BLOCKCHAIN TEXNOLOGIYALARINI KIBERXAVFSIZLIK TIZIMLARIGA INTEGRATSIYA QILISH

Xabibullayev Jahongirbek Doniyorbek o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti,
Chunayev Norquvvat Eshquvat o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti

Annotatsiya:*Ushbu maqolada blockchain texnologiyasining asosiy afzalliklar sifatida ma’lumotlarning ishonchliligi va o‘zgarmasligi, markazlashmagan kirish nazorati, o‘zgarishlarni kuzatish va tarqatilgan hujumlardan himoya kabi jihatlar ko‘rib chiqiladi. Shu bilan birga blockchainning tizim ishtirokchilari o‘rtasida ishonchni oshirish, ma’lumotlar xavfsizligini ta’minlash va buzilishlarning oldini olish uchun samarali vosita ekanligini ta’kidlaydilar. Ushbu texnologiyalarni joriy etish zamonaviy raqamli davrda yangi himoya darajasini ta’minlashga va kiberxavfsizlikning dolzarb muammolarini hal qilishga xizmat qiladi. Tahlil natijasida aniqlanishicha, blockchain ma’lumotlarning ishonchliligi va o‘zgarmasligini, markazlashmagan kirish nazoratini, operatsiyalarning kuzatilishi va shaffofligini ta’minlaydi. Ushbu xususiyatlar uni nafaqat kiberhujumlarning oldini olish uchun kuchli vositaga, balki axborot tizimlari ishtirokchilari o‘rtasidagi ishonchni mustahkamlovchi instrumentga aylantiradi.Shunday qilib, blockchain texnologiyalarining kiberxavfsizlik tizimlariga integratsiyasi nafaqat kiberxavf-xatarlarga qarshi himoya darajasini oshiradi, balki ishonchli va shaffof raqamli muhit yaratishga ham xizmat qiladi. Bunday yechimlarning rivojlanishi va joriy etilishi tezkor raqamli taraqqiyot davrida kiberxavfsizlikni yanada takomillashtirish uchun yangi imkoniyatlarni taqdim etadi.*

Kalit so‘zlar*: integratsiya, blockchain texnologiyalari, kiberxavfsizlik, ishonchlilik, o‘zgarmaslik, kuzatuvchanlik, shaffoflik, kiberxavf-xatarlar, innovatsiyalar.*

Kirish

Zamonaviy texnologik muammolar jamiyat oldiga axborotni himoya qilish va kiberxavfsizlik usullarini doimiy ravishda takomillashtirish zaruriyatini qo‘ymoqda. Shu nuqtai nazardan, dastlab kriptovalyuta tizimlarida tranzaksiyalar xavfsizligini ta’minlash uchun yaratilgan blockchain texnologiyasi raqamli dunyoda axborot xavfsizligini ta’minlash bo‘yicha samarali vosita sifatida e’tiborni tortmoqda. Ushbu

maqolada blockchain texnologiyalarining integratsiyasi kiberxavfsizlik tizimlarini qanday yaxshilashi mumkinligi ko‘rib chiqiladi.

Blockchain markazlashmagan tugunlar tarmog‘iga asoslangan bo‘lib, har bir tugun bloklar zanjirining to‘liq nusxasini saqlaydi. Bu xususiyat tizimning yuqori darajadagi ishonchliligi va buzilishlarga chidamliligini ta’minlaydi. Blockchainda saqlanadigan ma’lumotlar tarmoq ishtirokchilarining aksariyat qismi roziligisiz o‘zgartirilishi yoki o‘chirilishi mumkin emas. Bu ma’lumotlarning o‘zgarmasligini ta’minlaydi va blockchainni buzilishlar hamda axborotga noqonuniy aralashuvlarning oldini olish uchun samarali vositaga aylantiradi.

