqiqotlarida ham kriptografiyani o‘qitishda nazariya-amaliyot uyg‘unligini kuchaytirish masalasi alohida qayd etiladi. Mahalliy ilmiy ishlarda o‘quv jarayonini modul asosida o‘qitish, laboratoriya mashg‘ulotlarini real ssenariylar asosida tashkil etish, simulyatsiya vositalaridan (Python, OpenSSL, virtualizatsiya) foydalanish hamda loyiha asosida baholashni joriy etish g‘oyalari ilgari suriladi. MDH tajribasida esa muammoli vazifa →ilmiy tahlil → kod implementatsiyasi ketma-ketligi orqali talabalarda amaliy kompetensiyani shakllantirish samarali ekanligi ta’kidlanadi. Ushbu yo‘nalishdagi ishlar kriptografiya fanini faqat nazariy fan sifatida emas, balki real kiberxavfsizlik kompetensiyasini shakllantiruvchi amaliy fan sifatida ko‘rish zarurligini ko‘rsatadi.

Xorij adabiyotlarida kriptografiyani o‘qitishning metodik asoslari turli rakurslarda yoritilgan. Stallings (2017) kriptografik algoritmlarni real protokollar bilan bog‘lab o‘qitish zarurligini ko‘rsatadi. Shnayer (2015) esa amaliy xatolar, noto‘g‘ri konfiguratsiya va xavfsiz bo‘lmagan parametr tanlash real xavfsizlikka eng katta tahdid ekanini ta’kidlab, amaliy laboratoriya mashg‘ulotilarning didaktik ahamiyatini asoslaydi. Katz va Lindell (2020) kriptografik xavfsizlikni formal model asosida tushuntirish orqali talabalarda “nega xavfsiz?” degan savolga ilmiy javob shakllantirishga urg‘u beradi. Boneh va Shoup (2020) esa kriptografiyani real protokollar, hujum ssenariylari va loyiha asosida o‘qitish orqali o‘qitish samaradorligini ko‘rsatadi. Shu bilan birga, Menezes(1996) kriptografiyaning keng qamrovli amaliy va nazariy bazasini taqdim etadi, biroq uning murakkabligi bakalavr bosqichida metodik soddalashtirishni talab qiladi.

Shuningdek, kriptografiya ta’limida texnik standartlar ham muhim manba sifatida qaraladi. AES bo‘yicha FIPS 197 (NIST, 2001) hamda, raqamli imzo bo‘yicha FIPS 186-4 (NIST, 2015) standartlari talabalarga algoritmlarning rasmiy tuzilishi

va amaliy parametrlarini o‘rgatish imkonini beradi. Biroq standartlar matni murakkab bo‘lgani sababli, ularni o‘qitishda metodik soddalashtirish, laboratoriya va loyiha topshiriqlari bilan integratsiya qilish zarur.

Xulosa qilib aytganda, o‘zbek va xorijiy ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, “Kriptografik usullar” fanini samarali o‘qitish uchun integratsiyalashgan model talab etiladi. Bu model nazariy tushuncha, amaliy mashg’ulot implementatsiyasi va real amaliy loyiha elementlarini birlashtirishi, baholash esa faqat test bilan cheklanmay, kompetensiyaga asoslangan mezonlar orqali amalga oshirilishi kerak.

Tadqiqot maqsadi va savollari.

Tadqiqot maqsadi — “Kriptografik usullar” fanini o‘qitishda nazariya-amaliyot muvozanatini buzuvchi omillarni aniqlash va ularni bartaraf etishga qaratilgan pedagogik yechimlarni asoslash.

Tadqiqot savollari: (1) muvozanatni buzuvchi omillar nimalar? (2) qaysi metodlar uyg‘unlikni oshiradi? (3) minimal resurs sharoitida laboratoriya qanday tashkil qilinadi?

2. Metodologiya

Ushbu tadqiqot oliy ta’lim muassasasida “Kriptografik usullar” fanini o‘qitish jarayonida olib borilgan tajriba-sinov ishlari asosida shakllantirildi. Tadqiqotda aralash metodlar yondashuvi qo‘llanildi, ya’ni sifat va miqdoriy tahlil elementlari birlashtirildi.

