# O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

# MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

# ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

***mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami***

***(2024-yil 17-18-may)***

***(1-qism)***

**JIZZAX-2024**

“Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2024-yil 17-18-may. 410-bet.

Respublika miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., PhD. O‘ralov A.I.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., b.f.f.d. (PhD) O‘ralov A.I., t.f.f.d.(PhD), dotsent Abdumalikov A.A., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), dots. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dotsent Alibayev S.X., p.f.f.d. (PhD) Halimov O‘.H., p.f.f.d.(PhD), dotsent Karshiyev A.A., f.f.f.d.(PhD), dotsent Sindorov L.K., t.f.f.d.(PhD), dotsent Nasirov B.U., b.f.f.d. (PhD), dotsent Mustafaqulov M.A., f.f.f.d. (PhD) Alibekov D.A.., f-m.f.f.d. (PhD) Sharipov X.F., ps.f.f.d.(PhD) Norbekova B.Sh., i.f.n., dots. Tsoy M.P., Qayumov O.A., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

3. Toxir Turg'un o‘gli, A. (2023). OQIMLI SHIFRLASH ALGORITMLARINING KRIPTOGRAFIK XUSUSIYATLARI. In *Uz-Conferences* (Vol. 1, No. 1, pp. 142-144).

4. Norqo‘ziyev , Q. (2023). MOBIL ROBOTLAR UCHUN YO‘LNI REJALASHTIRISH ALGORITMI. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/746

5. Норкозиев, К., & Тоджиев, А. (2023). Использование искусственных нейронных сетей при разработке алгоритма поиска оптимального пути мобильных роботов в динамических средах. Информатика и инженерные технологии, 1(1), 25–29. извлечено от https://inlibrary.uz/index.php/computer-engineering/article/view/25025

6. Искандарова З., Иргашева У. Цифровизация и образование для устойчивого развития //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 1. – С. 197-200.

7. Oybek Kayumov, Obid Kayumov, & Isoqov Adham, Meliyeva Mohira. (2023). ELECTRONIC PLATFORM FOR RECOGNITION AND TEACHING OF SIGN LANGUAGE PICTURES BASED ON UZBEK GRAMMAR. International Journal of Contemporary Scientific and Technical Research, 263–268. Retrieved from https://journal.jbnuu.uz/index.php/ijcstr/article/view/587

8. Аликулов, С. Т., & Махкамов, Ш. С. (2018). ДИДАКТИЧЕСКАЯ КОМПЕТЕНТНОСТЬ ПЕДАГОГА. In Развитие интеллектуально-творческого потенциала молодежи: из прошлого в современность (pp. 150-152).

9. Баратов Ж.Р. (2021). ИСПОЛЬЗОВАНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ПРИ ВЫПОЛНЕНИИ ДИАГНОСТИКИ. Экономика и социум, (3-1 (82)), 458-464.

10. Жомуродов Д., Мелиева М. ИННОВАЦИИ В ОБУЧЕНИИ: НОВЫЕ ПОДХОДЫ К РАБОТЕ С МАССИВАМИ В ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММАХ //Uz-Conferences. – 2023. – Т. 1. – №. 1. – С. 867-872.

11. Жомуродов Д. Интерактивное обучение кибербезопасности //Новый Узбекистан: наука, образование и инновации. – 2024. – Т. 1. – №. 1. – С. 149-155.

## DSA ALGORITMIDAN FOYDALANIB XAVFSIZ BO‘LMAGAN TARMOQ ORQALI MA’LUMOTLAR UZATISHNING AVTOMATLASHTIRILGAN TIZIMINI ISHLAB CHIQISH

**Baratov Jasur Rustam o‘g‘li,**
**Xudoyqulov Diyorbek Shakar o‘g‘li,**
**Avazov Asadbek Egamberdi o‘g‘li**
O‘zbekiston Milliy universiteti Jizzax filiali
jasurjon2187@gmail.com