Raqamli axborot hajmining uzluksiz o‘sishi va kiberxavf-xatarlarning kuchayishi sharoitida kiberxavfsizlikni ta’minlash usullarini takomillashtirish dolzarb masalaga aylanmoqda. Dastlab kriptovalyuta tizimlarida tranzaksiya xavfsizligini ta’minlash uchun yaratilgan blockchain texnologiyasi raqamli muhitda axborot xavfsizligini ta’minlash bo‘yicha samarali vosita sifatida ajralib turadi. Markazlashmagan va o‘zgarmas ma’lumotlar bazalarini yaratish orqali blockchain kiberxavfsizlik tizimlarini yaxshilash uchun mustahkam asos yaratadi va ishonchlilik, markazlashmagan kirish nazorati hamda yuqori darajadagi shaffoflikni ta’minlaydi. Ushbu maqolada blockchain texnologiyalarining integratsiyasi asosiy jihatlari va ularning zamonaviy axborot jamiyatida kiberxavfsizlikni ta’minlashga ta’siri ko‘rib chiqiladi.

Asosiy qism

Dastlab kriptovalyutalar kontekstida yuzaga kelgan blockchain texnologiyasi nafaqat moliyaviy tizimlarga innovatsiyalar olib keldi, balki kiberxavfsizlik tizimlarini rivojlantirish uchun ham muhim asos bo‘ldi. Ushbu texnologiyaning kiberxavfsizlikni mustahkamlashga xizmat qiladigan ikkita asosiy xususiyati – ishonchlilik va o‘zgarmaslikdir.

Blockchainning ishonchliligi uning markazlashmagan tarmoq tuzilmasi bilan ta’minlanadi. Markazlashgan tizimlardan farqli o‘laroq, unda yagona ishdan chiqish nuqtasi mavjud emas. Blockchain tarmoqdagi ko‘plab tugunlarda joylashadi va har bir tugun bloklar zanjirining to‘liq nusxasini saqlaydi. Bu shuni anglatadiki, agar bir tugun ishdan chiqsa yoki kiberhujumga uchrasa, boshqa tugunlar tizimning ishlashini davom ettiradi. Ishonchlilikning qo‘shimcha darajasi tarmoq ishtirokchilari blockchainga kiritiladigan o‘zgarishlarni tasdiqlash uchun kelishuv mexanizmini (konsensus) qo‘llashi bilan ta’minlanadi. Bu soxta ma’lumotlar kiritilishining oldini oladi va axborot yaxlitligiga bo‘lgan ishonchni oshiradi, bu esa kiberxavfsizlik sohasida muhim ahamiyat kasb etadi.

Blockchainning o‘zgarmasligi uning oldindan kiritilgan ma’lumotlar o‘zgartirilmasdan saqlanishi xususiyati bilan bog‘liq. Bir marta blok zanjirga qo‘shilgach, uning tarkibini o‘zgartirish yoki uni o‘chirish faqat tarmoqdagi

tugunlarning aksariyatining roziligi bilangina amalga oshirilishi mumkin. Bu xususiyat ma’lumotlarning ishonchli saqlanishini kafolatlaydi. O‘zgarmaslik an’anaviy markazlashgan ma’lumotlar bazalaridan farqli o‘laroq, administratorlarga yozuvlarni o‘zgartirish yoki o‘chirish imkoniyatini cheklaydi. Blockchainda har qanday ma’lumot, hatto eng kichik blok ham, o‘zgarmas tarixning bir qismiga aylanadi, bu esa tranzaksiya jurnallari yoki autentifikatsiya ma’lumotlarini saqlash uchun uni ideal yechimga aylantiradi.

Ishonchlilik va o‘zgarmaslik xususiyatlari blockchain texnologiyasini kiberxavfsizlik tizimlariga integratsiya qilish uchun jozibador qiladi. Bu xususiyatlar tashqi hujumlardan himoya qilish hamda ichki ma’lumotlar yaxlitligini buzilishidan saqlash uchun barqaror mexanizmni ta’minlaydi. Kiberxavfsizlikda blockchain qo‘llanilishi nafaqat himoya darajasini oshiradi, balki uzluksiz rivojlanayotgan kiberxavf-xatarlarga qarshi yangi yondashuvlar uchun ham zamin yaratadi.

