

AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

BAKİ DÖVLƏT UNİVERSİTETİ

MAGİSTRATURA PİLLƏSİ ÜÇÜN

Tətbiqi riyaziyyat və kibernetika fakültəsi Elmi Şurasının
03.03. 2021-cı il tarixli iclasının qərarı ilə təsdiq edilmişdir
(protokol №6)

İXTİSAS: 060501-Riyaziyyat

FƏNN: MİF-B01 Kompüter elmlərinin müasir problemləri

(I kurs, I semestr)

Bakı- 2021

Tərtib edənlər: Rəhimova Gülarə Əli qızı, i.f.d, İnformatika kafedrası üzrə dosent

Rəy verənlər:

- 1. Əliyev Ələkbər Əli oğlu –İnformasiya texnologiyaları və proqramlaşdırma kafedrasının müdiri, professor.**
- 2. Əliyev Aydın Yunus oğlu – BDU, Hesablama riyaziyyatı kafedrasının dosenti**

Elmi redaktor:

Xəlilov Mübariz Sevdimalı oğlu- BDU, İnformatika kafedrasının müdiri, dosent

İzahat vərəqi

1. Fənnin əsas məqsədi

Bu gün Kompüter elmlərinin tədqiq etdiyi aktual problemlərin sırasına əqli mülkiyyətin əsası sayılan : NBİC texnologiyalar, Suni intellektlər, Eksper sistemləri, Genetik alqoritmlər, Bulud texnologiyalar, “Big Data” texnologiyaları, metaboliklər, robototexnika, nano və pikotexnologiyalar, prototip sistemlər, neyroinformatika, neyrokompyuterlər, şəbəkə texnologiyaları, informasiya cəmiyyətinin multidisiplinar problemləri, bioinformatika, e-tibb, tibbi diaqnostik aparatlar və digər intellektual qurğular sahəsində aparılan müasir tədqiqatlar, riyazi modelləşdirmənin təbiət elmlərinə tətbiqi zamanı meydana çıxan problemlər, Hesablama riyaziyyatının müasir problemləri aiddir. Ümumiyyətlə, intellektual sistemlər üzrə tədqiqatlar oblastı cox genişdir. Bura : İnformasiologiyanın problemləri, koqnitiv modelləşdirmə; intellektual interfeyslər; , kompüter dilçiliyi, obrazların tanınması, nitqin tanınması və sintezi; mətn tipli informasiyaların analizinin üsul və modelləri, mətnin semantik modelinin tədqiqi, deduktiv modellər, çoxagentli sistemlər; ontologiyalar; biliklər menecmenti; yumşaq hesablamalar, E-sənədlərin intellektual emalı, kriptografiyanın problemləri və s. daxildir. Bu sıranı kifayət qədər genişləndirmək olar.

Kursun əsas məqsədi müasir informatikada yeni elmi tədqiqatların nədən ibarət olduğunu açıqlamaq, yuxarıda sadalanan problemlərin elmi izahını və onların inkişaf istiqamətlərini göstərməkdən ibarətdir. Çünki, sadalanan bütün problemlər inkişaf etmiş ölkələrin əsas problemləri sayılır.

2. Fənnin Magistr tədris proqramında yeri

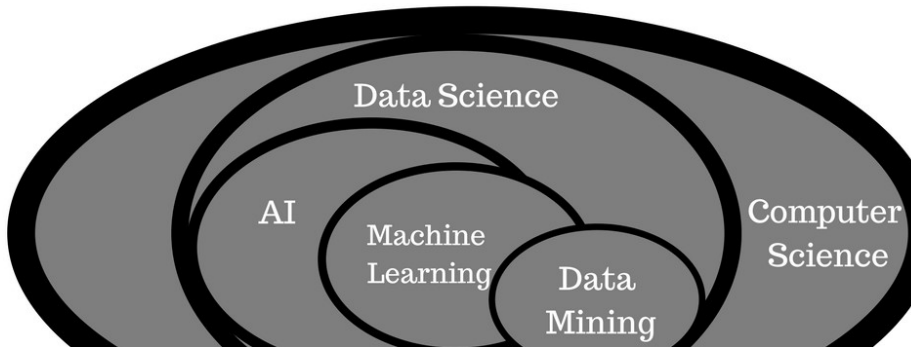
“Kompüter elmlərinin müasir problemləri” kursu Magistr proqramları fənninin baza hissəsinə daxildir.

