YANGI O‘ZBEKISTON, YANGI TADQIQOTLAR JURNALI
Volume 2 Issue 9 18.05.2025
https://phoenixpublication.net/ Online ISSN: 3030-3494

BANKLARNING KIBERXAVFSIZLIGI: RAQAMLI MOLIYA DUNYOSIDA XAVF VA IMKONIYATLAR

Xidirov Ulug‘bek Gulboy o‘g‘li
Toshkent xalqaro moliyaviy boshqaruv va texnologiyalar universiteti
Bank ishi va audit yo‘nalishi 2-kurs talabasi
email; @ulugbekjon0218gmail.com

Annotatsiya. *Ushbu maqola banklarning kiberxavfsizlik sohasidagi dolzarb masalalarni tahlil qiladi va raqamli moliya dunyosida yuzaga kelayotgan yangi xavf-xatarlarni muhokama qiladi. Banklar va moliyaviy institutlar uchun kiberhujumlar, ma'lumotlar o‘g‘irlanishi, soxta operatsiyalar, va boshqa virtual tahdidlar jiddiy xavf tug‘diradi. Maqolada, shu bilan birga, banklarning o‘z tizimlarini himoya qilish uchun joriy qilayotgan ilg‘or xavfsizlik chora-tadbirlaridan, jumladan, ma'lumotlarni shifrlash, ko‘p faktorli autentifikatsiya (MFA), tarmoqni monitoring qilish va penetratsion testlar kabi texnologiyalardan foydalanishlari haqida so‘z yuritiladi. Shuningdek, yangi texnologiyalar, masalan, sun'iy intellekt (AI) va mashina o‘rganish, blokcheyn texnologiyasi kabi innovatsion yondashuvlar orqali banklar kiberhujumlarning oldini olishga harakat qilmoqdalar. Maqola, banklar va foydalanuvchilar o‘rtasida hamkorlikning ahamiyatini ta'kidlab, kiberxavfsizlikni ta'minlashda faqat texnologik yondashuvlar emas, balki ta'lim va ongli xatti-harakatlarni ham muhim rol o‘ynashini ko‘rsatadi. Maqola bank tizimlarining xavfsizligini ta'minlash bo‘yicha zamonaviy yondashuvlar va texnologiyalarni tahlil qilishga qaratilgan.*

Kalit so'zlar: *Kiberxavfsizlik, Bank tizimlari, Raqamli moliya, Phishing (aloqa orqali aldatish), DDoS hujumlari, Malware (zararli dasturlar), Ma'lumotlar o'g'irlanishi, Ko‘p faktorli autentifikatsiya (MFA), Ma'lumotlarni shifrlash, Sun'iy intellekt (AI), Mashina o‘rganish, Blokcheyn texnologiyasi, Kiberhujumlar, Xavfsizlik choralarini joriy etish, Tarmoq monitoringi, Penetratsion testlar, Foydalanuvchi ta'limi, Xavfli faoliyatni aniqlash.*

Kirish

Bugungi kunda banklar va moliyaviy institutlar raqamli texnologiyalarni keng qo‘llash orqali global moliya tizimini o‘zgartirishda davom etmoqda. Internet banking, mobil ilovalar va elektron to‘lov tizimlari kabi xizmatlar foydalanuvchilarga qulaylik yaratishda, iqtisodiy faoliyatni tezlashtirishda muhim ro‘l o‘ynaydi. Biroq, bu raqamli transformatsiya bilan birga yangi xavf-xatarlar ham yuzaga kelmoqda. Kiberhujumlar, ma'lumotlar o‘g‘irlanishi, soxta operatsiyalar va boshqa virtual tahdidlar banklarning xavfsizligini

ta'minlashni yanada murakkablashtirmoqda. Banklar, o‘z navbatida, ushbu tahdidlarga qarshi kurashish va foydalanuvchilarini himoya qilish uchun ilg‘or kiberxavfsizlik texnologiyalarini joriy etishmoqda.

Bu maqolada, banklarning kiberxavfsizlik sohasidagi yangi yondashuvlari, ularga qarshi kurashishda qo‘llanilayotgan ilg‘or texnologiyalar va foydalanuvchilarni himoya qilish uchun amalga oshirilayotgan chora-tadbirlar haqida so‘z yuritiladi. Kiberxavfsizlik bugungi bank tizimining asosiy ustuvor yo‘nalishlaridan biriga aylangan va bu sohada muvaffaqiyatli ishlash uchun faqat banklar emas, balki mijozlar ham o‘z mas'uliyatini his qilishlari kerak.

