DDOS-HUJUMLARNING OLDINI OLISHDA BLOCKCHAIN TEXNOLOGIYASINING IMKONIYATLARINI TAHLILI

Xabibullayev Jahongirbek Doniyorbek o‘g‘li

Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti,

e-mail: xabibullayevj9@gmail.com

Annotatsiya: *Maqola blockchain texnologiyasini o‘rganishga bag‘ishlangan bo‘lib, u nafaqat axborot tizimlarida ma’lumotlarni saqlash va uzatishni ta’minlaydi, balki ularning xavfsizligini ham kafolatlaydi. Blockchain o‘zining markazlashmagan tabiati va ma’lumotlarni kriptografik himoya qilish qobiliyati tufayli DDoS hujumlarining oldini olish uchun kuchli vositaga aylanishi mumkin. Taqsimlangan tarmoqlar va blockchain texnologiyasidan foydalangan holda DDoS hujumlariga qarshi himoya mexanizmi onlayn xizmatlar va veb-ilovalarning xavfsizligi hamda barqarorligini ta’minlashga innovatsion yondashuvni ifodalaydi. Maqolada blockchain texnologiyasining DDoS hujumlarining oldini olishdagi qo‘llanilishi ko‘rib chiqilgan.*

Kalit so‘zlar: *taqsimlangan tizimlar, taqsimlangan reyestr texnologiyalari, axborot xavfsizligi, to‘lov xavfsizligi, blockchain, DDoS-hujumlar*

Blockchain texnologiyasining o‘zgarmaslik, markazlashmaganlik va yaxlitlik kabi xususiyatlari uning barqarorligini ta’minlaydi. Ushbu texnologiya turli sohalarda qo‘llanilmoqda. Blockchain asosidagi tizimlardan tahdidlarni aniqlash uchun foydalanish orqali tahdidlarni samarali aniqlash va ularga javob berish mumkin. Shu tariqa, blockchain texnologiyalaridan foydalangan holda DDoS hujumlarining oldini olishning samarali usullari amalga oshirilishi mumkin.

Ishda blockchain texnologiyasining taqsimlangan tizimlarda ma’lumotlarni saqlash funksiyasini ta’minlovchi tayyor yechimlari tahlil qilingan. Mazkur maqolada mualliflar blockchain asosidagi DDoS himoya yechimlarini tadqiq qilganlar. Ish davomida texnologiyaning afzalliklari shakllantirilib, mavjud DLT-yechimlari tahlil qilingan va taqsimlangan reyestr texnologiyasiga asoslangan, SIEM tizimlari bilan integratsiyalash imkoniyatiga ega innovatsion yechimlarni ishlab chiqish zarurati xulosalangan.

Axborot xavfsizligi muammosi turli axborot tizimlarida aylanib yuruvchi ma’lumot hajmining jadal o‘sishi fonida tobora dolzarb bo‘lib bormoqda. Axborot xavfsizligi masalalarini hal etishda kompleks yondashuv zarurati nafaqat hujumlar sonining ortishi, balki ularning murakkabligi oshishi bilan ham bog‘liq bo‘lib, bu esa zamonaviy avtomatlashtirilgan monitoring va xavfsizlik nazorati vositalaridan foydalanishni talab qiladi.

Bugungi kunda eng istiqbolli yo‘nalishlardan biri bu bank xizmatlari sohasida tranzaksiyalar xavfsizligini oshirish va ma’lumotlarni saqlashdir. Raqamli to‘lov usullarining kengayishi to‘lov xavfsizligini ta’minlash zaruratini oshirib, mijoz ma’lumotlari va tranzaksiyalarining maxfiyligini himoya qilish, ma’lumotlarning ruxsatsiz foydalanishi va o‘zgartirilishining oldini olishga yo‘naltirilgan choralarga bo‘lgan ehtiyojni kuchaytiradi. Markaziy bank ma’lumotlariga ko‘ra, 2023 yilda bank o‘tkazmalari va to‘lovlar jarayonida mijozlarning mablag‘larini o‘zlashtirish darajasi 11% dan oshdi.

Moliya sohasida ma’lumotlarni saqlash va uzatish xavfsizligini ta’minlashning istiqbolli yechimlaridan biri taqsimlangan reyestr texnologiyalaridir. Blockchain texnologiyasi aslida har bir tranzaksiya haqida ma’lumotlar bloklar shaklida qayd etilib, kriptografik usullar orqali o‘zaro bog‘langan taqsimlangan ma’lumotlar bazasidir. Markazlashmaganlik va kriptografik mexanizmlar axborot xavfsizligining muhim jihatlari bo‘lmish

ma’lumotlarning yaxlitligi va axborotga doimiy kirish imkoniyatini ta’minlashga yordam beradi.

