

Kiberxavfsizlik Va Raqamli Iqtisodiyotda Xavflarni Boshqarish

Muxitdinova Lobar Salixovna¹, Mirzayev Shohijahon Rustam o'g'li²

Annotatsiya: Maqola kiberxavfsizlik va raqamli iqtisodiyotda xavflarni boshqarish masalalariga bag'ishlanadi. Raqamli iqtisodiyotning rivojlanishi bilan kiberhujumlar va axborot o'g'irlash xavfi oshmoqda. Maqolada xavflarni aniqlash, baholash va samarali boshqarish usullari, shu jumladan, himoya vositalari va xavfsizlik siyosatlari tahlil qilinadi. Xavfsiz onlayn muhit yaratish, foydalanuvchilarni himoya qilish va davlat va xususiy sektor o'rtasida hamkorlik masalalari ko'rib chiqiladi.

Kalit so'zlar: Kiberxavfsizlik, raqamli iqtisodiyot, kiberhujumlar, axborot o'g'irlash, zararli dasturlar, xavflarni aniqlash, xavf-xatarlarni baholash, risklarni tasniflash, shifrlash texnologiyalari, monitoring va tahlil, tezkor javob choralari, bulutli texnologiyalar.

Raqamli iqtisodiyot bugungi kunda tez rivojlanayotgan va har kuni yangi texnologiyalarni o'z ichiga olgan bir tizimga aylangan. Internetda amalga oshirilayotgan barcha operatsiyalar, ma'lumotlar almashinuvi, elektron tijorat va boshqa onlayn faoliyatlar bizning hayotimizning ajralmas qismiga kiradi. Biroq, bu jarayonlar bilan birga, kiberhujumlar, axborot o'g'irlash, zararli dasturlar (malware) va boshqa turli xavf-xatarlar ham yuzaga keladi. Ushbu xavflar raqamli iqtisodiyotning barqaror ishlashiga salbiy ta'sir ko'rsatishi mumkin.

Kiberxavfsizlik, ayniqsa, raqamli iqtisodiyotda o'zaro bog'liq tizimlar va ma'lumotlarning himoyasini ta'minlash uchun zarur. Kiberhujumlar nafaqat moliyaviy zarar, balki ishonchni yo'qotish va kompaniyalar orasida raqobatbardoshlikni pasaytirishga olib kelishi mumkin. Shu sababli, kiberxavfsizlikni ta'minlash, risklarni boshqarish va xavfsiz tizimlar yaratish raqamli iqtisodiyotning muvaffaqiyatli ishlashi uchun zarurdir.

Kiberxavfsizlikning raqamli iqtisodiyotdagi ahamiyatini, xavflarni aniqlash va baholash usullarini, shuningdek, ularni samarali boshqarish strategiyalarini ko'rib chiqishdir. Raqamli xavfsizlikni ta'minlashda har bir tashkilot o'z xavfsizlik siyosatini ishlab chiqishi va zamonaviy texnologiyalar yordamida himoya tizimlarini mustahkamlashi kerak.

Raqamli iqtisodiyotning rivojlanishi bilan birga, xavfsizlikni ta'minlash muhim ahamiyatga ega bo'lmoqda. Kiberxavfsizlik, ayniqsa, raqamli iqtisodiyotning ustunliklariga ta'sir qiladigan xavf-xatarlarni aniqlash va boshqarish uchun zarurdir.

