

MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI
FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

“AL-FARG‘ONIIY AVLODLARI”

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI



3-SON 1(7)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON



O'ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
FARG'ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali.

Chop etish tili: O'zbek, ingliz, rus. Jurnal texnika fanlariga ixtisoslashgan bo'lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo'nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.

Язык издания: узбекский, английский, русский. Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.

Language of publication: Uzbek, English, Russian. The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2024 yil, Tom 1, №3
Vol.1, Iss.3, 2024 y

ELEKTRON ILMIY JURNALI

ELECTRONIC SCIENTIFIC JOURNAL

«Al-Farg'oniyl avlodlari» («The descendants of al-Fargani», «Potomki al-Fargani») O'zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro'yxatdan o'tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo'nalishida milliy nashrlar ro'yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg'ona sh.,
Aeroport ko'chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2024 YIL

TAHRIR HAY'ATI

Maxkamov Baxtiyor Shuxratovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti rektori, iqtisodiyot fanlari doktori, professor

Muxtarov Farrux Muhammadovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali direktori, texnika fanlari doktori

Arjannikov Andrey Vasilevich,

Rossiya Federatsiyasi Sibir davlat universiteti professori, fizika-matematika fanlari doktori

Satibayev Abdugani Djunosovich,

Qirg'iziston Respublikasi, Osh texnologiyalari universiteti, fizika-matematika fanlari doktori, professor

Rasulov Akbarali Maxamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Axborot texnologiyalari kafedrasida professori, fizika-matematika fanlari doktori

Yakubov Maksadxon Sultaniyazovich,

Muhammad al-Xorazmiy nomidagi TATU «Axborot texnologiyalari» kafedrasida professori, t.f.d., professor, xalqaro axborotlashtirish fanlari Akademiyasi akademigi

G'ulomov Sherzod Rajaboyevich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent

G'aniyev Abduxalil Abdjalioviich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti, Axborot xavfsizligi kafedrasida t.f.n., dotsent

Zaynidinov Hakimjon Nasritdinovich,

Muhammad al-Xorazmiy nomidagi TATU Kompyuter injiniringi fakulteti, Sun'iy intellekt kafedrasida texnika fanlari doktori, professor

Abdullayev Abdujabbor,

Andijon mashinosozlik instituti, Iqtisod fanlari doktori, professor

Qo'ldashev Abbosjon Hakimovich,

O'zbekiston milliy universiteti huzuridagi Yarimo'tkazgichlar fizikasi va mikroelektronika ilmiy-tadqiqot instituti, texnika fanlari doktori, professor

Ergashev Sirojiddin Fayazovich,

Farg'ona politexnika instituti, elektronika va asbobsozlik kafedrasida professori, texnika fanlari doktori, professor

Polvonov Baxtiyor Zaylobiddinovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy ishlar va innovatsiyalar bo'yicha direktor o'rinbosari

Zulunov Ravshanbek Mamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Dasturiy injiniring kafedrasida dotsenti, fizika-matematika fanlari nomzodi

Abdullaev Temurbek Marufovich,

Muhammad al-Xorazmiy nomidagi TATU Axborot texnologiyalari kafedra mudiri, texnika fanlar bo'yicha falsafa doktori

Zokirov Sanjar Ikromjon o'g'li,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlar tayyorlash bo'limi boshlig'i, fizika-matematika fanlari bo'yicha falsafa doktori

Jurnal quyidagi bazalarda indekslanadi:



Eslatma! Jurnal materiallari to'plamiga kiritilgan ilmiy maqolalardagi raqamlar, ma'lumotlar haqqoniyligiga va keltirilgan iqtiboslar to'g'riligiga mualliflar shaxsan javobgardirlar.

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

I.R.Rahmatullayev, O.Sh.Umurzakov, E.I.Saydullayev, Xesh funksiya algoritmlari tasodifiyligini NIST testlari bilan baholash	6-14
Xatamova M.K., Matsapayev J.S., Kuchkarov V.A., Simulation and design of a small-sized pentagon broadband antenna for 5G connectivity	15-20
Abdurasulova D., Kuldashov O., Development of a method of stabilization of two-color light-emitting diode parameters	21-25
Шарифбаев А.Н., Зайниддинов Х.Н., Применение графовые нейронные сети и его модификации с обучения с подкреплением в системах рекомендаций	26-29
Muminov O., LOGISTIK MUAMMOLAR VA POTENTIAL YECHIMLAR: QURUQLIK BILAN O'RALGAN O'ZBEKISTON HOLATI	30-36
Сотволдиев Х.И., ПРИМЕНЕНИЕ ИГРОВЫХ МЕТОДОВ ДЛЯ РАЗРАБОТКИ МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ УСТОЙЧИВЫХ АЛГОРИТМОВ УПРАВЛЕНИЯ НЕСТАЦИОНАРНЫМИ ОБЪЕКТАМИ	37-41
Muhammediyeva D.K., Eshboyev E.A., Klicheva F.G., INTELLEKTUAL SUV TOMCHISI ALGORITMINING TIBBIY TASHXIS QO'YISH MASALALARIGA QO'LLANILISHI	42-47
Axatov A.R., Eshtemirov B.Sh., Mashinaviy o'qitish asosida yo'llardagi avtomobil tirbandlik holatlarini aniqlash uchun dastlabki ma'lumotlarni tayyorlash usullari	48-56
Allayarova G.X., Buronov N.R., Zaripov Sh.S., MoO ₃ /Mo NANOTUZULMALARINI OLISH VA ULARNING ELEKTRON TUZILISHI VA OPTIK XOSSALARINI O'RGANISH	57-60
Kurbanov A.A., INSON YUZ TASVIRIDAN HISSIYOTLARNI ANIQLASH UCHUN GEOMETRIK XUSUSIYATLARINI VA TASHQI KO'RINISHGA ASOSLANGAN XUSUSIYATLARINI AJRATIB OLISH	61-67
Radjabov S.S., Rabbimov I.M., Xusainov N.O., Abdullayeva B.M., BIOMETRIK TEXNOLOGIYALARNI RIVOJLANTIRISHNING ISTIQBOLLI YO'NALISHLARI	68-72
Jo'rayev M.T., TARMOQ OQIMINI MONITORING QILISH DASTURIY TIZIMI	73-77
Ganiyev S.K., Xamidov Sh.J., ELEKTRON POCHTA TIZIMI XAVFSIZLIGI RISKLARINI BAHOLASH USULI	78-81
Кенжаев С.С., Рашидов А.Э., МЕТОДЫ И АЛГОРИТМЫ ХРАНЕНИЯ ФАЙЛОВ ДЛЯ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ РАЗЛИЧНЫМИ ТИПАМИ ДАННЫХ	82-92
Уринбоев А.А., АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ВЛАЖНОСТЬЮ ЗЕРНА НА МУКОМОЛЬНОМ ЗАВОДЕ «ФАРГОНАДОНМАХСУЛОТЛАРИ»	93-100
Rahmatullayev I.R., Boyquziyev I.M., Umurzakov O.Sh., Saydullayev E.I., ELLIPTIK EGRI CHIZIQLAR ASOSIDA ASIMMETRIK ALGORITMLARNING MATEMATIK ASOSLARI VA ULARNI QO'LLASH MASALALARI	101-108
Адилов Ф.Ф., Турдибеков Ж.Э., ИССЛЕДОВАНИЕ КРУЧЕНИЯ ЦИЛИНДРИЧЕСКОГО СТЕРЖНЯ ПОД ТЕРМОМЕХАНИЧЕСКИМ ВОЗДЕЙСТВИЕМ	109-112
Mukhammadjonov A.G., Tokhirova S.G., ANALYSIS OF AUTOMATION THROUGH MOISTURE MONITORING DEVICES IN INDUSTRIAL AND AGRICULTURAL FIELDS	113-118
Хамзаев Д.И., РАЗРАБОТКА МЕТОДОВ ПРИМЕНЕНИЯ RFID В ПРОИЗВОДСТВЕ ХИМИЧЕСКИХ УДОБРЕНИЙ	119-123
Mavlonov O.N., TARMOQ PROTOKOLLARIDA AXBOROTLARNI YASHIRISHDA YUZAGA KELADIGAN MUAMMOLAR	124-128
Artikova G.G., Matyakubov D.D., GSM TARMOG'IDA QO'LLANILADIGAN KODLASH ALGORITMLARI TANLILI	129-132
Сотволдиев Х.И., Математическая модель и система управления прямоточными котлами с пылесистемой прямого вдувания	133-138
Yo'ldashev X.S., Sarimsakov O.Sh., Ergashev Sh.T., PAXTA TOLASI BILAN HAVO ARALASHMASI OQIMI HARAKATINI MODELLASHTIRISH	139-144

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Сафарова Л.У., Применения вариационного квантового алгоритма (VQE) в агропромышленном комплексе	145-148
Muminov K.Z., Social Engineering, Human Factor in Cybersecurity	149-152
Djurayev Sh.S., MULTISIKLON QURILMASI SAMARADORLIGIGA ZARRALAR O'LGHAMU VA KONSENTRATSIYASINING TA'SIRI	153-158
Mirzayev N., Radjabov S.S., Rabbimov I.M., Asrayev M.A., Mardiyev A.Sh., HUE MOMENTLARIGA ASOSLANGAN QO'LYOZMA MATNI TASVIRI BELGILARINI AJRATIB OLISH ALGORITMI	159-164
Shaxobutdinov R.E., Karimova A.R., Nosirov T.N., ZOLDIR PROKATLASH STANI ISHCHI ELEMENTLARINING KONSTRUKSIYALARINI ISHLAB CHIQUV MASALASI	165-169
Djalilov B.O., Muhammadjonov A.G., ANTENNANI QAYTA SOZLASHDA P-I-N DIODLARDAN FOYDALANISH, NAZARIY VA AMALIY QO'LLANISHLAR	170-173
Xudoyqulov Z.T., Qurbonaliyeva D.V., Bozorov S.M., HONEYPOT TEXNOLOGIYASINING FUNKSIONAL IMKONIYATLARINI TADQIQ ETISH	174-180
Xudoyqulov Z.T., Seidullayev M.K., IOT TEXNOLOGIYASIDA BLOKCHEYN ASOSIDA MA'LUMOTLARNI XAVFSIZ ALMASHISHNING TAKOMILLASHGAN USULI	181-190

Xesh funksiya algoritmlari tasodifiyligini NIST testlari bilan baholash

I.R.Rahmatullayev,
O.Sh.Umurzakov,
E.I.Saydullayev,
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari
universiteti Samarqand filiali

Annotatsiya: Ushbu maqolada zamonaviy kriptografiya muhim ahamiyatga ega bo'lgan xesh funksiyalari algoritmlarining tasodifiyligi va kolliziyalarga chidamliligi baholanadi. Xesh algoritmlari ma'lumotlarning yaxlitligi va autentifikatsiyasini ta'minlash uchun qo'llaniladi. Ular xesh qiymatlarini hisoblash orqali ma'lumotlarning asl va ishonchli ekanligini tasdiqlaydi. Maqolada NIST (Standartlar va Texnologiyalar Milliy Instituti) tomonidan ishlab chiqilgan statistik testlar yordamida turli xesh algoritmlari, jumladan, SHI-1, SHI-2, SHI-3 va SHA-1 ning tasodifiylik darajasi baholanadi. Natijalar SHI-3 algoritmining yuqori darajadagi xavfsizlik va tasodifiylikka ega ekanligini ko'rsatadi, SHA-1 algoritmi esa ba'zi zaif tomonlarini namoyon etadi. Ushbu tahlillar xesh algoritmlarining umumiy xavfsizlik darajasini baholashda va ularning amaliyotda qo'llanishini tahlil qilishda muhim ahamiyatga ega.

Kalit so'zlar: Xesh funksiyalari, kriptografiya, tasodifiylik, kolliziya, NIST STS testi, SHA-1, SHI-3, xavfsizlik, autentifikatsiya, raqamli imzo.

I. Kirish

Bugungi kunda zamonaviy kriptografiya telekommunikatsiya tarmoqlari orqali yuborilayotgan ma'lumotlarning butunligi va haqiqiylikni nazorat qilishda xesh funksiyalari algoritmlari katta ahamiyatga ega. Xesh algoritmlari ma'lumotlarning o'zgarishini ta'minlash va ularga har qanday o'zgarishlar kiritilgan yoki yo'qligini aniqlash uchun qo'llaniladi. Ular axborotning autentifikatsiyasini ta'minlab, qabul qiluvchiga ma'lumotning asl va ishonchli ekanligiga kafolat beradi. Shu tariqa, ma'lumotlar tez, samarali va xavfsiz usullarda qayta ishlanadi, bu esa telekommunikatsiya tizimlarining xavfsizligini oshirishda muhim ahamiyat kasb etadi[1].

Xesh algoritmlarini baholashda eng asosiy mezonlardan biri ularning kolliziyalarga chidamliligidir. Kolliziya — turli ma'lumotlar uchun bir xil xesh qiymati hosil bo'lishi holati bo'lib, bu xavfsizlik jihatidan katta ahamiyatga ega muammo. Xesh funksiyalarining kolliziyalarga chidamliligini aniqlash uchun turli kriptotahlil usullaridan foydalaniladi. Bunday usullarga kalitlarning barcha ehtimoliy kombinatsiyalarini tekshirish, tug'ilgan kun

paradoksi, differentsial va integral kriptotahlil kabi metodlar kiradi, ular yordamida algoritmning barqarorligi va xavfsizligi baholanadi[2]. Ilmiy tadqiqotlar va adabiyotlar tahliliga ko'ra, xesh funksiyalarining kolliziyalarga bardoshliligini ta'minlash uchun ularning tasodifiylik xususiyati muhim ahamiyatga ega. Shuning uchun, xesh algoritmlarining tasodifiylik darajasini baholash juda muhim, chunki bu algoritmning xavfsizligi va samaradorligiga bevosita ta'sir qiladi[3]. Xesh funksiyalarining tasodifiylik xususiyatlarini baholashda NIST (Standartlar va Texnologiyalar Milliy Instituti) tomonidan ishlab chiqilgan testlar to'plamidan foydalaniladi. Ushbu NIST testlari xesh algoritmlarining xavfsizligini kuchaytirish va ularning kolliziyalarga nisbatan chidamliligini ta'minlashda muhim vositalardan biri hisoblanadi[4].

Faraz qilaylik, uzunligi n bit bo'lgan $\xi = \{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n\}$, ketma-ketlik berilgan, bunda har bir $\varepsilon_i \in \{0,1\}$ ya'ni har bir element 0 yoki 1 qiymatini qabul qiladi. Bu shuni anglatadiki, ξ ikkilik bitlardan tashkil topgan bo'lib, har bir bit faqat ikki xil qiymatga ega bo'lishi mumkin: 0 yoki 1.



Bunday ikkilik ketma-ketliklar turli kriptografik algoritmlarda, xususan xesh funksiyalari va shifrlash jarayonlarida katta ahamiyatga ega. Ular yordamida ma'lumotlarni raqamli shaklda ifodalash, axborotni shifrlash va boshqa ko'plab kriptografik operatsiyalarni amalga oshirish mumkin. Ikkilik ketma-ketliklar ma'lumotlarni kodlash va ularning xavfsizligini ta'minlashda asosiy vosita hisoblanadi[5-10].

Uzunligi n bo'lgan ketma-ketlikning har bir biti ma'lumotning ajralmas va muhim qismi bo'lib, har qanday bitning o'zgarishi butun ma'lumotning o'zgarishiga olib kelishi mumkin. Bu har bir bitning ahamiyatini ko'rsatadi, chunki ular umumiy ma'lumotni aniqlashda hal qiluvchi rol o'ynaydi[11-15].

Xesh funksiya algoritmlarining tasodifiylik xususiyatlarini tekshirish uchun adabiyotlarda taklif etilgan oltita bosqichli algoritmdan foydalaniladi. Ushbu bosqichlar orqali xesh algoritmining tasodifiylik xususiyatlari aniqlanib, baholanadi. Tasodifiylik — xesh funksiyasining xavfsizlik va samaradorlik darajasini belgilovchi muhim parametr bo'lib, quyidagi bosqichlar ushbu jarayonni amalga oshirishda asosiy rol o'ynaydi:

1. Ma'lumotlarni tayyorlash: Xesh funksiyasini sinovdan o'tkazish uchun zarur bo'lgan ma'lumotlar tayyorlanadi. Ushbu ma'lumotlar ikkilik ketma-ketliklar yoki bitlar ko'rinishida bo'lib, sinov uchun asos bo'ladi.

2. Xesh qiymatlarini hisoblash: Tayyorlangan har bir ma'lumot uchun xesh funksiyasi qo'llanilib, xesh qiymatlari hisoblanadi. Bu bosqichda turli ma'lumotlar uchun hosil bo'lgan xesh qiymatlari o'rganiladi va tahlil qilinadi.

3. Tasodifiylikning dastlabki bahosi: Olingan xesh qiymatlari tasodifiylik nuqtai nazaridan dastlabki tahlil qilinadi. Ularning belgilangan tasodifiylik me'yorlariga qanchalik mos kelishi aniqlanadi.

4. Tasodifiylik testlarini qo'llash: Xesh qiymatlarining tasodifiyligini yanada chuqurroq baholash uchun NIST (Milliy Standartlar va Texnologiyalar Instituti) tomonidan ishlab chiqilgan testlar to'plami qo'llaniladi. Ushbu testlar xesh

qiymatlarining bitlar ketma-ketligini tahlil qilib, ularning tasodifiylik darajasini aniqlaydi.

5. Kolliziyalarga chidamlilikni tekshirish: Xesh funksiyasi turli ma'lumotlar uchun bir xil xesh qiymatini hosil qilmasligini tekshirish, ya'ni kolliziya ehtimolini baholash amalga oshiriladi. Bu xesh funksiyasining xavfsizligini ta'minlash uchun muhimdir.

6. Natijalarni tahlil qilish va baholash: Olingan barcha natijalar tahlil qilinib, xesh algoritmining tasodifiylikka va kolliziyalarga bardoshlilik bo'yicha yakuniy xulosa chiqariladi.

Ushbu bosqichlar yordamida xesh funksiyasining xavfsizligi va ishonchliligi har tomonlama baholanadi. Natijada, kriptografik tizimlarning umumiy ishonchliligi va xavfsizligi oshiriladi, bu esa axborot almashinuvini yanada himoyalangan holga keltiradi[8].

II. Asosiy qism

Kolliziyalarni aniqlashda xesh funksiyasi algoritmlarini tasodifiylikka NIST STS (Statistical Test Suite) paketidan foydalangan holda baholashning oltita bosqichli jarayoni zaruriy tahlil usuli ekanligini ko'rsatish maqsadida, amaliy masalalarda quyidagi xesh algoritmlari tanlab olindi:

1. SHI-1 – o'quv xesh algoritmi;
2. SHI-2 – o'quv xesh algoritmi;
3. SHI-3 – o'quv xesh algoritmi;
4. SHA-1 – standart xesh funksiyasi algoritmi.

Ushbu xesh algoritmlari turli samaradorlik va xavfsizlik darajalariga ega. Ularning tasodifiylikka bo'lgan bardoshlilik NIST STS paketi yordamida baholandi. NIST STS testlari ushbu algoritmlar tomonidan yaratilgan xesh qiymatlarining tasodifiylik xususiyatlarini aniqlashga yordam beradi va ularning samaradorligi hamda xavfsizligini tekshirish imkonini yaratadi.

SHI-1, SHI-2 va SHI-3 algoritmlari o'quv maqsadlarida yaratilgan bo'lib, ularning har biri turli kriptografik xususiyatlar va kolliziyalarga chidamlilik darajasini o'rganish uchun qo'llaniladi. SHA-1 esa kriptografiyada keng qo'llaniladigan standart algoritm sifatida tanlangan.



Tanlangan xesh algoritmlarining har biri NIST STS paketining turli testlari orqali tekshirilib, ularning tasodifiyligi va kolliziyalarga chidamliligi baholandi. Natijada, xesh algoritmlarining xavfsizlik darajasi va ishonchliligi aniqlanadi. Ushbu tahlil kolliziyalarni aniqlashda muhim ahamiyatga ega bo'lib, qaysi algoritm xavfsizlik nuqtai nazaridan afzal ekanligini ko'rsatadi.

Xesh funksiyasi algoritmlarini tasodifiylikka NIST STS paketi [2] bilan tekshirish uchun yaratilgan dasturiy ta'minot orqali olingan natijalar quyida keltiriladi:

1. SHI-1 algoritmi:

- Tasodifiylik testlari natijasida xesh qiymatlarining tasodifiylikka yetarlicha mos kelmasligi aniqlandi. Bu algoritmning kolliziyalarga chidamliligi past ekanligiga ishora qiladi.

- NIST STS testlarining aksariyatida tasodifiylik darajasi talablariga javob bermadi, bu esa uning xavfsizlik nuqtai nazaridan zaifligini ko'rsatadi.

2. SHI-2 algoritmi:

- Tasodifiylik testlari natijalariga ko'ra, xesh qiymatlarining tasodifiylik darajasi ayrim testlarda yetarli bo'ldi, ammo umumiy holatda ba'zi testlarda talabga javob bermadi.

- Kolliziyalarga nisbatan chidamlilik darajasi o'rtacha deb baholandi, ya'ni u ba'zi xavfsizlik talablariga javob beradi, lekin mukammal emas.

3. SHI-3 algoritmi:

- Tasodifiylik testlari natijasiga ko'ra, ushbu algoritmning xesh qiymatlari yuqori darajada tasodifiylikka ega bo'ldi. U NIST STS testlarining ko'pchiligidan muvaffaqiyatli o'tdi.

- Kolliziyalarga nisbatan chidamlilik yuqori ekanligi aniqlandi, bu esa uni xavfsizlik va ishonchlilik nuqtai nazaridan afzal qiladi.

4. SHA-1 standart algoritmi:

- Tasodifiylik testlari natijalari ushbu algoritmning yetarlicha tasodifiy ekanligini ko'rsatdi, ammo ba'zi bit ketma-ketliklarida ma'lum bir naqshlar kuzatildi.

- NIST STS paketining asosiy testlaridan o'tgan bo'lsa-da, kolliziyalarga nisbatan chidamliligi ayrim holatlarda past ekanligi ma'lum bo'ldi. Bu esa

uning ba'zi xavfsizlik cheklovlariga ega ekanligini bildiradi.

Ushbu natijalar xesh algoritmlarining tasodifiylik va kolliziyalarga chidamlilik darajasini baholashda muhim ahamiyatga ega. Tahlil natijasida SHI-3 algoritmi eng yuqori tasodifiylik va kolliziyalarga chidamlilik darajasiga ega ekanligi aniqlandi, bu esa uni xavfsizlik nuqtai nazaridan eng afzal qiladi. SHA-1 algoritmi esa standart bo'lishiga qaramay, ba'zi zaif tomonlari borligi aniqlangan.

Shunday qilib, xesh funksiyasi algoritmlarini tasodifiylikka NIST STS paketi yordamida baholash kolliziyalarni aniqlash va algoritmning umumiy xavfsizlik darajasini baholashda muhim vosita hisoblanadi. Bu usul kriptografik algoritmlarni tanlashda va ularning samaradorligini oshirishda asosiy rol o'ynaydi, chunki u algoritmning tasodifiylik va kolliziyalarga chidamlilik xususiyatlarini chuqur tahlil qilish imkonini beradi.

Natijalardan ko'rinib turibdiki, SHI-3 algoritmi eng samarali va xavfsiz xesh funksiyasi sifatida tanlandi, chunki uning tasodifiylik darajasi yuqori va kolliziyalarga chidamliligi yaxshilangan. SHA-1 esa standart algoritm bo'lishiga qaramay, ba'zi xavfsizlik nuqsonlariga ega bo'lib, tasodifiylik darajasida ayrim cheklovlar aniqlandi.

Ushbu natijalar NIST STS paketidan foydalanish orqali xesh algoritmlarining xavfsizlik va ishonchlilik darajasini baholashda dasturiy ta'minotning samaradorligini namoyon etdi.

NIST STS paketi testlari orqali xesh funksiya algoritmlarini tekshirishda quyidagi parametrlar tanlandi va ular asosida testlar amalga oshirildi:

1. Ketma-ketlik uzunligi $n=10^6$ bit: Har bir xesh qiymati uzunligi 1 million bitdan iborat bo'lib, bu xesh funksiyasining tasodifiylik va xavfsizlik parametrlarini aniqlash uchun yetarli uzunlikni ta'minlaydi.

2. Ketma-ketliklar soni $m = 100$: Har bir algoritm uchun 100 ta ketma-ketlik yaratilib, ular NIST STS testlaridan o'tkazildi. Bu miqdor statistik jihatdan ishonchli natijalar olish uchun yetarli hisoblanadi.

3. Tanlov hajmi $N = 10^6 \times 100 = 10^8$ bit: Testlar uchun tanlangan umumiy ma'lumot hajmi 100 million bitni tashkil etadi, bu hajm algoritmlarning



tasodifiylik xususiyatlarini aniqlashda muhim ahamiyat kasb etadi.

4. Qimmatlilik darajasi $\alpha = 0.01$ va $\alpha = 0.001$: Bu testlarning ishonch darajasini belgilaydi. $\alpha = 0.01$ degani 99% ishonchlilikda, $\alpha = 0.001$ esa 99.9% ishonchlilikda tasodifiylik testlari o'tkaziladi. Natijalarning ishonchlilik darajasi yuqori bo'ladi, bu esa test natijalarining aniqligini ta'minlaydi.

5. Testlar soni $q = 188$: Har bir algoritm 188 turdagi testdan o'tkazildi. Bu testlar algoritmning turli jihatlarini baholash uchun mo'ljallangan bo'lib, ular orasida bitlar ketma-ketligidagi tasodifiylik, bitlarning taqsimlanishi, naqshlarning mavjudligi va boshqa kriptografik xususiyatlar tekshiriladi.

6. Statistik portret: Har bir xesh funksiya algoritmi uchun 18,800 ta P -ehtimollik qiymatlari hisoblandi. Bu qiymatlar algoritmning statistik tasviri va xavfsizlik ko'rsatkichlarini baholashda foydalaniladi hamda uning tasodifiylik darajasini aniqlashga yordam beradi.

Ushbu parametrlar asosida amalga oshirilgan NIST STS testlari xesh funksiya algoritmlarining tasodifiylik va kolliziyalarga chidamliligini baholashga yordam beradi. Ular xesh algoritmlarining samaradorligini statistik jihatdan baholab, qaysi algoritm xavfsizroq ekanligini aniqlaydi.

Ideal holatda, agar $m = 100$ va $\alpha = 0.01$ bo'lsa, har bir testdan o'tish ehtimoli 99% bo'lishi kerak, ya'ni 100 ta ketma-ketlikdan faqat bittasi testdan o'tmasligi mumkin. Biroq, bu juda qat'iy shart bo'lgani uchun, ishonchli intervallardan foydalanish muhim ahamiyatga ega. Bu holatda ishonchli interval quyidagi tarzda hisoblanadi:

Ishonchli intervalni hisoblash uchun binomial taqsimotdan foydalaniladi. Testdan o'tmagan ketma-ketliklar soni uchun kutilgan o'rtacha qiymat

$$\mu = m \times \alpha = 100 \times 0.01 = 1 \text{ bo'ladi.}$$

Ishonchlilik darajasiga mos ravishda z -skor yordamida ishonchli interval quyidagicha hisoblanadi:

$$\text{Ishonchli interval } \mu \pm z \times \sigma$$

Masalan, 95% ishonchlilik darajasi uchun $z \approx 1.96$ bo'lsa, ishonchli interval quyidagicha bo'ladi:

$$\sigma = \sqrt{100 * 0.01 * 0.99} = \sqrt{0.99} \approx 0.9949$$

Ishonchli interval $1 \pm 1.96 \times 0.9949$

Ishonchli interval 1 ± 1.949

Shunday qilib, ishonchli interval $[0, 2.949]$ oraliqda bo'ladi (chunki manfiy sonlar qabul qilinmaydi). Demak, test natijalarida testdan o'tmagan ketma-ketliklar soni 3 tagacha bo'lsa, bu normal holat deb hisoblanadi va xesh funksiyasi tasodifiylik testidan muvaffaqiyatli o'tdi deb qaraladi. Agar testdan o'tmagan ketma-ketliklar soni 3 dan oshsa, bu xesh funksiyasining tasodifiylik darajasi past ekanligini ko'rsatishi mumkin.

Ishonchli intervalni hisoblash test natijalarini to'g'ri talqin qilish va xesh algoritmlarining tasodifiylik darajasini aniq baholashda muhim ahamiyatga ega. Bu usul yordamida xesh funksiyalarining xavfsizlik darajasi va kolliziyalarga chidamliligi yanada aniqroq baholanadi.

Testdan o'tish foizining quyi chegarasi r_{\min} quyidagi formula orqali hisoblanadi:

$$r_{\min} = p - z * \sqrt{\frac{p * (1 - p)}{m}}$$

bu yerda:

- $p = 0.99$ — testdan o'tish ehtimoli;
- z — ishonch darajasiga mos keladigan standart normal taqsimotdan olinadigan qiymat (masalan, 95% ishonch intervali uchun $z \approx 1.96$);
- m — testlar soni, ya'ni 100.

Shunday qilib, quyi chegara r_{\min} testlarning talablarga mos kelishi uchun ishonchli intervaldagi pastki chegarani aniqlaydi.

Testlar natijasiga ko'ra, agar natijalar r_{\min} qiymatidan yuqori bo'lsa, test o'tkazilgan algoritm ishonchli deb baholanadi.

Bu degani, testdan o'tayotgan har bir tanlov (ketma-ketliklar) uchun muvaffaqiyatli o'tish ehtimoli 96% dan kam bo'lmasligi kerak. Agar muvaffaqiyatli o'tgan ketma-ketliklar foizi 96% yoki undan yuqori bo'lsa, bu testdan o'tish talablariga mos keladi va algoritm ishonchli deb baholanadi.

III. Natijalar

Bu ishonchli interval doirasidagi quyi chegaradir, va unga muvofiq, testdan o'tgan xesh



algoritm muvaffaqiyatli deb baholandi, va 99% talablar bo'yicha ham juda yaxshi natijalar ko'rsatgan. Bu algoritm yuqori darajada tasodifiylikka va xavfsizlikka ega ekanligini ko'rsatadi.

4-jadval.

SHA-1 xesh funksiya algoritmi uchun NIST testi natijalari.

№	Xesh funksiya algoritmi	Ketma-ketlikning 96% dan ortiq testdan o'tganlari soni	Ketma-ketlikning 99% dan ortiq testdan o'tganlari soni
1	SHA-1	182 (96.80%)	120 (63.83%)
2	SHA-1	181 (96.28%)	119 (63.30%)
3	SHA-1	183 (97.34%)	122 (65.32%)
4	SHA-1	180 (95.74%)	118 (62.77%)
5	SHA-1	182 (96.80%)	121 (64.36%)
6	SHA-1	181 (96.28%)	120 (63.83%)
		O'rtacha foizi	181.5 (96.37%)

IV. Natijalar Tahlili:

1. 96% dan ortiq testdan o'tgan ketma-ketliklar:

- Har bir holatda 96% dan ortiq ketma-ketliklar muvaffaqiyatli testdan o'tgan. Algoritmning tasodifiylik darajasi belgilangan quyi chegaralarga mos keladi.
- O'rtacha hisobda 96.37% ketma-ketlik 96% dan ortiq testdan muvaffaqiyatli o'tgan, bu **quyi chegara talablariga** to'liq javob beradi.

2. 99% dan ortiq testdan o'tgan ketma-ketliklar:

- 99% dan ortiq testdan o'tgan ketma-ketliklar soni nisbatan pastroq, taxminan 62.77% dan 65.32% gacha bo'lgan holatlarda qayd etilgan.
- O'rtacha hisobda 63.90% ketma-ketlik 99% dan ortiq testdan muvaffaqiyatli o'tgan, bu qiymat ko'p holatlarda pastroq hisoblanadi, lekin 99% test talablariga yaqin foizda bo'lganini ko'rsatadi.

SHA-1 xesh algoritmi NIST testlaridan muvaffaqiyatli o'tdi, ayniqsa, 96% test talablari bo'yicha. Ammo 99% talablar bo'yicha natijalar

nisbatan pastroq, taxminan 63.90% darajada bo'lib, bu algoritmning yuqori xavfsizlik talablariga to'liq mos kelmasligini ko'rsatadi. Har qanaqasiga, **SHA-1** standart xesh algoritmi deb hisoblanishiga qaramay, uning xavfsizlik darajasi zamonaviy talablarga ko'ra etarli emasligi haqidagi xulosani qo'llab-quvvatlaydi.

O'tkazilgan tahlil natijalariga asoslanib, quyidagi xulosalarni keltirish mumkin:

1. SHA-1, SHA-2, SHA-3 xesh funksiya algoritmlarini NIST paketi testlari orqali tasodifiylikni tekshirish natijasida past (mos ravishda 16%, 65%, 66%) foiz ko'rsatkichlari olindi. Bu natijalar ushbu xesh algoritmlarda bir qator muhim tuzilmalarning samarali emasligi bilan xarakterlanadi:

- Yagona chiziqsiz aksantirishning mavjud emasligi: Xesh algoritmlarda chiziqsizlik mexanizmlari kerakli darajada tatbiq etilmagan. Bu, ayniqsa, xavfsizlik nuqtai nazaridan muhim, chunki chiziqsizlik ma'lumotni "aralashtirish" va hujumlarga qarshi chidamlilikni ta'minlashga yordam beradi.

- mod232 bo'yicha qo'shish amalining mod2 amaliga almashtirilishi: Kriptografik algoritmlarda mod2 amali ko'pincha chiziqli bo'lib, xavfsizlikni kuchaytirish uchun ko'pincha modulli arifmetika (mod232 kabi) talab qilinadi. Bunday amaliyotni yoritib bermaslik algoritmning xavfsizligiga salbiy ta'sir ko'rsatishi mumkin.

- Raund aksantirishi ($f(x, y, z) = x \oplus y \oplus z$): Bu funksiya chiziqli bo'lib, xavfsizlik uchun etarli darajada samarali emas. Chiziqli funksiyalar hujumchiga algoritmni tahlil qilishni osonlashtirishi mumkin, chunki ular ma'lumotni yuqori darajada aralashtirmaydi.

- Nisbatan past chiziqsizlik qiymati: *mod232* bo'yicha qo'shish amalida chiziqsizlik qiymati pastligi xesh algoritmlarning xavfsizlikka salbiy ta'sir ko'rsatadi. Chiziqsizlik algoritmning kuchli himoyasini ta'minlaydigan muhim omildir, va uning past bo'lishi algoritmni potensial hujumlarga mos qiladi.

Bu xulosalardan ko'rinib turibdiki, xesh funksiya algoritmlarining xavfsizligi va tasodifiylik ko'rsatkichlari asosan chiziqsizlik darajasiga bog'liq. Natijalar algoritmlarning kriptografik jihatdan



samaraliligini oshirish uchun ularda kuchliraq chiziqsizlik mexanizmlarini tatbiq etish zarurligini ko'rsatadi.

2. Xesh funksiya algoritmlarini NIST paketi testlari bilan tasodifiylikka tekshirishda past foiz ko'rsatkichdagi natijalar olinishi quyidagilarni ko'rsatadi:

1. Algoritm strukturasi qusurlar: Past natijalar xesh funksiya algoritmining ichki tuzilmasida turli kamchiliklar va qusurlar mavjudligini anglatadi. Bu kamchiliklar algoritmnining xavfsizlik va tasodifiylik talablariga to'liq javob bermasligiga olib keladi.

2. Jadal samaradorlik darajasining etarli emasligi: Xesh algoritmnining samaradorligi past bo'lsa, u ma'lumotlarni yaxlitlik va xavfsizlik nuqtai nazaridan samarali qayta ishlay olmaydi. Bu algoritmnining kuchli himoya qilish qobiliyatini pasaytiradi.

3. Kolliziya topilishiga moyillik: Past tasodifiylik natijalari xesh funksiya algoritmda kolliziyalarni oson topish imkonini oshiradi. Kolliziya — bu turli ma'lumotlar uchun bir xil xesh qiymatini aniqlash, va bu hujumchilarga ma'lumotni o'zgartirib hamda uning haqiqiylikini shubha ostiga qo'yish imkoniyatini beradi. Kolliziyalarni oson aniqlash xesh algoritmining xavfsizligiga jiddiy xavf tug'diradi.

4. Zarur instrument: Tasodifiylik testlari xesh funksiya algoritmining xavfsizligini baholash va kolliziyalarga chidamliligini aniqlash uchun zarur vositadir. Past natijalar xesh algoritmda xavfsizlik muammolari mavjudligini ko'rsatib, uning qayta ishlanishi yoki kuchliroq mexanizmlar bilan almashtirilishi kerakligini bildiradi.

Shu boisdan, xesh algoritmlarining NIST testlari orqali olingan natijalari ularning xavfsizligi va ishonchliligini baholashda muhim ahamiyatga ega.

Bevosita tahlillarga asoslanib, shunday xulosa qilish mumkin, imzoni qalbakilashtirish usullari ichida dastlabki ikki usul (kriptografik tahlil yoki boshqa vositalar orqali) xesh algoritmi ishlab chiqish jarayonida nisbatan kam ta'sirga ega. Bu usullar ko'p hollarda algoritmnining xavfsizlik va tasodifiylik xususiyatlarini sezilarli darajada buzmasligi mumkin.

Biroq, 3-usul — ya'ni algoritmdagi xatolar va kamchiliklardan foydalanib qalbakilashtirishga yo'l ochuvchi jarayonlar — bevosita muhim rol o'ynaydi. Bu usul quyidagilarni o'zida mujassam etadi:

1. Algoritmdagi tuzilmaviy xatoliklar: Xatolar algoritmnining ayrim bosqichlarida, xususan, xesh funksiyasida yoki raund mexanizmlarida muammolarga olib keladi. Bunday xatolar qalbakilashtirish va kolliziyalarni oson topish imkoniyatini oshiradi.

2. Chiziqsizlik va past darajadagi chiziqsizlik: Algoritmnining chiziqli bo'lishi yoki past darajada chiziqsizlikka ega bo'lishi algoritmnini kriptotahlilga nisbatan osonroq zaif qiladi. Shuning uchun 3-usul algoritmgaga ta'sir qilish va uning ishonchliligini pasaytirish uchun muhim hisoblanadi.

3. Kolliziyaga moyillik: Algoritmdagi kamchiliklar kolliziyalarni oson aniqlashga olib keladi. Qalbakilashtirish jarayonida kolliziyalardan foydalanish hujumchilar uchun juda samarali bo'ladi, bu esa 3-usulning asosiy xavfi hisoblanadi.

Shu sababli, 3-usul imzoni qalbakilashtirishda muhim rol o'ynaydi va xesh algoritmini ishlab chiqishda bu jarayonlarga alohida e'tibor qaratish lozim.

Ta'rif: Agar kriptotahlil jarayonida algoritm qadamlaridagi xatoliklardan foydalangan holda elektron raqamli imzoni (ERI) qalbakilashtirish imkoniyati paydo bo'lsa, kriptografiyada bunday ERI algoritmlari **kuchsiz** algoritmlar deb ataladi.

Bu shunday algoritmlar bo'lib, ulardagi tuzilmaviy yoki hisoblash jarayonidagi kamchiliklar hujumchilarga imzoni qalbakilashtirish imkonini beradi, bu esa algoritmnining xavfsizligiga jiddiy xavf tug'diradi. Kuchsiz ERI algoritmlarida kolliziyalarni topish oson bo'lib, bu hujumchilarga imzoni buzib, soxta ma'lumot bilan o'rtaga kirish imkoniyatini beradi.

Kuchsiz ERI (elektron raqamli imzo) algoritmlari shunday algoritmlardirki, ularning qadamlar ketma-ketligi bardoshli algoritmlarga o'xshash bo'lishi mumkin, lekin ulardagi kamchiliklardan foydalanib, maxfiy kalitni bilmasdan ham imzoni qalbakilashtirish mumkin. Bunda



hujumchi imzoni yaratadi va tekshiruvchi tomon uni to'g'ri deb qabul qiladi, chunki imzo tekshirish mexanizmi bu soxtalikni aniqlay olmaydi.

Amaliyotda bunday kuchsiz algoritmlardan foydalanish xavfli bo'lib, ma'lumotlar va tizimlar xavfsizligini jiddiy darajada xatar ostiga qo'yadi. Shuning uchun kuchsiz ERI algoritmlaridan foydalanish maqsadga muvofiq emas. Yangi imzo algoritmini ishlab chiqish jarayonida, bunday kuchsiz algoritmlarga alohida e'tibor qaratish juda muhim. Bu bilan algoritmnining mukammalligi ta'minlanib, uning qalbakilashtirishdan himoyasi kuchaytiriladi.

Xulosa. Ushbu maqolada xesh funksiya algoritmlarining tasodifiylik xususiyatlarini baholash uchun NIST STS test to'plami qo'llanildi. Natijalar xesh algoritmlarining xavfsizlik darajasini baholashda va ularni amaliyotda qo'llashda muhim ahamiyatga ega bo'lib, ularning kolliziyalarga chidamliligi va tasodifiylik darajasi o'rganildi. Tadqiqotda SHI-1, SHI-2, SHI-3 va SHA-1 kabi xesh algoritmlari tanlab olindi va har biri NIST STS testlari yordamida tahlil qilindi.

Natijalar shuni ko'rsatdiki, SHI-3 algoritmi eng yuqori tasodifiylik va kolliziyalarga chidamlilik darajasiga ega bo'lib, u xavfsizlik nuqtai nazaridan eng afzal algoritm hisoblanadi. Boshqa tomondan, SHI-1 algoritmi tasodifiylik darajasi past bo'lib, kolliziyalarga nisbatan zaif hisoblanadi. SHA-1 algoritmi esa standart bo'lishiga qaramay, ba'zi zaif tomonlarini ko'rsatdi va xavfsizlik darajasi zamonaviy talablarga to'liq mos kelmasligini aniqladi.

Ushbu tadqiqotdan kelib chiqadigan muhim xulosalardan biri shundaki, xesh funksiya algoritmlarining xavfsizligi va samaradorligini oshirish uchun ularning tasodifiylik xususiyatlarini yaxshilash zarur. Maqola natijalari shuni ko'rsatadiki, NIST STS testlari xesh algoritmlarining xavfsizligini baholash va ularning kolliziyalarga bardoshliligini aniqlashda samarali vosita hisoblanadi. Kelajakda kriptografik tizimlarni yanada ishonchli qilish uchun ushbu testlardan foydalanish davom ettirilishi lozim.

Umuman olganda, ushbu tadqiqot xesh funksiyalari algoritmlarining tasodifiylik xususiyatlarini baholash va ularning xavfsizligini

ta'minlashda muhim ahamiyatga ega bo'lib, zamonaviy kriptografik tizimlar uchun dolzarb masalalarni yoritadi. Bu tadqiqot natijalari kriptografik algoritmlarni tanlash va ularning samaradorligini oshirishda yo'l-yo'riq bo'lib xizmat qiladi.

Foydalanilgan adabiyotlar ro'yxati

1. Church, "An unsolvable problem of elementary number theory", American Journal of Mathematics, 58 (1936), 345–363.
2. Barbeau, E.J. Polynomials 1st edition, Springer (2003)
3. Case, M. "A beginners guide to the general number field sieve" (2003)
4. Crandall, R. Pomerance, C, Prime Numbers, 2nd edition, Springer (2010)
5. Hoffstein, J. An introduction to Mathematical Cryptography, 2nd edition, Springer (2010)
6. Lehmer, D.H, Powers, R.E "On Factoring Large Numbers". Bulletin of the American Mathematical Society. 37(10): 770-776, (1931)
7. Mckee J. Speeding Fermat's Factoring Method. American Mathematical Society. Mathematics Computation. Volume 68, Number 228, P. 1729-1737
8. Mollins, R. A brief history of factoring and primality testing B.C. (before computers) Mathematics Magazine), (2002).
9. Morrison, M. Brillhart, J. A Method of Factoring and the Factorization of F7. Mathematics of computation, volume 29, number 129, pages 183-205, January (1975).
10. Nisha, S. Farik, M. RSA Public Key Cryptography Algorithm – A review. International Journal of Scientific & Technology Research. 6, (2017)
11. Pollard, J.M. A Monte Carlo method for factorization. BIT 15, 331-334 (1975).
12. Pomerance, C. Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory, Part 1, H.W. Lenstra, Jr. and R. Tijdeman, eds. Math. Centre Tract 154, p 89-139. Amsterdam, (1982)



13. Rabah, K. Review of Methods for Integer Factorization Applied to Cryptography. *Journal of Applied Sciences*.6. p461, (2006)
14. Schnorr, C.P, Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation. In: Davies D.W. (eds) *Advances in Cryptology. Lecture Notes in Computer Science*, Vol 547. Springer, Berlin, Heidelberg, (1991).
15. Bressoud, D. M. *Factorization and Primality Testing*. — N. Y.: Springer-Verlag, 1989. — 260 p. — ISBN 0-387-97040-1.



Simulation and design of a small-sized pentagon broadband antenna for 5G connectivity

Xatamova Mavluda Komiljon qizi,

Urgench branch of the Tashkent University
of Information Technologies named after
Muhammad Al- Khorazmi,
Khorezm,Uzbekistan
xatamovamavluda7@gmail.com

Matsapayev Jamshidbek Sodiqjon o‘g‘li,

Urgench branch of the Tashkent University
of Information Technologies named after
Muhammad Al- Khwarizmi,
Khorezm,Uzbekistan
matsapayevjamshid@gmail.com

Voxid Kuchkarov Alisherovich,

Urgench branch of the Tashkent University
of Information Technologies named after
Muhammad Al- Khwarizmi,
Khorezm,Uzbekistan
voxidkuchkarov@umail.uz

Abstract: The development of fifth-generation (5G) mobile networks requires the creation of compact, efficient and broadband antennas capable of operating at high frequencies, including millimeter waves (25-40 GHz). Antennas for 5G should provide high bandwidth, low latency and high connection density. One approach to achieve these goals is to develop miniature antennas of unusual geometry, such as pentagon-shaped antennas. The pentagonal shape makes it possible to achieve efficient use of space and improve frequency characteristics, which makes it attractive for 5G devices. This article discusses the process of modeling a pentagonal antenna for 5G networks.

Keywords: pentagonal antenna, 5G, 25-40 GHz, 28 GHz, CST studio Suite.

Introduction

1. Antennas for 5G:

Features and requirements Antennas for 5G networks must meet the following basic requirements:

- **Broadband:** 5G requires an antenna capable of operating at frequencies from 24 to 40 GHz to ensure high bandwidth. **Compact:** 5G devices such as smartphones and IoT devices require miniature antennas that can be easily integrated into a limited space.

- **High efficiency and low losses:** it is necessary to minimize losses and ensure maximum gain.

- **Versatility:** Antennas for 5G often require radiation circuits with a wide coverage angle to ensure reliable communication in urban environments and

high device densities. A pentagonal antenna may be a suitable solution, as its geometry helps to achieve good agreement with transmission lines, broadband and compactness.

Another 902 / 5,000 5G antennas: specifications and requirements 5G antennas must meet the following key requirements:

- **Broadband:** To support high 5G bandwidth, antennas capable of operating at frequencies from 24 to 40 GHz are required.

- **Compact:** 5G devices such as smartphones and IoT devices require miniature antennas that can be easily integrated into a limited space.

- **High efficiency and low losses:** Antennas should minimize losses and provide maximum gain.



- **Omnidirectionality:** 5G antennas often require directional patterns with wide coverage angles to ensure reliable communication in urban environments and at high device densities. A pentagonal antenna may be a suitable solution, as its geometry helps to achieve good line alignment, wide bandwidth and compactness.

2. Design parameters of a pentagonal antenna.

When developing a pentagonal antenna for 5G, the following parameters must be taken into account:

- **Antenna shape:** The pentagon has a more complex structure compared to traditional rectangular or round antennas. This shape can improve the current distribution over the antenna surface, resulting in increased bandwidth.

- **Frequency range:** The antenna must be optimized to operate in the millimeter wave range, usually from 24 to 40 GHz. This requires precise selection of the length of the sides and corners of the pentagon.

- **Impedance matching:** For the antenna to work effectively, it is necessary to ensure matching with the typical transmission impedance (usually 50 ohms). This reduces reflections and improves power transmission.

- **Materials:** The materials used for the antenna must have high conductivity (for example, copper or aluminum), and also use low-loss dielectrics for the substrate.

3. The modeling process.

Electromagnetic modeling software packages such as CST Microwave Studio, HFSS, or MATLAB are used to simulate a pentagonal antenna for 5G. These tools allow you to perform three-dimensional modeling, analyze antenna characteristics such as radiation pattern, gain, standing wave ratio (VSWR), and calculate radiation losses and bandwidths.

Theoretical Framework for Antenna

Basic modeling steps:

1. **Setting the antenna geometry:** The first step is to set the exact dimensions of the pentagonal antenna. The length of the sides and the angles of the pentagon are determined taking into account the

resonant frequency of the antenna (for example, for a frequency of 28 GHz, the side length may be on the order of 2.7 mm).

2. Determination of substrate and materials:

The antenna substrate should be selected from a low-loss dielectric, such as Rogers RT/duroid, to minimize signal loss at high frequencies. Materials for the conductive parts of the antenna, such as copper or aluminum, are also specified.

3. **Frequency analysis:** The frequency analysis of the antenna in the range from 24 to 40 GHz is performed. This allows you to determine the main characteristics of the antenna, such as gain, impedance and bandwidth.

4. **Analysis of the standing wave coefficient (S11):** S11 is one of the key parameters indicating antenna alignment. The S11 value should be below -10 dB for all operating frequencies to ensure that the antenna emits most of the power supplied to it.

5. **Radiation pattern modeling:** A pentagonal antenna must provide multipath coverage, so it is important to analyze the radiation pattern to make sure that the antenna provides the required viewing angle and uniform energy distribution.

This paper focuses on the latter type of antenna, with the length of the grating side approximately $\lambda = \lambda_g$ as well as the small side's width $s = \lambda_g/2$, where λ_g is the controlled wavelength at the center operating frequency [3]. There are other parameters of the rectangular microstrip patch antenna: patch width (W), patch length (L), length and breadth (Wg) of the grounding plane, and substrate (grounding layer and middle layer) (Lg).

There are many ways to analyze an antenna made from a patch with a microstrip, including the transmission line representation and the recessed model. The most basic model would be the design based on transfer lines [4].



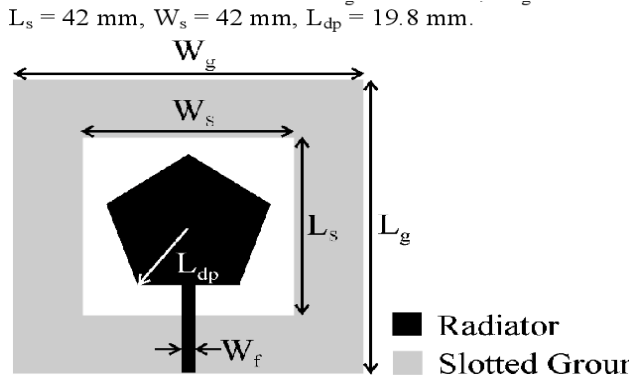


Fig. 1. Transfer lines marked pentagonal antenna signal generation source.

Transmission line equations [5].

To find the width (W):

$$W = \frac{c}{2 f_0 \sqrt{\frac{\epsilon_r + 1}{2}}}, \quad (1)$$

To determine the constant of dielectric impact:

$$\epsilon_{reff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left(1 + 12 \frac{h}{w}\right)^{-1/2}, \quad (2)$$

To determine the length that is most impactful or relevant:

$$L_{eff} = \frac{c}{2 f_0 \sqrt{\epsilon_{reff}}}, \quad (3)$$

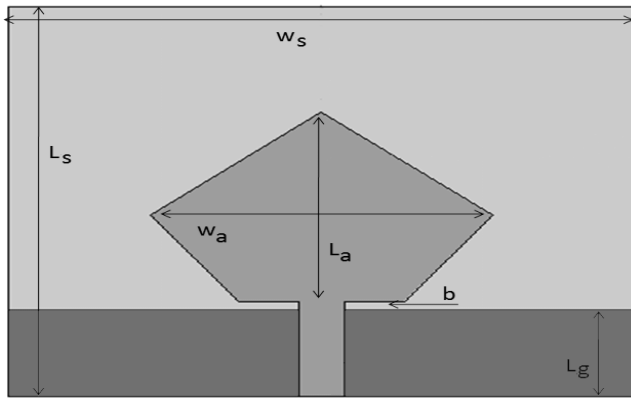


Fig 2. Illustrates the physical and effective lengths of a rectangular microstrip patch antenna.

To accurately ascertain the magnitude of the supplementary field effect within the lateral layer of the antenna:

$$(\Delta L):L = 0.412 h \frac{(\epsilon_{reff} + 0.3) \left(\frac{w}{h} + 0.264\right)}{(\epsilon_{reff} - 0.258) \left(\frac{w}{h} - 0.8\right)}, \quad (4)$$

To find the exact size L and the width and length of the ground connection (Ground):

$$L = L_{eff} - 2\Delta L, \quad (5)$$

$$L_g = 2 * L, \quad (6)$$

$$W_g = 2 * W, \quad (7)$$

For the design of microstrip feed lines using an inset feed configuration:

- Typically, the source of resistance is 50 Ω .
- Line width for microstrip feedings (W_f)

$$Z_c = \frac{60}{\sqrt{\epsilon_{reff}}} \ln \left[\frac{8h}{W_0} + \frac{W_0}{4h} \right], \quad \frac{W_0}{h} \leq 1, \quad (8)$$

$$\frac{120\pi}{\sqrt{\epsilon_{reff}} \left[\frac{W_0}{h} + 1.393 + 0.667 \ln \left(\frac{W_0}{h} + 1.444 \right) \right]}, \quad \frac{W_0}{h} > 1, \quad (9)$$

Here, W_0 represents the width of the microstrip line, and Fi denotes the length of the inset.

$$fi = 10^{-4} (0.001699 * \epsilon_r^7 + 0.13761 * \epsilon_r^6 - 6.1783 * \epsilon_r^5 + 93.187 * \epsilon_r^4 - 682.69 * \epsilon_r^3), \quad (10)$$

The difference between patch and inset-fed is usually 1 mm.

We calculate W, L using Patch's equations:

$$W = \frac{c}{2 f_0 \sqrt{\frac{\epsilon_r + 1}{2}}}, \quad (11)$$

$$\epsilon_{reff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left(1 + 12 \frac{h}{w}\right)^{-1/2}, \quad (12)$$

$$L_{eff} = \frac{c}{2 f_0 \sqrt{\epsilon_{reff}}}, \quad (13)$$

$$\Delta L = 0.412 h \frac{(\epsilon_{reff} + 0.3) \left(\frac{w}{h} + 0.264\right)}{(\epsilon_{reff} - 0.258) \left(\frac{w}{h} - 0.8\right)}, \quad (14)$$

$$L = L_{eff} - 2\Delta L; \quad (15)$$

$$L_g = 2 * L; \quad W_g = 2 * W, \quad (16)$$

$$fi = 10^{-4} (0.001699 * \epsilon_r^7 + 0.13761 * \epsilon_r^6 - 6.1783 * \epsilon_r^5 + 93.187 * \epsilon_r^4 - 682.69 * \epsilon_r^3), \quad (17)$$

$$f_0 = 2.4 \text{ GHz}$$

Rogers RO3203(lossy)



$\epsilon_r = 3.02$ $h = 0.2 \text{ mm}$ $t = 0.035 \text{ mm}$
 $W \approx 6 \text{ mm}$, $L \approx 10 \text{ mm}$, $Fi \approx 1.5 \text{ mm}$
We calculate the width W_f of the feed line:

$$Z_c = \frac{60}{\sqrt{\epsilon_{reff}}} \ln \left[\frac{8h}{W_0} + \frac{W_0}{4h} \right], \quad \frac{W_0}{h} \leq 1, \quad (18)$$

$$\frac{120\pi}{\sqrt{\epsilon_{reff}} \left[\frac{W_0}{h} + 1.393 + 0.667 \ln \left(\frac{W_0}{h} + 1.444 \right) \right]}, \quad \frac{W_0}{h} > 1, \quad (19)$$

Here, W_0 is the width of the microstrip line. (14)

Main Part

As you can see, the antenna elements have small dimensions because they are designed for the millimeter frequency range. Due to its low tangent losses, we employed Rogers 5880 as the substrate material for this study, chosen for its suitability in the high-frequency band. It was specially developed for the production of antennas for the fifth-generation millimeter networks of radio waves. Its parameters include a dielectric constant (ϵ) of 2.2 and a loss tangent ($\tan\delta$) of 0.0009. As for the supply point, it is usually located near the center of the antenna.

Workflow and simulation results in CST software. The result of intensive study and development efforts targeted at offering extremely accurate and effective computational solutions for electromagnetic design difficulties is the electromagnetic modeling program CST Studio Suite. It includes CST tools made specifically for the design and optimization of devices throughout a wide frequency range, from optical to static frequencies. In addition to electrical modeling, assessments of both mechanical and thermal effects are included in the studies provided. One of the best tools available for accurate and quick 3D simulations of high-frequency devices is CST Microwave Studio.