**Annotatsiya:** Ushbu maqolada xavfsiz bo‘lmagan tarmoqlar orqali ma’lumotlarni xavfsiz uzatish uchun mo‘ljallangan mustahkam tizimni yaratish haqida batafsil ma’lumot berilgan. Tarmoq orqali ma’lumotlarni uzatish jarayonida

ma’lumotlar yaxlitligi va maxfiyligini ta’minlashda kriptografik vosita sifatida raqamli imzo tizimini joriy etish uchun DSA algoritmidan foydalanilgan va jarayonni avtomatlashtirish uchun maxsus ilova ishlab chiqilgan. Bunda, shifrlash texnikasi, raqamli imzolar va aloqa infratuzilmasini mustahkamlash uchun xavfsiz protokollar integratsiyasi kabi asosiy komponentlarni muhokama qilingan.

**Kalit so‘zlar:** ma’lumotlarni uzatish, DSA, kriptografiya, raqamli imzolar, tarmoq xavfsizligi, shifrlash.

DSA (ing. Digital Signature Algorithm — raqamli imzo algoritmi) keng qo‘llaniladigan assimetrik kriptografik algoritm bo‘lib, asosan raqamli imzolar va kalitlarni almashtirish uchun ishlatiladi. Quyida DSA algoritmi va uning vazifalari keltirilgan:

- DSA raqamli imzolarni yaratish va tekshirish, ma’lumotlar yaxlitligini, autentifikatsiyani va raqamli aloqada rad etilmasligini ta’minlash uchun ishlatiladi;
- DSA assimetrik kriptografik algoritm bo‘lib, u shifrlash va shifrni hal qilish uchun bir juft kalitdan foydalanadi;
- DSA ma’lum matematik muammolarning hisoblash murakkabligiga, xususan, cheklangan sohadagi diskret logarifm muammosiga tayanadi. Ushbu murakkablik algoritmni ruxsatsiz kirish va xakerlikdan himoya qiladi;
- Raqamli imzoni yaratishda jo‘natuvchi ma’lumotlar uchun noyob imzo yaratish uchun o‘zining shaxsiy kalitidan foydalanadi. Keyin qabul qiluvchi ma’lumotlarning haqiqiyligi va yaxlitligini tasdiqlovchi jo‘natuvchining ochiq kaliti yordamida imzoni tekshirishi mumkin;

Shunday qilib, DSA algoritmi raqamli imzolarni yaratish va tekshirish usulini taqdim etish orqali raqamli aloqa xavfsizligi va haqiqiyligini ta’minlashda muhim rol o‘ynaydi. Uning turli xil xavfsizlik protokollari va ilovalarida qo‘llanilishi uning zamonaviy kriptografiyadagi ahamiyatga ega.

Ishlab chiqilgan loyihada DSA kriptografik algoritmdan foydalanib raqamli imzolarni yaratish va tekshirish imkoniniyati yaratilgan, bunda, ma’lumotlar yaxlitligini, autentifikatsiyasini va rad etilmasligini ta’minlash vositalarini mavjud. Bu yerda DSA algoritmidan foydalanib amalga oshiriladigan jarayonlar batafsil tushuntirilgan:

1. **Kalit avlodi:**
   - **Parametrlarni tanlash:** birinchi bosqichi algoritm parametrlarini tanlashni o‘z ichiga oladi. Bu parametrlarga tup son, ga qoldiqsiz bo‘linadiga tup son va oralig‘idagi butun *(generator)* butun son tanlab olinadi.
   - **Maxfiy kalit yaratish:** Maxfiy kalit oralig‘ida tasodifiy hosil qilinadi.
   - **Ochiq kalitni hisoblash:** Tegishli ochiq kalit $y$ uchun sifatida hisoblanadi. Imzoni tekshirish uchun ochiq kalit boshqalarga ulashiladi.
2. **Imzolash jarayoni:**
   - **Xeshlash:** Imzolanayotgan xabar avval kriptografik xesh funksiyasi SHA-256 yordamida qattiy uzunlikdagi dayjestni yaratish uchun xeshlanadi.
   - **Tasodifiy sonlarni yaratish:** oralig‘ida tasodifiy soni hosil qilinadi. Muayyan hujumlarning oldini olish uchun bu tasodifiy raqam har bir imzo uchun alohida olinadi.