2.1. **Ishtirokchilar**. Tadqiqotda amaliy matematika, axborot tizimlari va texnologiyalari yo‘nalishida tahsil olayotgan bakalavr bosqichining 3–4-kurs talabalari hamda mazkur fanni o‘qituvchi professor-o‘qituvchilar ishtirok etdi. Talabalar guruhlari tayyorgarlik darajasi bo‘yicha farqlanishi kuzatildi: ayrimlar matematik asosda kuchli, boshqalar esa dasturlashda kuchli bo‘ldi.

2.2. **Tadqiqot dizayni**. Tadqiqot uch bosqichda amalga oshirildi: (1) diagnostika bosqichi (so‘rovnoma, suhbat), (2) intervensiya bosqichi (yangi o‘qitish modeli joriy etish), (3) baholash bosqichi (yakuniy test, laboratoriya natijalari, loyiha himoyasi).

2.3. **Ma'lumot yig'ish vositalari**. Talabalar uchun so'rovnoma (fan qiyinchiliklari, motivatsiya, amaliy ko'nikma ehtiyoji), o'qituvchilar bilan yarim strukturalangan suhbat, yakuniy nazorat natijalari (test + amaliy topshiriq), laboratoriya ishlari va loyiha portfoliolari yig'ildi.

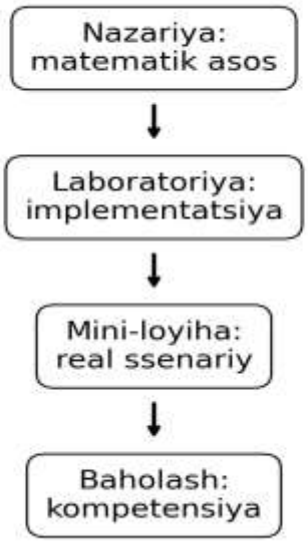
2.4. **Tahlil usullari**. Miqdoriy ma'lumotlar foiz ko'rsatkichlari orqali umumlashtirildi. Sifat tahlili orqali muammolar kategoriyalarga ajratildi. Nazariya-amaliyot muvozanatini baholash uchun kompetensiya indikatorlari ishlab chiqildi: algoritmni tushuntirish, implementatsiya, xavfsizlik xatolarini topish, protokolni tahlil qilish.

3. Natijalar

Tadqiqot natijalari kriptografiya fanini o'qitishda nazariya-amaliyot muvozanatini ta'minlashga to'sqinlik qiluvchi muammolarni 4 ta asosiy guruhga ajratish mumkinligini ko'rsatdi. Quyida har bir muammo guruhining didaktik ildizlari va o'qitish jarayoniga ta'siri batafsil yoritiladi.

Muammo	Ko'rinishi	O'qitishga ta'siri
Matematik tayyorgarlik tafovuti	Modul arifmetika, Eyler funksiyasi, tub sonlar mavzularida qiyinchilik	Nazariy blok sekinlashadi; motivatsiya pasayadi
Laboratoriya resurslari cheklanganligi	Maxsus laboratoriya, server, ajratilgan muhit yo'qligi	Amaliyot "qog'ozdagi masala" darajasida qoladi
Kutubxona darajasidagi amaliyot	AES/RSA faqat tayyor funksiyalar orqali ishlatiladi	Algoritm mexanizmi va xavfsiz parametr tanlash shakllanmaydi
O'qituvchi amaliy tajribasining cheklanishi	TLS, PKI, sertifikatlar bo'yicha real tajriba kam	Zamonaviy protokollar yuzaki tushuntiriladi

1-Jadval. Nazariya-amaliyot muvozanatini buzuvchi muammolar va ularning ta'siri.



1-Chizma. Kriptografiya fanida nazariya-amaliyot integratsiyasi modeli.

3.1. **Matematik tayyorgarlikdagi tafovut**. Talabalar orasida modul arifmetika, Evklid algoritmi, Eyler funksiyasi kabi mavzularni tushunish darajasi keskin farq qiladi. Bu holat kriptografiya fanining "kirish" qismidayoq muvozanatni buzadi: matematik tayyorgarligi kuchli talaba tez zerikishi mumkin, tayyorgarligi sust talaba esa fan "men uchun emas" degan xulosaga keladi. Shuning uchun diagnostika bosqichida qisqa pre-test va tayyorlov mini-modul joriy etish zarur.

