https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 46 | 2024

Economy and Innovation
ISSN: 2545-0573

For more information contact: editor@gospodarkainnowacje.pl

KIBERXAVFSIZLIKNI TA'MINLASHDA STRATEGIK CHORALARNING AHAMIYATI

J. B. Yo'ldoshev
Bojxona qo'mitasi bosh inspektori

ARTICLEINFO.

Kalit so'zlar: Kibermudofaa, milliy strategiya, kiberhujum, kiberxaxfsizlik, innovatsiya, standartlashtirish, fishing, kiberjinoyat, kiberhimoya, kibermakon.

Annotatsiya

Ushbu tezis orqali bugungi kunda Respublikamizda sodir bo'lgan kiberhujumlar, ularning turli sohadagi ko'rsatkichlari keltirilib o'tilgan. Bundan tashqari kiberhujumlarga qarshi Shvesariya davlati amalga oshirayotgan ishlar, ularning amaliyoti o'rganilib kiberhujumlarga qarshi kurashishda strategik choralar ko'rilishi aytib o'tilgan.

Kirish.

Bizga ma'lumki, hozirgi kunda raqamlashtirish ko'plab sohalarni qamrab olayotganligi sababli, axborot xavfsizligi sohasida ham ko'plab yangi terminlar paydo bo'lmoqda. Masalan:

Kiberjinoyat – kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi. Kompyuter jinoyat paytida maqsadli yo'naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi [1].

Kiberhujum – kompyuter axborot tizimlari, kompyuter tarmoqlari, infratuzilmalar yoki shaxsiy kompyuter qurilmalariga qaratilgan har qanday hujumkor manyovr. Hujumni amalga oshiruvchi shaxs ma'lumotlar, funksiyalarga yoki tizimni kirishini cheklangan joylariga ruxsatsiz, potensial ravishda yomon niyatda kirishga harakat qiladi [2].

Kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui [3].

Fishshing – Internetdagi firibgarliknin bir turi bo'lib, uning maqsadi foydalanuvchi maxfiy ma'lumotlariga login va parollarga kirishdir. Bunga mashhur brendlar nomidan elektron pochta xabarlarini, shuningdek, turli xizmatlar doirasidagi shaxsiy xabarlarni, masalan, banklar nomidan yoki ijtimoiy tarmoqlar ichida ommaviy yuborish orqali erishiladi.

Kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit [4].

Kiberhimoya — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma'lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui [5].

Asosiy qism.

Kiberxavfsizlik - bu dushman yoki zararli shaxs tomonidan axborot texnologiyalariga qarshi qasddan harakatlar natijasida yuzaga kelishi mumkin bo‘lgan kibermakondagi hodisalarning salbiy ta’sirini oldini olishga yoki yumshatishga yordam beruvchi texnologiyalar, jarayonlar va siyosatlarni o‘z ichiga olgan keng tushuncha. Bunga jismoniy xavfsizlik bilan bir qatorda kiberxavfsizlik, masalan, ichki tahdidlardan himoyalanish kiradi. Bu Internetning barcha darajalarini hamda ushbu infratuzilmani nazorat qiluvchi va quruvchilardan tortib, turli xil yakuniy foydalanuvchilargacha bo‘lgan tarmoqni ta’minlash va undan foydalanish bilan bog‘liq barcha ko‘plab sub’ektlarni o‘z ichiga oladi.

Ushbu keng ta’rifni hisobga olgan holda, javob berish kerak bo‘lgan savol - kiberxavfsizlik uchun kim javobgar? Unga qanday samarali kurashish kerak? Javobgarlik ko‘pincha muayyan faoliyat va kontekstga bog‘liq. Xususan, Internetning butun dunyo bo‘ylab qo‘llanilishi oxirgi foydalanuvchilarga nafaqat butun dunyo bo‘ylab ma’lumotlarga kirish, balki butun dunyo uchun o‘z ma’lumotlarini yaratish va boshqa yo‘llar bilan olish imkonini berdi. Bu ko‘p jihatdan foydalanuvchilarga kuch berdi, bu foydalanuvchilar matbuot kabi ta’sir qiluvchi shaxslarga kompensatsion ma’lumot bilan e’tiroz bildirishi mumkin bo‘lgan ko‘plab usullardan dalolat beradi. Biroq, bu Internetdagi axborot resurslarining xavfsizligi uchun mas’uliyat nafaqat kiberxavfsizlik bilan shug‘ullanadigan texnik mutaxassislarga emas, balki butun dunyo bo‘ylab foydalanuvchilar va ular ishtirok etadigan muassasalarga o‘tganligini anglatadi.

