Boshqacha aytganda RSA algoritmida xabar ochiq kalit bilan shifrlansa va shaxsiy kalit bilan deshifrlansa, $M = C^d \bmod N = M^{ed} \bmod N$ tenglik to'g'riligini isbotlash zarur.

Eyler teoremasi. Agar $x$ haqiqiqatdan $n$ bilan o'zaro tub bo'lsa, $^{(n)} = 1 \bmod n$ bo'ladi. Bu yerda, $(n)$ – funksiya, $n$ dan kichik va u bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsatadi. Agar $n$ soni tub bo'lsa, $(n) = n - 1$ bo'ladi. Shuning uchun $ed = 1 \bmod (N) = 1 \bmod (p-1)(q-1)$ tenglik kabi yozish mumkin. Mazkur tenglikning to'liq shakli aslida $ed = 1 \bmod (N) + k\ (N)$ ga teng. Ya'ni, $ed$ ko'paytmani $(N)$ ga bo'lganda $k$ tadan tegib, bir qoldiq qolgan. Shuning uchun ushbu tenglikni quyidagicha yozish mumkin:

$$ed - 1 = k\ \varphi(N).$$

Ushbu tengliklardan, RSA algoritmining to'g'ri ishlashini tasdiqlash mumkin:

$$C^d = M^{ed} = M^{(ed^{-1})+1} = M * M^{ed^{-1}} = M * M^{k\,\varphi(N)} = M * 1^k = M \bmod N.$$

Aytaylik, RSA algoritmida ma'lumotni shifrlash va deshifrlash amallarini tanlab olingan ($p = 11$ va $q = 3$) "katta" sonlar ustida amalga oshirish talab qilinsin. Mazkur holda modul $N = p * q = 33$ ga teng bo'ladi va $(N) = (p-1)(q-1) = 20$ ga teng bo'ladi. U holda shifrlash uchun zarur bo'lgan daraja e ni ($e = 3$) ga teng deb olish mumkin. Sababi, 3 soni $(N) = 20$ bilan o'zaro tubdir. Shundan so'ng, Evklidning kengaytirilgan algoritmi asosida deshifrlash kaliti ( = 7 ) aniqlanadi. Ya'ni, $ed = 3 * 7 = 1 \bmod 20$. U holda A tomonning ochiq kalit jufti $(N, e) = (33,3)$ va shaxsiy kaliti esa $d = 7$ ga teng.

Shundan so'ng, A tomon o'zining ochiq kalitini barchaga uzatadi. Biroq, shaxsiy kalitini maxfiy saqlaydi.

Faraz qilaylik, B tomon A tomonga $M = 15$ ma'lumotni shifrlab yubormoqchi. Buning uchun B tomon A tomonning ochiq kaliti juftini $(N, e) = (33,3)$ oladi va shifrmatnni quyidagicha hisoblaydi:

$$C = M^e \bmod N = 15^3 = 3375 = 9 \bmod 33$$

va uni A tomonga yuboradi.

A tomon $C = 9$ shifrmatnni deshifrlash uchun shaxsiy kalit $d = 7$ dan foydalanadi:

$M = C^d \bmod N = 97 = 4782969 = 144938 * 33 + 15 = 15 \bmod 33$

Agar RSA algoritmida kichik tub sonlardan ($p$ va $q$ uchun) foydalanilgan taqdirda, hujumchi ochik bo'lgan $N$ ni osonlik bilan ikkita tub sonning ko'paytmasi ko'rinishida yozishi mumkin. Shundan so'ng, ochiq kalitning ikkinchi qism $ee$ dan foydalangan holda, shaxsiy kalit $d$ ni hisoblay oladi. Shuning uchun RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida 2048 bit bo'lishi talab etiladi. Bundan tashqari, RSA algoritmini buzish faqat faktorlash muammosiga bog'liqligi isbotlanmagan. Boshqacha aytganda, RSA algoritmini buzishning faktorlash muammosini yechishdan tashqari biror usuli aniqlanmagan.