Taqsimlangan xizmatni rad etish (DDoS) hujumlari onlayn xizmatlar va korxonalar uchun jiddiy tahdid hisoblanadi, chunki ular axborot tizimini ortiqcha so‘rovlar bilan yuklab, tizim samaradorligining pasayishiga yoki butunlay ishdan chiqishiga olib kelishi mumkin. Blockchain texnologiyasidan foydalanish DDoS hujumlarining ehtimolini kamaytirishga yordam beradi:

- blockchain tarmoqlarining markazlashmaganligi markaziy DDoS hujumlarining samaradorligini pasaytiradi;
- blockchain tranzaksiyalarining shaffofligi va yaxlitligi tarmoq faoliyatidagi anomaliyalarni aniqlash imkonini beradi.

Shu tariqa, DDoS hujumlarini erta bosqichlarda aniqlash va oldini olish imkoniyati yuzaga keladi.

Markazlashgan va taqsimlangan dasturiy tizimlar

Dasturiy tizimlar ichki arxitekturasiga qarab ikki asosiy turga bo‘linadi: markazlashgan va taqsimlangan tizimlar. Markazlashgan tizimlar odatda yagona boshqaruv yoki ma’lumotlar saqlash nuqtasiga ega bo‘lib, barcha foydalanuvchilar va tizim komponentlari ushbu markazga axborot olish yoki operatsiyalar bajarish uchun murojaat qiladi.

Taqsimlangan tizimlar esa markazlashmagan arxitekturaga asoslanib, ma’lumotlar turli tugunlar orasida taqsimlanadi va har bir tugun o‘zining alohida vazifasini bajaradi. Bunday tizimlarning asosiy afzalliklari quyidagilardan iborat:

- **Masshtablanish** – tarmoq hajmi ortgani sari tizim unumdorligini oshirish imkoniyati;
- **Tarmoqni kengaytirish** – qo‘shimcha tugunlar qo‘shish orqali tizimni rivojlantirish;
- **Ishonchlilik** – bitta tugunning ishdan chiqishi butun tizimga ta’sir ko‘rsatmaydi.

Shu bilan birga, taqsimlangan tizimlarning kamchiliklari ham mavjud:

- **Murakkablik** – ishlab chiqish va sozlash jarayoni ko‘proq resurs talab qiladi;
- **Yuqori xarajatlar** – bunday tizimlarni ishlab chiqish va qo‘llab-quvvatlash ko‘pincha qimmatga tushadi.

Markazlashgan yoki taqsimlangan arxitektura o‘rtasidagi tanlov dasturiy ta’minotga qo‘yilgan talablar, foydalanuvchilar soni, yechilishi kerak bo‘lgan muammolar murakkabligi, ishlash samaradorligi hamda huquqiy va normativ cheklovlarga bog‘liq. Ba’zi holatlarda **gibrid yondashuv**dan foydalanish maqsadga muvofiq bo‘lishi mumkin, ya’ni har ikki turdagi tizimlarning afzalliklarini birlashtirib, ularning kamchiliklarini minimallashtirish.

Gibrid arxitektura misollaridan biri **markazlashgan piring tarmoqlari** bo‘lib, bu tarmoqlarda barcha ishtirokchilar tizim tomonidan taqdim etilgan bir xil funksiyalardan foydalanish va teng darajada javobgarlikni bo‘lishish imkoniyatiga ega. Bunday tugunlar kirish nuqtalari o‘rtasida aloqani ta’minlab, foydalanuvchilarni muvofiqlashtirish uchun ishlatiladi. Piring tizimlaridan foydalanish to‘lov tizimlari, ma’lumotlar yaxlitligini monitoring qilish va maxfiylikni ta’minlash kabi jarayonlarni tezlashtirish va soddalashtirishga xizmat qiladi. Bunday yondashuv yuqori hisoblash quvvatiga, ishonchlilikka ega bo‘lib, xarajatlarni kamaytirish bilan birga tizim ichidagi koordinatsiyani yaxshilash imkonini beradi.