Asosiy qism

Banklar va moliyaviy institutlar uchun kiberxavfsizlik hozirgi zamonning eng dolzarb masalalaridan biriga aylangan. Raqamli moliya dunyosida xavf-xatarlar tobora ortib borayotgan bir paytda, banklarning moliyaviy xizmatlari, foydalanuvchi ma'lumotlari va tizimlarining xavfsizligini ta'minlash nafaqat texnologik yondashuvni, balki ta'lim va hamkorlikni ham talab qilmoqda. Raqamli xizmatlarning jadal rivojlanishi bilan birga, banklar turli kiberhujumlarga qarshi kurashish uchun ilg‘or xavfsizlik chora-tadbirlarini joriy qilmoqdalar. Quyida banklarning kiberxavfsizlikni ta'minlashdagi asosiy strategiyalari, texnologiyalari va ularga qarshi kurashishda qo‘llanilayotgan chora-tadbirlar haqida batafsil so‘z yuritamiz.

Kiberxavfsizlik: Asosiy Tahdidlar va Xavflar

Kiberhujumlar banklar uchun jiddiy xavf tug'diradi. Bu xavflar bir nechta turli shakllarda namoyon bo‘ladi. Bank tizimlariga nisbatan keng tarqalgan tahdidlar quyidagilardan iborat:

Ma'lumotlar o'g'irlanishi: Banklarning onlayn tizimlari orqali foydalanuvchilar shaxsiy ma'lumotlarini, shu jumladan kredit kartalari raqamlari, PIN-kodlar, parollar va boshqa maxfiy ma'lumotlarni o‘g‘irlash maqsadida hujumlar amalga oshiriladi. Bunday hujumlar bank foydalanuvchilariga jiddiy moliyaviy zarar yetkazishi mumkin.

Phishing (aloqa orqali aldatish) hujumlari, odatda, hujumchilar tomonidan banklarning rasmiy yoki ishonchli manzillarini taqlid qilgan soxta elektron pochta xabarlarini yuborish orqali amalga oshiriladi. Hujumchilarning maqsadi — foydalanuvchilarni aldanib, o‘z shaxsiy yoki moliyaviy ma'lumotlarini (masalan, bank hisob raqamlari, parollar, PIN-kodlar yoki kredit karta ma'lumotlari) ularga berishga majbur qilish.

DDoS (Distributed Denial of Service) hujumlari haqida gapirganda, bu turdagi hujumlar bankning yoki boshqa tizimning ishlashini to‘xtatish yoki sekinlashtirish maqsadida amalga oshiriladi. Hujumchilarning maqsadi – tizimni haddan tashqari ko‘p so‘rovlar yoki

ma'lumotlar bilan to‘ldirishdir. Bu orqali, tizimga kirish imkoniyati to‘siladi yoki xizmatlar ishlamay qoladi.

DDoS hujumlari odatda, juda ko‘p kompyuterlardan yoki qurilmalardan bir vaqtning o‘zida tizimga hujum qilish orqali amalga oshiriladi. Hujumchilarning qo‘lida bir nechta kompyuterlar yoki qurilmalar *(botnet deb ataladi)* bo‘lishi mumkin, bu esa tizimni yanada qiyinlashtiradi, chunki hujumni to‘xtatish uchun faqat bitta manba bilan kurashishning o‘zi yetarli emas.

DDoS hujumlari bankning tizimlarini ko‘p so‘rovlar bilan to‘ldirib, foydalanuvchilarning tizimga kirishini yoki operatsiyalarni amalga oshirishini imkonsiz qiladi. Masalan, bankning internet banking yoki mobil banking xizmatlari ishlamay qolishi mumkin, bu esa mijozlar uchun katta noqulayliklar yaratadi.

Malware (zararli dasturlar) hujumlari, hujumchilar tomonidan bank tizimlariga zararli dasturlarni *(viruslar, trojanlar, spyware va boshqalar)* kirgizish orqali amalga oshiriladi. Bu dasturlar bank tizimlariga kirish imkoniyatini yaratadi va shu orqali hujumchilar bank tizimini nazorat qilish yoki foydalanuvchilarning shaxsiy ma'lumotlarini o‘g‘irlash imkoniga ega bo‘lishadi.