So‘nggi yillarda blockchainga asoslangan markazlashmagan kirish nazorati raqamli muhitda xavfsizlikni mustahkamlash uchun istiqbolli yechim sifatida e’tiborni tortmoqda. Markazlashmagan kirish nazorati – bu blockchain texnologiyasiga asoslangan axborot xavfsizligini ta’minlash tamoyili bo‘lib, u an’anaviy markazlashgan kirish huquqlarini boshqarish tizimlaridan farqli ravishda ishlaydi. Blockchain aqlli shartnomalarni yaratish imkonini beradi, ular jarayonlarni avtomatlashtirib, ma’lumotlarga kirishni boshqaradi. Ushbu aqlli shartnomalar oldindan belgilangan shartlar va qoidalarga asoslangan holda kirish huquqlarini belgilaydi, bu esa oraliq instansiyalarga ehtiyojni yo‘q qiladi va boshqaruv samaradorligini oshiradi. Markazlashmagan kirish nazorati ma’lumotlarni xavfsiz va moslashuvchan boshqarish imkonini beradi, ruxsatsiz harakatlar xavfini kamaytiradi va tizimlarning umumiy kiberxavfsizligini oshiradi.

Markazlashmagan kirish nazorati tamoyillari:

– *Aqlli shartnomalar.* Markazlashmagan kirish nazoratida aqlli shartnomalar qo‘llaniladi, ular o‘z kodiga asoslangan holda avtomatik ravishda bajariladigan dasturlar hisoblanadi. Blockchaindagi aqlli shartnomalar ma’lumotlarga kirish qoidalarini belgilash va amalga oshirish imkonini beradi, bunda markazlashgan nazoratga ehtiyoj qolmaydi. Ushbu shartnomalar oldindan belgilangan shartlar bajarilganda avtomatik ravishda ishga tushadi, bu esa kirishni boshqarish samaradorligini oshiradi.

– *Markazlashmagan identifikatorlar.* An’anaviy kirish boshqaruvi tizimlari odatda identifikatsiya ma’lumotlarini saqlash uchun markazlashgan ma’lumotlar bazalariga tayanadi. Blockchainga asoslangan markazlashmagan tizimlarda esa ishtirokchilar unikal kriptografik identifikatorlarga ega bo‘lishi mumkin, bu esa markazlashgan saqlash zaruratini bartaraf etgan holda shaxsni tasdiqlash imkonini beradi.

– *Shaffoflik va kuzatuvchanlik.* Markazlashmagan kirish nazorati shaffoflik va ma’lumotlarga kirish operatsiyalarini kuzatish imkoniyatini ta’minlaydi. Har qanday ruxsat o‘zgarishi blockchainga yoziladi, bu esa real vaqt rejimida ma’lumotlardan kim va qanday foydalanayotganini kuzatish hamda audit qilish imkonini beradi.

– *Markazlashmagan yondashuv.* An’anaviy tizimlardagi markazlashgan boshqaruv nuqtalariga tayanish o‘rniga, markazlashmagan kirish nazorati blockchainning teng huquqli tugunlari asosida ishlaydi. Har bir tugun kirish huquqlarini tasdiqlovchi valyidator rolini bajarishi mumkin, bu esa tizimni hujumlarga va nosozliklarga nisbatan yanada chidamli qiladi.

Markazlashmagan kirish nazoratining afzalliklari:

– Markazlashmagan kirish nazorati yagona ishdan chiqish nuqtasini yo‘q qiladi, bu esa tizimni xakerlik hujumlariga nisbatan kamroq zaif qiladi. Blockchaindagi aqlli shartnomalar va kriptografiya xavfsizlikni ta’minlash uchun ishonchli mexanizmlarni yaratadi.

– Blockchainning shaffofligi foydalanuvchilarga ularning ma’lumotlari qanday ishlatilayotganini ko‘rish imkonini beradi, bu esa ishonchni oshiradi hamda normativ talablarning bajarilishiga yordam beradi.

– Aqlli shartnomalar orqali avtomatlashtirish kirishni boshqarishni soddalashtiradi, vaqt kechikishlarini kamaytiradi va qo‘lda boshqarish natijasida yuzaga keladigan xatoliklarni minimallashtiradi.

Kuzatuvchanlik va shaffoflik — blockchain texnologiyasini kiberxavfsizlik tizimlariga integratsiya qilishning asosiy afzalliklaridan hisoblanadi. Blockchainning markazlashmagan tabiati tufayli tizimdagi har qanday o‘zgarish tarmoq ishtirokchilariga ochiq bo‘lgan taqsimlangan reyestrda aks etadi. Bu barcha harakatlarni va tranzaksiyalarni real vaqt rejimida kuzatish imkonini beradi hamda potensial zaif nuqtalarni yo‘q qiladi. Blockchainning shaffofligi tizim ichida ochiqlik va ishonch muhitini yaratib, har bir ishtirokchiga o‘zgarishlar tarixini tekshirish imkonini beradi. Bu xususiyat ruxsatsiz harakatlarni aniqlashga va umumiy xavfsizlik darajasini oshirishga yordam beradi.