Taqsimlangan reyestr texnologiyasi

Taqsimlangan reyestr texnologiyasi – bu ma’lumot almashinuvi va saqlashni tashkil etish usuli bo‘lib, unda har bir tugun reyestrning joriy holatining mahalliy nusxasiga ega bo‘ladi. Tranzaksiyalarni yaratish jarayonida asosiy element **konsensus** bo‘lib, uning xavfsizligi ma’lumotlarning xesh-funksiyasini hisoblash va kriptografik algoritmlarga asoslanadi.

Konsensus mexanizmlari ma’lumotlar yaxlitligi va haqiqiyligini tekshirish jarayonini o‘z ichiga oladi va tizimning uzluksiz ishlashini ta’minlaydi. Konsensusning asosiy vazifasi reyestrning joriy holati bo‘yicha umumiy kelishuvga erishishdan iborat. Amaliyotda turli xil **konsensus algoritmlari** mavjud bo‘lib, eng mashhurlari quyidagi tadqiqotlarda ko‘rib chiqilgan. Ushbu tadqiqotning asosiy maqsadi **blockchain texnologiyasidan DDoS hujumlarini oldini olishda foydalanish imkoniyatlarini o‘rganish va tahlil qilishdir**. Bundan tashqari, blockchain texnologiyasi asosida ma’lumotlarni taqsimlangan tizimlarda saqlash funksiyalarini taqdim etuvchi tayyor yechimlarning tahlili amalga oshiriladi.

Konsensus algoritmlari

Konsensus nomi	Konsensus mexanizmi	Afzalliklari	Kamchiliklari
Bajarilgan ish isboti (PoW)	Tugunlar murakkab hisoblash muammosini hal qiladi, birinchi bo‘lib to‘g‘ri yechimni topgan tugun yetakchi deb tan olinadi	Yuqori darajadagi xavfsizlik	Yuqori energiya sarfi
Ulgurji egalik isboti (PoS)	Yetakchilik egallangan ulush miqdori bilan belgilanadi	Energiya tejamkorligi, iqtisodiy xavfsizlik	Adolatli taqsimotni ta’minlash qiyin
Avtoritetga asoslangan egalik isboti (PoA)	Yetakchi faqat ma’lum bir ishonchli tugunlar orasidan tanlanadi, har qanday tugun yetakchi bo‘la olmaydi	Yuqori o'tkazuvchanlik, ishonchlilik	Markazlashganlik, cheklangan kirish imkoniyati

Amaliy Vizantiya xatolarga bardoshli konsensus (RBFT)	Yetakchi tanlanmaydi, ovoz berish asosida replikatsiyalangan xizmatlardan foydalaniladi	Xatolarga bardoshlilik, ovoz berish orqali konsensus	Masshtablanish muammosi, tizim bardoshliligi uchun zararli tugunlar uchdan bir qismidan ko‘p bo‘lmasligi kerak
Delegatsiyalangan Vizantiya xatolarga bardoshli konsensus (dBFT)	RBFT ga o‘xshash, lekin barcha tugunlar teng huquqli emas, faqat delegatlar konsensus jarayonida ishtirok etadi	Xatolarga bardoshlilik, ovoz berish orqali konsensus, RBFT ga nisbatan yaxshilangan masshtablanish	Tizim bardoshliligi uchun zararli delegatlar uchdan bir qismidan ko‘p bo‘lishi mumkin emas

Tadqiqot materiallari va usullari

Blockchain DDoS-hujumlarning oldini olish uchun kuchli vosita hisoblanadi. Bu, blockchainning ma’lumotlarni kriptografik himoya qilish imkoniyatiga ega taqsimlangan ma’lumotlar bazasi sifatida tashkil etilganligi bilan bog‘liq. Shu sababli, ushbu texnologiya DDoS-hujumlardan himoyalanish uchun samarali va ishonchli yechimni ta’minlaydi.

DDoS-hujumlar quyidagi mezonlar asosida tasniflanishi mumkin: zararli trafik hajmi (yuzlab Gbit/s), hujum qaratilgan abstraksiya darajasi (dasturiy ta’minot, apparat ta’minoti, tarmoq), shuningdek, hujum qaratilgan resurs turi. Eng keng tarqalgan DDoS-hujum turlari quyidagilardir: brute-force (xamla), spufing, ICMP-flood va UDP-flood.

Brute-force — bu hujum turi, bunda tajovuzkor maqsadli server yoki tarmoqqa katta hajmdagi so‘rovlarni yuborib, uni ortiqcha yuklash va xizmat ko‘rsatishni rad etishga olib keladi.