1-jadval Kiberhujumlarning real va prognoz qiymatlari (2021-2026)³

t(yil)	Kiberhujumlar soni (real)	Kiberhujumlar soni (prognoz)
2021	1300000	-
2022	4500000	-
2023	11000000	-
2024	12000000	-
2025	-	16850000
2026	-	20710000

¹ Buxoro davlat universiteti Iqtisodiyot va turizm fakul'teti Iqtisodiyot kafedrasini o'qituvchisi

² Buxoro davlat universiteti Iqtisodiyot va turizm fakulteti 3-bosqich talabasi

³ Giyazova N.B., Khabibov Sh.A. Data security in the digital economic environment. "YANGI O'ZBEKISTON IQTISODIYOTI" jurnali 3-son 2025 yil



So‘nggi yillarda kiberhujumlarning ortib borishini tahlil qilish uchun **chiziqli regressiya modeli** qo‘llandi. Ma‘lumotlar asosida quyidagi tenglama hosil qilindi:

$$y = -7799650000 + 3860000 \cdot t$$

Bu yerda:

- **Y** – kiberhujumlar soni
- **t** – yil (masalan, t = 2021, 2022, 2023 va h.k.)
- **a₀** = -7,799,650,000 – boshlang‘ich qiymat
- **a₁** = 3,860,000 – har yili kiberhujumlar sonining ortish tendensiyasi

Yuqoridagi tenglama asosida 2025–2026-yillarga prognoz qilindi.

Yuqoridagi regressiya modeli natijalariga ko‘ra, kiberhujumlar soni 2025–2026-yillarda sezilarli darajada oshishi kutilmoqda

Xavf-xatarlar oldindan aniqlanib, ularning ta‘sirini baholash orqali samarali xavfsizlik choralarini ko‘rish mumkin. Xavflarni aniqlash va baholash jarayonida tashkilotlar tizimlaridagi zaifliklarni va potentsial tahdidlarni aniqlashadi. Bu jarayonning asosiy bosqichlari quyidagilardir:

Xavflarni aniqlash. Xavflarni aniqlash jarayonida tizimdagi zaifliklar va potentsial tahdidlar aniqlanadi. Masalan, agar bir onlayn bank tizimida foydalanuvchi ma‘lumotlari noto‘g‘ri saqlanayotgan bo‘lsa, bu tizim uchun xavfdir. Yana bir misol, elektron tijorat do‘konida xakerlar phishing hujumlari orqali mijozlarning kredit kartalari ma‘lumotlarini olishga harakat qilishi mumkin.

Xavf-xatarlarni baholash. Xavf-xatarlarni baholashda, tahdidning tizimga ta‘sirini va uning ehtimoligini aniqlash kerak. Masalan, agar yuqoridagi bank tizimida foydalanuvchi ma‘lumotlari shifrlanmagan bo‘lsa, xavf yuqori hisoblanadi. Chunki xakerlar bu ma‘lumotlarni o‘g‘irlashi va bank hisoblariga kirish imkoniyatiga ega bo‘ladi. Elektron tijorat do‘konida esa phishing hujumlari ehtimoli bor. Agar do‘konda mijozlarning ma‘lumotlari himoyalangan bo‘lsa, bu xavf o‘rta darajada bo‘ladi.

Risklarni tasniflash. Xavf-xatarlar tasniflanadi va ular ta‘sirining jiddiyligi asosida tartiblanadi. Masalan, bank tizimida foydalanuvchi ma‘lumotlarining shifrlanmasligi, yuqori darajadagi xavf bo‘lib, tizimga katta zarar yetkazishi mumkin. Bunday xavf “yuqori” deb tasniflanadi. Elektron tijorat do‘koni uchun phishing hujumlari o‘rta darajada xavfli bo‘lishi mumkin, chunki do‘konda xavfsizlik choralarini kuchaytirish mumkin. Bunday xavf “o‘rta” darajada tasniflanadi.

Raqamli iqtisodiyotda xavflarni boshqarish samarali xavfsizlik choralarini ko‘rishni talab qiladi. Xavfsizlikni ta‘minlash uchun faqat xavf-xatarlarni aniqlash va baholash kifoya qilmaydi, balki ular bilan samarali kurashish uchun aniq strategiyalar ishlab chiqish zarur. Quyidagi strategiyalar xavf-xatarlarni kamaytirish va tizimlarni himoya qilishda muhim rol o‘ynaydi.