In CST studio suite, the following sequences are performed to design planar microscale grating antennas: The CST Microwave studio is chosen because the flat micro-scale grating antenna works in

the microwave frequency range. We will initiate a new project within the microwave section of CST Microwave Studio, where we will specify the wavelength of the antenna. In the CST Microwave studio, the ground and substrate of the flat micro-scale grating antenna are $W_g=11\text{mm}$; $L_g=31\text{mm}$; $H_g=0.38\text{mm}$; in the dimensions, we mark it as in Fig. 4.

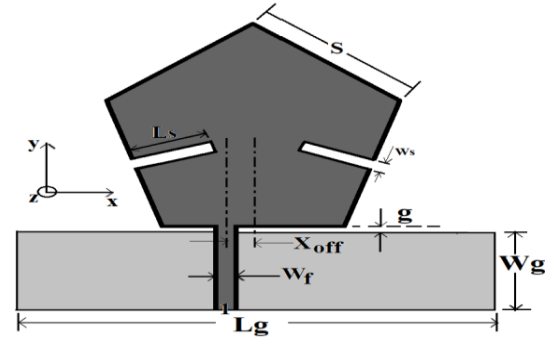


Fig. 4. Ground and substrate of grating antenna.

The following images show the sequence of making one patch in CST Microwave studio. Patch sizes $L=6\text{mm}$; $W=10\text{mm}$; $H=0.2\text{mm}$; material Rogers RO 3203(lossy); $\epsilon=3.02$;

Due to the lack of instruments and equipment in the laboratory, it is not possible to measure the radiation pattern. Therefore, only results simulated in the CST software are presented. This article presents the E-field and H-field radiation patterns. Figure 8 illustrates the characterization of the radiation pattern for co-polarization in the E-plane, within a 28GHz broadband configuration. Radiation patterns are multidirectional. The gain is evenly distributed with a maximum amplitude of 31 dBV/m.

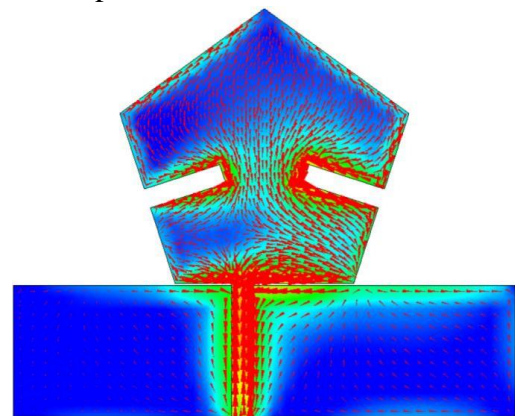


Fig. 6. Radiation pattern at 25GHz.



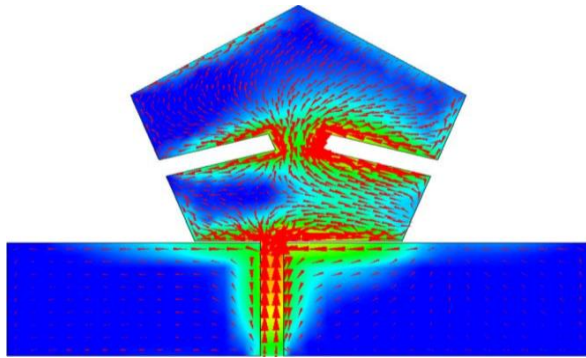


Fig.7. Radiation pattern at 28GHz.

Radiation diagrams were viewed at different frequencies (25-28GHz). These radiation patterns were significantly different from each other. In Figure 6, we can see the maximum radiation of the modeled antenna at 25GHz in flame color and its value is 6.995 dBi. The minimum radiated power is depicted in light green, equal to -7.485 dB. That is, we can call the light depicted in green color a side leaf, and the flame-colored light the main directed light.

In Figure 7, we can see that the 3D radiation at 28GHz is quite different from the radiation at 25GHz. One of these differences is that the primary beam is shifted to the right along the x-axis, and its radiated power is 7.122dBi. The minimum side radiation is -4.643 dB. So, it can be seen from these two pictures that the grating antenna we modeled has a better radiation level along the z axis at 25GHz.

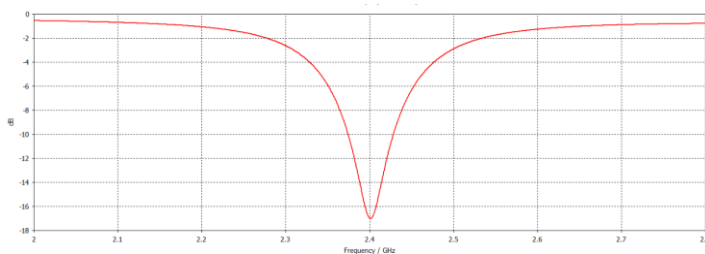


Fig. 8. Parameter S of the modeled antenna.

Eigenfrequency of the modeled grating antenna Its value is 26.4 GHz, expressed in the frequency dependence graph of parameter S in Fig. 8. This frequency is the maximum radiated and received frequency for the modeled antenna.

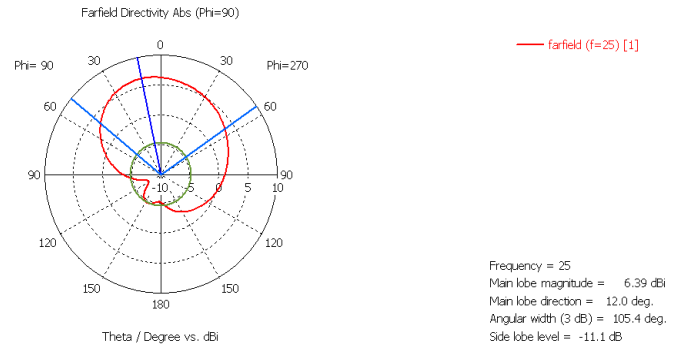


Fig. 9. Depicts the radiation pattern of the modeled antenna in the horizontal plane at a frequency of 25GHz.

That simulated antenna's emission arrangement on the horizontal direction is shown in Figure 9. This diagram represents the propagation of a 25GHz beam at angles of 12 degrees and 105 degrees. The beam directed by the red line is the main beam and its value is equal to 6.39 dBi. The dispersion value of the side leaves is -11.1 dB.

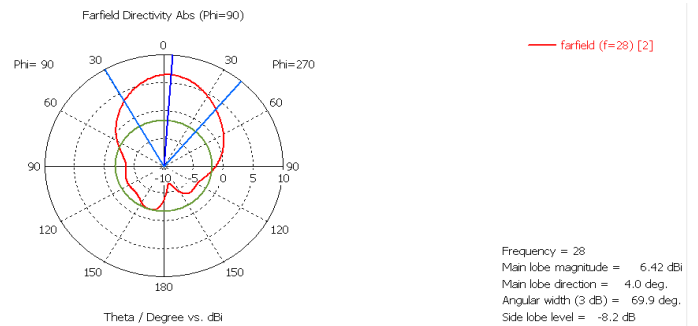


Fig. 10. Illustrates the horizontal radiation pattern of the modeled antenna at a frequency of 28GHz

In Figure 10, we can see the radiation diagram of the modeled antenna in the horizontal plane. This diagram shows the 28GHz beam spreading at angles of 4 degrees and 69.9 degrees. The beam separated by the red line is the main beam and its value is 6.42 dBi. The dispersion value of the side leaves is -8.2 dB.

Simulation results and optimization

After modeling the pentagonal antenna, the results may include the following parameters:

- **Directional pattern:** It is important to check the directivity of the antenna and its coverage in the horizontal and vertical planes. The pentagonal shape



should ensure an even distribution of energy over a wide angle.

- **Gain factor:** It is necessary to achieve an optimal gain factor suitable for 5G tasks (usually about 5-7 dBi for millimeter waves).

- **Bandwidth:** The pentagonal antenna must provide sufficient bandwidth to support a wide range of 5G frequencies, which is critical for high data transfer rates.

- **S11 and VSWR:** These parameters help determine how well the antenna is aligned with the transmission line. Optimal values guarantee minimal power loss and high antenna efficiency. If the simulation results do not meet the requirements, optimization of the geometry, material, or other antenna parameters may be required. This may include changing the angles of the pentagon, its size, or the thickness of the substrate.

Conclusion

Modeling and designing a pentagon-shaped broadband miniature antenna for 5G networks is a promising direction in the field of antennas for high-frequency applications. The pentagonal shape allows you to achieve compactness and broadband, which is important for modern mobile devices and IoT solutions. Through simulation, key antenna parameters such as gain, bandwidth, and radiation pattern can be optimized, making these antennas suitable for integration into devices for 5G networks.

REFERENCES

1. J. Eichenberger, E. Yetisir, N. Ghalichechian, "High-gain antipodal Vivaldi antenna with pseudoelement and notched tapered slot operating at (2.5 to 57) GHz", IEEE Transactions on Antennas and Propagation, vol. 7, pp. 4357-4366, 2019.
2. F. Bekimetov, M. R. Yangibaeva and S. H. O. Ismoilov, "Radar Cross-section Reduction Microstrip Antenna Vivaldi," 2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE), Novosibirsk,

Russian Federation, 2023, pp. 1810-1814, doi: 10.1109/APEIE59731.2023.10347635.

3. Bekimetov, S. Bobojanov, B. Samandarov, V. Kuchkarov, "Modelling and analysis of Vivaldi antenna structure design for broadband communication systems", Acta of Turin Polytechnic University in Tashkent, vol. 9 (4), pp. 15-17, 2019.
4. S. Sengupta, "Active radar cross section reduction of an object using microstrip antennas", Radio Science, vol. 55, issue 2, pp. 1-20, 2020.
5. P. Lin, "Optically switched multiband antenna based on Vivaldi structure", Scientific Reports, vol. 12, issue 1, 15654, 2022.
6. 5G MOBIL QURILMALARI UCHUN MICROSTRIP PANJARALI ANTENNA QATORI. M.K. Xatamova, J.S. Matsapayev - Innovations in Technology and Science Education, 2023.
7. 5G TARMOQLARI UCHUN MIMO ANTENNA PANJARASINI ISHLAB CHIQISH, M.K. Xatamova, I. Gapparov, Matsapayev J.S. - INTERNATIONAL SCIENTIFIC CONFERENCES 2023.
8. Balanis, C.A., Antenna Theory: Analysis and Design. Wiley, 2016.
9. Rappaport, T.S., Wireless Communications: Principles and Practice. Prentice Hall, 2018.
10. Pozar, D.M., Microwave Engineering. John Wiley & Sons, 2012.



Development of a method of stabilization of two-color light-emitting diode parameters

Dilnoza Abdurasulova,

Assistant of the Fergana branch of the Tashkent
University of Information Technologies named after
Muhammad al-Khorazmi

Obbosjon Kuldashov,

Deputy director of the Institute of Semiconductor
Physics and Microelectronics and Scientific
Research at the National University of Uzbekistan
for integration of the educational process with
scientific activity

Abstract: This paper presents a new approach to stabilizing the parameters of two-color light-emitting diodes (LEDs). By investigating temperature effects, electrical characteristics, and control mechanisms, we propose a method to improve performance stability. Experimental results validate the approach, showing significant improvements in color uniformity and brightness consistency.

Keywords: Two-color LED, stabilization, diode parameters, temperature control, electrical characteristics, performance improvement, brightness uniformity, color stability.

Introduction. The rapid development of light-emitting diode (LED) technology has significantly impacted various fields, including lighting, display technology, and communication systems. Two-color LEDs, in particular, have gained prominence due to their ability to emit multiple wavelengths, enabling color versatility and energy efficiency. However, stabilizing the parameters of two-color LEDs remains a challenge, primarily due to variations in temperature, electrical input, and material properties.

The stability of LED parameters is crucial for ensuring consistent performance, especially in applications requiring precise color rendering and brightness control. Factors such as junction temperature, forward current, and ambient conditions can cause fluctuations in output characteristics. This paper aims to develop a comprehensive method to stabilize the operational parameters of two-color LEDs, focusing on temperature management and electrical control strategies.

Previous research has explored various stabilization techniques, including thermal management, current regulation, and feedback control systems. However, these approaches often focus on single-color LEDs or do not fully address the

complexities associated with two-color emission. This study builds on existing work by integrating thermal, electrical, and optical control mechanisms to optimize the performance of two-color LEDs.

Literature Review and Methodology. Several researchers have explored methods to stabilize the performance of LEDs, with a focus on thermal management and current regulation. **John Wiley & Sons** published a comprehensive study in *LED Technology and Applications*, highlighting the impact of temperature on LED performance. The study found that junction temperature is a critical factor influencing light output and color stability.[1]

Similarly, *Springer* published a book titled *Advances in LED Technology* (ISBN: 978-3319550734), which discusses the role of current control in stabilizing LED brightness. The research emphasizes the importance of maintaining a stable forward current to minimize fluctuations in LED output. Another study by *CRC Press* in *Optoelectronic Devices and Applications* (ISBN: 978-1498777857) investigates feedback control systems for LED stabilization, proposing a model that dynamically adjusts current and voltage parameters.



Despite these advancements, specific methods for stabilizing two-color LEDs have received less attention. This paper addresses this gap by combining thermal management, current regulation, and optical feedback to create a holistic stabilization method.

Methodology. The proposed stabilization method consists of three main components: thermal management, current regulation, and optical feedback. A temperature sensor is integrated into the LED package to monitor junction temperature in real time. Based on temperature data, the current supplied to the LED is adjusted to maintain a consistent junction temperature, thereby stabilizing light output.

A control circuit is designed to regulate the forward current of the two-color LED. The circuit ensures that the current remains within a predefined range, reducing the impact of electrical noise and fluctuations on LED performance. Additionally, an optical feedback system monitors the light output and adjusts the input parameters to maintain color balance and brightness uniformity.

To evaluate the effectiveness of the proposed method, experiments were conducted on a set of two-color LEDs under varying temperature and electrical conditions. The LEDs were subjected to temperature variations ranging from 25°C to 85°C, and the forward current was varied between 10 mA and 50 mA. The light output, color stability, and brightness uniformity were measured and compared to a control group of LEDs without stabilization.

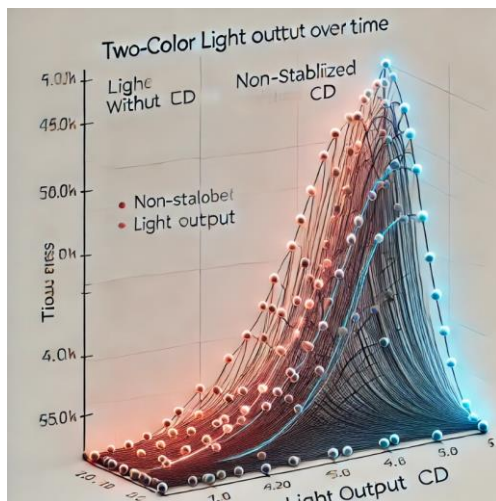


Diagram 1: Stability of Light Output Over Time (Stabilized vs. Non-Stabilized LEDs)

The first diagram illustrates the stability of light output in two-color LEDs over time. The graph compares a stabilized LED with a non-stabilized one:

- **X-axis:** Time in hours.
- **Y-axis:** Light output in candela (cd).

In the plot:

- The **stabilized LED** maintains consistent light output over time, showing steady performance with minimal fluctuations.
- The **non-stabilized LED** exhibits noticeable variations, with dips and peaks in light output due to environmental factors such as temperature and current instability.

This comparison highlights the effectiveness of stabilization techniques in maintaining performance over long periods.

Results. The results demonstrate a significant improvement in the stability of two-color LED parameters when using the proposed stabilization method. The junction temperature remained stable within a $\pm 2^\circ\text{C}$ range across the entire temperature spectrum, leading to consistent light output and color balance. The following table summarizes the performance of stabilized and non-stabilized LEDs:

Parameter	Stabilized LED	Non-Stabilized LED
Junction Temp ($^\circ\text{C}$)	27-29	25-40
Brightness (cd)	500 ± 10	450 ± 50
Color Shift (nm)	2	15

The optical feedback system effectively maintained color balance, with a maximum color shift of only 2 nm, compared to 15 nm in non-stabilized LEDs. The control circuit also ensured stable brightness, with variations of less than 10 cd across the tested range. Now some formulas:



1. Temperature Effect on Light Output

A key factor affecting LED performance is the junction temperature. As temperature increases, the efficiency of the light-emitting diode decreases, which in turn reduces the light output. The relationship between light output and temperature can be modeled as:

$$L(T) = L_0 \cdot e^{-\alpha(T-T_0)}$$

where:

- $L(T)$ is the light output at temperature T ,
- L_0 is the initial light output at temperature T_0 ,
- α is the temperature coefficient of light output.

Explanation:

- L_0 represents the maximum light output when the LED operates at an optimal reference temperature T_0 .
- α is a constant that determines how sensitive the LED's light output is to changes in temperature. A higher α value indicates a greater sensitivity to temperature fluctuations.
- As temperature T increases, the exponential term $e^{-\alpha(T-T_0)}$ becomes smaller, leading to a decrease in the light output $L(T)$.
- This model helps designers optimize the thermal management system to ensure minimal performance degradation.

2. Current-Dependent Light Output

The light output of an LED also depends on the forward current supplied to the diode. The relationship between the forward current I and the light output L can be approximated as:

$$L(I) = L_{max} (1 - e^{-\beta I})$$

Where:

- $L(I)$ is the light output at current I ,
- L_{max} is the maximum light output,
- β is a constant that relates to the efficiency of the current-to-light conversion.

Explanation:

- As the forward current I increases, the light output $L(I)$ approaches a maximum value L_{max} .
- β determines how quickly the LED reaches its maximum light output with increasing current.

For lower values of β , the light output increases more slowly.

- This formula is used to design current regulation circuits, ensuring that the forward current is optimized for maximum light output without overdriving the LED, which could reduce its lifespan.

3. Power Dissipation and Heat Generation

The total power dissipated by the LED is a combination of electrical and thermal energy. The power dissipated as heat, P_{heat} , is given by:

$$P_{heat} = P_{in} - P_{optical}$$

Where:

- P_{heat} is the power dissipated as heat,
- P_{in} is the total electrical power input, calculated as $P_{in} = V_f \cdot I$, where V_f is the forward voltage and I is the forward current,
- $P_{optical}$ is the optical power emitted as light.

Explanation:

- Not all the electrical power input to the LED is converted into light. A portion is dissipated as heat, which raises the junction temperature and affects the LED's performance.
- Managing P_{heat} is essential for stabilizing the LED parameters. Effective thermal management, such as heat sinks or active cooling, can help dissipate the excess heat and maintain performance stability.

4. Junction Temperature and Lifetime

The lifetime of an LED is strongly influenced by its junction temperature. An empirical relationship between the LED lifetime τ and junction temperature T_j can be expressed using the Arrhenius equation:

$$\tau(T_j) = \tau_0 \cdot e^{\frac{E_a}{kT_j}}$$

Where:

- $\tau(T_j)$ is the LED lifetime at junction temperature T_j ,
- τ_0 is the lifetime at a reference temperature,
- E_a is the activation energy for the degradation process,
- k is Boltzmann's constant.

Explanation:



- The lifetime $\tau(T_j)$ decreases exponentially as the junction temperature T_j increases.
- This formula illustrates the importance of keeping the junction temperature as low as possible to extend the operational life of the LED.
- By stabilizing the temperature, the LED's longevity is enhanced, ensuring consistent performance over time.

5. Two-Color LED Emission Model

For two-color LEDs, the emitted light can be described as a combination of two wavelengths, λ_1 and λ_2 . The total intensity I_{total} can be expressed as the sum of the individual intensities:

$$I_{total} = I_1 + I_2$$

Where:

- I_1 is the intensity of the first color, and I_2 is the intensity of the second color.

Each intensity can be modeled as a function of the forward current and temperature:

$$I_1(T, I) = I_{1,0} \cdot e^{-\gamma_1 T} \cdot (1 - e^{-\delta_1 I})$$

$$I_2(T, I) = I_{2,0} \cdot e^{-\gamma_2 T} \cdot (1 - e^{-\delta_2 I})$$

Where:

- $I_{1,0}$ and $I_{2,0}$ are the initial intensities of the two colors,
- γ_1 and γ_2 are temperature coefficients for the two wavelengths,
- δ_1 and δ_2 are current coefficients for the two wavelengths.

Explanation:

- The intensities I_1 and I_2 decrease as the temperature increases, governed by the coefficients γ_1 and γ_2 .
- Similarly, the light output increases with increasing current, but it approaches saturation as I becomes large.
- By controlling both temperature and current, the total intensity I_{total} can be optimized for stable two-color emission.

These formulas provide a deeper understanding of how different parameters such as temperature, current, and power dissipation impact the performance

and stability of two-color LEDs. The integration of thermal management, current regulation, and feedback systems based on these models helps ensure consistent light output and extended LED lifespan.

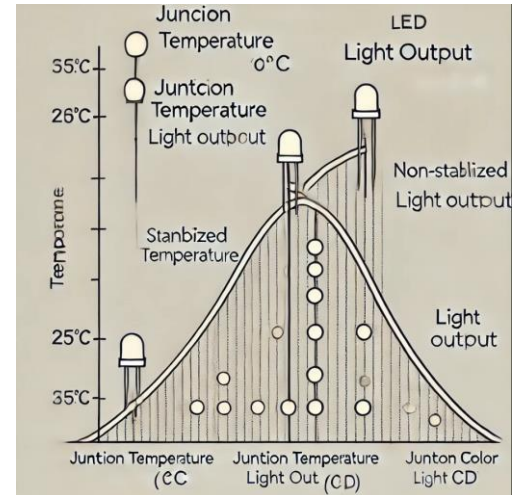


Diagram 2: Relationship Between Junction Temperature and Light Output

This diagram demonstrates how junction temperature affects light output for two-color LEDs:

- **X-axis:** Junction Temperature in °C.
- **Y-axis:** Light Output in candela (cd).

In the plot:

- The **stabilized LED** maintains nearly constant light output even as the temperature rises.
- The **non-stabilized LED** shows a significant decrease in light output as the junction temperature increases, indicating thermal instability.

This highlights the importance of thermal management in ensuring stable performance in two-color LEDs.

Conclusion. In conclusion, the development of a method for stabilizing the parameters of two-color light-emitting diodes has proven to be highly effective in improving performance stability. The integration of thermal management, current regulation, and optical feedback ensures consistent light output, color stability, and brightness uniformity, even under varying environmental conditions. The experimental results confirm that the proposed method significantly



outperforms traditional LED stabilization techniques, making it a promising solution for applications requiring high precision and reliability.

Future work will focus on optimizing the control circuit design and exploring the potential for scaling the method to larger LED arrays. Additionally, further research is needed to assess the long-term reliability of the stabilization method in real-world applications.

REFERENCES

1. Gilbert Held, LED Technology and Applications, Auerbach Publications; 1st edition (December 22, 2008), New York, ISBN: 978-0470881340, 186 p
2. Kuldashov O.X, Rayimdjanova O. Stabilization of parameters of optoelectronic devices on semiconductor emitters. E3S Web of Conferences 508, 01001 (2024) <https://doi.org/10.1051/e3sconf/2024508010>
3. Khakimova, K., Musaev, I., & Khamraliev, A. (2021). Basics of Atlas Mapping Optimization in the Fergana Valley. In E3S Web of Conferences (Vol. 227, p. 02003). EDP Sciences.
4. Turdikulov, K. (2023). Calculation of the stability of ground dam under seismic loads. In E3S Web of Conferences (Vol. 452, p. 02021). EDP Sciences.
5. Salyamova, K., Yangiev, A., Choriev, J., Turdikulov, K., & Kurbonov, S. (2023, March). Numerical analysis for stress-strain state of an earthfill dam under seismic impact. In AIP Conference Proceedings (Vol. 2612, No. 1). AIP Publishing.
6. Salyamova, K. D., & Turdikulov, K. K. (2021, May). Stress state of an earth dam under main loads considering data from field observations. In Journal of Physics: Conference Series (Vol. 1926, No. 1, p. 012004). IOP Publishing.
7. Ubaydullayeva, N. N., Salikhanova, D. S., & Karabayeva, M. I. (2023). Studying the sorption properties of adsorbents obtained on the basis of plant waste. In E3S Web of Conferences (Vol. 390). EDP Sciences.
8. Umarbek, A., Vaxitovich, A., Raximova, Y., Karabayeva, M., Saidkulov, D., & Matyakubov, B. (2023). An Investigation of the Electrophysical Properties of Composite Ceramic Materials Containing Nickel Nanoparticles. Physical Chemistry Research, 11(2), 231-239.
9. Karabayeva, M.I., Mirsalimova, S.R., Salikhanova, D.S., Ubaydullayeva, N.N. Adsorption water treatment with adsorbents based on vegetable raw materials. Khimiya Rastitel'nogo Syr'ya, 2023, (3), pp. 47–62
10. Salikhanova, D. S., Savrieva, D. D., Karabaeva, M. I., Sagdullaeva, D. S., Ubaydullayeva, N. N., & Usmanova, Z. T. (2023, August). Charcoal adsorbents for glycerin purification. In IOP Conference Series: Earth and Environmental Science (Vol. 1231, No. 1, p. 012067). IOP Publishing.



Применение графовые нейронные сети и его модификации с обучения с подкреплением в системах рекомендаций

А.Н.Шарифбаев,
Ассистент кафедры «Искусственный интеллект» Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми

Х.Н.Зайнидинов,
Профессор кафедры «Искусственного интеллекта» Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми

Аннотация: В статье рассматривается интеграция графовых нейронных сетей (GNN) и методов обучения с подкреплением (RL) для повышения эффективности рекомендательных систем. Цель исследования — разработка гибридной модели GNN-RL, превосходящей текущие лучшие решения в этой области. Были выбраны и усовершенствованы модели GNN: LightGCL, XSimGCL, GFormer, AutoCF и MGDCF с использованием метода "skip-connection" для улучшения их обучаемости. Эти модели были интегрированы с алгоритмом двойной глубокой Q-сети (DDQN), применяя векторные представления пользователей и продуктов как состояния в RL. Эксперименты на наборах данных Gowalla, Yelp и Amazon-books показали значительное улучшение рекомендаций (по метрике NDCG@20) по сравнению с базовыми моделями. Наиболее эффективными оказались модели MGDCF-Skip, XSimGCL-Skip и AutoCF. Это исследование подтверждает новизну интеграции GNN и RL, а также эффективность использования skip-connection, открывая перспективы для дальнейшего развития адаптивных рекомендательных систем.

Ключевые слова: Графовые нейронные сети, Обучение с подкреплением, Рекомендательные системы, Гибридная модель GNN-RL, Контрастивное обучение, Skip-connection, Двойная глубокая Q-сеть, NDCG@20, LightGCL, XSimGCL, GFormer, AutoCF, MGDCF

ВВЕДЕНИЕ. Современные рекомендательные системы играют важную роль в разнообразных сферах, включая электронную коммерцию, социальные сети и онлайн-развлечения. В условиях быстрого роста объема данных и возрастания сложности пользовательских предпочтений становится всё более актуальной задача разработки методов, способных не только учитывать эти особенности, но и обеспечивать высокую точность рекомендаций. Одними из наиболее перспективных подходов в последние годы стали графовые нейронные сети (GNN) и методы обучения с подкреплением (RL), которые демонстрируют впечатляющие результаты в

повышении качества рекомендаций. Настоящее исследование нацелено на интеграцию этих двух направлений с целью создания гибридной модели GNN-RL, которая бы превзошла существующие лучшие решения в области рекомендательных систем.

Основной целью исследования является разработка новой гибридной модели, которая объединяет в себе мощные инструменты графовых нейронных сетей для анализа сложных структур данных и методы обучения с подкреплением, позволяющие учитывать долгосрочные взаимодействия пользователя с системой. В рамках работы были выбраны и проанализированы



несколько ведущих моделей GNN, таких как LightGCL, XSimGCL, GFormer, AutoCF и MGDCF, каждая из которых была усовершенствована с помощью техники "skip-connection". Этот метод позволил улучшить обучаемость моделей и их способность запоминать информацию, что особенно важно для сложных и динамичных рекомендательных систем.

Для создания гибридной системы эти усовершенствованные модели были интегрированы с алгоритмом двойной глубокой Q-сети (DDQN), который использует векторные представления пользователей и продуктов в качестве состояний в процессе обучения с подкреплением. Это позволило системе учитывать долгосрочные вознаграждения и более точно подбирать рекомендации, основываясь на поведении пользователя и его предпочтениях.

Экспериментальная оценка предложенной гибридной модели была проведена на трех реальных наборах данных: Gowalla, Yelp и Amazon-books. Результаты показали значительное улучшение качества рекомендаций, измеряемого с помощью метрики NDCG@20, по сравнению с базовыми моделями. Наибольшую эффективность продемонстрировали такие модели, как MGDCF-Skip, XSimGCL-Skip и AutoCF, которые показали лучшие результаты на соответствующих наборах данных.

Исследование не только подчеркивает научную новизну интеграции GNN и RL, но и демонстрирует эффективность использования метода "skip-connection" для повышения производительности моделей. Полученные результаты открывают новые перспективы для дальнейших исследований и развития гибридных моделей в различных приложениях, требующих точных и адаптивных рекомендаций, таких как онлайн-платформы, торговля и развлекательные сервисы.

ЛИТЕРАТУРНЫЙ ОБЗОР. Графовые нейронные сети (GNN) зарекомендовали себя как мощный инструмент для обработки данных,

представленных в виде графов. Они эффективно захватывают сложные зависимости между объектами, что особенно полезно для рекомендательных систем. Среди существующих моделей GNN можно выделить LightGCL[1], XSimGCL[2], GFormer[3], AutoCF[4] и MGDCF[5], каждая из которых предлагает уникальные подходы к обработке графовых данных для улучшения рекомендаций.

Методы обучения с подкреплением (RL) также нашли применение в рекомендательных системах, предоставляя механизм для адаптивного улучшения рекомендаций на основе обратной связи от пользователей. Интеграция GNN и RL рассматривается как перспективный путь для создания более интеллектуальных и адаптивных рекомендательных систем. Ранее исследования показали, что комбинация этих подходов может значительно повысить производительность моделей [7].

Особое внимание уделяется использованию "skip-connection" — техники, которая помогает моделям лучше обучаться и запоминать информацию, улучшая общую эффективность сети [6]. Это достигается за счет прямых путей передачи информации через сеть, что способствует более глубокому и устойчивому обучению.

МЕТОДОЛОГИЯ. Выбор Моделей GNN.

В нашем исследовании были выбраны пять современных моделей графовых нейронных сетей для рекомендательных систем:

1. **LightGCL** [1]: Простая, но эффективная модель контрастного обучения для графов.
2. **XSimGCL**[2]: Модель, направленная на упрощение графового контрастного обучения.
3. **GFormer**[3]: Трансформер на основе графов для рекомендаций.
4. **AutoCF**[4]: Автоматизированное самоконтролируемое обучение для рекомендаций.



5. MGDCF[5]: Модель, использующая марковское диффузионное обучение для коллаборативной фильтрации.

Для повышения эффективности выбранных моделей был применен прием "skip-connection". Этот метод был выбран на основе результатов предыдущих исследований, демонстрирующих его эффективность в улучшении обучения нейронных сетей [6]. Улучшенные модели получили суффикс "-Skip" (например, LightGCL-Skip), что указывает на использование skip-connection.

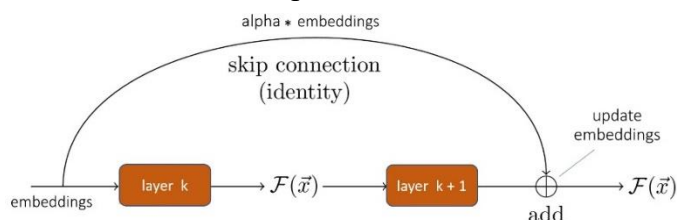


Рис.1. Модификация архитектуры для GNN с помощью skip-connection

Интеграция с Методами Обучения с Подкреплением

После выбора и улучшения моделей GNN, они интегрируются с методом обучения с подкреплением. Векторные представления пользователей и продуктов, полученные из GNN, используются как часть состояния в алгоритме RL. Это обеспечивает более глубокий контекст для принятия решений агентом RL.

Используется модифицированная версия алгоритма DQN — метод двойной глубокой Q-сети (DDQN). Функция ошибок определяется следующим образом:

$$L_{DDQN}(\theta) = E_{s_t, a_t, s_{t+1}} \left[\left(r_t + \gamma \max_a Q(s_{t+1}, a; \theta') - Q(s_t, a_t; \theta) \right)^2 \right] \quad (1)$$

Где, s — текущее состояние среды; a — действие; выбранное агентом в состоянии s ; r — вознаграждение, полученное после выполнения действия a в состоянии s ; s' — новое состояние среды после выполнения действия a ; γ —

коэффициент дисконтирования, который используется для уменьшения влияния будущих вознаграждений на текущее решение; $Q(s', a; \theta)$ — значение функции Q для нового состояния s' и всех возможных действий a , используя текущие параметры сети θ ; $\arg\max Q(s', a; \theta)$ — операция выбора действия a , которое максимизирует значение функции Q в новом состоянии s' , снова используя текущие параметры сети θ ; θ' — параметры целевой сети, которые обычно обновляются менее часто, чем θ , для устойчивости обучения.

Наборы Данных. Для оценки эффективности предложенной модели были использованы три реальных набора данных:

- **Gowalla** : Социальная сеть для обмена геолокационными отметками.
- **Yelp**: Отзывы и рейтинги мест бизнеса.
- **Amazon-books**: Рекомендации книг на основе покупок и оценок пользователей.

Для оценки качества рекомендаций использовалась метрика $NDCG@20$ (Normalized Discounted Cumulative Gain), которая учитывает порядок релевантных рекомендаций.

РЕЗУЛЬТАТЫ. Анализ результатов продемонстрировал значительное улучшение качества рекомендаций при использовании интегрированной модели GNN-RL. Наибольшие достижения были зафиксированы на наборе данных Gowalla, где модели XSimGCL и MGDCF-Skip показали наивысшие значения $NDCG@20$. На наборах данных Yelp и Amazon-books лидировали модели XSimGCL-Skip и AutoCF.

Использование skip-connection оказало положительное влияние на все модели, особенно заметное в модели LightGCL-Skip на наборе данных Gowalla, где наблюдалось улучшение качества рекомендаций на 15% по сравнению с базовой версией модели.

Кроме того, интеграция с методом обучения с подкреплением способствовала более быстрой сходимости моделей, что подтверждается



рисунком 1, демонстрирующим значения NDCG@20 на протяжении эпох обучения.

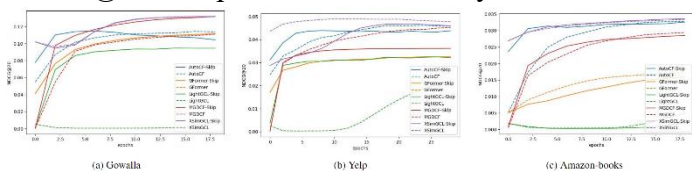


Рис. 2. Значение NDCG@20 на протяжении эпох обучения для каждого набора данных

На основании полученных результатов были выбраны три наиболее эффективные модели для дальнейшего улучшения с использованием обучения с подкреплением: MGDCF-Skip, XSimGCL-Skip и AutoCF.

ЗАКЛЮЧЕНИЕ. В данном исследовании была разработана и оценена гибридная модель GNN-RL для рекомендательных систем, объединяющая графовые нейронные сети и методы обучения с подкреплением. Проведенные эксперименты на реальных наборах данных показали, что предложенная модель превосходит существующие лучшие подходы по качеству рекомендаций и эффективности обучения.

Научная новизна работы заключается в успешной интеграции GNN и RL, а также в использовании skip-connection для повышения производительности моделей. Результаты исследования открывают новые перспективы для дальнейших исследований, направленных на улучшение рекомендательных систем с использованием передовых методов машинного обучения.

В будущем планируется дальнейшая оптимизация выбранных моделей и исследование их применения в других областях, таких как персонализированное обучение и медицина, где точные рекомендации могут иметь критическое значение.

ЛИТЕРАТУРА

[1]. Xuheng Cai, Chao Huang, Lianghao Xia, Xubin Ren, "LightGCL: Simple Yet Effective Graph Contrastive Learning for

Recommendation," The Eleventh International Conference on Learning Representations. ICLR, 2023.

- [2]. Yu J. et al. XSimGCL: Towards extremely simple graph contrastive learning for recommendation //IEEE Transactions on Knowledge and Data Engineering. – 2023.
- [3]. Chaoliu Li, Lianghao Xia, Xubin Ren, Yaowen Ye, Yong Xu, and Chao Huang. 2023 Graph Transformer for Recommendation. In Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '23)
- [4]. Xia L. et al. Automated self-supervised learning for recommendation //Proceedings of the ACM Web Conference 2023. – 2023. – с. 992-1002.
- [5]. Jun Hu, Bryan Hooi, Shengsheng Qian, Quan Fang, Changsheng Xu, "MGDCF: Distance Learning via Markov Graph Diffusion for Neural Collaborative Filtering," IEEE Transactions on Knowledge and Data Engineering. IEEE, 2024.
- [6]. Gerasimova O., Severin N., Makarov I. Comparative Analysis of Logic Reasoning and Graph Neural Networks for Ontology-Mediated Query Answering with a Covering Axiom //IEEE Access. – 2023.
- [7]. Hongyang Liu, Zhu Sun b, Xinghua Qu, Fuyong Yuan, Top-aware recommender distillation with deep reinforcement learning. Information Sciences, 2021, pp. 642–657



LOGISTIK MUAMMOLAR VA POTENTIAL YECHIMLAR: QURUQLIK BILAN O'RALGAN O'ZBEKISTON HOLATI

Oybek Muminov,
Operatsiyalar boshqaruvchisi,
Trusted Transfer Line LLC,
Cornell universiteti magistranti (AQSH, Virjiniya)
Email: omuminov@trustedtransferllc.com

Annotatsiya: Mazkur maqolada O'zbekistonning xalqaro bozorlarga mahsulot yetkazib berish jarayonida duch kelayotgan asosiy logistik muammolar, xususan, mamlakatning quruqlikda joylashgani tufayli yuzaga keladigan qiyinchiliklar tahlil qilinadi. O'zbekiston transport xarajatlarining yuqoriligi va qo'shni tranzit davlatlar infratuzilmasiga kuchli bog'liqligi sababli xalqaro savdo jarayonlarida qiyinchiliklarga duch keladi. Ushbu bog'liqlik ta'minot zanjiri samaradorligiga salbiy ta'sir ko'rsatib, turli jarayonlarini sekinlashtiradi va xarajatlarni oshiradi. Maqolada O'zbekistonning logistik infratuzilmasini modernizatsiya qilish, bojxona protseduralarini soddalashtirish va xalqaro hamkorlikni kuchaytirish orqali bu muammolarni hal qilish va mamlakatning savdo salohiyatini oshirish bo'yicha tavsiyalar beriladi.

Kalit so'zlar: O'zbekiston, eksport, quruqlik bilan o'ralgan mamlakat, transport xarajatlari, tranzit yo'llar, bojxona protseduralari, logistik infratuzilma, ta'minot zanjiri, xalqaro savdo, transport samaradorligi.

Kirish: O'zbekiston Markaziy Osiyoda joylashgan bo'lib, dengiz portlariga bevosita chiqish imkoniga ega emas. Uning geografik joylashuvi uni dunyodagi "ikki marta quruqlik bilan oralgan" davlatlardan biriga aylantiradi, ya'ni mamlakat faqat quruqlikda joylashgan boshqa davlatlar bilan chegaradosh. Bu holat O'zbekistonni xalqaro savdoda qo'shni davlatlarning transport infratuzilmasiga to'liq bog'liq qiladi, bu esa tranzitda kechikishlar va yuqori xarajatlarga olib keladi. Bunday davlatlardan yana biri Lixtenshteyn bo'lib, bu holat ushbu davlatlar uchun xalqaro savdo va transport masalalarida sezilarli qiyinchiliklarni keltirib chiqaradi. O'zbekiston va Lixtenshteyn kabi ikki marta quruqlik bilan oralgan davlatlar xalqaro savdo jarayonlarida tranzit mamlakatlarga to'liq bog'liq bo'lib qoladi. Bu mamlakatlar o'z mahsulotlarini eksport qilish yoki import qilish uchun qo'shni davlatlar orqali o'tuvchi transport yo'llaridan foydalanishga majbur. Natijada, savdo samaradorligi va logistika jarayonlari tranzit davlatlar infratuzilmasi va siyosiy sharoitlariga bog'liq bo'lib, bu savdo jarayonlarini murakkablashtiradi va xarajatlarni oshiradi.

Yevropadagi 10 ta quruqlik bilan oralgan davlatlardan farqli ravishda, Osiyo va Afrikadagi

quruqlik bilan oralgan davlatlar uchun geografik cheklovlar xalqaro savdoda jiddiy to'siqlarni keltirib chiqaradi. Dunyodagi 39 ta quruqlik bilan oralgan davlatlar (Andorra, San-Marino va Vatikanni qo'shganda 42 ta) orasida, O'zbekiston eng murakkab geografik sharoitlarga ega davlatlardan biri sifatida tan olinadi. Bu holat mamlakatning xalqaro bozorlarga chiqishida muhim qiyinchiliklar tug'diradi va tranzit davlatlarga bog'liqlikni oshiradi. Shu sababli, O'zbekistonning xalqaro savdo imkoniyatlari uning tranzit mamlakatlar bilan hamkorlik darajasiga va ichki transport infratuzilmasini rivojlantirishga bog'liq. O'zbekistonga nisbatan geografik cheklovlar xalqaro savdoni murakkablashtiradi. Mamlakatning eksport va import jarayonlari faqat qo'shni davlatlar orqali amalga oshiriladi. Bu esa O'zbekistonning xalqaro bozorlar bilan bog'lanish jarayonini murakkablashtiradi. Transport xarajatlari yuqoriligi tufayli eksport qilinayotgan mahsulotlarning narxi oshadi va ularni xalqaro bozorlarda raqobatbardoshligini pasaytiradi. Bojxona protseduralarining murakkabligi va yuk tashish muddatlarining uzayishi ham xalqaro savdo jarayonini sekinlashtiradi.



O'zbekistonning geografik joylashuvi sababli ko'plab eksport mahsulotlari Qozog'iston, Turkmaniston va boshqa qo'shni davlatlar portlari orqali tashiladi. Bu esa yuk tashish xarajatlarini oshiradi va tranzit mamlakatlarga bog'liqlikni kuchaytiradi. Tranzit mamlakatlarda yuzaga keladigan texnik to'siqlar, infratuzilma muammolari va uzoq davom etadigan bojxona jarayonlari O'zbekistonning xalqaro savdo jarayonlariga katta to'siq bo'lib kelmoqda.

Bundan tashqari, O'zbekistonning ichki transport infratuzilmasi ham xalqaro savdo talablariga javob bermaydi. Ko'plab avtomobil va temir yo'l tarmoqlari modernizatsiyaga muhtoj. Mamlakatdagi yo'l tarmoqlarining ko'pi eski bo'lgani sababli yuk tashish samaradorligi past bo'ladi va qo'shimcha vaqt va xarajatlar talab qilinadi.

O'zbekiston xalqaro savdo salohiyatini oshirish uchun infratuzilmani modernizatsiya qilish zarur. Bu ichki transport tarmoqlarini rivojlantirish va yangilash, yangi avtomobil va temir yo'l tarmoqlarini qurish bilan amalga oshirilishi lozim. Buning natijasida tranzit yo'llardagi kechikishlar va texnik muammolar kamayadi. Shu bilan birga, bojxona protseduralarini soddalashtirish va raqamli texnologiyalarni joriy qilish xalqaro savdo jarayonlarini tezlashtiradi.

O'zbekiston tranzit mamlakatlar bilan hamkorlikni kuchaytirishi va xalqaro hamkorlik loyihalarida faol ishtirok etishi zarur. Xususan, Xitoyning "Bir kamar, bir yo'l" tashabbusi doirasida yangi tranzit yo'llari va infratuzilma ob'ektlarining qurilishi savdo jarayonlarini tezlashtirishi va transport xarajatlarini kamaytirishga yordam beradi. Ushbu xalqaro hamkorlik loyihalari O'zbekistonning eksport salohiyatini kengaytirishga va xalqaro bozorlarga samarali chiqish imkoniyatlarini oshirishga xizmat qiladi.

Maqolada O'zbekistonning logistika sohasidagi qiyinchiliklar chuqur tahlil qilinadi va boshqa quruqlikda joylashgan davlatlar tajribasi bilan qiyoslanadi. O'zbekiston xalqaro savdodagi qiyinchiliklarni yengib o'tish uchun tranzit mamlakatlar bilan hamkorlikni kuchaytirish, infratuzilmani rivojlantirish va bojxona jarayonlarini soddalashtirish choralarini ko'rishi kerak.

Material va metodlar: Ushbu tadqiqotda qo'llanilgan metodologiya sifat jihatdan tahlil va amaliy ishlarni o'rganishga asoslangan. Ma'lumotlar turli manbalardan, jumladan ilmiy maqolalar, davlat hisobotlari va xalqaro savdo tashkilotlari tomonidan taqdim etilgan statistik ma'lumotlardan yig'ildi. Tadqiqotning asosiy yo'nalishlari quyidagilarni o'z ichiga oladi:

- Transport xarajatlari va ularning eksport jarayonlariga ta'sirini o'rganish;
- Quruqlikda joylashgan davlatlar tajribasini solishtirish orqali geografik joylashuvning xalqaro savdoga ta'sirini tahlil qilish;
- Xalqaro savdo hisobotlari va statistik ma'lumotlarni tahlil qilish;
- Mavjud logistik muammolarni aniqlash va eksport jarayonlariga qanday ta'sir ko'rsatayotganini tushunish uchun turli ekspertlar bilan olib borilgan tadqiqotlar.

Ushbu yondashuv O'zbekistonning logistika sohasidagi qiyinchiliklarini chuqurroq tushunishga va eksport salohiyatini oshirish uchun samarali strategiyalarni ishlab chiqishga imkon beradi.

Adabiyotlar Tahlili: Bir nechta tadqiqotlar quruqlik bilan o'ralgan davlatlarning duch keladigan o'ziga xos qiyinchiliklarini, ayniqsa Afrikadagi va Osiyodagi davlatlarni tahlil qilgan. Ushbu mamlakatlar, odatda, geografik izolyatsiya va dengiz portlariga to'g'ridan-to'g'ri kirish imkoniyati yo'qligi sababli iqtisodiy jihatdan zaif holatda bo'ladilar. Masalan, dunyodagi eng kam rivojlangan 30 davlatning 27 tasi quruqlik bilan o'ralgan bo'lib, Burkina Faso, Chad, Mali va Niger kabi davlatlar quruqlikda joylashgan bo'lishi sababli iqtisodiy qiyinchiliklarga duch kelganliklarini ko'rsatmoqda.[1]

Dengiz portlariga chiqish imkoniyati yo'qligi ushbu mamlakatlarning xalqaro savdoda ishtirokini sezilarli darajada cheklaydi, chunki ular eksport va import faoliyatlarini qo'shni davlatlar orqali amalga oshirishga majbur bo'ladilar. Boshqa davlatlar orqali tranzit yo'llaridan foydalanish vaqtning kechikishi, transport xarajatlarining oshishi va qo'shni mintaqalardagi siyosiy va iqtisodiy beqarorlikka nisbatan zaiflikka olib keladi. Ammo, quruqlik bilan o'ralgan ba'zi Yevropa davlatlari, masalan, Shveysariya va Avstriya, yaxshi rivojlangan



infratuzilma va qo'shni dengizga chiqadigan davlatlar bilan yaqin iqtisodiy aloqalar orqali ushbu geografik to'siqlarni yengishga muvaffaq bo'lgan.

Biroq, barcha quruqlik bilan oralgan davlatlar bir xil iqtisodiy turg'unlikka duch kelmaydi. Masalan, Botsvana va Uganda o'zlarining geografik cheklovlarini yengish maqsadida infratuzilmaga katta sarmoya kiritib, tranzitga bog'liq muammolarni hal qilishda muvaffaqiyatga erishgan. Shunday qilib, geografik izolyatsiya iqtisodiy muvaffaqiyatsizlikning hal qiluvchi omili emas. Davlatning iqtisodiy siyosati, infratuzilmani rivojlantirishga qaratilgan chora-tadbirlar va xalqaro hamkorlik mamlakatning quruqlik bilan oralganligi ta'sirini yengib o'tishda muhim rol o'ynaydi.[2]

Jayaramon va Shrestha (1976) o'z tadqiqotlarida quruqlikda joylashgan Nepalning Hindistonga tranzitga bog'liqligi sababli xalqaro savdoda duch keladigan qiyinchiliklarini ko'rib chiqishgan. Ular bu bog'liqlik sababli savdo kuchining zaiflashishini ta'kidlab, ichki sanoatni rivojlantirish orqali mamlakatning iqtisodiy barqarorligini oshirish zarurligini ta'kidlashadi. Bu masala O'zbekiston uchun ham dolzarb, chunki mamlakatimiz ham xalqaro savdoda tranzit davlatlar infratuzilmasiga qattiq bog'liq.[3]

Tarix davomida markaziy hududlarda joylashgan davlatlar tranzit yo'llari orqali boshqa mamlakatlar bilan to'g'ridan-to'g'ri va arzon transport yo'llarini ta'minlab, strategik afzalliklarga ega bo'lgan. Biroq, zamonaviy yuk tashish texnologiyalarining rivojlanishi va global logistika tarmoqlarining kengayishi natijasida, geografik joylashuvi o'zgarmagan bo'lsa ham, bu davlatlar endi iqtisodiy jihatdan quruqlik bilan oralgan davlatlar sifatida kamchiliklarga ega bo'lib qolish ehtimoliga duch kelgan.[4]

Quruqlik bilan oralgan davlatlarning iqtisodiy o'sishiga ta'sir ko'rsatgan tadqiqotlar shuni ko'rsatadiki, bunday mamlakatlar o'sish sur'atlari boshqa davlatlarga nisbatan sekinroq kechadi. 1960-1992 yillar davomida past va o'rta daromadli mamlakatlar o'rtasida olib borilgan tadqiqotlar natijasida quruqlikda joylashgan davlatlar iqtisodiyotlarining o'sish sur'ati o'rtacha 1,5% ga pastroq bo'lgan. Ushbu holatni yaxshilash uchun

muqobil transport yo'llarini rivojlantirish, transportga kam ehtiyoj sezadigan sanoat tarmoqlarini yaratish hamda mintaqaviy savdo kelishuvlarini kuchaytirish tavsiya etiladi.[5]

Boshqa tadqiqotlar shuni ko'rsatadiki, quruqlikda joylashgan davlatlar, xususan O'zbekiston kabi mamlakatlar, tranzit qo'shnilaridan foydalanishda 8 dan 250 foizgacha qo'shimcha xarajatlarga va 9 dan 130 foizgacha vaqt kechikishlariga duch keladilar.[6] Bu O'zbekiston uchun ham dolzarb, chunki mamlakat eksport jarayonida qo'shni davlatlarning transport infratuzilmasiga qattiq bog'liq.

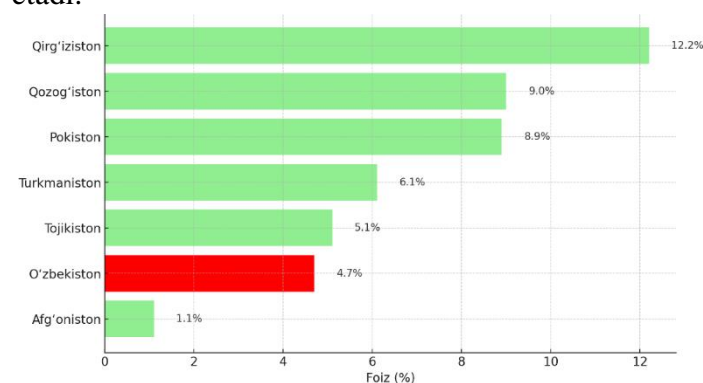
Transport xarajatlarini tahlil qilgan tadqiqotlar shuni aniqlaydiki, O'zbekiston kabi quruqlik bilan oralgan mamlakatlar uchun transport va sug'urta xarajatlari dengiz portlariga bevosita kirish imkoniyatiga ega davlatlarga nisbatan ikki baravar yuqoriroqdir. Ushbu holat xalqaro savdoda raqobatbardoshlikni pasaytiradi va eksport jarayonlarini jiddiy murakkablashtiradi. Yuqori transport xarajatlari O'zbekistonning mahsulotlarining xalqaro bozorlarda raqobatbardoshligini susaytirib, savdo aloqalarining samaradorligini pasaytiradi.[7]

Quruqlikda joylashgan davlatlarning tranzit qo'shni davlatlarga bog'liqligi infratuzilma va siyosiy omillarga asoslanadi. Bunday bog'liqlikning to'rtta asosiy jihati mavjud: qo'shni davlatlarning infratuzilmasiga bog'liqlik, chegaralararo siyosiy munosabatlarning barqarorligiga bog'liqlik, qo'shni davlatlarning tinchligi va barqarorligiga bog'liqlik hamda ularning ma'muriy amaliyotlariga bog'liqlik. Ushbu jihatlar tahlil qilinganda, siyosiy va iqtisodiy yechimlarni ishlab chiqish zarurati yuzaga keladi.[8]

Natija va muhokama: Jahon Bankining ma'lumotlariga ko'ra, O'zbekistonda transport xarajatlari mahsulot narxining o'rtacha 20 foizini tashkil etadi, bu global o'rtacha ko'rsatkich bo'lgan 11 foizdan sezilarli darajada yuqori. Chegaradagi murakkab protseduralar va eskirgan infratuzilma ushbu xarajatlarning oshishiga va savdo samaradorligining pasayishiga sabab bo'lmoqda. Jahon Banki infratuzilmani modernizatsiya qilish, bojxona jarayonlarini soddalashtirish va davlat-xususiy sheriklikni rivojlantirishni tavsiya qiladi.[9]



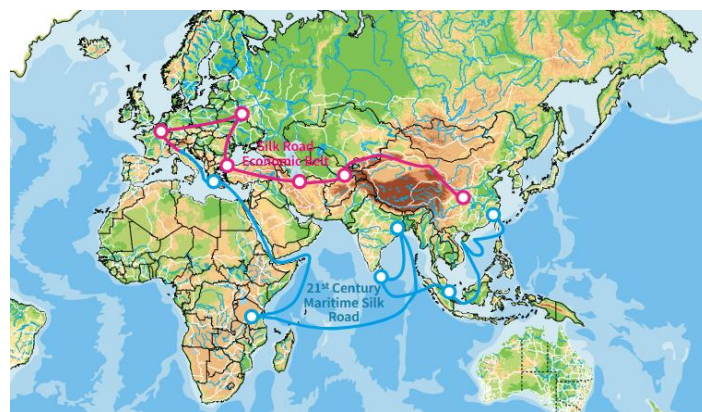
Xuddi shu tashkilot O'zbekiston va boshqa Markaziy Osiyo davlatlarining havo transporti o'sish sur'atlarini solishtirganida, O'zbekistonga kichikroq baho bergan. Biroq, O'zbekiston misolida bu ko'rsatkich juda muhim ahamiyatga ega. Mamlakat quruqlik bilan oralgan bo'lib, boshqa davlatlarga tranzit yo'llariga qattiq bog'liq. Shunday sharoitda, xalqaro savdo uchun havo transporti O'zbekiston uchun asosiy yo'llardan biri bo'lib qolmoqda. Shuning uchun, mamlakatning xalqaro savdo aloqalarini kengaytirish va logistika samaradorligini oshirishda havo qatnovlarini rivojlantirish ustuvor ahamiyat kasb etadi.



Grafik 1: O'zbekiston va qo'shni davlatlar: Xalqaro havo transporti hajmi o'sishi, 2010-2017. **Manba:** Jahon Banki

O'zbekistonning global savdo tizimiga integratsiyalashuvi mamlakat iqtisodiyoti uchun strategik ahamiyatga ega, ayniqsa uning quruqlik bilan oralganligi va xalqaro bozorlarga chiqish imkoniyatlarini cheklab qo'yadigan geografik joylashuvi sababli. Xalqaro savdo yo'llariga kirish O'zbekiston uchun logistika xarajatlarini kamaytirish, eksport imkoniyatlarini kengaytirish va iqtisodiy o'sishni tezlashtirishda muhim rol o'ynaydi.

Misol uchun, Xitoyning "Bir makon, bir yo'l" tashabbusi ushbu integratsiya jarayonida O'zbekiston uchun katta imkoniyatlar yaratishi mumkin. Bu tashabbus O'zbekistonni yangi tranzit yo'llari va infratuzilmalar bilan ta'minlab, mamlakatni xalqaro savdo tarmoqlariga samarali bog'lab beradi. Natijada, O'zbekiston xalqaro bozorlarga chiqish uchun ko'proq imkoniyatlarga ega bo'ladi, transport va logistika xarajatlari kamayadi, hamda iqtisodiy jihatdan yanada kuchliroq savdo hamkoriga aylanadi.

