Ўзбекистон Республикаси Олий ва Ўрта махсус таълим вазирлиги,
Тошкент кимё-технология институти

КИМЁ, НЕФТ-ГАЗНИ ҚАЙТА ИШЛАШ ХАМДА ОЗИҚ-ОВҚАТ САНОАТЛАРИ ИННОВАЦИОН ТЕХНОЛОГИЯЛАРИНИ ДОЛЗАРБ МУАММОЛАРИ

Республика илмий-техника анжуманининг мақолалар тўплами

2015 йил 18-19 ноябрь

Тошкент -2015

УДК 62:66+37(08)

Ушбу тўпламда «Кимё, нефт-газни қайта ишлаш хамда озиқ-овқат саноатлари инновацион технологияларини долзарб муаммолари» Республика илмий техникавий анжуманининг мақолалар матнлари ўрин олган. Тўпламда олий таълим муассасалари, илмий-текшириш институтлари хамда саноатни ишлаб чиқариш корҳоналари инновацион гурухларини кимё, нефть ва газни қайта ишлаш хамда озиқ-овқат саноатлари муаммоларига бағишланган илмий изланишларининг натижалари келтирилган. Муаллифлар мақолалар мазмунига жавобгардирлар.

Сборник составлен на основе материалов, представленных на Республиканскую научно-техническую конференцию **“**Актуальные проблемы инновационных технологий химической, нефте-газовой и пищевой промышленности”.
В сборнике нашли отражение результаты изысканий инновационных групп высших учебных заведений, научно-исследовательских институтов, а также предприятий отраслей экономики, направленных на решение проблем химической, нефтегазоперерабатывающей и пищевой промышленности. Авторы статей несут ответственность за их содержание.

ОБРАЗОВАНИИ, ЭКОНОМИКА И МЕНЕЖМЕНТ

120. **Муминов[1]Н.Ш., Гайратов [2]О.Г.**
Стандартизации и сертификации, техническое регулирования в качестве механизма совершенствования производственного потенциала предприятий пищевой и перерабатывающей промышленности, в обеспечении качества и безопасности, а также экспортоорентированности Республики Узбекистан

(ТХТИ) **255**

121. **Абдуллаева Ш.Ш., Алимджанова Д.И., Ахмедова А.А.**
Развитие познавательных и профессиональных творческих способностей студентов как условие подготовки высококвалифицированных специалистов (ТХТИ, Ташкентский архитектурно-строительный институт) **260**

122. **Абдурашидов А.А. Ганиева У.Ф.**
Инновации в образовании, менеджменте и экономике (ТХТИ) **262**

123. **Абдусатторова Д.Б.**
Хўжаликюритувчисубъектларфаолиятидасоликменежментиниташкилэтишнинг

ҳозиргидаврйўналишлари (ТДИУ) **264**

124. **Абдусатторова Д.Б.**
Солиқларни режалаштириш: амалиёт, таҳлил ва мулоҳаза (ТДИУ) **267**

125. **Alavutdinova N.G'**
O'zbek tili o'qitishning umumdidaktik va o'ziga xos prinsiplari (TKTI) **269**

126. **Гайратов [1]О.Г., Муминов [2]Н.Ш., Гайратов [3]О.Г.**
Особенности и схемы внедрения систем энергоменеджмента качества на предприятиях энергетического комплекса на основе опыта ведущих

энергетических компании (ТХТИ) **271**

127. **Ганиева.У**
Методология и методы педагогических исследований (ТХТИ) **274**

128. **Джураева Г.**
Приёмы и подходы обучению иностранному языку при помощи использования

информационных педагогических технологий (ТХТИ). **276**

129. **ЕлинаН.П., Садыков Х.С.**
Инновации в образовании на примере (ТХТИ) **278** 134. .**Захидов И.Г., Джуманиязова М.Р.**