O‘zbekiston ham bundan mustasno emas, 2021 yilda davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlari va boshqa tashkilotlar faoliyatiga axborot-kommunikatsiya texnologiyalarini keng joriy etish bo‘yicha ko‘plab loyihalar amalga oshirildi. O‘zbekistonda va jahonda qo‘llanilayotgan barcha axborot-kommunikatsiya texnologiyalari va uskunalari jami kibermakondir. Bu ishlanmaning salbiy tomoni ham bor – kiberjinoyat, bu “hujumchilar”ga pul undirish va kibermakondan zararli maqsadlarda foydalanishning yangi va murakkab usullarini beradi.

Kiberxavfsizlik markazi 2021-yil uchun “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash” [6] hisobotini e’lon qildi. Unda kibermakondagi tahdidlar, ularni himoya qilish bo‘yicha tavsiyalar va bir qator statistik ma’lumotlar o‘rin olgan.

Ma’lum qilinishicha, 2021-yil holatiga ko‘ra O‘zbekistonda “.uz” milliy internet segmentida 100 015 domen ro‘yxatga olingan bo‘lib, ulardan 38 000 tasi faoldir. Faqat 14 000 faol domen xavfsizlik sertifikatiga ega.

Markaz 2021 yilda milliy segmentda 17 milliondan ortiq zararli va shubhali tarmoq faoliyati holatlarini aniqladi. Ushbu faoliyatlarning aksariyati yoki 76 foizi bot-tarmoq ishtirokchilaridir. Shuningdek, Markazning veb-ilovalarni himoya qilish tizimi yordamida Internetning milliy segmentidagi veb-saytlarga 1,3 milliondan ortiq kiberhujumlar aniqlangan va bartaraf etilgan.

“Uz” domen zonasi veb-saytlariga nisbatan kiberxavfsizlik insidentlari monitoringi natijasida 444 ta hodisa qayd etilgan bo‘lib, ularning aksariyati kontentni ruxsatsiz yuklab olish – 341 ta va bosh sahifaga ruxsatsiz o‘zgartirishlar (Deface) – 89 tani tashkil etadi. Voqealarning tahlili shuni ko‘rsatadiki, davlat sektori veb-saytlari (134 ta hodisa) xususiy sektorga (310 ta hodisa) nisbatan 3 barobar kamroq hujumga uchragan.

2021-yilda tadqiqot va ekspertiza natijasida axborot resurslari egalariga 989 ta kiberxavfsizlik zaifligi haqida xabar berilgan. Ayniqsa:

- 683 tasi o‘ta xavfli;
- 271 nafari o‘rtacha xavf ostida;
- 24 tasi past xavf ostida.

2018 va 2019 yillardagi hodisalar sonining qiyosiy tahlili ijobiy tendensiyani, ya’ni hodisalar sonining

44 foizga kamayganini ko‘rsatdi. 2019-yilda internet tarmog‘ining milliy segmenti axborot tizimlari va veb-saytlarida 268 ta hodisa (shundan 222 tasi kontentni ruxsatsiz yuklab olish, 45 tasi sayt mazmunini yo‘q qilish yoki o‘zgartirish, 1 tasi yashirin qazib olish bilan bog‘liq) aniqlangan. Aniqlangan hodisalarning umumiy soni 27 tasi hukumat veb-saytlari, 816 ta zaiflik va 132 000 ga yaqin axborot xavfsizligi tahdidlaridir.

Yuqoridagilarning barchasi O‘zbekistonda kibertahdidlar kuchayib borayotganidan dalolat beradi. Bundan xulosa qilish qiyin emaski, bugungi kunda kibermakondagi xavfsizlikka, xususan, axborot tizimlari va veb-saytlarning xavfsizlik darajasini oshirish va kiberxavfsizlikni ta’minlashga, shuningdek, foydalanuvchilarning sohadagi bilim darajasini muntazam oshirib borishga alohida e’tibor qaratish lozim. Xususan, 2022-yil 14-apreldagi O‘RQ-764-sonli “Kiberxavfsizlik to‘g‘risidagi” [7] O‘zbekiston Respublikasi qonunning maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat. Qonunda kiberxavfsizlikni ta’minlashning quyidagi asosiy prinsiplari keltirilgan:

qonuniylik;

kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;

kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi.

