KORXONA TIZIMLARDA MA'LUMOTLARNI SAQLASH VA UZATISHDA FOYDALANUVCHI MAXFIYLIGI

O.N.Bekmirzayev[1], K.Q. G'ulomova[2]

[1]Toshkent davlat iqtisodiyot universiteti dotsenti,
[2]Toshkent davlat iqtisodiyot universiteti magistri
E-mail: bekmirzayevobidjon1989@gmail.com

K E Y W O R D S

Differentsial maxfiylik, hodisa, tizim, maxfiylik, xavfsizlik va xavfsizlik protokoli.

A B S T R A C T

Ma'lumotlar oqimlarining dinamik o'zgarishi, katta hajmi va murakkab tuzilishi, ularni real vaqt rejimida tahlil qilish va himoya qilish bugungi kunda murakab jarayon. An'anaviy holatda ma'lumotlar shaxsiylikni himoya qilish modellari, masalan, foydalanuvchi ma'lumoti shaxsiyligi, ishonchli serverlar yoki kompaniyalar tomonidan ishlatilishini talab qiladi, bu esa oqimlarni himoya qilishda noaniqlikni oshiradi. Ushbu maqolada ma'lumotlarni saqlash va uzatishda foydalanuvchi maxfiyligi va w-hodisasi shaxsiylik asosida ma'lumotlar oqimlari uchun yangi shaxsiylikni himoya qilish protokoli taklif qilinadi, bu vaqt o'tishi bilan yangilangan statistikalarni olishni imkonini beradi va uchinchi tomonlar ishonchsiz bo'lsa ham ma'lumotlar almashuvni ishlashni davom ettiradi. Foydalanuvchi real vaqt rejimida ma'lumotlar oqimlarini yig'ish uchun ishchi oynasini (sliding window) ishlatadi, muhim o'zgarishlarning yuzaga kelishini aniqlaydi, eng so'nggi ma'lumotlar taqsimoti tendensiyasini o'rganadi va buzilgan ma'lumotlar oqimlari hisobotini o'z vaqtida chiqaradi. Ushbu protokol tasdiqlangan shaxsiylikni himoya kafolatini taqdim etadi, hisoblash va saqlash xarajatlarini kamaytiradi va qiymatli statistik ma'lumotlarni taqdim etadi. Mavjud ma'lumotlar to'plamlaridagi tajriba natijalari ko'rsatadiki, taklif qilingan usul ma'lumotlar oqimlarining shaxsiyligini himoya qiladi va shu bilan birga mavjud statistik ma'lumotlarni taqdim etadi.

I. Kirish

Korxona tizimlarda ma'lumotlarni saqlash va uzatishda foydalanuvchi maxfiyligi zamonaviy IT infratuzilmalarning eng dolzarb masalalaridan biridir. Internetga ulangan korxonalar sonining oshishi va ularda katta hajmdagi konfidensial ma'lumotlar saqlanishi ma'lumotlarni himoya qilish usullarini takomillashtirishni talab qilmoqda. Foydalanuvchi maxfiyligi nafaqat ichki tizimlar, balki uchinchi tomon xizmatlari bilan o'zaro munosabatda ham katta ahamiyat kasb etadi.

Korxona tizimlarda ma'lumotlarni saqlash va uzatishda muhim jihatlari:

- Foydalanuvchi ma'lumotlarini himoya qilish usullari: shifrlash (encryption), farqlik shaxsiyligi (differential privacy), va autentifikatsiya texnologiyalari;
- Ma'lumotlarni uzatish xavfsizligi: ma'lumotlar transport protokollari (masalan, TLS/SSL) va xavfsiz kanallar orqali uzatish;
- Maxfiylikni ta'minlashdagi dolzarb muammolar: ruxsatsiz kirish, ma'lumotlar buzilishi, va ichki foydalanuvchilar tomonidan amalga oshiriladigan xavflar;
- Huquqiy talablar: GDPR, HIPAA, va boshqa global maxfiylik reglamentlarining korxona tizimlariga ta'siri.
- Korxona tizimlarda ma'lumotlarni saqlash va uzatishda quyidagi texnologiyalar alohida ko'rib chiqiladi:
- Mahalliy farqlik shaxsiyligi (Local Differential Privacy): Foydalanuvchi ma'lumotlarini o'zgartirish orqali ular himoyasini ta'minlash;
- Shifrlash algoritmlari: AES va RSA texnologiyalarining ma'lumotlarni himoyalashdagi roli;
- Zero Trust modeli: Korxona ichidagi barcha foydalanuvchilar va tizimlarga nisbatan ishonchsizlik tamoyiliga asoslangan xavfsizlik strategiyasi;
- Xavfsiz ma'lumotlar uzatish: VPN, TLS, va shifrlangan tarmoqlarni qo'llash.

