SPAIN

INTERNATIONAL SCIENTIFIC ONLINE CONFERENCE

PROSPECTS AND MAIN TRENDS IN MODERN SCIENCE

2025 YEAR

SPAIN, MADRID

PROSPECTS AND MAIN TRANDS IN MODERN SCIENCE

International scientific-online conference

Part 20

March 29th

COLLETIONS OF SCIENTIFIC WORKS

MADRID 2025

PROSPECTS AND MAIN TRANDS IN MODERN SCIENCE: a collection scientific works of the International scientific online conference (29th March, 2025) – SPAIN, Madrid: "CESS", 2025. Part 20– 243p.

Languages of publication: русский, india, english, казақша, o'zbek, limba română, Spanish, кыргыз тили, Հայերեն….

The collection consists of scientific research of scientists, graduate students and students who took part in the International Scientific online conference "**PROSPECTS AND MAIN TRANDS IN MODERN SCIENCE** ". Which took place in Madrid on March 29, 2025.

Conference proceedings are recomanded for scientits and teachers in higher education esteblishments. They can be used in education, including the process of post - graduate teaching, preparation for obtain bachelors' and masters' degrees. The review of all articles was accomplished by experts, materials are according to authors copyright. The authors are responsible for content, researches results and errors.

KIBERXAVFSIZLIK SOHASIDA SUN'IY INTELLEKT VA BLOKCHEYN TEXNOLOGIYALARINI QO'LLASH IMKONIYATLARI

Mirzayev Shohijahon Rustam o'g'li
Buxoro davlat universiteti Iqtisodiyot va turizm fakulteti 3-bosqich talabasi
Giyazova Nozima Bayazovna
Buxoro davlat universiteti Iqtisodiyot va turizm fakulteti Iqtisodiyot kafedrasi dotsenti, i.f.f.d (PhD)

Annotatsiya: *Maqolada kiber hujumlar, axborotlarni o'g'irlash, tizimlarning buzilishi kabi kiberxavf turlarining o'sishi va ularning iqtisodiyotga ta'siri tahlil qilinadi. Xavflarni boshqarishda yangi usullarni, shu jumladan sun'iy intellekt va blokcheyn texnologiyalarini qo'llash imkoniyatlari o'rganiladi. Shuningdek, xavf va muammolarni minimallashtirish uchun ilg'or yechimlar va amaliy ko'rsatmalarni taqdim etadi.*

Kalit so'zlar: *kiber xavfsizlik, raqamli iqtisodiyot, kiberxavf, sun'iy intellekt, blokcheyn texnologiyasi, phishing, zararli dasturlar, avtomatik javob, ma'lumotlar integriteti, decentralizatsiya, smart kontraktlar, kiberjinoyatlar.*

Zamonaviy raqamli iqtisodiyotning rivojlanishi va global tarmoqning kengayishi, bir tomondan iqtisodiyotni yanada samarali va tezkor qilish imkoniyatlarini yaratgan bo'lsa, ikkinchi tomondan, yangi xavflarni ham yuzaga keltirdi. Bugungi kunda iqtisodiyotning ko'plab sohalari raqamli texnologiyalar bilan chuqur integratsiyalashgan, bu esa o'z navbatida kiberxavfsizlikni ta'minlash zaruratini keskin oshiradi. Kiber hujumlar, axborotlarni o'g'irlash, tizimlarning buzilishi va boshqa zararli faoliyatlar nafaqat tashkilotlarning moliyaviy holatiga, balki ularning obro'siga ham salbiy ta'sir ko'rsatishi mumkin. Shuningdek, bunday xavflar iqtisodiy tarmoqlarda ishonchni yo'qotishga, foydalanuvchi ma'lumotlarining xavfsizligini buzishga va bozor barqarorligiga tahdid soladi.

Raqamli iqtisodiyotda xavflarni boshqarish va kiberxavfsizlikni ta'minlash masalasi bugungi kunda nafaqat texnologik, balki strategik ahamiyatga ega. Kiberxavfsizlikni ta'minlash orqali tashkilotlar o'z faoliyatini xavfsiz va uzluksiz davom ettirishi mumkin, ammo bu jarayon yangi usullar va texnologiyalarni qo'llashni talab qiladi. Kiberxavf turlarining o'sishi, ularning iqtisodiyotga ta'siri, shuningdek, xavf va muammolarni minimallashtirish uchun zamonaviy texnologiyalar, jumladan, sun'iy intellekt va blokcheyn texnologiyalarini qo'llash kerak bo'lmoqda. Bu texnologiyalar kiberxavfsizlikni samarali boshqarishda qanday yordam berishi mumkinligi va qanday ilg'or yechimlar mavjudligini ko'rsatadi.