Blockchain texnologiyasining kuzatuvchanligi va shaffofligi kiberxavfsizlik tizimlarida tahdidlarga samarali javob berish hamda raqamli muhitda ishonch darajasini oshirishga xizmat qiladi.

Ma’lumotlarning shaffofligi. Blockchain texnologiyasi barcha o‘zgarishlarni qayd etuvchi o‘zgarmas va markazlashmagan reyestrni yaratadi. Bu ma’lumotlarning shaffofligini ta’minlaydi, chunki har bir tarmoq ishtirokchisi tranzaksiyalar yoki hodisalar tarixiga to‘liq kirish huquqiga ega bo‘ladi. Kiberxavfsizlik kontekstida shaffoflik shubhali faollikni, ichki tahdidlarni aniqlash va xavfsizlik muammolarini hal qilish uchun kuchli vosita hisoblanadi.

Blockchainning muhim xususiyatlaridan biri uning ma’lumotlarni o‘zgarmas shaklda saqlash qobiliyatidir. Har bir blok o‘zidan oldingi blokning xeshini va o‘z ma’lumotlarini o‘z ichiga oladi. Bu esa ma’lumotlar blokga yozilgandan so‘ng, butun zanjirni o‘zgartirmasdan ularni o‘zgartirishning deyarli imkonsizligini anglatadi. Bunday o‘zgarmaslik ma’lumotlarning shaffofligini ta’minlaydi, chunki har qanday aralashuv darhol seziladi.

Blockchainda ma’lumotlar tarmoqdagi barcha uzellarda saqlanadi, bu esa taqsimlangan ma’lumotlar bazasini yaratadi. Natijada, markazlashgan nazorat va ma’lumotlarni manipulyatsiya qilish imkoniyati yo‘qoladi, bu esa blockchainsiz tizimlarda ko‘pincha zaif nuqta hisoblanadi. Ma’lumotlarning shaffofligi barcha tarmoq ishtirokchilarining bir xil ma’lumotlarga ega bo‘lishini ta’minlaydi va axborot buzilishi xavfini yo‘q qiladi. Bu shaffoflik tarmoq ishtirokchilari o‘rtasida ishonchni mustahkamlashga xizmat qiladi. Agar tizimda hodisa yoki xatolik yuz bersa, barcha o‘zgarishlarning o‘zgarmas tarixi saqlangani uchun javobgar shaxslarni tezda aniqlash mumkin bo‘ladi.

Bunday shaffoflik audit jarayonlarini va qonunchilik talablariga rioya qilishni soddalashtiradi. Blockchain tomonidan ta’minlangan ma’lumotlar shaffofligi kiberxavfsizlik tizimlariga kiber tahdidlarga qarshi kurashish uchun kuchli vosita bo‘lib, raqamli muhitdagi o‘zgarishlarga tezkor javob berish imkonini beradi. Bu axborotni nazorat qilish samaradorligini oshirib, xavfsiz va ishonchli onlayn makon yaratishga yordam beradi.

Hodisalarni kuzatish. Blockchain texnologiyasining kiberxavfsizlik tizimlarida asosiy jihatlaridan biri hodisalarni kuzatish imkoniyatidir. Bu element potensial tahdidlarni tezkor aniqlash va ularga javob berishda hamda ma’lumotlarning butunligini va xavfsizligini ta’minlashda muhim rol o‘ynaydi. Blockchain doimiy ravishda tizimdagi barcha voqea va o‘zgarishlarni qayd etuvchi markazlashmagan reyestr sifatida ishlaydi. Har bir hodisa alohida blok shaklida yozilib, bloklar zanjiriga qo‘shiladi va barcha operatsiyalar tarixini saqlaydi. Bu esa muammo yuzaga kelganda, administratorlarga qachon va qanday ma’lumotlar o‘zgarganligini aniq aniqlash imkonini beradi.

Barcha hodisalar tarixi doimiy ravishda ochiq va mavjud bo‘lgani sababli, kiberxavfsizlik tizimlari hodisalarni va potensial tahdidlarni tezkor aniqlash hamda ularga javob berish imkoniyatiga ega bo‘ladi.