Shuningdek, ushbu qonunda kiberxavfsizlik sohasidagi vakolatli davlat organi, hamda uning huquq va majburiyatlari keltirib o‘tilgan.

Qonun loyihasining qabul qilinishi davlat tomonidan kiberxavfsizlikni tartibga solish, axborot tizimlari va resurslarining yaxlitligini ta’minlash, ruxsat etilmagan harakatlar, o‘chirish, o‘zgartirish, buzish, nusxa ko‘chirish, blokirovka qilish va noqonuniy aralashuvlarning oldini olishga xizmat qiladi.

Shu jihatdan, kiberxavfsizlik bo‘yicha Shvesariya davlati amalga oshirayotgan choralarni ko‘rib chiqsak. Boshqa har qanday Yevropa davlatida bo‘lgani kabi, Shveysariya siyosatida kiberxavfsizlikning ahamiyati yuqori. Shveysariya kiberxavfsizlik va kibermudofaa siyosati ustida ish hali ham davom etayotgan bo‘lsa-da, mamlakat kiberxavfsizlik bo‘yicha to‘g‘ri siyosat, rol va mas’uliyatni shakllantirish bo‘yicha katta ishlarni amalga oshirib kelmoqda.

2018 yilda qabul qilingan “Shveysariyani kiberxavflardan himoya qilish bo‘yicha Milliy strategiya” [8] Shveysariyani asosiy siyosiy hujjatidir. Strategiya o‘nta harakat yo‘nalishini belgilaydi. Maqsadlarni quyidagicha umumlashtirish mumkin: Shveysariyani kiberxavfsizlik bo‘yicha kompetensiyalarni, inqirozlarni boshqarish tuzilmalarini yaratish, barqarorlikni oshirish va xalqaro hamkorlikni rag‘batlantirish orqali ertangi kun xatarlariga qarshi turishga tayyorlash.

Strategiyaga Shveysariya kiberxavfsizlik landshaftidagi asosiy ishtirokchilar bilan uch yillik maslahatlashuvlar natijasi bo‘lgan amalga oshirish rejasi hamroh bo‘ladi. Strategiyani boshqarish markazlashtirilgan. Amalga oshirish rejasida 2018 yilgi strategiyada belgilangan o‘nta harakat yo‘nalishi bo‘yicha aniq amalga oshirish chora-tadbirlari sanab o‘tilgan. Ular quyidagilardan iborat:

1. Qobiliyat va bilimlarni shakllantirish

1. chora: Texnologik innovatsiyalar tendensiyalarini kuzatish;
2. chora: kibersohada tadqiqot va ta’limni rivojlantirish;
3. chora: kiberxavfsizlik sohasida innovatsiyalarni rag‘batlantiradigan huquqiy bazani yaratish.

2. Tahdid manzarasi

4. chora: kibertahdidlar landshaftini tahlil qilish va taqdim etish qobiliyatini takomillashtirish va kengaytirish.

3. Barqarorlikni boshqarish

5. chora: Muhim infratuzilmalarning barqarorligini oshirish;
6. chora: federal boshqaruv tarmoqlarining barqarorligini oshirish;
7. chora: axborot va tajriba almashish orqali viloyatlararo tarmoqlarning barqarorligini oshirish.

4. Standartlashtirish/tartibga solish

8. chora: tarmoqning barqarorligini oshirish uchun minimal standartlarni belgilash va joriy etish;
9. chora: kiber hodisalar haqida xabar berish majburiyati asosida ko‘rib chiqishni tuzish;
10. chora: erkin va demokratik internetni rivojlantirishni ta’minlash maqsadida Shveysariyaning internetni xalqaro boshqarishda ishtirokini kengaytirish;
11. chora: kiberxavfsizlik sohasida tartibga solishni baholash uchun ekspert guruhlarini yaratish.

5. Voqealarni boshqarish

12. chora: Milliy kiberxavfsizlik markazini davlat-xususiy sheriklik sifatida rivojlantirish;
13. chora: Milliy kiberxavfsizlik markazi barcha turdagi korxonalar uchun xizmatlar ko‘rsatadi;
14. chora: Shveysariya hukumati va boshqa vakolat markazlari o‘rtasidagi hamkorlikni rivojlantirish;
15. chora: Federal ma’muriyat doirasida kiber hodisalarni boshqarish bo‘yicha mas’uliyatni aniq belgilash jarayonini o‘rnatish.