Xulosa qilib aytadigan bo'lsak, qishloq xo'jalik mahsulotlarnisamarali logistikasini ishlab chiqish uchun eksport qilishning yo'lga qo'yish lozim. Fermer va fermer xo'jaliklariga kengroq ko'lamda imkoniyatlar berilishi kerak. Transport va yetkazib berish yo'llarini oson va qulay usullarda tashkil etish lozim.

**Foydalanilgan adabiyotlar**

1. Аникин Б.А. Логистика: Учеб.пособие. М.: Инфра М. 2000 г.
2. Миротин Л.Б., Сергеев В.И. Основи логистики. Учебное пособие. Москва, "Инфра-М", 1999 г.

## MA'LUMOTLAR BAZALARINING – BIZNESNI TASHIL ETISH VA SAMARADORLIGINI OSHIRISHDAGI ROLI

***Abdukarimov Abdumanap***
*O'zbekiston Milliy universiteti Jizzax filiali dotsenti, texnika fanlari nomzodi*
***Rashidov Abror Ro'zimurod o'g'li***
*O'zbekiston Milliy universiteti Jizzax filiali stajyor-tadqiqotchisi*

**Annotatsiya:** *Hozirgi vaqtda katta hajmdagi ma'lumotlar bilan ishlaydigan kompaniyalar ma'lumotlarni uzatish, qayta ishlash va tahlil qilish uchun ko'plab vositalarni faol ravishda ishlab chiqmoqdalar va takomillashtirishmoqdalar. Ushbu maqolada ko'chmas mulk ob'ektlarini oldi – sottisida e'tiborga olish kerak bo'lgan atributlarni ilmiy nuqtai nazardan tanlash metodikasi ishlab chiqish zarurligi ta'kidlanadi. Bu atributlardan iborat berilganlar bazasi bo'yicha yaxshi ma'lumotlarga ega bo'lish ko'chmas mulk biznesini samarali tashkil etishda asosiy informatsiya bo'lib xizmat qiladi*.

**Kalit so'zlar:** *ma'lumotlar bazalari, biznes analitikasi, biznesni rivojlantirish strategiyalari, axborot texnologiyalari, ma'lumotlarni tahlil qilish*.

## Biznesni rivojlantirishda ma'lumotlar bazalarining roli

Ma'lumotlar bazalari o'nlab yillar davomida zamonaviy firmalarning biznes jarayonlarida asosiy rol o'ynab kelmoqda. Kompaniyalar o'z mahsulot va xizmatlarini elektron ko'rinishda taqdim etishlaridan qat'i nazar, ma'lumotlar bazasidan foydalanadilar yoki oflayn rejimda ishlaydilar. Ma'lumotlar bazasida har xil turdagi ob'ektlar (nomlar), hodisalar (operatsiyalar), odamlar (xodimlar) va joylashuvlar haqidagi ma'lumotlar mavjud [2].

So'nggi bir necha o'n yilliklarda ma'lumotlar bazalarining ahamiyati ortib bordi, chunki mavjud ma'lumotlar miqdori hisoblash texnikasi ixtiro qilinganidan beri juda katta sur'atlarda o'sdi. Lekin ma'lumotlar bazalarida nafaqat yangi ma'lumotlar yaratiladi va saqlanadi.

Mavjud ma'lumotlar hajmini raqamlashtirish fan va ishlab chiqarishning turli sohalarida ham, san'at, gumanitar va ijtimoiy fanlarning ko'plab sohalarida qo'llaniladi [1]. Shuning uchun katta hajmdagi ma'lumotlar bilan muvaffaqiyatli ishlash uchun ma'lumotlar bazalari bilan qanday ishlashni va ma'lumotlarga asoslangan biznes strategiyalarini qanday ishlab chiqishni bilish kerak.

## Ma'lumotlar bazasi turlari

Hozirgi vaqtda tuzilishi va maqsadiga ko'ra bir-biridan farq qiluvchi 3 xil ma'lumotlar bazalari mavjud [1].