Preventiv choralarning qo‘llanilishi. Preventiv choralar xavf-xatarlarni oldini olishga qaratilgan bo‘lib, tizimlar va ma‘lumotlarga qarshi hujumlarni kutmasdan oldin xavfni kamaytiradi. Masalan, tizimlarda ma‘lumotlarni shifrlash, kuchli autentifikatsiya tizimlarini joriy etish va zararli dasturlarni aniqlash uchun antivirus dasturlarini o‘rnatish preventiv choralarga kiradi. Yana bir misol, tashkilotlarning o‘z xodimlariga kiberxavfsizlik bo‘yicha treninglar berish orqali phishing hujumlariga qarshi kurashish.

Tezkor javob choralari. Agar xavf allaqachon yuzaga kelgan bo‘lsa, tezkor javob choralarini ko‘rish zarur. Bu jarayonda tashkilotlar o‘z xavfsizlik siyosatiga asoslanib, xavfli vaziyatlarga tezkor javob berishga tayyor bo‘lishi kerak. Masalan, kiberhujumlar sodir bo‘lsa, ma‘lumotlarni tiklash uchun zaxira nusxalarini ishlatish yoki tizimni karantinlashtirish, zararli dasturlarni to‘liq olib tashlash, hamda hujumni amalga oshirgan shaxslarni aniqlash va huquqni muhofaza qilish organlariga xabar berish zarur.

Risklarni tarqatish. Risklarni tarqatish strategiyasi xavf-xatarlarning ta‘sirini kamaytirishga qaratilgan. Bu usul, xavf-xatarni yagona tizimda to‘plamagan holda, resurslarni turli tizimlarga yoki tashkilotlarga tarqatishga asoslanadi. Masalan, ma‘lumotlarni bulutli xizmatlarga saqlash orqali tizimda yuzaga



keladigan xavfni tarqatish mumkin. Yana bir misol, tashkilotlar o'z xavfsizlikni ta'minlash uchun xizmat ko'rsatadigan uchinchi tomon provayderlari bilan hamkorlik qilishlari mumkin.

Xavflarni yengillashtirish va boshqarish nafaqat texnologik choralar bilan, balki ijtimoiy va tashkilot ichidagi madaniyat bilan ham bog'liqdir. Xavfsizlik masalalarida odamlarning ongini o'zgartirish, ularga kerakli bilimlarni berish va tashkilotdagi barcha darajadagi xodimlar o'rtasida hamkorlikni rivojlantirish zarur.

Xodimlarni o'qitish va xabardor qilish. Kiberxavfsizlikni ta'minlashda xodimlar, ayniqsa, tashkilot ichida faoliyat yuritayotganlarning roli katta. Xodimlarga xavfsizlikni ta'minlashda mas'uliyatni tushuntirish va ularga kiberhujumlar, phishing, ma'lumotlarni himoya qilish va xavfsizlik protokollariga rioya qilish bo'yicha doimiy treninglar o'tkazish zarur. Masalan, kompaniyada muntazam ravishda kiberxavfsizlik bo'yicha seminarlar va workshoplar tashkil etish orqali xodimlar kiberhujumlarga qarshi o'zini qanday tutishlari kerakligini bilib olishadi.

Ijtimoiy hamkorlik va tizimni yaxshilash. Raqamli xavfsizlikni boshqarish faqat tashkilot ichidagi siyosatlar va choralardan iborat emas. O'zbekiston va boshqa davlatlarda kiberxavfsizlikni mustahkamlash uchun davlat, xususiy sektor va jamoatchilik o'rtasida o'zaro hamkorlikni rivojlantirish zarur. Misol uchun, hukumatning kiberxavfsizlikni kuchaytirish bo'yicha qonunchilik va tartibga solish siyosatlarini ishlab chiqishi, shuningdek, xususiy kompaniyalar va IT-professionallar bilan hamkorlikda kiberxavfsizlikni yaxshilash mumkin.