3.2. **Amaliy laboratoriya resurslarining cheklanganligi**. Kriptografiya laboratoriyasi ko'pincha maxsus jihozlar talab qiladigandek ko'rinadi. Aslida esa ko'plab amaliy mashg'ulotlar bepul va ochiq manbali vositalar asosida tashkil etilishi mumkin: OpenSSL, Python, Docker, VirtualBox, Wireshark. Bu yondashuv zamonaviy "hands-on" kiberxavfsizlik ta'limi tamoyillariga mos keladi (Stallings, 2017).

3.3. **Dasturlash amaliyotining "kutubxona" darajasida qolishi**. Talabalar ko'pincha AES yoki RSA algoritmlarini tayyor kutubxona orqali chaqirib ishlatadi. Bu esa algoritm ichki mexanizmini tushunish, xavfsizlik parametrlarini to'g'ri tanlash, xatolarni aniqlash kabi ko'nikmalarni shakllantirmaydi. Masalan, RSA implementatsiyasida padding (to'ldirish) ishlatilmasa, tizim real hujumlarga ochiq bo'lib qoladi (Katz & Lindell, 2020).

3.4. **O‘qituvchining amaliy kiberxavfsizlik tajribasi cheklanishi**. O‘qituvchi nazariy jihatdan kuchli bo‘lsa-da, real hayotdagi TLS, PKI, sertifikatlar, kalitlarni boshqarish, parol xeshlash amaliyoti kabi mavzularda yetarli tajribaga ega bo‘lmasligi mumkin. Bu esa talabaning real tizimlarni tahlil qilish kompetensiyasini cheklaydi (Schneier, 2015).

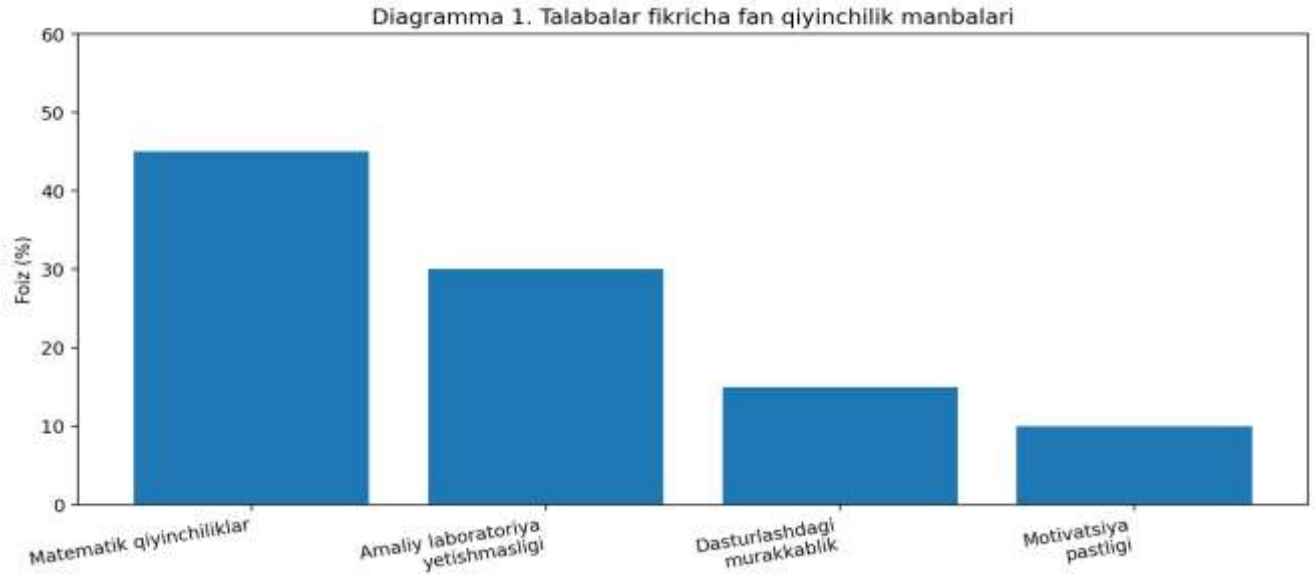


Diagramma 1. Talabalar fikricha fan qiyinchilik manbalari (so‘rovnoma natijalari, %).

4. **Muhokama**

Natijalar shuni ko‘rsatadiki, kriptografiya fanini samarali o‘qitish uchun nazariya va amaliyot o‘rtasidagi muvozanatni aniq metodik model asosida qurish zarur. An’anaviy yondashuvlarda nazariya asosiy o‘rinni egallab, amaliy mashg‘ulotlar ikkinchi darajaga tushib qoladi. Bu esa kriptografiyaning real hayotdagi qo‘llanishlarini tushunishni qiyinlashtiradi.