Foydalanuvchi maxfiyligini ta’minlash korxona tizimlarining uzluksiz ishlashini, mijozlar ishonchini va xalqaro standartlarga mosligini ta’minlaydi. Zamonaviy texnologik yechimlardan foydalanish nafaqat ma’lumotlarning xavfsizligini oshiradi, balki foydalanuvchilarning ma’lumotlar uzatishdagi risklarini ham kamaytiradi. 5G texnologiyasining rivojlanishi bilan aqlli qurilmalar va sensorlar tobora ko‘proq dinamik ma’lumotlar ishlab chiqarmoqda, bu ma’lumotlarg ma’lumot oqimi (data stream) deb ataladi. Oqim ma’lumotlarini real vaqt rejimida tahlil qilish muhim hodisalarni tushunish uchun qimmatli ma’lumotlarni olish imkonini beradi[1]. Shu sababli, bu texnologiya turli sohalarda keng qo‘llanilmoqda, masalan, mobil olomonni kuzatish [2], transport oqimlari xizmatini monitoring qilish [3] va ijtimoiy tarmoqdagi nuqtalar va harakat markazlarini kuzatish [4]. Ma’lumot xizmatlarini taqdim etuvchilar real vaqt rejimida ma’lumot oqimlarini to‘playdi, bu ma’lumotlarga oid statistikalarni e’lon qiladi, va ularni qiziqqan uchinchi tomonlar bilan ulashib, tahlil qilib, xizmat sifatini yaxshilashga yordam beradi [5].

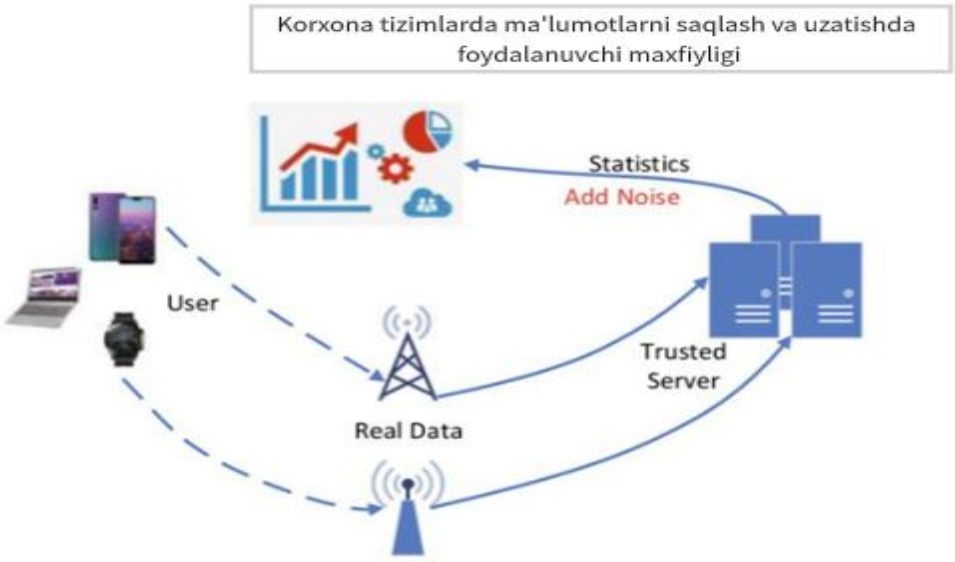
Biroq, ushbu jarayonda potentsial maxfiylik xavflari mavjud. Ishonchsiz uchinchi tomonning aralashuvi sababli, buzg‘unchi bir foydalanuvchining bir nechta vaqt belgilari (timestamp) bo‘yicha asl ma’lumotlarini farqlash hujumi orqali so‘rab olish mumkin, bu esa foydalanuvchining ma’lumot izini olishga va uning maxfiy axborotini oshkor qilishga olib kelishi mumkin [6]. Yaqinda olib borilgan tadqiqotlar [4] shuni ko‘rsatdiki, foydalanuvchining mobil yo‘nalishi mobil telefon operatorlaridan olingan foydalanuvchining mobil ma’lumotlaridan juda o‘ziga xos bo‘ladi. Hatto desensitizatsiya qilingan ma’lumotlar to‘plami ozgina anonim axborot taqdim etsa ham, bu ma’lumotlar tegishli orqa fond ma’lumotlari bilan bog‘lanib, belgilangan foydalanuvchiga ulanib qolishga imkon berishi mumkin. Shunga o‘xshash bir qator tadqiqotlar shuni ko‘rsatadiki, shaxsiy ma’lumotlar oqimining maxfiyligi katta xavf ostida, shuning uchun ma’lumotlar oqimi maxfiyligini to‘plash va chiqarish mexanizmlarini tadqiq qilish va rivojlantirish juda muhimdir. Ammo real vaqtda, qaytarib bo‘lmaslikda va ma’lumotlar oqimining katta hajmida o‘ziga xos qiyinchiliklar mavjud.