Ommaviy axborot vositalarining roli. Xavflarni yengillashtirishda ommaviy axborot vositalarining o'rni katta. Xavfsizlik bilan bog'liq ma'lumotlarni keng ommaga yetkazish orqali, foydalanuvchilar va tashkilotlar o'zlarining ma'lumotlarini qanday himoya qilishlari kerakligini bilib olishlari mumkin. Misol uchun, kiberhujumlar, onlayn firibgarliklar va boshqa xavf-xatarlar haqida ommaviy axborot vositalarida muntazam ravishda xabarlar berish, ijtimoiy tarmoqlarda xavfsizlik bo'yicha postlar va video materiallar tarqatish orqali keng ommani xabardor qilish mumkin.

Ijtimoiy jihatlarni ham inobatga olgan holda xavflarni yengillashtirish va boshqarish jarayoni nafaqat texnologik xavfsizlikni ta'minlashga, balki tashkilot va jamiyatdagi keng miqyosdagi xabardorlik va hamkorlikni rivojlantirishga qaratilgan bo'lishi kerak. Bu jarayonlarning muvaffaqiyati, oxir-oqibatda, barcha tomonlarning yagona maqsadga — xavfsizlikni ta'minlashga erishishga qaratilgan bo'lishiga bog'liq.

So'nggi yillarda butun dunyoda kiberxavfsizlik muammosi dolzarb mavzulardan biriga aylandi. 2024-yilgi statistik ma'lumotlar shuni ko'rsatadiki, davlatlar miqyosida kiberhujumlar soni va ularning ko'lamini keskin oshgan. Quyida O'zbekiston, AQSH, Buyuk Britaniya, Hindiston va Isroil davlatlari misolida kiberxavfsizlik holati tahlil qilinadi.

2-jadval 2024-yil Davlatlar bo'yicha kiberhujumlar statistikasi⁴

Davlat	Yillik o'sish (%)	Eng ko'p nishonga olingan sohalar	Qo'shimcha ma'lumotlar
O'zbekiston	34% (2023-yilga nisbatan)	Davlat veb-saytlari, ta'lim, moliya	2024-yil 1-chorakda 3 mln hujum, 70 zaiflik aniqlangan
AQSH	+56%	Ta'lim, sog'liqni saqlash, kommunal xizmatlar	\$16 mlrd zarar, phishing, ransomware eng keng tarqalgan tahdidlar
Buyuk Britaniya	+17%	Telekommunikatsiya, moliya	Ransomware kuchaygan, AI asosidagi tahdidlar o'sgan
Hindiston	+46%	Energetika, IT, davlat tashkilotlari	Dunyo bo'yicha eng ko'p hujum qayd etilgan
Isroil	+13%	Harbiy texnologiya, infratuzilma	Targeted AI tahdidlar ko'paygan

⁴ Internet ma'lumotlariga asoslanib muallif tomonidan tuzildi.



O'zbekistonda 2024-yilda 12 milliondan ortiq kiberhujum qayd etilgan. Yilning birinchi choragida 3 millionga yaqin hujum amalga oshirilgan. Bu hujumlar asosan davlat tashkilotlari, ta'lim muassasalari va bank tizimlariga qaratilgan. O'tgan yilga nisbatan tahdidlar soni 34% ga oshgan.

AQShda esa har bir tashkilot haftasiga o'rtacha 1,300 ta kiberhujumga uchragan. Yillik o'sish darajasi 56% bo'lib, asosiy hujumlar sog'liqni saqlash, kommunal xizmatlar va ta'lim sohalariga qaratilgan. AQSh fuqarolari 2024-yilda 16 milliard dollar zarar ko'rgan.

Buyuk Britaniyada haftasiga o'rtacha 1,458 ta hujum ro'yxatga olingan. Hujumlar asosan telekommunikatsiya va moliyaviy sektorga qaratilgan. Ransomware va AI asosidagi hujumlar ko'paygan.