Spufing — bu hujumda IP-manzillar yoki boshqa identifikatorlar soxtalashtiriladi, bu esa hujum manbasini yashirishga yordam beradi.

Flood-hujumlar — bu usulda jabrlanuvchining aloqa kanali katta hajmdagi trafik bilan to‘ldiriladi, natijada uning faoliyati to‘xtashi yoki sezilarli darajada sustlashishi mumkin.

Barcha ushbu hujumlar puxta rejalashtirilgan va to‘g‘ri amalga oshirilgan taqdirda juda samarali bo‘lishi mumkin. Axborot tizimlarining xavfsizligi taqsimlangan reyestr texnologiyalarining asosiy xususiyatlariga tayanadi. Ulardan biri **detsentralizatsiya** bo‘lib, bu ma’lumotlarning yagona joyda saqlanmasligini anglatadi va ularning yo‘qolishi yoki buzilish ehtimolini kamaytiradi. Detsentralizatsiya DDoS-hujumlarga qarshi kurashish imkonini beradi, chunki hujum muvaffaqiyatli bo‘lishi uchun tarmoqdagi barcha tugunlarni ishdan chiqarish talab etiladi.

Shuningdek, blockchain texnologiyasida **xesh-funksiyalardan** foydalanish ma’lumotlarning soxtalashtirilishiga sezgirligini oshiradi. Bundan tashqari, tizimning yana bir muhim xususiyati — uzellardagi ma’lumotlar o‘zgarishlarining tarixini kuzatish imkoniyatidir. Ushbu xususiyatlarning kombinatsiyasi tizimga qaratilgan hujumlarni aniqlash va ularning oldini olishda yuqori aniqlikni ta’minlaydi.

DDoS-hujumlarning oldini olishga asoslangan mexanizm taqsimlangan tarmoqlar va blockchain texnologiyasidan foydalanish orqali onlayn xizmatlar va veb-ilovalarning xavfsizligi va barqarorligini ta’minlashga qaratilgan innovatsion yondashuv hisoblanadi. Blockchainning muhim afzalliklaridan biri shundaki, ma’lumotlar taqsimlangan tarmoqda saqlanadi, bu ularni kiberhujumlar va buzilishlardan yaxshiroq himoya qiladi. Shuningdek, blockchain ma’lumotlarning shaffofligi va o‘zgarmasligini ta’minlaydi.

Himoya mexanizmining asosi — taqsimlangan tarmoq orqali foydalanuvchi so‘rovlarini qayta ishlashdir. Bu server yuklamasini kamaytirishga va tizimning ortiqcha yuklanishining oldini olishga yordam beradi.

Bu rasmda “DLT asosida SIEM saqlash modulining afzalliklari” keltirilgan bo‘lib, quyidagi jihatlar ta’kidlangan:

1. **Ma’lumotlarning shaffofligi va butunligi**
2. **Kiberhujumlarga bardoshlilik**
3. **Hodisalarning tezkor aniqlanishi**
4. **Masshtablanuvchanlik**

Bundan tashqari, blockchaindan foydalanish ma’lumotlarni ishonchli saqlash va himoya qilishni ta’minlab, ularning yo‘qolishi yoki o‘zgartirilishining oldini oladi. Ushbu mexanizmning mohiyati shundan iboratki, DDoS-hujumga urinish bo‘lganda, taqsimlangan tarmoq foydalanuvchilardan kelgan so‘rovlarni qayta ishlaydi va ularni blockchain orqali serverga yuboradi.

Taqsimlangan reestr texnologiyasiga asoslangan axborot almashinuvi va saqlash masalasining amaliy yechimi sifatida quyidagi kriptografik yechimlar taklif etilishi mumkin: TLS (Transport Layer Security) protokolining 1.3 versiyasidan foydalanish, u Rossiya kriptografik to‘plamlarini qo‘llab-quvvatlaydi. TLS protokoli bo‘yicha himoya uch bosqichda amalga oshiriladi, har bir bosqich maxsus kriptografik algoritmlarni o‘z ichiga oladi. Ushbu algoritmlar standartlashtirilgan hujjatlar asosida belgilanadi va simmetrik kalit hosil qilish, shifrlash hamda xesh-funksiyani yaratish algoritmlarini qamrab oladi.