Kurs bir semestr öyrənilir. Fənnin mənimsənilməsi üçün tələbədən riyaziyyat, diskret riyaziyyat, informatika və yüksək səviyyəli proqramlaşdırma dillərində proqram tərtibinin incəliklərini dayanıqlı bilmək tələb olunur.

“Kompüter elmlərinin müasir problemləri” fənninin tədrisi üçün 30 saat (30 saat müəhazirə, 10 saat məşğələ) həcmində dərs yükü nəzərdə tutulmuşdur.

3. Tədris ilində fənnin həcmi

Tədris işinin növü	Saatların miqdarı	Semestr	
		1	0
Auditor məşğələlər (cəmi)	40	10	0
O cümlədən:			
Mühazirə	30	30	0
Praktik məşğələlər	10	10	0
Seminarlar	–	–	–
Laboratoriya işləri	-	-	–
Sərbəst işlər (cəmi)	10	10	



Mühazirə dərslərinin mövzuları

№	Mövzuların adı	Cəmi	M	S
1.	XXI əsrin konvergent texnologiyaları. NBIC Texnologiyalar. Kompüter elmləri və koqnitiv informasiya texnologiyalarının nəzəri problemləri	3	2	1
2	Koqnitiv informasiya texnologiyaları idarəetmə sistemində. Rəqəmsal iqtisadiyyatda koqnitiv informasiya texnologiyaları	2	2	
3	Kompüter elmlərinin tətbiq sahələrinin problemləri. Hərbi informatika, fiziki-informatika və bioinformatikanın problemləri.	2	2	
4	Optimallaşdırmanın tətbiqi problemləri. Viki mühitdə informasiya təsirinn intellektual analizi sistemləri	2	2	
5	Paralel və Paylanmış proqramlaşdırma, qrid texnologiyalar, qrafiki prosessorlarda proqramlaşdırma problemləri	2	2	
6	Verilənlər elminin (Data Science) problemləri	2	2	
7.	“Big Data” texnologiyaları və informasiya təhlükəsizliyi problemləri	3	2	1
8.	Bulud texnologiyaları iqtisadiyyatı və təhlükəsizliyi problemləri	3	2	1
9.	Riyazi modelləşdirmənin və Hesablama Riyaziyyatının müasir problemləri	3	2	1
10.	İnformasiya texnologiyalarının korpus linqvistikasında tətbiqi. Kompüter tərcüməsinin problemləri. Obrazların tanınması. Mətn tipli informasiyaların analizi və modelləri.	3	2	1
11.	Sinergetik İdarəetmə sistemləri. Təkamül	3	2	1

	hesablamalar . Genetik alqoritmlərin problemləri			
12.	Suni intellektlərlə bağlı problemlər. Robototexnika, Nano və pikotexnologiyalar. Soft computing nəzəriyyəsi. Neyrokompüterlər. Neyroşəbəkələr	3	2	1
13.	Kompüter biotibbinin problemləri. Biotibbi texnologiya mühəndisliyi. Elektron tibbin problemləri.	3	2	1
14.	Superkompüter texnologiyaları. Superkompüterlərin hesblama məhsuldarlığı	3	2	1
15	Kriptoqrafiya elminin problemləri. Kibermühit və Kibercinayətçilik. Kodlaşdırma və verilənlərin sıxılması	3	2	1
	Cəmi	40	30	10

Mövzuların qısa məzmunu

Mövzu №1

XXI əsrin konvergent texnologiyaları. NBIC Texnologiyalar. Kompüter elmləri və koqnitiv informasiya texnologiyalarının nəzəri problemləri

Qısa icmal. Mövzuda XXI əsrin geniş spektrli texnologiyalarından (GPT), radikal yeniliklərdən, Robotika və kosmik texnologiyalardan danışılır. İndi yeni, radikal yeniliklərə nano və pikotexnologiyalar, biotexnologiya və gen mühəndisliyi, yeni nəsil informasiya və kommunikasiya texnologiyaları (kvant, optik və DNT kompüterləri; lazer televizorları, ekransız ekranlar və s.) və idrak texnologiyaları daxildir. Bunlara ümumi olaraq NBIC texnologiyaları deyilir. Başqa sözlə, NBIC-Nano, Bio, İnfö və İdrak texnologiyaları deməkdir. Mövzuda tətbiqi riyaziyyatın, kompüter elmləri və koqnitiv informasiya texnologiyalarının nəzəri problemləri şərh olunur.