Differentsial maxfiylik (Differential privacy – DP) [6] - keng qo‘llaniladigan shaxsiylikni himoya qilish modeli bo‘lib, qat’iy shaxsiylik kafolatini va nazariy isbotni taqdim etadi, shuningdek, buzg‘unchining soxta ma’lumotlarini hisobga olishni talab qilmaydi. Farqlik shaxsiyligi bilan ma’lumotlarni tadbiq etishning keng tarqalgan usullaridan biri – ma’lumotlarni taqdim etishdan oldin buzish va statistik tahlil va ma’lumotlar ishlanish jarayonida shaxsiy ma’lumotlarni yashirishdir. Hozirgi kunda farqlik shaxsiyligi modeli bo‘yicha tadqiqotlar asosan statik holatga qaratilgan, ammo real vaqt ma’lumotlari dinamik holatda to‘planadi va tadqiq etiladi [5]. Farqlik shaxsiyligi modelining markazlashgan interaktiv holatida ishonchli nazoratchilar turli entitiyalardan sezgir ma’lumotlarni yig‘adi, aniq shovqin qo‘shadi va keyin yakuniy natijalarni ma’lumotlar tahlilchilariga ulashadi. Model 1-rasmda ko‘rsatilgan. Dwork va boshqalar [7] uzluksiz ma’lumotlar to‘plami uchun ikki xil shaxsiylik sxemasini taklif qilishdi: hodisa darajasidagi va foydalanuvchi darajasidagi shaxsiylik. Hodisa darajasidagi shaxsiylik ma’lumotlar oqimidagi bitta vaqt belgisida foydalanuvchining shaxsiyligini himoya qiladi, ammo foydalanuvchining shaxsiyligini butun ma’lumotlar oqimida himoya qilmaydi; foydalanuvchi darajasidagi shaxsiylik butun ma’lumotlar oqimiga shovqin qo‘shishni talab qiladi, bu esa uzoq muddatda ma’lumotlarning foydaliligini kamaytiradi.