- **va *ni* hisoblash:**

(1)

bu yerda - imzo qiymati (1) formula yordamida hisoblanadi.

(2)

bu yerda imzo jufti, bo‘lib ikkinchi tomonga uzatiladi, xabar xeshi va ning modulli multiplikativ teskarisidir.

- **Imzo:** Imzo juftidan iborat.

3. **Tasdiqlash jarayoni:**

- **Xeshlash:** Qabul qilingan xabar SHA-256 kriptografik xesh funksiyasi yordamida hisoblanadi.
- **Imzoni tekshirish:**

hisoblanadi. va qiymatlari topiladi.

(3)

hisoblab topilgandan so‘ng (1) va (3) taqqoslab ko‘riladi. Agar (1) va (3) qiymatlar teng bo‘lsa imzo haqiqiy hisoblanadi, aks holda imzo haqiqiy emas deb hisoblanadi.

**Tayyorlangan ilovaning interfeysi va vazifalari**

Avtomatlashtirilgan xavfsiz aloqa uchun tayyorlangan maxsus ilova ikki qismdan iborat:

– admin;
– foydalanuvchi.

Admin oynasi foydalanuvchining identifikatsiya ma’lumotlari (familya, ism, sharif, viloyat, tuman, tug‘ilgan sanasi, pasport seriyasi, telefon raqam) va tizimga kirish uchun ikki bosqichli autentifikatsiya ma’lumotlari (login, parol, kalit so‘z, kalit raqam) admin tomonidan to‘ldiriladi va kalit tugmasi bosilganda tizim tomonidan DSA parametrlari generatsiya qilinib, ma’lumotlar bazasidagi DSA parametrlari bilan taqqoslanadi.

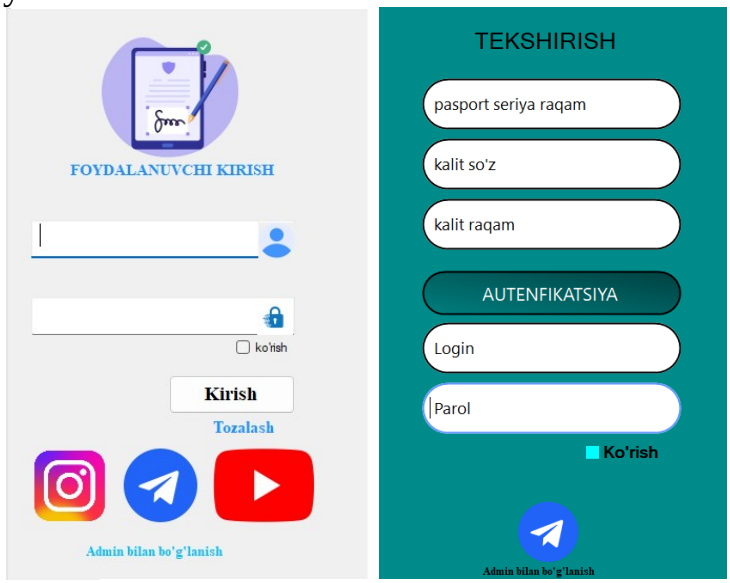



1-rasm. Admin oynasi.

Agarda ma’lumotlar bazasida DSA parametrlari oldindan mavjud bo‘lib bu parametrlar qaysidir foydalanuvchiga tegishli bo‘lsa, tizim qaytadan DSA parametrlari generatsiya qiladi. Bu holat ma’lumotlar bazasida DSA parametrlari bilan har xil

bo‘lmaguncha davom etadi (agar ma’lumotlar bazasida 10000 tadan ortiq foydalanuvchi bo‘lsa 2-3 daqiqa sarflanadi).

Agarda foydalanuvchi login yoki parolini unutsa uni qayta tiklash uchun 2-rasmda ko‘rsatilgan ijtimoiy tarmoqlar bilan integratsiya qilinadi va parolni qayta tiklash imkoniyati yaratiladi.