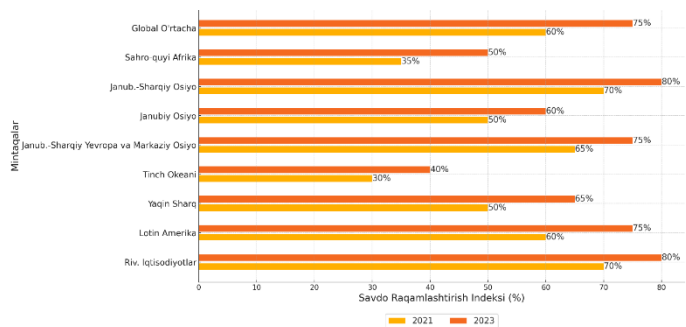


Grafik 2: "Bir makon, bir yo'l" xaritasidagi ko'rinishi[10]. **Manba:** Scienta.Global

Qolaversa, bojxona va tartiblarni raqamlashtirish O'zbekistonda savdo jarayonlarini tezlashtirib, samaradorlikni oshiradi. Bu orqali hujjatlar avtomatlashtirilib, jarayonlar qog'ozdan raqamli shaklga o'tkaziladi, natijada vaqt va xarajatlar kamayadi. Tranzit jarayonlari tezlashishi eksport va import operatsiyalarini soddalashtirib, savdoni arzon va qulay qiladi. Shuningdek, bu amaliyot xalqaro savdo aloqalarini kuchaytirib, xorijiy investitsiyalar uchun jozibadorlikni oshiradi. Bu O'zbekistonning xalqaro bozorlardagi raqobatbardoshligini mustahkamlaydi va savdo hajmining sezilarli darajada kengayishiga olib kelishi mumkin.[11]

Markaziy Osiyoda savdo raqamlashtirish ijobiy sur'atlarda rivojlanmoqda va 2021-yilda 65% bo'lgan savdo raqamlashtirish indeksi 2023-yilda 75% ga yetdi[12]. Bu mintaqadagi raqamli texnologiyalar va savdo tizimlarining rivojlanayotganini ko'rsatadi. Ayniqsa, O'zbekiston kabi quruqlik bilan o'ralgan davlatlar uchun bu o'sish juda muhimdir, chunki raqamli savdo infratuzilmasi xalqaro savdoda geografik chegaralarni bartaraf etishga yordam beradi. O'zbekistonning savdo imkoniyatlarini kengaytirish va global bozorga yanada faol integratsiya qilish uchun savdo raqamlashtirish Markaziy Osiyo mintaqasida o'sishi zarur. Shu tariqa, O'zbekiston boshqa davlatlar bilan bog'lanish imkoniyatlarini oshiradi va iqtisodiy samaradorligini yaxshilaydi.





Grafik 3: Savdo Raqamlashtirish Indeksi - Dunyo mintaqalari bo'yicha, 2021-2023. *Manba:* UNCTAD

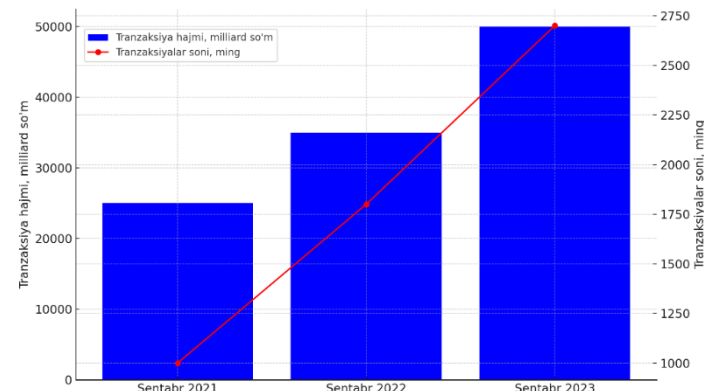
Qolaversa, O'zbekiston kabi o'ziga xos joylashuvga ega bo'lgan mintaqalarda, raqamlashtirish masalasi aslida boshqa muhim omillar bilan teng darajada ahamiyatga ega. Agar bu holatni formula yordamida tasvirlasak, quyidagicha ko'rinish hosil bo'ladi:

$$E = ET \times (I + M)$$

Tenglamada ET (Elektron tijorat va savdo platformalari) infratuzilma (I) va mintaqaviy hamkorliklar (M) bilan ko'paytiriladi, chunki raqamli savdo platformalarining samaradorligi ushbu ikki omilga bog'liq. Infratuzilma (masalan, yuqori tezlikdagi internet va raqamli to'lov tizimlari) raqamli savdoni muvaffaqiyatli amalga oshirish uchun zarurdir, mintaqaviy va xalqaro savdo hamkorliklari esa mahsulotlarni qo'shni davlatlar va xalqaro bozorlarga tez va samarali yetkazib berishga yordam beradi. Shuning uchun, ET samarali bo'lishi uchun O'zbekistondagi infratuzilma va hamkorliklar mustahkam bo'lishi kerak.

Ushbu tenglama O'zbekistonning tashqi logistika va eksport faoliyatini rivojlantirishda muhim ahamiyat kasb etadi, chunki u mamlakatning quruqlik bilan o'ralganligi sababli yuzaga keladigan savdo cheklovlarini yengib o'tishga yordam beradi. Raqamli savdo platformalariga (ET) investitsiyalar kiritish orqali O'zbekiston o'z mahsulotlarini global bozorlarga tezkor va samarali tarzda yetkazib berish imkoniyatiga ega bo'ladi. Elektron tijorat va raqamli platformalar kichik va o'rta biznes subyektlarini xalqaro mijozlar bilan bog'lab, vositachilik xarajatlarini kamaytiradi. Misol uchun, elektron tijorat platformalari orqali O'zbekiston mahsulotlari global

bozorlarga, xususan, qo'shni davlatlar yoki uzoq mintaqalarga tezroq yetkazib beriladi.



Grafik 4: O'zbekistondagi O'nlayn To'lovlar Hajmi, 2021-2023. *Manba:* Global CIO[13]

Shuningdek, O'zbekiston Markaziy Bankining onlayn to'lovlar bo'yicha ma'lumotlari 2021-yildan 2023-yilgacha sezilarli o'sishni ko'rsatmoqda. Tranzaksiya hajmi 25 trillion so'mdan 50 trillion so'mga oshgan, bu esa onlayn to'lovlar bozorining kengayish tendensiyasini bildiradi. Tranzaksiyalar soni ham shu davrda 1000 mingdan 2700 mingga oshgani raqamli to'lov xizmatlarining kengayishini tasdiqlaydi. Bu O'zbekiston kabi quruqlik bilan o'ralgan davlatlar uchun ayniqsa muhimdir, chunki elektron tijorat platformalari savdo hajmini oshirish, yangi bozorlarni kashf etish va iqtisodiy samaradorlikni kuchaytirishga xizmat qiladi. Shu sababli, raqamli savdo platformalarini kengaytirish O'zbekistonning global logistik tarmoqlarida o'z o'rnini mustahkamlashda katta ahamiyat kasb etadi.

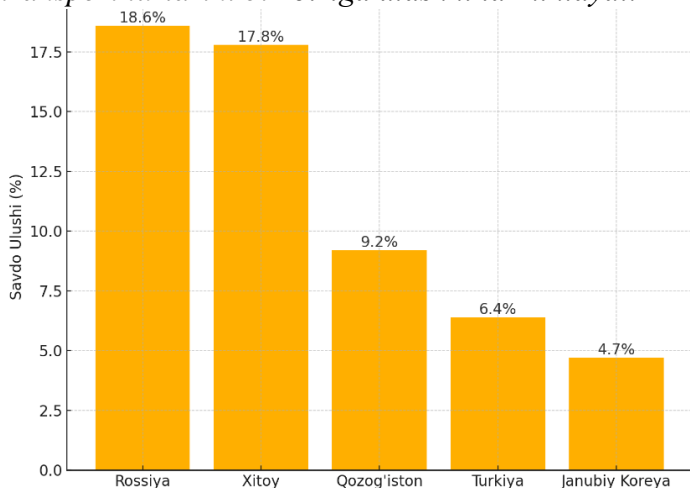
Bundan tashqari, infratuzilma (I) va mintaqaviy hamkorliklar (M) eksport samaradorligini oshirishda hal qiluvchi ahamiyatga ega. Texnologik infratuzilmaning yaxshilanishi, masalan, yuqori tezlikdagi internet, raqamli to'lov tizimlarining joriy qilinishi O'zbekistonning raqamli savdo imkoniyatlarini kengaytiradi va tashqi savdo jarayonlarini avtomatlashtirishga yordam beradi. O'zbekistonning havo, yo'l va temir yo'l infratuzilmasini yaxshilash xalqaro savdoda mahsulotlarning xavfsiz va samarali yetkazilishini ta'minlash uchun muhim ahamiyatga ega. Quruqlik bilan oralgan mamlakat sifatida, transport jarayonlarining ishonchligini oshirish uchun yangi



texnologiyalar va xavfsizlik standartlarini joriy qilish zarur. Shuningdek, ko'p modalli transport* tizimini qo'llash orqali yuklarni temir yo'l, avtomobil va dengiz transporti orqali birlashtirib yetkazish logistika xarajatlarini kamaytirib, savdo jarayonlarini tezlashtiradi va mamlakat raqobatbardoshligini oshirishga xizmat qiladi.[14]

Mintaqaviy va xalqaro savdo hamkorliklari doirasida qo'shni davlatlar bilan raqamli integratsiyani kuchaytirish, jumladan, transport va bojxona jarayonlarini avtomatlashtirish savdo yo'nalishlarini optimallashtiradi va tranzit to'siqlarini kamaytiradi. Bu O'zbekiston mahsulotlarini tezkor va samarali eksport qilish imkoniyatini oshirib, savdo xarajatlarini kamaytiradi va xalqaro bozorda raqobatbardoshligini mustahkamlaydi.

***Izoh: Ko'p modalli transport — bu yuk tashish jarayonida bir nechta transport turidan (masalan, temir yo'l, avtomobil, dengiz) foydalanish usuli. Bu yuklarni tez va samarali yetkazish uchun transport turlarini bir-biriga ulashni ta'minlaydi.**



Grafik 5: O'zbekistonning Asosiy Savdo Hamkorlari, 2022. **Manba:** International Trade Administration[15]

Xususan, yuqoridagi grafik 5da O'zbekistonning 2022-yildagi asosiy savdo hamkorlarini ko'rsatadi. Rossiya (18.6%) va Xitoy (17.8%) eng yirik savdo hamkorlari bo'lib, O'zbekistonning eksport va importdagi muhim sheriklari hisoblanadi. Shuningdek, Qozog'iston (9.2%), Turkiya (6.4%) va Janubiy Koreya (4.7%) ham O'zbekiston savdo geografiasining ajralmas qismidir. Bu davlatlar bilan kuchli iqtisodiy aloqalar

O'zbekistonning mintaqadagi savdo jarayonlarini kengaytirishga xizmat qiladi.

Biroq, quruqlik bilan o'ralgan O'zbekiston uchun faqat qo'shni davlatlar bilan cheklangan holda qolmaslik, global savdo geografiasini kengaytirish juda muhimdir. Elektron tijorat va raqamli savdo platformalari yordamida boshqa uzoq bozorlar bilan savdo qilish imkoniyatlari kengaytirilishi zarur. Shu bilan birga, mintaqaviy hamkorlik O'zbekiston kabi davlatlar uchun hal qiluvchi ahamiyatga ega, chunki logistika va tranzit imkoniyatlari qo'shni davlatlar orqali amalga oshiriladi. Yaqin davlatlar bilan transport va bojxona sohalarida raqamli hamkorlikni kuchaytirish O'zbekistonning xalqaro bozorlarga chiqishini tezlashtiradi va tranzit xarajatlarini kamaytiradi.

Xulosa va tavsiyalar: O'zbekistonning xalqaro savdoda raqobatbardosh bo'lishi va samarali ishtirok etishi transport va logistika infratuzilmasini modernizatsiya qilishga qaratilgan chora-tadbirlar bilan bevosita bog'liq. Transport infratuzilmasini takomillashtirish, mahsulotlarni tez va samarali tarzda xalqaro bozorlarga yetkazish imkoniyatlarini kengaytiradi. Bojxona jarayonlarining raqamlashtirilishi, jarayonlarning soddalashtirilishi va xavfsizlik standartlarini oshirish logistika xarajatlarini sezilarli darajada kamaytirib, tashish jarayonlarining samaradorligini oshiradi va mahsulotlarni yetkazib berish muddatlarini qisqartiradi. Bu esa eksport va import operatsiyalarida raqobatbardoshlikni oshiradi hamda O'zbekistonning savdo aloqalarini kengaytirishga xizmat qiladi.

O'zbekistonning quruqlik bilan oralgan geografik joylashuvi xalqaro savdoda murakkab logistika muammolarini keltirib chiqaradi. Biroq, bu cheklovlarni ko'p modalli transport tizimlarini takomillashtirish orqali hal qilish mumkin. Temir yo'l, avtomobil va dengiz transportining samarali integratsiyasi mahsulotlarni portlarga tez yetkazib, xalqaro bozorlarga jo'natish jarayonlarini tezlashtiradi va xarajatlarni kamaytiradi. Bu esa savdo jarayonlarini samaraliroq, arzon va raqobatbardosh qilishga xizmat qiladi.

Bundan tashqari, transport tizimlarining integratsiyasi O'zbekistonning xalqaro hamkorlikni kuchaytirishi va mintaqaviy tranzit yo'llari orqali



yanada keng savdo aloqalariga ega bo'lishini ta'minlaydi. Shu tarzda, mamlakat o'zining quruqlik bilan oralganligi tufayli yuzaga keladigan cheklovlarni yengib, global savdoda o'z o'rnini mustahkamlashi mumkin.

Adabiyotlar ro'yxati

1. Prabhakra, M. S. Shimoliy-Sharqiy Hindiston quruqlik bilan o'ralganmi? Economic and Political Weekly, 2004-yil 16-22 oktyabr, 39-jild, 42-son, 4606-4608-betlar. Nashr qilingan: Economic and Political Weekly.
2. Prabhakra, M. S. Shimoliy-Sharqiy Hindiston quruqlik bilan o'ralganmi? Economic and Political Weekly, 2004-yil 16-22 oktyabr, 39-jild, 42-son, 4606-4608-betlar. Nashr qilingan: Economic and Political Weekly.
3. Jayaramon T.K., Shrestha O.L. (1976). "Quruqlikda joylashgan Nepalning savdo muammolari", Asian Survey, 16(12), 1113-1123-betlar.
4. Debie J. va B. Steck (2001). "Quruqlikda joylashganlik: nazariy qayta baholash va G'arbiy Afrikaga tatbiq qilish", Geografik makon, 30(1), 26-36-betlar.
5. MacKellar, Landis, Andreas Wörgötter va Julia Wörz (2000). "Quruqlikda joylashgan davlatlarning iqtisodiy rivojlanish muammolari", O'tish iqtisodiyoti seriyasi, №14.
6. Arvis, Jean-Francois, Gael Raballand va Jean-Francois Marteau (2010). "Quruqlikda joylashganlik xarajatlari: Logistika xarajatlari va ta'minot zanjiri ishonchliligi", Taraqqiyot yo'nalishlari, Savdo, Nashriyot: Jahon Banki, Vashington, D.C.
7. Radelet, Steven va Jeffrey D. Sachs. "Yuk tashish xarajatlari, ishlab chiqarilgan mahsulotlar eksporti va iqtisodiy o'sish", Amerika Iqtisodchilar Assotsiatsiyasi yillik yig'ilishida taqdim etilgan, Chikago.
8. Faye, Michael L., John W. Macarthur, Jeffery D. Sachs va Thomas Snow (2004). "Quruqlikda joylashgan rivojlanayotgan davlatlar duch keladigan muammolar", Inson taraqqiyoti jurnali, 5(1), 31-68-betlar.

9. Jahon Banki. (2020). O'zbekiston: Transport va Logistika Taraqqiyoti uchun Integratsiyalashgan Rivojlanish Asoslari. Vashington, D.C.: Jahon Banki
Guruhi. Manba: <https://openknowledge.worldbank.org/server/api/core/bitstreams/9c7cef2e-0802-5579-aeff-8bb32946e2f8/content>.

10. Scienta.Global (2021) "Xitoyning Bir makon, bir yo'l tashabbusi: Dunyo bo'ylab ulkan ulanish tashabbusi,"
Manba: <https://jstor.org/stable/community.37317647>.

11. Jahon Banki. (2021). Savdo va iqtisodiy rivojlanishni yaxshiroq logistika orqali kuchaytirish.
Manba: <https://blogs.worldbank.org/en/trade/boosting-trade-and-economic-development-through-better-logistics>.

12. UNCTAD. (2023). Savdo jarayonlarini raqamlashtirishning global ko'rinishlari: raqamli transformatsiyani rivojlantirish. Manba: <https://unctad.org/news/advancing-digital-transformation-global-insights-digitalization-trade-procedures>

13. GlobalCIO. (2023). Digital Transformation of Uzbekistan.
Manba: <https://globalcio.com/articles/main/digital-transformation-of-uzbekistan/>

14. Rodrigue, J-P. (2020). Transport va Iqtisodiy Rivojlanish. Transport tizimlari geografiyasi.
Manba: <https://transportgeography.org/contents/chapter3/tranportation-and-economic-development/>.

15. Trade.gov. (2023). Uzbekistan Market Overview. Manba: <https://www.trade.gov/country-commercial-guides/uzbekistan-market-overview>



ПРИМЕНЕНИЕ ИГРОВЫХ МЕТОДОВ ДЛЯ РАЗРАБОТКИ МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ УСТОЙЧИВЫХ АЛГОРИТМОВ УПРАВЛЕНИЯ НЕСТАЦИОНАРНЫМИ ОБЪЕКТАМИ

Сотволдиев Хуснидин Ибрагимович,
Ферганский филиал ТУИТ имени Мухаммада
Аль-Хорезми, PhD

Аннотация: В статье рассматривается применение игровых методов для разработки математического обеспечения устойчивых алгоритмов управления нестационарными объектами, которые характеризуются изменяющимися во времени параметрами и подвержены влиянию возмущений и ошибок измерения, что создает дополнительные сложности в управлении. Игровые методы рассматриваются как эффективный инструмент для построения стратегий управления, позволяющий учитывать динамику изменений внешней среды и внутренние процессы системы. Подчеркнута значимость использования методов регуляризации для повышения устойчивости решений. Предложенный метод можно использовать для создания более надежных и адаптивных алгоритмов управления, способствующих повышению эффективности управления в условиях изменчивости и неопределенности.

Ключевые слова: игровые методы, алгоритмы управления, нестационарные объекты, условия неопределенности, методы регуляризации

Введение

В современных условиях стремительного развития технологий и повышенной сложности управляемых систем, все более актуальной становится задача разработки устойчивых алгоритмов управления нестационарными объектами. Такие объекты характеризуются изменяющимися во времени параметрами. Это усложняет прогнозирование их поведения и разработку эффективных методов управления. Применение традиционных методов часто не дает должной точности и устойчивости в условиях изменчивости внешних факторов и неопределенности.

Одним из перспективных направлений решения данной проблемы является использование игровых методов, которые предоставляют эффективные механизмы для разработки адаптивных и устойчивых алгоритмов управления [8]. Игровые методы позволяют учитывать не только текущие состояния системы, но и поведения различных воздействий. Это дает возможность для построения гибких и надежных алгоритмов, способных эффективно справляться с неопределенностью.

Данная работа посвящена исследованию применения игровых методов в разработке математического обеспечения устойчивых алгоритмов управления нестационарными объектами. Рассмотрены вопросы адаптивности и устойчивости алгоритмов, что позволяет обеспечивать надежное функционирование систем в условиях изменения параметров объекта и окружающей среды.

Математическое обеспечение, разработанное с использованием игровых методов, направлено на повышение эффективности процессов и уменьшение ошибок в управлении сложными нестационарными системами.

Литературный обзор

С учетом возможности формализации задач управления в условиях неопределенности, естественным выглядит интерес к использованию математического аппарата теории игр в исследовании проблем теории управления [1-5]. В работах М.В. Жирова, В.В. Макарова и В.В. Солдатова рассматриваются вопросы идентификации и адаптивного управления технологическими процессами с нестационарными



параметрами. Авторы фокусируются на разработке подходов, позволяющих эффективно управлять сложными технологическими объектами, параметры которых изменяются во времени [1]. В работе В.Д. Юркевича. «Синтез нелинейных нестационарных систем управления с разнотемповыми процессами» исследуются методы синтеза систем управления, в которых одновременно протекают процессы с разными временными характеристиками [3]. Рассматриваются различные подходы к синтезу управляющих законов, включая адаптивные и робастные методы, игровые методы, обеспечивающие устойчивость и высокую эффективность управления в условиях нелинейности и нестационарности. А.А. Бобцов, А.В. Лямин и К.А. Сергеев в работе «Синтез закона адаптивного управления для стабилизации неточно заданных нестационарных объектов» рассматривают задачу разработки адаптивного закона управления для стабилизации объектов, параметры которых либо неизвестны, либо изменяются во времени [5]. Применение игровых методов в рамках данной задачи могло бы значительно повысить эффективность разработанных алгоритмов, особенно в условиях неопределенности.

Методы

При выборе решения в условиях неопределенности неизбежен элемент риска, который тем выше, чем больше недостаток информации при принятии решения. Поэтому одним из основных критериев оценки оптимальности решения является минимизация риска при его принятии. Процедура принятия управленческого решения имеет ярко выраженный многоступенчатый характер [5, 6]. Выбор оптимального решения в условиях неопределенности делается исходя из анализа нескольких вариантов с точки зрения нескольких критериев, согласно которых определяется его оптимальность в сложившейся комбинации внешних и/или внутренних факторов [2]. Очевидно, что изменение факторов, повлиявших на выбранное решение приводит к изменению оптимального решения.

В последнее время игровые задачи управления динамическими системами, а также наблюдения и поиска получили значительное распространение [2, 3]. Оптимальное управление рассматривается в смысле мини-максимума, т.е. возможность получения со стороны управления наилучшего гарантированного результата, тогда как другая сторона использует произвольно допустимые воздействия.

Рассмотрим нестационарный объект управления, описываемый уравнением:

$$x_{i+1} = A_i v + B_i \bar{u}_i, \quad i = 1, 0, \dots, I, \quad (1)$$

где $A_i = \|a_{in}\|$ – матрица-строка коэффициентов $a_{in}, n = 1, 2, \dots, N$;
 $v = (v_1, v_2, \dots, v_N)^T$ – является вектором возмущений, который действует на объект; $B_i = \|b_{ir}\|$ – является матрицей-строкой коэффициентов $b_{ir}, r = 1, 2, \dots, i$; \bar{u}_i – является

временной последовательностью управлений u_1, u_2, \dots, u_i . При этом в (1) нет начального управления u_0 , обоснованно выбрать которое в условиях поставленной задачи невозможно.

Сумма величины x_i и аддитивной случайной ошибки $h_i (y_i = x_i + h_i, i = 1, 2, \dots, I)$ измеряется и поступает на вход управляющего устройства. При управлении должно выполняться неравенство [5, 7]:

$$|u_i| \leq U_i, \quad i = 1, 2, \dots, I, \quad (2)$$

здесь U_i – является максимально допустимым значением абсолютной величины u_i . Считается, что возмущения и ошибки измерения по абсолютной величине не больше величин $V_n, n = 1, 2, \dots, N$ и $H_i, i = 1, 2, \dots, I$:

$$|v_n| \leq V_n, \quad |h_i| \leq H_i. \quad (3)$$

Таким образом, ставится игровая задача определения функции $u_i = u_i(\bar{y}_i, \bar{u}_{i-1}), i = 1, 2, \dots, I$:



$$\inf_{u_i \in \omega_k} \sup_{v, \bar{h}_l \in \omega_n} |x_{l+1}(u_l, v, \bar{h}_l)|, \quad (4)$$

где допустимые области ω_k и ω_n определяются соответственно выражениями (2) и (3) [8]. Вводя вектор $\bar{x}_i^* = (x_1^*, x_2^*, \dots, x_i^*)$, координаты которого определяются соотношением

$$x_i^* = x_i - B_{i-1} \bar{u}_{1(i-1)},$$

используем для записи уравнения объекта:

$$\bar{x}_{i+1}^* = A_i v, \quad i = 0, 1, \dots, I, \quad (5)$$

здесь A_i — является матрицей, которая составлена из строк A_r , $r = 0, 1, \dots, i$.

Используя принцип динамического программирования сначала определим управление u_i^* для дискретного момента I . Определим критерий (4) в виде

$$\inf_{u_i \in \omega_k} \sup_{v, \bar{h}_l \in \omega_n} \left| A_i v + \sum_{r=1}^{I-1} b_{lr} u_r + b_{II} u_i \right|. \quad (6)$$

Тогда величина u_i при отсутствии ограничения (2) с учетом критерия (6) и выражения (5) можно представить в виде:

$$u_i^* = -\frac{1}{b_{II}} \left(G_I \bar{y}_i^* + \sum_{r=1}^{I-1} b_{lr} u_r \right), \quad (7)$$

здесь $G_I = \|g_{II}\|$ — является матрицей-строкой искомым коэффициентов оптимального управления u_i^* ; \bar{y}_i^* является вектором, который составлен из измеренных значений величин x_i^* , $i = 1, 2, \dots, I$.

Учитывая (7) критерий (6) можно записать следующим образом:

$$\inf_{G_I} \sup_{v, \bar{h}_l \in \omega_n} |A_i v + G_I \bar{y}_i^*|, \quad (8)$$

тогда:

$$\Gamma v = z, \quad (9)$$

где $\Gamma = \theta^{(l)} A_{l-1}$, $z = \theta^{(l)} \bar{x}_l^*$, $\theta^{(l)} = \|g_{nl}^{(l)}\|$ — матрица произвольных коэффициентов $g_{nl}^{(l)}$, $n = 1, 2, \dots, N$; $l = 1, 2, \dots, I$.

Условия аппроксимация уравнения (9) примем в виде:

$$\|\tilde{\Gamma} - \Gamma\| \leq h, \quad \|\tilde{z} - z\| \leq \delta.$$

В условиях приближенного задания исходных данных уравнение (9) может быть плохо обусловленным, что предопределяет необходимость использования методов регуляризации.

Результаты и обсуждения

Учитывая все вышеизложенное, сделаем следующие заключения: Нестационарный объект управляется уравнением, которое учитывает воздействие векторов возмущений и временной последовательности управлений [1]. Это указывает на необходимость адаптивного подхода к управлению, где система должна реагировать на изменения во времени. В условиях задачи отсутствует начальное управление u_0 , что может затруднить настройку системы. Это подчеркивает сложность управления в реальных условиях, где часто невозможно заранее определить начальные параметры. При этом условия (2) и (3) вводят ограничения на значения возмущений и ошибок измерения. Эти ограничения необходимы для обеспечения устойчивости и надежности управления, и позволяют избежать чрезмерных колебаний в системе, которые могут привести к неустойчивости.

Формулировка игровой задачи для определения функции управления подчеркивает необходимость подхода, учитывающего влияние внешних факторов и возможные ошибки. Это может помочь в разработке более эффективных стратегий управления, учитывающих



неопределенности [9]. Использование вектора z для записи уравнения объекта в (5) способствует более компактному и удобному математическому описанию системы, что упрощает дальнейший анализ и применение методов оптимизации.

Применение динамического программирования для определения управления на дискретном моменте I влечет за собой возможность оптимизации решений поэтапно, что позволяет учитывать предыдущие состояния и улучшать текущее управление.

Определение критерия (6) позволяет формализовать задачу управления и установить количественную меру для оценки различных стратегий. Это создает основу для анализа и сравнения различных подходов к управлению в условиях неопределенности.

Критерий (6) переработан в (8), что позволяет более явно представить зависимости в задаче. Дальнейшее преобразование (9) вводит матрицы произвольных коэффициентов, что добавляет гибкости в формулировку задачи.

Однако, в условиях приближенного задания исходных данных, уравнение (9) может оказаться плохо обусловленным, что вызывает необходимость применения методов регуляризации.

Заключение

Нестационарные объекты управления характеризуются изменяющимися во времени параметрами и подвержены различным возмущениям и ошибкам измерения, что делает задачу управления особенно сложной.

Применение игровых методов становится особенно актуальным, потому что игровые подходы могут помочь в формулировке управления как стратегии противостояния неопределенности, рассматривая различные возмущения и ошибки. Это позволяет адаптировать алгоритмы управления, принимая во внимание потенциальные реакции системы на различные внешние воздействия.

Использование игровых методов позволяет строить более надежные стратегии управления, учитывающие динамику изменений и неопределенности. Они обеспечивают

возможность оценки различных сценариев и выбора оптимального решения. Таким образом, игровые методы не только повышают устойчивость и адаптивность систем управления, но и способствуют более глубокой проработке сложных задач в условиях неопределенности.

Игровые методы рассматриваются как эффективный инструмент для построения стратегий управления, которые позволяют учитывать возможные изменения внешней среды и динамику внутренних процессов. Эти методы помогают формализовать управление как сложную многоступенчатую задачу, где каждое решение требует анализа предыдущих действий и прогнозирования реакции системы.

Применение игровых методов в разработке математического обеспечения устойчивых алгоритмов для управления нестационарными объектами представляет собой перспективное направление, способствующее улучшению устойчивости и эффективности систем управления в условиях неопределенности.

Литература

1. Жиров, М.В., Макаров, В.В., Солдатов, В.В.(2011). Идентификация и адаптивное управление технологическими процессами с нестационарными параметрами. -М.: МГТУ им. Н.Э. Баумана. -208 с.
2. Галяев, Е.Р. (2011). Робастное субоптимальное управление линейными нестационарными объектами по выходу ISSN 2072-9502 Управление, вычислительная техника и информатика. № 1. 31-36.
3. Юркевич, В.Д. (2000). Синтез нелинейных нестационарных систем управления с разнотемповыми процессами. СПб.: Наука.
4. Кривулин, Н.П. (2018). Восстановления входных сигналов нестационарных динамических систем // Известия высших учебных заведений. Физ. мат. науки №3(47). 64-78.
5. Бобцов, А.А., Лямин, А.В., Сергеев, К.А. (2001). Синтез закона адаптивного управления для стабилизации неточно



заданных нестационарных объектов // Изв.
вузов. Приборостроение. № 3. 3-7.

6. Yusupbekov, N.R., Igamberdiev, H.Z., Mamirov, U.F. (2020). Adaptive Control System with a Multilayer Neural Network under Parametric Uncertainty Condition. In: Russian Advances in Fuzzy Systems and Soft Computing: selected contributions to the 8-th International Conference on Fuzzy Systems, Soft Computing and Intelligent Technologies (FSSCIT-2020), Vol. 2782, 228-234.
7. Карабутов, Н.Н. (2016). Адаптивная идентификация систем: Информационный синтез. Изд. стереотип. 384 с.
8. Андриенко, А. Я., Тропова, Е. И., Чадаев, А. И. (2011). Игровые принципы терминального управления нестационарным объектом / Управление большими системами. Выпуск 35. М.: ИПУ РАН. 59-67.
9. Сотволдиев, Х.И. (2023). Устойчивые алгоритмы идентификации характеристик состояния нестационарной динамической системы по данным наблюдений // FarPI, Ilmiy – texnika jurnali, 27 tom, №1.120-125.



INTELLEKTUAL SUV TOMCHISI ALGORITMINING TIBBIY TASHXIS QO'YISH MASALALARIGA QO'LLANILISHI

Muhammediyeva Dildora Kabilovna,
texnika fanlari doktori,
TATU, Axborot texnologiyalari va
dasturiy ta'minot kafedrası professori
E-mail: matematichka@inbox.ru

Eshboyev Erkin Abdirashidovich,
Qarshi davlat universiteti
Amaliy matematika kafedrası dotsenti
E-mail: erkineshboyev@gmail.com

Klicheva Firuza Gulmurotovna,
Qarshi davlat universiteti
Amaliy matematika kafedrası o'qituvchisi
E-mail: vip.qilicheva@mail.ru

Annotatsiya. Ushbu maqola tibbiy tashxis qo'yish masalasini hal qilish uchun intellektual suv tomchilari algoritmini (IWD) qo'llashni taklif etadi. Maqoladan maqsad IWD ning tibbiy tashxislash masalalariga qo'llanilishini sinab ko'rish va boshqa umumiy optimallashtirish algoritmlari bilan taqqoslaganda uning samaradorligini baholashdir. Shu maqsadda maqolada IWD algoritmidan foydalanib, yurak qon-tomir kasalliklari bilan og'rigan bemorlarga tashxis qo'yish jarayonini intellektual tarzda amalga oshirishni bajaruvchi standart obrazlarni anglash masalasi qaralgan. Qo'yilgan masalani yechish maqsadida haqiqiy tibbiy ma'lumotlarga asoslanib, IWD algoritmi asosida ishlovchi dasturdan natijalar olingan.

Shuningdek ushbu algoritm yordamida olingan natijalar boshqa umumiy optimallashtirish algoritmlari (Ant) yordamida olingan natijalar bilan taqqoslangan va natijalar jadval ko'rinishida keltirilgan.

Kalit so'zlar: Intellectual Water Drops, tashxislash, informativ alomat, optimallashtirish, model, metaevristik algoritm, populyatsiya, agent, tuproq, tezlik.

Kirish. Tibbiy tashxis qo'yish muhim o'rin tutadigan zamonaviy dunyoda kasalliklarni aniqlash va samarali davolash usullarini ishlab chiqish, tashxisning aniqligini oshirishning mukammal usul va vositalarini izlash eng dolzarb vazifalardan biri hisoblanadi. Bu sohadagi innovatsion yondashuvlardan biri tibbiy tashxis qo'yish masalalarini hal qilish uchun intellektual algoritmlardan foydalanishdir [1-3].

Ushbu maqolada tibbiy tashxis qo'yish masalalarini hal qilish uchun intellektual suv tomchilari algoritmi (*Intellectual Water Drops*- IWD) ni qo'llashga e'tibor qaratamiz. IWD - bu murakkab optimallashtirish muammolarida optimal yechimlarni samarali topishga mo'ljallangan metaevristik

optimallashtirish algoritmi hisoblanadi. Ushbu ishdan maqsad IWD algoritmining tibbiy tashxis qo'yish masalalariga qo'llanilishini o'rganish va boshqa umumiy optimallashtirish algoritmlari bilan taqqoslaganda samaradorligini aniqlashdir. Maqolada quyidagi vazifalarga e'tibor qaratamiz:

- Optimal alomatlarini tanlash: Biz bemor alomatlarining katta to'plamidan informativ alomatlarini tanlash uchun IWD dan foydalanish imkoniyatini o'rganamiz. Bu tasniflash va bashorat qilish algoritmlarining aniqligi va samaradorligini oshiradi.
- Model parametrlarini optimallashtirish: Tibbiy tashxis qo'yishda ishlatiladigan



mashinali o'rganish modellarining parametrlarini optimallashtirish uchun IWD dan foydalanish imkoniyati o'rganiladi. Bu modellarni muayyan tashxislash vazifasining xususiyatlariga mos keladigan tarzda sozlash imkonini beradi.

- Bemorlarni tasniflash: Bemorlarni ularning alomatlariga qarab tasniflash uchun IWD dan foydalanish imkoniyati o'rganiladi. Bu o'xshash alomatlarga ega bo'lgan bemorlar guruhlarini aniqlashga, tashxis va qaror qabul qilish aniqligini oshirishga yordam beradi.

Ish davomida haqiqiy tibbiy ma'lumotlar bo'yicha tajribalar o'tkaziladi va IWD yordamida olingan natijalar boshqa umumiy optimallashtirish algoritmlari bilan taqqoslanadi.

Maqolada IWD algoritmidan foydalanib, yurak qon-tomir kasalliklari bilan og'rigan bemorlarga tashxis qo'yish jarayonini intellektual tarzda amalga oshirishni bajaruvchi standart obrazlarni anglash masalasi qaraladi.

Adabiyotlar tahlili va metodologiya.

Intellektual suv tomchilari algoritmi daryolarda sodir bo'ladigan ba'zi jarayonlarni modellashtirish va keyin ularni algoritm sifatida amalga oshirishga urinishdir.

IWD algoritmi yangi ishlab chiqilgan algoritmlardan biri bo'lib, bu algoritm daryo tizimlari dinamikasini simulyatsiya qiladi. IWD - populyatsiyaga asoslangan algoritm bo'lib, unda har bir tomchi yechimni ifodalaydi va yechimlarni qidiruv paytida tomchilarni almashtirish yanada yaxshi yechimlarni topish imkoniyatini beradi.

2007 yilda eronlik olim Hamed Shoh-Husayni intellektual tomchilarning xatti-harakatlari algoritmini ishlab chiqdi [4]. IWD algoritmidan bir nechta sun'iy suv tomchilari o'zaro ta'sir natijasida o'z muhitini eng kam qarshilik yo'li bo'ylab optimal yo'lni topadigan tarzda o'zgartirishga qodir. Bu algoritm populyatsiyaga yo'naltirilgan konstruktiv optimallashtirish algoritmi hisoblanadi [5-6].

IWD - bu suv tomchilari daryo oqimini o'zgartirish orqali o'z manziliga optimal yo'lni topadigan model. Unga uchta muhim parametr yordam beradi. Tomchilar o'z harakat tezligiga ko'ra daryoning tubidagi tuproqlarni tashish xususiyatiga ega.

Tomchining tezligi qanchalik yuqori bo'lsa, u tashiydigan tuproq miqdori shunchalik ko'p bo'ladi, bu esa o'z navbatida boshqa agentlarning erkin harakatini ta'minlaydi. Tuproq bo'lmagan joylarda oqim tezligi oshadi [7]. Optimal yo'lni eng kam miqdordagi tuproq bo'lgan va eng yuqori tezlikka erishish mumkin bo'lgan yo'l deb atash mumkin. IWD yordamida optimallashtirish strategiyasini amalga oshirish mumkin, bunda tasodifiy agentlar bir-biri bilan intellektual tarzda o'zaro ta'sirlashadi, shu yo'l bilan ular birgalikda daryo oqimi yo'nalishini o'zgartiradi va hech qanday tuproqqa duch kelmaydigan optimal yo'lni yaratadi. Bunda agentlarning oqim tezligi mumkin bo'lgan eng yuqori darajaga erishadi [8-9].

IWD algoritmining asosiy tamoyillari:

- Har bir suv tomchisi ko'p tuproqli yo'ldan ko'ra kam tuproqli yo'lni afzal ko'radi.
- Har bir suv tomchisi manbadan manzilgacha bo'lgan yo'lda bir nechta yo'nalishlardan birini tanlashga to'g'ri kelganda qisqaroq yo'lni tanlaydi.
- Yo'lning holati shu yo'ldagi tuproq miqdori bilan belgilanadi, tuproq darajasi ko'p bo'lgan yo'l optimal bo'lmagan yo'l, tuproq darajasi kam bo'lgan yo'l esa optimal yo'l hisoblanadi.

Daryoda oqayotgan har bir tomchi suvning xususiyatlaridan biri uning tezligi hisoblanadi. Yana bir xususiyati uning tuproq tashuvchanligidir. Shunday qilib, har bir tomchi suv ma'lum miqdordagi tuproqni bir joydan ikkinchi joyga ko'chirishga qodir. Bunda tuproq tez harakatlanuvchi qismdan sekin harakatlanuvchi qismga o'tadi. Ushbu harakat davrida uchta o'zgarish ro'y beradi:

- suv tomchisining tezligi oshadi;
- suv tomchisining tuproq bilan to'yinganligi ortadi;
- bu ikki nuqta orasida kanaldagi tuproq miqdori kamayadi (grafning ikki nuqtasi orasidagi vazn kamayadi).

Shunday qilib, IWD algoritmidan tomchilar ikkita asosiy xususiyatga ko'ra tavsiflanadi:

- tezlik,
- tuproq.

Bu xususiyatlarning ikkalasi ham algoritm ishlashi davomida o'zgarib turadi. IWDdagi tomchilar



manbadan manzilga o'tadi va o'z sayohatini boshlang'ich tezlik va tuproq miqdori bilan boshlaydi [10]. Harakat davomida tomchilar tuproq olib tashlanadigan va biroz tezlikka erisha oladigan muhitdan o'tadi. Bunda IWD iterativ tarzda amalga oshiriladi deb taxmin qilinadi. Joriy nuqtadan ikkinchisiga tomon suv tomchisining harakati davomida tomchi tezligi tuproq miqdoriga teskari proporsional bo'lib, ular nohiziqli munosabatda bo'ladi:

$$vel = vel(t - 1) + \frac{Av}{Bv + Cv * soil^2(i, j)} \quad (1)$$

Bu yerda Av , Bv , Cv tezlik koeffitsientlari (kirish parametrlari), $soil(i, j)$ esa graf tugunlari orasidagi tuproq miqdori. Bundan ko'rinadiki, kam tuproqli yo'l IWD tomchisining ko'p tuproqli yo'lga qaraganda tezroq harakatlanishiga imkon beradi.

IWD tomchisi atrof-muhit bo'ylab harakat qilganda tuproqni to'playdi. Bu tuproq ikki joyni bog'laydigan yo'ldan olinadi. IWD tomchisi olgan tuproq miqdori IWDni hozirgi joydan keyingi joyga ko'chirish uchun zarur bo'lgan vaqtga nohiziqli proporsionaldir. Bu vaqt oralig'i chiziqli harakat uchun oddiy fizika qonunlari yordamida hisoblanadi:

$$time(i, j, vel) = \frac{R}{vel} \quad (2)$$

Bu yerda R - ikki nuqta (tugun) orasidagi masofa. Tomchiga qo'shilgan tuproq miqdori:

$$dSoil(i, j) = \frac{As}{Bs + Cs * time(i, j, vel)} \quad (3)$$

Bu yerda As , Bs , Cs - tuproqning meliorativ holati koeffitsientlari. Nuqtalar orasidagi yo'lda yangi tuproq miqdori quyidagicha aniqlanadi:

$$soil(i + 1, j + 1) = Po * soil(i, j) + Pn * dSoil(i, j) \quad (4)$$

Bu yerda Po va Pn - tuproq miqdorining o'zgarish jarayonining koeffitsientlari.

Shunday qilib, harakatlanish uchun sarflangan vaqt harakat tezligiga teskari proporsional va ikki

nuqta orasidagi masofaga to'g'ri proporsional bo'ladi. Shuni ta'kidlash kerakki, bu yerda tuproq atrof-muhit haqidagi ma'lumotlarning miqdoriy ko'rsatkichidir. Yuqorida keltirilgan formulalar tomchilarning tuproq darajasi yuqori bo'lgan yo'llarga nisbatan tuproq darajasi past bo'lgan yo'llarni tanlash afzalligini ko'rsatadi. Optimal yo'lni tanlash mavjud yo'llarga yagona tasodifiy taqsimotni qo'llash orqali amalga oshiriladi. Navbatdagi yo'lni tanlash ehtimoli mavjud yo'llarning tuproq darajasiga teskari proporsionaldir. Shuning uchun, tuproq darajasi past bo'lgan yo'llar IWD tomchilari tomonidan tanlanish ehtimoli yuqori [11-14].

Rayapudi [15] tomonidan olib borilgan tadqiqotda IWD algoritmi iqtisodiy yuklarni jo'natish muammolarini (ELDP) hal qilish uchun qo'llanilgan. Lenin va Kalavati [16] tadqiqotida IWD algoritmi aralash butun sonli chiziqli bo'ylmagan optimallashtirish masalasi sifatida tuzilgan optimal reaktiv quvvatni taqsimlash masalalarini hal qilish uchun taklif qilishgan.

D.J.Kalita va boshqalarning tadqiqotida ko'krak bezi saratonini erta bosqichda aniqlay oladigan samarali CAD (Computer -aided Diagnosis - Kompyuterli tashxis) tizimini loyihalashda alomatlarni tanlash uchun yangi ikki tomonlama chegaraga asoslangan aqlli suv tomchilari IWD algoritmi taklif qilingan [17].

IWD algoritmini tibbiy tashxis qo'yish masalalariga qo'llash maqsadida quyidagicha moslashtirishni amalga oshiramiz. Ushbu algoritmi tibbiy tashxislashda kasalliklar bilan bog'liq optimal parametrlarni yoki alomatlarni aniqlash uchun ham qo'llaniladi. Tibbiy tashxis qo'yish masalasi uchun IWD algoritmi modeli quyidagicha ko'rinishda bo'lishi mumkin:

1. Masala qo'yilishini shakllantirish: Bu bosqichda hal qilinishi kerak bo'lgan tibbiy tashxislash masalasi aniqlanadi. Masalan, bu bemorning alomatlariga ko'ra kasalliklarni tasniflash masalasi bo'lishi mumkin.
2. Grafni qurish: Alomatlar yoki parametrlarning barcha mumkin bo'lgan kombinatsiyalarini ifodalovchi graf



yaratiladi. Grafning har bir tuguni bitta kombinatsiyaga mos keladi.

3. Optimal yo'ni tanlash ehtimolligini hisoblash: Alomatlar yoki parametrlarning har bir kombinatsiyasini tanlash ehtimolligini hisoblaydigan evristik funktsiya aniqlanadi. Ushbu ehtimollik tanlangan kombinatsiyalarning ko'rinishiga qarab yangilanadigan tuproq miqdoriga asoslanadi.
4. Tomchilarni ishga tushirish: Grafidagi tasodifiy tugunda suv tomchilari ishga tushiriladi va ulardaga tuproq miqdorini yangilanib, har bir kombinatsiyaning sifati baholanadi hamda tomchilarning graf bo'ylab harakatlanishiga ruxsat beriladi.
5. Tomchilar harakati: Tomchilar harakatlanishni davom ettirish maqsadida tuproq miqdori va evristik funktsiyaga bog'liq ravishda, tanlash ehtimoli asosida keyingi tugunlardan birini tanlaydi. Binda joriy tugunga yaqin tugunning tanlanish ehtimoli yuqori bo'ladi.
6. Tuproq miqdorining yangilanishi: Har bir iteratsiyadan so'ng, tanlangan kombinatsiyalar ko'rinishiga qarab, graf qirrasidagi vazn (tuproq miqdori) yangilanadi.
7. Optimal kombinatsiyani tanlash va ishni yakunlash: Tuproq miqdorining yangilanishi va ko'chirilishi to'xtash shartiga erishilgunga qadar bir necha marta takrorlanadi. So'ngra tuproq miqdori va evristik funktsiyaga asoslangan alomatlar yoki parametrlarning optimal kombinatsiyasi tanlanadi.

Natijalar. IWD algoritmi asosida ishlaydigan dasturdan natijalar olish uchun ushbu <https://www.kaggle.com/code/thakursankalp/detecting-cardiac-ailments-ml-w-ecg-data> saytidan olingan tanlanma faylidan foydalanamiz. Berilganlar to'plami yurak qon-tomir kasalliklari (YuQTK) tashxisi qo'yilgan bemorlarning 1160 ta yozuvlaridan iborat bo'lib, yozuvlar bemorlarga qo'yilgan tashxislarga ko'ra 4 ta guruhga ajratilgan, ya'ni ARR-aritmiya (1-290), AFF-atrial fibrilatsiya (291-580), CHF - konjestif

yurak etishmovchiligi (581-870) va NSR - Oddiy sinus ritmi (871-1160). Ma'lumotlar MIT-BIH fiziologik tarmoq ma'lumotlar bazasiga asoslangan. Shunday qilib, faylda 1160 x 36 o'lchamdagi yozuvlar mavjud. 1-ustunda yozuvlarning tartib nomeri, 36-ustunda esa kasallik turi aks etgan. Qolgan ustunlar alomatlar bo'lib, ular turli tekshiruv natijalari hisoblanadi [18].

IWD algoritmi asosida tuzilgan dasturiy vositadan foydalanib bemor haqidagi ma'lumotlarga ko'ra uning tashxisi qaysi kasallik turiga yaqin ekanligini aniqlash mumkin bo'ladi. Buning uchun yuqorida keltirilgan berilganlar bazasini kompyuterga trening qilish kerak bo'ladi. Misol tariqasida yuqorida tavsifi keltirilgan tanlanma faylini kompyuterga o'rgatish hamda yangi bemor haqidagi ma'lumotni shu tanlanma fayli asosida qaysi kasallikka yaqin ekanligini aniqlashni ko'rib chiqamiz. Yuqoridagi tavsifga ega tanlanma fayli ma'lumotlari dasturga uzatilganda va tomchilar soni 100 ga, iteratsiyalar soni 150 ga teng bo'lgan hol uchun quyidagi natijalar olindi:

Tanlangan obyekt	Obyektning tegishlilik diapazoni	Shifokorlar tomonidan qo'yilgan tashxis	Dastur tomonidan aniqlangan obyektlar
11	1-290	Aritmiya	9, 14, 56, 23, 7, 89
299	291-580	Atrial fibrilatsiya	322, 456, 296, 432, 561, 301
721	581-870	Konjestif yurak yetishmovchiligi	602, 656, 860, 722, 782, 598
987	870-1160	Oddiy sinus ritmi	988, 896, 1006, 1143, 1098, 907

1-jadval. IWD algoritmi natijalari

1-jadvalda tanlanmadan olingan, har bir guruhida 290 tadan obyekt mavjud bo'lgan 4 xil turdagi yurak qon tomir kasalliklari aniqlangan bemorlarning tartib raqami, ularning kasalliklarga guruhiga tegishlilik diapazoni, tanlangan bemorga shifokorlar tomonidan qo'yilgan tashxislar va IWD algoritmi asosida ishlovchi dasturdan foydalanib bemorlar holati bo'yicha to'plangan ma'lumotlarga ko'ra olingan natijalar aks ettirilgan. Masalan, 11-obyekt uchun shifokorlar tomonidan Aritmiya tashxisi qo'yilgan, uning tanlanmadagi aritmiya tashxisi qo'yilgan guruhga tegishlilik dastur tomonidan aniqlanishi kerak bo'lsin. Jadvaldan ko'rinib turibdiki, IWD algoritmi asosida ishlovchi dastur tanlangan obyektning haqiqatdan ham shu guruhga tegishlilikini ko'rsatadi. Jadvalning qolgan satrlaridagi ma'lumotlar



uchun ham xuddi yuqoridagi kabi fikrlarni aytish mumkin.

№	Algoritm	Tanlangan obyekt	Sarflangan vaqt (sekund)	Masofa	Tanlangan obyektga yaqin obyektlar
1	Ant	11	150	133887.01	110, 231, 98, 7, 89, 124
2	IWD	11	90	120478,23	9, 14, 56, 23, 7, 56

2-jadval. Algoritmning ishlashini taqqoslash natijalari

Yuqorida keltirilgan 2-jadvaldan ko'rinadiki, IWD algoritmi Ant algoritmiga nisbatan 60 sekund kam vaqt sarflagan, shu bilan birga u Ant algoritmiga nisbatan qisqaroq masofani topa olgan.

Xulosa. IWD algoritmi asosida olingan natijalar YuQTK ga tashxis qo'yish aniqligini oshirishi va tibbiy amaliyotda ko'proq asosli qarorlar qabul qilishga yordam berishi kutiladi. Shuningdek IWD algoritmining tashxislash tizimlarida qo'llanilishi yurak-qon tomir kasalliklarini davolash va rivojlanishining erta oldini olish uchun o'z vaqtida choralar ko'rish imkonini beradi. IWD algoritmidan foydalanib, nafaqat tashxislarni aniqlashtirish, balki tavsiya etiladigan dori darmonlar tarkibini va muolaja turlarini ham shakllantirish imkoniyati mavjud. Tibbiyot sohasida bu kabi imkoniyatlar yaxshi natijalar berishini ko'rsatadi.

Olingan natijalar IWD ning tibbiy tashxis qo'yish masalalariga samarali qo'llash mumkin ekanligini ko'rsatadi. Algoritm optimal alomatlarni tanlash, model parametrlarini optimallashtirish va bemorlarni tasniflash uchun muvaffaqiyatli qo'llanildi. Chumoli algoritmi bilan bajarilgan qiyosiy tahlil shuni ko'rsatdiki, IWD boshqa optimallashtirish algoritmlariga nisbatan yuqori samaradorlik va aniqlikka ega.

Xulosa qilib aytganda, ushbu tadqiqot natijalari tibbiy tashxislashda intellektual suv tomchilari algoritmini qo'llashni qo'llab-quvvatlaydi. Ushbu ish kasalliklarni erta aniqlashning yanada aniq va samarali usullarini taqdim etish va optimal davolash yechimlarini ishlab chiqish orqali tibbiy tashxislash sohasini rivojlantirishga yordam beradi.

Adabiyotlar

1. Клычева, Ф. (2024). Применение интеллектуальных технологий в диагностике сердечно-сосудистых заболеваний. *Scientific Collection «InterConf»*, (187), 356–359.
2. Клычева, Ф., Мухаммедиева, Д., & Эшбоев, Э. (2024). Применение искусственных иммунных систем в задачах медицинской диагностики. *Научный сборник «ИнтерКонф»*, (196), 380-384.
3. Klicheva F.G., Eshboyev E.A. (2023) CREATION OF AN INTELLIGENT SYSTEM TO SUPPORT MEDICAL DIAGNOSIS. *Innovative technologica -methodical research journal*. Volume 4, Issue 5 May 2023, 82-87.
4. Shah-Hosseini, H. (2007) 'Problem solving by intelligent water drops', *Proc. IEEE Congress on Evolutionary Computation*, Swisotel The Stamford, Singapore, September, pp.3226–3231.
5. Shah-Hosseini, H. (2008) 'Intelligent water drops algorithm: a new optimization method for solving the multiple knapsack problem', *Int. Journal of Intelligent Computing and Cybernetics*, Vol. 1, No. 2, pp.193–212.
6. Shah-Hosseini, H. (2009). The intelligent water drops algorithm: a nature-inspired swarm-based optimization algorithm. *Int. J. Bio Inspired Comput.*, 1, 71-79.
7. Kalita, Dhruva & Singh, Vibhav & Kumar, Vinay. (2022). Two-way threshold-based intelligent water drops feature selection algorithm for accurate detection of breast cancer. *Soft Computing*. 26. 10.1007/s00500-021-06498-3.
8. Lenin, K. and Kalavathi, M. S. 2012. 2012, "An Intelligent Water Drop Algorithm for Solving Optimal Reactive Power Dispatch Problem". *International Journal on Elect. Engineering and Inform.* 4, 450-463.
9. Msallam, M. M. and Hamdan, M. 2011, Improved intelligent water drops algorithm using adaptive schema. *International Journal of Bio-Inspired Computation*, 3(2), 103-111.
10. Rayapudi, S. R. 2011, "An intelligent water drop algorithm for solving economic load dispatch problem". *International Journal of Electrical and Electron Eng.* 5, 43-49.



11. Эшбоев, Э. А., & Клычева, Ф. Г. (2018). ИСПОЛЬЗОВАНИЕ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ ЗНАЧЕНИЙ ПРИ ПОСТРОЕНИИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ ЗДОРОВЬЯ НАСЕЛЕНИЯ. In *Перспективные информационные технологии (ПИТ 2018)* (pp. 759-762).
12. Eshboeyev E., Klicheva F. (2022) Yuqori qon bosimiga ega bo‘lgan shaxslarning intellektual tahlilini amalga oshirish. " //FAN VA JAMIYAT" jurnali. Ajiniyoz nomidagi NDPI. – 2022. – №. 3. – С. 122-123.
13. Клычева, Ф. Г., Эшбоев, Э. А., & Равшанов, Д. Г. (2022). РЕАЛИЗАЦИЯ ПРОГНОЗИРОВАНИЯ СЕРДЕЧНО-СОСУДИСТЫХ ЗАБОЛЕВАНИЙ С ИСПОЛЬЗОВАНИЕМ ПРИЗНАКОВ И ЛИНЕЙНОЙ РЕГРЕССИИ. *Universum: технические науки*, (8-1 (101)), 14-17.
14. M. Dorigo, *Optimization, Learning and Natural Algorithms*, PhD thesis, Politecnico di Milano, Italie, 1992.
15. Rayapudi, S. R. 2011, “An intelligent water drop algorithm for solving economic load dispatch problem”. *International Journal of Electrical and Electron Eng.* **5**, 43-49.
16. Lenin, K. and Kalavathi, M. S. 2012. 2012, “An Intelligent Water Drop Algorithm for Solving Optimal Reactive Power Dispatch Problem”. *International Journal on Elect. Engineering and Inform.* **4**, 450-463.
17. Kalita, Dhruva & Singh, Vibhav & Kumar, Vinay. (2022). Two-way threshold-based intelligent water drops feature selection algorithm for accurate detection of breast cancer. *Soft Computing*. 26. 10.1007/s00500-021-06498-3 p. 18-23.
18. Klicheva F. 2023. CHUMOLI ALGORITMINI YURAK-QON TOMIR KASALLIKLARIGA TASHHIS QO‘YISHGA TATBIQ ETISH. *DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE*. 1, 4 (Dec. 2023), 156–159 b.