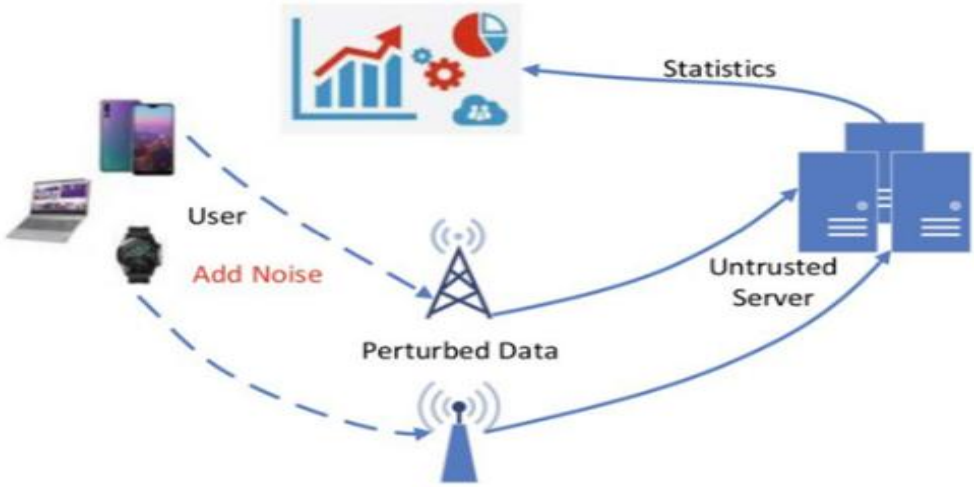
Ushbu modelda ishonchli ma’lumotlar mas’ulining mavjudligi talab etiladi, ammo agar mas’ul ishonchli bo‘lmasa, uchinchi tomon tomonidan maxfiylikning buzilishi xavfi paydo bo‘ladi. Buzg‘unchi esa takroriy so‘rovlar orqali ma’lumotlar mas’ulining asl ma’lumotlaridan bir qismini olish va foydalanuvchining maxfiyligini aniqlash imkoniyatiga ega bo‘ladi. Mahalliy differentsial maxfiylik (LDP) [8] - differentsial maxfiylikning taqsimlangan varianti bo‘lib, bu model ishonchli ma’lumotlar mas’uliga ehtiyoj sezmaydi. Foydalanuvchilar o‘zlarining shaxsiy ma’lumotlarini yuborishdan oldin, ma’lumotni lokal qurilmada buzib, shovqin qo‘shilgan maxfiylik hisobotlarini markazlashtirilgan model ostida maxfiylik buzg‘unchilariga qarshi himoya qilish uchun yuboriladi. Bu model 2-rasmda ko‘rsatilgan. Hozirda mahalliy

differentsial maxfiylik modeli bo‘yicha tadqiqotlar asosan bitta ma’lumotni chiqarishga qaratilgan [3], ammo LDP modeli murakkab real vaqt ma’lumotlarini qayta ishlashda qiyinchiliklarga duch keladi. Ma’lumotlar oqimi rivojlanishi bilan hisoblash quvvati va saqlash joyi iste’moli ortadi va maxfiylik byudjeti asta-sekin kamayadi.

An’anaviy ma’lumotlarni yig‘ish bilan solishtirganda, ma’lumotlar oqimlarining uzunligi va mazmuni dinamik tarzda o‘zgaradi, ma’lumot hajmi juda katta va ma’lumot turlari murakkab. Mahalliy differentsial maxfiylik modeli ostida oqim maxfiyligini qanday himoya qilish masalasiga yo‘naltirilgan holda, mahalliy differentsial maxfiylik va W-hodisa maxfiylik [8] asosida Mahalliy farqli maxfiylikka asoslangan oqim (LDPS -Locally Differential Private Streaming) protokolini taklif qilamiz. LDPS protokoli ma’lumotlar oqimining turiga qarab statistikalarni olish uchun turli algoritmlarni tanlaydi. Yig‘ilgan ma’lumotlar oqimlari real vaqt rejimida raqamli atributlar bo‘lsa, masalan, harorat va namlik, uzunlik va kenglik, yurak urishi va hokazo, o‘rtacha qiymatni hisoblanadi [9]; agar ma’lumotlar oqimi real vaqt rejimida tasniflangan atributlardan iborat bo‘lsa, masalan, foydalanuvchining default brauzeri, qidiruv tizimi sozlamalari va eng ko‘p ishlatilgan emojilar yoki so‘zlar [10], tezlikni baholashni amalga oshiramiz va og‘ir vaznli elementlarni aniqlaymiz [11]. Agar ma’lumot turlari aralash bo‘lsa, turli protokollar qo‘llaniladi va har xil atributlar bilan ma’lumotlar ishlanadi.



1-rasm. Maxfiylikni himoya qilishning differentsial modeli



2-rasm. Maxfiylikni himoya qilishning mahalliy differensial modeli

Asosiy hissa qo‘shishlar:

1. Mahalliy differentsial maxfiylikni joylashtirish orqali shaxsiy foydalanuvchi ma’lumotlarining qurilmadan chiqib ketishini oldini olish;

2. Taklif qilingan protokol ma’lumotlar oqimiga kuchliroq maxfiylik kafolatini taqdim etadi va buzg‘unchilarga maxfiylikni buzishning imkoniyatlarini kamaytiradi, shu bilan birga qimmatli statistik ma’lumotlarni himoyalaydi.