2-rasm. Kirish va Autentifikatsiya oynasi.

Belgilangan muddatda foydalanuvchi o‘zi tizimdan foydalanayotganligini doimiy tekshirish maqsadida ikki bosqichli autentifikatsiyadan o‘tish talab qilinadi. Agarda ikki bosqichli autentifikatsiya ma’lumotlarini (kalit so‘z yoki kalit raqamini) unutgan bo‘lsa admin bilan bog‘lanishi zarur. Foydalanuvchi login parolini to‘g‘ri kiritganda asosiy menu oynasiga o‘tadi (3-rasm). Bu oyna asosiy ikkita bo‘limdan iborat:

1. Xabar jo‘natish;
2. Kelgan xabarlar.




3-rasm. Menu oynasi

Asosiy menudan xabar jo‘natish bo‘limini tanlaganida. Xabar jo‘natish oynasi ochiladi (4-rasm). Xabar jo‘natishi uchun kerakli shaxsni jadvaldan tanlaydi. Tanlangan foydalanuvchining shaxsiy ma’lumotlari oynada chiqariladi. Tanlangan

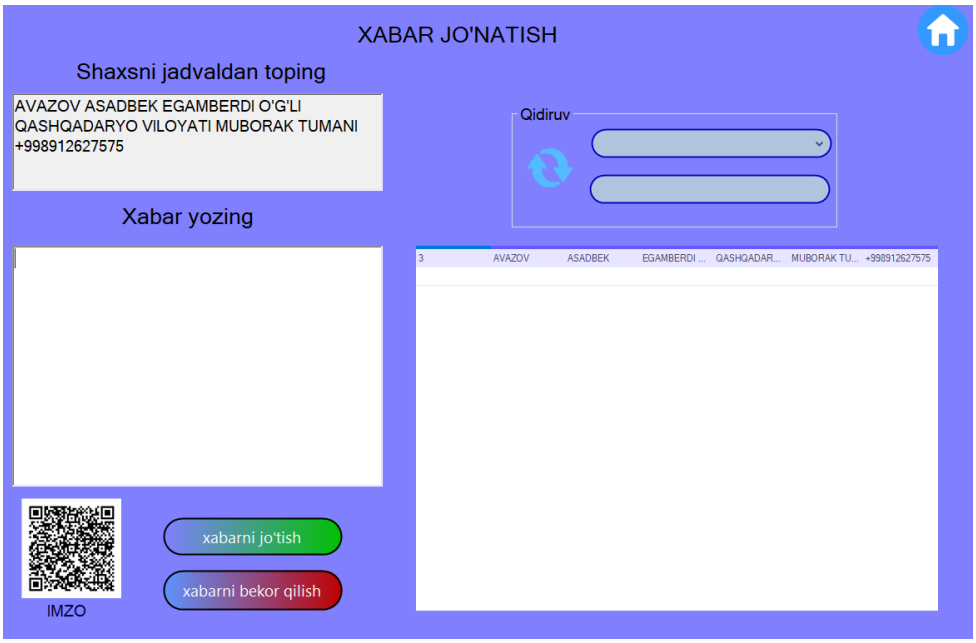
foydalanuvchiga yubormoqchi bo‘lgan xabar matnini yozadi. Xabarni jo‘natish tugmasini bosganida:

1) Tizimga kirgan foydalanuvchining shaxsiy raqami va DSA parametrlari orqali shaxsiy kaliti yig‘iladi.

2) Xabar va shaxsiy kalitdan foydalanilgan holda imzo yaratiladi.

3) Imzo QR-kod sifatida chiqariladi.

4) Tanlangan foydanuvchiga (Shaxsiy ma’lumotlari, xabari, xabarga biriktirilgan imzosi, shaxsiy raqamidan boshqa barcha DSA parametrlari) yuboriladi.




4-rasm. Xabar jo‘natish oynasi

Asosiy menudan xabar ko‘rish bo‘limini tanlaganida xabar ko‘rish oynasi ochiladi va foydalanuvchiga kelgan xabarlar ro‘yxati ko‘rinadi.