Sun'iy intellekt kiberxavfsizlik sohasida xavf-xatarlarni aniqlash, ularga javob berish va oldini olishda samarali vosita sifatida keng qo'llanilmoqda. Bugungi kunda kiberhujumlar murakkab va tezkor tarzda amalga oshirilayotgani sababli, sun'iy intellekt kiberxavfsizlikni ta'minlashda juda muhim rol o'ynaydi. Quyida sun'iy intellekt texnologiyasining kiberxavfsizlikdagi asosiy qo'llanilish yo'nalishlari ko'rib chiqiladi:

1. Xavfni aniqlash va tahlil qilish

Sun'iy intellekt tizimlari kiberxavfsizlikda eng samarali xavf-xatarlarni aniqlash va tahlil qilish vositalaridan biridir. Sun'iy intellekt algoritmlari, foydalanuvchi faoliyatini va tarmoqdagi trafikni doimiy ravishda kuzatib boradi va odatiy holatlardan og'ishlarni tezda aniqlaydi. Bu tizimlar yirik ma'lumotlar bazalaridan foydalanib, zararli harakatlarni yoki tahdidlarni erta bosqichda sezadi, bu esa kiberhujumlarga qarshi tezkor choralar ko'rish imkonini beradi. Masalan, AQShdagi moliyaviy kompaniyada sun'iy intellekt real vaqt rejimida kiberhujumni aniqlab, uni dastlabki bosqichdayoq to'xtatishga yordam bergan. Bugungi kunda Darktrace kabi tizimlar 110 dan ortiq mamlakatda minglab tashkilotlarni xuddi shunday real vaqt rejimida himoya qilmoqda.

2. Zararli dasturlarni aniqlash

Sun'iy intellekt zararli dasturlarni aniqlashda keng qo'llaniladi. Traditsion antivirus dasturlari faqat ma'lum bir zararli dasturlarni aniqlay oladi, lekin sun'iy intellekt tizimlari yangi va ilgari noma'lum zararli dasturlarni o'z-o'zini o'rgatish asosida aniqlash imkoniyatiga ega. Sun'iy intellekt yordamida, zararli dasturlar tizimga kirish usulini va uning qanday faoliyat yuritishini o'rganadi, bu esa unga mutatsiyalangan yoki yangi turdagi zararli dasturlarni oldindan aniqlash imkonini beradi. Sun'iy intellektning o'rganish qobiliyati tizimni doimiy ravishda yangilab boradi va tahdidlarni yangi shakllariga moslashishga yordam beradi. Sun'iy intellekt asosidagi Cylance kabi tizimlar WannaCry kabi global tahdidlarni tahlil qilib, yangi mutatsiyalangan versiyalarini oldindan aniqlash imkonini bergan. Tadqiqotlarga ko'ra, sun'iy intellekt asosidagi antiviruslar an'anaviy antiviruslarga qaraganda 60% ko'proq yangi tahdidlarni erta aniqlaydi.

3. Phishing hujumlarini oldini olish

Phishing hujumlari kiberjinoyatchilar tomonidan foydalanuvchilarni aldanishga undash uchun ishlatiladi. Sun'iy intellekt tizimlari foydalanuvchi xatti-harakatlarini tahlil qilish va shubhali xabarlar yoki havolalarni avtomatik tarzda aniqlash imkoniyatiga ega. Shuningdek, phishing hujumlariga oid ilg'or usullarni (masalan, soxta veb-saytlar yoki manipulyatsiya qilingan email xabarlar) avtomatik tarzda identifikatsiya qilishda sun'iy intellekt tizimlarining o'z-o'zini o'rgatish funksiyasi yordam beradi. Bunda sun'iy intellekt foydalanuvchini ogohlantirishi yoki xabarni avtomatik tarzda bloklashi mumkin. Shu bilan birga, Google sun'iy intellekti 2021-yilda Gmail orqali yuborilgan 100 milliondan ortiq phishing xabarlarini avtomatik ravishda bloklagan. Bugungi kunda Gmail AI tizimi phishing hujumlarini 99,9% aniqlik bilan aniqlay oladi.