Birinchi bosqich – ulanishni o‘rnatish tekshiruvi (Handshake), ikkinchi bosqich – sessiyani qayta tiklash tartibi (False Start), uchinchi bosqich esa apparat va dasturiy ta’minotning har bir komponentini oxirgi nuqtadan ildiz sertifikatgacha tekshirishdan iborat (Chain of trust).

Axborot xavfsizligini boshqarish bo‘yicha samarali echimlardan biri bu **axborot xavfsizligi hodisalari va voqealarini boshqarish tizimlari (SIEM)** bo‘lib, ular xakerlik hujumlari, ruxsatsiz kirish, ma’lumotlar sizib chiqishi kabi turli tahdidlardan axborot tizimlarini himoya qilishda yuqori darajada xavfsizlikni ta’minlaydi. SIEM tizimlari nafaqat tizimlardagi zaifliklarni aniqlashga, balki

korporativ xavfsizlik siyosatlariga rioya etilishini nazorat qilishga ham imkon beradi.

SIEM tizimlari ma’lumotlar bazalarini boshqarish tizimlari, monitoring va kirishni nazorat qilish tizimlari kabi turli manbalar tomonidan yaratilgan ma’lumotlarni yig‘ib, ularni jamlab tahlil qiladi. **Taqsimlangan reestr texnologiyasiga (DLT) asoslangan SIEM hodisalarini saqlash moduli** axborot tizimlarining xavfsizligini ta’minlash va ularni kuzatib borish uchun innovatsion yechim hisoblanadi. DLT asosidagi SIEM saqlash modulining asosiy afzalliklari rasmda keltirilgan.

Tadqiqot natijalari va muhokamasi

Bugungi kunda taqsimlangan tizimlarda ma’lumotlarni saqlash uchun ishlatiladigan bir qator tayyor **DLT-yechimlar** mavjud.

- **Fluree** – bu markazlashmagan ma’lumotlar boshqaruv platformasi bo‘lib, SIEM tizimining saqlash modulini yuqori darajada himoya qiladi, moslashuvchanlik va kengaytirish imkoniyatiga ega. Biroq, Fluree'ning kamchiligi past unumdorlik va ekspluatatsiya murakkabligidir.
- **Enigma** – shaxsiylik kafolatlangan markazlashmagan hisoblash platformasi. Uning afzalliklari shifrlangan ma’lumotlar hatto hisoblash jarayonida ham ochilmasligi, kengaytirish imkoniyati va ishonchliligi. Biroq, ushbu tizimning kamchiligi cheklangan moslashuvchanlik va shaxsiylikni ta’minlash uchun ortiqcha resurs sarflash natijasida umumiy unumdorlikning pasayishidir.
- **Ethereum** – ochiq blockchain platformasi bo‘lib, smart-kontraktlar yaratish imkonini beradi va markazlashmagan ilovalar (DApps) hamda ma’lumotlarni boshqarish uchun moslashuvchan muhit taqdim etadi. Biroq, Ethereum'ni SIEM tizimlariga integratsiya qilish qiyin, shuningdek, kengaytirish bilan bog‘liq muammolar, smart-kontraktlarning zaifligi, murakkab ishlab chiqish jarayoni va katta hisoblash resurslarini talab qilishi kabi kamchiliklarga ega.

- **Corda** – moliyaviy sektor ehtiyojlariga moslashtirilgan ochiq blockchain platformasi bo‘lib, ma’lum darajadagi o‘zgarishlar orqali SIEM tizimlari bilan integratsiya qilish imkoniyatini beradi. Corda yuqori darajada xavfsizlikni ta’minlaydi, chunki u shifrlash va autentifikatsiya nazoratini o‘z ichiga oladi. Ammo bu tizimda ham xakerlik hujumlari yoki ma’lumotlar sizib chiqishi xavfi mavjud. Uning asosiy kamchiliklari cheklangan moslashuvchanlik va boshqa platformalarga loyihalarni ko‘chirishdagi qiyinchiliklardir.
- **Guardtime MIDA** – xavfsizlik bo‘yicha yangi yondashuv bo‘lib, ma’lumotlarni kriptografik konteyner bilan solishtirish orqali ularning yaxlitligini aniq darajada tekshiradi. Ushbu konteynerlar taqsimlangan reestrdan foydalangan holda ma’lumotlarning yaxlitligini sezilarli darajada oshiradi. Guardtime MIDA uzoq infratuzilmalar, masalan, bulutli texnologiyalar va IoT (Internet of Things) bilan samarali ishlaydi. Uning afzalliklari real vaqt rejimida buzilishlarni aniqlash va past operatsion xarajatlar bo‘lsa, kamchiligi – hal qilinadigan muammolar doirasining cheklanganligidir.