Malware hujumlari quyidagicha ishlaydi:

1. *Zararli dasturlarni tarqatish:* Hujumchilar foydalanuvchilarga yoki bank tizimiga zararli dasturlarni yuboradilar. Bu dasturlar ko‘pincha e-pochta orqali, soxta ilovalar, yoki havolalar yordamida tarqatiladi. Foydalanuvchi bu dasturlarni yuklab olganida, ular bank tizimiga kirish imkonini beruvchi zararlanishni boshlashadi.
2. *Shaxsiy ma'lumotlarni o‘g‘irlash*: Zararli dastur foydalanuvchilarning kompyuter yoki mobil qurilmalariga kirib, ularning shaxsiy ma'lumotlarini *(parollar, kredit karta ma'lumotlari, hisob raqamlari)* o‘g‘irlaydi. Hujumchilar bu ma'lumotlardan foydalangan holda bank hisoblarini bo‘shatish yoki firibgarlik qilishlari mumkin.
3. *Tizimni nazorat qilish:* Ba'zi malware turlari bank tizimlarini yoki foydalanuvchilar kompyuterlarini to‘liq nazoratga olish imkonini beradi. Hujumchilar bu orqali tizimlarni boshqarish, operatsiyalarni amalga oshirish yoki bankning ishlashini to‘xtatish imkoniyatiga ega bo‘ladilar.

Bunday hujumlar nafaqat bank tizimining xavfsizligini buzadi, balki mijozlarning ishonchini yo‘qotishga olib keladi. Agar banklar va foydalanuvchilar zararli dasturlarga qarshi samarali choralar ko‘rmasalar, bankning obro‘si zarar ko‘rishi mumkin. Foydalanuvchilarning ma'lumotlari o‘g‘irlangan bo‘lsa, ular bank tizimiga nisbatan ishonchni yo‘qotadilar va bu bankni iqtisodiy jihatdan katta yo‘qotishlarga olib kelishi mumkin.

Shu sababli, banklar va boshqa moliyaviy institutlar malware hujumlariga qarshi kurashishda ilg‘or xavfsizlik choralarini ko‘rishlari, shu jumladan antivirus dasturlarini yangilash, tizimni muntazam ravishda tekshirish va foydalanuvchilarni ma'lumotlarini himoya qilish bo‘yicha ta'lim berish zarur.

Banklarning Kiberxavfsizlikka Qarshi Kurashdagi Chora-Tadbirlari

Ma'lumotlarni Shifrlash

Banklar o‘z mijozlarining ma'lumotlarini himoya qilish uchun eng samarali metodlardan biri sifatida ma'lumotlarni shifrlashni qo‘llamoqdalar. Shifrlash, ma'lumotlar tarmoq orqali yuborilayotganda uning o‘qilishini imkonsiz qiladi. Shu bilan birga, *SSL (Secure Socket Layer) va TLS (Transport Layer Security)* kabi protokollar foydalanuvchilarning tizimga kirishi va tranzaktsiyalarni amalga oshirishi davomida ma'lumotlar xavfsizligini ta'minlashda qo‘llaniladi.

Shifrlashning asosiy maqsadi – bank tizimiga kirgan ma'lumotlarning hech kim tomonidan o‘qib olinmasligi va ular noto‘g‘ri qo‘llanilmasligi uchun ularni himoya qilishdir. Banklar shifrlashning eng ilg‘or variantlarini joriy qilgan holda foydalanuvchi ma'lumotlarini maksimal darajada himoya qilishni maqsad qilganlar.

Ko‘p Faktorli Avtorizatsiya (MFA)

Ko‘p faktorli autentifikatsiya (MFA) texnologiyasi banklarning foydalanuvchilar hisoblarini himoya qilishda muhim rol o‘ynaydi. Ushbu tizimda foydalanuvchidan bir nechta xavfsizlik qadamlarini bajarish talab qilinadi. Masalan, foydalanuvchi tizimga parol orqali kirishi bilan birga, telefoniga yuborilgan tasdiqlash kodini ham kiritishi kerak bo‘ladi. Bunday ikki yoki undan ortiq xavfsizlik qadamlarini qo‘llash, tizimga kirishning noqonuniy bo‘lishi ehtimolini sezilarli darajada kamaytiradi.

Tarmoqni Monitoring Qilish va Xavfli Faoliyatni Aniqlash

Banklar o‘z tizimlarini har doim monitoring qilib, har qanday shubhali faoliyatni erta aniqlash va tezda javob berishga harakat qilishadi. Xavfsizlik tizimlari foydalanuvchilarning hisoblarida noxush yoki odatdagi harakatlardan farq qiladigan faoliyatni tahlil qilib, bunday holatlarni tezda aniqlaydi. Shubhali faoliyat aniqlanganda, tizim avtomatik tarzda signal yuboradi va xavf darajasi aniqlanadi.