4. Avtomatik javob va reaksiya

Kiberxavfsizlikni ta'minlashda sun'iy intellektning asosiy afzalliklaridan biri uning avtomatik javob berish imkoniyatidir. Kiberhujumlar aniqlangach, Sun'iy intellekt tizimlari avtomatik tarzda zarur choralarni ko'rishga o'rgatilgan. Masalan, tizimga kirish urinishlarini bloklash, zararli dasturlarni o'chirish yoki zarar ko'rgan tizimni izolyatsiya qilish kabi chora-tadbirlar Sun'iy intellekt tomonidan tezkor amalga oshiriladi. Inson aralashuvisiz amalga oshiriladigan bu jarayonlar, kiberhujumlarni oldini olishda samarali bo'lib, tizimning uzluksiz ishlashini ta'minlaydi. Bunday avtomatik javoblar nafaqat vaqtni tejaydi, balki kiberxavfsizlikning yanada samarali boshqarilishini ta'minlaydi. Shuningdek,

Microsoft'ning Azure Sentinel tizimi sun'iy intellekt yordamida hujumlarni aniqlagandan so'ng, zararli trafikni bloklash, shubhali qurilmalarni ajratish va xavf darajasini baholash kabi chora-tadbirlarni avtomatik ravishda amalga oshiradi. Shunday tizimlar kiberhujumlarga javob berish samaradorligini 70% ga oshirgan.

So'nggi yillarda sun'iy intellekt texnologiyalari kiberxavfsizlik sohasida samarali vosita sifatida faol qo'llanilmoqda. Xususan, turli mamlakatlarda sun'iy intellekt asosida kiberjinoyatchilikka qarshi kurashish bo'yicha aniq natijalarga erishilmoqda. 2024-yilga oid quyidagi tahliliy ma'lumotlar sun'iy intellekt texnologiyalarining kiberxavfsizlikda tutgan o'rnini yaqqol namoyon etadi.

1-jadval

Sun'iy intellekt – kiberxavfsizlik sohasidagi qo'llanilishi va oldini olish natijalari (mamlakatlar kesimida, 2024)[21]

Mamlakat	Qo'llanilish sohasi	Oldini olingan kiberjinoyatlar soni
AQSH	Firibgarlikni aniqlash	420000
	Fishing xurujlarini aniqlash	300000
	Zararli dasturlarni aniqlash	550000
Germaniya	Firibgarlikni aniqlash	200000
	Fishing xurujlarini aniqlash	180000
Yaponiya	Tarmoqlardagi hujumlarni aniqlash	200000
Xitoy	Firibgarlikni aniqlash	380000
O'zbekiston	Firibgarlikni aniqlash	12000
	Fishing xurujlarini aniqlash	15000

Yuqoridagi jadvalda ko'rishimiz mumkinki, AQSHda sun'iy intellekt yordamida firibgarlikni aniqlash sohasida 420 mingdan ortiq kiberjinoyatlarning oldi olingan bo'lsa, fishing xurujlarini aniqlash orqali yana 300 ming holat barvaqt fosh etilgan. Shuningdek, zararli dasturlarni aniqlash tizimlari orqali 550 mingta tahdidning oldi olingan. Germaniyada esa sun'iy intellektdan firibgarlikni aniqlashda faol foydalanilib, natijada 200 mingta kiberjinoyatning oldi olingan. Shu bilan birga, fishing xurujlarini aniqlash tizimlari yordamida 180 mingta holat fosh etilgan.Yaponiyada sun'iy intellekt texnologiyalari tarmoqlardagi hujumlarni aniqlash sohasida keng qo'llanilib, 200 mingta kiberjinoyatning oldi olingan.Xitoyda esa firibgarlikni aniqlash sohasida sun'iy intellekt tizimlari orqali 380 mingta tahdid barvaqt bartaraf etilgan.O'zbekistonda sun'iy intellekt texnologiyalaridan foydalanish hali dastlabki bosqichda bo'lsa-da, firibgarlikni aniqlashda 12 mingta, fishing xurujlarini aniqlashda esa 15 mingta holatning oldi olingan.