Ishonchsiz serverlar muammosini hal qilish maqsadida, ko‘plab olimlar va tadqiqotchilar mahalliy farq xususiyati (local differential privacy) modeli doirasida tadqiqot ishlarini olib bormoqda, ya’ni har bir shaxsiy yarim tayyor ma’lumot, mijozdan serverga yuborilishidan oldin buziladi. Biroq, taklif qilingan mexanizm tasodifiy ravishda k ta atributni buzish uchun tanlaydi, bu ba’zi amaliy ilovalarda realistik bo‘lmasligi mumkin. Mutaxassis va boshqalar [12] mahalliy farq xususiyati yordamida ishonchli ma’lumotlari oqimi uchun mexanizm ishlab chiqdilar. Bundan tashqari, bu mexanizmlar buyruq tartibida va tartibsiz atributlarni ajratib ko‘rsata olmaydi.

Yuqorida aytib o‘tilgan mexanizmlar har bir vaqt markazida xususiylik byudjetini ehtiyotkorlik bilan taqsimlaydi. Biroq, hatto nisbatan qisqa davrda ham, takrorlanadigan farq xususiyati hisoblashlar xususiylik yo‘qotilishini katta qiymatga oshirishi mumkin, shuning uchun xususiylik byudjetining yo‘qolishini kamaytirish uchun moslashuvchan siqish mexanizmi zarur.

Tajriba sozlamalari

Ma’lumotlar to‘plami. uchta jamoat ma’lumotlar to‘plamini tajriba ma’lumotlar to‘plamlari sifatida tanlash.

1-jadval

Tajriba ma’lumotlar to‘plamlari

Ma’lumotlar to‘plami	IPUMS	Twitter kundalik faoliyatlari	Gaz sensori
Namunalar soni	1 000 000	60 093 175	919 438
Soha o‘lchami/o‘rtacha qiymat	78	635	27.1767, 57.5680

Ushbu holatda 2017-yilgi Integratsiyalashgan Jamoat Mikrodata Seriyalari (IPUMS) [1] ma’lumotlar to‘plamini tanladik va undagi yosh atributini tanlab oldik, bu atributda 25 ta ma’lumot kategoriyasi mavjud. Ma’lumotlar to‘plamidan 1% ni tanlab, birinchi millionta ma’lumotni tajriba ma’lumotlari sifatida olib, kategorik atribut sifatida ishlatdik.

Twitter kundalik faoliyatlari [13] - bu Microsoft Research tomonidan taqdim etilgan ma’lumotlar to‘plami bo‘lib, unda Twitter foydalanuvchilarining har kuni, har bir mahalliy bo‘yicha faoliyat davrlari keltirilgan. Foydalanuvchi 500,000 ta hodisani tanlab, har bir mahalliy atributini kategorik atribut sifatida tajriba ma’lumotlari sifatida ishlatildi.

Gas-sensor ma’lumotlar to‘plami [14] - bu 8 ta MOX gaz sensori va bir dona harorat va namlik sensoridan iborat gaz sensori massividan olingan yozuvlarni o‘z ichiga oladi. Foydalanuvchi namlik va harorat atributlarini sonli atributlar sifatida tajriba ma’lumotlari sifatida ishlatildi.

Ma’lumotlar to‘plamlarining namuna soni, soha o‘lchamlari yoki o‘rtacha qiymatlari 1-jadvalda ko‘rsatilgan.

Tajriba holati. Ushbu tajribalar Python 3.7 versiyasida, NumPy va xxhash kutubxonalari yordamida amalga oshirildi va Intel Core i7-7700HQ CPU hamda 16 GB RAMga ega kompyuterda bajarildi. Har bir tajriba natijalariga tasodifiy omillarning ta’sirini kamaytirish maqsadida 100 marta takrorlandi.

2-jadvalda ma’lumotlarni saqlash va uzatish jarayonida xavfsizlik va maxfiylikka ta’sir qiluvchi risklar va ularning tahlili keltirilgan.