Hindistonda haftasiga o'rtacha 3,201 ta hujum qayd etilgan. Bu 2023-yilga nisbatan 46% o'sishni bildiradi. Hujumlar asosan energetika, IT va davlat tashkilotlariga qaratilgan.

Isroilda esa haftasiga o'rtacha 1,062 ta kiberhujum ro'yxatga olingan. Hujumlar harbiy texnologiyalar va strategik infratuzilmalarga qaratilgan, ayniqsa AI vositasida amalga oshirilgan hujumlar ko'paygan.

Xavflarni boshqarish jarayonining oxirgi bosqichi sifatida, xavf-xatarlar yuzaga kelganda ularga tezkor va samarali javob berish zarur. Xavf yuzaga kelganida faol reaksiyalar tizimi tashkilotning mustahkamligini ta'minlash uchun muhim rol o'ynaydi. Bu bosqichda tashkilotlar nafaqat zararni kamaytirishga, balki tizimni tezda tiklashga ham e'tibor berishlari kerak.

Zararni minimallashtirish. Xavf yuzaga kelganda, birinchi navbatda, zarar minimallashtirilishi kerak. Misol uchun, agar tizimga xakerlar tomonidan hujum qilingan bo'lsa, tashkilot darhol tizimni offline rejimga o'tkazib, hujumni to'xtatish uchun kerakli choralarni ko'rishi kerak. Bank tizimlarida bu holatda mijozlarning hisobi uchun xavfsizlik choralari ko'rish, ya'ni operatsiyalarni to'xtatish va xavfsizligiga ta'sir qilgan ma'lumotlarni himoya qilish zarur.

Shoshilinch tiklash va javob choralari. Xavf yuzaga kelganidan so'ng tizimni tezda tiklash va har qanday zararli faoliyatni bartaraf etish lozim. Masalan, serverlarda kiberhujumlar orqali o'zgartirilgan ma'lumotlar bo'lsa, zaxira nusxalaridan ma'lumotlarni tiklash kerak. E-tijorat kompaniyasida esa, agar mijozlar ma'lumotlari o'g'irlangan bo'lsa, tegishli organga xabar berish va foydalanuvchilarga ogohlantirish yuborish zarur.

Zararli faoliyatni aniqlash va tahlil qilish. Xavf-xatar yuzaga kelganida, zararli faoliyatni aniqlash va tahlil qilish uchun maxsus jamoa yoki ekspertlar guruhini tashkil etish kerak. Ular tizimdagi o'zgartirishlarni tahlil qilib, hujumning manbasini aniqlashlari va qayta takrorlanishining oldini olish uchun zarur choralarni ko'rishlari lozim. Misol uchun, kiberhujumlarda zararli dasturdan qanday foydalanganligini va hujumni qanday to'xtatish mumkinligini aniqlashga yordam beradi.

Ma'lumotlar xavfsizligini tiklash. Hujumdan so'ng, tizimdagi ma'lumotlar xavfsizligini tiklash juda muhimdir. Tizimdagi barcha ma'lumotlar, xususan, mijozlarning shaxsiy ma'lumotlari va moliyaviy operatsiyalarni himoya qilish lozim. Bank tizimlari yoki elektron tijorat do'konlari uchun bu jarayonlarda ma'lumotlarni shifrlash va tasdiqlash mexanizmlarini kuchaytirish kerak bo'ladi.

Jamoaviy javob va kommunikatsiya. Xavf yuzaga kelganda, tashkilot ichida va tashqarida samarali kommunikatsiya juda muhim. Tizimning xavfsizligini ta'minlash uchun tashkilot ichidagi barcha bo'limlar birlashib, tizimni qayta tiklash jarayoniga qo'shilishlari kerak. Bunday hollarda, tashkilotlar mijozlar va hamkorlarga xavf haqida tezkor va aniq xabarlar yuborishlari zarur.

