

MVC моделини амалга оширишдаги фарқлардан ташқари, фреймворклар фойдаланувчи интерфейсларини яратиш учун компонентларнинг бойлиги, функционалиги, босқичма-босқич амалга ошириш имконияти, архитектуранинг қулайлиги ва бошқа хусусиятлари билан ҳам фарқланади. Масалан, агар биз Google Material UX ёрдамида оддий бир саҳифали веб-сайт яратмоқчи бўлсак, Angular фреймворк танлашимиз аниқдир. Мавжуд лойиҳага фреймворкни босқичма-босқич киритиш зарурати туғилса, Vue.js-га эътибор беришимиз мақсадга мувофиқдир. Агар лойиҳа узоқ муддатли қўллаш ва ривожлантириш талаб қиладиган мураккаб веб-илова бўлса, Emberни ишлатиш яхши ечимдир. Бундан ташқари, бир вақтнинг ўзида бир нечта фреймворклардан фойдаланиш ҳам мақбул десак хато қилмаймиз. Масалан, интерфейсларни яратишда кучли восита сифатида React фреймворкидан фойдаланиш мумкин. Мураккаб масалаларни ечишга мўлжалланган ва сунъий интеллект қўлланиладиган веб-иловаларни ишлаб чиқишда Django [3], Flask аби фреймворклар қулай ҳисобланади.

Таҳлил қилинган фреймворклар, веб-технологиялар асосида тиббиёт муассасаси ахборот тизимини ишлаб чиқиш учун Django фреймворки танланди. Ахборот тизимининг маълумотлар базаси PostgreSQLда лойиҳаланди, маълумотларни қайта ишлаш учун функциялар ишлаб чиқилди. Ахборот тизимини ишлаб чиқишда Django фреймворкининг қулайликларидан самарали фойдаланилди.

#### **Фойдаланилган адабиётлар**

1. Krasner G. E. et al. A description of the model-view-controller user interface paradigm in the smalltalk-80 system //Journal of object oriented programming. – 1988. – Т. 1. – №. 3. – С. 2649.
2. <https://vincent-nguyen8931.medium.com/mvc-vs-mvvm-mvp-hmvc-and-mva-4afec3a2cab3>
3. <https://www.djangoproject.com/>

## **QISHLOQ XO\_JALIK MAXSULOTLARI SAMARALI LOGISTIKASINI TASHKIL ETISH ALGORITMI TAHLILI**

*Abduqayumov Shohruh*

*O'zbekiston Milliy universitetining Jizzax filiali magistranti*

**Annotatsiya:** *Mazkur tezisda bugungi kunda qishloq xo'jalik mahsulotlarini eksport qilish, ulardan qulay yo'l bilan foydalanish va samarali logistikasi algortimlari ustida so'z yuritiladi.*

**Kalit so'zlar:** *qishloq xo'jalik mahsulotlari, algortimlari, samarali logistika, eksport tizimlari, o'zgaroeksport, ishlab chiqarish konsepsiyasi.*

### **Qishloq xo\_jaligi mahsulotlarini export qilishning samarali tizimini tashkil qilish**

Qishloq xo\_jaligi mahsulotlarini export qilayotganda bir qator muammolar kelib chiqadi, minglab fermerlar, dehqon va fermer xo'jaliklari yetishtiradigan qishloq xo'jalik mahsulotlarini kam hajmda yetishtirish. Shuning uchun mahsulotlarni harid qilish muammosi.

O\_zagroeksport tominidan eksport shartnomalarini tuzish uchun tavsiya etilgan narxlar ancha shartli. Qishloq xo'jalik mahsulotlari narxlarini aniq aniqlash va tuzatish qiyin. Ular doimiy o'zgaruvchan omillarga bog'liq, jumladan:

- yetkazib berishning mavsumiyliги;
- boshqa mamlakatlardan ushbu turdagi qishloq xo'jaligi mahsulotlarini iste'mol qiluvchi hududni to'ldirishdan;

- yetkazib berilayotgan hududdan bir xil sabzavotlar Moskvada turli narxlarda bo'lishi mumkin, yoki, ehtimol

Umuman olganda, —O'zagroeksportl tomonidan taklif qilingan narxlar talab va taklifning tijorat emas, balki eksportni rivojini oshirish uchun vosita bo'lishi mumkin emas.

Qishloq xo'jalik mahsulotlarini eksport qilish imkoniyatlarini dehqonlar, ulgurji tashkilotlar, birjalar va banklar ishtiroki, barcha idoralar eksport bilan shug'ullanuvchi va yagona axborot makonida, qishloq xo'jaligi bilan bog'liq, sa'y-harakatlarini birlashtirish zarur. **Ishlab-chiqarishni tashkil etishning an'anaviy va logistik konsepsiyalari**

- ishlab-chiqarishni tashkil etishning logistic konsepsiyasi quyidagi asosiy holatlarni o'z ichiga oladi;
  - ortiqcha zahiralardan voz kechish;
  - asosiy va transport-ombor operatsiyalarini ishlab-chiqarishdan voz kechish;
  - iste'molchi buyurtmasi bo'lmagan mahsulotlarni ishlab-chiqarishdan voz kechish;
  - xo'jalik ichidagi noratsional tashishlarni yo'q qilish; - yetkazib beruvchilani hamkorlarga aylantirish.