*Relyatsion* ma'lumotlar bazalari jadvallar to'plamidan iborat bo'lib, unda ma'lumotlarni jadvallarni qayta tiklamasdan turli usullar bilan guruhlash mumkin. Bunday ma'lumotlar bazalari ma'lumotlarni qidirish va tahlil qilish ustida ishlashda juda qulaydir. Ulardan foydalanish uchun maxsus boshqaruv tizimlari ixtiro qilinadi. Ushbu turdagi ma'lumotlar bazasi bilan o'zaro ishlash uchun *Structured Query Language* **(SQL)** deb nomlangan so'rovlar va boshqaruv tili ishlab chiqilgan.

*Tarmoqli* ma'lumotlar bazalari ma'lumotlarni va ular o'rtasidagi munosabatlarni shunday saqlaydiki, ma'lumotlar bazasidagi har bir yozuv boshqa ma'lumotlar bo'laklariga havolalar tarmog'iga ega.

*Ierarxik* ma'lumotlar bazalari daraxt tuzilishiga ega bo'lib, unda har bir yozuv yana bir nechtasi bilan bog'langan. Bunday tuzilma juda vizual va mantiqiy ravishda qurilgan va tarmoq ma'lumotlar bazasiga qaraganda aniqroq va tushunarli ko'rinadi.

Ierarxik va tarmoq ma'lumotlar bazalari **SQL** so'rovlar tilidan foydalanishni talab qilmaydi. Shuning uchun ular **No-SQL** ma'lumotlar bazalari deb ataladi. Ular katta hajmdagi ma'lumotlarni to'playdigan va tahlil qiladigan kompaniyalar tomonidan faol foydalaniladi. ***Netflix*** va ***Hulu*** kabi multimedia kontent provayderlari o'z xizmatlariga bir vaqtda yuzlab million obunachilarga xizmat ko'rsatadilar, **Apache Cassandra** nomli **No-SQL** ma'lumotlar bazasidan foydalanadilar.

## Ma'lumotlar bazalari bilan ishlashda ma'lumotlar to'plamining sifatini aniqlash

Sifatli tayyorlangan ma'lumotlar to'plamlari to'liq bo'lmagan, ahamiyatsiz va tizimlashtirishga yaroqli bo'lmagan "keraksiz ma'lumotlar" mavjudligini istisno qiladi [4]. Keraksiz ma'lumotlar yetishmayotgan yoki takroriy yozuvlarni ham o'z ichiga oladi. Agar bunday past sifatli ma'lumotlar to'plami tahlil qilinsa, bunday tahlil natijasi noto'g'ri bo'ladi. Shuning uchun yuqori sifatli natijalarga erishish uchun tahlilchilar ish uchun ma'lumotlar to'plamini tayyorlashlari kerak. Tayyorgarlik jarayoni noto'g'ri, to'liq bo'lmagan yoki ziddiyatli

ma'lumotlarni tuzatish yoki olib tashlashni o'z ichiga oladi [2]. Yuqorida tavsiflangan tarzda tashkil etilgan ma'lumotlar to'plamlari bilan tahlilchilar tavsiflovchi, bashoratli ma'lumotlar yondashuvlaridan aniq natijalarni kutishlari mumkin.

**Biznesni rivojlantirishda ma'lumotlar bazalaridan foydalanish**

Kompaniyalar o'zlarining to'laqonli va aniq ma'lumotlar bazalari yaratilganligi tufayli ular o'z mijozlariga yuqori sifatli xizmat ko'rsatish va shu bilan birga xarajatlarni kamaytirish va daromadlarni oshirish uchun biznes jarayonlarini optimallashtirishga qodir.

Har qanday biznesda bunday ma'lumotlar bazalariga ega bo'lish – katta foydani kafolatlaydi.

***Amazon Prime, Apple Plus, Netflix*** kabi striming xizmatlari har kuni millionlab odamlarga ko'ngilochar video kontentini taqdim etadi. O'z ishlarida ular foydalanuvchi ma'lumotlarini keyinchalik tahlil qilish va foydani oshirish uchun jamlaydi, saqlaydi va boshqaradi. Bunday xizmatlar uchun obunaga bo'lgan qiziqishni yo'qotmaslik uchun har kuni o'z foydalanuvchilariga tegishli kontentni taqdim etish juda muhim, chunki mijozlar xizmatlar uchun oylik a'zolik to'lovi asosida to'laydilar va istalgan vaqtda obunani tugatishlari mumkin.