Mövzu №2

Koqnitiv informasiya texnologiyaları idarəetmə sistemində. Rəqəmsal iqtisadiyyatda koqnitiv informasiya texnologiyaları

Qısa icmal. Mövzuda intellektual idrak texnologiyaları və onların tətbiqinin ən perspektivli sahələri; ağıllı informasiya sistemlərinin (İMS) inkişafının əsas metodları və müvafiq problem sahələrinin xüsusiyyətləri ; tətbiq olunan İMS-in quruluşunu tərtib etmək; İMS dizaynının əsas vasitələri ilə işləmək; İdarəetmə problemlərinin həlli üçün yeni koqnitiv informasiya texnologiyadan istifadə etməklə tətbiq olunan İMS-in funksional quruluşu; Avtomatlaşdırılmış ağıllı informasiya sistemlərinin (AİS) və qərar dəstəyi sistemlərinin inkişafında bilik və heuristika ilə təmsil və emal üçün ağıllı texnologiyalar və modellərdən istifadə etmək haqqında danışılır.

Göstərilir ki, bununla əlaqədar olaraq, iqtisadiyyat sahəsində informasiya texnologiyalarının və məlumatlandırmanın inkişafının hazırkı mərhələsində vacib problemlər bunlardır: - "yumşaq hesablama" əsasında sahibkarlığın müxtəlif sahələrində qərarlar dəstəyi sistemlərinin adekvat modellərinin işlənilib hazırlanması: qeyri-səlis məntiq (Qeyri-səlis məntiq), sinir şəbəkələri, təkamül proqramı və genetik alqoritmlər, məlumatların yaradılması, öyrənmə alqoritmləri, qeyri-müəyyənlik qarşısında proqnozlaşdırma.

Mövzu №3

Kompüter elmlərinin müasir tətbiq sahələrinin problemləri. Hərbi informatika, fizikiinformatika və bioinformatikanın problemləri.

Qısa icmal. Mövzuda kompüter elmlərinin müasir tətbiq sahələrinin problemlərindən danışılır, hərbi, fiziki informatika və bioinformatikanın müasir problemləri izah olunur. Hərbi sferada informasiya texnologiyaları, şəbəkə texnologiyaları: hərbi sferada robotlaşdırılmış vasitələr, pilotsuz uçuş aparatları və onların proqram təminatı haqda informasiya verilir.

Qeyd edilir ki, Fizika və İnformasiya nəzəriyyəsi bir-birinə qarşılıqlı təsir etməklə iki sintetik sahənin – Tətbiqi informasiya nəzəriyyəsinin və informasiya fizikasının yaranmasına səbəb olur. İnformatikanın inkişafında fizika və informasiya nəzəriyyəsinin bir-biri ilə birləşməsi yeni sintetik bir sahəni- fiziki informatikanı meydana gətirmişdir.

Sonda DNT kodunun nəzarətinə əsaslanan yeni istiqamət olan Sintetik biologiya, - kodun yeni xüsusiyyətlərini təyin edərək, yeni və ya təkmilləşdirilmiş bioloji orqanizmlər və toxumalar yarada bilən bioloji sistemlərin proqramlaşdırılmasından danışılır.

Mövzu №4

Optimallaşdırmanın tətbiqi problemləri. Viki mühitdə informasiya təsirinin intellektual analizi sistemləri

Qısa icmal. Mövzuda modelləşdirmənin, optimallaşdırmanın və tətbiqetmənin problemlərindən bəhs olunur. Viki texnologiyalar, viki mühit, viki səhifələr, İnformasiya təsirinin İntellektual analiz sistemləri, onların strukturu, verilənlərin analitik emalı sistemi (*OLAP*), verilənlərin intellektual analizi sistemi (*Data Mining*) və verilənlərin təsviri sistemi haqqında informasiya verilir.