6. Inqirozni boshqarish

16. chora: kerak bo‘lganda xususiy sektor bilan hamkorlikni rag‘batlantirish uchun kibermutaxassislarni inqirozni boshqarish bo‘limlariga integratsiyalash;
17. chora: kiberxavfsizlik bilan bog‘liq elementlarni yanada inklyuziv mashg‘ulotlarga integratsiyalashgan holda inqirozni boshqarish bo‘yicha qo‘shma mashqlarni tashkil etish va kibermashqning o‘zini tashkil etish.

7. Prokuratura

18. chora: Shveysariyadagi joriy jinoiy kiber jinoyatlar ro‘yxatini tuzish;
19. chora: turli vakolat markazlari va kiberjinoyat tergovchilarining milliy tarmog‘i o‘rtasidagi hamkorlikni kengaytirish;
20. chora: Kiberjinoyatlarni ta’qib qilish bilan bog‘liq bilimlarni shakllantirish uchun huquqni muhofaza qilish bo‘yicha ta’limni rivojlantirish;
21. chora: kiberjinoyat ishlari bo‘yicha viloyatlar o‘rtasidagi hamkorlikni kuchaytirish maqsadida yangi Kiberjinoyatchilik bo‘yicha Markaziy idorani tashkil etish uchun federal jinoiy departamentlarning mavjud tuzilmasini o‘zgartirish.

8. Kibermudofaa

22. chora: tahdidlar bo‘yicha razvedka va atributlashtirish imkoniyatlarini rivojlantirish;
23. chora: qurolli kuchlarning barcha sharoitlarda tezkor tayyorgarligini ta’minlash imkoniyatlarini rivojlantirish.

9. Xalqaro kiberxavfsizlik siyosatida Shveysariyaning faol pozitsiyasi

24. chora: Shveysariya kiberxavfsizlik bo‘yicha xalqaro forumlarning dastlabki muhokamalarida ishtirok etishi;

25. chora: kiberxavfsizlik bo‘yicha imkoniyatlar va axborot almashishni takomillashtirishga qaratilgan xalqaro hamkorlikni kengaytirish;

26. chora: kiberxavfsizlik nuqtai nazaridan tashqi xavfsizlik siyosati bo‘yicha ikki va ko‘p tomonlama muloqotlarni yo‘lga qo‘yish.

10. Jamoatchilik ta’siri va xabardorligi

27. chora: kiberxavfsizlik strategiyasining aloqa strategiyasini amalga oshirish;

28. chora: aholining kiberxavflar haqida xabardorligini oshirish.

Strategiyani o‘ziga xos tomoni u bir necha yilga mo‘ljallangan, hamda u bosqichma-bosqich har bir sohada qo‘llanila boshlanishida. O‘zbekistonda kiberxavfsizlikka qarshi kurashda esa qaysi sohada kibertahdidlar ko‘payotgan bo‘lsa o‘sha sohada amaliy ishlar ko‘proq olib boriladi. Xususan, hozirda fishshing orqali kartadagi pullarni o‘zlashtirish ko‘paygan va Kiberxavfsizlik markazi bu bo‘yicha amaliy ishlar ko‘rib, aholi bilan profilaktika tadbirlarini olib bormoqda.

Xulosa.

Respublikamizda kibertahdidlarga qarshi Strategiyani qabul qilinishi ko‘plab ijobiy natijalarni olib kelishi mumkin. Birinchidan, kiberhujumlar soni kamayadi, bosqichma-bosqich barcha sohada xavfsizlik ta’minlanadi. Ikkinchidan, kibertahdidlar manbaasini o‘rganish va bartaraf etish imkoniyati yuzaga keladi. Uchinchidan, kiberxavfsizlik sohasidagi normativ-huquqiy baza takomillashadi, kiberxavfsizlik sohasida ilmiy-texnika yutuqlariga asoslangan mahsulotlar va ilg‘or texnologiyalar joriy etiladi. Shuningdek, muhim axborot infratuzilmasi ob’ektlarining xavfsizligi ta’minlanadi.