Penetratsion Testlar va Xavfsizlik Auditi

Banklar o‘z tizimlarining xavfsizligini mustahkamlash uchun muntazam ravishda penetratsion testlar o‘tkazadilar. Penetratsion testlar – bankning tizimiga hujumchilar kabi kirib, tizimdagi zaifliklarni aniqlash va ularni tuzatishga yordam beradigan jarayon. Bu jarayonlar bank tizimlarining zaif tomonlarini aniqlash va ularga qarshi chora-tadbirlarni ishlab chiqishga yordam beradi.

Xavfsizlik auditi ham banklarning tizimlarining holatini tahlil qilish va ulardagi xavf-xatarlarni aniqlash uchun amalga oshiriladi. Auditarlar bank tizimlarini chuqur tahlil qilib, xavfsizlikni kuchaytirish bo‘yicha tavsiyalar beradi.

Foydalanuvchilarni O‘qitish va Xavfsizlik Masalalari Bo‘yicha Ta'lim Berish

Banklar o‘z mijozlarini kiberhujumlardan himoya qilish uchun xavfsizlik masalalari bo‘yicha ta'lim berishadi. Phishing hujumlari va soxta veb-saytlardan ehtiyot bo‘lish, kuchli parollarni yaratish va o‘z ma'lumotlarini himoya qilish bo‘yicha treninglar o‘tkaziladi. Foydalanuvchilarning onlayn xavfsizlikka bo‘lgan hushyorligi bankning tizimiga qarshi hujumlar xavfini kamaytiradi.

Yangi Texnologiyalar va Imkoniyatlar

Sun'iy Intellekt (AI) va Mashina O‘rganish

Banklar kiberxavfsizlikni yanada samarali ta'minlash uchun sun'iy intellekt va mashina o‘rganish texnologiyalarini joriy qilmoqdalar. AI yordamida banklar tizimdagi anomaliyalarni, noxush harakatlarni va potentsial xavflarni erta aniqlay olishadi. Sun'iy intellekt algoritmlari foydalanuvchi faoliyatini tahlil qilib, shubhali harakatlarni avtomatik tarzda aniqlashga yordam beradi.

Shuningdek, mashina o‘rganish texnologiyalari bank tizimlarida tajribalar orqali xavfsizlikni mustahkamlash va har xil turdagi kiberhujumlarni oldindan aniqlash imkoniyatlarini yaratadi.

Blokcheyn Texnologiyasi

Blokcheyn, tranzaktsiyalarni o‘zgartirib bo‘lmas tarzda saqlash imkonini beradigan texnologiya bo‘lib, u banklarning xavfsizlik choralarini kuchaytirishga yordam beradi. Blokcheynning afzalliklari shundaki, uning asosida barcha ma'lumotlar shifrlangan holda saqlanadi, bu esa hujumchilarning tranzaktsiyalarni o‘zgartirishini yoki noto‘g‘ri foydalanishini deyarli imkonsiz qiladi.

Banklar blokcheyn texnologiyasini nafaqat raqamli to‘lovlar, balki boshqa moliyaviy xizmatlar uchun ham qo‘llamoqda, bu esa tizimning xavfsizligini oshiradi.

Xulosa

Banklarning kiberxavfsizlikka bo‘lgan e'tibori zamonaviy raqamli moliya tizimlarida xavf-xatarlarning oshishi bilan yanada ortib bormoqda. Maqolada kiberhujumlar, ma'lumotlar o‘g‘irlanishi, phishing hujumlari, DDoS hujumlari va zararli dasturlar (malware) kabi xavflar bank tizimlarining xavfsizligini tahdid qilayotgan asosiy omillar sifatida ko‘rsatilgan. Bunday xavf-xatarlar bilan kurashish uchun banklar ilg‘or xavfsizlik chora-tadbirlarini, jumladan, ma'lumotlarni shifrlash, ko‘p faktorli autentifikatsiya, tarmoqni monitoring qilish va penetratsion testlar kabi texnologiyalarni joriy qilishmoqda.