Xavflarga qarshi faol javob choralari nafaqat tizimni tezda tiklash, balki kelajakda yuzaga kelishi mumkin bo'lgan xavf-xatarlar uchun tayyor turish imkonini beradi.

Xulosa qilib aytganda, raqamli iqtisodiyotda xavflarni boshqarish, zamonaviy texnologiyalar va global aloqalar rivojlanishi bilan yanada murakkablashgan. Ushbu jarayonning samarali amalga oshirilishi uchun xavf-xatarlarni aniqlash, baholash, boshqarish va ular bilan kurashish uchun kompleks yondashuv talab etiladi. Kiberxavfsizlik, tizimlar va ma'lumotlarni himoya qilish, shuningdek, ijtimoiy va tashkilot ichidagi madaniyatni o'zgartirish orqali xavf-xatarlarni minimallashtirish zarur. Xavfsizlik strategiyalari, preventiv choralardan tortib, tizimlarni monitoring qilish va javob choralarigacha keng



qamrovli bo‘lishi lozim. Xavf-xatarlar oldini olish uchun samarali strategiyalar, xodimlarni o‘qitish va xavfsizlik madaniyatini rivojlantirish orqali tizimlarning barqarorligini ta‘minlash mumkin. Shuningdek, xavflarga faol javob berish va zararlarni kamaytirish jarayonlari, tashkilotlar va davlatlar o‘rtasidagi hamkorlikni kuchaytirishni talab etadi. Yakuniy maqsad — raqamli iqtisodiyotda xavfsizlikni ta‘minlash va kelajakda yuzaga kelishi mumkin bo‘lgan xavf-xatarlarni samarali boshqarishdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Abdulloev, A. J. (2023). THE ROLE AND IMPORTANCE OF STRATEGIC PLANNING IN MARKETING.
2. Abdullayeva, H. N., & Sardor, M. (2024). RAQAMLASHTIRISH-MAMLAKAT TARAQQIYOTNING MUHIM OMILI. INTELLECTUAL EDUCATION TECHNOLOGICAL SOLUTIONS AND INNOVATIVE DIGITAL TOOLS, 3(27), 113-121.
3. Abdullayeva, H. (2024). KORXONA FAOLIYATIDA INNOVATION MARKETINGDAN FOYDALANISH. *ЦЕНТР НАУЧНЫХ ПУБЛИКАЦИЙ (buxdu. uz)*, 49(49).
4. Axrorovna, B. M. (2022). The Importance of Digitizing the Tax System. *European Journal Of Business Startups And Open Society*, 2(11), 1-5.
5. Giyazova, N.B. (2024). INCREAZING THE EFFICIENCY OF WASTE RECYCLING IN THE ECONOMY OF OUR COUNTRY. *MODELS AND METHODS FOR INCREASING THE EFFICIENCY OF INNOVATIVE RESEARCH*, 3(34), 455-461.
6. Giyazova, N.B., & Sh,B.S. (2024). ZAMONAVIY RAQAMLI IQTISODIYOTDAGI MUAMMOLAR VA CHORA-TADBIRLAR. *Science and innovation*, 3(Special Issue 42), 482-489.
7. Shukhratovna, U. M., & Bayazovna, G. N. (2025). FOREIGN EXPERIENCE IN THE DEVELOPMENT OF MOBILE INTERNET. *INNOVATION IN THE MODERN EDUCATION SYSTEM*, 6(49), 250-256.
8. Таирова, М. М., & Зойитов, Д. (2024). ЗНАЧЕНИЕ МАРКЕТИНГОВЫХ ИССЛЕДОВАНИЙ В СЕЛЬСКОМ ХОЗЯЙСТВЕ. *Science and innovation*, 3(Special Issue 42), 371-376.
9. Таирова, М. М., & Рахматуллаева, Ф. М. (2015). Условия формирования инновационной экономики. *Наука 21 века: вопросы, гипотезы, ответы*, (1), 115-118.
10. Hakimovna, U. M., & Muhammedrisaevna, T. M. S. (2022). The role of banking and accounting in the development of small business and entrepreneurship. *INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH ISSN: 2277-3630 Impact factor: 8.036, 11*, 136-143.
11. Sayfullayeva, M. (2023). Establishment Of Agritourism Clusters In Uzbekistan Based On The Principles Of Sustainable Tourism. *Центр Научных Публикаций (Buxdu. Uz)*, 35(35).
12. Raxmatullayeva, F. M. (2024). MINTAQALAR RAQOBATBARDOSHLIGINI OSHIRISHDA RAQAMLI TEXNOLOGIYALARNING AHAMIYATI. *Indexing*, 1(1).
13. Raxmatullayeva, F. M., & Shaxzod, J. (2024). RAQAMLI IQTISODIYOTNING RESURLAR ISTE'MOLIGA TA'SIRI. *MODELS AND METHODS FOR INCREASING THE EFFICIENCY OF INNOVATIVE RESEARCH*, 3(34), 496-502.
14. Mubinovna, R. F. (2025). RAQAMLI IQTISODIYOTDA PLATFORMALAR AHAMIYATI. THE THEORY OF RECENT SCIENTIFIC RESEARCH IN THE FIELD OF PEDAGOGY, 3(30), 220-225.
15. Rasul o'g'li, K. U., & Bayazovna, G. N. (2025). KICHIK BIZNESNI RIVOJLANTIRISHDA RAQAMLI IQTISODIYOTNING ROLI. *INNOVATIVE DEVELOPMENTS AND RESEARCH IN EDUCATION*, 4(37), 342-348.