Foydalanilgan adabiyotlar:

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime, "Cleveland, Mississippi: Anderson Publishing. https://composite-indicators.jrc.ec.europa.eu/ “Kiberxavfsizlik tog’risida”gi qonun.
2. https://csec.uz/uz/news/mahalliy-yangiliklar/-zbekiston-respublikasi-kiberkhavfsizligi-2021-yil-isoboti/.
3. https://lex.uz/uz/docs/5960604.
4. Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022(Bern:Federal IT Steering Unit FITSU,April2018), https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/(link is external).
5. Ergashev, R. X., Sh, F. S., & Xamraeva, S. N. (2011). Agricultural Economics-7 (textbook) T.
6. Эргашев, Р. Х., Хамраева, С. Н., & Файзиева, Ш. Ш. (2020). Инновационное развитие инфраструктуры сельского хозяйства: проблемы и пути его достижения. In *Феномен рыночного хозяйства: от истоков до наших дней. Партнерство в условиях риска и неопределенности* (pp. 310-319).
7. Ергашев, Р. Х., & Тайлакова, Д. Б. (2019). Економічний механізм державної підтримки малого бізнесу та приватного підприємництва в Узбекистані. *Український соціум*, (4), 124-132.
8. Эргашев, Р. Х. Зухра Джабборова Значение инновационной деятельности в туризме European Scholar Journal (ESJ) Доступно на сайте: https://www. scholarzest. com Vol. 2 Нет. 4, апрель 2021 г.
9. Эргашев, Р. Х., & Хамраева, С. Н. (2019). Совершенствавоние механизмы инновационного развития инфраструктуры сельского хозяйства. *Друкується за рішенням Вченої ради*

Державного університету «Житомирська політехніка»(Протокол № 12 від 25.11. 2019 р.) Редакційна колегія: д. е. н., проф. ВВ Євдокимов, 355.

10. Ergashev, R. H., & Khamraeva, S. N. (2012). Economics of agricultural infrastructure. *Training manual. Tashkent,"Yangi Avlod*.
11. Egamberdiyeva, S. R., Qodirov, F. I., & Shopiyev, R. R. (2022). BUXGALTERIYA HISOBINING MILLIY STANDARTLARINI MHXS GA UYG 'UNLASHTIRISH ASOSIDA TAKOMILLASHTIRISH. *Gospodarka i Innowacje.*, *24*, 353-358.
12. Эгамбердиева, С. Р. (2021). ИНВЕСТИЦИОН ФАОЛИЯТНИ РЕЖАЛАШТИРИШ ВА ЛОЙИҲАЛАРНИ АСОСЛАШДА ИННОВАЦИОН ҲИСОБ ТИЗИМИНИНГ АҲАМИЯТИ. *Журнал Инновации в Экономике*, *4*(5).
13. Rayimovna, E. S. Aralov Sabir Javli ugli.(2022). Issues of Compliance of Financial Statements with International Standards. *Journal of Corporate Finance Management and Banking System (JCFMBS) ISSN*, 2799-1059.
14. Rayimovna, E. S., & Rayimovich, S. R. (2021). Specific Features and Importance of Organization of Financial Results Accounting on the Basis of International Standards. *Academic Journal of Digital Economics and Stability*, 297-303.
15. Rayimovna, E. S. (2023). IMPROVING CAPITAL INVESTMENTS AND ASSETS ACCOUNTING AND REPORTING IN AGRICULTURE ACCORDING TO INTERNATIONAL STANDARDS. *Gospodarka i Innowacje.*, *42*, 439-446.
16. Rayimovna, E. S. (2023). NECESSARY AND IMPORTANCE OF IMPROVING ACCOUNTING AND FINANCIAL STATEMENTS. *Gospodarka i Innowacje.*, *42*, 61-66.
17. Раҳмонкул, Джалилов. "ҚЎШИЛГАН ҚИЙМАТ СОЛИҒИ БЎЙИЧА ИМТИЁЗЛАР ҲИСОБИНИ ТАКОМИЛЛАШТИРИШ." *Gospodarka i Innowacje*. (2023): 377-388.
18. Djalilov, R. H. "PROBLEMS OF CALCULATION OF VALUE ADDED TAX IN THE TAX SYSTEM OF THE REPUBLIC OF UZBEKISTAN." *Intent Research Scientific Journal* 2.3 (2023): 65-71.
19. Djalilov, Rakhmonkul Khamidovich. "QO 'SHILGAN QIYMAT SOLIG 'INING NOL DARAJALI STAVKADAGI HISOBINI TAKOMILLASHTIRISH MASALALARI." *THE INNOVATION ECONOMY* 1.04 (2023).
20. Hamidovich, Djalilov Rakhmonkul. "REGULATORY AND LEGAL FRAMEWORK FOR THE ORGANIZATION OF CAMERAL CONTROL IN THE REPUBLIC OF UZBEKISTAN AND ITS SIGNIFICANCE." *Gospodarka i Innowacje.* 30 (2022): 49-54.
21. Djalilov, Rakhmonkul Hamidovich. "The role of the cameral tax audit in the tax control of the republic of uzbekistan." *European Scholar Journal* 2.6 (2021): 11-16.
22. Djalilov, R. H. "Problems of calculation of value added tax in the tax system of the republic of Uzbekistan. Intent Research Scientific Journal, 2 (3), 65–71." (2023).
23. Ergasheva, N. (2023). MAKTABGACHA TA'LIM TASHKILOTLARIDA AUTSORSING XIZMATLARIDAN FOYDALANISH SIFATINI BAHOLASH. *Innovatsion texnologiyalar*, *51*(03), 142-148.
24. Ergasheva, N. (2023). AUTSORSING XIZMATLARIDAN FOYDALANISH MEXANIZMINING MAZMUN-MOHIYATI. *THE INNOVATION ECONOMY*, *1*(03).