Некоторые виды инновационной технологии в процессе обучения

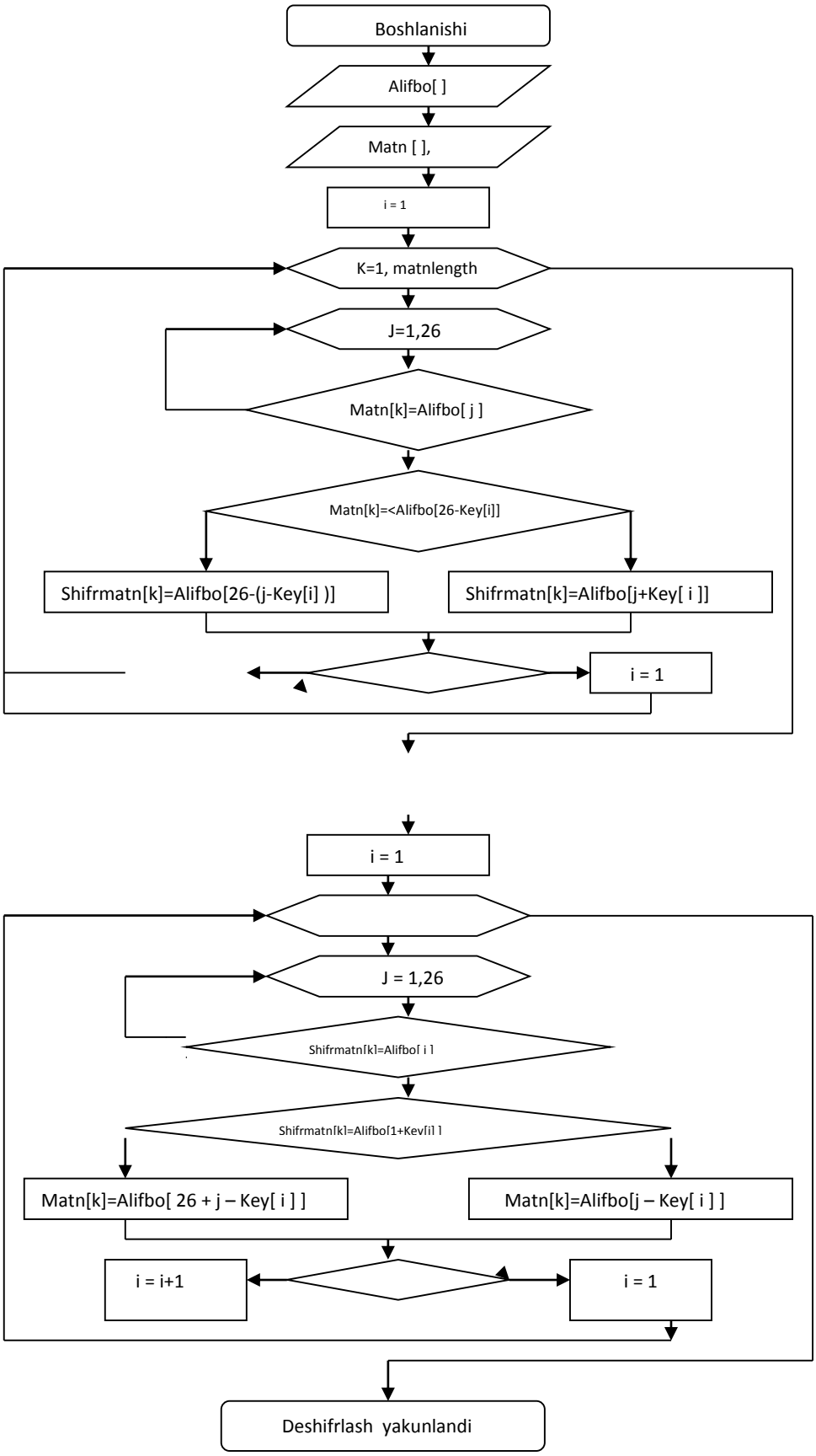
иностранного языка в техническом вузе (ТХТИ) **280**

135. **Imamov N.K. Yakubova N.S.**
Kriptografiyadaqo'llaniladiganusulto'g'risida (TKTI) **282**

KRIPTOGRAFIYADA QO'LLANILADIGAN USUL TO'G'RISIDA

Imamov N.K. Yakubova N.S.
Toshkent kimyo-texnologiya instituti

Gronsfild usuli algoritmining blok-sxema ko'rinishidagi ifodasini keltiramiz: Gronsfildusulida kalit Tsezar usulidagidek bir xonali son emas , balki bir nechta xonali sondan iborat bo'lishi mumkin. Matndan iborat ma'lumotni shifrlash uchun algoritm Tsezar usuliga o'xshash xolda tuziladi, faqat axborotdagi xarfni alifbo bo'yicha uchinchi xarf (Tsezarg' usuli) bilan almashtirmasdan, kalit raqamlariga mos keladigan matn xarflari alifbo buyicha mos raqamlarga o'ng tomonga siljitiladi . Misol uchun, kalit sifatida **e** sonining birinchi to'rtta raqamlarini olsak, ya'ni 2718, u xolda **matematika** so'zidan iborat axborot uchun quyidagi shifrmatn xosil bo'ladi.