Mövzu №5

Paralel və Paylanmış proqramlaşdırma, qrid texnologiyalar, qrafiki proessorlarda proqramlaşdırma problemləri

Qısa icmal. Mövzuda elmin müxtəlif sahələrində meydana çıxan Qrid texnologiyaları əsasında paylanmış hesablama sistemlərinin arxitektur-texnoloji prinsiplərinin işlənməsi hesablama və yaddaş resursları tələb edən mürəkkəb məsələlərin həllində paralel və paylanmış

proqramlaşdırma texnologiyasından istifadə məsələləri analiz olunur. Paralel proqramlaşdırma zamanı istifadə olunan alqoritmlər və platformalar haqqında geniş məlumat verilir. Qrid texnologiyaları, Qrid sistemlər, Qrid hesablamalar, Klaster texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması, Qrid texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması, Bulud texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması, arxitektur-texnoloji prinsiplərinin işlənməsi haqda məlumat verilir.

Mövzu №6

Verilənlər elminin (Data Science) problemləri

Qısa icmal. Verilənlər elmi (Data Science) informasiyanın alınması üsullarına sahib olmaqdır. [Verilənlər](#) elmi ənənəvi informatikadan başlayaraq riyaziyyata qədər müxtəlif sahələr üzrə bacarıq və vərdiş tələb edir. Bu elmin əsas məqsədi verilənlərdə qanunauyğunluqların tapılması, verilənlərdən ümumiləşdirilmiş halda biliklərin aşkarlanmasıdır. Bu sahədə vacib olan bacarıqlar adətən, mütəxəssisə lazım olan ümumi fənlərlə informasiya texnologiyalarındakı təcrübələrin və riyazi statistika biliklərinin kəsişməsi – [Venn diaqramı](#) vasitəsilə izah olunur. Verilənlərin müasir emal metodları “[data scientist](#)” adlanan kadrların hazırlanmasına marağı stimullaşdırır.

Mövzu №7

“Big Data” texnologiyaları və informasiya təhlükəsizliyi problemləri

Qısa icmalı. *Böyük verilənləri* (ing. Big data) bəzən mineral resurslarla – böyük filiz mədəni (largeore), yeni neft (new oil) , gizli biliklərin mənbəyi kimi “data mining”, təbiət kataklizmləri (data tornado, data deluge), təbii fəlakət (sunami) və s. ilə müqayisə edirlər. Bəzən bu problemi Mur qanunu kimi də interpretasiya edirlər. Bu termin o verilənlər toplusuna aid edilir ki, onun həcminə informasiyanın daxil edilməsi, saxlanması, idarə edilməsi və analizi üçün tipik verilənlər bazasının imkanları çatmır. Böyük verilənlər dedikdə “həcmi mövcud üsul və sistemlərin imkanlarını ötüb keçən verilənlər” təsəvvür edilir. “Böyük” məfhumu mövcud hesablama səviyyəsinə görə nisbidir. S. Madden “böyük verilənlər”i “çox böyük”, “çox sürətli”, “cox çətin” kimi təsvir edir. Burada “çox çətin” ifadəsi mövcud alətlərlə emal oluna bilməyən verilənlərə aiddir. “Big data”

idarəçilik, səhiyyə, elm, biznes və kommersiya, sənaye və digər sahələrdə inqilabi dəyişikliklər edə biləcək bir texnologiyadır. Bu texnologiya bir tərəfdən cəmiyyət üçün yeni imkanlar açır, digər tərəfdən isə yeni təhlükəsizlik problemləri yaradır .

Mövzu №8

Bulud texnologiyaları və təhlükəsizlik problemləri

Qısa icmal: Mövzuda bulud texnologiyalarının mahiyyəti, inkişaf mərhələləri, Bulud xidmətlərinin təsnifatı, formaları şərh olunur. Bulud texnologiyalarının inkişaf tempi ilə bağlı statistika və proqnozlar analiz edilir. Müvafiq texnologiyaların iqtisadi cəhətdən üstünlükləri və çatışmazlıqları, hüquqi tənzimləmə problemləri araşdırılır. Göstərilir ki, bu texnologiyaların xüsusiyyətləri sırasına istifadəçilərin bulud servislərlə sərbəst işləmək bacarığının olması, buluda girişin istənilən məkandan, istənilən vaxt, istənilən qurğu (smartfon, noutbuk, planşet, laptop və s.) vasitəsilə mümkünlüyüdür. Lakin bu texnologiyaların təhlükəsizlik səviyyəsinin olduqca zəif olması onun geniş tətbiqinə böyük maneə yaradır. Bu səbəbdən bulud texnologiyalarının təhlükəsizlik problemlərinin müəyyənləşdirilməsi, onlara qarşı mübarizə üsullarının işlənməsi hazırda ən aktual məsələlərdən biridir.