2-jadval

Ma’lumotlarni saqlash va uzatish jarayonida xavfsizlik va maxfiylikka ta’sir qiluvchi risklar

Jarayon	Risk turi	Tavsif	Ta’sir darajasi	Yuzaga kelish ehtimoli	Oldini olish choralari
Ma’lumotlarni saqlash	Ruxsatsiz kirish	Tizimga ruxsatsiz shaxslarning kirishi, maxfiy ma'lumotlarning oshkor bo'lishi.	Yuqori	O‘rta	Tizimga kirishni autentifikatsiya va roli asosida boshqarish.
	Ma’lumotlarning buzilishi	Ichki yoki tashqi tahdidlar tufayli ma’lumotlarning yo‘qotilishi yoki o‘zgartirilishi.	Yuqori	O‘rta	Zaxira nusxalarni yaratish, ma’lumotlarni shifrlash.
	Ichki xodimlar tahdidi	Xodimlarning noto‘g‘ri yoki zararli xatti-harakatlari.	Yuqori	Past	Xodimlarning kirish huquqlarini cheklash va nazorat qilish.
	Tizimdagi zaifliklar	Dasturiy ta’minotdagi yoki apparatdagi xavfsizlik nuqsonlari.	Yuqori	Yuqori	Dasturiy ta’minotni muntazam yangilash va xavfsizlik sinovlari.
Ma’lumotlarni uzatish	Ma’lumotlarni tinglash	Tarmoqqa ruxsatsiz ulanish orqali ma’lumotlarning ushlab qolinishi.	Yuqori	Yuqori	Shifrlash protokollari (masalan, TLS/SSL) ni qo‘llash.
	O‘g‘irlik	Uzatilayotgan ma’lumotlarning uchinchi tomon tomonidan ushlab qolinishi.	Yuqori	O‘rta	VPN va xavfsiz tarmoq kanallarini qo‘llash.
	Ma’lumotlarning o‘zgartirilishi	Uzatilayotgan ma’lumotlarga shaxslarning zararli ta’siri.	Yuqori	O‘rta	Ma’lumotlar yaxlitligini tekshirish mexanizmlarini joriy qilish (hashing).
	Tashqi hujumlar	DDoS yoki MITM (Man-In-The-Middle) kabi kiberhujumlar.	Yuqori	O‘rta	Tarmoqlararo ekran, IDS/IPS tizimlarini qo‘llash.

Ushbu jadvalda ta’sir darajasi va yuzaga kelish ehtimoli quyidagicha darajalarga ajratiladi.

- Ta’sir darajasi: Riskning tizimga yetkazadigan zarar darajasi: Yuqori, O‘rta, yoki Past.

- Yuzaga kelish ehtimoli: Riskning qanchalik tez-tez sodir bo'lish ehtimoli.
- Oldini olish choralari: Risklarni minimallashtirish yoki bartaraf etish uchun qo‘llaniladigan texnologik va tashkiliy yechimlar.

II. Xulosa

Ushbu maqola ma’lumot oqimlarini maxfiylikni himoya qilishga qaratilgan. Ishonchsiz uchinchi tomonlar bitta foydalanuvchining bir nechta vaqt tamg‘alari (timestamps) bo‘yicha asl ma’lumotlarga so‘rov yuborish orqali foydalanuvchining maxfiyligini buzishi mumkin, shu bilan birga hozirgi mahalliy differentsial maxfiylik protokollari ma’lumot oqimlarini yaxshi boshqara olmaydi. Biz mahalliy differentsial maxfiylikka ega oqim protokolini taklif qilamiz, bu nafaqat oqim maxfiyligini himoya qilish, balki yuqori foydalilikni, kamroq saqlash va hisoblash quvvati sarfini ham ta’minlaydi. Taklif etilgan metod w-hodisa maxfiylikni ta’minlovchi slaydli oynadan foydalanadi va real vaqt rejimida barqaror kichik oqimlarni va muhim harakatlarni topishga imkon beradi. Eksperiment natijalari taklif etilgan protokol yuqori foydalilikka ega ekanligini, sonli va kategorik atributlar uchun mosligini, hamda turli taqsimotlar va oqim o‘lchamlari ostida o‘z foydaliligini saqlab qolishini ko‘rsatadi.