DDoS-hujumlardan himoya

Taqsimlangan xizmat ko‘rsatish rad etilishiga (DDoS) qarshi himoya blockchain texnologiyalarini kiberxavfsizlik tizimlariga integratsiya qilish orqali sezilarli darajada kuchaytirilishi mumkin bo‘lgan asosiy yo‘nalishlardan biridir. DDoS-hujumlarga qarshi an’anaviy usullar odatda markazlashgan yondashuvlardan foydalanadi, bu esa tizimlarni keng ko‘lamli hujumlarga nisbatan zaif qiladi. Blockchain kontekstida esa

tarmoqning markazlashmagan tuzilishi tugunlarning bir-biridan mustaqil ishlashiga imkon yaratadi va tizimning barqarorligini oshiradi. Yakkama-yakka tugunlarning ishlamay qolishi butun tizimning izdan chiqishiga olib kelmaydi, bu esa DDoS-hujumlarga nisbatan chidamliligini oshiradi. Shu sababli, blockchain texnologiyalaridan foydalangan holda kompaniyalar va tashkilotlar o‘z resurslarini zararli hujumlardan samarali himoya qila oladilar.

Blockchainning kiberxavfsizlik tizimlariga integratsiyasi DDoS-hujumlarga qarshi quyidagi samarali himoya mexanizmlarini taqdim etadi:

− Markazlashmagan tarmoq. Blockchain markazlashmagan tarmoq tugunlari asosida ishlaydi va har bir tugun mustaqil hamda teng huquqli ishtirokchi hisoblanadi. DDoS-hujumlar odatda maqsadli resursga katta hajmli so‘rovlar yuborish orqali amalga oshiriladi. Biroq, blockchainning markazlashmagan tabiati bunday hujumlarga kuchli qarshilik ko‘rsatadi, chunki yagona zaif nuqta mavjud emas. Bu blockchain tarmoqlarining keng ko‘lamli hujumlarga bardoshli bo‘lishini ta’minlaydi.

− Yuklamani taqsimlash. Blockchain har bir tugunning butun bloklar zanjiri nusxasiga ega bo‘lish tamoyiliga asoslangan bo‘lib, bu yuklamani barcha ishtirokchilar o‘rtasida taqsimlaydi. Natijada, muayyan tugunlarga ortiqcha yuk tushishi natijasida xizmatning rad etilish ehtimoli kamayadi. Blockchain tarmoqdagi trafikni teng taqsimlashni ta’minlab, DDoS-hujumlarning samaradorligini pasaytiradi.

− Aqlli shartnomalar orqali avtomatlashtirilgan javob. Blockchainda aqlli shartnomalardan foydalanish tarmoqdagi trafikdagi noodatiy naqshlarni avtomatik ravishda aniqlash va ularga tezkor javob berish imkonini yaratadi. Aqlli shartnomalar shubhali so‘rovlarni bloklash yoki trafikni qayta taqsimlash kabi chora-tadbirlarni ko‘rishi mumkin. Bu esa himoyaning samaradorligini oshirib, DDoS-hujumlarga qarshi tezkor choralar ko‘rish imkonini beradi.

− Kriptografik mustahkamlik. Blockchain texnologiyasining asosi bo‘lgan kriptografik tamoyillar tizimning buzilishlar va soxtalashtirishlarga nisbatan himoyalanganligini ta’minlaydi. Bu blockchain tarmoqlarini manipulyatsiyalarga kamroq moyil qiladi va tizimning yaxlitligini hatto kuchli DDoS-hujumlar sharoitida ham saqlashga yordam beradi.

Blockchain texnologiyalarining kiberxavfsizlik tizimlariga integratsiyasi nafaqat DDoS-hujumlarga qarshi himoyani kuchaytiradi, balki jarayonni yanada aqlli, moslashuvchan va raqamli tahdidlarga nisbatan tezkor javob bera oladigan holatga keltiradi.