**Foydalanilgan adabiyotlar ro‘yxati:**

1. Баратов Ж.Р. (2021). ИСПОЛЬЗОВАНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ПРИ ВЫПОЛНЕНИИ ДИАГНОСТИКИ. Экономика и социум, (3-1 (82)), 458-464.

2. Жомуродов, Д. (2024). Интерактивное обучение кибербезопасности. Новый Узбекистан: наука, образование и инновации, 1(1), 149-155.

3. Жомуродов, Д. (2024). Оптимизация и улучшение производительности алгоритма шифрования Blowfish. Новый Узбекистан: наука, образование и инновации, 1(1), 155-158.

4. Mirzaev, O., Radjabov, S., Mirzaev, N., Rabbimov, I., & Baratov, J. (2024). Construction of statistical recognition algorithms based on two-dimensional threshold functions. Procedia Computer Science, 234, 123-130.

5. Мирзаев, Н. М., Мелиев, Ф. Ф., & Баратов, Ж. Р. (2022). ИККИ ЎЛЧОВЛИ БЎСАҒАВИЙ ФУНКЦИЯЛАРГА АСОСЛАНГАН СТАТИСТИК ТАНИБ ОЛИШ АЛГОРИТМЛАРИНИ ҚУРИШ. ББК 22.18 С 56, 210.

6. Mirzaev, N. M., Meliev, F. F., & Baratov, J. R. (2022). ARTIFICIAL INTELLIGENCE TECHNOLOGIES TO DETECT CANCERS FROM HUMAN COLON HISTOLOGICAL IMAGES. ББК 22.18 С 56, 181.

7. Meliyev, F. F., & Baratov, J. R. (2022). RAQAMLI PATOLOGIYANING HOZIRGI HOLATI VA UNDA MASHINAVIY O ‘QITISH USULLARINI QO ‘LLASHNING ISTIQBOLLARI. ББК 22.18 С 56, 243.

8. Toxir Turg‘un o‘gli A. et al. OQIMLI SHIFRLASH ALGORITMLARINING KRIPTOGRAFIK XUSUSIYATLARI //Uz-Conferences. – 2023. – Т. 1. – №. 1. – С. 142-144.

9. Turakulov, O., & Jomurodov, D. (2023). VIRTUAL AND AUGMENTED REALITY TECHNOLOGIES: DEVELOPMENT, APPLICATIONS, AND PERSPECTIVES. International Journal of Contemporary Scientific and Technical Research, 250-253.

10. Xolbutayevich T. O., Mamasoliyevich J. D. O‘QUV JARAYONIDA TO‘LDIRILGAN REALLIK TEXNOLOGIYALARIDAN FOYDALANISH //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 334-338.

11. Abdumo‘minovich S. A., Xolbutayevich T. O., Mamasoliyevich J. D. To‘ldirilgan reallik sun’iy intellekt bilan kelajak texnologiyasiga aylanmoqda //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 187-190.

12. Jomurodov D., Meliyeva M. THE ADVANTAGES OF IMPLEMENTING AUTOMATED SYSTEMS IN COMPUTER SCIENCE LEARNING //International Scientific and Practical Conference on Algorithms and Current Problems of Programming. – 2023.

13. Zhomurodov D., Ulashev A., Tozhiyev A. THE SYSTEM FOR DETERMINING THE QUALIFICATIONS OF INDUSTRY EXPERTS //Евразийский журнал академических исследований. – 2023. – Т. 3. – №. 4 Special Issue. – С. 280-289.

14. Абдумаликов А. А. и др. МОДЕЛЬ И АЛГОРИТМЫ ПРОЦЕССА УСТРОЙСТВ КОНТРОЛЯ И МОНИТОРИНГА УПРАВЛЕНИЯ ЭНЕРГОСНАБЖЕНИЕМ //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2023. – Т. 6. – №. 2. – С. 120-129.

15. Maxammadi R., Umida I., Noyob U. BILVOSITA KUZATUVLARDAN HARORAT O‘ZGARISHINI QAYTA TIKLASH MUAMMOSI //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 367-369.