4.1. **Modul + laboratoriya + loyiha integratsiyasi**. Taklif etilgan modelda har bir mavzu uch bosqichda beriladi: (1) nazariy tushuncha, (2) laboratoriya implementatsiyasi, (3) real ssenariy asosidagi mini-loyiha. Bu yondashuv Bloom taksonomiyasi bo‘yicha “tushunish → qo‘llash → tahlil” ketma-ketligini tabiiy ta’minlaydi.

4.2. **Minimal resurs laboratoriya modeli**. Kriptografik laboratoriya uchun alohida maxsus qurilmalar shart emas. Bepul vositalar orqali talabalar real amaliy

ko‘nikmalarni egallashi mumkin. Masalan, OpenSSL orqali sertifikat yaratish, Wireshark orqali TLS maxsus boshqaruv paketlarini ko‘rish, Python orqali xesh va shifrlashni implementatsiya qilish mumkin.

4.3. **Kompetensiyaga asoslangan baholash**. Faqat test bilan baholash kriptografiya fanida yetarli emas. Talabaning amaliy natijasi, kod sifati, xavfsizlik parametrlarini to‘g‘ri tanlashi va protokolni tahlil qila olishi baholashning markazida bo‘lishi kerak.

4.4. **O‘qituvchi kompetensiyasi**. Kriptografiya tez rivojlanayotgan soha bo‘lib, algoritmlar va standartlar yangilanib boradi. Shu sababli o‘qituvchi ham nazariy, ham amaliy kompetensiyasini muntazam yangilab borishi zarur. Bu sanoat hamkorligi, amaliy seminarlar, sertifikatlash va laboratoriya metodikasini o‘rganish orqali amalga oshirilishi mumkin.

XULOSA

Maqolada oliy ta’limda “Kriptografik usullar” fanini o‘qitishda nazariya va amaliyot muvozanatini ta’minlash muammolari va pedagogik yechimlari tahlil qilindi. Tadqiqot natijalariga ko‘ra, muvozanatni buzuvchi asosiy omillar: matematik tayyorgarlikdagi farqlar, laboratoriya resurslarining yetishmasligi, amaliyotning “kutubxona darajasida” qolishi hamda o‘qituvchilarning amaliy tajribasi cheklanganligidir.

Taklif etilgan modul asosidagi o‘qitish, minimal resurs laboratoriya modeli, loyiha yondashuvi va kompetensiyaga asoslangan baholash tizimi nazariya va amaliyot uyg‘unligini sezilarli oshirishi aniqlandi.

Amaliy tavsiya sifatida, OTMlarda kriptografiya fanini o‘qitishda har bir mavzu “nazariya + laboratoriya + mini-loyiha” ketma-ketligida tashkil etilishi, baholash esa test bilan cheklanmay, amaliy natijalar va loyiha himoyasini ham o‘z ichiga olishi kerak.

Foydalanilgan adabiyotlar

1.Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson. 2017.
2.Schneier, B. Applied Cryptography. Wiley. 2015.
3.Katz, J., & Lindell, Y. Introduction to Modern Cryptography. CRC Press. 2020.
4. Boneh, D., & Shoup, V. A Graduate Course in Applied Cryptography. 2020.

5. Gaziyev Q.A. Kriptografik usullar maxsus fanini o'qitishda Moodle tizimidan foydalanish. "Global transformatsiyalar asrida fan, texnologiyalar, innovatsiyalar" mavzusidagi xalqaro onlayn ilmiy-amaliy anjumani .- Farg'ona, FarDU, 2025 - yil 18 - 19 - noyabr.– 127-129-betlar.
6. Gaziyev Q.A. Kriptografik algoritmlarni o'qitishda talabalar tomonidan murakkab matematik modellarning o'zlashtirilishidagi muammolar va ularni vizual, interaktiv metodlar orqali bartaraf etish. "Raqamli iqtisodiyot sharoitida fan va ta'limni ishlab chiqarish bilan integratsiyasini rivojlantirishning ustuvor yo'nalishlari" mavzusida xalqaro ilmiy amaliy anjuman.-Toshkent, TATU, 2025-yil, 19-20-dekabr, 523-525 betlar