Tahlil qilingan DLT-yechimlar orasida faqat **Fluree** va **Corda** SIEM tizimlari bilan integratsiya imkoniyatiga ega. Shu bilan birga, aksariyat yechimlar ortiqcha funksionallikka ega bo‘lib, bu tizim unumdorligini sezilarli darajada pasaytiradi. Shuningdek, mavjud yechimlarning umumiy muammosi ularning universal emasligi, ya’ni, keng turdagi vazifalarni qamrab ololmasligidir.

Shu sababli, SIEM tizimlari bilan integratsiya qilish imkoniyatiga ega, taqsimlangan reestr texnologiyasiga asoslangan, moslashuvchan, yuqori unumdorlikka ega va ishonchli **innovatsion ma’lumotlar saqlash yechimlarini ishlab chiqish zarurati** mavjud.

Xulosa

Taqsimlangan reestr texnologiyasidan foydalanish istiqbolli yo‘nalishlardan biri bo‘lib, u ma’lumotlarning yaxlitligi va mavjudligini ta’minlash, tizimning

iqtisodiy samaradorligini oshirish hamda ma’lumotlarni saqlash va uzatishda yuqori darajadagi xavfsizlikni ta’minlash imkonini beradi. Ushbu texnologiyaning afzalliklari moliya bozorida operatsiyalar samaradorligining oshishiga ham xizmat qiladi.

Ushbu ishda taqsimlangan tizimlarda ma’lumotlarni saqlash uchun mavjud bo‘lgan **DLT-yechimlar** tahlil qilindi, ularning asosiy afzalliklari va kamchiliklari aniqlab berildi. Tahlil natijalariga ko‘ra, **SIEM tizimlari bilan integratsiyalash mumkin bo‘lgan, taqsimlangan reestr texnologiyasiga asoslangan, moslashuvchan, yuqori unumdorlikka ega va xavfsizlik darajasi yuqori bo‘lgan universal yechimni ishlab chiqish zarurligi** belgilandi.

Foydalanilgan adabiyotlar ro‘yxati

1. Gataullin T.M., Gataullin S.T. Endpoint Functions: Mathematical Apparatus and Economic Applications // Mathematical Notes. 2022. T. 112, № 5–6. C. 656–663.
2. Ivanyuk V. Forecasting of digital financial crimes in Russia based on machine learning methods // Journal of Computer Virology and Hacking Techniques. 2023. C. 1–14.
3. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты. Litres, 2022. 538 с.
4. Zhang J. et al. A Secure and Lightweight Multi-Party Private Intersection-Sum Scheme over a Symmetric Cryptosystem //Symmetry. 2023. T. 15, № 2. C. 319.
5. Timofeev I., Pleshakova E., Dogadina E., Osipov A., Kochkarov A., Ignar S., Suvorov S., Gataullin S., Korchagin S. Mathematical Models and Methods for Research and Optimization of Protein Extraction Processes from Chickpea and

Curd Whey Solutions by Electroflotation Coagulation Method // Mathematics. 2022. T. 10, № 8. C. 1284.

6. Yerznkyan B.H., Gataullin T.M., Gataullin S.T. Mathematical Aspects of Synergy // Montenegrin Journal of Economics. 2022. T. 18, № 3. C. 197–207.

7. Petrosov D.A., Pleshakova E.S., Osipov A.V., Ivanov M.N., Zelenina A.N., Lvovich I.Ya., Preobrazhenskiy Yu.P., Petrosova N.V., Lopatnuk L.A., Kupriyanov D.Y., Roga S.N. Modeling of resource allocation in industrial organizations // Procedia Computer Science. 2022. T. 213. C. 355–359.

8. Petrosov D.A., Pleshakova E.S., Osipov A.V., Ivanov M.N., Lopatnuk L.A., Radygin V.Y., Roga S.N. Mathematical apparatus of artificial neural networks for genetic algorithm controlling under structural parametric synthesis of large discrete systems // Procedia Computer Science. 2022. T. 213. C. 346–354.

9. Беларев И.А., Обаева А.С. О распределенном реестре и возможности его применения // Финансы: теория и практика. 2017. Т. 21, № 2. С. 94–99.

10. Walport M. Distributed ledger technology: Beyond block chain. Government Office for Science, 2016. 88 p.