16. Aliyor o'g'li, X. S., & Bayazovna, G. N. (2025). KIBERXAVFSIZLIK–RAQAMLI IQTISODIYOTNI RIVOJLANISHINING MUHIM OMILI. *THE THEORY OF RECENT SCIENTIFIC RESEARCH IN THE FIELD OF PEDAGOGY*, 3(31), 113-117.
17. Shuxratovich, T. B., & Bayazovna, G. N. (2025). INSON KAPITALINING RAQAMLI IQTISODIYOTDAGI O 'RNI. *INNOVATIVE ACHIEVEMENTS IN SCIENCE 2024*, 4(38), 187-191.
18. Shokirjon o'g'li, J. S., & Bayazovna, G. N. (2025). RAQAMLI TEXNOLOGIYALAR VA EKOLOGIK BARQARORLIK: BLOKCHEYNNING YASHIL IQTISODIYOTDAGI ROLI. *INNOVATION IN THE MODERN EDUCATION SYSTEM*, 6(50), 418-425.
19. Ramz o'g'li, S. D., & Bayazovna, G. N. (2025). RAQAMLI VALYUTA VA UNING IQTISODIYOTGA TA'SIRI. *THE THEORY OF RECENT SCIENTIFIC RESEARCH IN THE FIELD OF PEDAGOGY*, 3(31), 130-135.
20. Rustam o'g'li, R. J., & Bayazovna, G. N. (2025). MOBIL TO 'LOVLAR VA ULARNING IQTISODIYOTDAGI AHAMIYATI. *THE THEORY OF RECENT SCIENTIFIC RESEARCH IN THE FIELD OF PEDAGOGY*, 3(30), 193-197.
21. Giyazova, N. B., & Azimxon ogli, Q. S. (2024). GLOBALLASHUV SHAROITIDA ENERGIYA RESURLARIDAN OQILONA FOYDALANISH. *FORMATION OF PSYCHOLOGY AND PEDAGOGY AS INTERDISCIPLINARY SCIENCES*, 3(29), 159-163.
22. Giyazova, N. B., & Dildora, I. (2024). YASHIL IQTISODIYOT VA UNING KELAJAKDAGI ISTIQBOLLARI. *FORMATION OF PSYCHOLOGY AND PEDAGOGY AS INTERDISCIPLINARY SCIENCES*, 3(29), 213-217.
23. Bayazovna, G. N., & Ayubovich, X. A. L. (2024). THE CONCEPT OF FINANCE AND THE STAGES OF ITS FORMATION. *Raqamli iqtisodiyot (Цифровая экономика)*, (7), 673-679.
24. Bayazovna, G. N. (2024). GEOMARKETINGNING RESTORAN BIZNESIGA TADBIQ ETILISHINING BUGUNGI KUNDAGI AHAMIYATI. *MODELS AND METHODS FOR INCREASING THE EFFICIENCY OF INNOVATIVE RESEARCH*, 3(34), 484-490.
25. Giyazova, N. (2023). The share of world countries in the textile industry and the importance of marketing in its development. *Центр Научных Публикаций (Buxdu. Uz)*, 27, 27.