Boshlanishi
Alifbo[ ]
Matn [ ],
i = 1
K=1, matnlength
J=1,26
Matn[k]=Alifbo[j]
Matn[k]=<Alifbo[26-Key[i]]
Shifrmatn[k]=Alifbo[26-(j-Key[i])]
Shifrmatn[k]=Alifbo[j+Key[i]]
i = 1
i = 1
J = 1,26
Shifrmatn[k]=Alifbo[i]
Shifrmatn[k]=Alifbo[1+Kev[i]]
Matn[k]=Alifbo[26 + j – Key[i]]
Matn[k]=Alifbo[j – Key[i]]
i = i+1
i = 1
Deshifrlash yakunlandi

Axborot	m	a	t	e	m	a	t	i	k	a
Kalit	2	7	1	8	2	7	1	8	2	7
shifrmatn	o	h	u	m	o	h	u	q	m	h

Misol tariqasida quidagi ma'lumotni to'ldirib shifrmatn tuzish mumkin: **Familiya+Ism+Otaismi+tugilganyilsanasi+yashashmanzili**

Vazifani bajarish uchun malumot bir o'lchamli massivga yoziladi va boshqa bir o'lchamli massivga lotin alifbosi yoziladi. Matn yozilgan massivning xar bir elementini alifbo yozilgan massiv elementlari bilan solishtiriladi. Elementlar bir xil bo'lganda matn yozilgan massivning mos elementi Gronsfild usuligabinoanalifbo bo'yicha o'ng tomonga siljitiladi va shifrmatn xosil qilinadi. So'ngra shifrmatnga deshifrlash amali qo'llaniladi, ya'niamallarteskaritartibdabajariladi.

Bu usulda matn shifrlanishining murakkablik darajasini oshirish maqsadida avval matn ikki o'lchamli matritsaga elementlari sifatida kiritiladi, matritsa transponirlanadi va elementlari bir o'lchamli matritsaga yoziladi. So'ngra bir o'lchamli matritsa elementlariga Gronsfild usuli qo'llaniladi. Bunda kalit Tsezar usulidagidek bir xonali son emas, balki bir nechta xonali sondan iborat bo'lishi mumkin. Matndan iborat ma'lumotni shifrlash uchun algoritm Tsezar usuliga o'xshash xolda tuziladi, faqat axborotdagi xarfni alifbo bo'yicha uchinchi xarf (Tsezar usuli) bilan almashtirmasdan, kalitni raqamlariga mos keladigan matn xarflari alifbo bo'yicha mos raqamlarga o'ng tomonga siljitiladi.

Bu usulni kombinatsiyalashtirilgan Gronsfild usuli deb atadik va usulni amalda qo'llash uchun quyidagi algoritm taqdim etiladi:

1- bosqich.

1.Berilgan axborotni A(**n** x **m)** ikki**o'**lchamli matritsaga elementlari sifatida kiriting.

Matritsaning **n** va **m** o'lchamlari kiritilayotgan axborot xajmiga qarab aniqlanadi.

2. A(**n** x **m)** matritsani ekranga ikkio'lchamli matritsa ko'rinishida chiqaring.

3. A(**n** x **m)** matritsa qatorlarini ustunlari bilan almashtiring (transponirlang) va B(**m** x **n**) matritsa nixosilqiling.

4. B(**m** x **n**) matritsani ekrangaikkio'lchamlimatritsako'rinishidachiqaring.

2-bosqich.

1. B(**m** x **n**) matritsa elementlarini ekranga bir qator ko'rinishida chiqaring va xosil bo'lgan axborotdan **m*n** elementlardan iborat bir o'lchamli matritsa M (**m*n)** ni tashkil eting. 2. Biro'lchamli**S**matritsagaelementlarisifatidalotinalifbosixarflarinitartibibilankiriting.

3.M(**m*n**) matritsa elementlarini xar birini **S** matritsaning barcha elementlari bilan solishtiring. Birxil elementlar chiqsa, M(**m*n**) matritsaning shu elementiga Gronsfild usulini qo'llab shifrogramma xosil qiling va natijani bir o'lchamli N(**m*n)** matritsaga yozing va ekranga chiqaring.

3-bosqich.

1. Qayta shifrlash amalini bajarish uchun N (**m*n**) matritsa elementlariga Gronsfild usulini teskari tartibda qo'llang va natijani L (**m*n**) bir o'lchamli matritsaga yozing.

2. M1(**m** x **n**) ikkio'lchamli matritsani biro'lchamli L (**m*n**) matritsa elementlari bilan to'ldiring. M1(**m** x **n**) matritsa ustunlarini qatorlari bilan almashtiring, natijaniA1(**n** x **m)** matritsaga yozing va A(**n** x **m)** matritsa bilan solishtiring.

Keltirilgan algoritm asosida Java dasturlash tilida dastur kodi tuzildi va algoritm natija berishi tasdiqlandi. Ushbu algoritmdan "Axborot xavfsizligi" va "Kriptografiya" soxalarini o'rganuvchi talabalar gao'quvmash g'ulotlarida foydalanish tavsiya etiladi.