Blokcheyn texnologiyasi kiberxavfsizlikni ta'minlashda samarali vosita sifatida qabul qilinmoqda. Uning asosiy afzalliklari, ya'ni ma'lumotlarni o'zgartirishning imkonsizligi, shaffoflik va ishonchlilik, kiberxavfsizlikni mustahkamlashda katta rol o'ynaydi. Blokcheyn texnologiyasi ma'lumotlarning xavfsizligini ta'minlashda bir qator imkoniyatlar yaratadi. Quyida blokcheynning kiberxavfsizlikda qo'llanilishining asosiy yo'nalishlari ko'rib chiqiladi:

[21] IBM Security X-Force Threat Intelligence Index 2024 – https://www.ibm.com/reports/threat-intelligence
O'zbekiston Respublikasi Kiberxavfsizlik Markazi 2024 yillik hisobotidan (https://csrc.uz)

1. Ma'lumotlar integritetini ta'minlash

Blokcheyn texnologiyasining asosiy afzalligi uning o‘zgartirilmasligi hisoblanadi. Har bir blok o‘zaro kriptografik bog‘lanishlar bilan ulanib, tizimdagi ma'lumotlar ishonchliligini ta'minlaydi. Blokcheyn orqali ma'lumotlarni soxtalashtirish yoki o‘zgartirish deyarli imkonsiz bo‘ladi, bu esa kiberxavfsizlikni kuchaytiradi. Misol uchun, Walmart o‘zining ta’minot zanjirini boshqarishda blokcheyn texnologiyasidan foydalanadi. Har bir mahsulotning kelib chiqishi va yetkazib berish jarayonidagi har bir qadam blokcheynga yoziladi. Agar mahsulot sifati bo‘yicha muammo chiqsa, Walmart bir necha soniya ichida uning manbasini aniqlay oladi.

2. Decentralizatsiya va xavfsizlik

Blokcheynning markazlashtirilmagan tuzilishi tizimni yanada xavfsiz qiladi. Ma'lumotlar bir nechta joyda saqlanadi, bu esa tizimga kirish va ma'lumotlarni o‘g‘irlashni qiyinlashtiradi. Markazlashtirilgan tizimlarga nisbatan blokcheynning decentralizatsiya qilingan strukturasida biror qismning buzilishi butun tizimga zarar yetkazmaydi. Blokcheyn tarmoqlariga hujum qilish uchun kiberjinoyatchilar tarmoq quvvatining kamida 51% ini egallashi kerak. Bu esa katta energiya va resurs talab qiladi, shuning uchun blokcheyn tizimlariga bo‘lgan muvaffaqiyatli hujumlar darajasi an’anaviy markazlashgan tizimlarga nisbatan 90% kam.

3. Xavfsiz autentifikatsiya va identifikatsiya

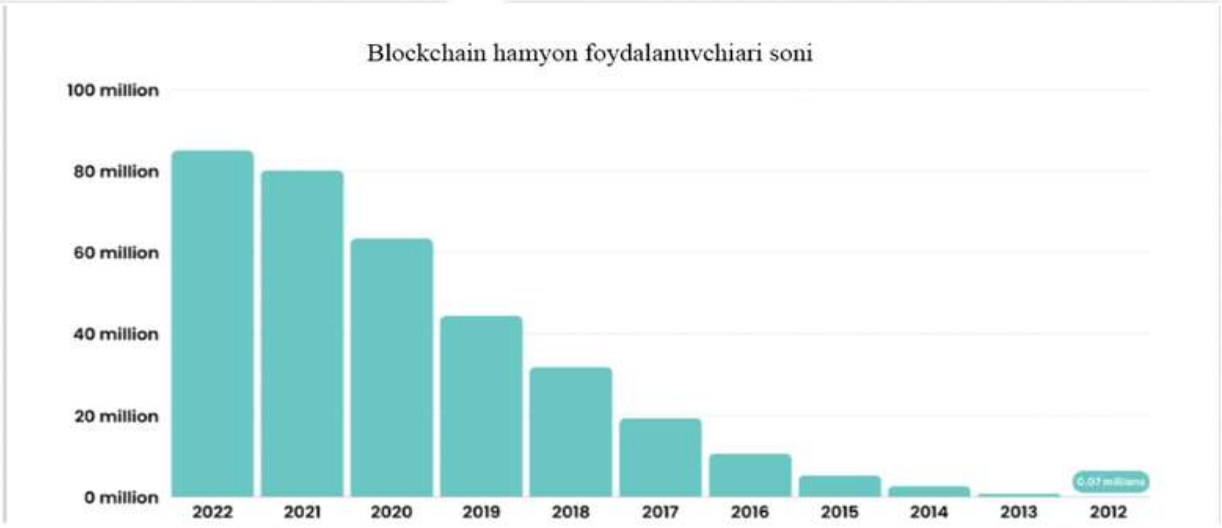
Blokcheyn foydalanuvchi identifikatsiyasini xavfsiz va ishonchli tarzda amalga oshirish imkonini beradi. Kriptografik kalitlar yordamida foydalanuvchilarni tasdiqlash jarayoni an'anaviy tizimlarga nisbatan yanada xavfsizdir, bu esa "account takeover" kabi hujumlarga qarshi samarali himoya yaratadi. Bunga qo‘shimcha, Microsoft o‘zining Azure Active Directory (Azure AD) tizimiga blokcheyn asosida Decentralized Identity funksiyasini qo‘shgan. Bu funksiyada foydalanuvchilar o‘z shaxsiy ma’lumotlarini blokcheynga joylashtirib, nazoratni o‘z qo‘lida saqlaydi.