Banklar sifatli ma'lumotlar bazalaridan foydalanishning yana bir misolidir. Sobiq va amaldagi mijozlar bo'yicha yaxshi ma'lumotlarga ega bo'lgan banklar mijozlar tomonidan kreditlarni qaytarish ehtimolini hisoblashlari va aholining turli qatlamlari uchun kredit shartlarini hisoblashlari mumkin. Bunday prognozlarning to'g'riligi bevosita ma'lumotlarni yig'ish va tahlil qilish sifatiga bog'liq.

Ijtimoiy tarmoqlar, shuningdek, foydalanuvchilar to'g'risidagi juda ko'p ma'lumotni yig'uvchi bazalari mavjuddir. ***Facebook*** o'zaro havolalar bilan to'ldirilgan ma'lumotlar bilan ishlash uchun **MySQL** ma'lumotlar bazasidan foydalanadi. Ma'lumotlarni tahlil qilish ijtimoiy tarmoqqa foydalanuvchilarga reklama qilingan mahsulotlar, potentsial do'stlar va qiziqish guruhlari bo'yicha tegishli tavsiyalar berishga yordam beradi. Shu bilan birga, ijtimoiy tarmoq maqsadli auditoriyaga o'z mahsulot va xizmatlarini reklama qiluvchi kompaniyalarga foydalanuvchi ma'lumotlarini taqdim etadi. Sifatli ma'lumotlar to'plamiga ega ma'lumotlar bazalaridan foydalanmasdan, iste'molchi xatti-harakatlarini tahlil qilish noaniq bo'lib qoladi va daromadning yo'qolishiga olib keladi [5].

Kichik, o'rta va mikro -korxonalarda ma'lumotlar bazalaridan foydalanish holatlariga alohida e'tibor qaratish lozim. Ko'pincha, ushbu korxonalar hozirgi va sobiq mijozlar to'g'risidagi mavjud ma'lumotlarni tizimlashtirmaydi. Ko'pgina korxonalar hujjatlarning asl nusxalari va nusxalari qog'oz nusxalarda papkalarda saqlanadigan fayllarni saqlash tizimini afzal ko'rishadi. Mijozlarning ma'lumotlari bilan ishlashning bunday tizimi, ayniqsa, turizm, ta'lim va ko'chmas mulk sohalarida faoliyat yurituvchi kompaniyalar uchun xosdir. Biroq, bir necha yillar davomida asl hujjatlarni saqlash qonunlariga rioya qilish zarur bo'lsa ham, ushbu kompaniyalar ish jarayonlarini optimallashtirish uchun ma'lumotlar bazalaridan foydalanishga o'tishlari mumkin, masalan, to'g'ri ma'lumotni topish, kompaniya samaradorligini tahlil qilish va o'tgan statistik ma'lumotlarni o'rganish, foydani oshirish. Ma'lumotlar bazalaridan foydalanishni muvaffaqiyatli amalga oshirish uchun bunday kompaniyalar kerak bo'lganda arxivlarni raqamlashtirishlari va mijozlar bilan munosabatlarni boshqarish (CRM) tizimlaridan foydalanishni joriy etishlari kerak. Ushbu tizimlar mijozlar bilan o'zaro munosabatlar jarayonlarini standartlashtirish va shu bilan birga ma'lumotlarni jamlash imkonini beradi, keyinchalik ularni keyingi tahlil qilish uchun ma'lumotlar bazasiga eksport qilish mumkin. Bunday echimlardan foydalanish xodimlar sonini kamaytirishga yordam beradi, vakolatli foydalanuvchilar uchun barcha ma'lumotlarga kirishni ta'minlaydi va ofisda bo'lmasdan masofadan turib ma'lumotlarni boshqarish imkonini beradi.

Ko'chmas mulk biznesini tashkil etishda quyida keltirilgan atributlardan iborat relyatsion berilganlar bazasini yaratish maqola avtorlarini asosiy maqsadidir.