Mövzu №9

Riyazi modelləşdirmənin və Hesablama riyaziyyatının müasir problemləri

Qısa icmal: Mövzuda Kompüter elmlərinin və tətbiqi riyaziyyatın aktual həll olunmayan məsələləri və hesablama elmi haqda danışılır. Kompüter elmləri məntiq, cəbrə, qraflar nəzəriyyəsinə və kombinatorikaya əsaslandığından bu haqda tələbələrə informasiya verilir.

Riyazi modelləşdirmənin Ekoloji problemlərin həllində, təbii fəlakətlərin tədqiqində rolundan, Kainat haqqında elmlərdə və təbiət elmlərində, tibbdə Kompyuter elmlərinin aktual problemlərindən, İdentifikasiya nəzəriyyəsinə, Hesablama Riyaziyyatının və alqoritmlər nəzəriyyəsinin çətin həll olunan məsələlərin həllinə tətbiqindən, çevik və dəyişən mühitdə işləyən, mümkün həlli tapmağa çalışan və çox yaxşı qərarlar qəbul edən Təbiət əsaslı alqoritmlərdən bəhs edilir.

Mövzu №10

İnformasiya texnologiyalarının korpus linqvistikasında tətbiqi. Kompüter tərcüməsinin problemləri. Obrazların tanınması. Mətn tipli informasiyaların analizi və modelləri

Qısa icmal. Mövzuda elektron tərcümə və lüğətlər, linqvistik verilənlər, linqvistikada hipermətn texnologiyalar, linqvistin Avtomatlaşdırılmış İş Yerləri, korpus linqvistikası, informatikanın aktual problemlərindən olan koqnitiv modelləşdirmə; intellektual interfeyslər; nitqin tanınması və sintezi; deduktiv modellər, çoxagentli sistemlər; ontologiyalar; biliklər menecmenti; yumşaq hesablamalar, mətn sənədlərinin avtomatlaşdırılmış məzmunca intellektual emalının təminatı nəzəriyyəsi, e-fondların yaradılması və informasiya-axtarış sistemlərinin effektivliyinin artırılmasından danışılır. Göstərilir ki, biliklərin əldə edilməsi və çıxarılması üçün istifadə edilən mövcud axtarış sistemlərinin effektivliyi, daha çox birbaşa analiz üsullarından asılıdır.

Mövzu №11

Sinergetik İdarəetmə sistemləri. Təkamül hesablamalar . Genetik alqoritmlərin problemləri

Qısa icmal. Mövzuda elmi tədqiqatların kəsişdiyi sahə olan Sinergetika haqda məlumat verilərək göstərilir ki, Sinergetika —özünütəşkil əsasında təbiətin və ətraf mühitin vəziyyətini öyrənir. Özünütəşkil, təbiətin strukturlarının meydana gəlməsi, dayanıqlığı və məhv olması prosesini öyrənir. Bu zaman Sinergetik sistemlərdə informasiya axınlarının və informasiyanın entropiyasının müəyyən edilməsi lazım gəlir. Sonra Təkamül hesablamalar və Xaos nəzəriyyəsi haqda informasiyalar verilir. Daha sonra kompüter elmlərinin təbiət elmlərindən (biologiya) öyrəndiyi və öz problemlərini həll etmək üçün istifadə etdiyi üsul olan Genetik Alqoritmlər, bu alqoritmlərin əsas strategiya və prinsipləri, genetik alqoritmlər operatorlarının bir neçə modelləri, müxtəlif optimallaşdırma məsələlərində genetik alqoritmlərin üstünlükləri və çatışmazlıqları şərh olunur, genetik alqoritmlərin tətbiqinə aid misallar göstərilir.

Krossover, Genetik proqramlaşdırma, Evristik kombinə olunmuş metod, Genetik metodların tətbiqinə aid nümunələr: klasterləşdirmə; təsnifatlandırma; paylanmış hesablamalar; neyron şəbəkələr; qarışqa alqoritmləri; diferensial təkamül alqoritmləri; arı alqoritmləri; particle swarm optimization (“sürü” intellekti əsasında optimallaşma) alqoritmləri haqda danışılır. İnformasiya texnologiyaları sahəsində optimallaşdırma

məsələlərinin həlli, neyron şəbəkələr, intellektual sistemlərin yaradılması, elm, texnika, tədris, biznes və iqtisadiyyatda yeni İT-nın tətbiqi ilə məşğul olan mütəxəssislərin bu cür alqoritmlərdən istifadənin zəruriliyi göstərilir.