Shuningdek, banklar foydalanuvchilarga xavfsizlik masalalari bo‘yicha ta'lim berish orqali kiberxavfsizlikni ta'minlashda muhim ro‘l o‘ynashadi. Yangi texnologiyalar, masalan, sun'iy intellekt va mashina o‘rganish, banklarga xavfsizlikni kuchaytirish va kiberhujumlarning oldini olishda yordam beradi. Blokcheyn texnologiyasi esa banklarning xavfsizlik choralarini yanada kuchaytirishga xizmat qiladi, chunki u tranzaktsiyalarni o‘zgartirib bo‘lmas tarzda saqlash imkonini beradi.

Maqolada ko‘rsatilgan xavfsizlik choralarining to‘liq amalga oshirilishi va banklar hamda foydalanuvchilar o‘rtasidagi hamkorlikning samarali bo‘lishi, kiberxavfsizlikni ta'minlashda muhim ahamiyatga ega. Shuning uchun banklar o‘z tizimlarini himoya qilishda nafaqat texnologiyalarni, balki foydalanuvchilarni ongli ravishda xavfsizlikka o‘rgatish va ta'lim berishni ham davom ettirishi zarur.

FOYDALANILGAN ADABIYOTLAR

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O’quv qo’llanma. – T.: «Aloqachi», 2020, 221 bet.
2. Ismoilov, U. (2023). Raqamli to‘lov tizimlari va ularning O‘zbekiston moliyaviy xizmatlariga ta’siri. O‘zbekiston moliya bozori, 14(1), 59-78.
3. “Banklar va bank faoliyati to‘g‘risida”gi qonun, 05.11.2019 yildagi O‘RQ-580-son
4. Axadjon o‘g‘li, A. A., & Tursunboy o‘g‘li, N. J. (2023). SANOATNING YAIMGA TA’SIRINI BAHOLASH. *QO ‘QON UNIVERSITETI XABARNOMASI*, 290-293.
5. Axadjon o‘g‘li, A. A. (2023). RAQAMLI IQTISODIYOTNING RIVOJLANISHDAGI O ‘RNI. *QO ‘QON UNIVERSITETI XABARNOMASI*, 271-273.
6. Axadjon o‘g‘li, A. A. (2023). ZAMONAVIY AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARINING MUAMMOLARI VA YECHIMLARI. *QO ‘QON UNIVERSITETI XABARNOMASI*, 333-338.
7. Azamjon o’g’li, U. A., & Axadjon o‘g‘li, A. A. (2023). Sun'iy intellekt va raqamli iqtisodiyot rivojlanishi. *Qo ‘qon universiteti xabarnomasi*, *1*, 73-75.
8. Tursunboy o‘g‘li, N. J., & Axadjon o‘g‘li, A. A. (2023). O ‘zbekistonning jahon savdo tashkilotiga a’zo bo ‘lish uchun uzoq yo ‘li va xitoy tajribasi. *Qo ‘qon universiteti xabarnomasi*, *1*, 43-47.
9. Ahrorjon, A., & Gafurov, X. (2023). IQTISODIY SIYOSATNING RIVOJLANISHIDA FISKAL VA PUL-KREDIT SIYOSATI. *Qo ‘qon universiteti xabarnomasi*, 310-313.