Bu berilganlar bazasini yaratisda standart berilganlar bazasini bosqarish tizimi(BBBT) SQL ACCESSdan foydalanilmoqda. Bu BBBT MS WINDOWS operatsion tizimining MS OFISE dasturlar paketida mavjud bo'lib, foydalanuvchi uchun qulaylik yaratadi.

Xulosa qilib aytadigan bo'lsak, ma'lumotlar bazalaridan foydalanish boshlanganidan beri kompaniyalar ma'lumotlar tahliliga kirishni boshladilar, bu esa samaradorlikni sezilarli darajada oshirish imkonini beradi. Ma'lumotlar bazalaridan foydalanishni amalga oshiruvchi kompaniyalar jamlangan ma'lumotlar sifatini nazorat qilishlari kerak. Yaxshi ma'lumotlar to'plamiga ega bo'lish sizga unumdorlikni oshirish uchun kerakli statistik ma'lumotlarni beradi. Ma'lumotlar bazalarining joriy etilishi ham axborot bilan ishlashga yondashuvni standartlashtiradi va uning yo'qolishining oldini oladi.

**Foydalanilgan adabiyotlar**


1. *Alfonso-Goldfarb, A. M., Waisse, S., & Ferraz, M. H. (2018). New proposals for organization of knowledge and their role in the development of databases for history of science.* Circumscribere: International Journal for the History of Science, 21, 1. doi:10.23925/1980–7651.2018v21.
2. *Baltzan, P., & Phillips, A. (2015). Business driven information systems. McGraw-Hill Higher Education.*
3. *Celko, J. (2014) Complete Guide to NoSQL. What every SQL professional needs to know about non-relational databases. Morgan Kaufmann*
4. *Schultz J., Crawford K., Richardson R. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review.*
5. *Ten ways databases run your life. (2020). Retrieved from https://www.liquidweb.com/blog/ten-ways-databases-run-your-lif*


## ТАЪЛИМНИНГ КРЕДИТ-МОДУЛЬ ТИЗИМИДА ТАЛАБАЛАРНИНГ МУСТАҚИЛ ИШЛАШИНИНГ АҲАМИЯТИ


***Акбарова Сайёра Шухратовна***

*Тошкент давлат иқтисодиёт университети таянч докторанти*



**Аннотация:** *Мақолада таълимда кредит-модуль тизимини қўллаш билан боғлиқ масалалар, яъни бу тизимда аҳамиятли бўлган мустақил ишлашнинг моҳияти, шакллари, турлари, ўрни ва вазифалари кўрсатилган ҳамда уларнинг таълим иштирокчиларида намоён бўлаётган компетентликларга таъсири ҳақида фикр юритилган.*



**Калит сўзлар:** *кредит-модуль тизими, мустақил таълим, мустақил ишлаш, мустақил иш, индивидуал-ижодий ишлаш, креатив компетенциялар*.


Ўзбекистон Республикаси Президентининг 2019 йил 8 октябрдаги фармони билан тасдиқланган “Ўзбекистон Республикаси олий таълим тизимини 2030 йилгача ривожлантириш концепция”га кўра юртимиздаги олий таълим муассасалари босқичма-босқич кредит-модул тизимига ўтмоқда [1]. Таълимнинг кредит-модуль тизимида талабаларнинг мустақил ишлашига асосий эътибор берилган. Бизга маълумки ўқув жараёни талабаларни мустақил фикр юрита олишга ўргатса, ундай таълимни ривожлантиришга асосланган ўқув-билув жараёни деб қабул қилиш мумкин. Талабаларни мустақил фикрлашга йўналтирилган махсус воситаларни қўллаб, уни фанга қизиқтириш, эркин фикрлашга ўргатиш, ривожлантириш тизими яратиш орқали уларда креатив ғояларни шакллантириш мумкин.

***Кредит-модуль тизими,*** бу — таълимни ташкил этиш жараёни бўлиб, *ўқитишнинг* модуль технологиялари жамламаси ва кредит ўлчови асосида *баҳолаш модели* ҳисобланади. Кредит-модуль тамойилида иккита асосий масалага аҳамият берилади: талабаларнинг мустақил ишлашини таъминлаш; талабалар билимини рейтинг асосида баҳолаш.