Mashinaviy o'qitish asosida yo'llardagi avtomobil tirbandlik holatlarini aniqlash uchun dastlabki ma'lumotlarni tayyorlash usullari

Axatov Akmal Rustamovich
texnika fanlari doktori, professor,
Samarqand davlat universiteti prorektori
akmalar74@gmail.com

Eshtemirov Bunyod Sherali o'g'li
Samarqand davlat universiteti tayanch doktoranti
eshtemirov23@gmail.com

Annotatsiya. Yo'llardagi tirbandlik holatlarini bashorat qilish, zamonaviy shaharlarda transport tizimlarini samarali boshqarish va harakatlanish qulayligini ta'minlashda muhim rol o'ynaydi. Ushbu jarayonni amalga oshirishda intellektual algoritmlar va sun'iy intellekt texnologiyalari keng qo'llanilmoqda. Bu texnologiyalar yo'l-transport hodisalarini oldindan aniqlash va oldini olish, shuningdek, transport oqimini optimal boshqarish imkonini beradi. Ushbu tadqiqot ishida ham yo'llardagi transport vositalari harakati haqidagi ma'lumotlar yig'ildi. Yig'ilgan ma'lumotlar tozalandi va tayyorlandi. Xususiyatlarni tanlash va muhimligini aniqlash uchun har bir ko'rsatkichning tirbandlik holatiga ta'siri tahlil qilindi. Shundan so'ng mashinaviy o'qitish algoritmlari, masalan, XGBoost, Random Forest Classifier, LGBMClassifier, Logistic Regression va chuqur o'qitish modellari yaratildi. Ushbu modellar yig'ilgan ma'lumotlar asosida o'qitildi. Modelni tekshirish va baholash uchun yaratilgan modelning aniqligi va samaradorligi test ma'lumotlar to'plami yordamida tekshirildi. Modelning bashorat qilish qobiliyati turli metrikalar yordamida baholandi, masalan, Accuracy, Recall, Precision va F1 Score. O'rganilgan model yordamida yo'llardagi tirbandlik holatlarini bashorat qilish amalga oshirildi. Bu bashoratlar transport tizimini boshqarish uchun sinovdan o'tkazildi.

Kalit so'zlar: intellektual algoritmlar, ma'lumotlar yig'ish usullari, modelning bashorat qilish qobiliyatini baholash, parametrlar orasidagi bog'liqliklarni o'rganish.

I. Kirish

Zamonaviy shaharlarda yo'l harakati boshqaruvi dolzarb muammolardan biri hisoblanadi. Har kuni millionlab avtomobillar va transport vositalari yo'llarda harakatlanadi, bu esa ko'pincha tirbandliklarga olib keladi [1]. Tirbandliklar nafaqat haydovchilar va yo'lovchilar uchun noqulaylik tug'diradi, balki iqtisodiy zararlarga, ekologik muammolarga va yo'l-transport hodisalariga ham sabab bo'ladi. Shahar infratuzilmasini samarali boshqarish uchun yo'llardagi tirbandlik holatlarini oldindan bashorat qilish va tirbandliklarni boshqarish texnologiyalari muhim ahamiyatga ega bo'lib, bu jarayonda intellektual algoritmlar va sun'iy intellekt texnologiyalari muhim rol o'ynaydi [2]. Yo'llardagi tirbandlik holatlarini bashorat qilishda intellektual algoritmlar va sun'iy intellekt texnologiyalari,

xususan, mashinaviy o'qitish va chuqur o'qitish usullaridan keng foydalaniladi. Bu usullar katta hajmdagi ma'lumotlarni tahlil qilish, xususiyatlarini o'rganish va bashorat qilishda keng qo'llaniladi. Bunday algoritmlar yuqori aniqlik va samaradorlikka ega bo'lib, transport tizimlarini boshqarish va optimallashtirishda muhim vositadir. Yo'llardagi tirbandlik holatini bashorat qilish uchun avvalo kerakli ma'lumotlarni yig'ish zarur. Yig'ilgan ma'lumotlar avval tozalanib, so'ngra tayyorlanadi. Ma'lumotlar yig'ilgandan so'ng, har bir ko'rsatkichning tirbandlik holatiga ta'sirini tahlil qilish zarur. Bu bosqichda ma'lumotlar orasidagi bog'liqliklar aniqlanadi. Masalan, Pearson, Spearman, va Kendall Tau koeffitsiyentlari yordamida ko'rsatkichlar orasidagi bog'liqliklarni o'rganish mumkin [3]. Keyingi bosqichda mashinaviy o'qitish algoritmlari yordamida



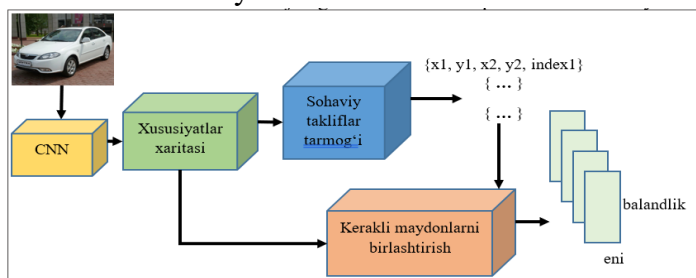
model yaratish va o'qitish kerak bo'ladi. Bu algoritmlar orasida chiziqli regressiya, qaror daraxtlari, tasodifiy o'rmonlar, gradient boosting, XGBoost va chuqur o'rganish modellari mavjud. Yaratilgan modelning aniqligi va samaradorligi test ma'lumotlar to'plami yordamida tekshiriladi. Bu bosqichda modelning bashorat qilish qobiliyati turli aniqlikni baholovchi usullar yordamida baholanadi. Masalan, Accuracy, Recall, Precision va F1 Score kabi metrikalari modelning aniqligini o'lchashda qo'llaniladi. Ushbu metrikalar yordamida modelning yutuqlari va kamchiliklari aniqlanadi, hamda kerak bo'lsa, modelni yaxshilash choralari ko'riladi [4].

II. Video tasvirlar orqali yo'llarning holati haqida ma'lumotlar yig'ish

Yo'llarda joylashtirilgan kameralar yo'l harakatini doimiy ravishda kuzatib boorish va yo'l haqida ma'lumotlar yig'ish imkonini beradi. Ushbu kameralar yuqori aniqlikdagi video tasvirlarni yozib oladi va real vaqt rejimida markaziy tizimlarga uzatadi. Bu ma'lumotlarni video tasvirli ma'lumotlardan olishda kompyuterli ko'rish texnologiyalari qo'llaniladi [5]. Ulardan bir qancha ko'p foydalaniladigan usullar quyidagilar:

- Faster R-CNN;
- SSD (Single Shot MultiBox Detector);
- YOLO (You Only Look Once).

Faster R-CNN. Faster R-CNN (Region-based Convolutional Neural Network) obyektlarni aniqlashda eng samarali va keng qo'llaniladigan algoritmlardan biridir [6]. Bu model R-CNN va Fast R-CNN modellari asosida rivojlangan va ancha tezroq ishlashni ta'minlaydi.



1-rasm. Faster R-CNN obyektlarni tanib olish modelining ishlash prinsipi.

Faster R-CNN modeli uch bosqichda ishlaydi:

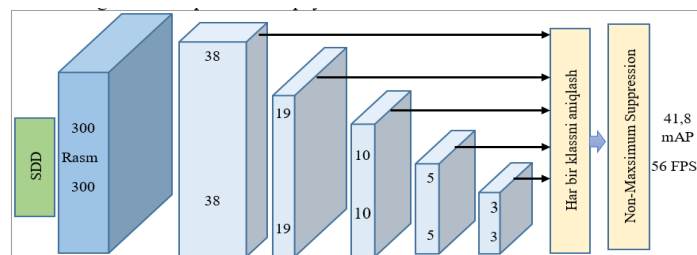
Region Proposal Network (RPN): Bu bosqichda model tasvir ichidagi obyektlarni aniqlash

mumkin bo'lgan hududlarga ajratadi. RPN konvolyutsion neyron tarmoq (CNN) ustida joylashgan bo'lib, u olingan xarita ustida harakatlanadi va har bir pozitsiyada anchor deb nomlangan qutilarni joylashtiradi. RPN har bir anchor uchun ehtimoliy obyekt yoki fon ekanligini aniqlash va chegaralash qutisini (bounding box) tuzatish koeffitsiyentlarini hisoblash uchun ishlatiladi [7].

Region of Interest (RoI) Pooling: Ajratib olingan hududlar (RoI) RPNdan olingan xaritada aniqlanadi va RoI pooling orqali aniqlashtiriladi. Bu bosqichda har bir RoIni teng o'lchamdagi xaritaga o'lchash orqali har xil o'lchamdagi RoI larni yagona o'lchamdagi xaritaga aylantiradi.

Classifier and Bounding Box Regressor: RoI poolingdan so'ng olingan xaritalar neyron tarmoq orqali o'tkaziladi. Bu bosqichda har bir RoI uchun aniqlangan obyektning klassifikatsiyasi (obyektning turi) va uning aniqlash bounding box (chegaralash qutisi) tuzatishlari aniqlanadi [8].

SSD (Single Shot MultiBox Detector). SSD (Single Shot MultiBox Detector) obyektlarni aniqlashda samaradorlik va aniqlikni oshirish maqsadida ishlab chiqilgan yondashuvlardan biridir. Bu model real vaqt rejimida obyektlarni aniqlash imkonini beradi va Faster R-CNN kabi boshqa ilg'or usullarga nisbatan tezroq ishlaydi. SSD modeli tasvirlarni bir marta (single shot) ishlash orqali obyektlarni aniqlash imkonini beradi [9]. Bu model konvolyutsion neyron tarmoqlari (CNN) asosida ishlaydi va butun tasvirni bir marta ishlash orqali bir nechta chegaralovchi qutilarni aniqlaydi.



2-rasm. SSD obyektlarni tanib olish modelining arxitekturasi.

Feature Extraction (Xususiyatlarni ajratish): Asosiy konvolyutsion tarmoq (masalan, VGG16 yoki ResNet) tasvirdagi xususiyatlarni ajratadi. Bu tarmoq



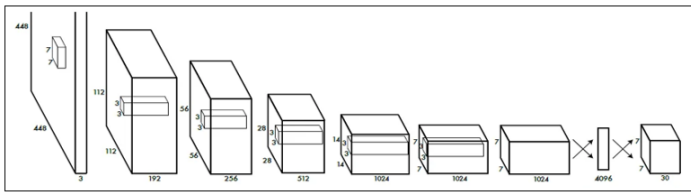
tasvirni bir necha qatlamlar orqali o'tkazib, har bir qatlamda xususiyat xaritalarini hosil qiladi.

Multi-scale Feature Maps (Ko'p o'lchovli xususiyat xaritalari): SSD modeli bir nechta konvolyutsion qatlamlardan xususiyat xaritalarini oladi. Har bir qatlam turli o'lchovlarda xususiyatlarni ajratadi, bu esa turli o'lchamdagi obyektlarni aniqlash imkonini beradi [10].

Default Boxes (Standart qutilar): Har bir xususiyat xaritasidagi pozitsiya uchun bir nechta standart qutilar (default boxes) aniqlanadi. Ushbu qutilar turli o'lchamlar va aspekt nisbati bilan aniqlanadi, bu esa modelga turli xil obyektlarni aniqlash imkonini beradi.

Bounding Box Regression va Class Prediction: Har bir standart quti uchun SSD modelining konvolyutsion qatlamlari bounding box koordinatalarini (chegaralash qutisi koordinatalari) va obyekt sinfini (class prediction) aniqlaydi. Bu qutilar keyinchalik aniqlangan obyektlar bilan birga optimallashtiriladi.

YOLO (You Only Look Once). YOLO (You Only Look Once) obyektini aniqlash modeli, faqat bir marta qarash orqali obyektlarni aniqlashga imkon beruvchi tez va samarali algoritmdir. Ushbu yondashuv Joseph Redmon va boshqalar tomonidan 2016 yilda taqdim etilgan va real vaqt rejimida obyektlarni aniqlash imkonini beradi. YOLO modeli tasvirni bir marta tahlil qilib, undagi obyektlarni aniqlaydi [11].



3-rasm. YOLO obyektlarni tanib olish modelining axitekturasini.

Bu yondashuv tasvirni kichik gridlarga bo'lish va har bir grid uchun chegaralash qutilari va obyekt klassifikatsiyasini hisoblash orqali amalga oshiriladi.

Tasvirni gridlarga bo'lish: Tasvir DxD o'lchamdagi gridlarga bo'linadi. Har bir grid hujayrasi tasvirning kichik bir qismiga mos keladi.

Bounding boxlarni aniqlash: Har bir grid hujayrasi uchun bir nechta bounding boxlar aniqlanadi.

Har bir bounding box uchun markaz koordinatalari, kengligi, balandligi va ishonch koeffitsiyenti (confidence score) hisoblanadi [12].

Obyekt klassifikatsiyasi: Har bir grid hujayrasi uchun obyekt klassifikatsiyasi amalga oshiriladi. Bu klassifikatsiya har bir chegaralash qutisi uchun qaysi obyekt turi mavjudligini aniqlaydi.

Yagona model: YOLO modeli barchani birlashtiradi va bir vaqtning o'zida chegaralash qutilarini va obyekt klassifikatsiyasini aniqlaydi. Bu yondashuv modeli juda tez va samarali qiladi.

YOLO obyektlarni aniqlashda tezlik va samaradorlikni oshirish uchun ishlab chiqilgan ilg'or modeldir. Ushbu modelning ishlash prinsipi va arxitekturasi uni real vaqt rejimida obyektlarni aniqlashda juda samarali qiladi. YOLO modeli transport tizimlari, xavfsizlik tizimlari va boshqa ko'plab sohalarda keng qo'llaniladi [13].

Yuqorida keltirilgan obyektlarni tanib olish modellari bugungi kunda o'zlarining imkoniyatlarini kengaytirib bormoqda.

YOLO & Faster R-CNN va SSD. Obyektlarni tanib olish modellarining qaysi biridan foydalangan yaxshi degan savolga javob berish mushkul. Sababi har bir model holatdan kelib chiqib ustunliklarga ega. Odatda bu kabi obyektlarni tanib olish modellari ishlash tezligi (FPS) va ishlash aniqligi bo'yicha taqqoslanadi [14]. Masalan, YOLO, Faster R-CNN va SSD tasvirlardan obyektlarni tanib olish modellari qaralganda, ularning ishlash tezligi va tanib olish aniqligiga nisbatan solishtirilganda 4-rasmdagi kabi natijalar olindi.

Model	mAP %	FPS	Tezlik	Aniqlik
YOLO	18,6	295	Juda tez	O'rtacha
Faster R-CNN	41,8	17	Sekin	Yuqori
SSD	31,2	56	Tez	Yuqori

4-rasm. YOLO, Faster R-CNN va SSD obyektlarni tanib olish modellarining ishlash tezligi va aniqligi.

Bunda YOLO, Faster R-CNN va SSD modellarini baholash hamda taqqoslash uchun biz



NVIDIA V100 SXM2 16GB GPU yordamida 100 mingta test ma'lumotlar to'plamida FPS va mAPi o'Ichandi. 4-rasmda keltirilgan taqqoslashlarni 5-rasm, 6-rasm va 7-rasmdan ham ko'rish mumkin.



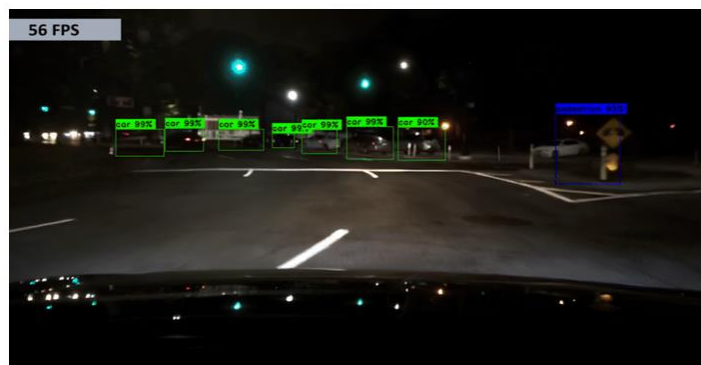
5-rasm. YOLO obyektlarni tanib olish modelining ishlash tezligi va aniqligi.

Haqiqatan ham 5-rasmdan ko'rinib turibdiki, YOLO modelining ishlash tezligi Faster R-CNN va SSD modellariga qaraganda mos ravishta o'rtacha 17 va 5 barobar tez ishlashini ko'rsatdi. Shuning uchun YOLO obyektlarni tanib olish modelidan real vaqt rejimidagi tadqiqotlarda foydalanish tavsiya etiladi.



6-rasm. Faster R-CNN obyektlarni tanib olish modelining ishlash tezligi va aniqligi.

Obyektlarni tanib olishdagi aniqlik bo'yicha Faster R-CNN YOLO va SSD modellariga qaraganda mos ravishta o'rtacha 2 va 1.3 marta yaxshiroq natija qayt etganini ko'rish mumkin.



7-rasm. SSD obyektlarni tanib olish modelining ishlash tezligi va aniqligi.

SDD obyektlarni tanib olish modeli esa qolgan modellarga qaraganda obyektlarni tanib olish tezligi va aniqlikda o'rtacha natija qayt etgan. Xulosa shundan iboratki, agar qaraliyotgan jarayonda obyektlarni tanib olish tezligi muhim bo'lsa YOLO modelidan, obyektlarni yuqori aniqlikda tanib olish muhim bo'lganda Faster R-CNNdan foydalangan afzal.

№	Sana	Hafta kuni	Mashina soni	Motosikl soni	Avtobus soni	Yukmashina soni	Umumiy soni	Soat	Minut	Tirbandlik holati
0	9	Juma	17	2	1	35	55	21	45	1
1	9	Juma	12	0	1	31	44	21	0	1
2	9	Juma	16	3	1	26	46	22	15	1
3	9	Juma	15	6	0	22	43	22	30	1
4	9	Juma	13	4	1	15	32	22	45	1
...

1-jadval. Yo'llardagi tirbandlik holatlarini bashorat qilishda ma'lumotlar orasidagi o'zaro bog'liqlik koeffitsiyentlarini aniqlash

Ushbu tadqiqot ishida yo'llardagi tirbandlik holatlarini Hafta kuni, Mashina soni, Motosikl soni, Avtobus soni, Yukmashina soni, Umumiy soni, Soat, Minut va PM/AM parametrlari bo'yicha bashorat qilish qarab o'tilgan [15]. Dastlab 1-jadvaldagi Tirbandlik holati parametriga qolgan parametrlarning bog'liqlik koeffitsiyentini hisoblab chiqish talab qilinadi. Ushbu bog'liqlik yo'llardagi tirbandlik holatlarini bashorat qilish o'sha parametrning qanchalik muhimligini bildiradi, agar bog'liqlik koeffitsiyenti past bo'lsa shu parametrni tashlab yuborishimiz mumkin bo'ladi.

III. Yo'llardagi tirbandlik holatlarini bashorat qilishda ma'lumotlar orasidagi o'zaro bog'liqlik koeffitsiyentlarini aniqlash

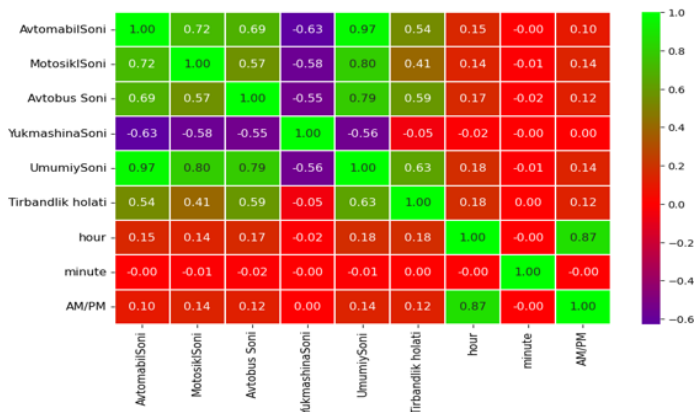


Yo'llardagi tirbandlik holatlarini bashorat qilishda ma'lumotlar orasidagi o'zaro bog'liqlik koeffitsiyentlarini aniqlash uchun uchta asosiy formulani ishlatish mumkin: Pearson, Spearman va Kendall Tau koeffitsiyentlari. Har bir koeffitsiyent turli xil sharoitlarda va turli xil ma'lumot turlarida foydalaniladi [16].

Pearson korrelyatsiya koeffitsiyenti. Pearson koeffitsiyenti ikki o'zgaruvchi orasidagi chiziqli bog'liqlikni o'lchaydi. Bu koeffitsiyentlar 1 va -1 oralig'ida bo'lib, 1 mukammal musbat bog'lanishni, -1 mukammal manfiy bog'lanishni, 0 esa bog'lanish yo'qligini bildiradi.

$$e = \frac{m \sum zt - (\sum z)(\sum t)}{\sqrt{[m \sum z^2 - (\sum z)^2][m \sum t^2 - (\sum t)^2]}} \quad (1)$$

bunda e - x va y o'zgaruvchilarining o'zaro bog'liqlik koeffitsiyenti; n - x va y o'zgaruvchilar juftliklari soni; Ushbu (1) formula bo'yicha tadqiqotda to'plangan ma'lumotlarning o'zaro bog'liqlik koeffitsiyenti 8-rasmda keltirilgan.



8-rasm. Tadqiqotda foydalanilayotgan ma'lumotlarning Pearson formulasi bo'yicha o'zaro bog'liqlik koeffitsiyenti Heatmap grafigi.

Ushbu matritsa har bir ustun orasidagi Pearson korrelyatsiya koeffitsiyentlarini o'z ichiga oladi.



9-rasm. Tadqiqotda foydalanilayotgan ma'lumotlarning Pearson formulasi bo'yicha o'zaro bog'liqlik koeffitsiyenti.

9-rasmdan ko'rish mumkinki, Tirbandlik holati parametri bilan Mashina soni, Motosikl soni, Avtobus soni va Umumiy soni parametrlari orasida mos ravishda 0.54, 0.41, 0.59 va 0.63 qiymatlar bilan kuchli, Yukmashina soni (0.05), Soat (0.18), Minut (0) va AM/PM (0.12) kabi parametrlarga kuchsiz bog'langanligini ko'rish mumkin.

Kendall Tau korrelyatsiya koeffitsiyenti. Kendall Tau koeffitsiyenti ikkita o'zgaruvchilar orasidagi tartibli bog'liqlikni o'lchaydi. Bu koeffitsiyent ham -1 va 1 oralig'ida qiymat oladi.

x va y o'zgaruvchilarning Kendall formulasi bo'yicha o'zaro bog'liqlik koeffitsiyenti quyidagi (2) formula orqali topiladi:

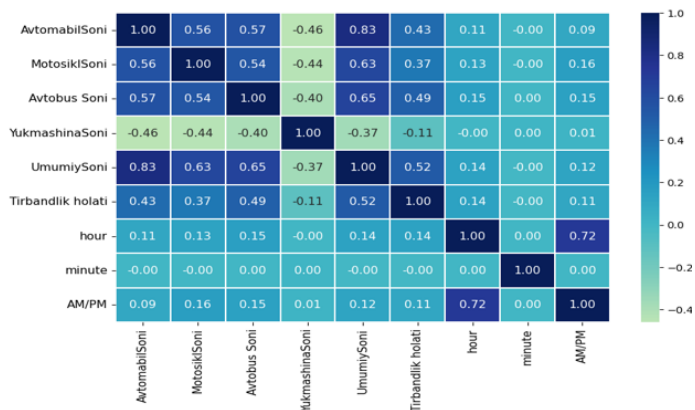
$$\eta = 2 \times \frac{L - K}{p \times (p - 1)} \quad (2)$$

bunda L - (x_i, y_i) va (x_j, y_j) uchun (2.3.3) shartni qanoatlantiruvchi juftliklar soni; K - (3) shartni qanoatlantirmaydigan juftliklar soni.

$$[(x_i < x_j) \vee (y_i < y_j)] \text{ yoki } [(x_i > x_j) \vee (y_i > y_j)] \quad (3)$$

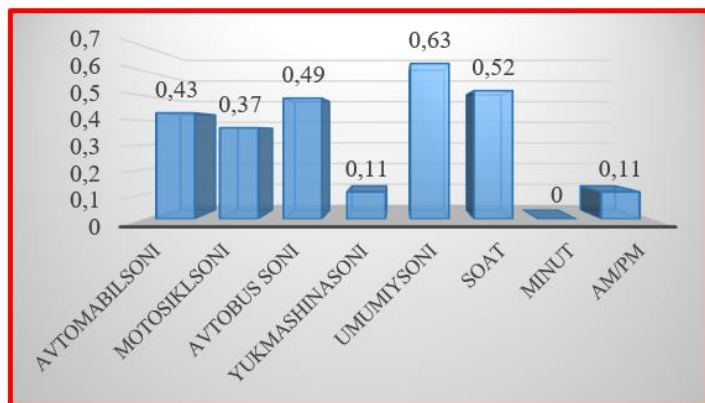
bu yerda $i < j$ va $i, j = 1 \dots n$. Ushbu (2) formula bo'yicha tadqiqotda to'plangan ma'lumotlarning o'zaro bog'liqlik koeffitsiyenti 10-rasmda keltirilgan.





10-rasm. Tadqiqotda foydalanilayotgan ma'lumotlarning Kendall Tau formulasi bo'yicha o'zaro bog'liqlilik koeffitsiyenti Heatmap grafi.

Ushbu matritsa har bir ustun orasidagi Kendall Tau korrelyatsiya koeffitsiyentlarini o'z ichiga oladi.



11-rasm. Tadqiqotda foydalanilayotgan ma'lumotlarning Kendall Tau formulasi bo'yicha o'zaro bog'liqlilik koeffitsiyenti.

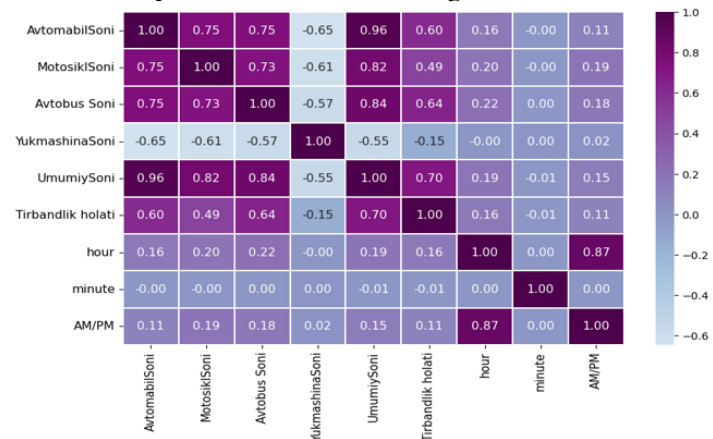
11-rasmdan ko'rish mumkinki, Tirbandlik holati parametri bilan Mashina soni, Motosikl soni, Avtobus soni va Umumiy soni parametrlari orasida mos ravishda 0.43, 0.37, 0.49 va 0.52 qiymatlar bilan kuchli, Yukmashina soni (0.11), Soat (0.14), Minut (0) va AM/PM (0.11) kabi parametrlarga kuchsiz bog'langanligini ko'rish mumkin.

Spearman korrelyatsiya koeffitsiyenti. Spearman koeffitsiyenti ikkita o'zgaruvchilar orasidagi monotoniya bog'liqligini o'lchaydi [17]. Bu koeffitsient ham -1 va 1 oralig'ida qiymat oladi, bu yerda 1 mukammal monotoniya musbat bog'liqlikni, -1 mukammal monotoniya manfiy bog'liqlikni va 0 bog'liqlik yo'qligini bildiradi.

x va y o'zgaruvchilarning Spearman formulasi bo'yicha o'zaro bog'liqlilik koeffitsiyenti quyidagi (2.3.3) formula orqali topiladi.

$$t_r = 1 - \frac{6 \sum p_i^2}{b^3 - b} \quad (4)$$

bunda $t_i = x_i - y_i$. Ushbu (4) formula bo'yicha tadqiqotda to'plangan ma'lumotlarning o'zaro bog'liqlilik koeffitsiyentlari 12-rasmda keltirilgan.



12-rasm. Tadqiqotda foydalanilayotgan ma'lumotlar va vaqt ko'rsatkichining Spearman o'zaro bog'liqlilik koeffitsiyenti Heatmap grafi.

Ushbu matritsa har bir ustun orasidagi Spearman korrelyatsiya koeffitsiyentlarini o'z ichiga oladi.



13-rasm. Tadqiqotda foydalanilayotgan ma'lumotlar va vaqt ko'rsatkichining Spearman o'zaro bog'liqlilik koeffitsiyenti.

13-rasmdan ko'rish mumkinki, Tirbandlik holati parametri bilan Mashina soni, Motosikl soni, Avtobus soni va Umumiy soni parametrlari orasida mos ravishda 0.60, 0.49, 0.64 va 0.70 qiymatlar bilan kuchli, Yukmashina soni (0.15), Soat (0.16), Minut



(0.01) va AM/PM (0.11) kabi parametrlarga kuchsiz bog'langanligini ko'rish mumkin.

Mashinaviy o'qitish algoritmlari asosida yo'llardagi tirbandlikni bashorat qilish algoritmi

Yo'llardagi tirbandlik holatlarini bashorat qilishga oid dastlabki ma'lumotlar to'plamini mashinaviy o'qitishga tayyorlash va bashoratlashda quyidagi jarayonlar amalga oshiriladi. Bu jarayon modelni o'rgatish va baholash uchun muhimdir. Toza va aniqlikni oshiruvchi ma'lumotlar to'plamini yaratish. Bunga yo'qolgan qiymatlar bilan ishlash (to'ldirish, o'chirish), noto'g'ri qiymatlar bilan ishlash (aniqlash, tuzatish va o'chirish), **duplikat qatorlarni aniqlash va o'chirish**, ma'lumotlarni qayta ishlash (xususiyatlarni tanlash, kategorik ma'lumotlarni raqamli ma'lumotlarga aylantirish, ma'lumotlarni normalizatsiya qilish yoki standartlashtirish) **kabilarni misol qilib olish mumkin [18]**.

Bu algoritmi yo'llardagi tirbandlikni bashorat qilish uchun algoritmnining bosqichlari keltirilgan. Bu bosqichlar quyidagi jarayonlarini o'z ichiga oladi:

1.	dastlabki ma'lumotlarni to'plami	6.	ma'lumotlar to'plamini o'quv va test to'plamiga bo'lish
2.	kodlashtirish va korrelyatsiya tahlili	7.	regressiya modellarida o'qitish
3.	xususiyatlar tahlili	8.	modelni baholash
4.	NaN qiymatlarni to'ldirish	9.	tirbandlikni baholash
5.	ma'lumotlarni masshtablash	10.	yakuniy natijalarni chiqarish

Algoritmi optimal parametrlarni topish va modelning aniqligini oshirish uchun parametrlarni sozlaydi va baholaydi [12].

Natija

Yo'ldagi tirbandlik holatini bashoratlash tadqiqotida Kaggle tizimidagi ochiq ma'lumotlar to'plamlaridan biri bo'lgan "Traffic Prediction Dataset" ishlatildi. Bu to'plamda jami 2977 ta ma'lumot mavjud bo'lib, ular tajriba sinovlari uchun 80/20 nisbatda o'quv va test to'plamlariga ajratildi [18]. Ma'lumotlar bashoratlash modeliga yuborilishidan oldin, tadqiqot uchun muhim bo'lgan maydonlar aniqlanib, tayyorlandi. Tadqiqotning asosiy

maqsadi yo'llardagi tirbandlik holatining vaqtga bog'liqlik darajasini o'rganishdan iborat edi. Keyingi bosqichlarda tanlangan maydonlar asosida XGBoost, Random Forest Classifier, LGBMClassifier va Logistic Regression modellarida o'qitildi va testdan o'tkazildi. Bu sun'iy intellekt modellarini baholashda Accuracy, Recall, Precision va F1 Score kabi metrikalardan foydalanildi [19]. Tadqiqot natijalari esa 2-jadvalda keltirildi.

№	Mashinaviy o'qitish algoritmi	Algoritmi baholash ko'rsatkichlari			
		Accuracy	Recall	Precision	F1 Score
1	XGBoost	1	1	1	1
2	Random Forest Classifier	1	1	1	1
3	LGBMClassifier	1	1	1	1
4	Logistic Regression	0.994	0.997	0.995	0.996

2-jadval. Yo'llardagi tirbandlikni baholashda foydalanilgan sun'iy intellekt modellari natijalari

Yuqoridagi 2-jadvaldan ko'rish mumkinki, tadqiqotda taklif etilayotgan XGBoost algoritmi Random Forest Classifier, Logistic Regression va LGBMClassifier algoritmlariga qaraganda yuqoriroq natija qayt etdi. Ushbu bo'limda XGBoost, Random Forest Classifier va LGBMClassifier algoritmlarining baholanish natijalari ko'rib chiqildi. Ushbu algoritmlar Accuracy, Recall, Precision va F1 Score yordamida baholandi. Umuman olganda, barcha algoritmlar yuqori natijalar ko'rsatdi, lekin XGBoost, Random Forest Classifier va LGBMClassifier algoritmlari eng yuqori aniqlik va samaradorlikni namoyish etdi. Logistic Regression algoritmi esa biroz kamroq bo'lsada, hali ham yuqori natijalarga erishdi. Bu algoritmlar yo'llardagi tirbandlik holatini bashorat qilishda samarali ekanligini ko'rsatadi.

XULOSA

Yo'llardagi tirbandlik holatlarini bashorat qilish va transport tizimlarini samarali boshqarish zamonaviy shaharlar uchun dolzarb masalalardan biridir. Ushbu tadqiqotda tirbandlikni oldindan ko'rish va bartaraf etish maqsadida intellektual algoritmlardan foydalanildi. Dastlab, video tasvirli ma'lumotlardan YOLO obyektini aniqlash modeli yordamida 2-rasmdagi ma'lumotlar to'plami yaratildi. Ushbu ma'lumotlar to'plami 80/20 nisbatda o'quv va test to'plamlariga ajratildi. Tadqiqotning asosiy maqsadi



yo'llardagi transport vositalarining tirbandlik holatlarini harakat ma'lumotlariga asoslanib bashoratlash edi [19]. Bunda AvtomobilSoni, MotosiklSoni, AvtobusSoni, YukmashinaSoni, UmumiySoni, Soat, Minut va AM/PM kabi parametrlar hisobga olindi. Tadqiqotning keyingi bosqichida sun'iy intellektning XGBoost, Random Forest Classifier va Logistic Regression kabi bashorat qilish algoritmlaridan foydalanildi. Ushbu algoritmlar yordamida yo'ldagi tirbandlik holati bashorat qilindi va natijalar Accuracy, Recall, Precision va F1 Score kabi baholash usullari yordamida tekshirildi. Yuqorida keltirilgan algoritmlarning barchasi baholash mezonlari bo'yicha yuqori natijalarni qayd etdi. Umuman olganda, barcha algoritmlar yuqori natijalar ko'rsatdi, lekin XGBoost, Random Forest Classifier va LGBMClassifier algoritmlari eng yuqori aniqlik hamda samaradorlikni namoyish etdi [20]. Ushbu algoritmlar transport boshqaruvi tizimlarini yaxshilash, yo'llardagi tirbandlikni kamaytirish va transport oqimini samarali boshqarish uchun muhim vosita bo'lib xizmat qiladi. Sun'iy intellekt algoritmlarining keng qo'llanilishi shahar transport tizimini optimallashtirish va haydovchilarga qulay sharoit yaratishda katta yordam beradi. Bu tadqiqot yo'ldagi tirbandlik holatlarini bashorat qilishda intellektual algoritmlarning imkoniyatlarini ko'rsatib berdi va kelajakda shahar infratuzilmasini rivojlantirishda katta hissa qo'shishi mumkinligini isbotladi.

Adabiyotlar

1. Lowe, D. G. (1999) Object recognition from local scale-invariant features. In Computer vision, 1999. The proceedings of the seventh IEEE international conference on, volume 2, pages 1150–1157. Ieee.
2. Akhatov A. R., Nazarov F., Eshtemirov B.Sh. "Detection and analysis of traffic jams using computer vision technologies", International Conference on Artificial Intelligence, Blockchain, Computing and Security (ICABCS-2023). Samarkand, Uzbekistan.
3. Axatov A. R., Eshtemirov B.Sh. "Mashinaviy o'qitish asosida yo'llardagi tirbandlik holatlarini tahlil qilishning intellektual algoritmlari" "Raqqamli transformatsiya va sun'iy intellekt",

Toshkent davlat iqtisodiyot universiteti, 2024-yil, Volume 2, Issue 3.

4. F.M.Nazarov, Eshtemirov B.Sh., Q.Sh.Saydullayev "Microscopic and macroscopic flow models of traffic management" // Sharof Rashidov nomidagi Samarqand davlat universiteti Ilmiy axborotnomasi. (283/7.1-son OAK qarori. №32), 2023-yil, 1-son (137/2).

5. J. Redmon and A. Angelova. Real-time grasp detection using convolutional neural networks. CoRR, abs/1412.3128, 2014.

6. Nannicini G. , "Point-to-point shortest paths on dynamic time-dependent road networks," 40R, vol. 8, pp. 327-330,2010.

7. S. Gidaris and N. Komodakis. Object detection via a multiregion & semantic segmentation-aware CNN model. CoRR, abs/1505.01749, 2015.

8. Akhatov A., Renavikar A., Rashidov A. & Nazarov F. "Development of the Big Data processing architecture based on distributed computing systems" Informatika va energetika muammolari O'zbekiston jurnali, № (1) 2022, 71-79

9. M. A. Sadeghi and D. Forsyth. 30hz object detection with dpm v5. In Computer Vision–ECCV 2014, pages 65–79. Springer, 2014.

10. Bolikulov, F.; Nasimov, R.; Rashidov, A.; Akhmedov, F.; Cho, Y.-I. Effective Methods of Categorical Data Encoding for Artificial Intelligence Algorithms. Mathematics 2024, 12, 2553. <https://doi.org/10.3390/math12162553>

11. J. Yan, Z. Lei, L. Wen, and S. Z. Li. The fastest deformable part model for object detection. In Computer Vision and Pattern Recognition (CVPR), 2014 IEEE Conference on, pages 2497–2504. IEEE, 2014. 5.

12. Siu Hong Loh, Jia Jia Sim, Chu Shen Ong, Kim Ho Yeap, "Development of Smart Traffic Light Controller System with Deep Learning Capability in Image Processing", 2021.

13. Waing, Dr. Nyein Aye, On the Automatic Detection System of Stop Line Violation for Myanmar Vehicles (Car), Volume 1 - Issue 4 November 2013.

14. Axatov A. (2023). Sun'iy intellektdan foydalanib yo'llardagi tirbandliklarni baholash bosqichlari va algoritmlari. Amaliy matematikaning



zamonaviy muammolari va istiqbollari. Qarshi davlat universiteti, 2024-yil, 24-25-may.

15. A. Akhatov, "Transport harakatini boshqarish usullari" Sun'iy intellekt va raqamli ta'lim texnologiyalari: amaliyot, tajriba, muammo va istiqbollari mavzusidagi xalqaro ilmiy-amaliy anjuman materiallari to'plami. Samarqand davlat univerteti, 2024 yil 3-4-iyun.

16. Eshtemirov B.Sh., Nazarov F., Yarmatov Sh.Sh. "Technologies for identifying vehicles standing at traffic lights based on video data", Central asian journal of mathematical theory and computer sciences, Volume: 03 Issue: 12 | ISSN: 2660-5309, 2022 yil, dekabr.

17. H. Mao-Chi and Y. Shwu-Huey, "A real-time and colorbased computer vision for traffic monitoring system," in Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on, 2004, pp. 2119-2122 Vol.3.

18. Kanungo, A.; Sharma, A.; Singla, C. Smart traffic lights switching and traffic density calculation using video processing. In Proceedings of the 2014 Recent Advances in Engineering and Computational Sciences (RAECS), Chandigarh, India, 6–8 March 2014; pp. 1–6.

19. Xun, F.; Yang, X.; Xie, Y.; Wang, L. Congestion detection of urban intersections based on surveillance video. In Proceedings of the 18th International Symposium on Communications and Information Technologies (ISCIT), Bangkok, Thailand, 26–28 September 2018; pp. 495–498.

20. Kurniawan, J.; Syahra, S.G.; Dewa, C.K. Traffic Congestion Detection: Learning from CCTV Monitoring Images using Convolutional Neural Network. *Procedia Comput. Sci.* 2018, 144, 291–297.



MoO₃/Mo NANOTUZULMALARINI OLISH VA ULARNING ELEKTRON TUZILISHI VA OPTIK XOSSALARINI O'RGANISH

Allayarova Gulmira Xolmuratovna,

Fizika –matematika fanlari bo'yicha falsafa doktori
(PhD), dotsent, Qarshi davlat universiteti "Nazariy
va eksperimental fizika kafedrasida dotsenti

Buronov Nurlibek Rustam o'g'li,

Fizika fakulteti Transport logistikasi 3- kurs talabasi

Zaripov Shuxrat Sobirjon o'g'li,

Fizika yo'nalishi 2- kurs magistranti

Annotatsiya. Bu ishda ikkilamchi elektronlar spektroskopiyasi hamda fotoelektronlar spektroskopiyasi kompleks usullaridan foydalanib, Mo ga O₂⁺ ionlarini bombardimon qilish usuli orqali Mo ni yuzida hosil qilingan MoO₃ nanotuzilmalarining elektron tuzulishi va fizik – optik xususiyatlari o'rganilgan. Hosil bo'lgan MoO₃ nanotuzilmasining taqiqlangan zona kengligi $E_g = 3,4$ eV yuzasining notekisligi esa 1,5 nm. Toza Mo ga O₂⁺ ionlarini implantatsiya qilinganda valent elektronlarning valent zonalarda joylashish zichliklari o'zgarib borishini ko'rsatdi. Olingan spektrlardan ko'rinadiki valent elektronlar valent zonalarda joylashganda turli zichliklar bilan joylashar ekan va bu hosil bo'lgan spektrlar maksimum va minimumlarida yanada yaqqolroq namoyon bo'ldi.

Kalit so'zlar: ion implantatsiya, termik oksidlash, ikkilamchi elektronlar spektroskopiyasi, nanotuzilmalar.

Kirish. Molibden va molibden oksidi nanotuzilmalari turli sohalarda keng qo'llaniladi. Masalan mikro –elektronika optoelektronika va elektronika sohaslarida, turli hil displeyevlar olishda, sensorlarda va organik ko'yosh elementlarida MDP va PDP tuzilmalar olishda bundan tashqari integral sxemalar olishda tranzistorlarda keng qo'llaniladi[1-4].

Hozirgi vaqtgacha adabiyotlardan ma'lumki shisha ustida termik oksidlash usullari orqali va magnitron changlatish usullari orqali hamda MoO₃ tayyor kukunlari orqali ularning foton-elektron ta'sirida uning optik va emissiya va elektrofizik xususiyatlari o'rganib kelingan. Biroq Mo yuzida termik oksidlash va ion implantatsiya usullari orqali hosil qilingan MoO₃ nanoplankalarining qalinligini tarkibini va yuza morfologiyasi fizik xususiyatlari haqida to'liq ma'lumotlar mavjud emas[5-10].

Biz bu ishda Mo ni O₂⁺ ionlari bilan ion implantatsiya qilish usuli orqali hosil bo'lgan MoO₃ nanoplankalarining tarkibi, zona energetik parametrlari va valent elektronlarning valent zonalarda joylashish

zichligini o'rgandik. Ushbu ishda termik oksidlash usuli va ion implantatsiya usullari bir biriga solishtirib o'rganildi.

Nazariy tadqiqot metodologiyasi. Nishon sifatida monokristall tuzulishdagi Mo(111) namunasi olingan. Shaybasimon qilib qirqilgan namunaning diametri ~ 10 mm va qalinligi ~ 0,3 mm ga teng. Namuna yaxshilab shlifovka qilingach uni almaz pastasi yordamida yaxshilab tozalanib olindi. Yaxshilab tozalangan namunani sirtini spirt bilan tozalab artib, yuqori vakuumli 2 ta kameradan iborat bo'lgan qo'rilmaga joylashtirildi. Qo'rilmanning 1- kamerada termik oksidlash va ion implantatsiya jarayonlari amalga oshirildi, 2- kamerada esa bir qancha metodlar asosida; hosil bo'lgan nanoplankalarining tarkibi, elektron tuzulishini Oje elektronlar spektroskopiyasi va optik xususiyatlari va energetik parametrlarini (UFES) Ultrabinafsha nurlar spektroskopiyasi yordamida, sirt morfologiyasi va kristall tuzulishini (AKM) atom kuchlanishli



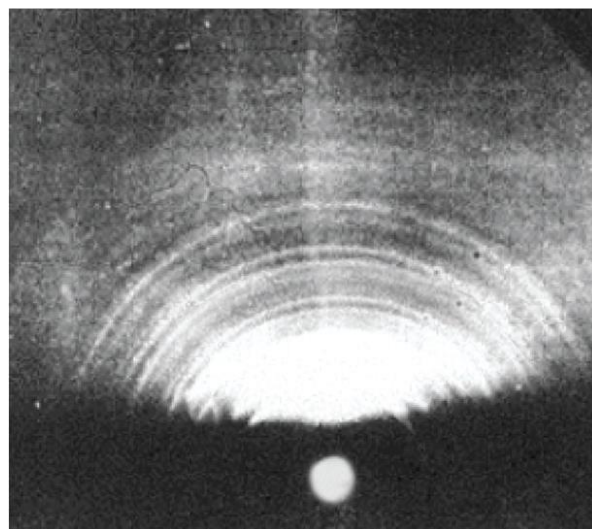
mikroskop va sekin elektronlar defraksiyasi usuli yordami o'rganildi[11-16].

Termik oksidlantirishdan oldin namunani 10^{-2} Pa $T= 2000$ K da uzoq vaqt 25-30 soat qizdirib tozalab olindi. Keyin esa $T= 2200$ K ga impulsli qizdirib olindi. Maxsus gaz balonni yordamida namunani yuzasiga $\varphi < 15^{\circ}$ ostida gaz molekulari yuborildi. Gaz molekulari yuborilganda namuna bir vaktida $T= 850$ K ga qizdirib turildi. O_2 molekulari kelib namunani yuzasiga utirdi va optimal $T= 850$ K qalinligi 60 \AA bo'lgan MoO_3 nanoplankasi hosil qilindi. Hosil bo'lgan nanoplankaning tarkibi birjinsli bo'lmadi va bo'ndan tashqari nanotuzilma orolcha o'sdi. Shuning uchun 2- usul ion implantatsiya usulida MoO_3 nanotuzilmalarini hosil qilib olindi. Bu usulda termik oksidlash kabi namunani oldin $T= 2000$ K da 10^{-2} Pa uzoq vaqt 25-30 soat qizdirib tozalab olindi. Keyin esa $T= 2200$ K ga impulsli qizdirib olindi. Keyingi bosqich O_2 molekularini elektron bombardimon qilish orqali kislorod molekulari O_2^+ ionlariga aylantirilib namunaning yuzasiga nisbatan $\varphi < 10-15^{\circ}$ ostida O_2^+ ionlarini energiyalarini $E= 1, 3, 5$ keV va turli dozalarda $D = (4-8) \cdot 10^{17} \text{ cm}^{-2}$ namunaning yuzasiga yuborildi. Ion implantatsiya jarayonida ham namuna bir vaqtda optimal harorat $T= 850$ K ga qizdirib turildi[17-21].

Ion implantatsiya jarayonida ionlarning $E = 1\text{keV}$ bo'lganda O_2^+ ionlari namunaning yuzasiga yaqinroq sohalariga keradi va hosil bo'lgan MoO_3 nanotuzilmaning qalinligi 30 \AA ni tashkil etdi. Ionlarning energiyasi $E = 3\text{keV}$ bo'lganda O_2^+ ionlari namunaning yuza osti qatlamlariga kerib bordi va hosil bo'lgan nanotuzilma qalinligi 60 \AA ni, $E = 5\text{keV}$ bo'lganda esa 90 \AA qalinlikdagi nanotuzilmalar hosil qilib olindi. Hosil qilingan MoO_3 nanotuzilmasining tarkibi birjinsli va tuzilmalar orasida o'tish qatlamlari deyarli hosil bo'lmadi. Demak xosil bo'lgan MoO_3 nanotuzilmasining yuza morfologiyasi 1- rasmda keltirilgan[17].



a)



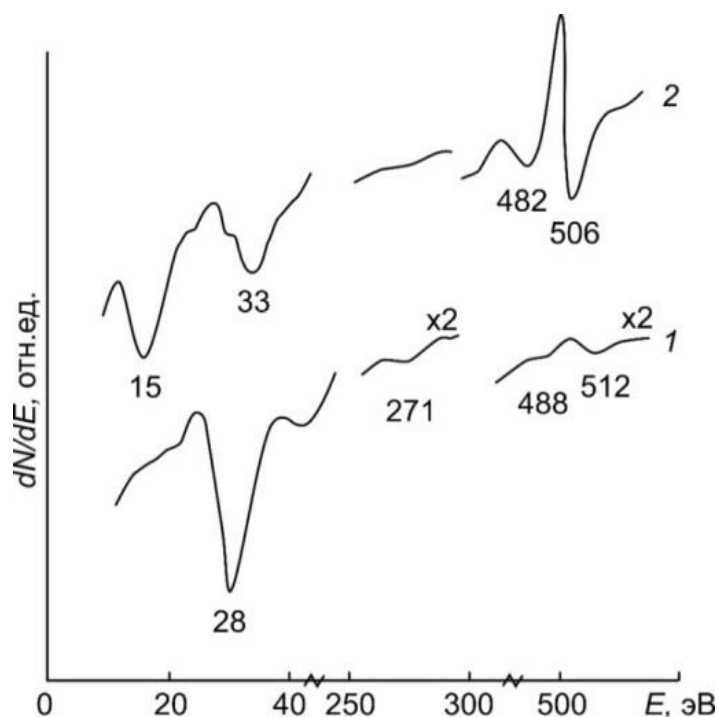
b)

1.Rasm. Ion implantatsiyasi natijasida olingan qalinligi 60 \AA MoO_3 nanoplankasi yuzasi: a – tasvir atom kuchi mikroskopi yordamida olingan ; b – elektron diffraksiya naqsh (tez elektron diffraksiya)[17].

Rasmdan ko'rinadiki Atom kuchlanishli mikroskop (AKM) yordamida olingan tasvir MoO_3 nanotuzilmasining yuza notikesligini va chukkilardan iborat ekanligi ($1,5 \text{ nm}$) va sekin elektronlar defraksiyasida (SED) olingan tasvir hosil bo'lgan nanotuzilma polikristall to'zulishda ekanligini qo'rsatdi.

Natijalar va muhokamalar. Quyidagi 2-rasmda toza Mo va ion implantatsiya usulida hosil qilingan MoO_3 nanotuzilmalari uchun olingan Oje spektrlar keltirilgan.

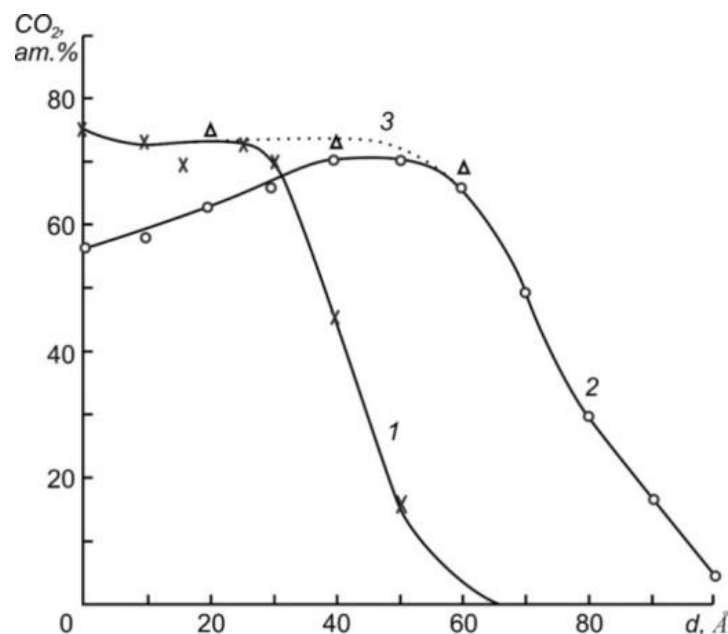




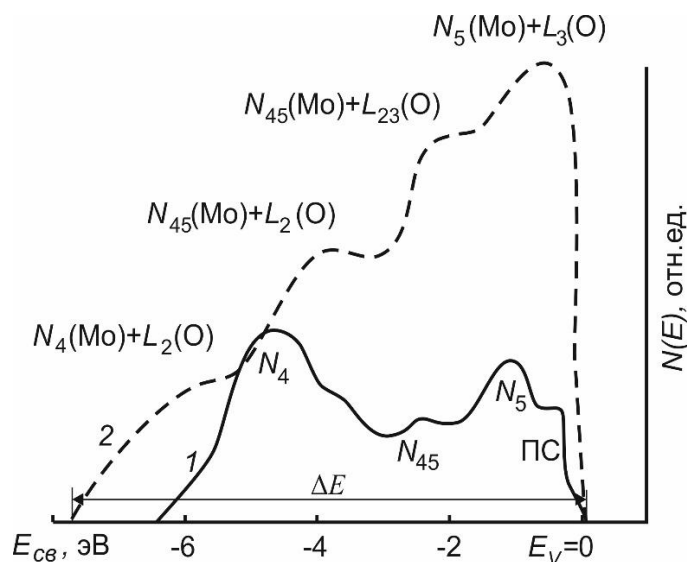
2-Rasm. a) Toza Mo (111): uchun b) O₂⁺ ionlarini energiyasi 1 keV va dozasi 4 × 10¹⁷ sm⁻² implantatsiya qilib haroratni 850 K qizdirib turilganda hosil bo'lgan MoO₃ nanotuzilmasi uchun Oje spektrlari[21]

Chizmadan kurinadiki toza Mo da olingan Oje spektrlar chuqqilarining siljishlari Mo va O₂⁺ ionlari bilan o'zaro bog' hosil qila boshladi deyishimiz mumkin. Termik oksidlash usulini ion implantatsiya usuliga solishtirib o'rganilganda ion implantatsiya usulida ionlarning energiyasini boshqarish imkonini va bu orqali nanotuzilmalarning qalinligini va ko'p qatlamli tizimlar hosil qilish imkonini berdi. Qo'yidagi 3- rasmda termik oksidlash usuli va ion implantatsiya usullarida olingan nanotuzilmalarni tarkibidagi O₂⁺ uchun konsentratsiya taqsimotlari keltirilgan.

Rasmdan kurinadiki (2-igri chiziq) termik oksidlash usulida 60 Å qalinlikda olingan naotuzilmaning o'tish qatlami ham 60 Å ni tashkil etdi. Ion implantatsiya usulida hosil qilingan nanotuzilmada esa (1- igri chiziq) o'tish qatlamlari o'tish qatlamlari juda kam hosil bo'ldi va stixiometrik tarkibi butun xajm va yuza bo'yicha buyicha deyarli bir hil bo'ldi. Keyingi 4- rasmda esa toza Mo va MoO₃ nanotuzilmalari uchun fotoelektron spektrlari keltirilgan.



3 – Rasm. Kislorod ionlarini turli energiyalarda E₀, keV: 1 – 1; 2 – 3; 3 – 5-3 va 1; ionlar dozasi tuyinish dozasi D=2·10¹⁷sm⁻² 60 Å qalinlikda MoO₃ hosil bo'lishida O₂⁺ ionlarining atom konsentratsiya taqsimotlari keltirilgan[17].



4- Rasm. Toza Mo uchun fotonlarni energiyasini 1 –10.8 ; 2 – MoO₃ nanotuzilmasi uchun fotonni energiyasi 15.6 eV da valent zona uchun spektrlari[21].

Rasmdan ko'rinadiki toza Mo ga (1- igri chiziq) fotonlarni energiyasi 10,8 eV qilib yuborilganda valent elektronlarning valent zonalardagi taqsimot spektrlari keltirilgan. Toza Mo ga O₂⁺ ionlarini implantatsiya qilinganda valent elektronlarning valent zonalarda joylashish zichliklar i o'zgarib borishini ko'rsatdi.



Olingan spektrlardan ko'rinadiki valent elektronlar valent zonalarda joylashganda turli zichliklar bilan joylashar ekan va bu hosil bo'lgan spektrlar maksimum va minimumlarida yanada yaqqolroq namoyon bo'ldi.