26. Xasanova, S. (2023). Analysis of the Work Carried Out in Uzbekistan and the World to Prevent Tax Violations. *EUROPEAN JOURNAL OF INNOVATION IN NONFORMAL EDUCATION*, 3(12), 47-50.
27. Islamovna, X. S. (2024). OZIQ-OVQAT TOVARLARI B2B BOZORI GEOGRAFIYASINI KENGAYTIRISHDA AXBOROT TIZIMLARIDAN VA RAQAMLI MARKETING STRATEGIYALARIDAN FOYDALANISHNI TAKOMILLASHTIRISH. *Scientific Journal of Actuarial Finance and Accounting*, 4(03), 493-500.
28. Islamovna, X. S. (2024). AHOLINING O'ZINI O'ZI BANDLIGINI RIVOJLANTIRISHNING NAZARIY ASOSLARI. *Scientific Journal of Actuarial Finance and Accounting*, 4(03), 390-396.
29. Islamovna, X. S., & Karimbek, K. (2024). IQTISODIYOTDA ZAMONAVIY MENEJER BOSHQARUVI. *Gospodarka i Innowacje.*, 46, 361-365.
30. Наврўззода, З. Б., & Хасанова, С. И. (2022). АҲОЛИНИНГ ЎЗИНИ ЎЗИ БАНДЛИГИНИ РИВОЖЛАНТИРИШ–ИҚТИСОДИЙ БАРҚАРОРЛИКНИ ТАЪМИНЛАШ ОМИЛИ СИФАТИДА. *Central Asian Academic Journal of Scientific Research*, 2(5), 769-773.
31. Jamshedovna Q. H. GREEN ECONOMY AS A FACTOR OF SUSTAINABLE DEVELOPMENT //AMERICAN JOURNAL OF EDUCATION AND LEARNING. – 2024. – Т. 2. – №. 5. – С. 785-794.



32. Otabek o'g'li O. M., Jamshedovna Q. H. RAQAMLI IQTISODIYOTDA FOYDALANUVCHI MA'LUMOTLARINING XAVFSIZLIGINI TA'MINLASHDAGI MUAMMOLAR VA YECHIMLAR //INNOVATIVE ACHIEVEMENTS IN SCIENCE 2024. – 2025. – T. 4. – №. 38. – C. 167-174.
33. Jamshedovna Q. H., Lutfullayevna X. L. BUSINESS MANAGEMENT: WAYS TO ACHIEVE DOMINANCE IN THE MARKET //INNOVATION IN THE MODERN EDUCATION SYSTEM. – 2025. – T. 6. – №. 49. – C. 247-249.
34. Khurramov O. K., Kasimova H. J. The main advantages of internet marketing and differences from traditional marketing //Мировая наука. – 2019. – №. 4 (25). – C. 65-68.
35. Jamshedovna Q. H., Askarovich S. M. Effective Development of the Economy on the Basis of "Green Economy". – 2023.