10. Otto, M., & Thornton, J. (2023). CHATGPTNING IQTISODIYOTGA TA’SIRI: SUN’IY INTELLEKTNING KASBIY MEHNAT BOZORIGA TA’SIRI. *QO ‘QON UNIVERSITETI XABARNOMASI*, *7*, 65-71.
11. Akhrorjon, A., & Oybek, A. (2023). ISLAMIC FINANCE PROBLEMS AND SOLUTIONS: Study guide. *AMAZON PUBLICATION ISBN-13: 9798863282282*, *1*, 200.
12. Akhmadjonov, O. X. (2023). ISLOMIY MOLIYA BARQARORLIK OMILLARI: EKONOMETRIK TAHLILLAR VA DALILLAR. *Educational Research in Universal Sciences*, *2*(9), 74-94.
13. Axrorjon, A., & Maxliyoxon, O. (2024). TA’LIM SIFATI OSHISHIDA JSTNING O ‘RNI. *YANGI O ‘ZBEKISTONDA IJTIMOIY-INNOVATSION TADQIQOTLAR*, *2*(1), 113-118.
14. Акабирходжаева, Д. Р., & Абдуллаев, А. А. (2024). ВЛИЯНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЧЕСКИХ ИННОВАЦИЙ НА РАЗВИТИЕ МИРОВОГО ФИНАНСОВОГО РЫНКА. *Экономика и социум*, (11-1 (126)), 729-739.
15. Akabirxodjayeva, D., & Abdullayev, A. (2024). TEXNOLOGIK INNOVATSIYALARNING JAHON MOLIYA BOZORINING RIVOJLANISHIGA TA’SIRI. *QO ‘QON UNIVERSITETI XABARNOMASI*, *13*, 89-96.
16. Akhrorjon, A., & Oybek, A. (2023). SUN'IY INTELLEKT (AI) VA ISLOM MOLIYASI. *Qo ‘qon universiteti xabarnomasi*, 188-190.
17. Keldiboyeva, Z. M. Q., & Abdullaev, A. A. O. G. L. (2022). Inklyuziv ta’limga bo’lgan ehtiyojlar va sabablar, inklyuziv ta’limga jalb qilish. *Science and Education*, *3*(11), 704-711.
18. Oybek, A., Abdullaev, A., Mavlonbekov, X., & Sharifjonov, Z. (2023). ISLOM MOLIYASIDA MUSHORAKA SHARTNOMASI. *Umumjahon fanlari bo ‘yicha ta'lim tadqiqotlari*, *2*(1), 593-599.
19. Turanboyev, B., Abdupattayev, A., & Abdullaev, A. (2023). INFLYATSIYANING QIMMATLI QOG'OZLAR DAROMADIGA TA'SIRI. *Yosh tadqiqot Jurnali*, *2*(2), 88-100.
20. Akhmadjonov, O. X. (2023). ISLOM BANK TIZIMI UCHUN SHARTNOMA HUQUQI VA ASOSIY TAMOYILLARI. *Educational Research in Universal Sciences*, *2*(5), 600-613.
21. Abdullaev, A. (2022). BOBUR VA BOBURIYLAR SULOLASINING JAHON SIVILIZATSIYASINING YANGILANISHIGA QO ‘SHGAN HISSASI. *NEW RESEARCH ON THE WORKS OF ALISHER NAVOI AND ZAHIRUDDIN MUHAMMAD BABUR*, *1*.
22. Xusanovich, A. O. (2023). MALAYZIYADA ISLOMIY MOLIYA, TO‘G‘RIDAN-TO‘G‘RI XORIJIY INVESTITSIYALAR VA IQTISODIY RIVOJLANISH O‘RTASIDAGI MUNOSABATLARNING EKONOMETRIK TAHLILI ASOSIDA

O‘ZBEKISTON UCHUN TAVSIYALAR. *QO ‘QON UNIVERSITETI XABARNOMASI*, *7*, 60-64.

23. Mulaydinov, F. (2024). Application, place and future of digital technologies in the educational system. *Nordik ilmiy-amaliy elektron jurnali*.

24. Jumanova, S. (2024). Analysis of PISA test results in Uzbekistan and prospects of preparing primary education students for PISA test. *Nordik ilmiy-amaliy elektron jurnali*.

25. Ikromjonovna, J. S., & Axadjon o‘g‘li, A. A. (2023). O ‘ZBEKISTONDA PISA TESTI NATIJALARI VA BOSHLANG ‘ICH TA’LIM O ‘QUVCHILARINI BU TESTGA TAYYORLASH ISTIQBOLLARI. *QO ‘QON UNIVERSITETI XABARNOMASI*, *9*, 159-162.

26. Turanboyev, B., & Abdullayev, A. (2023). DAVLAT, KORXONA VA TASHKILOTLAR BYUDJETINI TO ‘G ‘RI TAQSIMLASH TENDENSIYALARI. *Oriental renaissance: Innovative, educational, natural and social sciences*, *3*(4), 304-309.

27. Akhrorjon, A., & Maxliyoxon, O. (2024). IMPACT, RESULTS AND CONSEQUENCES OF WTO ACCESSION ON THE EDUCATION SYSTEM. *International Multidisciplinary Journal of Universal Scientific Prospectives*, *2*(1), 6-15.

28. Abdullaev, A., & Odilova, M. (2024). The Role of WTO in İmproving the Quality of Education. *Yosh Tadqiqotchi Jurnali*, *3*(1), 140-148.

29. Gulboy o‘g, X. U. B. (2025). AKSIYADORLIK TIJORAT BANKLARINING RIVOJLANISHIDA XALQARO STANDARTLARINING RO ‘LI. ZAMIN ILMIY TADQIQOTLAR JURNALI, 1(3), 52-56.