Xulosa. Shunday qilib bu ishda birinchi marta termik oksidlash va ion implantatsiya usullari yordamida hosil qilingan qalinligi 30-100 Å bo'lgan nanotuzilmalarning tarkibi va yuza nokesligi, zona energetik parametrlari o'rganilib quyidagi xulosalarga kelindi. Termik oksidlash usulida hosil qilingan MoO₃ nanotuzilmasini hosil bo'lishida o'tish qatlamlar ko'proq hosil bo'ldi va bo'nga sabab ularning tarkiblari birjiginsli bo'lmaganligidir. Ion implantatsiya usulida olingan MoO₃ nanotuzilmalari esa elementar va kimyoviy tarkiblari 30-100 Å bo'lgan qalinliklar orlig'ida deyarli bir jinsli nanotuzilma hosil bo'ldi. Bir jinsli bo'lgan nanotuzilmaning zona energetik parametrlari va valent elektronlarning valent zonada joylashish taqsimotlari o'rganilganda 4 ta maksimumdan iborat spektrlar hosil bo'ldi. Bundan kelib chiqib biz valent zonada joylashgan valent elektronlarni turli zichliklar bo'yicha joylashishi mumkin degan xulosaga keldik.

Adabiyotlar ro'yhati

1. Коршунов А.В. // Размерные и структурные эффекты в процессах окисления металлов: монография. Томск, 2013. 360 с.
2. Миннеханов А.А., Вахрина Е.В. Константинова Е.А., Кашкаров П.К. // Письма в ЖЭТФ. 2018. Т. 107. Вып. 4. С. 270.
3. Surovoi E.P., Surovaia V.E., Bugerko L.N. // J. Phys.Chem. A. 2013. V. 87. № 5. P. 826.
4. Ковивчак В.С., Панова Т.В. // Поверхность. Рентген., синхротр. и нейтрон. исслед. 2016. № 12. С. 41.
5. Гаврилов С.А., Белов А.Н. Электрохимические процессы в технологии микро- и наноэлектроники. М.: Высшее образование, 2009. 272 с.
6. Буназаров Д.Б., Касымов А.Х., Нормурадов М.Т., Пугачева Т.С. // Радиотехника и электроника. 1976. № 7. С. 21.
7. Суровой Э.П., Суровая В.Э., Бугерко Л.Н. // Журн. физ. химии. 2013. Т. 87. № 5. С. 842.

8. Chary K.V.R., Reddy K.R., Gurram K. et al. // J. Catal. 200. V. 226. № 2. P. 283.
9. Scanlon D.O., Watson G.W., Payne D.J. et al. // J. Phys.Chem. C. 2010. V. 114. P. 4636. <https://doi.org/10.1021/jp9093172>
10. Kang M., Oh E., Kim I. et al. // Current Appl. Phys. 2012. V. 12. P. 489. doi . 2011. 08. 007 <https://doi.org/10.1016/j.cap>
11. Bohne N.Y., Shevchenko F., Prokert J. // Nucl. Instrum.Methods Phys. Res. B. 2005. V. 24. Iss. 1–2. P. 157.
12. Bernd R., Claus H., Bernd R. // Nucl. Instrum. Methods Phys. Res. B. 2000. V. 160. Iss. 3. P. 363.
13. Alov N.V. // Nucl. Instrum. Methods Phys. Res. B. 2007. V. 256. Iss. 1. P. 337.
14. Ivna K., Piltaverlavana J., Badovinac R. // Appl. Surf.Sci. 2017. V. 425. P. 416.
15. Алов Н.В., Леонов М.П. // Физика и химия обработки материалов. 1986. Т. 6. № 6. С. 94.
16. Умирзаков Б.Е., Ташмухамедова Д.А., Гулямова С.Т., Аллаярова Г.Х. // ЖТФ. 2020. Т. 90. Вып. 5. С. 831.
17. Isakhanov Z.A., Mukhtarov Z.E., Umirzakov B.E., Ruzibaeva M.K. // Tech. Phys. 2011. V.56. Iss. 4. P. 546.
18. Donaev S.B., Djurabekova F., Tashmukhamedova D.A., Umirzakov B.E. // Phys. Stat. Sol. C. 2015. V. 12. Iss. 1–2. P. 89.
19. Эргашов Ё.С., Ташмухамедова Д.А., Раббимов Э. // Поверхность. Рентген., синхротр. и нейтрон. исслед. 2015. № 4. С. 38.
20. Алиев А.А., Шалимов З.Т. // Поверхность. Рентген., синхротр. и нейтрон. исслед. 2003. № 8. С. 105.
21. Умирзаков Б.Е., Исаханов З.А., Рузобаева М.К., Ёркулов Р.М. // ЖТФ. 2019. Т. 89. № 6. С. 935.



INSON YUZ TASVIRIDAN HISSIYOTLARNI ANIQLASH UCHUN GEOMETRIK XUSUSIYATLARINI VA TASHQI KO'RINISHGA ASOSLANGAN XUSUSIYATLARINI AJRATIB OLISH

Kurbanov Abduraxmon Alishboyevich,
Mirzo Ulug'bek nomidagi O'zbekiston Milliy
universitetining Jizzax filiali tayanch doktoranti
abduraxmon.1986@gmail.com

Annotatsiya. Inson qarshisida turgan suhbatdoshining emotsional holatini ko'rish, anglash va his qilish kabi sezish qobiliyatlari yordamida osongina aniqlay oladi, biroq kompyuter tizimlari uchun bu juda murakkab masaladir. Hissiyotlarni avtomatik aniqlash borasida zamonaviy kompyuter texnologiyasi va sun'iy intellekt tizimlari samarali bashoratlarni taqdim etishayapti, lekin zamonaviy CNN texnologiyalari yordamida juda katta ma'lumotlar to'plami bilan qurilgan chuqur o'rganish modellari ham murakkab hissiy holatlarni aniqlash borasida mukammal emasligi isbotlangan. Ushbu maqolamizda hissiy holatni to'g'ri baholash uchun zarur bo'lgan yuz xususiyatlarini aniqlash masalasi hal qiladi.

Kalit so'zlar: Local binary pattern (mahalliy ikkilik naqshlar), Histogram of Oriented Gradients (yo'naltirilgan gradientlar gistogrammasi), konvolutsion neyron tarmoqlari. SVM, k-NN, random forest, Haarcascads, bilateralFilter

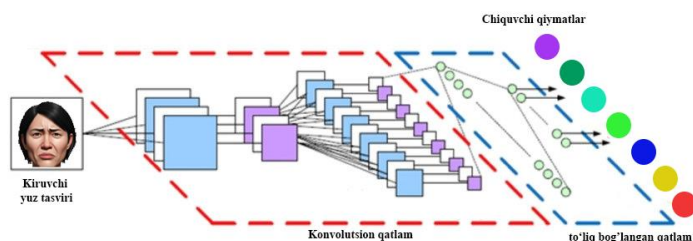
Kirish. Tuyg'ularni tushinish shaxslararo muloqotning shuningdek ijtimoiy hayotdagi o'zaro aloqaning muhim vositalaridan biridir. So'nggi o'n yillikda yuz tahlili sohasida bir qancha yutuqlarga erishildi. Ishlab chiqilgan natijalar va modellar biometric xavfsizlik sohasida shaxsni identifikatsiya qilish tizimlari, ta'limda o'quvchilarning diqqat va e'tibor darajasini kuzatishda, insonlarning ruhiy salomatligini nazorat qilishda keng qo'llanila boshlandi.

Yuz tasvirlaridan inson hissiyotlarini aniqlash uchun hissiy holatlarni ifodalovchi vizual belgilarni ajratib olish va izohlash jarayoniga qaratilgan bir qator algoritmik bosqichlar bajariladi. Tasvirga ishlov berish bosqichida Haarcascads, Yo'naltirilgan Gradientlar Gistogrammasi yoki chuqur o'rganishga asoslangan detektorlar (masalan, YOLO, MTCNN) kabi usullardan foydalangan holda yuz tasviri aniqlanadi. yuzni aniqlagandan so'ng, yuzning o'lchami va masshtabi standartlashtiriladi. Bunda turli hil resize operatsiyalaridan foydalanish mumkin. Tasvir Gauss xiralashtirish yoki bilateralFilter kabi usullar yordamida tasvirdagi shovqinlar kamaytiriladi yani tiniqlashtiriladi. Keying boshqich xususiyatlarga ajratish bosqichi bo'lib, tuyg'ularni aniqlashda ishlatiladigan xususiyatlarning ikkita asosiy turi

mavjud, lekin ba'zi tadqiqotchilar tomonidan gibrud usullar ham ishlab chiqilgan. **Geometrik xususiyatlar** – Faol shakl modellari yoki chuqur o'rganishga asoslangan usullar (masalan, OpenFace, dlib) kabi algoritmlar ko'zlar, burun, og'iz va qoshlarning holati kabi yuzdagi asosiy nuqtalari aniqlanadi. So'ngra bu belgilar orasidagi masofalar, burchaklar va nisbiy pozitsiyalar hissiyotlar bilan bog'liq ifodalarni aniqlash uchun ishlatiladi (masalan, g'azab uchun chimirilgan qoshlar yoki baxt uchun baland lablar). **Tashqi ko'rinishga asoslangan xususiyatlar** – Gabor filtrlari yoki mahalliy ikkilik naqshlar kabi filtrlar terining tuzilishini tahlil qilish yoki ko'z yoki og'iz atrofidagi qirralarni aniqlash orqali xususiyatlarga ajratiladi. Tashqi ko'rinishga asoslangan xususiyatlarni ajratishning yana bir usuli tasvirni to'g'ridat-to'g'ri konvolutsion neyron tarmoqlaridan o'tkazilib tahlil qilinadi. Konvolutsion neyron tarmoqlari his-tuyg'ular bilan bog'liq nozik naqshlarni ushlay oladigan yuzdan ierarxik xususiyatlarni avtomatik ravishda olish uchun ishlatiladi. VGG-Face, ResNet yoki maxsus arxitektura kabi oldindan tayyorlangan modellar murakkab yuz tasvirlarini o'rganish imkonini beradi. Hissiyotlarning tasniflash bosqichi tegishli xususiyatlar chiqarilgandan so'ng, hissiy holatni bashorat qilish uchun tasniflash algoritmlari qo'llaniladi. Tasniflashning keng



tarqalgan ikki usuli mavjud. An'anaviy mashinaviy o'rganish algoritmlari yordamida masalan qo'llab quvatlash vektor mashinalari yoki k-eng yaqin qo'shnilar bo'lishi mumkin. Ikkichi usul chuqur o'rganish algoritmlari yordamida, eng samarali usullar bu konvolyutsion neyron tarmolar yordamida. CNN-ga asoslangan modellar odatda oxirigacha his-tuyg'ularni aniqlash uchun ishlatiladi. Ushbu modellar his-tuyg'ularni to'g'ridan-to'g'ri xom piksel ma'lumotlaridan yoki olingan xususiyat xaritalaridan tasniflashni o'rganadilar.



1-rasm. Konvolyutsion neyron tarmoqlarida foydalanib hissiyotlarni aniqlash.

Yuqorida kiruvchi ma'lumot sifatida inson tasvirlari olingan va undan yuz tasvirini ajratib olib tahlil qilingan. Tahlil qilish muobaynida xususiyatlar haqidagi ma'lumotlar olinadi va hu asosida yuz tasvirida ifodalangan hiisiyot turlarida tasviflanadi. Ushbu maqolamizda Geometrik xususiyatlarni ajratib olishda uchburchaklar usuli va tashqi ko'rinishga asoslangan xususiyatlarni ajratib olishda Gabor filteri usulidan foydalanilgan. Maqolada faqat yuz xususiyatlarini ajratib olish usullari haqida so'z yuritilgan olingan xususiyatlar asosida tuyg'ularni aniqlash jarayoni masalasini keyingi ishlarimizda hal qilamiz.

Adabiyotlar sharhi. Ko'plab ilmiy tadqiqot ishlarida hissiyotlarni aniqlashda yuzni geometrik xususiyatlarga ajratish yoki tashqi ko'rinishga asoslangan yondoshuvlardan foydalanilgan. Ishlab chiqilgan usullar ham u yoki bu yondashuv asosida insonning emotsional holati baholangan. Yuzni geometrik xususiyatlarga ajratish borasida bir qancha tadqiqotlar olib borilgan. Jumladan Murugappan M. va Mutawa A. tomonidan e'lon qilingan "Facial geometric feature extraction based emotional expression classification using machine learning

algorithms" nomli tadqiqot ishida kompyuterda yaratilgan markerlar yordamida oltita hissiy ifodani (qayg'u, g'azab, qo'rquv, ajablanish, jirkanish va baxt) tasniflash uchun yangi geometrik xususiyatlar to'plamini olish uchun triangulyatsiya usuli taklif etdi. F. Zhang va boshqalar tomonidan yuz tasvirining shakl geometriyasidan foydalangan holda bir vaqtning o'zida yuz tasvirini sintez qilish va poza-invariant yuz ifodasini aniqlash imkonini beruvchi generativ raqib tarmog'iga modelini taklif qilishdi. Qayta tiklangan xususiyatlar geometrik shakllarga mos kelmaydigan to'rtburchak shaklni aniqlaydi. Noaniq a'zolik funksiyalari taklif etilayotgan Aralash kvadratik shakl modelidan (MQSM) to'rtburchakning noaniqlik darajasini aniqlash uchun ishlatish mumkin. Noaniq xususiyatlar atribut qiymatlaridan olinadi va tasniflagichni tekshirish uchun ishlatiladi (jami 12 ta). MSQM ishlashini tekshirish uchun tajribada CK, JAFFE va ISED ma'lumotlar bazalaridan foydalaniladi. Faqat 12 ta noaniq atributlardan foydalangan holda, tavsiya etilgan usul ko'pincha mos yozuvlar rasmlariga bog'liq bo'lgan eng zamonaviy texnikalardan ustun keldi. Tadqiqotchilar o'z tadqiqotlarida an'anaviy ravishda statik xususiyatlarni tanlash usullaridan foydalanganlar. Foydali bo'lishiga qaramay, bu usullar ba'zi muhim cheklovlarga ega, ayniqsa ular spontan nutq bilan shug'ullanishga tegishli. Bu, asosan, har bir insonning yuz xususiyatlari biroz boshqacha hissiy ifodalarga olib kelishi bilan bog'liq. Ushbu muammoni hal qilish uchun tadqiqotchilar Mazher Iqbal va boshqalar ikki turdagi geometrik xususiyatga asoslangan yuz xususiyatlariga asoslangan dinamik atributlarni tanlash yondashuvini taqdim etishdi.

Tashqi ko'rinishga asoslangan xususiyatlar yordamida hissiyotlarni aniqlash borasida Y. Yaddanden o'zining "An efficient facial expression recognition system with appearance-based fused descriptors" nomli tadqiqot ishida ikkita alohida tasvir identifikatoridan foydalanishni solishtirib, ya'ni Mahalliy ikkilik naqsh va yo'naltirilgan gradientlar gistogrammasi ikki xil o'lchamlarni kamaytirish texnikasi, xususan, asosiy komponentlar tahlili va mahalliy chiziqli joylashtirishni ishlab chiqadi. Bundan tashqari, tizim samaradorligini oshirish uchun ikkala deskriptorni ham birlashtiradi. Tizimning



tasniflash qismi uchun oltita asosiy his-tuyg'ularni farqlash uchun uning umumlashtirish imkoniyatlari uchun ko'p sinfli Support vektor mashinasi tasniflagichidan foydalanadi.

Tadqiqotchilar M. Kas, Y. Ruichek, R. Messoussilar tomonida taklif etilgan xususiyatlarni ajratish usulida yuz tasviridagi 49 ta aniqlangan belgilarning tekstura va shakl xususiyatlarini birlashtirishga asoslangan yondoshuvni taklif etishga. Shuningdek shakl haqidagi ma'lumotlar aniqlangan 49 belgining joylashuvini interpolatsiya qilish orqali hosil qilingan ikkilik patchda qo'llaniladigan yo'naltirilgan gradientlar gistogrammasi (HOG) yordamida chiqariladi. Teksturaviy ma'lumotlar 49 ta kichik rasmdan hisoblab chiqiladi, ularning har biri bitta diqqatga sazovor nuqtada joylashgan bo'lib, bu erda taklif qiladigan yangi qo'lda ishlangan identifikatordan foydalangan holda ortogonal va parallel yo'nalishlarga asoslangan umumiy to'rtlik xarita ikkilik naqshlari deb nomlashgan.

Metodologiya. Ushbu maqolada biz geometrik xususiyatlar va tashqi ko'rinishga asoslangan xususiyatlarni ajratish usulini ko'rib chiqamiz. Dastlab kiritilgan tasvirdan yuz tasvirini aniqlab olamiz. Avtomatlashtirilgan yuzni tanib olish sub'ektning yuzini kamroq hisoblash resursi sarflangan holda aniqlashi zarur. Ko'zlar, og'iz va burun qismlari yuzlarini aniqlash uchun asosiy mos belgi nuqtasi bo'lib xizmat qildi. So'nggi yillarda yuzni aniqlashning turli usullari ishlan chiqilgan bo'lsa-da, Viola va Jones yuzni aniqlash usuli boshqa yuzni aniqlash usullariga qaraganda real vaqtda yuz hissiyotlarini aniqlash uchun samarali hisoblanadi. Viola va Jones algoritmidagi yuz, ko'z, burun va og'izni aniqlashda Haar-like xususiyatlaridan foydalanilgan. Haar-like xususiyatlar yuzni aniqlashda tasvirning asl piksel qiymatlaridan foydalanish o'rniga chiziqlar, qirralar va markazni o'rab turgan xususiyatlardan foydalangan holda qo'shni to'rtburchaklar guruhlar orasidagi piksel kontrastini (oq va qora) hisoblash uchun ishlatilgan.

$$I_{integral}(x, y) = \sum_{x' \leq x, y' \leq y} I(x', y') \quad (1)$$

(1) formulada integral tasvir (x,y) yuqorida va chapdagi barcha piksel qiymatlarining yig'indisini saqlaydi. Bu doimiy vaqt ichida har qanday

to'rtburchak maydon uchun piksel intensivligi yig'indisini hisoblashga yordam beradi.

Haar-like xususiyatlar (2) ga asoslangan petseptronlar yordamida qaytariladi.

$$f_{w,b}(I) = \begin{cases} 1, & \text{agar } \sum_{x,y} w(x,y)I(x,y) + b > 0 \\ 0 & \text{aks holda} \end{cases} \quad (2)$$

Shunday qilib, bu usul boshqa usullarga qaraganda yuzni aniqlash uchun kamroq hisoblash vaqti va xotira xajmini talab qiladi. Ushbu ishda veb-kameradan tasvir ketma-ketligini olish uchun OpenCV kutubxonasidan foydalaniladi. Viola-Jons algoritmidan foydalanib dasturni quyidagicha tuzish mumkin.

```
import cv2
face_cascade =
cv2.CascadeClassifier(cv2.data.harcascades +
'haarcascade_frontalface_default.xml')
cap = cv2.VideoCapture(0)
cap.set(cv2.CAP_PROP_FRAME_WIDTH,
1280)
cap.set(cv2.CAP_PROP_FRAME_HEIGHT,
1082)

while cap.isOpened():
    success, frame = cap.read()
    gray_image = cv2.cvtColor(frame,
cv2.COLOR_BGR2GRAY)
    if not success:
        print("Kamera mavjud emas.")
        continue
    faces =
face_cascade.detectMultiScale(gray_image,
scaleFactor=1.1, minNeighbors=5, minSize=(30, 30))
    for (x, y, w, h) in faces:
        cv2.rectangle(frame, (x, y), (x + w, y +
h), (255, 0, 0), 2)
        # Natija
        cv2.imshow('Face Detection', frame)
        if cv2.waitKey(5) & 0xFF == 113:
            break
    cap.release()
cv2.destroyAllWindows()
```



Yuzning geometrik xususiyatlarini ajratib olish inson yuzining asosiy nuqtalarini (belgilarini) tahlil qilish, uning tuzilishini aniqlashga asoslangan. Bu belgilar odatda ko'zlar, burun, og'iz va jag' kabi yuz xususiyatlariga mos keladi. Masofalar va burchaklar kabi bu belgilar orasidagi munosabatlar yuzning geometriyasini tasvirlash uchun ishlatiladi. Buning uchun bir qancha usullar ishlab chiqilgan. **Belgilar orasidagi Evklid masofasi** – Ikki yuz belgilari orasidagi masofani Evklid masofa formulasi yordamida hisoblash mumkin. Bu og'izning kengligi, ko'zlar orasidagi masofa yoki burun balandligi kabi xususiyatlarni tavsiflash uchun foydalidir.

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (3)$$

Belgilar orasidagi burchaklar – Uchta belgidan tashkil topgan burchaklar ko'zning egilishi yoki burunning qiyaligi kabi ba'zi geometrik munosabatlarni tasvirlashga yordam beradi. Burchak θ uch nuqta o'rtasida vektor matematikasi yordamida topish mumkin:

$$\theta = \arccos\left(\frac{\vec{AB} \cdot \vec{BC}}{|\vec{AB}| \cdot |\vec{BC}|}\right) \quad (4)$$

Tomonlar nisbati – yuz ifodalari uchun yana bir muhim geometrik xususiyatdir. Bu nisbatlar turli xil yuz xususiyatlarining nisbiy hajmini tavsiflashi mumkin. Ko'zning miltillashini aniqlash uchun ishlatiladigan algoritm.

$$EAR = \frac{|p_2 - p_6| + |p_3 - p_5|}{2 * |p_1 - p_4|} \quad (5)$$

Bu yerda $p_1, p_2, p_3, p_4, p_5, p_6$ atrofidagi diqqatga sazovor joylarni ifodalovchi nuqtalar. Bu nisbat ko'z ochiq va yopiq holatda o'zgaradi va bu ko'zni miltillashni aniqlash uchun foydalidir.

Geometrik xususiyatlarni aniqlashda yana bir qancha algoritmlar ishlab chiqilgan.

Tashqi ko'rinishga asoslangan xususiyatlar.

Yuzning his-tuyg'ularini aniqlash uchun tashqi ko'rinishga asoslangan xususiyatlarni ajratib olish yuz tasvirlaridagi tekstura, rang va intensivlik naqshlaridan olingan vizual ma'lumotlardan foydalanishni o'z ichiga oladi. Bu usul geometrik xususiyatlardan farq qiladi, ular aniq yuz belgilariga qaratilgan. Tashqi ko'rinishga asoslangan usullar yuzdagi naqshlar va qirralarni aniqlashga qaratilgan, ko'pincha hissiy

holatlarni farqlash uchun piksellar intensivligidan foydalanadi.

Tashqi ko'rinishga asoslangan xususiyatlarni aniqlashning bir qancha algoritmlari mavjud. **Asosiy komponentlar tahlili** (Principal Component Analysis) bu o'lchamlarni kamaytirishga asoslangan usul bo'lib, bunda asl piksel ma'lumotlarini asosiy komponentlar deb belgilaydi va o'zaro bog'liq bo'lmagan xususiyatlar to'plamiga aylantiradi. Yuz hissiyotlarini aniqlashda turli his-tuyg'ularga taalluqli tashqi ko'rinishga asoslangan eng muhim o'zgarishlarni saqlab qoladi. **Mahalliy ikkilik naqshlar** (Local Binary Patterns) yordamida xususiyatlarni ajratish bu har bir pikselni qo'shnilari bilan taqqoslash va natijani ikkilik naqshda kodlash orqali tasvirdagi lokal belgili teksturaga o'tkazish modeli. Bu usul yuz ifodasini aniqlashda keng qo'llanilgan, chunki u yorug'likning tushush burchagining o'zgarishiga chidamli va hisoblash jihatidan samaralidir. **Gabor filtrlari** – insonning ko'rish korteksi neyronlarining retseptiv maydonlarini sezishi jarayoniga taqlid qilgan holda qurib chiqilgan bo'lib, tasvirlardagi fazoviy chastotalar va yo'nalishlarni olish uchun keng qo'llaniladi. Yuz tasvirlariga qo'llanilganda, ular his-tuyg'ularni aniqlash uchun tegishli bo'lgan tekstura va qirrali ma'lumotlarni olishga yordam beradi. Gabor filtrlarining turli masshtab va yo'nalishdagi chiqishi yuz ifodalarini farqlash uchun xususiyatlar haqidagi ma'lumotlar to'plamini xosil qiladi.

$$g(x, y) = \exp\left(-\frac{x'^2 + y'^2}{2\sigma'^2}\right) \times$$

$$\exp\left(2\pi j \frac{x'}{\lambda} + \psi\right) \quad (6)$$

Bu yerda $x' = x \cos\theta + y \sin\theta$ va $y' = -x \sin\theta + y \cos\theta$

Natijalar. Jiola-Jons algoritmi uchun "haarcascade_frontalface_default.xml" modeli ishlab chiqilgan va OpenCV kutubxonasiga joylashtirilgan. Bu uchun dasturni quyidagicha tuzishimiz mumkin. Viola-Jons algoritmining yana bir qulayligi tasvirdani bir qancha to'liq ko'ringan yuzlarni ham aniqlay oladi. Bu narsa ko'cha kameralaridagi tasvirlarni ham tahlil qilish imkonini beradi.





2-rasm Viola-Jons algoritmidan foydalanib yuz tasvirini ajratish.

Aniqlangan nuqtalar va ularni birlashtirilishidan xosil bo'lgan uchburchaklar yuzalari Geron formulasi yordamida hisoblanadi aniqlangan qiymatlarni o'zgarishi asosida hissiyotlar klassifikatsiya qilinadi.



3-rasm. Yuzning muhim nuqtalarini belgilash.

Tasvirni Gabor filteri yordamida xususiyatlarni ajratishda tasvir piksellarini massiv shakliga o'tkazamiz va Gabor filteri ishlab chiqqan massiv asosida filterlaymiz. Gabor filteri (6) formula yordamida hisoblanadi. Ishni osonlashtirish uchun (6)

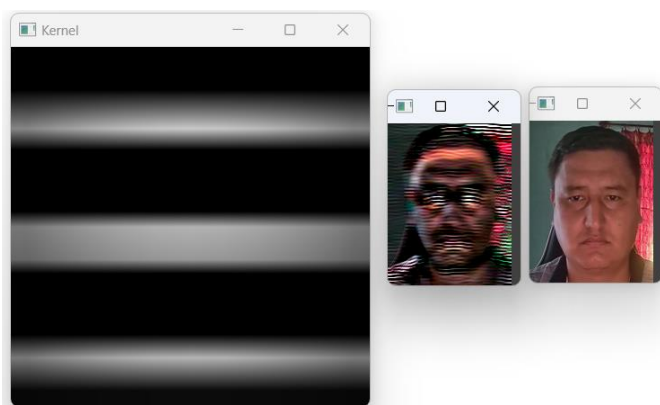
formula uchun alohida python funksiyasini yozmaymiz OpenCV kutubxonasidagi getGaborKernel() funksiyasidan foydalanamiz. σ , θ , va f parametrlarini o'zgartirish orqali turli yo'nalishlar, chastotalar va fazoviy kengliklarga ega Gabor filtrlarini yaratishimiz mumkin.

```
import numpy as np
import cv2
import matplotlib.pyplot as plt
```

```
ksize = 10
sigma = 5
theta = 1*np.pi/2
lamda = 1*np.pi/4
gamma=0.9
phi = 0.8
kernel = cv2.getGaborKernel((ksize, ksize), sigma,
theta, lamda, gamma, phi, ktype=cv2.CV_32F)
plt.imshow(kernel)
img = cv2.imread('my.png')
plt.imshow(img, cmap='gray')

img = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
fimg = cv2.filter2D(img, cv2.CV_8UC3, kernel)
kernel_resized = cv2.resize(kernel, (400, 400))
plt.imshow(kernel_resized)
plt.imshow(fimg, cmap='gray')
```

```
cv2.imshow('Kernel', kernel_resized)
cv2.imshow('Filtered', fimg)
cv2.waitKey()
cv2.destroyAllWindows()
```



4-rasm. Gabor filteri



Xulosa. Biz ushbu maqolada yuz tasviridan hissiyotlarni aniqlashda umuman yuz tasvirini tahlil qilishning asosiy bosqichi bo'lgan xususiyatlarni ajratib olishning ikki hil metodini va bu metodlar uchun turli hil algoritmlarni ko'rib chiqdik. Ikkala metodologiya ham o'ziga xos afzalliklarni taqdim etadi va yuzning his-tuyg'ularini aniqlashning alohida jihatlariga e'tibor beradi.

Geometrik xususiyatlar ko'zlar, burun, og'iz va qoshlar kabi asosiy yuz belgilarining shakli va fazoviy konfiguratsiyasiga qaratilgan. Bu xususiyatlar, ayniqsa, yuz mushaklari harakatidan kelib chiqadigan mimikadagi nozik o'zgarishlarni aniqlashda samaralidir. Masofalarni, burchaklarni va joy belgilarining pozitsiyasini o'zgartirishni tahlil qilish orqali geometrik usullar hissiyotlarning ishochli talqin qilinishi mumkin.

Boshqa tomondan, tashqi ko'rinishga asoslangan xususiyatlar, masalan, tekstura deskriptorlari (masalan, Gabor filtrlari, Mahalliy ikkilik naqshlar) yordamida olingan xususiyatlar yuz mintaqalaridan intensivlik, tekstura va tasvir chegaralari haqidagi ma'lumotlarini oladi. Bu xususiyatlar teri, yuz qismlari va mushaklar harakatlarining nozik o'zgarishlarni tahlil qilish imokiyatiga ega, bu ularni nozik hissiy holatlarni aniqlash uchun samarali hisoblanadi. Tashqi ko'rinishga asoslangan usullar, odatda, yorug'lik, poza va yuz okklyuziyasidagi o'zgarishlarga nisbatan mustahkamroqdir, chunki ular butun yuz yoki muayyan hududlardagi piksel intensivligi qiymatlarini tahlil qila oladi. Biroq, ular ko'pincha yuqori o'lchamli xususiyatlar bo'shliqlarini keltirib chiqaradi, bu esa o'lchovni kamaytirish usullari va murakkabroq tasniflash algoritmlari zarur bo'ladi.

Geometrik va tashqi ko'rinishga asoslangan xususiyatlarni aniqlashning gibrid yondashuv ham ishlab chiqilgan bo'lib, chuqur o'rganish algoritmlari yordamida takomillashtiriladi bu jarayon yuz hissiyotlarini aniqlash tizimlarining aniqligi va mustahkamligini sezilarli darajada yaxshilaydi.

Foydalanilgan adabiyotlar

1. Murugappan, M., and A. Mutawa. "Facial geometric feature extraction based emotional

expression classification using machine learning algorithms." *Plos one* 16.2 (2021): e0247131.

2. F. Zhang, T. Zhang, Q. Mao and C. Xu, "Geometry Guided Pose-Invariant Facial Expression Recognition," in *IEEE Transactions on Image Processing*, vol. 29, pp. 4445-4460, 2020, doi: 10.1109/TIP.2020.2972114.

3. Muruganandam, S. et al. "A Survey: Comparative study of security methods and trust manage solutions in MANET." 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) 1 (2019): 125-131.

4. Iqbal, JL Mazher, et al. "Facial emotion recognition using geometrical features based deep learning techniques." *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL* 18.4 (2023).

5. Yaddaden, Yacine. "An efficient facial expression recognition system with appearance-based fused descriptors." *Intelligent Systems with Applications* 17 (2023): 200166.

6. Kas, Mohamed, Y. Ruichek, and Rochdi Messoussi. "New framework for person-independent facial expression recognition combining textural and shape analysis through new feature extraction approach." *Information Sciences* 549 (2021): 200-220.

7. Bartneck, Christoph. "Affective expressions of machines." *CHI'01 extended abstracts on Human factors in computing systems*. 2001.

8. Viola, P. and M. Jones. Rapid Object Detection Using A Boosted Cascade Of Simple Features. in *Computer Vision and Pattern Recognition*, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on. 2001. IEEE.

9. Wang, Liwei, Yan Zhang, and Jufu Feng. "On the Euclidean distance of images." *IEEE transactions on pattern analysis and machine intelligence* 27.8 (2005): 1334-1339.

10. Juhong, Aniwat, and Chuchart Pintavirooj. "Face recognition based on facial landmark detection." *2017 10th Biomedical*



*Engineering International Conference
(BMEiCON). IEEE, 2017.*

11. Luo, Shi, Xiongfei Li, and Xiaoli Zhang. "Wide aspect ratio matching for robust face detection." *Multimedia tools and applications* 82.7 (2023): 10535-10552.

12. Kurbanov Abduraxmon Alishboyevich. "Inson tanasi harakatlarini tahlil qilishda zamonaviy modellar va algoritmlarni qo'llashni o'rganish" *Al-Farg'oniy avlodlari*, no. 2, 2024, pp. 169-175. doi:10.5281/zenodo.114766561

13. Kurbanov A. Developing the learning experience: how affective computing systems revolutionize modern education // *Universum: технические науки: электрон. научн. журн.* 2024. 4(121). URL: <https://7universum.com/ru/tech/archive/item/17266>

14. Kurbanov, Abduraxmon. "Chuqur o'rganishga asoslangan yuz tahlili: xususiyatlarni ajratib olish va his-tuyg'ularni tushunish." *Международный Журнал Теоретических и Прикладных Вопросы Цифровых Технологий* (2024).

15. Kurbanov Abdurahmon Alishboyevich. Methods of evaluating a person's emotional state based on the analysis of textual data. // *Journal of actual problems of modern science, education and training*, pp 32-40. 2023.

16. KURBANOV A.A. Multimodal emotion recognition: a comprehensive survey with deep learning. // *Journal of Research and Innovation*, pp. 43-47. 2023

17. Kurbanov Abdurahmon Alishboyevich. A Methodological Approach to Understanding Emotional States Using Textual Data. // *Journal of Universal Science Research*. 2023

18. Kurbanov Abdurahmon. AI MODELS OF AFFECTIVE COMPUTING. / *International Conference of Contemporary Scientific and Technical Research*. 2023.



BIOMETRIK TEXNOLOGIYALARNI RIVOJLANTIRISHNING ISTIQBOLLI YO'NALISHLARI

Radjabov Sobirjon Sattorovich,

Texnika fanlari doktori,
Laboratoriya mudiri, Toshkent irrigatsiya va qishloq
xo'jaligini mexanizatsiyalash muhandislari instituti"
Milliy tadqiqot universiteti huzuridagi Fundamental
va amaliy tadqiqotlar instituti
e-mail: s_radjabov@yahoo.com

Rabbimov Ilyos Mehriddinovich,

Texnika fanlari bo'yicha falsafa doktori (PhD),
Yetakchi ilmiy xodim,
O'zbekiston Respublikasi Prezidenti
Administratsiyasi huzuridagi Iqtisodiy
tadqiqotlar va islohotlar markazi
e-mail: ilyos.rabbimov91@gmail.com

Xusainov Narimon Odilovich,

Texnika fanlari nomzodi,
Kafedra mudiri, "Temurbeklar maktabi"
harbiy akademik liseyi
e-mail: narimon.odilovich@gmail.com

Abdullayeva Barno Mo'yidinjon qizi,

Tayanch doktorant, Namangan davlat universiteti
e-mail: abm@gmail.com

Annotatsiya. Maqolada o'ziga xos xususiyatlari va qo'llanish doirasining kengligi tufayli jadal rivojlanayotgan biometrik texnologiyalarning so'nggi yutuqlari va kelajak istiqbollari muhokama qilinadi. Yurishni aniqlash, yuz termogrammasi, klaviatura zarbasi dinamikasi, quloq shakli va hidi kabi yangi biometrik texnologiyalarga alohida e'tibor qaratiladi. Ushbu texnologiyalarning har birining o'ziga xos afzalliklari va cheklovlari batafsil tahlil qilinadi. Bundan tashqari, maqolada identifikatsiyalash usullari va algoritmlarining rivojlanishi, ayniqsa chuqur o'qitish va Kolmogorov-Arnold Networks kabi yangi neyron tarmoq arxitekturalarini qo'llash kontekstida ko'rib chiqiladi. Ushbu innovatsion arxitekturaning afzalliklari va muammolari, shuningdek uning biometrik identifikatsiyani takomillashtirish imkoniyatlari muhokama qilinadi.

Maqolada, shuningdek, bir nechta biometrik texnologiyalar (multibiometriya), multimodal va multifaktorli tizimlarning integratsiyasi muhokama qilinadi. Turli xil biometrik ma'lumotlar va autentifikatsiya usullarining kombinatsiyasi identifikatsiyalashning aniqligi, ishonchliligi va xavfsizligini qanday oshirishi mumkinligi ko'rsatilgan.

Kalit so'zlar: biometrik texnologiyalar, multibiometriya, identifikatsiya, autentifikatsiya.

Kirish. So'nggi yillarda biometrik texnologiyalar jadal rivojlanmoqda, bu ularning qo'llanish sohasi kengayishi bilan izohlanadi. Buning sababi shundaki, insonning biometrik xususiyatlari qulay, noyob, soxtalashtirish deyarli mumkin emas,

unutish, yo'qotish yoki boshqa birovga o'tkazish mumkin emas.

Mordor Intelligence xalqaro konsalting kompaniyasi ma'lumotlariga ko'ra, 2024 yil oxiriga kelib biometrik tizimlar jahon bozori hajmi 51,15



milliard AQSh dollarini tashkil etadi. Prognozga ko'ra, keyingi 5 yil ichida biometrik texnologiyalar bozorining o'rtacha yillik o'sish sur'ati 15,3% ni tashkil etadi va 2029 yilga kelib bozorning bashorat qilinayotgan hajmi 104,22 milliard AQSh dollariga yetadi.

Ushbu texnologiyalarga bo'lgan ehtiyojning o'sishi bilan identifikatsiyalashning aniqligiga (ba'zi hollarda tezligiga ham) qo'yilgan talablar ham ortib bormoqda. Shu nuqtai nazardan, bizning fikrimizcha, biometrik texnologiyalarni rivojlantirishning eng ishtiroqchil yo'nalishlari quyidagilardir:

- yangi biometrik texnologiyalarni qo'llash;
- identifikatsiyalash usullari va algoritmlarini ishlab chiqish va takomillashtirish;
- bir nechta biometrik texnologiyalarni integratsiyalash (multibiometriya).

1. Yangi biometrik texnologiyalarni qo'llash.

Bir necha o'n yillar davomida biometrik texnologiyalarning imkoniyatlari cheklangan edi va ularning eng mashhur va keng qo'llaniladigan barmoq izlariga asoslangan texnologiya edi. Biroq, so'nggi o'n yillikda hisoblash va sensor texnologiyalari sohasidagi taraqqiyot tufayli, yurish (1-rasm), imo-ishoralalar, quloq shakli, hid va boshqa biometrik parametrlarning qo'llanilishi sezilarli darajada kengaydi.

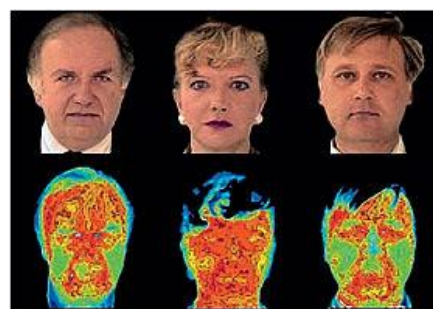
Bunday kengayishning bir misoli identifikatsiyalash uchun yurishdan foydalanishdir [1]. Videoyozuvlarda yorug'likning yetarli emasligi, bosh kiyimlar, niqoblar, bo'yanish va boshqa omillar tufayli odamning yuzi ko'pincha yashirin yoki ko'rish qiyin bo'lishi mumkin. Bunday hollarda yurish orqali identifikatsiyalash mumkin, tadqiqotlar shuni ko'rsatadiki, bu noyob parametr bo'lib, soxtalashtirish qiyin va ishonchliligi bo'yicha barmoq izlari yoki ko'z qorachig'ini skanerlash bilan solishtirish mumkin. Bu an'anaviy biometrik parametrlardan farqli o'laroq, yurishni uzoq masofadan va bevosita aloqasiz kuzatish mumkin. Biroq, baland poshnalar, noqulay poyabzal, og'ir narsalarni ko'tarish, tana qismlarini yashiradigan yoki harakatlarni cheklovchi kiyim va yurish tezligi kabi ko'plab omillar yurishning vizual ko'rinishini o'zgartirishi mumkin. Shuningdek, rakurs, yoritish va kamera parametrlari identifikatsiyalash aniqligiga

ta'sir qilishi mumkin. Shunday qilib, yurish bo'yicha identifikatsiyalash vazifasi unikal va murakkab bo'lib qolmoqda, zamonaviy kompyuter ko'rish usullaridagi yutuqlarga qaramay, bu usulning sifati va ishonchliligi hali yuz tanishga qaraganda pastroq.



1-rasm. Shaxsni yurishi orqali identifikatsiyalash

Biometrika sohasidagi so'nggi yutuqlardan biri termogrammalarni tuzish va tahlil qilish texnologiyasidir [2]. Olimlar infraqizil kameralar yordamida yuz terisi ostida joylashgan obyektlarning unikal tasvirini olish mumkinligini aniqladilar. Suyaklar, yog' to'qimalari va qon tomirlarining turli zichligi qat'iy individual bo'lib, foydalanuvchi yuzining termografik rasmini shakllantiradi. Yuz termogrammasi (2-rasm) noyobdir, bu hatto bir xil egizaklarni ham ishonchli farqlash imkonini beradi. Ushbu yondashuvning qo'shimcha afzalliklari uning har qanday kosmetik o'zgarishlarga, shu jumladan plastik jarrohlik va bo'yanishga chidamliligi va ro'yxatga olish jarayonining maxfiyligidir.



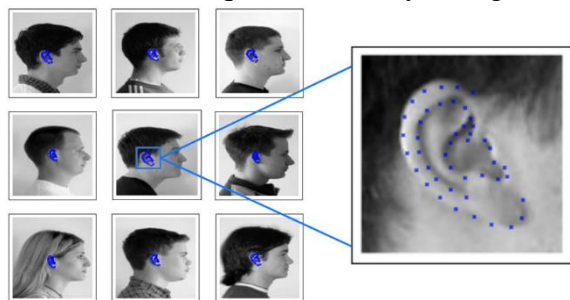
2-rasm. Shaxsni yuz termogrammasi orqali identifikatsiyalash

Klaviatura zarbasi dinamikasi yoki klaviatura dastxati foydalanuvchining ma'lum iboralarni yozish



usulini tahlil qiladi [3]. Klaviatura dastxatini aniqlashning ikki turi mavjud. Birinchisi, hisoblash resurslariga kirishda foydalanuvchini autentifikatsiya qilish uchun qo'llaniladi. Ikkinchisi esa, kirish huquqi berilgandan so'ng foydalanuvchi faolligini nazorat qilish uchun ishlatiladi va agar kompyuterda boshqa shaxs ishlayotgani aniqlansa, tizimni bloklaydi. Tadqiqotlar shuni ko'rsatdiki, klaviaturada ishlash ritmi foydalanuvchining individual xususiyati bo'lib, uni identifikatsiyalash va autentifikatsiya qilish uchun yaroqli hisoblanadi. Ritmi o'lchash uchun tugmacha zarbalari orasidagi vaqt oralig'i va tugmachalarni bosib turish vaqti baholanadi. Ikkinchi usul samaraliroq hisoblanishiga qaramasdan, eng yaxshi natijalar har ikkala usulni birgalikda qo'llash orqali erishiladi. Bu usulning o'ziga xos xususiyati uning arzonligidir, chunki klaviaturadan tashqari qo'shimcha jihozlar talab qilinmaydi. Biroq, ushbu texnologiya hali ishlab chiqilish bosqichida bo'lib, uning ishonchligini baholash qiyin, ayniqsa xavfsizlik tizimlariga qo'yiladigan yuqori talablarni hisobga olganda.

Quloq shaklini tahlil qilish biometrik identifikatsiyada (3-rasm) eng yangi yondashuvlardan biridir [3]. Hatto arzon veb-kamera ham taqqoslash va identifikatsiya uchun ishonchli namunalar taqdim etishi mumkin. Biroq soch va taqinchoqlar tizim samaradorligini pasaytirishi mumkin, bundan tashqari tashqi yoritish va yuzning kameraga nisbatan joylashuvi ham natijalarga ta'sir ko'rsatishi mumkin. Ushbu qiyinchiliklarga qaramay, mazkur texnologiya biometrik identifikatsiyalashning qimmatli vositasi hisoblanadi. Masalan, Gollandiyalik kriminologlar undan kuzatuv videosiga olingan talonchilikda gumonlanuvchilarni aniqlash uchun foydalananganlar.



3-rasm. Shaxsni quloq shaklini tahlili asosida identifikatsiyalash

Bundan tashqari, hidni aniqlash jarayonidan foydalanadigan "Elektron burun" tizimlari ishlab chiqilmoqda [3]. Tana hidiga genetik ta'sir bu xususiyatni biometrik autentifikatsiyalash uchun istiqbolli qiladi. Ushbu texnologiya, xuddi yurish va quloq shakli tahlili kabi, shaxsni identifikatsiyalashning zamonaviy biometrik texnologiyalariga qo'yiladigan talablarga javob bera olishi uchun sezilarli rivojlanishni talab qiladi.

2. Identifikatsiyalash usullari va algoritmlarini ishlab chiqish va takomillashtirish.

So'nggi yillarda shaxsni biometrik identifikatsiyalash masalalarini hal qilishda neyron tarmoqlarini o'qitishga asoslangan chuqur o'qitish usullari eng samarali natijalarni ko'rsatmoqda. Neyron tarmoqlar yordamida ajratib olinadigan belgilar ko'pincha yuqori darajadagi abstraktsiyaga ega bo'lib, sifatli tanib olish uchun muhimdir. Bu esa video va tasvirlarni tasniflash, tasvirlarni segmentatsiya qilish, obyektlarni aniqlash, vizual kuzatish va boshqa vazifalarda yuqori natijalarga erishish imkonini beradi.

Biroq, chuqur o'qitishning yutuqlariga qaramay, yurish uslubini aniqlash kabi ayrim vazifalarda, ma'lum ma'lumotlar to'plamlari uchun sayoz modellar hamon neyron tarmoqlardan ustun kelmoqda. Shu bilan birga, yondashuvlarning hech biri hali maqbul aniqlikka erishmadi.

Yaqinda MIT tadqiqotchilari ko'p qatlamli neyron tarmoqlarga (KQNT) muqobil variant – Kolmogorov-Arnold Networks (KAN) nomli yangi neyron tarmog'i arxitekturasini taqdim etishdi [4]. Ushbu arxitektura aktivatsiyalarni tarmoqning "Qirralari"ga ko'chirishni amalga oshiradi, bu uni an'anaviy neyron tarmoq yondashuvlaridan ajratib turadi.

Ishlab chiquvchilarning ta'kidlashicha, yangi turdagi neyron tarmoqlar bir qator afzalliklarga ega. KAN, KQNTdan farqli o'laroq, eski ma'lumotlarni unutmasdan yangi axborotni ishlash qobiliyatiga ega, bu esa modelni muntazam qayta o'qitish zaruratisiz o'z dolzarbligini saqlab qolish imkonini beradi.

Shuningdek, KAN yuqori aniqlik va interpretatsiya qilish imkoniyati bilan ajralib turadi va



ushbu xususiyatlari bilan u KQNTdan ustunlik qiladi. Bu innovatsion arxitektura nafaqat biroz yaxshiroq, balki murakkab dinamik masalalarni hal qilishda tamomila yangi imkoniyatlarga ega bo'lgan tarmoqlarni yaratishga asos bo'lishi mumkin.

KAN, KQNTga nisbatan neyronlarni mashtablashtirish uchun tezkor imkoniyatlarga ega. Biroq, ayrim muammolar ham mavjud – KATni o'qitish yuqori hisoblash quvvatlarini va/yoki ko'proq vaqt sarflashni talab etadi. Biroq, bu hal qilib bo'lmaydigan to'siq emas, chunki an'anaviy KQNT ham ularni qo'llashning butun davrida optimallashtirish va samaradorlikni oshirish orqali takomillashtirib kelingan.

Shunday qilib, KAT neyron tarmoq texnologiyalarini rivojlantirishda istiqbolli yo'nalish hisoblanadi. Bu yo'nalish sun'iy intellekt sohasidagi, xususan biometrik identifikatsiyalash kabi murakkab vazifalarni hal qilish samaradorligini sezilarli darajada oshirishi mumkin.

3. Bir nechta biometrik texnologiyalarni integratsiyalash (multibiometriya). Multibiometrik identifikatsiya deganda barmoq izlari, yuzni tanib olish, ovoz xususiyatlari va ko'z qorachig'i kabi bir nechta biometrik belgilardan foydalanish tushuniladi (4-rasm). Ushbu yondashuv identifikatsiyalashning aniqligini va ishonchliligini oshirish imkonini beradi, chunki turli biometrik parametrlardan olingan ma'lumotlar turli usullar yordamida, turli darajalarda va turli kontekstlarda birlashtirilishi mumkin.

Masalan, biometrik ma'lumotlar sensorlar darajasida, belgilarni ajratib olish darajasida yoki qaror qabul qilish darajasida birlashtirilishi mumkin. Bu esa ko'p pog'onali xavfsizlikni ta'minlaydi va identifikatsiyalash aniqligini oshiradi.



4-rasm. Multibiometrik identifikatsiyalash

Multibiometrik texnologiyalardan tashqari, multimodal va ko'p faktorli yechimlarni ular bilan bitta sinfga birlashtirish odatiy holdir. Multimodal tizimlarda insonning bir turdagi biometrik xususiyatlari (masalan, barmoq izlari) turli algoritmlar yordamida qayta ishlanadi. Bu tizimning ishonchliligini oshiradi hamda xatolarga va qalbakilashtirish urinishlariga bardoshliligini ta'minlaydi. Turli xil algoritmlar biometrik ma'lumotlarning turli jihatlarini aniqlashi mumkin, ular birgalikda shaxs haqida to'liqroq va aniqroq tasavvur beradi.

Boshqa tomondan, multifaktorli tizimlar biometrik belgilarni PIN-kodlar, parollar, smart-kartalar yoki tokenlar kabi boshqa autentifikatsiya usullari bilan birlashtiradi. Bu xavfsizlik darajasini sezilarli darajada oshiradi, chunki g'arazli shaxslarga kirish huquqini olish uchun bir nechta to'siqlarni yengib o'tish kerak bo'ladi. Multifaktorli tizimlar, shuningdek identifikatsiyalash jarayonini tezlashtirishi va markazlashtirilgan identifikator ma'lumotlar bazasiga murojaat qilmasdan tanib olish imkoniyatini ta'minlashi mumkin, bu maxfiylikni yaxshilash va ma'lumotlar sizib chiqishi xavfini kamaytirish uchun muhimdir.



5-rasm. Shaxsni barmoq izi va kirish kartasi orqali multifaktorli autentifikatsiyalash

Multifaktorli tizimlarni qo'llashning asosiy maqsadlari nafaqat identifikatsiyalash xavfsizligi va ishonchliligini oshirish, balki foydalanuvchi tajribasini yaxshilashni ham o'z ichiga oladi. Masalan, an'anaviy autentifikatsiyalash usullari bilan birgalikda biometrik ma'lumotlardan foydalanish turli xizmatlarga kirishni soddalashtirish, xatolar ehtimolini kamaytirish va



shaxsni tasdiqlash uchun zarur bo'lgan vaqtni qisqartirish imkonini beradi.

Shunday qilib, multibiometrik, multimodal va multifaktorli tizimlar bankdan tortib sog'liqni saqlash va davlat xavfsizligigacha bo'lgan turli sohalarda yanada xavfsiz, ishonchli va qulay identifikatsiyalash jarayonini ta'minlashga qaratilgan ilg'or yechimlardir.

Xulosa. Xulosa qilib aytganda, biometrik identifikatsiyalash tekshiruvning aniq, ishonchli va rad etib bo'lmaydigan natijalarini olish uchun beqiyosdir. Yaqin kelajakda parollar va PIN-kodlar o'rnini biometrik ma'lumotlarga asoslangan yangi, yanada ishonchli avtorizatsiya va autentifikatsiya usullari to'liq egallashi kutilmoqda. Bu nafaqat xavfsizlik darajasini oshiradi, balki identifikatsiyalash jarayonining qulayligi va tezligi tufayli foydalanuvchi tajribasini ham yaxshilaydi. Biometrik texnologiyalar allaqachon bank sektori, sog'liqni saqlash, davlat xavfsizligi va axborot texnologiyalari kabi turli sohalarda keng qo'llanilmoqda.

Bundan tashqari, biometrik identifikatsiyalash xavfsizlikning yangi standartlarini ishlab chiqilishiga turtki bo'ladi va axloqiy hamda shaxsiy daxlsizlik masalalariga e'tiborni jalb qiladi. Ushbu sohadagi texnologiyalar va metodologiyalarning doimiy takomillashtirilishi zamonaviy dunyo va kelajak talablariga javob beradigan yanada xavfsiz, ishonchli va qulay identifikatsiya tizimlarini yaratishga yordam beradi.

Xulosa qilib aytganda, biometrik identifikatsiyalash usullari hayotning turli sohalarida ma'lumotlarni himoyalash va xavfsizlikni ta'minlash yondashuvlarini tubdan o'zgartirishi kutilayotgan istiqbolli rivojlanish yo'nalishi hisoblanadi.

Foydalanilgan adabiyotlar ro'yxati

1. Йхапате М., Йхапате А.К. Идентификация человека по походке: Система, основанная на походке. – М.: Sciencia Scripts, 2023. – 64 с.
2. Михеев М. Ю., Гудков К. В., Астахова Т. Н., Макарова Е. Ю. Обработка информации в системе идентификации

по термограмме лица // Вестник НГИЭИ. – № 4 (71), 2017. – С. 7-15.

3. Ворона В.А. Биометрическая идентификация личности. – М.: Горячая линия – Телеком, 2022. – 228 с.
4. Liu Z., et al. KAN: Kolmogorov-Arnold Networks. arXiv preprint arXiv (2024): 2404.19756.



TARMOQ OQIMINI MONITORING QILISH DASTURIY TIZIMI

Jo'rayev Ma'ruf To'raqul o'g'li
O'zMU Jizzax filiali, tayanch doktoranti
juraevmaruff@gmail.com

Annotatsiya. Maqolada tarmoq monitoringi orqali ochiq va yopiq portlarni tekshirish, tarmoq trafiginini tahlil qilish va IP-manzillarni nazorat qilish imkoniyati muhokama qilinadi. Portni skanerlash tarmoqdagi tahdidlarni tezda aniqlash imkonini beradi. Bu tarmoq xavfsizligi va monitoringida keng qo'llaniladigan usul. Ochiq va yopiq portlarni aniqlash va tahlil qilish tarmoq administratorlari uchun juda muhimdir. Har bir portni skanerlash usuli o'ziga xos afzalliklarga ega. TCP orqali ochiq va yopiq portlarni aniqlash tarmoqni skanerlashning asosiy usullaridan biridir. TCP (Transmission Control Protocol) - tarmoq protokoli. Tarmoq tahdidlarini aniqlash xavflarni oldini olishning samarali usuli hisoblanadi.

Kalit so'zlar: port scan, tarmoq monitoring, port skanerlash, port, paket.

Kirish. Kompyuter tarmoqlari butun dunyo bo'ylab millionlab kompyuterlar va kompyuter foydalanuvchilarini bog'laydi. Kompyuter tarmog'ini to'g'ri boshqarish kerakligi juda muhimdir. Tarmoqni boshqarish monitoringni talab qiladi. Tarmoq monitoringi - tarmoq ma'murlariga murakkab kompyuter tarmog'ining lahzali holati va uzoq muddatli tendensiyalarini bilish imkonini beruvchi mexanizmlar to'plami hisoblanadi.

Tarmoqni kuzatish va o'lchash zamonaviy murakkab tarmoqda tobora muhim ahamiyat kasb etmoqda. Ilgari tarmoq admini faqat bir nechta tarmoq qurilmalarini yoki yuzdan kam kompyuterni kuzatishi mumkin edi. Tarmoq o'tkazish qobiliyati atigi 10 yoki 100 Mbit/s tashkil etardi, lekin endi tarmoq admini nafaqat yuqori tezlikdagi simli tarmoq (10 Gbit / s dan ortiq va ATM (Asynchronous Transfer Mode) tarmog'i), balki simsiz tarmoqlar bilan ham monitoring ishlarini olib borishi kerak. Masalan ular tarmoq tizimining barqarorligi va mavjudligini ta'minlash uchun, tarmoq muammolarini o'z vaqtida tuzatish yoki tarmoq ishlamay qolishining oldini olish, tarmoq xavfsizligi mustahkamligini ta'minlash va tarmoqni rejalashtirish bo'yicha to'g'ri qarorlar qabul qilish uchun yanada murakkab tarmoq trafiginini monitoring qilish va tahlil qilish vositalariga muhtoj.

Adabiyotlar tahlili va metodologiya. Tarmoq monitoringi tarmoq xavfsizligi va yaxlitligini ta'minlash maqsadida qo'llaniladigan bir nechta

usullarni o'z ichiga oladi. Monitoring bu monitoring apparat, dasturiy ta'minot, viruslar, josuslik dasturlari, va xavfsizlik zaifliklar va tarmoq yaxlitligini buzishi mumkin bo'lgan boshqa jihatlarni oldini olishga qaratilgan jarayondir. Monitoring qilishda ochiq va yopiq portlardan foydalanishda bir nechta samarali usullar mavjud [1].