Logistikadan farqli o'laroq ishlab-chiqarishni tashkil etishning an'anaviy konsepsiyasi quyidagilardan iborat:

mahsulotlarni iloji boricha yirik partiyalarda ishlab chiqish;

«har ehtimolga qarshi» moddiy resurslarning maksimal kata zaxirasiga ega bo'lish; Mahsulot talab va taklifdan ko'p bo'lsa, hech ikkilanmasdan aytish mumkinki, bozor konyukturasini hisobga olib ishlab-chiqarilgan mahsulot to'liq sotiladi. Shuning uchun asosiy ishlab chiqarish fondlari maksimal yuklash ustuvorlikga ega bo'ladi. Shu bilan birga ishlab chiqarilgan partiya qancha yirik bo'lsa mahsulot birligining tan narxi shuncha kam bo'ladi. Mahsulotni sotish birinchi darajali muammo bo'lmaydi.

Bozorga istemolchi «diktaturasi» kelishi bilan vaziyat o'zgaradi. Raqobat sharoitida ishlab chiqarilgan mahsulotni sotish vazifasi birinchi o'ringa chiqadi. Bozor talabini muntazam emasligi va oldindan bilib bo'lmazligi sharoitida katta zaxiralar yaratish va saqlash maqsadga muvofiq emasdir. Shu bilan birga, ishlab chiqaruvchi bitta buyurtmani ham qo'yib yubormaydi. Bundan, paydo bo'lgan talabga tez javob qaytara oladigan, egiluvchan ishlan chiqarish quvvatlariga ehtiyoj paydo bo'ladi.

### **Qishloq xo'jaligi mahsulotlarini yetkazish algoritmi**

Hozirgi kunda qishloq xo'jalik mahsulotlarini bir viloyatdan boshqa bir viloyatga yoki davlatga yetkazib berish mexanizmi unchalik rivojlanmagan, buni rivoji uchun biror algoritm asosida ish olib borilishi lozim.

Qishloq xo'jalik mahsulotlarini yetkazish algoritmini tuzib chiqish uchun bizga dasturiy vosita kerak bo'ladi, bunda biz python dasturlash tili va Django fremworkidan foydalanamiz. Hozirgi kunda Python dasturlash tili va Django fremworki imkoniyatlari kengayib bormoqda, bugungi kunga kelib ko'plab kompaniyalar bu dasturlash tilidan samarali logistakalarda ishlab kelmoqda. Qishloq xo'jalik mahsulotlarini yetkazib berish algoritmini tuzishning qisqacha mazmuni.

**RSA algoritmi** - RSA nomi algoritmi yaratuvchilari familiyalarining birinchi harflaridan olingan (Rivest, Shamir va Adleman). RSA algoritmi modul arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan [20].

RSA algoritmidagi ochiq va shaxsiy kalitlar juftini generatsiya qilish uchun ikkita katta uzunlikdagi  $p$  va  $q$  sonlari tanlanadi va ularning ko'paytmasi hisoblanadi:  $N = p * q$ . Shundan so'ng  $(N) = (p - 1) * (q - 1)$  bilan o'zaro tub bo'lgan,  $e$  soni tanlanadi ( $(N)$  funksiya ma'nosi quyida keltirilgan). Shundan so'ng  $(N)$  modulda  $e$  sonining teskarisi hisoblanadi va u  $d$  ga teng bo'ladi. Shundan so'ng, ikkita tub sonlarning ( $p$  va  $q$ ) ko'paytmasi  $N$  va  $ed = 1 \text{ mod } (N)$  shartni qanoatlantiruvchi  $e$  va  $d$  sonlari mavjud. Shundan so'ng,  $p$  va  $q$  lar esdan chiqariladi (o'chirib

tashlanadi). Bu yerda,  $N$  modul hisoblanib,  $(N, e)$  ochiq kalit juftini va  $d$  maxfiy kalitni tashkil etadi. RSA algoritmidan shifrlash va deshifrlash modul bo'yicha darajaga oshirish asosida bajariladi. RSA algoritmidan shifrlash uchun  $M$  xabarni son ko'rinishida ifodalash talab etiladi va  $N$  modul bo'yicha  $e$  darajaga ko'tariladi, ya'ni  $C = M^e \pmod N$ .

$S$  ni deshifrlash uchun uni  $N$  modul bo'yicha shaxsiy kalit  $d$  darajaga ko'tarish talab etiladi:

$$M = C^d \pmod N.$$

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

Eyler teoremasi. Agar  $x$  haqiqiqatdan  $n$  bilan o'zaro tub bo'lsa,  $(x)^n = 1 \pmod n$  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  $ed = 1 \pmod (N) = 1 \pmod (p - 1)(q - 1)$  tenglik kabi yozish mumkin. Mazkur tenglikning to'liq shakli aslida  $ed = 1 \pmod (N) + k(N)$  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:

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

Aytaylik, RSA algoritmidan ma'lumotni shifrlash va deshifrlash amallarini tanlab olingan ( $p = 11$  va  $q = 3$ ) — kattal 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 ( $d = 7$ ) aniqlanadi. Ya'ni,  $ed = 3 * 7 = 21 = 1 \pmod 20$ . 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 kalit juftini  $(N, e) = (33, 3)$  oladi va shifratmatni quyidagicha hisoblaydi:

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

va uni  $A$  tomonga yuboradi.

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

$$M = C^d \pmod N = 9^7 = 4782969 = 144938 * 33 + 15 = 15 \pmod 33$$

Agar RSA algoritmidan kichik tub sonlardan ( $p$  va  $q$  uchun) foydalanilgan taqdirda, hujumchi ochiq 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 mahsulotlarini samarali 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. Основы 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*