4. Smart kontraktlar va avtomatik shartnomalar

Blokcheyn asosidagi smart kontraktlar taraflar o‘rtasidagi shartnomalarni avtomatik tarzda bajarilishini kafolatlaydi. Shartnomalar blokcheynda xavfsiz tarzda saqlanadi va barcha harakatlar tasdiqlanishi kerak, bu esa shaffoflikni ta'minlab, soxtalashtirish va manipulyatsiya qilish imkoniyatlarini kamaytiradi. Shuningdek, Siemens smart kontraktlar orqali logistika va yuk tashish jarayonlarini avtomatlashtirishda blokcheyn texnologiyasidan foydalanilmoqda. Yuk jo‘natish va qabul qilish shartlari to‘liq bajarilgandagina to‘lov amalga oshiriladi, bu ishonchli va xavfsiz hamkorlik uchun zamin yaratadi. Smart kontraktlar asosidagi tizimlar 2023-yilda xalqaro savdoda hujjatlarni soxtalashtirish holatlarini 70% ga kamaytirgan.

Blockcheyn hamyon foydalanuvchilari sonining keskin o‘sishi (2016 yilda 10 mln.dan 2021 yilda 80 mln.ga) kiberxavfsizlik tahdidlarini oshirdi. Bu phishing hujumlari, kalitlarni o‘g‘irlash va firibgarlik kabi xatarlarning ko‘payishiga olib keldi. Foydalanuvchilarni himoya qilish uchun ikki bosqichli autentifikatsiya, apparat hamyonlari va xavfsizlik bo‘yicha xabardorlikni talab qiladi. Blockcheyn tizimining kengayishi bilan xavfsizlikni

ta'minlash ustuvor vazifa bo‘lib qolyapti. Quyidagi diagramma blockcheyn hamyon foydalanuvchilari sonining yillar kesimidagi o‘sish dinamikasini aks ettiradi.



1-rasm. Blokcheyn hamyon foydalanuvchilar soni[22]

Grafikdan ko‘rinib turibdiki, blockchain texnologiyasiga qiziqish va uni qo‘llovchi foydalanuvchilar soni yildan-yilga sezilarli darajada ortib borgan.2012-2015-yillar oralig‘ida blockchain hamyonlariga bo‘lgan talab juda past bo‘lgan. 2012-yilda atigi 0,07 million foydalanuvchi mavjud bo‘lgan bo‘lsa, 2015-yilga kelib bu ko‘rsatkich biroz oshgan, ammo sezilarli darajada emas.2016-yildan boshlab blockchain texnologiyalari ommalasha boshladi va bu hamyon foydalanuvchilar soniga ham ta’sir qildi. Aynan shu davrdan boshlab raqamli aktivlarga (kripto aktivlarga) bo‘lgan qiziqish ortib, blockchain texnologiyasidan foydalanish hajmi tez sur’atlar bilan oshdi.2017-2018-yillarda bu o‘sish ancha tezlashdi va millionlab foydalanuvchilar blockchain hamyonlarini yaratib, undan turli tranzaksiyalar va investitsiyalar uchun foydalana boshladi. Ayniqsa, 2017-yildagi kriptovalyutalar bozoridagi yuksalish bu jarayonga katta turtki bergan.2019-2022-yillarda blockchain hamyon foydalanuvchilari soni muttasil oshib, 2022-yilda 80 milliondan ortiq ko‘rsatkichga yetdi. Bu davrda blockchain texnologiyasi nafaqat kriptovalyuta savdosida, balki DeFi (markazlashmagan moliya), NFT (noo‘rin almashinuvchi tokenlar) va smart kontraktlar orqali turli sohalarda faol qo‘llanila boshladi.