25. Raxmatullayevna, E. N., & Akbarshoh, M. (2023). CHORVACHILIKNI INTENSIV RIVOJLANTIRISHDA XORIJ TAJRIBASIDAN SAMARALI FOYDALANISH. *Gospodarka i Innowacje.*, 467-472.

26. Ergasheva, N. (2023). POSSIBILITIES OF APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN TEACHING FOREIGN LANGUAGES IN UNIVERSITIES. *International Journal of Pedagogics*, *3*(05), 46-51.

27. Эргашева, Н. Р. (2023). БУХГАЛТЕРСКИЙ АУТСОРСИНГ В ШКОЛЬНЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ УЗБЕКИСТАНА. *Экономика и социум*, (10 (113)-2), 884-891.

28. Ergasheva, N. R. (2023). MAKTABGACHA TA'LIM TASHKILOTLARIDA AUTSORSING XIZMATLARI SIFATINI "AMUI" USULIDA BAHOLASH XUSUSIYATLARI. *THE INNOVATION ECONOMY*, *1*(04).

29. Xurramov, A., Xushmuradov, O., Turobov, S., Faxriddinov, B., & Namozov, B. (2023). Issues of improving cotton reform. In *E3S Web of Conferences* (Vol. 452, p. 01041). EDP Sciences.

30. Хушмурадов, О. (2023). TIJORAT BANKLARI MOLIYAVIY BARQARORLIGINI TA'MINLASH ISTIQBOLLARI. *Ижтимоий-гуманитар фанларнинг долзарб муаммолари/Актуальные проблемы социально-гуманитарных наук/Actual Problems of Humanities and Social Sciences.*, *3*(10).

31. Хужакулов, Х. Д., & Хушмурадов, О. Н. (2023). ЎЗБЕКИСТОНДА ДЕМОГРАФИК ЖАРАЁНЛАРНИНГ ЎЗИГА ХОС ХУСУСИЯТЛАРИНИНГ СТАТИСТИК ТАҲЛИЛИ. *Gospodarka i Innowacje.*, 9-18.

32. Хушмурадов, О. (2023). ҒАЛЛАЧИЛИКДА БОЗОР МЕХАНИЗМЛАРИНИ ЖОРИЙ ҚИЛИШ ЭРКИН РАҚОБАТ ГАРОВИ. *Gospodarka i Innowacje.*, 411-419.

33. Alisherovich, T. S., & Ugli, N. B. B. (2023). Internal Control in Banks. *EUROPEAN JOURNAL OF BUSINESS STARTUPS AND OPEN SOCIETY*, *3*(3), 34-39.

34. Alisherovich, T. S. (2023). IMPROVING ACCOUNTING AND ITS MAINTENANCE IN BANKS. *Gospodarka i Innowacje.*, *31*, 15-20.

35. Oman, X., & Alisherovich, T. S. (2022). THE ROLE AND IMPORTANCE OF CLUSTERS IN THE AGRICULTURAL SECTOR. *Gospodarka i Innowacje.*, *29*, 202-206.

36. Туробов, Ш. А. (2022). АЁЛЛАР МЕҲНАТИДАН САМАРАЛИ ФОЙДАЛАНИШ ИСТИҚБОЛЛАРИ. *IJTIMOIY FANLARDA INNOVASIYA ONLAYN ILMIY JURNALI*, 127-134.

37. Alisherovich, T. S. (2022). ECONOMIC CONTENT OF HOUSEHOLDS. *Gospodarka i Innowacje.*, 150-155.

38. Alisherovich, T. S., & Isoqovna, A. G. (2022). Organizing Fundamentals of Digital Audit in the International Practice. *Miasto Przyszłości*, *24*, 424-426.