16. Тоджиев, А., & Норкузиев, К. (2023). The role of artificial intelligence technology in individualized teaching . Информатика и инженерные технологии, 1(2), 153–156. извлечено от https://inlibrary.uz/index.php/computer-engineering/article/view/25014

17. Nasriddinovich U. A., Xayriddin o‘g‘li E. F. ELEKTRON FITNESS KLUBINING DASTURIY TAMINOTINI YARATISH USLUBLARI //Journal of new century innovations. – 2023. – Т. 26. – №. 4. – С. 143-149.

18. Nasriddinovich U. A., Nasriddinovich U. A. GORIZONTGA BURCHAK OSTIDA OTILGAN JISM HARAKATI VA DASTURIY TAMINOTI //Scientific Impulse. – 2023. – T. 1. – №. 8. – C. 437-444.
19. Nasriddinovich U. A. AXBOROTLASHGAN PEDAGOGIK TEXNOLOGIYALAR–TA'LIM SAMARADORLIGINI OSHIRISHNING SAMARALI VOSITASI //TADQIQOTLAR. UZ. – 2024. – T. 37. – №. 3. – C. 166-168.
20. Alisher T., Asrorjon U. APPLICATION AND RESULTS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN EDUCATION //International Journal of Contemporary Scientific and Technical Research. – 2023. – C. 28-30.
21. Zhomurodov D., Ulashev A., Tozhiyev A. THE SYSTEM FOR DETERMINING THE QUALIFICATIONS OF INDUSTRY EXPERTS //Евразийский журнал академических исследований. – 2023. – T. 3. – №. 4 Special Issue. – C. 280-289.

## O‘ZBEKISTONNING EKSPORT FAOLIYATINI RIVOJLANTIRISHDA EKSPORTNI RAG‘BATLANTIRISH AGENTLIGINING O‘RNI

**Bo‘ltakov Sardor Oqbo‘ta o‘g‘li**
**Asrayev Shavkat Baxtiyor o‘g‘li**
O‘zbekiston Milliy universitetining Jizzax filiali
sardorboltakov9@gmail.com

**Annotatsiya.** Bugungi kunda mamlakatimizda iqtisodiy hududlar va kichik sanoat zonalari tashkil etishga alohida e’tibor berilmoqda. Tashkil etilayotgan iqtisodiy hududlardan ko‘zlangan muhim maqsadlardan biri hududning eksport salohiyatini oshirish. Mazkur maqolada mamlakatimiz eksport salohiyatini oshirish maqsadida tashkil etilgan Eksportni rag‘batlantirish agentligi va uning amalga oshirayotgan keng ko‘lamli ishlari hamda natijalari o‘z aksini topgan.

**Kalit so‘zlar.** eksport, Eksportni rag‘batlantirish agentligi, tovarlar va xizmatlar, tadbirkorlik, tashqi savdo aylanmasi.

Bizning global iqtisodiyotimizda iste’molchilar o‘zlarining mahalliy oziq-ovqat do‘konlari va chakana savdo do‘konlarida dunyoning har bir burchagidan mahsulotlarni ko‘rishga odatlangan. Ushbu chet el mahsulotlari yoki import iste’molchilarga ko‘proq tanlovlar beradi. Ular odatda mahalliy ishlab chiqarilgan har qanday ekvivalentga qaraganda arzonroq ishlab chiqarilganligi sababli, import iste’molchilarga uy xo‘jaliklari byudjetini boshqarishda yordam beradi. Import va eksportdagi narxlarning o‘zgarishi Mehnat statistikasi byurosi tomonidan e’lon qilingan Import/eksport indeksi (MXP) tomonidan kuzatiladi.

Agar mamlakatga eksportga nisbatan import juda ko‘p bo‘lsa - bu o‘sha mamlakatdan chet elga jo‘natilgan mahsulotlar - bu mamlakatning savdo balansini buzishi va uning valyutasini qadrsizlantirishi mumkin. Mamlakat valyutasining qadrsizlanishi mamlakat fuqarolarining kundalik hayotiga katta ta’sir ko‘rsatishi