Mövzu №12

Süni intellektlərlə bağlı problemlər. Robototexnika, Nano və pikotexnologiyalar. Soft computing nəzəriyyəsi. Neyrokompüterlər. Neyroşəbəkələr

Qısa icmal. Mövzuda Süni intellektlər, ekspert sistemlər, biliklər bazası, robototexnika haqda məlumat verilir. İnsan kimi düşünən, İnsan məntiqi ilə işləyən və insan kimi qərar qəbul edə bilən texniki sistemlərin yaradılması sahəsində aparılan elmi araşdırmalar sistemi olaraq nəzərdə tutulan Süni intellektlər informatika, psixologiya, fəlsəfə, linqvistika, iqtisadiyyat, optimallaşdırma, məntiq nəzəriyyəsi və bir sıra başqa sahələrə əsaslanan tədqiqat sahəsi olmaqla, kompüter elmlərinin xüsusi bölməsi hesab edilir. Müasir kompüterlərin element bazaları , Nano və Pikotexnologiyalar, Soft computing-in əsas məsələsi. Neyrokompüterlər. Neyroşəbəkələr, Paylanmış intellektual idarəetmə sistemlərində texnoloji proseslərin intellektual tənzimləmə sistemləri onların tətbiqləri haqda informasiyalar verilir.

Mövzu №13

Kompüter biotibbinin problemləri. Biotibbi texnologiya mühəndisliyi. Elektron tibbin problemləri

Qısa icmal: Mövzuda elektron tibbin mahiyyəti, imkanları, formalaşması, teletibbin inkişaf istiqamətləri və problemlərinin analizindən danışılır, e- tibbin elmi-nəzəri problemləri şərh edilir, həkim qərarlarının qəbul olunması üçün tibbi ekspert sistemlərinin işlənilməsi, fərdi tibbi məlumatların informasiya təhlükəsizliyi və tibbdə Big Data problemlərinə baxılır, əşyaların İnterneti və sosial medianın elektron tibbdə yaratdığı imkanlar nəzərdən keçirilir. Biotibbi texnologiya mühəndisliyi haqda danışılarkən qeyd edilir ki, bu mütəxəssislər biologiya, informatika, biofizika, diaqnoz qoymanın tibbi metodları, kompüter texnologiyaları, fizika, kompüter və mühəndis qrafikası, İT, biomateriallar və s. kimi sahələri öyrənir, yeni biotibbi aparatları (kompüter tomoqrafiyası) istehsalə yeni ixtiralar üçün tətbiq etməyi bilirlər.

Mövzu №14

Superkompüter texnologiyaları. Superkompüterlərin hesblama məhsuldarlığı

Qısa icmal: Mürəkkəb hesablamalar və böyük həcmli yaddaş tələb edən məlumatları daha sürətlə emal edib, istifadəçilərə çatdırmaq üçün yüksək hesablama məhsuldarlığına və böyük yaddaşa malik olan superkompüterlərdən elmin müxtəlif sahələrində: fiziki-kimyəvi proseslərin, nüvə reaksiyalarının, qlobal atmosfer proseslərinin real zaman kəsiyində modelləşdirilməsində, kriptografiyada, geologiyada, yeni dərman növlərinin yaradılmasında və s. meydana çıxan böyük hesablama və yaddaş resursları tələb edən mürəkkəb məsələlərin həllində geniş istifadə olunur. Superkompüterlər paralel hesablama sistemləri əsasında yaradılır. Buna görə də superkompüterlərlə bağlı problemlər Kompüter elmlərinin həlli vacib olan məsələlər sinfinə aid edilir.

Mövzu 15.

Kriptografiya elminin problemləri. Kibermühit və Kibercinayətkarlıq. Kodlaşdırma və verilənlərin sıxılması

Qısa icmal. Mövzuda əvvəlcə kibercinayətkarlıq və kriptografiya haqda, sonra isə İnformasiyanın miqdarı. İnformasiya entropiyası. İnformasiyanın kodlaşdırılması. Şennon teoremi. Mətn sənədlər üçün kodlar. Zaman kodları. Verilənlərin sıxılması. Sıxma üsulları və verilənlərin formatı. MPEG formatı. Veyvletlər. Veyvlet çevirmələr haqda danışılır.