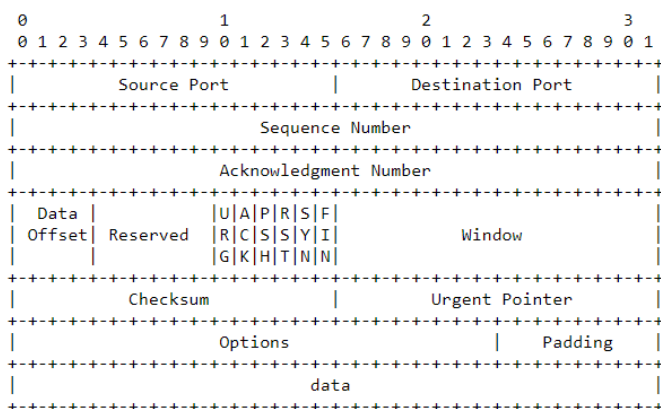
Portlarni skanerlash usullari:

- *TCP SYN Scan* SYN paketlari yordamida portlarning holatini aniqlovchi eng keng tarqalgan usuldur. "Half-open" skanerlash deb ham ataladi, chunki aloqa to'liq o'rnatilmaydi (ACK paketi yuborilmaydi).
- *TCP Connect Scan* "three-way handshake" ya'ni tekshirish to'liq o'tkaziladi. SYN → SYN/ACK → ACK jarayoni bajarilib, port ochiq bo'lsa, aloqa to'liq amalga oshiriladi. Yopiq port esa RST bilan javob beradi.
- *TCP FIN Scan* skanerlovchi qurilma yoki dastur serverga SYN emas, balki FIN (finish) paketi yuboradi. Ochiq port hech qanday javob bermaydi, yopiq port esa RST qaytaradi.
- *UDP Scan* TCP o'rniga UDP (User Datagram Protocol) skanerlashdan foydalaniladi. UDP skanerlash TCP kabi aniq javob bermaydi, chunki u "connectionless" protokol hisoblanadi. UDP skanerlash TCP skanerlashga qaraganda sekinroq ishlaydi.



- *Window Scan* Window skanerlash TCP SYN yoki ACK paketlariga javobdagi window sizeni tahlil qilish orqali portlarning ochiq yoki yopiq ekanligini aniqlaydi [2].

Portlarni skanerlashda yuqorida berilgan usullardan farqli usullar ham mavjud, 1-rasmda portlarni skanerlashda paket ma'lumotlari tuzilishini ko'rish orqali yanada tushunarli tahlil qilinadi.



1-rasm. Paket ma'lumot tuzilishi

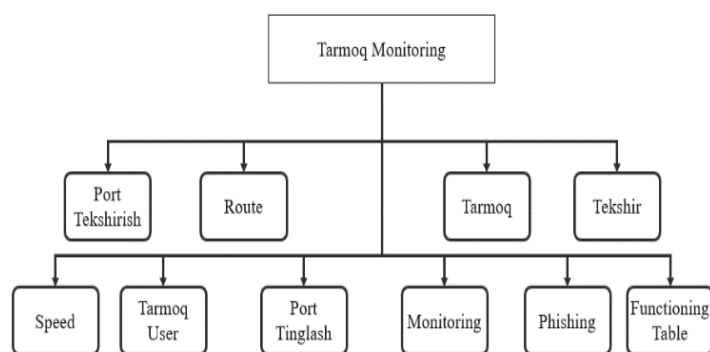
Tadqiqot uchun TCP Connect Scan usulidan foydalanildi, chunki bu usul “three-way handshake” hisoblanib tekshirish to‘liq o‘tkaziladi [3].

Natijalar. Tarmoq monitoringi tarmoq boshqaruvchisi ishining muhim qismi bo‘lgan qiyin va mashaqqatli vazifadir. Tarmoq ma'murlari doimiy ravishda o‘z tarmoqlarining uzluksiz ishlashini ta'minlashga intilishadi. Tarmoq nosozliklari yuzaga kelganda, monitoring dasturlari tarmoqdagi nosozliklarni aniqlashi, ajratishi va tuzatishi va ehtimol nosozlikni tiklashi kerak.

Tarmoq monitoring qilishda 2-rasm misolida ko‘rib chiqiladi. Struktura ko‘rinishi quyidagilardan tashkil topgan:

- Port Tekshirish – tarmoqqa ulangan kompyuterlarni ochiq va yopiq portlarni tekshirish;
- Route – tarmoqqa ulangan mavjud qurilmaning ip adres, maska va tarmoq kartasi ma'lumotlarini taqdim etish;
- Tarmoq – paket ma'lumotlarini olish uchun foydalanilinish;

- Tekshir – paketdan yozib olingan ma'lumotlarni tahlil qilish;
- Speed – tarmoqdan kirib kelayotgan va chiqib ketayotgan ma'lumotlar tezligini aniqlash va internet tezligini aniqlash;
- Tarmoq User – tarmoqda mavjud online va offline qurilmalari haqida ma'lumot berish;
- Port Tinglash – kompyuterda real vaqtda ishlab turgan xizmatlar ro'yxati va ularning holatini taqdim etish;
- Monitoring – tarmoqdagi ma'lumotlar almashinuv jarayoni grafik tasviri, protokollar bo'yicha ma'lumotlar hajmi, ip adreslar bo'yicha ma'lumotlar almashinuv miqdori va tarmoqdan o'tuvchi ma'lumotlar sturukturasini aniqlash;
- Phishing – murojaat qilinuvchi url manzillarning zararli ekanligini aniqlash;
- Functioning Table – axborot xavfsizligi va tahdidlarni aniqlash va bartaraf qilishning imitatsion modellashtirish



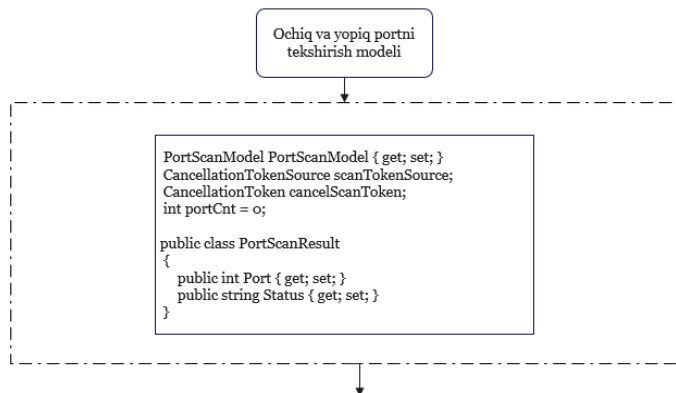
2-rasm. Tarmoq monitoring strukturasi

Ochiq va yopiq portni aniqlashda TCP Connect Scan usuli tanlab olindi. Chunki boshqa usullarga qaraganda ancha samarali hisoblanadi. Portlarni umumiy soni $2^{16} - 1$ ya'ni 65535 taga teng. Aslida ularning soni 65536 ta lekin 0 port umumiy foydalanish uchun ishlatilmaydi. Portlar 3 turga bo‘linadi [4].



- 0, ..., 1023 tizim yoki taniqli portlar.
- 1024, ... , 49151 foydalanuvchi yoki ro‘yxatdan o‘tgan portlar.
- 49152, ... , 65535 dinamik, shaxsiy yoki vaqtinchalik portlar.

Yaratilgan dasturda Port Tershish qismi aynan shu portlarni tekshirish uchun xizmat qiladi.



3-rasm. Ochiq va yopiq portni tekshirish modeli

3-rasmda berilgan ip manzilning ochiq va yopiq portlari tekshiriladi. Bunda tekshirish uchun IP ip manzili, P portlar to‘plami p_i port raqami,

$$P = \{p_0, p_1, \dots, p_n\}$$

portlar intervali $0 \leq n \leq 65535$ oraliqda hamma portlar tekshirib chiqiladi.

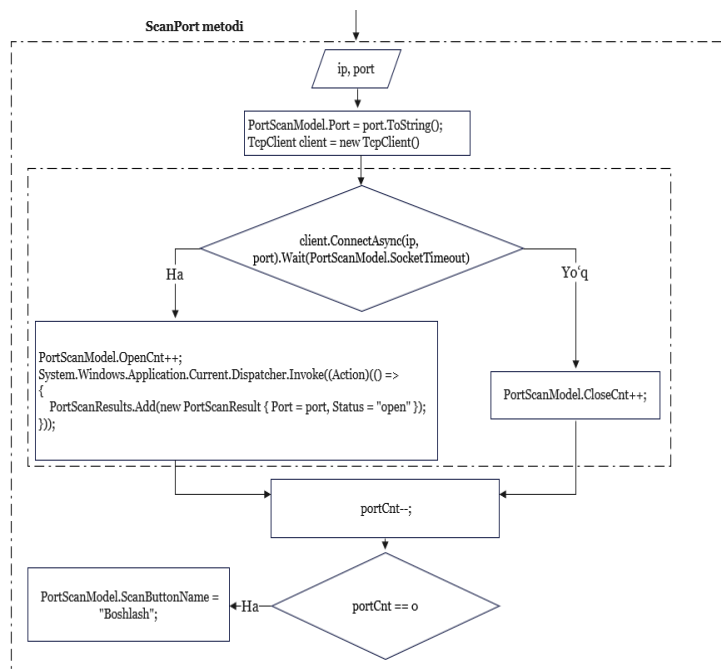
$$S(IP, p_i) \rightarrow true \text{ yoki } false$$

S port skanerlash funksiyasi;

$portCnt = 0$ tekshirilgan portlar soni aniqlash uchun foydalaniladi.

$Port$ aniqlangan ochiq port raqamini chiqarish uchun foydalaniladi.

$Status$ aniqlangan ochiq portga status beriladi.



4-rasm. ScanPort metodi

ScanPort metodi tekshirish uchun berilgan ip manzilini $port$ larni tekshirish, ochiq va yopiq port hisobini yuritadi [5]. Tekshirish qayta amalga oshirilganda esa jayaron boshidan boshlanadi.

$$O = \{p_i \in P \mid S(IP, p_i) = true\}$$

O ochiq portlar to‘plami.

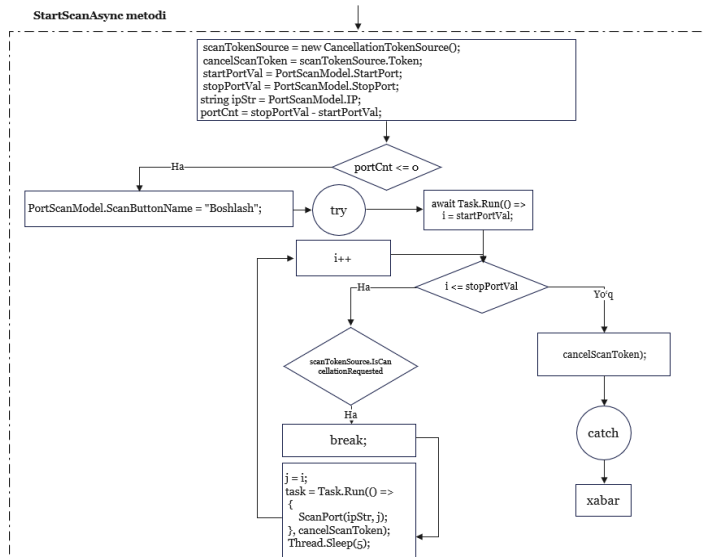
$$Y = \{p_i \in P \mid S(IP, p_i) = false\}$$

Y yopiq portlar to‘plami.

- $OpenCnt$ ochiq port sonini hisoblaydi. Har safar yangi ochiq port aniqlansa 1 qiymati qo‘shiladi.
- $CloseCnt$ yopiq port sonini hisoblaydi. Har safar yangi yopiq port aniqlansa 1 qiymati qo‘shiladi.

ScanPort metodi asosan ochiq va yopiq port sonini hisoblaydi. Bunda berilgan ip manzilini portga murojaat qiladi va murojaat amalga oshsa ochiq portlar soni bittaga [6] oshadi. Aks holda yopiq portlar soni bittaga oshadi. Natijalar PortScanResultga yuboriladi.





5-rasm. StartScanAsync metodi

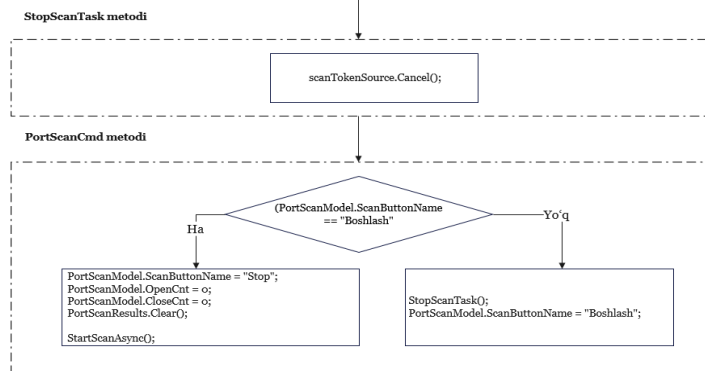
StartScanAsync metodi oraliq interval bo‘yicha berilgan ip manzil bo‘yicha $0 \leq n \leq 65535$ oraliqda ketshirish boshlaydi.

$$O = \{p_i \in [P_{start}, P_{end}] \mid S(IP, p) = true\}$$

p_i ochiq port va O to‘plamga tegishli.

$$Y = \{p_i \in [P_{start}, P_{end}] \mid S(IP, p) = false\}$$

p_i ochiq port va Y to‘plamga tegishli.



6-rasm. StopScanTask va PortScanCmd metodi

StopScanTask va PortScanCmd metodi dastur ishga tushirish va to‘xtatish uchun foydalaniladi.

Dasturiy ta‘minotdan olingan natija TCP Connect Scan usuli samarali ekanligini tasdiqladi (7-rasmga qarang). Tekshirilgan portlarning umumiy soni 8182 ta shundan ochiq portlar 4 ta va yopiq portlar 8177 tani tashkil etdi. Topilgan ochiq portlar raqami ham keltirildi.

1. 135 port windows muhitida mijozlar va serverlar o‘rtasida masofaviy aloqani ta‘minlaydi
2. 139 port ikki qurilma o‘rtasida tarmoqdagi fayllar va printerlarni almashishda NetBIOS orqali SMB seans xizmatiga ruxsat beradi.
3. 445 port server xabar bloki (SMB) protokoliga bag‘ishlangan bo‘lib, u TCP yordamida tarmoq Ichida fayllar va printerlar kabi resurslarni almashish imkoniyatini taqdim etadi.
4. 5040 port Microsoft HTTPAPI xizmatiga tegishlidir.

Port Tekshirish		Port	Status
IP va Port Sozlamasi		135	open
IP Address: 192.168.137.4		139	open
Start Port: 1		445	open
End Port: 65535		5040	open
Socket Timeout(ms): 1000			
Boshlash			
Statistika			
Tekshirilgan	8182		
Ochiq	4		
Yopiq	8177		

7-rasm. Dasturiy ta‘minotdan olingan natija

Xulosa. Tarmoq monitoringi va portlarni skanerlash texnikalari batafsil ko‘rib chiqildi. Tarmoq xavfsizligini ta‘minlash va mavjud xavflarni aniqlashda monitoring jarayoni muhim o‘rin tutadi. TCP Connect Scan kabi port skanerlash usullari tahlilidan ochiq va yopiq portlarni aniqlash, tarmoq boshqaruvchilari uchun asosiy vazifalardan biri hisoblanadi. Bu usullar tarmoqdagi zaifliklarni aniqlash, tahdidlarni tezkor aniqlash va ularni bartaraf etishga imkon beradi. Tadqiqot natijalari TCP Connect Scan usulining samarali ekanligini taqdim qildi, chunki u tarmoqning portlarini to‘liq tekshirish va ochiq portlarni aniqlashda ishonchli natijalar beradi. Kelgusida tarmoq monitoringi va portlarni skanerlash bo‘yicha yanada rivojlangan usullardan foydalanish, tarmoq xavfsizligini yanada mustahkamlashga yordam beradi.



Foydalanilgan adabiyotlar

1. Park, Seongchul & Kim, Juntae. (2017). A Study on Risk Index to Analyze the Impact of Port Scan and to Detect Slow Port Scan in Network Intrusion Detection. *Advanced Science Letters*. 23. 10329-10336. 10.1166/asl.2017.10446.
2. Vivo, Marco & Ke, Le & Isern, Germinal & Vivo, Gabriela. (1999). A review of port scanning techniques. *Computer Communication Review*. 29. 41-48. 10.1145/505733.505737.
3. Mirza, Ali. (2023). Port Scanning: Techniques, Tools and Detection. 10.31224/3053.
4. Bhuyan, Monowar & Bhattacharyya, Dhruva K & Kalita, Jugal. (2011). Surveying Port Scans and Their Detection Methodologies. *The Computer Journal*. 54. 1565-1581. 10.1093/comjnl/bxr035.
5. Majed, Hussein & Noura, Hassan & Salman, Ola & Chehab, Ali & Couturier, Raphaël. (2021). Efficient and Secure Statistical Port Scan Detection Scheme. 10.1007/978-3-030-67550-9_6.
6. S. Balram and M. Wisecy. Detection of tcp syn scanning using packet counts and neural network. In 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, pages 646–649, 2008.



ELEKTRON POCHTA TIZIMI XAVFSIZLIGI RISKLARINI BAHOLASH USULI

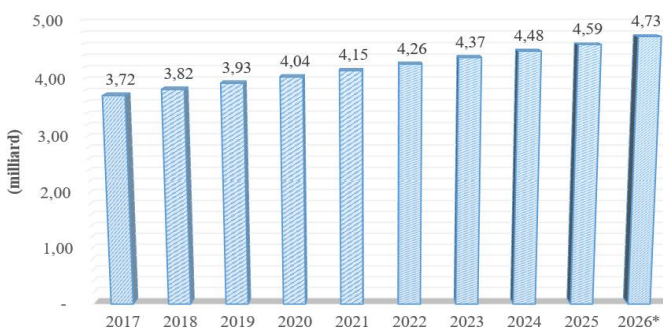
Ganiyev Salim Karimovich,
texnika fanlari doktori, professori,
Muhammad al-Xorazmiy nomidagi TATU
Axborot xavfsizligi kafedrasida
sharofidinov1990@gmail.com

Xamidov Sherzod Jaloldin o'g'li,
tayanch-doktorant
Muhammad al-Xorazmiy nomidagi TATU,
sherzod.hamidov@tuit.uz

Annotatsiya. Elektron pochta aloqaning muhim usullaridan biri bo'lib qolmoqda. Elektron pochta xavfsizligi bilan bog'liq muammolar soni va ko'lami keskin oshib bormoqda. Tashkilot va korxonalar uchun elektron pochta tizimining xavfsizligini ta'minlash hozirgi kunda juda muhim. Elektron pochta xavfsizligi risklarini baholash tizimni himoya qilishda eng muhim bosqichlardan biri hisoblanadi, bu o'z navbatida xavflarni aniqlash, yuzaga kelish ehtimolini va ta'sirini baholash hamda zaruriy choralarni amalga oshirish imkonini beradi.

Kalit so'zlar: nomaqbul xabarlar, spam, fishing, zararli qo'yilmalar, korporativ elektron pochta obro'sizlantirish, risk.

KIRISH. Zamonaviy axborot-kommunikatsiya tizimlarining jadal sur'atlar bilan rivojlanishi va tatbiq etilishi, odamlar uchun ulkan imkoniyatlarni taqdim etdi, shu bilan birga ular axborot xavfsizligi nuqtai nazaridan ham katta xavflarni yuzaga keltirmoqda. Bugungi kunda xabar almashish platformalari va ilovalarining yaratilishi hamda rivojlanishiga qaramay, elektron pochta tizimi aloqa infratuzilmasi uchun ma'lumotni uzatish va konfidensial axborotni almashishning muhim vositalaridan biri bo'lib qolmoqda. Internet servislari ko'lamini ortishi bilan birgalikda, dunyo bo'ylab elektron pochta foydalanuvchilarining soni oshib bormoqda [1] (1.1-rasm).



1.1 – rasm. Butun dunyo bo'ylab elektron pochta foydalanuvchilari soni (2017-2026 yillar)

Biroq, uning keng tarqalganligi bilan bir qatorda, xavfsizlik tahdidlari yanada keskinlashib tobora murakkablashib bormoqda va undan foydalanish tashkilotlar uchun eng katta risklardan biri bo'lib qolmoqda.

Elektron pochta bugungi kunda faqat muloqot qilish uchun emas, balki onlayn servislarda ro'yxatdan o'tish va turli tizimlardan foydalanish huquqini olish uchun qo'llanilmoqda.

Xavfsizlik tizimidagi kamchiliklar sabab elektron pochta kiberxujumlarni amalga oshirishda suqilib kirish nuqtasi va kiberjinoyatchilarning keyingi nishoniga aylanmoqda.

ELEKTRON POCHTA XAVFSIZLIGI RISKLARI. Kiberjinoyatchilar elektron pochtdan ma'lumotlarni o'g'irlash va soxtalashtirish, firibgarlik xabarlarini va zararli dasturlarni tarqatishning samarali usuli sifatida foydalanmoqdalar. Elektron pochta xavfsizligi bugungi kunda har qachongidan ham muhim bo'lib bormoqda. Keng tarqalgan kiberhujumlarni amalga oshirishda elektron pochta asosiy vosita bo'lib xizmat qilmoqda. Quyida so'ngi

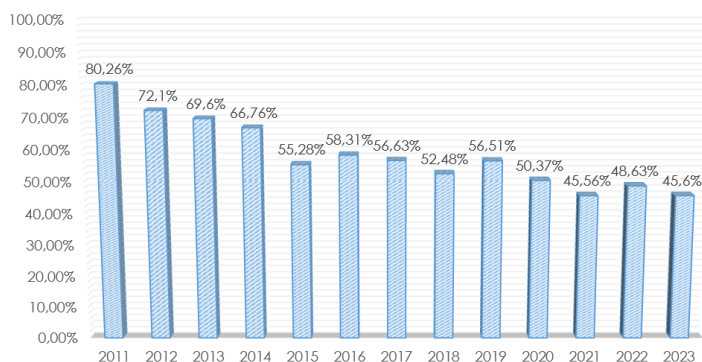


yillardagi statistik ma'lumotlarga asoslanib, elektron pochta xavfsizligidagi asosiy risklar tahlil qilinadi.

Nomaqbul xabarlar - foydalanuvchilarning ma'lum soniga ularning roziligisiz tijoriy, firibgarlik yoki zararli mazmunda jo'natiladigan elektron pochta xatlari. Elektron pochta spam xabarlari zamonaviy axborot kommunikatsiya infrastrukturasi eng dolzarb muammolardan biri. Nomaqbul xabarlar tarmoqning o'tkazish qobiliyatini sarflab foydalanuvchilarning pochta qutilarida joy egallaydi va haqiqiy elektron xatlarning kirib kelishiga to'sqinlik qiladi, shu bilan birgalikda butun tarmoq tizimi resurslarining haddan tashqari yuklanishiga olib keladi, bu esa elektron pochta xizmatlari va aloqa kanallarining uzluksiz ishlashiga salbiy ta'sir ko'rsatadi. Spam xabarlar elektron pochta tizimiga ta'sir etuvchi quyidagi risklarni yuzaga keltiradi:

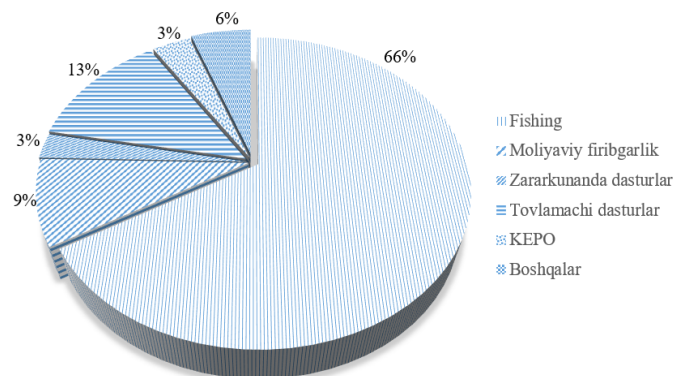
- ishchi stansiyalarni zararkunanda dasturlar yordamida zararlanishi (viruslar, qurtlar va troyan dasturlar);
- kiruvchi ko'p sonli nomaqbul xabarlar oqibatida tarmoqning o'tkazish qobiliyatining yuklanishi;
- ma'lumotlar va hisoblash resurslari saqlanuvchi makondan noto'g'ri foydalanish;
- moliyaviy firibgarliklar (fishing va u bilan bog'liq boshqa xujumlar natijasida moliyaviy yo'qotishlar) [2].

Dunyo pochta trafigida nomaqbul elektron xabarlarning o'rtacha ulushi 1.2-rasmda keltirilgan.



1.2-rasm. Dunyo pochta trafigida nomaqbul elektron xabarlarning o'rtacha ulushi (2011-2023 yillar)

Butun dunyona elektron pochta tizimlari xavfsizligidagi asosiy muommolardan biri hisoblanib, zararli dasturlar tarqalishining asosiy yo'nalishi biri bo'lib qolmoqda. Spam-xabarlar har xil turlari mavjud, ular foydalanuvchi qurilmalarini zararlash va ishdan chiqarishga qaratiladi. Ushbu turdagi xabarlardan ko'plab hujumlarni amalga oshirishda foydalaniladi. Ular orasida, fishing xujumi niyati buzuqlar tomonidan qo'llaniladigan xavfli usul bo'lib, barcha xujumlarning uchdan ikki qismini tashkil qilmoqda. Keng tarqalgan nomaqbul xabarlar turlari bo'yicha statistikasi 1.3-rasmda keltirilgan.



1.3 – rasm. Nomaqbul xabarlar turlari bo'yicha statistikasi

Fishing xabarlar

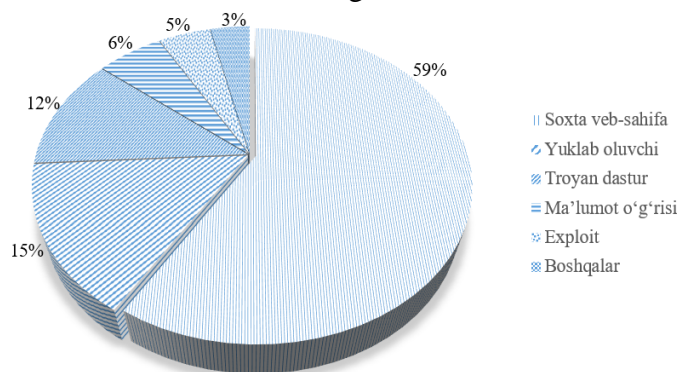
Ijtimoiy muhandislik usullaridan foydalangan holda amalga oshiriladigan xujumlarning eng keng tarqalgan shakllaridan biri bo'lib, kiberxavfsizlik sohasidagi ko'plab insidentlar fishing xabarlaridan boshlanadi. Fishing xujumidan asosiy maqsad foydalanuvchining muhim (tizim qayd yozuvlari va shaxsiy parollar, moliyaviy hisob raqamlar) ma'lumotlarini yig'adigan soxta va zararli veb-sahifaga yo'naltirish, kiritilgan ma'lumotlarni niyati buzuq tomonidan belgilangan manzilga yuborishdan iborat. Elektron pochta fishing xujumning ko'plab turlari mavjud, ular quyidagi qadamlar orqali amalga oshiriladi:

- tarkibida havola yoki yuklab oluvchi bo'lgan firibgarlik elektron xati yaratiladi;
- tegishli vosita yordamida jabrlanuvchiga xat jo'natiladi;



- havola foydalanuvchini firibgarlik veb-sahifasiga yoki zaruriy dasturni yuklashga yo‘naltiradi;
- veb-sahifa foydalanuvchidan maxfiy va qayd yozuvi ma‘lumotlarini kiritishni yoki dasturni yuklab o‘rnatishni so‘raydi. Ushbu ma‘lumotlar niyati buzuq tomonidan yig‘iladi va shu bilan keyingi xujumlarda foydalaniladi [3].

Fishing xabarlarining turlari bo‘yicha statistikasi 1.4-rasmda keltirilgan.



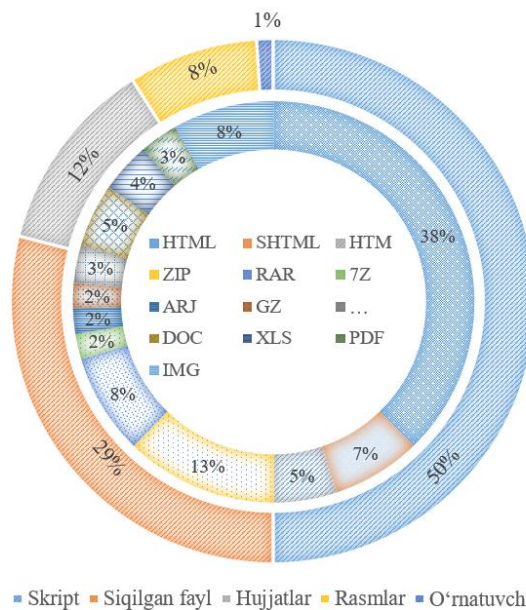
1.4 – rasm. Fishing xabarlarni turlari bo‘yicha statistikasi

Zararli qo‘yilmalar

Bugungi kunda elektron pochta zararli qo‘yilmalari zararkunanda dasturlarni tarqatishning eng keng tarqalgan usullaridan biri bo‘lib foydalanuvchi kompyuteriga hujum qilish uchun mo‘ljallangan. Ushbu elektron xatlar, tarkibidagi zararli qo‘yilmalar, xujjatlar elektron fayllar tusida niqoblangan bo‘lishi mumkin. Deyarli har qanday turdagi fayl elektron pochtaga biriktirilishi mumkin, shuning uchun kiberjinoatchilar ma‘lumotlarni yo‘qotish yoki o‘g‘irlash imkoniga ega zararli dasturlarni o‘rnata oluvchi fayllarni ushbu elektron xatlarga biriktiradilar.

Elektron pochta tarkibida ko‘rish yoki chop etish uchun yuklab olishni taklif qiluvchi fayl mavjud bo‘ladi. Foydalanuvchi faylni ochganida biriktirilgan skriptlar, makroslar yoki tizim zaifliklari avtomatik ravishda ishga tushadi hamda kompyuterga troyan yoki viruslarni masofadan yuklab oladi va ishga tushiradi. Zararkunanda dasturlar turli xil va murakkab ko‘rinishda bo‘lib, ular ma‘lumotlarga zarar yetkazishi

(o‘chirib yuborishi, shifrlashi), masofadan ulanishga ruxsat berishi, ishchi stansiyaning to‘liq yoki qisman ishdan chiqarishi hamda blokirovkalashi mumkin [4]. Zararli qo‘yilmalarning keng tarqalgan turlari 1.5-rasmda ko‘rsatilgan.



1.5 – rasm. Zararli qo‘yilmalarning turlari bo‘yicha statistikasi

Korporativ elektron pochta obro‘sizlantirish (BEC- business email compromise) - maqsadli kiberhujum turi bo‘lib, kiberjinoatchi o‘zini ishonchli shaxs (kompaniyaning vakolatli vakili) sifatida ko‘rsatadi va maxfiy ma‘lumotlarni taqdim etish uchun elektron pochta xabarlarini muayyan shaxslar(kompaniya hodimlari yoki hamkorlari)ga yuboradi. Mazkur turdagi hujum quyidagi qadamlar orqali amalga oshiriladi:

- kompaniyaning faoliyati va boshqaruv strukturasi xususida ma‘lumot to‘plash;
- kompaniyaning vakolatli vakilining elektron pochta qayd yozuvi ma‘lumotlarini olish uchun maqsadli hujum qilish;
- elektron pochta qayd yozuvidan vakolatli hodimlarga ishonchli shaxs nomidan xabar yuborish [5].

RISKLARNI BAHOLASH USULI

Elektron pochta tizimi xavfsizligi bilan bog‘liq risklarni baholash, elektron pochta himoyalash



vositalarida mavjud kamchiliklarni aniqlash va kiberhujumlarni oldini olish uchun zarur bo'lgan ma'lumotlarni taqdim etadi.

Yuqorida keltirilgan risklarni (1.1) formula yordamida baxolash mumkin. Ushbu formula 10 dan 50 gacha oralig'dagi qiymatni beradi. Qolgan beshta parametr va ularning har biri uchun reyting shkalasi 1.4-jadvalda keltirilgan.

$$R_i = MA_i * 1 + FQ_i * 2 + CH_i * 3 + T_i * 4 \quad (i = 1, 2, \dots, n) \quad (1.1)$$

bu yerda:

R_i - riskning umumiy reytingi;

MA_i - aniqlash murakkabligi;

FQ_i - foydalanishda qulayligi;

CH_i - chastotasi;

T_i - tizim xavfsizligiga ta'siri;

Aniqlash murakkabligi: tarmoq ma'muri tomonidan hujumni aniqlashdagi taxminiy qiyinchiliklarni belgilaydi. (1 = aniqlash deyarli ahamiyatsiz; 5 = aniqlash deyarli mumkin emas).

Foydalanish qulayligi: hujumni amalga oshirish qanchalik qiyinligini belgilaydi. (1 = yuqori malaka va ko'nikmalar; 5 = skript yozish qobiliyati);

Chastotasi: hujum tarmoqning himoyalangan qismida qanchalik tez-tez sodir bo'lishini belgilaydi. (1 = hujum deyarli uchramaydi; 5 = yirik korxonalar tarmoqlari har kuni hujumga duchor keladi).

Ta'sir: muvaffaqiyatli hujum natijasida yetkazilgan zararni belgilaydi. (1 = deyarli hech qanday ta'sir ko'rsatmaydi; 5 = har qanday holatda tizim sozlamalarini o'zgartirgan ma'qul) [6].

1.3 – jadval.

Risklarni baholash jadvali

Risk	Aniqlash murakkabligi	Foydalanishda qulayligi	Chastotasi	Tizim xavfsizligiga ta'siri	Riskning umumiy reytingi
Nomaqbul-xabarlar	4	4	5	4	43
Fishing	5	3	5	4	42
Zararli qo'yilmalar	5	2	4	5	41
BEC	5	3	4	4	39

XULOSA. Elektron pochta tizimi risklari tashkilot va korxonalarda axborot xavfsizligini

ta'minlashda asosiy muammolarni yuzaga keltiradi hamda axborot tizimiga qaratilgan hujumlarni amalga oshirish uchun boshlang'ich nuqta bo'lib xizmat qiladi. Yuqorida elektron pohta tizimi xavfsizligi risklari tahlil qilindi va baholash amalga oshirildi. Baholash natijalari yuzaga keladigan tahdid va hujumlarni oldindan aniqlash himoya mexanizmlarini qurishga va yaxshilashga, hamda ularga qarshi choralar ishlab chiqishga imkon beradi.

FOYDALANILGAN ADABIYOTLAR.

- Email Statistics Report, 2021-2025. The Radicati Group, Reproduction Prohibited.
- Хамидов Ш.Ж. Применение искусственного интеллекта для фильтрации спам-сообщений в электронной почте. Электронный сборник научных статей по материалам XII Международной научно-технической конференции «Энергетика, инфокоммуникационные технологии и высшее образование», Алматы-Казань, 20-21 октября 2022. - 611-620 с.
- Ганиев С. К., Хамидов Ш. Ж. Безопасность систем электронной почты: проблемы и решения. Электронный сборник научных статей по материалам XXI Международной научно-методической конференции «Информатика: проблемы, методы, технологии», Воронеж, 11-12 февраля 2021. - 690-699 с.
- Muralidharan T., Nissim N. Improving malicious email detection through novel designated deep-learning architectures utilizing entire email. Neural Networks Vol. 157, January 2023, pp. 257-279.
- Papathanasiou, A., Lontos, G., Liagkou, V., Glavas, E. Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures. A Perspective on the Greek Landscape. J. Cybersecur. Priv., Vol. 3, Iss. 3. September 2023, 3, pp 610–637.
- Raja S.H., Afrooz F. New method for assessing risks of email. International Conference on Graphic and Image Processing (ICGIP 2012), Proceedings of the SPIE. Vol. 8768, pp 6.



МЕТОДЫ И АЛГОРИТМЫ ХРАНЕНИЯ ФАЙЛОВ ДЛЯ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ РАЗЛИЧНЫМИ ТИПАМИ ДАННЫХ

Кенжаев Санжар Собирович,
Докторант Самаркандского
государственного университета,
s.kenjayev22@gmail.com

Рашидов Акбар Эргаш угли,
Доктор философии технических наук (PhD),
Самаркандский государственный университет
Заведующий кафедрой искусственного
интеллекта и информационных систем
researcher.are@gmail.com

Аннотация: Важно выбрать подходящие методы работы для типа данных. Успешное применение алгоритмов управления базами данных на основе задач, почти полностью зависит от доступности данных. И чем больше объем этих данных, тем лучше результаты работы алгоритмов. Существующие подходы в управлении данными работающие на уровне блочных, файловых и объектных указывает что имеется много нерешённых задач по работе над разнородными данными. Данная статья посвящена решению этой проблемы. Предложен метод оптимизации работы с различными типами данных на уровнях сбора, хранения, обработки и передачи данных.

Ключевые слова: блочные хранилища, файловые хранилища, SAN, NAS, оптимальное управление файлами

Введение. В современном информационном мире эффективное управление файлами в частности хранение и обработка является одним из важнейших факторов обеспечения качества получаемой информации. В процессе разработки информационных систем, особенно с использованием больших объемов данных, важно выбирать эффективные методы сбора, хранения и обработки данных, обеспечивающие целостность, доступность и безопасность этих данных [1-3]. Хранение файлов в системах управления данными требует тщательного учета таких факторов, как объем данных, шаблоны доступа, требования безопасности и масштабируемости. Используя, выбранные методы хранения и комплексно интегрируя их с системами управления данными, пользователи могут обеспечить оптимальное хранение, управление и доступ к своим файлам. Методами классификации данных можно быстро

определить, где они хранятся, чем эти данные являются и для каких операций используются. В настоящее время одним из основных параметров эффективной организации процесса работы с файловыми данными является правильный выбор типов файлов и структуры данных [4,5]. В результате увеличения объёма генерируемых данных, разнообразия типов файлов и создания различных форматов хранения файлов закономерно возникает проблема временной сложности обработки данных с физической точки зрения [6-9]. Кроме того, существует проблема растущих требований к большим наборам данных и распространения типов файлов, что приводит к неструктурированности многих современных технологий искусственного интеллекта. Во многих случаях, такие проблемы приводят к критической точке временной сложности [10]. При работе с большими объемами данных широко применяется



использование иерархических (HSP) и распределенных технологий для поиска решений большинства проблем неструктурированных данных [4]. Выбор использования различных технологий зависит от цели поставленной задачи, что позволяет добиться оптимального решения проблемных вопросов.

При использовании технологий хранения информации для анализа больших данных необходимо уделять внимание не только алгоритмам анализа, но и всем этапам работы с данными, включая сбор, агрегацию, анализ и визуализацию данных. На каждом этапе возникают своего рода вопросы оптимизации процесса, особенно по мере увеличения степени неоднородности.

Цель исследования - повысить доступность разнообразия, анализ и визуализации данных в системах управления базами данных посредством использования технологий гибридного хранения как часть более широкого процесса, такого как миграция или интеграция данных. Этот процесс включает в себя извлечение данных из таких источников как базы данных, файлы, а также веб-сервисы, их преобразование и загрузку в нужную целевую систему.

Для достижения поставленной цели решаются следующие задачи:

1. Изучены архитектурные особенности и способы хранения информации в файловых системах и облачных хранилищах.
2. Рассматриваются и сравниваются различные методы и технологии управления данными.
3. Вероятностные модели решения задач при работе с неструктурированными данными.

С учетом закономерностей и недостатков, выявленных на основе проанализированных исследований, определены, систематизированы и показаны преимущества гибридных технологий хранения данных в контексте повышения эффективности нереляционных баз данных. [1]

Хранение данных в файловых системах и облачных хранилищах

Существует три способа хранения данных: блочный, файловый и объектный вид. Они организуют и представляют данные по-разному, и каждый из них имеет свои возможности и ограничения. Ниже рассмотрим основные преимущества и недостатки этих методов:

1. Блочное хранилище. За счет хранения данных блочным способом достигается максимальная скорость реагирования на запросы, а также изменения части данных, кроме того, так как не используются специальные приложения, не теряется время на такие задачи, как передача данных из одного формата другому. Это связано с тем, что основной принцип хранения данных в блочной форме заключается в разделении их на блоки предопределённого одинакового размера, доступ к которым и управление ими осуществляется так же, как и на отдельных дисках. Для операционных систем это низкоуровневый тип доступа к дискам, установленным непосредственно на сервере, без использования промежуточного преобразования и смешивания данных.

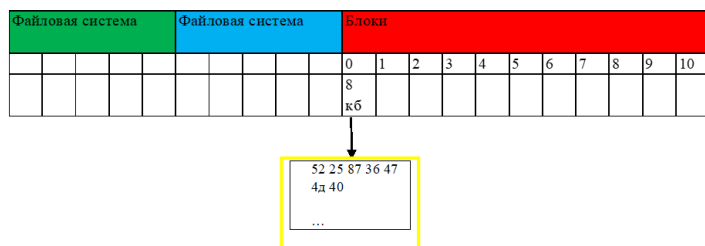


Рисунок 1. Хранение данных в ячейках в виде блоков.

Адресация блоков:

Линейная адресация: если известен базовый адрес блока и его размер В, адрес i -го блока можно вычислить следующим образом:

$$\text{Адрес } (i) = \text{Базовый адрес} + i \times В$$

Хэш- адресация: Ключ k использует хеш-функцию H для нахождения адреса данного блока:

$$\text{Адрес}(k) = H(k)$$

Оптимизация производительности:



Алгоритмы сортировки внутри блока: например, слияние или быстрая сортировка. Время сортировки блока размера B равно $O(B \log B)$.

Структуры индексов: используются для быстрого доступа к данным внутри блока, таким как B-деревья или хэш-таблицы.

Модели целостности данных:

Контрольная сумма (CRC): используется для проверки целостности данных. CRC для блока данных D может быть рассчитан как $CRC(D)$.

Хеширование: для проверки целостности или быстрого доступа к данным.

Модели сжатия и шифрования:

Сжатие данных: использует алгоритмы сжатия (например, LZ77, LZ78, DEFLATE) для уменьшения размера данных в блоке.

Шифрование: Для защиты данных при помощи алгоритмов шифрования, например, AES (Advanced Encryption Standard).

В управлении данными таким способом файлы можно изменять часто без ущерба для производительности, при этом позволяя изменять только те блоки, которые необходимо изменить, а не весь файл. Блочное хранилище характеризуется высокими значениями IOPS (операций ввода/вывода в секунду). Оно обеспечивает быстрый доступ для чтения, редактирования и других операций. Если объем данных вырастет, можно добавить новые тома и расширить дисковое пространство. Хранение данных в блочной технологии может использоваться одновременно в разных средах (например, Windows и Linux), включая серверные операционные системы. Заблокированные данные можно беспрепятственно перемещать между отдельными серверами, что, в свою очередь, позволит избежать сильной зависимости от конкретной инфраструктуры. Кроме того, дисковое пространство, разделенное на блоки, может одновременно использоваться несколькими разными серверами. При необходимости для дальнейшего повышения производительности отдельные блоки можно сгруппировать и разместить на быстрых SSD-

накопителях для «горячих» данных и медленных HDD для «холодных» данных.

Технология SAN-«Storage Area Network» (Сеть хранения данных) работает как один огромный локальный диск, обеспечивающий доступ к отдельным блокам через протокол Fibre Channel или iSCSI, что является более экономичной альтернативой и может быть построено поверх существующей сетевой альтернативы. Это архитектурное решение, при котором внешние накопители (дисковые массивы, оптические приводы, ленточные библиотеки и т.д.) напрямую подключаются к серверу, где установленная операционная система видит их как локальные ресурсы.

К существующим недостаткам блочной системы хранения относятся, прежде всего, более медленные варианты работы с метаданными, что очень важно во времена увеличенного потока данных. Если возникнет необходимость их добавить или обработать дополнительные данные, то это можно сделать только на уровне приложения или базы данных. Еще одна проблема это управление. По сравнению с другими типами хранилищ, оно может потребовать от пользователей дополнительных навыков и может оказаться более сложным в настройке и управлении.

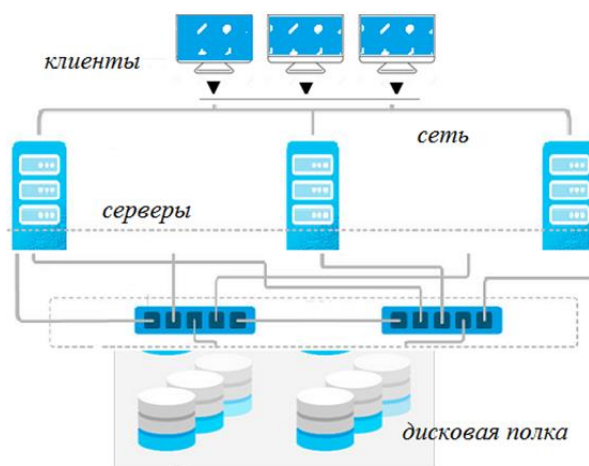


Рис. 2. Сеть хранения данных SAN.



2. Файловые хранилища. Преимуществом технологии хранения данных файлового типа является простота использования. Сервер присваивает файлу имя и метаданные, за которыми следует фрагмент этого идентификатора файла, который содержит имя сервера, путь к каталогу (папке) и имя файла, который необходимо найти (имя сервера + путь к каталогу + имя файла). В результате работы управляющей программы она переходит на поиск своего местоположения в каталогах и подкаталогах. Хранить данные в виде стандартных файлов и папок несколько удобнее, чем разбивать данные на блоки, а при работе с большими объемами данных привычная иерархическая концепция организации хранения понятна и логически несложна.

По мере значительного роста количества папок и файлов файловое хранилище существенно ограничивает возможности быстрого поиска, поэтому в случаях, когда требуется быстрый доступ к данным, временная сложность увеличивается и файловое хранилище теряет часть своих преимуществ.

В случаях, когда данные разделены на классы, для их хранения, поиска и обработки предпочтительнее использовать файловую систему, поскольку при таком подходе каждый объект можно отправить в свою папку. Естественно, метод очень удобный и легкий. Но когда объем обрабатываемых данных измеряется петабайтами, начинают появляться новые проблемы. Один путь может занимать сотни или даже тысячи подпапок, и в этом случае не так легко обеспечить очень высокую скорость доступа к нужному файлу. Технология NAS (Network Attached Storage) управляется специальным программным обеспечением, которое позволяет контролировать доступ пользователей, устанавливать права доступа и создавать резервную копию данных. Основными преимуществами NAS являются возможность удаленного доступа к накопителям, обмена файлами между пользователями и даже создания совместных проектов. Устройства NAS могут

работать в разных конфигурациях для разных нужд, таких как увеличение емкости хранилища, выделение сервера для мультимедиа, каталогизация доступа к контенту, резервное копирование, управление данными и синхронизация между устройствами.

Файлы могут быть фрагментированы, если длина файла превышает количество доступных последовательных блоков. В этом случае необходимо выполнить дополнительные операции по поиску деталей и компиляции их в целостный файл. Выполнение таких дополнительных ненужных задач снижает производительность всей системы и приводит к потере ресурсов. Кроме того, требуется, чтобы пространство, выделенное для файла в методе нулевой разметки, то есть длина файла, было объявлено при его создании. В случае цепного распределения (Linked Allocation) его также называют несмежным распределением, распределение выполняется поблочно. При этом блоки в файле не обязательно должны быть последовательными по номеру. Каждый блок содержит указатель на следующий блок в цепочке, в которой продолжается файл.

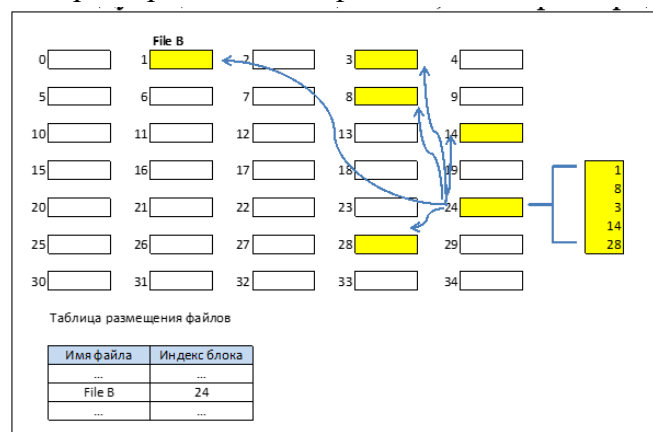


Рис.3 Блоки файлов, содержащие указатели

Последние блоки файлов могут быть заняты не полностью. Каждый предыдущий блок требует дополнительной информации (overhead) для управления указателем на следующий блок. Если указатель исчезнет, файл может быть разорван и недоступен.



Математическая модель хранилища файлов учитывает ключевые аспекты системы хранения, такие как размер, использование, избыточность и производительность.

Расчет емкости хранилища определяется соотношением между переменными:

$$C=U+F; \quad (1)$$

Где C – Общая емкость хранилища,

U - используемая ёмкость и

F - свободная ёмкость.

Использование хранилища является отношением использованной ёмкости к общей мощности:

$$\text{использование} = \frac{U}{C}. \quad (2)$$

Для оценки эффективности можно использовать следующие критерии:

R и W - средняя скорость чтения или записи данных;

L - задержка, то есть время, необходимое для доступа или записи данных;

I - IOPS, количество операций чтения или записи в секунду.

Если файлы распределены по разным устройствам хранения, модели доступа можно смоделировать с использованием вероятностей:

R_i – вероятность обращения к файлу i .

S_i - размер i – го файла

Ожидаемый размер включаемых файлов рассчитывается по следующей формуле:

$$E(S) = \sum_{i=1}^n P_i \cdot S_i, \quad (3)$$

Рассчитывая на постоянную скорость роста данных g , использование операций хранения с течением времени можно смоделировать с помощью следующей формулы:

$$U(t) = U(0) + g \cdot t \quad (4)$$

Указанный размер моделей хранения файлов предоставляет основу для количественной оценки и прогнозирования различных аспектов систем хранения файлов, таких как показатели использования, избыточности и производительности k . Регулируя все эти

параметры, заявленную модель можно адаптировать к конкретным архитектурам и требованиям хранения данных.

Современные подходы успешно решают ряд проблем, связанных с управлением данными типов файлов. К таким файловым системам относятся существующие технологии, такие как сетевые, кластерные и распределенные. Из них, в частности, распределенные файловые системы, делятся на два типа: параллельные и полностью параллельные. Отметим, что на сегодняшний день большая часть данных хранится в распределенных файловых системах. Особенно при работе с «неструктурированными» типами данных, используемыми при анализе «больших данных» (Big Data). Для управления большими объемами данных предусмотрены различные типы программного обеспечения, они могут относиться к той или иной и даже к нескольким технологиям, но наряду с их эффективными аспектами существуют и различные проблемы, ожидающие решения.

3. Объектные хранилища. Методы хранения объектов работают не по методу иерархической системы и в основном содержат данные в неструктурированном виде, при этом каждому объекту присваивается собственный адрес, служащий уникальным идентификатором. Каждый объект может иметь множество метаданных, описывающих его содержимое. Например, для фотографии это размеры, местоположение, фотография, время и другая подобная информация. Процесс хранения объектов легко масштабируется до работы с петабайтами данных и стал стандартным для многих онлайн-сервисов (таких как Facebook, Dropbox). Объектное хранилище - это вариант, который ближе подходит для хранения неструктурированных данных. Его можно масштабировать непрерывно без ухудшения производительности, что возможно для ресурсоемких приложений.

Технология объектного хранения близка к файловому способу хранения, но имеются некоторые различия в основных подходах. Модели



объектного хранилища также включают такие системные отличия, как том, использование, доступность, производительность и репликация. Рассмотрим элементы этой модели ниже. Определим R как количество копий каждого объекта. Тогда эффективный объем места для хранения уникальных данных составит:

$$\text{Эффективный объем} = \frac{C}{R} \quad (5)$$

Размеры файлов определяются практически по той же формуле, что и выше:

$$U = \sum_{i=1}^n S_i \quad (6)$$

Если объекты распределены по разным серверам (узлам), доступность можно моделировать вероятностью отказа этих узлов. Мы можем определить:

N - общее количество узлов;

P_f - вероятность отказа одного узла

Для системы с репликацией данных вероятность недоступности объекта (если используется репликация) можно определить как:

$$P_{\text{недоступности}} = P_f^R$$

Рассмотрим пример сценария для объектного хранилища C :

Общая емкость $C=100$ ТБ.

Удобство использования $U=30$ ТБ.

Свободная емкость $F=70$ ТБ.

Репликация данных $R=3$.

$$\text{Эффективная мощность} = \frac{100\text{ТБ}}{3} = 33.33\text{ТБ}$$

$$\text{Используется} = \frac{30\text{ТБ}}{100\text{ТБ}} = 0.3 \quad \text{или } 30\%$$

Возьмем скорость роста данных $g=1$ ТБ в месяц:

$$U(t) = 30\text{ТБ} + 1 \cdot t$$

Представленная модель помогает рассчитать и спрогнозировать ключевые параметры хранилища данных, такие как объем, загрузка, репликация, доступность и производительность. Настраивая параметры

модели, ее можно адаптировать под конкретные требования и архитектуру хранения данных.

Одним из основных преимуществ объектного хранилища является его гибкость. В отличие от реляционных баз данных, которые имеют фиксированную схему данных, объектное хранилище позволяет добавлять и удалять свойства объекта без изменения схемы данных. Это делает такие хранилища более адаптируемыми к меняющимся потребностям.

В отличие от файловых систем, хранилища объектов не поддерживают вызовы POSIX, такие как открытие, закрытие файла, чтение, запись и поиск ввода-вывода. Вместо этого у них есть только две основные операции: PUT и GET. Объектное хранилище четко управляет данными с помощью «метаданных» - коротких информационных вкладок о целом наборе данных (таблица, текстовый документ, видео и т. д.), с помощью которых его можно легко найти в общей памяти.

Объектное хранилище особенно полезно для сайтов с большим количеством статических файлов. Вместо того, чтобы загружать веб-сервер и заставлять его предоставлять статические данные клиентам, гораздо проще делегировать эту задачу облачному хранилищу, которое изначально было рассчитано на высокие нагрузки. Использование таких технологий, как сеть доставки контента (CDN), может еще больше повысить производительность и масштабируемость. Масштабируемость, в свою очередь, это еще одно преимущество объектного хранилища. На основе распределенной архитектуры объектного хранилища можно добавлять в кластер новые узлы для увеличения его емкости. Из-за простой структуры данных и эффективной индексации объектное хранилище позволяет быстро считывать и записывать данные с высокой скоростью, что особенно важно для высоконагруженных приложений.



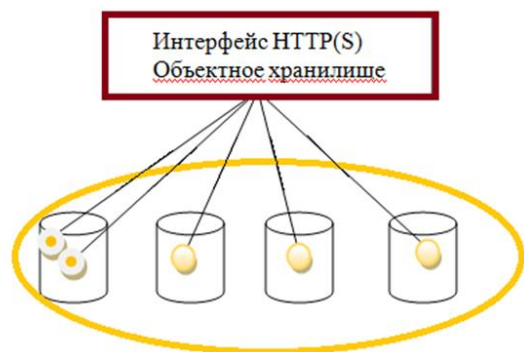


Рис.4 Способ хранения объектов

Стоит отметить расширенные возможности технологии объектного хранения, такие как восстановление данных. Современные жесткие диски имеют высокую надежность но, несмотря на это, они всё же могут выйти из строя. Во избежание потери данных пользователей информации в объектных хранилищах можно делать реплицирование двукратно. При такой организации хранилища опасность потери информации сведена к минимуму. Вот почему хранение бэкапов, логов и архивов это еще одна задача, которую объектное хранилище может решить с лёгкостью. При объектном хранении не нужно задумываться о репликации или о том, что скоро в хранилище закончится доступное место. По крайней мере в краткосрочной перспективе. Это также позволяет проводить регулярное обучение восстановлению в рамках плана аварийного восстановления после сбоев (Disaster Recovery Plan, DRP).

Объектно-ориентированное хранилище можно использовать для хранения различных типов данных, таких как медиаконтент, метаданные, структурированные данные и данные Интернета вещей. Например, большие фотографии и видео можно хранить в памяти объекта, а метаданные, такие как теги, описание и автор, в свойствах объекта. Ключевой принцип производительности объектного хранилища заключается в управление метаданными. Метаданные, такие как описания объектов, свойства и индексы, хранятся в отдельной таблице, что упрощает управление ими и их обновление.

Однако, исходя из характеристик объектно-ориентированного хранилища, производительность на определенных этапах уступает файловому или блочному хранилищу. Система должна выполнить несколько операций по «связыванию» данных с метаданными, и только потом предоставить их по запросу. Простота объектного хранилища делает его более удобным, но в то же время существуют ситуации, ограничивающие его функциональность, а именно:

1. Из-за неизменности объектов варианты использования ограничены однократной записью и многократным чтением. Объектное хранилище не используется для временного или горячего хранения, а его применение ограничивается архивированием данных.