Xulosa

Blockchain texnologiyalarining kiberxavfsizlik tizimlariga integratsiyasi zamonaviy raqamli muhit tahdidlariga samarali javob bera oladigan istiqbolli yo‘nalish hisoblanadi. Tahlil jarayonida blockchainning ma’lumotlarning ishonchliligi va o‘zgartirilmasligini ta’minlashi, markazlashmagan nazorat tizimi, operatsiyalarning

kuzatilishi va shaffofligini oshirishi aniqlangan. Ushbu xususiyatlar uni nafaqat kiberhujumlarning oldini olish vositasi sifatida, balki axborot tizimlari ishtirokchilari o‘rtasida ishonchni mustahkamlovchi mexanizm sifatida ham ahamiyatli qiladi. Blockchain texnologiyalarining kiberxavfsizlik tizimiga integratsiya qilinishiga doir tahlil asosida quyidagi xulosalar shakllantirildi:

− Blockchain markazlashmagan tuzilishi va tarmoq ishtirokchilarining ko‘pchilik roziligisiz ma’lumotlarni o‘zgartirish imkonsizligi sababli yuqori darajadagi ma’lumotlar himoyasini ta’minlaydi;

− blockchain asosidagi aqlli shartnomalar ma’lumotlarga kirishni samaraliroq boshqarishga yordam beradi, jarayonlarni avtomatlashtirib, ruxsatsiz kirish xavfini kamaytiradi;

− blockchain shaffoflik va operatsiyalarni kuzatish imkonini beradi, bu esa xavf-xatarlarni aniqlash va ularga javob berish jarayonini soddalashtiradi hamda ishonchli xavfsizlik auditini ta’minlaydi;

− blockchainning markazlashmagan tuzilishi uni DDoS kabi taqsimlangan hujumlarga nisbatan chidamli qiladi va tizimning umumiy barqarorligini oshiradi.

Ushbu xulosalar asosida aytish mumkinki, blockchain texnologiyalarining kiberxavfsizlik tizimlariga integratsiyasi nafaqat kiberxavfsizlik darajasini oshiradi, balki yanada ishonchli va shaffof raqamli muhitni shakllantirishga yordam beradi. Bunday yechimlarning rivojlanishi va joriy etilishi tezkor raqamli o‘zgarishlar davrida kiberxavfsizlikni takomillashtirish uchun yangi imkoniyatlar yaratadi.

Foydalanilgan adabiyotlar

1. Xabibullayev J.D., DDoS-hujumlarning oldini olishda blockchain texnologiyasining imkoniyatlarini tahlili // Лучшие интеллектуальные исследования, 2025-yil 26-fevral. Vol. 39, №-3. –b 121-131.
2. Chunayev N.E., Xabibullayev J.D., Application of blockchain technology to ensuring reliability and data security in the internet of things // “Moliya-kredit tizimini strategik rivojlantirishning muammolari va ustuvor yo‘nalishlari” mavzusida xalqaro ilmiy-amaliy konferensiya 2024-yil 25-aprel. –b. 27-29.
3. Kim-Kwang R.Ch., Ali D., Reza M. P., Blockchain Cybersecurity, Trust and Privacy. 2021
4. Alex Mathew, Cyber Security through Blockchain Technology, 2019.
5. Васильева Е.П. Блокчейн и кибербезопасность: вызовы и возможности для российских предприятий // Информационная безопасность в условиях цифровизации. 2019. С. 155-167.
6. Григорьев М.Н. Эффективность применения технологии блокчейн в защите от киберугроз // Инн овации в кибербезопасности. 2021. С. 33-45.
7. Иванов П.С. Роль блокчейн-технологий в обеспечении кибербезопасности корпоративных информационных систем // Компьютерные технологии и

безопасность. 2019. № 2 (18). С. 78-92.
8. Назаров А.Н. Блокчейн в кибербезопасности: проблемы и перспективы // Информационная безопасность. 2018. № 3 (25). С. 45-58.
9. Петров Д.А. Блокчейн и кибербезопасность: перспективы применения в российских компаниях // Информационные технологии в бизнесе. 2016. № 1 (10). С. 56-68.
10. Смирнов В.С. Применение технологии блокчейн в сфере кибербезопасности в России // Инновации в информационной безопасности. 2020. С. 112-126.
11. Соколов Н.Н. Развитие блокчейн-технологий как средства обеспечения кибербезопасности в России. 2020. № 4 (30). С. 112-125.
12. Чернов А.К. Применение технологии блокчейн в системах обеспечения кибербезопасности критической информационной инфраструктуры // Информационная безопасность и защита данных. 2018. С. 87-99