Blokcheyn texnologiyasi kiberxavfsizlikni ta'minlashda muhim innovatsiya sifatida ajralib turibdi. Ma’lumotlarning o‘zgartirilmasligi va shaffofligi bu texnologiyani ishonchli qilish bilan birga, xavfsizlikni mustahkamlash imkoniyatini beradi. Blokcheyn raqamli xavflarga qarshi barqaror yechim bo‘lib, zamonaviy xavfsizlik talablariga javob beradi.

Xulosa qilib aytganda, bugungi globallashgan dunyoda raqamli texnologiyalarning keng qo‘llanilishi yangi imkoniyatlar yaratish bilan birga, turli xavf-xatarlarni ham yuzaga keltirmoqda. Kiberxavfsizlik nafaqat texnologik, balki strategik ahamiyatga ega bo‘lib, uning to‘g‘ri boshqarilishi iqtisodiyot barqarorligi va rivojlanishi uchun muhimdir.

Sun’iy intellekt va blokcheyn texnologiyalari kabi ilg‘or texnologiyalar kiberxavfsizlik sohasida yangi ufqlarni ochmoqda. Sun’iy intellekt xavf-xatarlarni aniqlash va ularga

[22]Mamadjanov Sh.Sh., Odilov A. Kokand University, Xalqaro ilmiy-amaliy konferensiyasi (2023)

tezkor javob berishda samarali vosita bo‘lib, zararli dasturlarni aniqlash va phishing hujumlarini oldini olish kabi yo‘nalishlarda muvaffaqiyatli qo‘llanilmoqda. Blokcheyn texnologiyasi esa ma’lumotlarning yaxlitligi va ishonchliligini ta’minlash, decentralizatsiya orqali tizimlarni mustahkamlash hamda xavfsiz autentifikatsiya kabi muhim imkoniyatlarni taqdim etadi.

Kiberjinoyatlar natijasida global miqyosda iqtisodiy zararlar ortib borayotgani raqamli xavfsizlikni ta’minlashga yanada jiddiy e’tibor qaratishni talab qiladi. Maqola kiberxavfsizlikni mustahkamlashda zamonaviy texnologiyalarni joriy etish va ulardan foydalanish zarurligini ta’kidlaydi. Shuningdek, bu texnologiyalarlar kelajakda kiberxavfsizlik sohasida yanada barqaror va ishonchli tizimlar yaratishga xizmat qiladi.

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 INNOVATSION MARKETINGDAN FOYDALANISH. ЦЕНТР НАУЧНЫХ ПУБЛИКАТSIЙ (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. 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.
9. Таирова, М. М., & Зойитов, Д. (2024). ЗНАЧЕНИЕ МАРКЕТИНГОВЫХ ИССЛЕДОВАНИЙ В СЕЛЬСКОМ ХОЗЯЙСТВЕ. Science and innovation, 3(Special Issue 42), 371-376.
10. Таирова, М. М., & Рахматуллаева, Ф. М. (2015). Условия формирования инноватsионной экономики. Наука 21 века: вопросы, гипотезы, ответы, (1), 115-118.

11. 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.

12. Sayfullayeva, M. (2023). Establishment Of Agritourism Clusters In Uzbekistan Based On The Principles Of Sustainable Tourism. Центр Научных Публикатsій (Buxdu. Uz), 35(35).

13. Raxmatullayeva, F. M. (2024). MINTAQALAR RAQOBATBARDOSHLIGINI OSHIRISHDA RAQAMLI TEXNOLOGIYALARNING AHAMIYATI. Indexing, 1(1).

14. Raxmatullayeva, F. M., & Shaxzod, J. (2024). RAQAMLI IQTISODIYOTNING RESURSLAR ISTE'MOLIGA TA'SIRI. MODELS AND METHODS FOR INCREASING THE EFFICIENCY OF INNOVATIVE RESEARCH, 3(34), 496-502.

15. Mubinovna, R. F. (2025). RAQAMLI IQTISODIYOTDA PLATFORMALAR AHAMIYATI. THE THEORY OF RECENT SCIENTIFIC RESEARCH IN THE FIELD OF PEDAGOGY, 3(30), 220-225.

16.IBM Security X-Force Threat Intelligence Index 2024 – https://www.ibm.com/reports/threat-intelligence

17. O‘zbekiston Respublikasi Kiberxavfsizlik Markazi 2024 yillik hisobotidan (https://csrc.uz).

18. Mamadjanov Sh.Sh., Odilov A. Kokand University, Xalqaro ilmiy-amaliy konferensiyasi (2023).