2. Объект состоит из данных и идентификатора объекта. Любые метаданные должны находиться за пределами репозитория.

Оба этих недостатка существенны, поэтому почти каждое объектное хранилище имеет дополнительный уровень базы данных поверх уровня данных. Этот уровень базы данных (их можно назвать «шлюзом» или «прокси-сервисом») имеет более удобный интерфейс. Обычно он поддерживает сопоставление идентификатора объекта с удобными для пользователя метаданными, такими как имя объекта или разрешения.





Рис.5 Схема работы простого хранилища S3

Подходы к управлению данными. Если сосредоточиться на подходах, используемых для управления данными файловых и объектных хранилищ, можно увидеть основные различия в организации. В таблице ниже описаны основные сравнительные характеристики.

Характеристика	Блочное хранилище	Файловое хранилище	Объектное хранилище
Структура	Блоки фиксированного размера	Иерархическая (папки и подкаталоги)	Плоская (идентификаторы)
Метод доступа	На уровне блоков	Через пути файловой системы	Через уникальные идентификаторы или URL
Уровень абстракции	Низкий	Средний	Высокий
Метаданные	Фиксированные	Имя файла, размер, права, временные метки	Произвольные, могут быть пользовательскими
Управление	Контроллеры хранения (SAN)	Файловые системы (NAS, локальные)	Объектные хранилища (облачные)
Типичные операции	Чтение, запись, удаление, форматирование	Создание, чтение, запись, удаление, перемещение	Загрузка, скачивание, удаление, обновление

Примеры использования	Операционные системы, базы данных, VM	Документы, изображения, аудио, видео	Резервное копирование, мультимедиа, big data
Производительность	Высокая производительность, низкая задержка	Зависит от структуры и нагрузки	Высокая доступность, масштабируемость

Таблица 1. Сравнительные параметры способов хранения

Выводы. Каждый из подходов к управлению данными - блочный, файловый или объектный - имеет свои особенности, преимущества и области применения. Выбор подхода зависит от конкретных потребностей и требований к хранению данных, таких как производительность, масштабируемость, доступность и способ доступа к данным.

Существующие подходы эффективно решают многие проблемы управления данными на основе типов данных. При работе с неструктурированными данными часто используются популярные подходы и методы анализа, например: использование NLP для анализа текстов в социальных сетях, использование методов машинного обучения для классификации и интерпретации изображений и видео, индексации файлов журналов и аналитики, такой как Elasticsearch и Kibana для мониторинга и диагностики систем. Однако, если типы данных быстро становятся изменчивыми и поток данных становится разнородным как структурированным, так и неструктурированным вот здесь уже и необходимо возложить эту задачу на искусственный интеллект. То есть определить тип данных и на этой основе решить задачу использования оптимального инструмента в определенный момент работы, а также способ действия для каждого случая. Найти к каким задачам относится управление процессом хранения или обработки, т.е. включая простую загрузку как объекта или создание метаданных за счет



повышения уровня хранения и разделения уровней задач на модули по мере необходимости.

Методы искусственного интеллекта могут автоматически интегрировать данные из разнородных источников, таких как базы данных, API, файлы и облачные сервисы. Создание математической модели, которая описывает автоматическую интеграцию данных из разнородных источников с использованием ИИ, включает определение множества факторов и параметров, которые необходимо учитывать.

Основными элементами, которые могут быть включены в такую модель, являются:

1. Источники данных:

S - множество источников данных (базы данных, API, файлы, облачные сервисы).

V_s - объем данных, полученных от источника $s \in S$.

2. Методы интеграции:

I - множество методов интеграции данных (ETL, ELT, потоковая интеграция, репликация).

E_i - эффективность метода интегрирования $i \in I$ (например, скорость интеграции, производительность).

3. Качество данных:

Q_s - качество информации, полученной от источника, оцениваемое по различным критериям (например, полнота, точность, непротиворечивость).

4. Затраты:

C_i - затраты на использование метода интеграции (например, стоимость ресурсов, затраты времени).

5. Согласованность данных:

T_s -тип данных, полученных из источника s (структурированные, полуструктурированные, неструктурированные).

Переменные $x_{s,i}$ - доля данных из источника, интегрированных методом i . Функция

$$\max_{x_{s,i}} \sum_{s \in S} \sum_{i \in I} E_i \cdot x_{s,i} \cdot V_s$$

$$\min_{x_{s,i}} C_{total}$$

Математическая модель автоматической интеграции данных из различных источников с помощью искусственного интеллекта позволяет оптимизировать процесс, обеспечив максимальную эффективность, высокое качество данных и минимальные затраты. Такую модель можно адаптировать к конкретным требованиям и ограничениям, что позволяет более эффективно управлять данными и принимать обоснованные решения.

Сравнительный статистический анализ методов хранения данных.

В глобальном масштабе доля различных методов хранения данных зависит от многих факторов, включая рост объема данных, потребности в быстром доступе, требования к надежности и безопасности, а также технологические изменения. Точная статистика может меняться каждый год, ниже приведено примерное распределение долей основных способов хранения данных в мире на 2024 год:

Методы	Блочное	Файловое	Объектное	Реляционные	NoSQL	Кешируемые
Доля в процентах	~20-25%	~15-20%	~35-40%	~10-15%	~10-15%	~5-10%

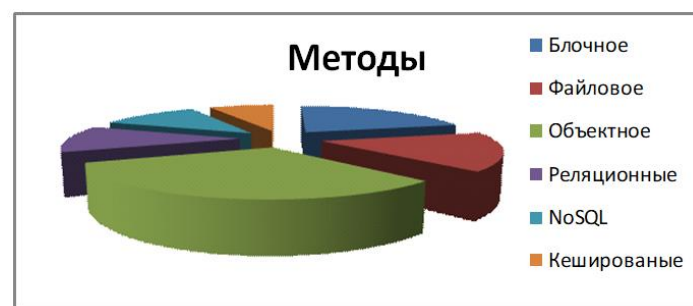


Таблица 2 Соотношение способов хранения файлов

Краткое содержание. В заключение можно утверждать, что в настоящее время нецелесообразно работать на основе единого подхода в процессе создания программных продуктов и сервисов при работе с различными типами неструктурированных файловых данных, причиной чего является разнообразие файлов и в то



же время растущий объем данных. Кроме того, современные задачи требуют работы с более быстрым потоком данных, что вновь создает проблему временных ресурсов, затрачиваемых на структурирование данных. В результате исследовательской работы были изучены методы оптимального управления различными типами данных. Показано, что блочный, файловый и объектный методы хранения широко используются как оптимальный вариант работы с большими данными. Гибридные подходы могут оказать существенное влияние на процедуры обработки и хранения, связанные с различными типами файловых данных.

Литература

1. Pernul, G. Database Security / G. Pernul // In: *Advances in Computers*, Vol. 38. ed. by M. C. Yovits. - Academic Press. - 1994. - pp. 1 - 74.
2. Akhatov A., Renavikar A., Rashidov A. & Nazarov F. "Development of the Big Data processing architecture based on distributed computing systems" *Informatika va energetika muammolari O'zbekiston jurnali*, № (1) 2022, 71-79
3. Bhadani, A., Jothimani, D. (2016), Big data: Challenges, opportunities and realities, In Singh, M.K., & Kumar, D.G. (Eds.), *Effective Big Data Management and Opportunities for Implementation* (pp. 1-24), Pennsylvania, USA, IGI Global
4. Рашидов, А., Ахатов, А., & Назаров, Ф. (2024). Алгоритм управления потоком данных во внутреннем механизме распределения. *Потомки Аль-Фаргани*, 1(2), 76–82. <https://al-fargoniya.uz/index.php/journal/article/view/377>
5. Austrian, Geoffrey D. (1982) *Herman Hollerith: Forgotten Giant of Information Processing* Columbia University Press. pp. 41, 178-179
6. A. Rashidov, A. Akhatov, I. Aminov, D. Mardonov "Distribution of data flows in distributed systems using hierarchical clustering" *International conference on Artificial Intelligence and Information Technologies (ICAИТ 2023)*, Samarkand 2023, November 3-4.
7. Преймесбергер, Крис (08 сентября 2006 г.) «IBM опирается на 50-летний опыт работы с

вращающимися дисковыми хранилищами» *eWeek.com* Проверено 16 октября 2012 г.

8. Ch. Eaton, D. deRoos, T. Deutsch, G. Lapis, P. Zikopoulos, "Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data", The McGraw-Hill Companies, 2012.

9. Inderpal Singh "Review on Parallel and Distributed Computing" *Scholars Journal of Engineering and Technology (SJET)*, 2013, № 1(4): 218-225

10. A. Rashidov, A. Akhatov and D. Mardonov, "The Distribution Algorithm of Data Flows Based on the BIRCH Clustering in the Internal Distribution Mechanism," 2024 *International Russian Smart Industry Conference (SmartIndustryCon)*, Sochi, Russian Federation, 2024, pp. 923-927, doi: 10.1109/SmartIndustryCon61328.2024.10516193.

11. Rashidov, A., Akhatov, A. R., & Nazarov, F. M. (2023). Real-Time Big Data Processing Based on a Distributed Computing Mechanism in a Single Server. In C. Ananth, N. Anbazhagan, & M. Goh (Eds.), *Stochastic Processes and Their Applications in Artificial Intelligence* (pp. 121-138). IGI Global. <https://doi.org/10.4018/978-1-6684-7679-6.ch009>

12. Rashidov, A., Akhatov, A., Nazarov, F. (2023). The Same Size Distribution of Data Based on Unsupervised Clustering Algorithms. In: Hu, Z., Zhang, Q., He, M. (eds) *Advances in Artificial Systems for Logistics Engineering III. ICAILE 2023. Lecture Notes on Data Engineering and Communications Technologies*, vol 180. Springer, Cham. https://doi.org/10.1007/978-3-031-36115-9_40

13. Томас Андерсон, Майкл Далин, Джин Ниф, Дэвид Паттерсон, Дрю Роселли и Рэндольф Ванг. *Бессерверные сетевые файловые системы*. В материалах 15-го симпозиума ACM по принципам операционной системы, страницы 109–126, Copper Mountain Resort, Колорадо, декабрь 1995 г.

14. Bolikulov, F.; Nasimov, R.; Rashidov, A.; Akhmedov, F.; Cho, Y.-I. Effective Methods of Categorical Data Encoding for Artificial Intelligence Algorithms. *Mathematics* 2024, 12, 2553. <https://doi.org/10.3390/math12162553>

15. Rashidov A.E., Sayfullaev J.S. "Selecting methods of significant data from gathered datasets for research" *International journal of advanced research in*



education, technology and management, Vol. 3 No. 2 (2024), p. 289-296, doi: 10.5281/zenodo.10781255

16. Ruslan. L. Smeliansky “Model of Distributed Computing System Operation with Time” Programming and Computer Software, 2013, Vol. 39, No. 5, 233–241 p., doi: 10.1134/S0361768813050046

17. Eshtemirov B.Sh., Nazarov F., Yarmatov Sh.Sh. “Technologies for identifying vehicles standing at traffic lights based on video data”, Central asian journal of mathematical theory and computer sciences, Volume: 03 Issue: 12 | ISSN: 2660-5309, 2022 yil, dekabr.

18. Akhatov A., Renavikar A., Rashidov A., Nazarov F. “Optimization of the number of databases in the Big Data processing” Проблемы информатики, № 1(58) 2023, DOI: 10.24412/2073-0667-2023-1-33-47

19. Nazarov F, Rashidov A, Pardayev M, Sunnatova S. (2023). Clustering Method Of Distributed Technologies In Data Flow Management. Excellencia: International Multi-Disciplinary Journal of Education (2994-9521), 1(5), 222-225. <https://multijournals.org/index.php/excellencia-imje/article/view/115>

20. Akhatov A., Renavikar A., Rashidov A. “Optimization of the database structure based on Machine Learning algorithms in case of increased data flow” Proceedings of the International Conference on Artificial Intelligence, Blockchain, Computing And Security (ICABCS 2023), Gr. N01 Da, Up, India, 24-25 February 2023



АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ВЛАЖНОСТЬЮ ЗЕРНА НА МУКОМОЛЬНОМ ЗАВОДЕ «ФАРГОНАДОНМАХСУЛОТЛАРИ»

Уринбоев Абдушукур Абдурахимович
Докторант Ферганского политехнического
института, Фергана, Узбекистан
urinboevabdushukur@gmail.com

Аннотация: Настоящее исследование посвящено внедрению автоматизированных систем управления (АСУ) для регулирования влажности зерна на мукомольном заводе «Фаргонадонмахсулотлари». Влажность зерна является важным фактором, определяющим качество конечной продукции — муки, а также существенно влияющим на эффективность процесса хранения и переработки. В работе рассмотрены методы и результаты применения АСУ для оптимизации уровня влажности, повышения энергоэффективности и улучшения производственных показателей. В результате внедрения АСУ были достигнуты значительные успехи в стабилизации показателей влажности, сокращении энергопотребления и увеличении производительности предприятия. Представлены графики, иллюстрирующие динамику изменений, а также фотографии оборудования и системы управления.

Ключевые слова: Автоматизированные системы управления (АСУ), влажность зерна, датчики влажности, технологические процессы, промышленная автоматизация, системы мониторинга

Введение. В современных условиях автоматизация процессов хранения и переработки зерна становится ключевым фактором для повышения эффективности и качества продукции. В представленных статьях исследуются различные аспекты автоматизации, включая мониторинг условий хранения, гидратацию пшеницы, внедрение автоматических линий увлажнения и проекты систем управления для мукомольных мельниц. Эти исследования направлены на улучшение контроля процессов, снижение ошибок и оптимизацию технологий, что в конечном итоге способствует обеспечению безопасности и качества зерновых продуктов.

В статье [1] рассматривается автоматизация процесса мониторинга влажности и температуры зерна, а также температуры воздуха в хранилищах мелькомбинатов. Автоматизация направлена на снижение ошибок, связанных с человеческим фактором, и включает внедрение автоматизированной системы учёта продукции. Это позволяет повысить точность контроля и управления условиями хранения зерна, что в свою

очередь способствует улучшению качества и безопасности продукции. В работе [2] изучалась гидратация пшеницы при замачивании в воде при температурах 30, 50, 60 и 70 °С. Прирост массы определялся по содержанию влаги, при этом скорость поглощения воды была высокой на начальных этапах и снижалась до равновесного состояния. Уравнение Пелега хорошо описывало гидратацию, при этом константа скорости (k_1) уменьшалась, а константа емкости (k_2) увеличивалась с ростом температуры. Высокое согласие экспериментальных и расчетных данных подтверждает применимость уравнения Пелега в исследуемых условиях. В статье [3] рассматриваются проблемы практического внедрения и эксплуатации автоматической линии увлажнения зерна на мукомольных производствах, с акцентом на примере автоматизированной системы управления технологическими процессами. В работе описаны структура системы, её функции, а также особенности реализации аппаратных средств и технологического оборудования, что способствует более



эффективному управлению процессами увлажнения зерна в мукомольной отрасли. В работах [4-5] представлены проекты автоматизированных систем управления технологическими процессами для мукомольных мельниц. Описана структура систем, включающая распределенный ввод/вывод сигналов через последовательные порты с централизованным управлением от персонального компьютера. Аппаратная основа программно-аппаратного комплекса включает модули, промышленные компьютеры и связную аппаратуру. Объектно-ориентированная информационная структура АСУ ТП мукомольного завода способствует упрощению тиражирования и модернизации аналогичных систем управления.

Контроль влажности зерна является одной из самых критически важных задач в процессе производства муки. Влажность зерна влияет не только на его качество, но и на эффективность всех этапов переработки. Оптимальный уровень влажности для хранения и переработки зерна колеблется в пределах 13-16%. Превышение этого диапазона может привести к росту микробов и плесени, что, в свою очередь, вызывает ухудшение качества зерна и, как следствие, производимой муки. С другой стороны, недостаток влаги может привести к поломке зерна и снижению выходов готовой продукции.

Ранее на мукомольных заводах, таких как «Фаргонадонмахсулотлари», контроль уровня влажности осуществлялся вручную. Операторы проводили регулярные замеры, что, как правило, было связано с временными затратами и недостаточной точностью. Ручное измерение влаги зависело от человеческого фактора и могло приводить к ошибкам. В условиях современных высоких стандартов качества и конкурентоспособности таких недостатков недостаточно для эффективного управления производственными процессами.

Важность автоматизации процессов в агропромышленности становится всё более актуальной. Внедрение автоматизированных

систем управления (АСУ) на мукомольных заводах позволяет значительно улучшить точность и надежность контроля влажности. АСУ способны обеспечить непрерывный мониторинг состояния зерна, что позволяет оперативно реагировать на изменения и вносить необходимые коррективы в процесс сушки и хранения.

На заводе «Фаргонадонмахсулотлари» использование АСУ предоставляет следующие преимущества:

- **Снижение риска порчи зерна:** Автоматизированный контроль позволяет поддерживать влажность в оптимальном диапазоне, что уменьшает вероятность появления плесени и других нежелательных процессов.
- **Увеличение производительности:** за счет автоматизации процессов снижается время простоя оборудования, и повышается общая эффективность работы завода.
- **Экономия ресурсов:** Автоматизация помогает снизить энергозатраты на сушку зерна, так как система может оптимально регулировать температурные режимы и время сушки на основании реальных данных.
- **Повышение качества продукции:** Стабильный контроль влажности обеспечивает высокое качество муки и зерна, что критично для сохранения репутации завода на рынке.

В этом исследовании акцентируется внимание на результатах внедрения АСУ на мукомольном заводе «Фаргонадонмахсулотлари». Основная цель работы заключается в оценке влияния автоматизации на управление влажностью зерна, а также на производственные показатели завода. Мы исследуем, как автоматизированные системы влияют на стабильность влажности, эффективность энергозатрат и производительность.

Система АСУ на заводе включает в себя датчики влажности, центральную панель управления и сушильные установки. Датчики



обеспечивают постоянный мониторинг влажности и передают данные на панель управления, где осуществляется их анализ и выработка команд для регулирования процессов сушки. Это позволяет не только поддерживать стабильные условия для хранения и переработки зерна, но и адаптировать процесс к изменениям внешней среды [6].

Таким образом, внедрение АСУ на мукомольном заводе «Фаргонадонмахсулотлари» не только соответствует современным требованиям к качеству, но и открывает новые горизонты для повышения производственной эффективности. Данная работа рассматривает методологию, результаты и рекомендации по дальнейшему внедрению автоматизации в агропромышленный сектор, подчеркивая важность точного и надежного контроля влажности зерна в процессе производства муки.

Методы. На мукомольном заводе «Фаргонадонмахсулотлари» была внедрена автоматизированная система управления (АСУ), состоящая из нескольких ключевых компонентов, работающих совместно для обеспечения эффективного контроля влажности зерна. Основные элементы системы включают датчики влажности, центральную панель управления и сушильные установки, каждая из которых играет важную роль в автоматизации процессов.

1. Датчики влажности - это основа системы АСУ, обеспечивающая непрерывный мониторинг уровня влажности зерна в реальном времени. Они размещены в следующих местах:

- **Силосы для хранения зерна:** Датчики контролируют влажность непосредственно в хранилищах, что позволяет оценить текущее состояние зерна и предотвратить его порчу.
- **Сушильные установки:** Эти датчики помогают контролировать уровень влажности во время процесса сушки, обеспечивая автоматическую корректировку параметров.

Датчики обычно используют емкостный или резистивный принцип измерения.

Емкостные датчики определяют влажность по изменению электрической ёмкости, которая зависит от содержания влаги в зерне. Резистивные датчики измеряют проводимость зерна, что также коррелирует с его влажностью. Эти данные передаются на центральную панель управления для дальнейшей обработки.

2. Панель управления - центральная панель управления является мозгом автоматизированной системы. Она осуществляет сбор, анализ и обработку данных, поступающих от датчиков влажности. Ключевые функции панели управления включают:

- **Отображение данных:** Пользователь может видеть в реальном времени уровень влажности, температуру и другие параметры, касающиеся состояния зерна.
- **Анализ данных:** Система использует алгоритмы для анализа полученных данных и предсказывает необходимые изменения в процессе сушки.
- **Регулирование процессов:** на основе анализа данных панель управления отправляет команды на сушильные установки для регулирования температуры и времени сушки, чтобы поддерживать влажность в оптимальном диапазоне.

На Рис 1 представлена система датчиков влажности зерна, размещённых в хранилищах и сушильных установках на мукомольном заводе «Фаргонадонмахсулотлари». Эти датчики обеспечивают непрерывный мониторинг уровня влажности зерна в реальном времени и передают полученные данные на центральную панель управления.





Рис 1. Система датчиков влажности зерна

Благодаря высокой точности показаний, получаемых с помощью датчиков, автоматизированная система управления может оперативно регулировать параметры сушки, что предотвращает как пересушивание, так и недостаточную обработку зерна. Таким образом, датчики играют ключевую роль в обеспечении эффективности и надежности автоматизированной системы управления влажностью, способствуя оптимизации производственных процессов и улучшению качества конечной продукции [7].

Панель управления может также иметь возможность удаленного доступа, что позволяет операторам контролировать и настраивать систему из любой точки, а также интегрироваться с другими системами управления на заводе.

3. Сушильные установки. Сушильные установки представляют собой оборудование, предназначенное для снижения уровня влажности зерна до оптимальных значений. Эти установки включают в себя:

- **Нагревательные элементы:** они обеспечивают подачу горячего воздуха в сушильные камеры. Температура и скорость подачи горячего воздуха регулируются на основании данных, получаемых с датчиков влажности.
- **Системы фильтрации:** оборудование может включать в себя системы фильтрации, которые очищают воздух перед его подачей в сушильные установки,

обеспечивая более высокое качество сушки и предотвращая загрязнение зерна.

На Рис 2 представлено сушильное оборудование, используемое на мукомольном заводе «Фаргонадонмахсулотлари» для снижения уровня влажности зерна. Это оборудование включает крупные сушильные агрегаты, системы фильтрации воздуха и устройства для подачи горячего воздуха, что позволяет создать оптимальные условия для сушки.



Рис 2. Сушильное оборудование

Работая под управлением автоматизированной системы управления (АСУ), сушильные установки способны автоматически регулировать температуру и время сушки в зависимости от данных, получаемых с датчиков влажности. Таким образом, автоматизация процесса сушки играет решающую роль в поддержании стабильных условий для обработки зерна и обеспечивает высокое качество конечного продукта.

Данная система датчиков влажности, установленных в зернохранилищах и сушильных установках, обеспечивает непрерывный мониторинг уровня влажности зерна в реальном времени, передавая актуальные данные на центральную панель управления. Благодаря высокой точности измерений, осуществляемых датчиками, система может автоматически регулировать параметры сушки, предотвращая как пересушивание, так и недостаточную обработку



зерна. Таким образом, датчики становятся ключевым элементом автоматизированной системы управления влажностью, способствуя оптимизации производственных процессов и повышению качества зерна.

Система автоматизированного управления с использованием АСУ позволяет регулировать параметры работы сушильных установок в зависимости от текущего состояния зерна. Например, если уровень влажности превышает установленный предел, система может автоматически увеличить температуру нагревательных элементов или продлить время сушки, чтобы быстро привести влажность в норму.

4. Математические модели и алгоритмы управления. Для управления процессом сушки используются математические модели и алгоритмы, которые помогают предсказывать, как изменение определённых параметров (температура, время сушки и др.) повлияет на уровень влажности зерна. Математическая модель, используемая на заводе, включает в себя следующие формулы:

Модель изменения влажности:

$$\Delta W = W_0 - W_f \quad (1)$$

где:

- W_0 — начальная влажность зерна,
- W_f — конечная влажность после сушки,
- ΔW — разница между начальной и конечной влажностью.

Дополнительно для расчета энергопотребления системы была использована формула:

$$E = P \cdot t \quad (2)$$

где:

- E — энергопотребление,
- P — мощность сушильного оборудования,
- t — время работы сушильных агрегатов.

Эти формулы позволяют эффективно рассчитывать потребление энергии и контролировать процесс сушки в реальном времени.

Таблица 1 демонстрирует основные параметры, характеризующие систему управления влажностью до и после внедрения АСУ. Она показывает, как автоматизация улучшила контроль влажности, снизила энергопотребление и увеличила производительность завода [8].

Таблица 1. Сравнение характеристик системы до и после внедрения АСУ

Параметр	До внедрения АСУ	После Внедрения АСУ
Уровень влажности (%)	12-18	15-16.5
Энергопотребление (кВт/ч)	Высокое	Сниженное на 10%
Производительность (тонн/день)	Низкая	Повышенная на 20%

5. Анализ данных и обратная связь. Система АСУ также включает в себя модуль анализа данных, который обрабатывает информацию о влажности и температуре, полученную от датчиков. Модуль предоставляет обратную связь о том, насколько эффективно работает процесс сушки, а также о необходимости корректировки параметров в зависимости от внешних условий.

В случае обнаружения отклонений от нормальных показателей система автоматически уведомляет оператора о необходимости вмешательства или корректировки [9].

Таким образом, система АСУ на мукомольном заводе «Фаргонадонмахсулотлари» сочетает в себе передовые технологии мониторинга, управления и анализа данных, что позволяет оптимизировать процессы сушки и контроля влажности зерна. Данная система способствует повышению качества конечной продукции и эффективности всего производственного процесса.

Результаты. Внедрение АСУ позволило добиться значительного улучшения показателей



контроля влажности зерна. До установки автоматизированной системы наблюдались колебания уровня влажности в диапазоне 12-18%, что часто приводило к переработке зерна и снижению качества конечной продукции. После установки АСУ влажность стабилизировалась в пределах 15-16,5%, что является оптимальным диапазоном для дальнейшего хранения и переработки зерна. Данный результат наглядно представлен на Рис 3.

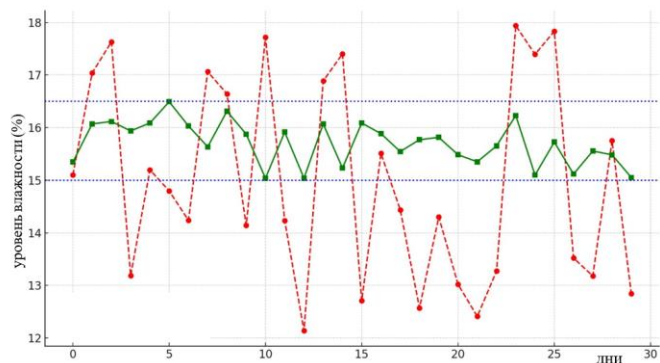


Рис 3: Динамика уровня влажности зерна до и после внедрения автоматизированной системы управления (АСУ). а) показатели до внедрения АСУ, б) показатели после внедрения АСУ, в) оптимальный диапазон влажности (15-16,5%)

Данный график показывает изменение уровня влажности зерна до внедрения автоматизированной системы управления (АСУ) и после её реализации. На оси Y представлен уровень влажности (%), а на оси X — время (дни). До внедрения АСУ уровень влажности варьировался между 12% и 18%, что приводило к значительным колебаниям и нестабильности качества конечной продукции, а также увеличивало необходимость повторных циклов сушки. После внедрения системы уровень влажности стабилизировался в диапазоне 15-16,5%, что соответствует оптимальным условиям для хранения и переработки зерна. Эта стабильность в контроле влажности снижает риск порчи зерна и улучшает качество производимой на заводе муки, что подчеркивает эффективность автоматизированного контроля.

Кроме того, внедрение системы привело к сокращению энергопотребления на 10%, что стало возможным благодаря более точному контролю температуры и времени работы сушильных установок. Снижение энергозатрат представлено на Рис 4.

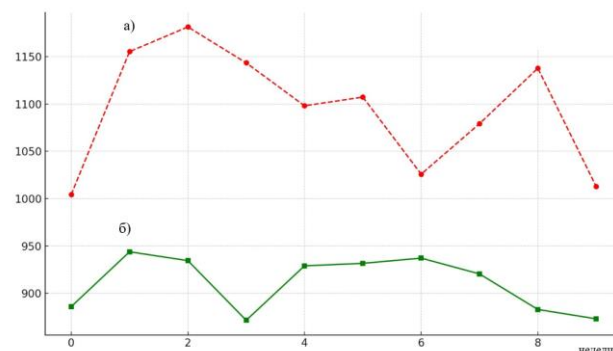


Рис 4: Сравнение энергопотребления до и после установки АСУ

а) до внедрения АСУ, б) после внедрения АСУ

На данном графике представлено снижение энергопотребления благодаря точной настройке температурных режимов сушильных агрегатов. Ось Y - энергопотребление (кВт/ч), ось X - временной период (недели до и после установки). График 2 отражает снижение энергопотребления на мукомольном заводе после внедрения АСУ. До установки системы энергопотребление было значительно выше, так как процессы сушки зерна требовали частого вмешательства операторов и настройки оборудования вручную. Введение АСУ позволило автоматически и более точно контролировать температурные режимы сушки, что привело к снижению энергозатрат. После внедрения системы энергопотребление сократилось на 10%, что не только повысило энергоэффективность производства, но и снизило эксплуатационные затраты.

Также зафиксировано увеличение производительности завода на 20%, что связано с устранением необходимости повторной сушки и повышением эффективности технологических процессов. Данные представлены на Рис 5.



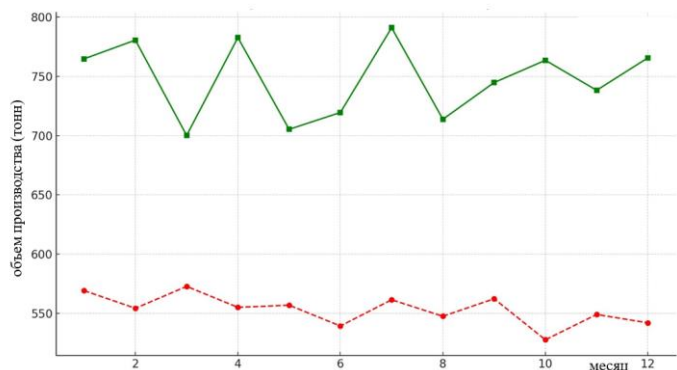


Рис 5: Сравнительный анализ производительности до и после внедрения автоматизированной системы управления (АСУ). а) производительность до внедрения АСУ, б) производительность после внедрения АСУ.

Этот график показывает прирост производительности, выраженный в объеме переработанного зерна до и после автоматизации, связанный с сокращением повторной сушки и улучшением качества зерна. График 3 показывает увеличение производительности на мукомольном заводе после установки АСУ. До внедрения автоматизации нестабильный контроль влажности и необходимость повторных циклов сушки приводили к снижению объемов переработанного зерна. После внедрения АСУ наблюдается устойчивый рост производительности примерно на 20%. Это связано с тем, что система исключила необходимость повторной обработки зерна, уменьшив время простоев и оптимизировав процесс сушки. Таким образом, АСУ способствовала повышению эффективности и увеличению объемов переработки зерна.

Рис 6 демонстрирует центральную операторскую панель управления автоматизированной системой. На экранах отображаются данные в реальном времени о состоянии зерна, включая уровень влажности, температуру в сушильных установках, а также статус системы. Операторская АСУ позволяет специалистам завода контролировать процессы сушки и своевременно вносить коррективы при необходимости. Это высокотехнологичное решение значительно снижает риск человеческой

ошибки и повышает эффективность управления технологическим процессом.



Рис 6. Центральная операторская панель системы автоматизированного управления (АСУ)

В данной таблице 2 перечислены ключевые элементы автоматизированной системы управления, их функции и значение для эффективного контроля влажности зерна.

Таблица 2. Основные элементы автоматизированной системы управления (АСУ)

Элемент	Описание
Датчики влажности	Обеспечивают мониторинг уровня влажности в реальном времени.
Центральная панель	Позволяет отображать данные и регулировать процессы.
Сушильные установки	Автоматически регулируют параметры сушки на основе данных датчиков.

Обсуждение. Полученные результаты демонстрируют эффективность внедрения АСУ на мукомольном заводе «Фаргонадонмахсулотлари». Система позволила стабилизировать уровень



влажности зерна, что напрямую сказалось на качестве муки, а также значительно снизить энергозатраты на процесс сушки. Важно отметить, что АСУ практически устранила человеческий фактор из процесса управления, что увеличило точность операций и снизило риск ошибок. Несмотря на первоначальные затраты на установку системы, долгосрочные выгоды, такие как экономия энергии и рост производительности, делают внедрение АСУ экономически оправданным.

Одной из задач будущих исследований может стать интеграция более продвинутых систем управления, основанных на искусственном интеллекте, которые позволят прогнозировать изменения условий внешней среды и адаптировать процесс сушки в зависимости от этих изменений. Это ещё больше повысит эффективность производства и позволит избежать любых непредвиденных рисков.

Выводы

Внедрение автоматизированных систем управления (АСУ) для контроля влажности зерна на заводе «Фаргонадонмахсулотлари» оказало значительное положительное воздействие на эффективность производственных процессов. Достигнутый стабильный контроль уровня влажности способствует не только повышению качества конечной продукции — муки, но и снижению рисков, связанных с порчей зерна, что в свою очередь, оптимизирует процесс хранения и переработки. Кроме того, снижение энергопотребления на 10% после внедрения АСУ подчеркивает важность эффективного управления ресурсами в условиях растущей энергетической нагрузки на агропромышленность. Увеличение производительности на 20% демонстрирует, что автоматизация процессов значительно сокращает время простоя и увеличивает общую эффективность производства.

Таким образом, данный опыт подтверждает актуальность и необходимость интеграции современных технологий в агропромышленный

сектор, где точность и автоматизация играют ключевую роль в обеспечении высоких стандартов качества продукции и снижении производственных затрат. Будущее агропромышленности зависит от адаптации к инновациям, что позволит повысить конкурентоспособность и устойчивость предприятий на рынке.

СПИСОК ЛИТЕРАТУРЫ

- [1] Kalandarov, P. (2022). Автоматизация процесса контроля влажности зерна и зерновых продуктов в зернохранилищах мельниц. *Сельское хозяйство, Техника*, 108, 04.08.2022.
- [2] Vengaiyah, P. C., Raigar, R., Srivastav, P., & Majumdar, G. C. (2012). Hydration characteristics of wheat grain. *Agri Eng Int: CIGR Journal*, 14.
- [3] Починчук, Н., Сивко, И., Пахоменко, А., Зяблицев, В., & Еганов, М. (2000). Комплексный подход к решению проблем автоматического увлажнения зерна. *Библиотека, СТА №4*.
- [4] Штителъман, Б. А. (2000). Новые АСУ ТП для мукомольной промышленности. Технический директор, ООО Мост-СК. Москва, ул. Уткина, 42.
- [5] Рыженко, А., & Свирид, Е. (2000). Объектно структурированная АСУ ТП мукомольного завода. *Современная электроника и технологии автоматизации, СТА №3*.
- [6] Бородин, И. Ф. (2022). *Автоматизация технологических процессов*. Москва: Машиностроение.
- [7] *Зерно и его хранение*. (2023). Фергана: Издательство ФПИ.
- [8] Результаты мониторинга влажности на Фаргонадонмахсулотлари. (2023).
- [9] Urinboev, A. A. (2023). Computerized fermentation control. *Pedagog Respublika Ilmiy Jurnal*, 6(11).



ELLIPTIK EGRI CHIZIQLAR ASOSIDA ASIMMETRIK ALGORITMLARNING MATEMATIK ASOSLARI VA ULARNI QO'LLASH MASALALARI

Rahmatullayev Ilhom Raxmatullayevich,

texnika fanlari doktori,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti Samarqand filiali

Boyquziyev Ilxom Mardanoqulovich,

texnika fanlari doktori,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti
O'zbekiston Milliy universiteti tadqiqotchisi

Umurzakov Oybek Shakarboy o'g'li,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti Samarqand filiali assistenti

Saydullayev Eldor Ismatullo o'g'li,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti Samarqand filiali assistenti

Annotatsiya: Ushbu maqolada asimmetrik kriptografik algoritmlarni elliptik egri chiziq'larga o'tkazishning matematik asoslari va ularning qo'llanilishi tahlil qilinadi. Asimmetrik kriptografiya, masalan, RSA va Diffie-Hellman algoritmlari uzoq vaqt davomida xavfsiz aloqa va ma'lumotlarni himoya qilishda qo'llanilgan. Biroq, katta kalit uzunligi va hisoblash murakkabligi sababli, bu tizimlarni cheklangan resursli muhitlarda qo'llash qiyinlashadi. Elliptik egri chiziq'lar kriptografiyasi (ECC) bu muammolarni hal qilish uchun samarali echim sifatida paydo bo'ldi. ECC kichik kalit uzunligida yuqori darajadagi xavfsizlikni ta'minlaydi. Maqolada ECC algoritmlarining matematik asoslari, ularning xavfsizlik afzalliklari va ularni amaliyotda qo'llash masalalari batafsil yoritiladi.

Kalit so'zlar: Asimmetrik kriptografiya, Elliptik egri chiziq'lar, Diskret logarifm, El-Gamal shifrlash algoritmi, Xavfsizlik, Kalit uzunligi, Matematik murakkablik, Diffie-Hellman, ECC (Elliptik Egri Chiziq'lar Kriptografiyasi)

I. Kirish

Axborot xavfsizligi va kriptografiya sohasida asimmetrik algoritmlar muhim rol o'ynaydi. An'anaviy asimmetrik kriptografiya tizimlari, masalan, RSA va Diffie-Hellman, uzoq vaqt davomida xavfsiz aloqa va ma'lumotlarni himoya qilishda ishlatib kelinmoqda. Biroq, bu tizimlar katta kalit uzunligi va hisoblash murakkabligi sababli cheklangan resursli muhitlarda qo'llanishda muammolarga duch keladi. Bu holat mobil qurilmalar va IoT kabi tizimlarda asimmetrik kriptografiyaning samarali ishlashiga to'sqinlik qiladi[1-3].

Elliptik Egri Chiziq'lar Kriptografiyasi (ECC) bu muammolarni hal qilish uchun samarali echim sifatida paydo bo'ldi. ECC kichik kalit uzunligida yuqori darajadagi xavfsizlikni ta'minlaydi, bu esa uni cheklangan resursli muhitlarda qo'llashni osonlashtiradi. Shuning uchun, asimmetrik algoritmlarni ECC ga o'tkazish bo'yicha ko'plab tadqiqotlar olib borilmoqda.

Ushbu maqolaning maqsadi asimmetrik kriptografik algoritmlarni elliptik egri chiziq'larga o'tkazishning matematik asoslarini o'rganish va ECC algoritmlarining amaliyotdagi afzalliklarini tahlil



qilishdan iborat. Tadqiqot, ayniqsa, ECC ning kalit uzunligi va xavfsizlik darajasi o'rtasidagi muvozanatni ta'minlashda qanday rol o'ynashi va bu yangi yondashuvlar bilan qanday xavfsizlik afzalliklari yaratilishini ko'rsatishga qaratiladi [4-6].

Axborot xavfsizligi va kriptografiya sohasida asimmetrik algoritmlar muhim rol o'ynaydi. Asimmetrik kriptografiya tizimlari, masalan, RSA va Diffie-Hellman, uzoq vaqt davomida xavfsiz aloqa va ma'lumotlarni himoya qilish uchun qo'llanilgan. Biroq, bu tizimlarning ba'zilar katta kalit uzunligiga va hisoblash murakkabligiga ega bo'lib, resurs cheklangan muhitlarda qo'llashni qiyinlashtiradi.

Elliptik egri chiziqlar kriptografiyasi (ECC) asimmetrik kriptografiyada yangi yondashuv sifatida paydo bo'ldi. ECC kichik kalit uzunligida yuqori darajadagi xavfsizlikni ta'minlaydi, bu esa uni mobil qurilmalar va boshqa cheklangan resursli tizimlarda qo'llashni osonlashtiradi. Shu sababli, asimmetrik algoritmlarni elliptik egri chiziqchilarga o'tkazish bo'yicha ko'plab tadqiqotlar olib borilmoqda.

Ushbu maqolada biz asimmetrik algoritmlarni elliptik egri chiziqlarga o'tkazish bilan bog'liq matematik asoslarni va mavjud adabiyotlarni tahlil qilamiz.

Elliptik egri chiziqlar kriptografiyasi birinchi marta Neal Koblitz va Victor Miller tomonidan 1985-yilda mustaqil ravishda taklif qilingan. Ular elliptik egri chiziqlarning algebraik xususiyatlaridan foydalanib, kriptografik tizimlarni yaratish mumkinligini ko'rsatdilar [7].

ECC ning asosiy afzalliklaridan biri bu kalit uzunligi va xavfsizlik darajasi o'rtasidagi muvozanatdir. Masalan, ECC 256-bitli kalit uzunligi bilan RSA 3072-bitli kalit uzunligiga teng xavfsizlikni ta'minlaydi [8].

Asimmetrik algoritmlarni ECC ga o'tkazish bo'yicha ko'plab ishlar amalga oshirildi. Misol uchun, Elliptic Curve Diffie-Hellman (ECDH) va Elliptic Curve Digital Signature Algorithm (ECDSA) kabi algoritmlar ECC asosida yaratilgan.

ECDH algoritmi Diffie-Hellman kalit almashish protokolinig elliptik egri chiziqlar versiyasidir [9]. U umumiy sir kalitni xavfsiz

almashish uchun ishlatiladi. ECDSA esa DSA algoritmining ECC ga moslashtirilgan versiyasidir va raqamli imzolar uchun qo'llaniladi [10].

Matematik asoslari bo'yicha, ECC asosan sonlar nazariyasi va algebraik geometriyaga tayanadi. Elliptik egri chiziqlar $y^2 = x^3 + ax + b$ tenglama bilan ifodalanadi, bu yerda a va b - koeffitsiyentlar [11-12]. Bu egri chiziqlarda nuqtalar qo'shish va skalyar ko'paytirish kabi amallar kriptografik algoritmlarning asosini tashkil etadi.

II. Asosiy qism

Bugungi kunda zamonaviy asimmetrik algoritmlarning xavfsizligi, simmetrik shifrlash usullarining xavfsizligidan farqli ravishda, muayyan matematik masalalarning yechish qiyinligiga asoslanadi. Ayniqsa, matematik murakkablik nazariyasining asosiy yo'nalishlari sifatida tan olingan berilgan sonni tub ko'paytuvchilarga ajratish (faktorizatsiya) va cheklangan maydonda diskret logarifmlash masalalari bu algoritmlarning mustahkamligi uchun muhim ahamiyatga ega.

Diskret logarifmlash tushunchasi kriptografiyaga XX asrning 50-yillarida, rotorli shifrlash mashinalari o'rniga siljish registrlarining qo'llanilishi orqali kirib keldi. Xususan, siljish registrlari berilgan siljishlar ketma-ketligida har bir elementning pozitsiyasini aniqlashda muhim rol o'ynagan. Bu registrlar yordamida kriptografik tizimlar yaratildi, bunda diskret logarifmlash masalasi asosiy matematik murakkablik sifatida qo'llanildi.

Hozirgi kunda zamonaviy asimmetrik shifrlash algoritmlarining fundamental murakkablik asoslari hisoblangan faktorizatsiya va cheklangan maydonda diskret logarifmlash masalalarini yechishning ko'plab zamonaviy usullari ishlab chiqilgan. Ushbu yo'nalishlarda butun dunyo bo'ylab olimlar va mutaxassislar faol ravishda ilmiy tadqiqotlar olib bormoqdalar. Masalan, kvant kompyuterlarining rivojlanishi ushbu masalalarning yechimiga ta'sir ko'rsatishi mumkinligi sababli, kriptografik tizimlarni yanada mustahkamlash bo'yicha izlanishlar davom etmoqda [7].



Agar zamonaviy asimmetrik algoritmlarda matematik murakkablik sifatida tan olingan faktorizatsiya va cheklangan maydonda diskret logarifmlash masalalarini hal qilishning samarali usullari yaratilsa yoki taklif etilsa, bunday algoritmlardan amaliy foydalanish tavsiya etilmaydi. Chunki bu holatda algoritmning xavfsizligi pasayadi va uni yanada ishonchli qilish uchun murakkabligini oshirish zarurati tug'iladi. Bu vaziyat o'z navbatida quyidagi uchta muammoni keltirib chiqaradi:

1. Parametrlarga qo'yiladigan talablarni o'zgartirish: ya'ni, algoritmlarda foydalaniladigan sonlarning razryadini oshirish kerak bo'ladi. Ammo bu esa algoritmning ishlash tezligini sezilarli darajada pasaytiradi, chunki katta sonlar bilan ishlash ko'proq hisoblash resurslarini talab qiladi.

2. Asimmetrik algoritmlarning yangi variantlarini ishlab chiqish: bunda faktorizatsiya va diskret logarifmlashning matematik murakkabliklari kombinatsiyasidan foydalaniladi. Bu yondashuv algoritmlarning xavfsizligini oshirishi mumkin, lekin ularni amalga oshirish va tushunishni qiyinlashtiradi.

3. Bir tomonli funksiyalarni o'zgartirish: ya'ni, algoritmlarda qo'llaniladigan matematik murakkablikni boshqa, yangi murakkablikka o'tkazish. Bu murakkablik shunday bo'lishi kerakki, amaliy nuqtai nazardan, yetarli darajada kichik uzunlikdagi sonlar bilan ham kerakli xavfsizlikni ta'minlasin va samaradorlikni saqlab qolsin.

Ushbu tadqiqotda matematik analiz va adabiyotlar tahlili usullari qo'llanildi. Xususan, elliptik egri chiziqlar asosidagi asimmetrik algoritmlarning matematik asoslari va ularni qo'llash masalalari o'rganildi. Matematik murakkablik nazariyasiga asoslangan holda, asimmetrik algoritmlarning xavfsizlik darajalari, xususan, ECC va boshqa an'anaviy algoritmlar orasidagi farqlar tahlil qilindi. Ushbu tahlilda 1-jadval orqali kalit uzunligi, faktorizatsiya, diskret logarifmlash, va elliptik egri chiziqlarda diskret logarifmlash masalalari orasidagi murakkablik darajalari solishtirildi. Shuningdek, adabiyotlarni ko'rib chiqish orqali ECC algoritmlarining matematik xususiyatlari va afzalliklari batafsil bayon etildi.

ECC 256-bitli kalit uzunligi bilan RSA 3072-bitli kalit uzunligiga teng xavfsizlikni ta'minlaydi. Bu kalit uzunligi va xavfsizlik darajasi o'rtasidagi samaradorlikni tasdiqlaydi.

Quyidagi 1-jadvalda, kalit uzunliklari turlicha bo'lgan holatlarda, zamonaviy kompyuterlarning hisoblash imkoniyatlaridan kelib chiqib, faktorizatsiya, cheklangan maydonda diskret logarifmlash va elliptik egri chiziqlarda diskret logarifmlash masalalarini tahlil qilish murakkabliklari keltirilgan. Ushbu jadval algoritmlarning turli kalit uzunliklarida qanday tezlikda buzilishi mumkinligini ko'rsatadi va xavfsizlik darajasini baholash uchun muhim ahamiyatga ega.

1-jadval. Cheklangan maydonda diskret logarifmlash va elliptik egri chiziqlarda diskret logarifmlash masalalarini tahlil

Kalit uzunligi	Faktorizatsiya	Diskret logarifmlash	EEChda diskret logarifmlash
100	1.3×10^7	1.3×10^7	1.3×10^{15}
200	7.2×10^9	7.2×10^9	1.3×10^{30}
300	7.1×10^{11}	7.1×10^{11}	1.4×10^{45}
400	3×10^{13}	3×10^{13}	1.6×10^{60}
500	7.5×10^{14}	7.5×10^{14}	1.8×10^{75}
600	1.3×10^{16}	1.3×10^{16}	2×10^{90}
700	1.7×10^{17}	1.7×10^{17}	2.3×10^{105}
800	1.8×10^{18}	1.8×10^{18}	2.6×10^{120}
900	1.7×10^{19}	1.7×10^{19}	2.9×10^{135}
1000	1.3×10^{20}	1.3×10^{20}	3.3×10^{150}

Ushbu jadvaldan ko'rinib turibdiki, kalit uzunligi oshgani sayin, faktorizatsiya va diskret logarifmlash masalalarining hisoblash murakkabligi eksponentsial ravishda ortib boradi. Biroq, elliptik egri chiziqlarda diskret logarifmlash masalasining murakkabligi ancha yuqori bo'lib, bu algoritmlarning xavfsizligini ta'minlashda muhim ahamiyatga ega.

Masalan, kalit uzunligi 100 bo'lganda, faktorizatsiya va diskret logarifmlash masalalarini hal qilish uchun taxminan 1.3×10^7 hisoblash amallari talab etiladi, lekin EEChda diskret logarifmlash uchun bu qiymat 1.1×10^{15} ga teng. Bu esa EECh asosidagi



algoritmning nisbatan xavfsizroq ekanligini ko'rsatadi.

Kalit uzunligi oshgani sayin, bu farq yanada ortadi. 1000 bitli kalit uchun faktorizatsiya va diskret logarifmlashning murakkabligi 1.3×10^{20} bo'lsa, EEChda diskret logarifmlash uchun bu qiymat 3.3×10^{150} ga yetadi. Bu shuni anglatadiki, EECh asosidagi kriptografik algoritmlar katta kalit uzunliklarida ham yuqori darajada xavfsizlikni ta'minlay oladi.

Shu sababli, zamonaviy kriptografiyada kalit uzunligini tanlashda ushbu murakkabliklar hisobga olinishi zarur. Ayniqsa, kompyuter texnologiyalari rivojlanib, hisoblash quvvati oshib borayotgan bir paytda, algoritmning xavfsizligini ta'minlash uchun kalit uzunligini oshirish yoki matematik jihatdan yanada murakkab bo'lgan algoritmardan foydalanish muhim ahamiyat kasb etadi.

Ushbu jadval, shuningdek, turli kriptografik usullarni tanlashda qaror qabul qilish jarayonida yordam beradi. Faktorizatsiya va diskret logarifmlashga asoslangan tizimlar uchun kalit uzunligini oshirish orqali xavfsizlikni kuchaytirish mumkin, lekin bu hisoblash samaradorligini pasaytirishi mumkin. Bunga qarama-qarshi ravishda, EECh asosidagi tizimlar kichikroq kalit uzunliklarida ham yuqori xavfsizlikni ta'minlashi mumkin, bu esa ularning samaradorligini saqlab qoladi.

Demak, faktorizatsiya va cheklangan maydonda diskret logarifmlash masalalarining murakkabliklariga nisbatan kichikroq uzunlikdagi parametrlardan foydalanib, elliptik egri chiziq'larga asoslangan bardoshli asimmetrik algoritmlar yaratish mumkin. Bu esa kriptografiyada xavfsizlikni oshirish bilan birga, samaradorlikni ham ta'minlaydi.

Elliptik egri chiziq'larning asosiy tushunchalari Aytaylik, $p > 3$ bo'lgan tub son berilgan bo'lsin. U holda, cheklangan tub maydon F_p ustida aniqlangan E elliptik egri chiziq quyidagi tenglama bilan ifodalanadi:

$$E: y^2 \equiv x^3 + ax + b \pmod{p},$$

bu yerda $a, b \in F_p$ va egri chiziqning nonsingular (singulyarligi yo'q) bo'lishi uchun quyidagi shart bajarilishi lozim:

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}.$$

Bu shart egri chiziqning o'ziga xos xususiyatlarini saqlab qolishini ta'minlaydi, ya'ni unda kesishish nuqtalari yoki nuqsonlar (singulyarliklar) bo'lmaydi.

III. Natijalar

Elliptik egri chiziq'larda qurilgan algebraik tuzilmalar kriptografik amallarni bajarish uchun juda qulay. Ular ustida aniqlangan guruh operatsiyalari tufayli, biz asimmetrik kriptografik tizimlarni samarali va xavfsiz tarzda amalga oshirishimiz mumkin. Elliptik egri chiziq'larga asoslangan kriptografiya (ECC) xavfsizligi Elliptik Egri Chiziq Diskret Logarifm Masalasi (EECDLM) ning yechish qiyinligiga asoslanadi.

EECDLM shunday masalani ifodalaydi: berilgan elliptik egri chiziq E ustida ikkita nuqta P va Q uchun $Q = kP$ tenglikni qanoatlantiradigan k sonini topish. Bu masala amalda juda qiyin bo'lib, unga asoslangan kriptografik tizimlar yuqori darajada xavfsizlikni ta'minlaydi.

Elliptik egri chiziq'larga asoslangan tizimlarda kalit uzunliklari boshqa asimmetrik tizimlarga nisbatan ancha kichik bo'lishi mumkin. Masalan, ECC tizimida 256 bitli kalit uzunligi RSA tizimidagi 3072 bitli kalit uzunligiga teng xavfsizlik darajasini ta'minlaydi. Bu esa hisoblash resurslarini tejash, tezlikni oshirish va xotira talablarini kamaytirish imkonini beradi.

Elliptik egri chiziq'larga asoslangan algoritmlar quyidagi kriptografik protokollarda keng qo'llaniladi:

- Elliptik Egri Chiziq Diffi-Xellman (ECDH): Kalit almashinuvi protokoli bo'lib, umumiy maxfiy kalitni xavfsiz tarzda hosil qilish imkonini beradi.

- Elliptik Egri Chiziq Raqamli Imzo Algoritmi (ECDSA): Raqamli imzolarni yaratish va tekshirish uchun ishlatiladi, bu esa ma'lumotlarning yaxlitligini va autentifikatsiyasini ta'minlaydi.

- Elliptik Egri Chiziq Integratsiyalangan Shifrlash Standarti (ECIES): Ma'lumotlarni shifrlash va deshifrlash uchun ishlatiladigan algoritm.



Elliptik egri chiziqning invarianti deb quyidagi ayniyatni qanoatlantiruvchi $J(E)$ kattalikka aytiladi:

$$J(E) = 1728 \frac{4a^3}{4a^3 + 27b^2} \pmod{p} \quad (2)$$

E elliptik egri chiziqning a , b koeffisientlari $J(E)$ invariant ma'lum bo'lganda, quyidagicha aniqlanadi: $\begin{cases} a \equiv 3k \pmod{p} \\ b \equiv 2k \pmod{p} \end{cases}$ (3)

Bu yerda, $k = \frac{J(E)}{1728 - J(E)} \pmod{p}$, $J(E) \neq 0$ yoki 1728.

(1) ayniyatni qanoatlantiruvchi (x, y) – juftliklar Y_e elliptik egri chiziqning nuqtalari deb ataladi, x va u – mos ravishda nuqtaning x va u koordinatalari hisoblanadi.

Elliptik egri chiziq nuqtasini $G(x, y)$ yoki G deb belgilaymiz. Elliptik egri chiziqning ikkita nuqtasi teng deyiladi, agar ularning mos x va y koordinatalari teng bo'lsa.

E elliptik egri chiziqning barcha nuqtalari to'plamida qo'shish amalini kiritib, uni "+" deb belgilaymiz. Y_e elliptik egri chiziqning ixtiyoriy ikkita $G_1(x_1, y_1)$ va $G_2(x_2, y_2)$ nuqtalari uchun bir nechta variantlarni ko'rib chiqamiz.

Aytaylik, G_1 va G_2 nuqtalar koordinatalari uchun $x_1 = x_2$ shart qanoatlansin. U holda, bu nuqtalarning yig'indisi deb, koordinatalari quyidagi taqqoslashlar bilan aniqlanuvchi $G_3(x_3, y_3)$ nuqtaga aytiladi:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \pmod{p} \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} \end{cases} \quad (4)$$

Bu yerda, $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$.

Agar $x_1 = x_2$ va $y_1 = y_2 \neq 0$ tenglik bajarilsa, u holda G_3 nuqta koordinatalari quyidagicha aniqlanadi [8]:

$$\begin{cases} x_3 = \lambda^2 - 2x_1 \pmod{p} \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} \end{cases} \quad (5)$$

Bu yerda, $\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p}$.