Göstərilir ki, Kriptografiya kriptologiya elminin hissələrindən biridir. Kriptologiya elminin digər hissəsi kriptotəhlil (və ya kriptozanaliz) ilə məşğul olur. XX əsrin 70-ci illərinə kimi elmin bu sahəsi şifrələmə üsullarının zəif və güclü tərəflərini, şifrələrin sındırılması üsullarını öyrənirdi. İndiki zamanda kriptotəhlil kriptografik sistemin müdafiəsi ilə məşğul olan elm sahəsi hesab olunur. Kriptografik alqoritmlər riyazi əsasla söykənərək qurulurlar. Bu sahə informasiya təhlükəsizliyinin pozulma üsullarının axtarılması ilə məşğul olur və cari sistemin informasiya təhlükəsizliyini təmin edir. Beləliklə, kriptotəhlil şifrələnmiş mətnin açarsız oxunma üsullarını, e- rəqəmsal imzanın saxtalaşdırılma üsullarını öyrənir. Kriptografiya və kriptozanaliz güclü elm sahələri olsada, bir-birinin əksinə yönəlmiş məqsədə qulluq edirlər.

Әдәбиyyат:

1. Авдошин, С. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. Авдошин. - Москва: **СИНТЕГ**, 2016. - **260** с.
2. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2019. - 376 с.
3. Гасумова С. Е. Социальная информатика. Учебник и практикум для вузов. М.: Юрайт, 2019. 284 с.
4. Гилярова М. Г. Информатика для медицинских колледжей. Учебник. М.: Феникс, 2018. 528 с.
5. Грошев А. С., Замятов П. В. Информатика. Учебник. М.: ДМК Пресс, 2019. 674 с.
6. Далингер В. А., Симонженков С. Д. Информатика и математика. Решение уравнений и оптимизация в Mathcad и Maple. Учебник и практикум для вузов. М.: Юрайт, 2019. 156 с.
7. Информатика для экономистов. Учебник для СПО / ред. Поляков В. П. М.: Юрайт, 2019. 524 с.
8. Набиуллина С.Н. Информатика и ИКТ. Курс лекций. М.: Лань, 2019. 72 с.
9. Новожилов О. П. Информатика. Учебник. М.: Юрайт, 2014. 620 с.
10. Попов А. М., Сотников В. Н., Нагаева Е. И. Информатика и математика для юристов. Учебник / ред. Попов А. М. М.: Юрайт, 2014. 512 с.
11. Правовая информатика. Учебник и практикум / ред. Элькин В. Д. М.: Юрайт, 2014. 402 с.
12. Софронова Н. В., Бельчусов А. А. Теория и методика обучения информатике. Учебное пособие. М.: Юрайт, 2020. 402 с.
13. Трофимов В. В. Информатика. Учебник для академического бакалавриата. В 2-х томах. Том 2. М.: Юрайт, 2019. 406 с.
14. Филимонова Е. В. Информатика и информационные технологии в профессиональной деятельности. Учебник. М.: Юстиция, 2019. 216 с.
15. Хлебников А. А. Информатика. Учебник. М.: Феникс, 2017. 448 с.
16. Цапкина Е. П., Царегородцев А. В. Информатика и методы математического анализа. Учебно-методическое пособие. В 2 частях. Часть 1. Информатика. М.: Проспект, 2019. 96 с.

17. Шмелева А. Г., Ладынин А. И. Информатика. Информационные технологии в профессиональной деятельности: Microsoft Word. Microsoft Excel: теория и применение для решения профессиональных задач. М.: ЛЕНАНД, 2020. 304 с.
18. Самые мощные суперкомпьютеры мира 2018 [Электронный ресурс]. Режим доступа [//http://economtermin.ru/it-biznes/243-samye-moshhnye-superkompjutyery-mira-2018.html](http://economtermin.ru/it-biznes/243-samye-moshhnye-superkompjutyery-mira-2018.html)
19. Генетические алгоритмы, Гладков Л.А., Курейчик В.В., Курейчик В.М., 2016