III. Foydalanilgan adabiyotlar

1. Bekmirzaev, O., & Shirinov, B. (2024, May). An algorithm for viewing node state events under attack for information systems. In AIP Conference Proceedings (Vol. 3147, No. 1).
2. Bekmirzaev, O., & Samarov, H. (2024, May). A method of evaluating the effectiveness of information system protection. In AIP Conference Proceedings (Vol. 3147, No. 1).
3. B. O. Nuralievich, M. B. Boltaevich and B. U. Bahrom Ugli, "The Procedure for Forming a List of Sources of Attack in the Information System," 2022 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2022, pp. 1-4.
4. B. O. Nuralievich and M. B. Boltaevich, "Method of Detection and Elimination of Tracks of Attacks in the Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2021, pp. 1-2.
5. Muminov B., Bekmirzaev O. Classification and analysis of network attacks in the category of “denial of service” information system //central asian journal of education and computer sciences (CAJECS). – 2022. – Т. 1. – №. 1. – С. 7-15.
6. Muminov B., Bekmirzaev O. Structure and algorithms of online discussion information system //Scientific Collection «InterConf». – 2022. – №. 114. – С. 373-384.
7. Axmedova N., Bekmirzaev O. Analysis of methods of fighting against network attacks of the “denial of service” category on information systems //central asian journal of education and computer sciences (CAJECS). – 2022. – Т. 1. – №. 5. – С. 17-23.
8. Bekmurodov O., Usmanbayev D., Eshonqulov N. Kompyuter tarmoqlarini ddos hujumlaridan himoya qiluvchi dasturiy vositalarning qiyosiy tahlili // DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 2. – С. 46-50.
9. Bekmirzayev O. Algorithm for Constructing and Configuring Parameters of a Model for Searching for Traces of Attacks in an Information System //DTAI–2024. – 2024. – Т. 1. – №. DTAI. – С. 171-174.
10. Bekmirzayev O., Muminov B. The Role and Application of Artificial Intelligence in Identifying Threats to Information Systems //DTAI–2024. – 2024. – Т. 1. – №. DTAI. – С. 85-90.
11. Бекмирзаев О., Турсунов Ж. Алгоритмы системы одностороннего межсетевого взаимодействия и система обнаружения вторжений //Digital Transformation and Artificial Intelligence. – 2023. – Т. 1. – №. 4. – С. 135-145.
12. Bekmirzayeva M. Vizuallashtirish tizimlarida yomg ‘ir va qor muammolarini tasvirga dastlabgi ishlov berish yordamida bartaraf etish // Digital Transformation and Artificial Intelligence. – 2024. – Т. 2. – №. 1. – С. 120-124.

13. Bekmirzayev O., Sabirov X. “Kompyuter arxitekturasi” fanini o‘qitish samaradorligini oshirishda zamonaviy pedagogik texnologiyalarning interfaol usullaridan foydalanish //Science and innovation. – 2023. – Т. 2. – №. Special Issue 14. – С. 549-551.
14. Samarov, H. K., & Bekmirzayev, O. N. (2023). Masofaviy o‘qitish tizimlarida mavjud risklar va ularni minimallashtirish istiqbollari. Research and Education, 2(4), 146-155.
15. Бекмирзаев О. Муассаса ахборот тизимларида ҳужум изларини таснифлашда мослаштирилган нейро–норавшан тизими //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2023. – Т. 1. – №. 2. – С. 28-32.
16. Турапов У. У., Бекмирзаев О. Н. Системный подход при обеспечении информационной безопасности в информационно-библиотечных сетях //Информатика: проблемы, методология, технологии. – 2015. – С. 219-224.
17. Bekmurodov O. Ахборот тизимларида ҳужум манбалари рўйхатини шакллантириш процедураси //Digital Transformation and Artificial Intelligence. – 2023. – Т. 1. – №. 3. – С. 129-136.
18. Bekmirzayev O. N., Bekmirzayeva M. S. Recognize faces by the selecting degree of security //Информатика: проблемы, методология, технологии. – 2016. – С. 3-7.
19. Мўминов Б., Бекмирзаев О. Построение узлов о событиях под влиянием атаки в информационной системе //Scientific Collection «InterConf». – 2022. – №. 114. – С. 388-396.
20. Ташев К. А., Бекмирзаев О. Н. К вопросу анализа проблем информационной безопасности //Информатика: проблемы, методология, технологии. – 2015. – С. 211-214.