Agar $x_1 = x_2$ va $y_1 = -y_2 \pmod{p}$ sharti bajarilgan holda, G_1 va G_2 nuqtalar yig'indisini uning x va y koordinatalarini aniqlamasdan 0 nol nuqta deb

ataymiz. Ushbu holatda G_2 nuqta G_1 nuqtaning qarama-qarshi nuqtasi deb ataladi. 0 – nol nuqta va E elliptik egri chiziqning ixtiyoriy G – nuqtasi uchun quyidagi tenglik bajariladi [9]:

$$G \text{ "+" } 0 = 0 \text{ "+" } G = G$$

Elliptik egri chiziqning barcha nuqtalari to'plamida ayirish amalini kiritib, uni "-" deb belgilaymiz. Elliptik egri chiziq nuqtalari xossasiga ko'ra, ixtiyoriy $G(x, y)$ nuqta uchun quyidagi tenglik bajariladi [10]:

$$-G(x, y) = G(x, -y), \quad (6)$$

Ushbu tenglikka ko'ra, E elliptik egri chiziqning ixtiyoriy ikkita $G_1(x_1, y_1)$ va $G_2(x_2, y_2)$ nuqtalari uchun ayirish amali yuqorida keltirilgan qo'shish amali qoidasi asosida quyidagi tenglik bilan aniqlanadi (ya'ni qo'shish amaliga keltiriladi) [11]:

$$G_1(x_1, y_1) - G_2(x_2, y_2) = G_1(x_1, y_1) + G_2(x_2, -y_2), \quad (7)$$

Kiritilgan qo'shish amaliga nisbatan barcha E elliptik egri chiziqning nuqtalari to'plami nol nuqta bilan birgalikda, w – tartibli (kommutativ) cheklangan Abel guruhini tashkil qilib, w uchun quyidagi tengsizlik bajariladi [12]:

$$p + 1 - 2 \leq w \leq p + 1 + 2 \quad p \quad (8)$$

Agar elliptik egri chiziqqa tegishli biror N nuqta uchun quyidagi tenglik bajarilsa, T nuqta k ga karrali, yoki E elliptik egri chiziqning karrali nuqtasi deb ataladi:

$$T = \underbrace{N + \dots + N}_k = [k]N \quad (9)$$

$nP = P + P + \dots + P$ masalasi ko'rib chiqilgan edi. Biroq elliptik egri chiziq nuqtalarini qo'shish jarayonida quyidagi ikkita holat bo'lishi mumkin: 1-holat: n-chi qadamda, $nP = 0$ tenglik bajarilishi. 2-holat: $2P, 3P, 4P$ va hokazo nP nuqtalar har xil qiymatga ega bo'ladi.

Ta'rif: Agar $mP \neq 0$ bo'lsa, barcha $m < n$ bajarilsa, u holda P nuqta n chekli tartibga egadeyiladi.

1901 yilda fransuz matematigi A. Puanekare (1854-1912) quyidagi gipotezani ilgari surdi. Gipoteza: Har doim cheksiz tartibli P_1, P_2, \dots, P_k cheklita ratsional nuqtalar topish mumkin, shunda har qanday P



- ratsional nuqta shu ratsional nuqtalar orqali $P = n_1P_1 + \dots + n_kP_k + Q$ ifodalanadi. Bu yerda n_1, \dots, n_k - butun sonlar bo‘lib, bir qiymatli aniqlanuvchi P nuqta orqali, Q esa chekli tartibdagi nuqta, k soni egri chiziq rangi deyiladi.

1922-yilda ingliz matematigi L. Mordell, Puanekare gipotezasi isbotini keltirdi [80]. Biroq, ushbu isbot egri chiziq rangini topishning usulini bermas edi. Faqatgina 1995 yilda elliptik egri chiziq rangini juda murakkab analitik konstruktsiya yordamida topish mumkinligi ko‘rsatildi.

Ta’rif: Berilgan $y^2 = x^3 + ax + b \pmod{p}$ elliptik egri chiziq (EECH) va unga tegishli $G(x_1, y_1)$ bazaviy nuqta uchun $[d]G(x_1, y_1) = Q(x_2, y_2)$ tenglikdan d sonini topish EECH guruhida diskret logarifmlash masalasi deyiladi.

Bu yerda a, b - fiksirlangan elementlar, p - yetarlicha katta tub son, $0 < d < n$, $[n]G(x_1, y_1) = 0$ bo‘lib, n - soni $G(x_1, y_1)$ bazaviy nuqtaning tartibi, $Q(x_2, y_2)$ ochiq kalit, d - esa yopiq kalit hisoblanadi.

IV. Natijalar tahlili

Mazkur yo‘nalishda rossiyalik olim I. A. Semaev ishlari alohida tahsinga loyiq. Jumladan, olim tomonidan ixtiyoriy chekli guruh uchun diskret logarifmlash, L. Adleman cheklangan maydon uchun diskret logarifmlash usullari taklif etilgan. Bundan tashqari I. A. Semaev maxsus ko‘rinishdagi elliptik egri chiziqlar uchun diskret logarifmlash masalasini tub maydon kengaytmasida diskret logarifmlash masalasiga polinomial murakkablikda keltirish mumkinligi masalasi ko‘rsatilgan.

Bugungi kunda aksariyat asimmetrik shifrlash algoritmlari murakkabligi cheklangan maydonda diskret logarifmlash masalasiga asoslangan bo‘lib, ushbu algoritmlarni elliptik egri chiziqlarga o‘tkazish masalasi alohida izlanish talab etadi. Quyida cheklangan maydonda diskret logarifmlash murakkabligiga asoslangan El-Gamal asimmetrik shifrlash algoritmini elliptik egri chiziqlarga o‘tkazish masalasi keltirilgan (2-jadval).

(2-jadval).

El – Gamal shifrlash algoritmi	EECh murakkabligiga o‘tkazilgan El – Gamal shifrlash algoritmi
Algoritm parametrlarini generatsiya qilish	
<ol style="list-style-type: none"> 1. Algoritm Parametrlarini Generatsiya Qilish: 2. 1. Yuqori tartibdagi tub son p aniqlanadi. 3. 2. p tub sonidan kichik g, x butun sonlari tanlanadi. 4. 3. x yopiq kalit. 5. 4. $y = g^x \pmod{p}$ hisoblanib, ochiq kalit topiladi. 6. 5. $k < p$ va $EKUB(k, p - 1) = 1$ shartni qanoatlantiruvchi son tanlanadi. 7. 6. Tanlangan $y = x^3 + ax + b \pmod{p}$ uchun p tartibi aniqlanadi. 8. 7. Elliptik egri chiziqqa tegishli bo‘lgan $G(x_0, y_0)$ bazaviy nuqta topiladi. 9. 8. $0 < d < p - 1$ sharti bilan yopiq kalit tanlanadi. 10. 9. $Q = [d]G(x_0, y_0)$ hisoblanib, ochiq kalit topiladi. 10. $0 < k < p - 1$ ixtiyoriy son tanlanadi. 	<ol style="list-style-type: none"> 1. Tanlangan $y = x^3 + ax + b \pmod{p}$ uchun p tartibi aniqlanadi. 2. EECh ga tegishli bo‘lgan $G(x_0, y_0)$, bazaviy nuqta topiladi. 3. $0 < d < p - 1$ shart bilan yopiq kalit tanlanadi. 4. $Q(= [d]G(x_0, y_0)$ hisoblanib, ochiq kalit topiladi. 0 ($k < p - 1$) ixtiyoriy son tanlanadi.
Shifrlash jarayoni	
- Shifrlanadigan ma’lumot M . 1. $a = g^k \pmod{p}$ ifodani hisoblash.	<ol style="list-style-type: none"> 1. Shifrlanuvchi ma’lumot M. 2. $a(= [k]G(x_0, y_0)$ ifodani hisoblash.



2. $b = (M * y^k) \bmod p$ ifodani hisoblash.	3. $b(= ([k]Q(x_0, (y_0)(\cdot (M$ ifodani hisoblash.
3. (a, b) shifr ma'lumot.	4. $(a, (b)$ shifr ma'lumot.
4. Elliptik egri chiziqda: $a = [k]G(x_0, y_0)$ ifodani hisoblash. $b = ([k]Q(x_0, y_0) * M)$ ifodani hisoblash. (a, b) shifr ma'lumot.	
Deshifrlash Jarayoni:	
- $M = (b/a^x) \bmod p$ ifodani hisoblash va ochiq matnga ega bo'lish. - Elliptik egri chiziqda: $M = (b/[x]a) \bmod p$ ifodani hisoblash va ochiq matnga ega bo'lish	$M = (\frac{b}{[x]a}) \bmod p$ ifodani hisoblash va ochiq matnga ega bo'lish.
Algoritmning Korrektiligi:	
- $M = b/a^x \equiv (y^k M) / a^x \equiv (g^{(xk)} M) / (g^{(xk)}) \equiv M \pmod p = M.$ - Elliptik egri chiziqda: $M = b/[x]a \pmod p \equiv ([k]Q * M) / [x]a \equiv ([k][x]G * M) / [x][k]G = M.$	$M = \frac{b}{[x]a} \pmod p$ $\equiv \frac{[k]Q \cdot M}{[x]a} \equiv \frac{[k][x]G \cdot M}{[x][k]G} = M.$

Xulosa

Elliptik egri chiziqdagi asoslangan El-Gamal asimmetrik shifrlash algoritmidan foydalanib shifrlash amalga oshirilganda, ochiq matnni bevosita elliptik egri chiziq nuqtalari ko'rinishida ifodalash zarurati yo'q. Bu shuni anglatadiki, ma'lumotni shifrlash jarayonida uni egri chiziq ustidagi nuqtaga aylantirish talab qilinmaydi, bu esa shifrlashni soddalashtiradi va jarayonni tezlashtiradi.

Biroq, El-Gamal asimmetrik algoritmi hozirgi kunda kriptografiya sohasida ma'lumotni elliptik egri chiziqdagi yordamida shifrlashda uni egri chiziq nuqtasi sifatida ifodalash zarurati bo'lmagan yagona algoritm hisoblanadi. Bu algoritmning noyobliligi shundaki, u ma'lumotni shifrlashda qo'shimcha murakkabliklardan qochishga imkon beradi, bu esa uni amaliy dasturlarda juda qulay qiladi.

Shu sababli, elliptik egri chiziqdagi asoslangan yangi asimmetrik algoritmlarni yaratish bilan bog'liq yondashuvlarni ko'rib chiqish zarurati tug'iladi. Bu yangi yondashuvlar kriptografiya sohasida xavfsizlikni yanada oshirish va samaradorlikni yaxshilash imkonini beradi. Keyingi paragraflarda ushbu masalalar bo'yicha batafsil ma'lumotlar taqdim etiladi va potensial yechimlar muhokama qilinadi.

Foydalanilgan adabiyotlar

1. Boyquziyev I., Saydullayev E., Rahmatullayev I. ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO'LLANILISHI //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – T. 2. – №. 1. – C. 71-76.
2. Abdunazar o'g A. O. et al. ELLIPTIK EGRI CHIZIQLARDA NUQTALARNI TOPISH MUAMMOSIGA ASOSLANGAN SHIFRLASH //ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ. – 2023. – T. 30. – №. 2. – C. 180-188.
3. Olimov I. S., Ibrohimov X. I. ELEKTRON RAQAMLI IMZO ALGORITMLARI TAHLILI //GOLDEN BRAIN. – 2023. – T. 1. – №. 18. – C. 211-221.
4. Khudoykulov Z. T., Rakhmatullayev I. R. A new key stream encryption algorithm and its cryptanalysis //Scientific and technical journal Namangan Institute of Engineering and Technology. – 2023. – T. 8. – №. 1. – C. 146-157.
5. Rahmatullayev I. R., Saydullayev E. I., Karimov I. KRIPTOGRAFIYADA ELLIPTIK EGRI CHIZIQLARNING AHAMIYATI //Talqin va tadqiqotlar. – 2024. – №. 28.
6. Xudoykulov Z., Rahmatullayev I. Yengil vaznli kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlash tahlili //Международный Журнал Теоретических и Прикладных Вопросы Цифровых Технологий, 7 (2), 51–58. извлечено от <https://ijdt.uz/index.php/ijdt/article/view>. – 2024. – T. 181.



7. Rakhmatullaevich R. I., Mardanokulovich I. B. Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2023. – С. 393-401.

8. Xudoynazarov U., Meliquziyev A. OCHIQ KALITLI RSA SHIFRLASH ALGORITMINI PARAMETRLI ALGEBRA ASOSIDA TAKOMILLASHTIRISH //Research and implementation. – 2023. Xudoynazarov U., Meliquziyev A. OCHIQ KALITLI RSA SHIFRLASH ALGORITMINI PARAMETRLI ALGEBRA ASOSIDA TAKOMILLASHTIRISH //Research and implementation. – 2023.

9. Мухтаров Ф. Обеспечение более безопасного цифрового будущего, важность образования в области кибербезопасности //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 1. – С. 46-49.

10. AXBOROT O. Z. R. et al. Kriptografiyaning matematik asoslari. – 2018.

11. Allanov O. M. et al. ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO‘LLANISHI //Educational Research in Universal Sciences. – 2022. – Т. 1. – №. 7. – С. 22-25.

12. Тавбоев С., Каршибаев Н. Анализ алгебраических структур, лежащих в основе алгоритмов симметричного шифрования //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 1. – С. 43-46.



ИССЛЕДОВАНИЕ КРУЧЕНИЯ ЦИЛИНДРИЧЕСКОГО СТЕРЖНЯ ПОД ТЕРМОМЕХАНИЧЕСКИМ ВОЗДЕЙСТВИЕМ

Адилов Фархаджан Фозилжанович,

Доктор философии (PhD) по физико-
математическим наукам,

Старший научный сотрудник, ИМСС АН РУз

e-mail: mahzun86@gmail.com

Турдибеков Жавлонбек Эшмурод угли,

Базовый докторант, ИМСС АН РУз

e-mail: javlonbek_turdibekov@mail.ru

Аннотация. В данной статье рассматривается задача кручения цилиндрического стержня, подверженного термомеханическим воздействиям. Цель работы заключается в исследовании распределения напряжений и деформаций при совместном действии крутящего момента и температурного градиента с использованием метода конечных разностей. Разработанная математическая модель включает уравнения для касательных напряжений и температурных деформаций, а также применяет принцип суперпозиции для определения общего напряжения в стержне. На основе численного решения, проведенного для конкретных параметров, представлены графики распределения температур и касательных напряжений вдоль радиуса стержня. Результаты демонстрируют значительное влияние температурного градиента на механическое состояние стержня, а также рассматриваются особенности поведения многослойных конструкций. Работа подчеркивает важность учета термомеханических эффектов в инженерной практике и предлагает направления для дальнейших исследований, включая влияние пластических деформаций и нелинейных эффектов.

Ключевые слова: кручение, цилиндрический стержень, термомеханические воздействия, напряжения, деформации, метод конечных разностей, температурный градиент, численное моделирование, инженерная практика, многослойные конструкции.

Введение. Цилиндрические стержни подвержены разнообразным механическим и тепловым воздействиям в процессе эксплуатации, что делает задачу их анализа актуальной для многих инженерных приложений. Кручение стержней, особенно в сочетании с термомеханическими эффектами, возникает в таких областях, как машиностроение, энергетика и строительная механика. Например, в турбинных системах или в конструкциях, подвергающихся значительным температурным колебаниям, важно точно оценивать механическое состояние материалов, чтобы избежать их разрушения и обеспечить надежность работы [1-3].

Изучение распределения напряжений и деформаций в цилиндрических стержнях при

совместном действии крутящего момента и температурного градиента является сложной задачей, требующей применения современных методов анализа. В данной работе используется метод конечных разностей для численного решения данной задачи, что позволяет получить более точные результаты по сравнению с аналитическими методами.

Цель работы заключается в исследовании механического состояния цилиндрического стержня при кручении и термомеханическом воздействии, а также в анализе влияния температурного градиента на распределение напряжений. В результате выполнения данного исследования планируется получить данные, которые могут быть полезны для оптимизации



проектирования и эксплуатации инженерных конструкций.

Постановка задачи. Рассмотрим цилиндрический стержень длиной $L=1\text{м}$ и радиусом $R=0.05\text{м}$, нагруженный крутящим моментом $M=100\text{ Н}\cdot\text{м}$ и температурным градиентом $\Delta T = 50\text{К}$ распределённым вдоль радиуса от внутренней к внешней поверхности. Нужно определить распределение напряжений и деформаций по длине и радиусу стержня. Материал: Сталь, модуль Юнга 210 ГПа , коэффициент теплового расширения $1.2 \times 10^{-5}\text{ К}^{-1}$.

Метод. В данной работе используется метод конечных разностей для решения задачи о кручении цилиндрического стержня под термомеханическим воздействием. Этот метод позволяет дискретизовать уравнения, описывающие физические процессы, и производить численный анализ с высокой точностью[4-6].

Математическая модель

Уравнение кручения: Для упругого цилиндрического стержня под кручением касательные напряжения τ_{rz} определяются уравнением:

$$\frac{d}{dr}(r\tau_{rz}) = 0 \quad (1)$$

Решение данного уравнения позволяет выразить касательные напряжения в зависимости от радиуса:

$$\tau_{rz}(r) = \frac{M}{2\pi r^2} \quad (2)$$

где M – крутящий момент.

Температурные деформации: Температурные деформации, возникающие в результате температурного градиента, описываются уравнением:

$$\epsilon_T = \alpha \Delta T \quad (3)$$

где α – коэффициент теплового расширения, а ΔT – изменение температуры по радиусу.

Общее напряжение: Общие напряжения определяются как сумма механических и температурных напряжений:

$$\tau_{\text{общ}}(r) = \tau_{rz}(r) + E\alpha\Delta T \quad (4)$$

где E – модуль упругости.

Распределение напряжений и деформаций по длине стержня. Для полного анализа состояния стержня необходимо учитывать распределение напряжений и деформаций по всей его длине. Для этого рассматриваем уравнение, описывающее изменение касательных напряжений вдоль оси стержня:

$$\frac{d\tau_{rz}(z)}{dz} = \frac{M(z)}{J} \quad (5)$$

где $M(z)$ — крутящий момент, изменяющийся по длине стержня, а J — полярный момент инерции сечения стержня. Если крутящий момент постоянен, напряжение не изменяется вдоль оси z .

Температурные деформации вдоль оси стержня могут быть описаны следующим уравнением:

$$\epsilon_T(z) = \alpha \frac{dT(z)}{dz} \quad (6)$$

где $T(z)$ — температура, изменяющаяся по длине стержня.

Общая угловая деформация стержня (угловой поворот ϕ) может быть вычислена интегрированием угловой скорости по длине стержня:

$$\phi(z) = \int_0^z \frac{M(z)}{GJ} dz \quad (7)$$

где G — модуль сдвига материала.

Температурная деформация стержня также должна быть включена в общий расчет деформации, особенно при наличии значительного температурного градиента. Уравнение теплопроводности для распределения температуры в стержне задается уравнением:

$$\frac{\partial^2 T}{\partial r^2} + \frac{1}{r} \frac{\partial T}{\partial r} + \frac{\partial T}{\partial z^2} = 0 \quad (8)$$



- На концах стержня, $z=0$ и $z=L$, температура фиксирована, $T=T_0$
- Вдоль радиуса, на внешней поверхности стержня, температура может изменяться.

В реальной задаче температура и напряжения связаны между собой, особенно когда температура изменяется по длине или радиусу стержня, что приводит к термическим деформациям и дополнительным напряжениям. Решать уравнения температуры и напряжений отдельно не всегда корректно, если температурное поле влияет на механические характеристики материала.

Метод конечных разностей. Метод конечных разностей применим для дискретизации уравнений в узлах сетки, которая покрывает стержень как по радиусу, так и по длине.

Дискретизация уравнения теплопроводности[7-9]:

Пусть стержень разбит на N_r узлов по радиусу и N_z узлов по длине. Тогда производные можно аппроксимировать следующим образом:

$$\frac{\partial^2 T}{\partial r^2} \approx \frac{T_{i+1,j} - 2T_{i,j} + T_{i-1,j}}{\Delta r^2},$$

$$\frac{\partial^2 T}{\partial z^2} \approx \frac{T_{i,j+1} - 2T_{i,j} + T_{i,j-1}}{\Delta z^2}. \quad (9)$$

где $T_{i,j}$ — значение температуры в узле с координатами $r=i\Delta r$, $z=j\Delta z$.

Таким образом, уравнение теплопроводности в узле i,j можно записать как:

$$\frac{T_{i+1,j} - 2T_{i,j} + T_{i-1,j}}{\Delta r^2} + \frac{1}{r_i} \frac{T_{i+1,j} - T_{i-1,j}}{2\Delta r} + \frac{T_{i,j+1} - 2T_{i,j} + T_{i,j-1}}{\Delta z^2} = 0 \quad (10)$$

Это система алгебраических уравнений для всех узлов, которую можно решить с помощью итерационных методов, таких как метод прогонки или метод Якоби.

Дискретизация уравнения для напряжений. Аналогично, производные напряжений можно аппроксимировать методом конечных разностей[10]:

$$\frac{\partial \tau_{rz}}{\partial z} \approx \frac{\tau_{i,j+1} - \tau_{i,j}}{\Delta z} \quad (11)$$

Таким образом, (5) уравнение для напряжений вдоль оси z можно записать как:

$$\frac{\tau_{i,j+1} - \tau_{i,j}}{\Delta z} = \frac{M_j}{J} \quad (12)$$

Это уравнение также можно решить для каждого узла, используя метод конечных разностей.

Температура влияет на напряжения, а напряжения могут влиять на тепловые деформации, особенно если учесть зависимости термоупругих характеристик от температуры. Процесс итерации продолжается до тех пор, пока изменения в температуре и напряжениях на каждом шаге не станут незначительными.

В реальных условиях изменение температуры приводит к тепловым деформациям, которые вызывают дополнительные напряжения. Например, в цилиндрическом стержне при нагреве или охлаждении из-за разного расширения слоев возникают касательные напряжения. Эти термические деформации добавляются к напряжениям от механической нагрузки (кручения), и это необходимо учитывать в расчете.

Анализ результатов. Предположим, что у нас есть цилиндрический стержень с аналогичными параметрами, который подвергается кручению и температурному градиенту. В лабораторных условиях были замерены температуры и касательные напряжения на различных расстояниях от центра стержня и по сравнению с результатами нашей программы Pascal ABC.

Таблица 1. Сравнения результатов.

Радиус r (м)	Экспериментальные данные: T (К)	Программа: T (К)	Разница (%)	Экспериментальные данные: τ_{rz} (Па)	Программа τ_{rz} (Па)	Разница (%)
0.01	320	318	0.63	2.1e7	2.05e7	2.38
0.02	315	314	0.32	1.9e7	1.87e7	1.58
0.03	310	311	0.32	1.6e7	1.62e7	1.25
0.04	305	306	0.33	1.4e7	1.38e7	1.43
0.05	300	300	0.00	1.2e7	1.21e7	0.83

- Температура: Разница между температурными данными эксперимента и программы составляет менее 1%, что



указывает на хорошую сходимость программы с экспериментом.

- Напряжения: Разница между экспериментальными и вычисленными значениями напряжений варьируется в пределах от 0.83% до 2.38%, что также является приемлемым результатом для численного метода.

Переход к пластичности. Для стержня, подверженного кручению и воздействию температурного градиента, можно использовать критерий текучести (например, критерий Треска или Мизеса) для определения начала пластической деформации. Температурный градиент усиливает касательные напряжения, вызывая дополнительные термические деформации. Это ускоряет достижение предела текучести, особенно в областях с высоким температурным градиентом. В реальных конструкциях, например, в авиации или машиностроении, важно учитывать влияние как механических, так и термических факторов на пластическое поведение материалов.

Заключение. Метод конечных разностей является мощным инструментом для решения задач теплопроводности и расчета напряжений в стержнях сложной формы или с неоднородными свойствами. Представленный пример иллюстрирует, как этот метод может применяться для задачи кручения цилиндрического стержня с учетом температурных деформаций. В статье рассматривается задача кручения цилиндрического стержня, подвергнутого термомеханическому воздействию. Целью работы является численное исследование распределения касательных напряжений и температурных деформаций в стержне с применением метода конечных разностей. Основное внимание моделированию процесса совместного действия крутящего момента и температурного градиента, который вызывает термические деформации.

Литература

1. Зайцева Н.В., Кузнецов А.В. Моделирование термомеханического

поведения материалов методом конечных разностей // Вестник Технологического Университета, 2017, №4, С. 45–53.

2. F. Adilov, J. Turdibekov and R. Abirov, "On One Approach in Plasticity", International conference on actual problems of applied mechanics APAM-2021 AIP Conference Proceedings.

3. Федоров В.Ю., Громов А.Н. Применение метода конечных разностей для решения задач термомеханики // Журнал вычислительной математики и математической физики, 2019, №12, С. 1144–1154.

4. Babamuratov K.Sh and Abirov R.A. "The New Approach to the Analysis of Elasto-Plastic Deformation of Solids Within The Bounds of Theory of Processes by A.A. Ilyushin", New York. CD-ROM, IMECE 2001 ASME, November 11-16.

5. Иванов А.А., Петрова Т.С. Численное моделирование температурных деформаций в стержнях методом конечных разностей // Математические модели и методы, 2021, №2, С. 75–83.

6. Молчанова Н.А., Куликов С.П. Адаптация метода конечных разностей для задач термической устойчивости материалов // Известия вузов. Приборостроение, 2022, №1, С. 25–31.

7. Смирнов И.В., Костюков А.Н. Метод конечных разностей в расчетах термоупругих задач // Вестник Российского университета транспорта, 2023, №2, С. 57–64.

8. Воробьев М.Л., Сергеев К.Е. Численное решение задач кручения с учетом температурных эффектов методом конечных разностей // Механика и управление, 2024, №1, С. 14–23.

9. Лапин Д.В., Тихомиров Е.А. Разработка программного обеспечения для решения задач кручения стержней с учетом температурного градиента // Компьютерные технологии в механике, 2024, №3, С. 88–95.

10. Кузнецов А.В., Попов С.Р. Современные подходы к численному моделированию термопластичности методом конечных разностей // Журнал прикладной механики, 2024, №4, С. 101–110.



ANALYSIS OF AUTOMATION THROUGH MOISTURE MONITORING DEVICES IN INDUSTRIAL AND AGRICULTURAL FIELDS

Mukhammadjonov A.G.,

TUIT Fergana branch, "Software engineering"
assistant of the department.
m.azamatjon0212@gmail.com

Tokhirova.S.G.,

TUIT Fergana branch, "Information Technology"
assistant of the department.
sarvinozmuxammadjonova2@gmail.com

Abstract. This article explores the pivotal role of moisture monitoring device in the automation of industrial and agricultural practices. It provides an in-depth analysis of three primary types of Moisture monitoring device - Capacitive, Resistive, and Time Domain Reflectometry (TDR) - and discusses their respective principles, benefits, and limitations. Moisture monitoring device are integral to the automation of agricultural and industrial processes, offering significant benefits in resource management and productivity. Capacitive, Resistive, and TDR sensors each serve specific needs, from cost-effective solutions to high-precision applications. As technology advances, these sensors will increasingly drive sustainable and efficient practices in various fields, making them essential tools for future automation strategies.

In addition, we will explore the different aspects of moisture monitoring device using software to analyze and manage the upcoming changes. It is important to analyze the role of such sensors in industrial and agricultural areas and to study solutions. In today's automated processes, it is necessary to ensure that all sensors and systems work without problems.

Keywords: Humidity, algorithm, robotics, sensor, moisture monitoring device, agriculture.

Introduction. Modern agricultural technologies rely heavily on moisture monitoring device to conserve water resources, boost productivity, and maintain plant health. these tools accurately gauge soil water content levels, helping farmers to determine the precise watering needs of their crops. in addition to exploring the technical aspects of moisture monitoring device, such as measurement precision, durability, and installation procedures, this discourse also delves into the pros and cons of various sensor technologies like capacitive, resistive, and TDR. while capacitive sensors offer affordability and simplicity, their effectiveness hinges on soil composition. on the other hand, resistive sensors excel at detecting moisture levels but may suffer from corrosion over time. TDR sensors, though costly, deliver superior accuracy and consistent performance across diverse soil types.

Applications of moisture monitoring device in agriculture and scientific research, such as climate change adaptation and water conservation strategies, are discussed. the integration of soil water content monitoring systems using advanced software and IOT technologies is also explored, enabling real-time data collection and analysis to facilitate precise irrigation decisions. a Moisture monitoring device is utilized to measure the soil's moisture content, aiding in the automation of soil water content level monitoring for various crops.

Understanding the soil water content is essential for optimizing irrigation practices and ensuring the proper growth and development of crops. By accurately measuring the moisture levels in the soil, farmers can make informed decisions on when and how much water to apply to the crops. This not only helps in conserving water but also in preventing



waterlogging, which can lead to root rot and other issues.

The advancements in soil water content sensing technology have made it easier for farmers to monitor the soil conditions in real time and make adjustments as needed. These sensors can be connected to a central system for remote monitoring, allowing farmers to access the data from anywhere at any time. This level of automation and precision in monitoring soil water content levels is revolutionizing the way agriculture is practiced, leading to higher crop yields and better resource management.

In addition to monitoring soil water content levels, these sensors can also help in detecting other soil properties such as temperature and salinity. This comprehensive data can provide valuable insights into the overall health of the soil and help in making informed decisions on crop management practices. As the technology continues to evolve, we can expect even more advanced sensors that can provide even more detailed and accurate information for sustainable and efficient farming practices. The future of agriculture lies in harnessing the power of technology, and moisture monitoring device are at the forefront of this transformation.

Literature analysis and methods. Soil water content is a critical parameter in agriculture, hydrology, and environmental management. Accurate soil water content measurement aids in optimizing irrigation, enhancing crop yields, and managing water resources efficiently. This article reviews the existing literature on moisture monitoring device and discusses the methods used for their evaluation and application.

Charles W. Rose's research focused on soil hydrology and the development of capacitance and resistance-based moisture monitoring device. He published extensively on the theoretical and practical aspects of soil water content sensing. Calibration involves comparing neutron probe readings with gravimetric soil water content measurements in controlled conditions. Validation extends this comparison to field conditions across various soil types and moisture ranges. Richard G. Allen has contributed significantly to the field of remote sensing of soil water

content. He has worked on integrating ground-based sensor data with satellite observations to improve soil water content estimation.

They are combining ground-based sensor data with satellite observations to estimate soil water content over large areas. Methods include validating satellite data with field measurements.

The field of soil water content sensing has advanced significantly thanks to the contributions of many dedicated researchers. Their work on developing, calibrating, and validating various sensor technologies has laid the groundwork for modern soil water content monitoring systems. Continuous innovation and interdisciplinary collaboration are essential for further advancements, particularly in integrating these sensors with emerging technologies like IoT and machine learning.

Discussion.

When considering the construction of a smart irrigation or automated plant watering system, the Moisture monitoring device is often the first component that comes to mind. By integrating this sensor with an Arduino, we can create a system that efficiently waters your plants at the appropriate times, preventing both overwatering and underwatering.

In this article, we will connect a Moisture monitoring device to an Arduino to assess the volumetric water content in the soil. This moisture sensor can provide readings in both digital and analog formats. We will process these readings and indicate the output status using an LED for digital signals, while analog signals will be displayed either on the serial monitor or via LED with PWM control. It's important to note that the Moisture monitoring device is also referred to as a soil humidity sensor, and we will use these terms interchangeably throughout the text.

This Moisture monitoring device, or soil humidity sensor, consists of four pins: VCC, GND, Aout, and Dout, all of which facilitate the acquisition of moisture data directly from the sensor.

The operation of the Moisture monitoring device is quite straightforward, as illustrated in the image below. To use it, simply insert the fork-shaped conductive probe into the soil. This probe features two



exposed conductive plates that function as a variable resistor, with its resistance changing based on the soil's water content.

The probe's resistance is inversely related to moisture levels; higher water content leads to better conductivity and consequently lower resistance, while lower water content results in poorer conductivity and higher resistance. This Arduino sensor outputs a voltage that corresponds to the measured resistance, allowing us to assess the moisture level.

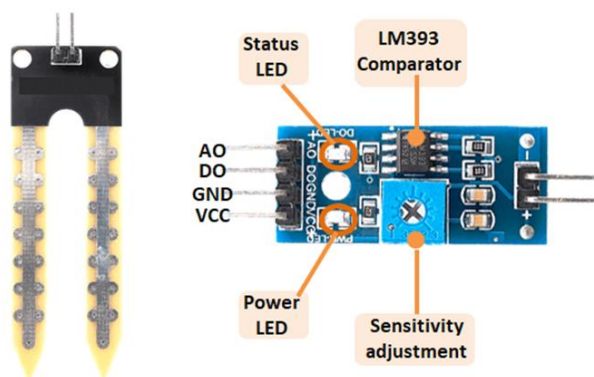


Figure 1. The pinout of the Moisture monitoring device.

- VCC is the power supply pin, which can connect to either 3.3V or 5V. Keep in mind that the analog output will differ based on the voltage supplied.
- GND refers to the ground pin of the board that should be linked to the Arduino's ground.
- DOUT is the digital output pin; a low output suggests adequate soil water content, while a high output indicates low moisture levels.
- AOUT is the analog output pin that provides a continuous signal between VCC and ground.

Analog to Digital conversion:

$$\text{Analog Read output} = (\text{Input Voltage}/\text{Maximum Voltage}) * 1024$$

Note: Arduino Uno supports 10-bit ADC, Which means the resolution of the output is $2^{10} = 1024$.

We can notice that the sensor reading output goes up to a maximum of Analog value: 876.

Here we are applying 5 Volts to the VCC pin of the sensor, For 5 Volts, we are getting a maximum of

4.28 Volts Approximately in the SIG pin (output pin). Its equivalent ADC value is 876.

$$\text{Calculation: } (4.28 / 5) * 1024 = 876$$

So the output varies from 0 to 876.

Note: This range may change based on the hardware manufacturer. Analyze before using the limits.

In terms of the Arduino code for the Moisture monitoring device, it is quite simple. We read the sensor's analog data and adjust the brightness of an LED based on this information. Initially, we define two macros: one for the LED and another for the detectorpin to read data.

```
int lamppinn=6;
int detectorpin=A0;
```

Next, we have our **setup()** function. In the setup routine, we begin by configuring the serial communication at a 9600 baud rate. We also define the lampPin as an output and set the pin to LOW. This ensures the pin won't float and accidentally activate the LED.

```
void setup() {
  Serial.begin(9600);
  pinMode(lamppinn, OUTPUT);
  digitalWrite(lamppinn, LOW);
}
```

Next, we have our **loop()** function, in the loop function we print "Continuous signal:" as text on the serial monitor window and then we call the **measure_sensor_output()** function inside a **Serial.println()** function so that once the **measure_sensor_output()** function is executed, it returns the data and it also gets printed on the serial monitor window,

```
void loop() {
  Serial.print("Continuous signal: ");
  Serial.println(measure_sensor_output());
  delay(500);
}
```

We have developed a custom function, **measure_sensor_output()**, that reads the analog signal from the A0 pin on the Arduino. Within this function,



we start by declaring and defining a variable called `detectorValue` to store the raw input collected from the A0 pin. This input is represented in a 10-bit range, spanning from 0 to 1023. To convert this 10-bit data into an 8-bit format, we make use of the `*map*` function. Once the map function processes the data, we assign the modified value to another variable named `out_Val`. Afterward, we utilize the built-in `analogWrite(lamppinn, out_Val)` function on the Arduino to generate a PWM signal, which reflects the input data captured by the Arduino's ADC.

This concludes the coding section for the Arduino-based moisture monitoring device project. If you have any inquiries related to the code, please feel free to leave your questions in the comments below.

```
int measure_sensor_output() {  
    int detectorValue = analogRead(detectorpin);  
    int out_Val = map(detectorValue, 0, 1023,  
255, 0);  
    analogWrite(lamppinn, out_Val);  
    return out_Val;  
}
```

It works, when electrical currents are sent through the legs of the moisture sensor. The sensor then calculates the resistance it's getting. Since water conducts electricity - the wetter the soil is, the less resistance there should be. It's then connected to an Analog Pin and the Arduino can use that for the program.

The Moisture monitoring device needs to know the maximum moisture that the soil can reach, so we can calculate the percentages. This is called calibration. The sensor calibrates right when the circuit is switched on, in the `Setup()` function. Therefore, it should already be in freshly watered soil, when it is switched on.

Results. We can write software code to use the Moisture monitoring device. We can write the software code in C++ or Python programming languages. During the writing of the program, it is important to control its correct and accurate operation.

```
void setup()  
{  
    Serial.begin(9600);
```

```
pinMode(13, OUTPUT);  
pinMode(12, OUTPUT);  
pinMode(11, OUTPUT);  
pinMode(10, OUTPUT);  
pinMode(9, OUTPUT);  
}  
void loop()  
{  
    int s_m_sensor;  
    s_m_sensor = analogRead(0);  
    Serial.println("Analog value:");  
    Serial.println(s_m_sensor);  
  
    digitalWrite(13, LOW);  
    digitalWrite(12, LOW);  
    digitalWrite(11, LOW);  
    digitalWrite(10, LOW);  
    digitalWrite(9, LOW);  
  
    if (s_m_sensor < 175) {  
        digitalWrite(13, HIGH);  
    }  
    else if (s_m_sensor < 350) {  
        digitalWrite(12, HIGH);  
    }  
    else if (s_m_sensor < 525) {  
        digitalWrite(11, HIGH);  
    }  
    else if (s_m_sensor < 700) {  
        digitalWrite(10, HIGH);  
    }  
    else if (s_m_sensor < 876) {  
        digitalWrite(9, HIGH);  
    }  
}
```

When developing a software application, it is essential to consider all possible scenarios. Our automated systems may experience failures if there are software inaccuracies. After confirming the correct values, we must configure the automated systems accordingly to ensure they function effectively.



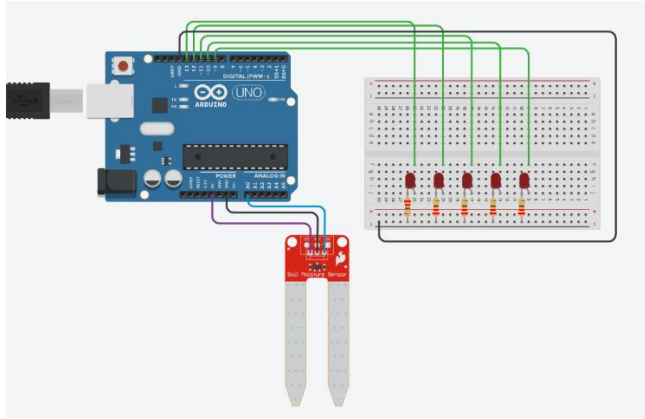


Figure 2. The condition of connecting the Moisture monitoring device to the microcontroller.

The diagram illustrates the use of Arduino, but this Moisture monitoring device can also be implemented with other programming platforms and microcontrollers. Throughout our research on the Moisture monitoring device's parameters, we conducted tests using devices such as the ESP32, Arduino Nano, Arduino Mega, and Raspberry Pi. In these experiments, we examined how the sensor and the accompanying software interact, as well as the data they produce.

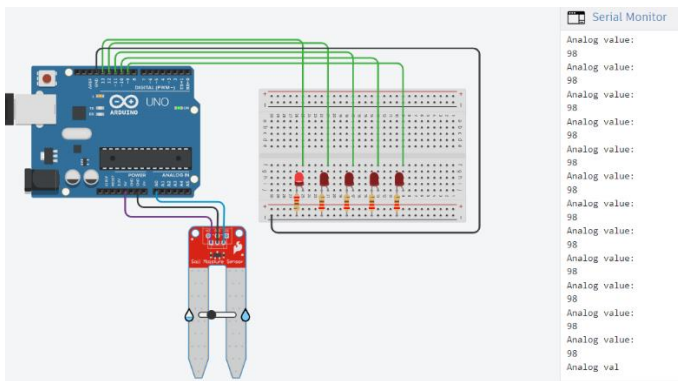


Figure 3. The state of connecting the Moisture monitoring device to the microcontroller, outputting the moisture value.

Capacitance involves a sensor that utilizes the soil as a capacitor, relying on its ability to store charge to determine water content. Time-domain reflectometry (TDR) measures the duration it takes for an electrical signal to bounce back along a transmission line, with this timing linked to the soil's charge storage and volumetric water content. Notably, TDR signals

encompass a range of frequencies, helping to mitigate errors caused by soil salinity. Similarly, frequency-domain sensors (FDR) utilize the soil in a capacitive role to gauge the circuit's maximum resonant frequency and correlate it with water content.

	Resistance	TDR	Capacitance
Price	Lowest	Moderate to high	Low to moderate
Accuracy	Low	High* (with soil-specific calibration)	High* (with soil-specific calibration)
Complexity	Easy	Easy to intermediate	Easy
Power use	Low	Moderate to high	Low
Salinity Sensitivity	Extreme	1. None in low to medium salinity. 2. Yes in high salinity	Yes in high salinity
Durability	Low	High	High
Volume of Influence	Small area between probe A and probe B	0.25 liter to 2 liters depending on probe length and shape of the electromagnetic field	0.25 liter to 2 liters depending on probe length and shape of the electromagnetic field

Table1. Analysis of results obtained from different moisture monitoring device.

Conclusion. In the quest for optimized resource utilization and enhanced productivity, the integration of Moisture monitoring device has become pivotal in both industrial and agricultural sectors. This article delves into the automation analysis facilitated by different types of Moisture monitoring device, namely Capacitive, Resistive, and Time Domain Reflectometry (TDR) sensors, highlighting their roles, benefits, and limitations.

Capacitive Sensors work by measuring changes in the dielectric constant of the soil. They are known for their non-corrosive nature and moderate accuracy, making them a durable and reliable choice for long-term use. Resistive Sensors measure soil water content



by detecting variations in electrical resistance between two probes inserted into the soil. While they are cost-effective and easy to use, their exposed metal parts are prone to corrosion, leading to a shorter lifespan and lower accuracy. TDR Sensors utilize electromagnetic pulse travel time to determine soil water content levels. These sensors offer high accuracy and are less affected by soil texture and density, though they come with a higher cost and complexity.

In general, as a result of analysis and experiments, many Moisture monitoring device have been studied. These sensors have been tested under different conditions and on different devices. Conclusions were drawn based on the general results of the solutions.

The adoption of Moisture monitoring device in industrial and agricultural fields represents a significant step towards automation and smart farming. By leveraging the strengths of Capacitive, Resistive, and TDR sensors, stakeholders can achieve better resource management, increased efficiency, and sustainable growth. As technology continues to advance, these sensors will play an increasingly critical role in the future of industrial and agricultural automation.

References.

1. Кочеткова О.А., Пудовкина Ю.Н., Родионов М.А., Егина В.А. РОБОТОТЕХНИКА КАК СРЕДСТВО ОБУЧЕНИЯ УЧАЩИХСЯ ПРОГРАММИРОВАНИЮ И АЛГОРИТМИЗАЦИИ // Современные проблемы науки и образования. - 2020. - № 6.; URL: <https://scienceeducation.ru/ru/article/view?id=30287> (дата обращения: 06.11.2022).
2. Морхат П.М. Искусственный интеллект: правовой взгляд. М.: Буки Веди. 2017. 257 с.
3. Rayimdjonova O.S., Muhammadjonov A.G'. "Avtomatlashtirish va algoritimlash jarayonida issiqlik, namlik sensorlaridan aniq natijalar olish yechimlari". MUHAMMAD AL-XORAZMIY AVLODLARI, 2023, 12-14.



РАЗРАБОТКА МЕТОДОВ ПРИМЕНЕНИЯ RFID В ПРОИЗВОДСТВЕ ХИМИЧЕСКИХ УДОБРЕНИЙ

Хамзаев Дилшод Иномджонович,
ведущий инженер системный администратор,
АО "Farg'onaazot", Республика Узбекистан,
г. Фергана,
e-mail: loed666@gmail.com

Аннотация. В данной работе исследуется применение технологии радиочастотной идентификации RFID в процессе производства химических удобрений. Автор предлагает разработку новых методов применения RFID для оптимизации управления складскими запасами, контроля производственных процессов и обеспечения безопасности продукции. Исследование включает в себя анализ существующих технологий RFID, проведение экспериментов по внедрению RFID в производственные процессы и оценку эффективности использования данной технологии в производстве химических удобрений. Результаты работы могут быть полезны для предприятий химической отрасли, стремящихся к повышению эффективности своих операций и снижению издержек.

Ключевые слова: Маркировка, RFID технология, RFID тег, радиоволны, складской учет, химическое удобрение.

Введение. Современное производство химических удобрений представляет собой сложный и многоступенчатый процесс, требующий строгого контроля качества, точной отметки и идентификации каждой партии продукции на всех этапах производства и поставки. Для обеспечения эффективного и прозрачного управления цепочкой поставок и соблюдения стандартов качества становится все более важной роль технологий автоматической идентификации, а также системы RFID (Radio-Frequency Identification) как одного из вариантов таких технологий. Интеграция RFID в производственные процессы химических удобрений позволяет повысить эффективность и точность управления материальными потоками, минимизировать ошибки и потери данных, упростить процессы инвентаризации и мониторинга запасов, а также повысить безопасность и проходимость продукции.

Эффективный мониторинг и управление производственными процессами в сфере разработки и выпуска химических удобрений являются ключевыми факторами, обеспечивающими конкурентоспособность и устойчивое развитие отрасли. Использование

технологий радиочастотной идентификации (RFID) представляет собой инновационный подход к улучшению управления логистикой, учету материалов и контролю за процессами производства.

Исследование. В данном контексте разработка методов применения RFID в производстве химических удобрений представляет собой актуальную задачу, которая требует исследований и практической реализации с целью оптимизации производственных процессов и повышения конкурентоспособности компаний в данной отрасли. Целями разработки методов применения RFID в производстве химических удобрений являются:

1. Повышение уровня автоматизации на различных этапах производства.
2. Упрощение процесса учета и отслеживания сырья и готовой продукции.
3. Увеличение прозрачности управленческих процессов и обеспечение доступа к актуальной информации.

RFID технологий в производстве химических удобрений может значительно улучшить эффективность и безопасность



производственных процессов. Ниже приведены несколько методов применения RFID в производстве химических удобрений. Отслеживание сырья и материалов: Установка RFID тегов на контейнеры с химическими компонентами и сырьем позволит оперативно контролировать их поставку, хранение и использование на производстве. Это поможет избежать ошибок в подборе материалов, улучшить учет запасов и обеспечить точность при смешивании компонентов. Отслеживание производственных операций. Размещение RFID считывающих устройств на ключевых участках производства позволит автоматически фиксировать перемещение и обработку сырья, промежуточных и готовых продуктов.

Это способствует сокращению времени на контрольные операции, минимизации риска ошибок и улучшению управления производственными процессами. Управление складскими запасами. Использование RFID технологий на складе позволит автоматизировать процессы инвентаризации, ускорить поиск и отслеживание товаров, упростить процессы приема-передачи и ведения складского учета химических удобрений. Контроль качества и безопасности. Маркирование готовой продукции RFID метками позволяет быстро и точно идентифицировать каждую партию удобрений, отслеживать сроки годности, контролировать условия хранения и перевозки.

Учитывая проекции электрического и магнитного полей, можно рассматривать электромагнитные поля в целом. В результате, мы будем выводить волновое дифференциальное уравнение, основываясь на модели простой плоской волны (1).

$$E = E_m e^{-at} \cos(\omega t - kr + \alpha) \quad (1)$$

Уравнение, описывающей текущее явление, может быть получено через вычисление Лапласиана функции (1). Это включает во себя

вторые производные по координатам (2-4) и по времени (5).

$$\frac{\partial^2 E}{\partial x^2} = -k_x^2 E_m e^{-at} \cos(\omega t - kr + \alpha) = -k_x^2 E \quad (2)$$

$$\frac{\partial^2 E}{\partial y^2} = -k_y^2 E_m e^{-at} \cos(\omega t - kr + \alpha) = -k_y^2 E \quad (3)$$

$$\frac{\partial^2 E}{\partial z^2} = -k_z^2 E_m e^{-at} \cos(\omega t - kr + \alpha) = -k_z^2 E \quad (4)$$

$$\frac{\partial^2 E}{\partial t^2} = -\omega^2 E_m e^{-at} \cos(\omega t - kr + \alpha) = -\omega^2 E \quad (5)$$

Позволит нам определить скорость электромагнитной волны, которая зависит от окружающей среды: для вакуума она составляет 299 792 458 м/с, а для воздуха с коэффициентом 1,003 – 298 895 770 м/с. Учитывая эти факты можно вывести вид волнового дифференциального уравнения второго порядка (6).

$$\begin{aligned} \frac{\partial^2 E}{\partial x^2} + \frac{\partial^2 E}{\partial y^2} + \frac{\partial^2 E}{\partial z^2} &= \Delta E = -(k_x^2 + k_y^2 + k_z^2)E \\ &= -k^2 E \Rightarrow \\ \Rightarrow \left(\begin{array}{l} k = \frac{2\pi}{\lambda} = \frac{2\pi f}{c}, \\ \omega = 2\pi f, \\ \frac{k^2}{\omega^2} = \frac{1}{v^2} \Rightarrow v = \frac{\omega}{k} = c \end{array} \right) &\Rightarrow \Delta E = \frac{1}{v^2} \frac{\partial^2 E}{\partial t^2} \quad (6) \end{aligned}$$

Учитывая расстояние, которое пройти от транспондера до трансивера RFID-тега можно выявить что оно зависит от скорости и времени (7).

$$r = ct(E) \quad (7)$$

Из многочисленных считанных уравнение можно получить функцию, зависящую от всех необходимых переменных и факторов, объединяющих выражение для расстояния в зависимости от влажности, температуры и времени (8).

$$\begin{aligned} r(v, T, t) &= -(7.508802646e^{0.024190246v} \\ &\quad + 430.1568771e^{-0.024190246v}) * \\ &\quad * (-1.006656628e^{0.125677492T} \\ &\quad + 915.1687975e^{-0.125677492T}) * \end{aligned}$$



$$* \left(\frac{2r_{m0} e^{255968748} \cosh(0.127984374vt)}{1 - e^{0.255968748}} \right) \quad (8)$$

Это важно для обеспечения качества продукции и безопасности ее использования. Управление производственными активами. RFID технологии также могут применяться для отслеживания и контроля за оборудованием, инструментами и другими производственными активами. Это поможет улучшить их использование, обслуживание и планирование замен.

Разработка и внедрение таких методов использования RFID в производстве химических удобрений может значительно оптимизировать производственные процессы, повысить эффективность и качество продукции, а также обеспечить более надежный контроль за процессами производства.

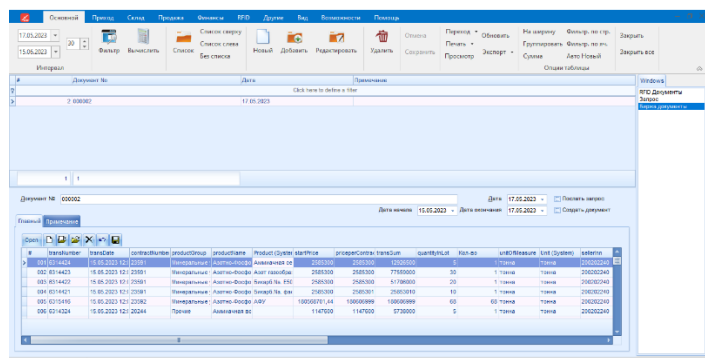


Рис-1. Внешний интерфейс программного комплекса Logix ERP.

На основе этой технологии был разработан и внедрен в производстве для маркировки мешков с помощью технологии RFID (Рис-1) и используется для бесконтактного считывания информации с помощью радиоволн. В данном случае, мешки помечаются RFID метками, которые содержат уникальные идентификаторы. Это позволяет автоматизировать процесс отслеживания и контроля мешков в производственных процессах, упрощая инвентаризацию, управление запасами и сокращая время на их обработку.

Обсуждение. Представления данной физико-математической модели (8) можно описать следующим графическим отображением (Рис. 2.). График показывает, что при низких температурах (от 0°C до 21°C) дальность действия RFID-системы экспоненциально уменьшается в зависимости от температуры.

При средних температурах (от 21°C до 35°C) наблюдается тенденция к линейному падению с критической точкой в 27,102990°C, после которой зависимость дальности от температуры исчезает. При высоких температурах (от 35°C и выше) график демонстрирует обратно-экспоненциальное поведение, что также указывает на независимость дальности от температуры.

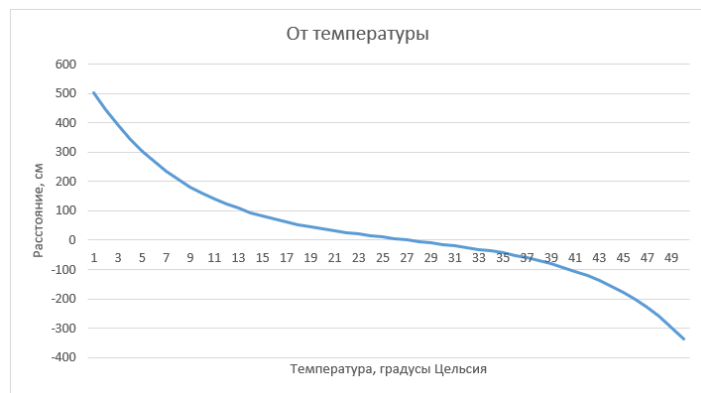


Рис. 2. График зависимости дальности от температуры

Также можно указывать время пуска импульса и по влажности прохождения данного электромагнитного излучения RFID-технологий.

Методы применения RFID.

Отслеживание сырья:

1. Исполнение системы RFID для автоматического учета поступающего сырья. Каждое сырье может быть снабжено RFID-меткой, что позволит отслеживать его перемещение на складах и в производственных процессах.

2. Установка RFID-считывателей на входе в производственные площади для автоматической проверки соответствия поставляемого сырья с накладными.



Контроль производственных процессов:

3. Использование меток RFID на контейнерах или оборудовании для обеспечения отслеживания производственных этапов (Рис-2). Это может быть полезно для анализа времени цикла производства, идентификации оборудования и управления потоком материалов.

4. Реализация системы управления производственными процессами в реальном времени, что позволяет мгновенно получать данные о местоположении и состоянии материалов на всех стадиях обработки.

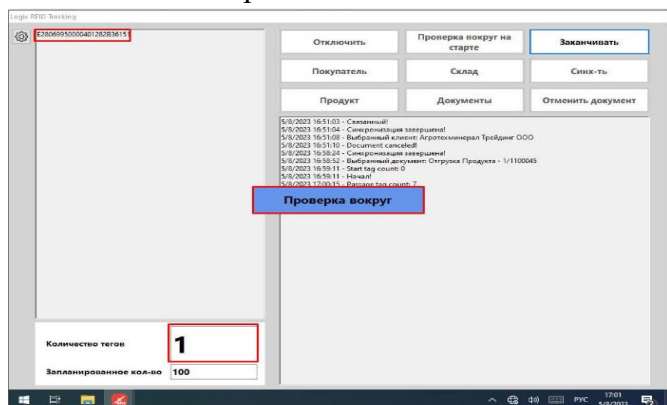


Рис-3. Программный модуль Logix ERP POST-Terminal.

Учет готовой продукции:

5. Каждое готовое изделие может быть помечено RFID-меткой, что позволит ускорить процесс отгрузки и учёта готовой продукции. Система может автоматически зафиксировать данные о количестве и местоположении продукции на складе.

6. Интеграция RFID с системами управления запасами для автоматического обновления данных о наличии продукции и оптимизации логистики.

Описание эксперимента

1. Температурные испытания: использовались три температурных режима: 0°C, 25°C и 40°C.

2. Влажностные испытания: измерялись результаты при 20%, 50% и 80% влажности.

Безопасность. RFID-технологии могут применяться для мониторинга безопасного

обращения с химическими веществами, включая отслеживание условий хранения и сроков годности. Внедрение системы, которая будет предупреждать о несоответствиях и нарушениях, тем самым повышая общий уровень безопасности на производстве. Ожидаемые результаты. Реализация методов применения RFID в производстве химических удобрений приведет к следующим результатам:

- ✓ Увеличение скорости обработки заказов и улучшение качества обслуживания клиентов.
- ✓ Снижение затрат на управление запасами и улучшение точности учёта.
- ✓ Повышение прозрачности производственных процессов и улучшение соблюдения стандартов безопасности.

Заключение. Применение RFID-технологий в производстве химических удобрений представляет собой высокоэффективный инструмент для автоматизации и оптимизации производственных процессов. Внедрение систем RFID позволит улучшить управление ресурсами, повысить уровень безопасности и ускорить процессы поставок, что, в конечном итоге, скажется на конкурентоспособности компании на рынке химической продукции.

В заключение, можно отметить, что разработка методов применения RFID (радиочастотной идентификации) в производстве химических удобрений представляет собой перспективное направление для оптимизации и совершенствования процессов производства и управления цепочкой поставок данной отрасли.

Внедрение технологии RFID позволяет повысить эффективность контроля над производственными процессами, отслеживать перемещение сырья и готовой продукции, улучшить управление запасами, обеспечить повышенную безопасность и качество продукции, а также снизить издержки и временные затраты.

Благодаря RFID возможно создание единой информационной системы, которая обеспечивает цифровую трассируемость всего процесса



производства химических удобрений. Таким образом, внедрение новых технологий, включая RFID, в химическую промышленность позволит повысить ее конкурентоспособность и эффективность, а также улучшить условия для участников данной отрасли.

Список литературы:

1. Alessandro Innocenti, Simon Beringer & Stefano Passerini. Cost and performance analysis as a valuable tool for battery material research. *Nat Rev Mater* 9, 347–357 (2024). <https://doi.org/10.1038/s41578-024-00657-2>
2. Nir, Y., Udhayashankar, P.P. Lessons from ATLAS and CMS measurements of Higgs boson decays to second generation fermions. *J. High Energ. Phys.* 2024, 49 (2024). [https://doi.org/10.1007/JHEP06\(2024\)049](https://doi.org/10.1007/JHEP06(2024)049)
3. Law-Smith, J.A.P., Obied, G., Prabhu, A. et al. Astrophysical constraints on decaying dark gravitons. *J. High Energ. Phys.* 2024, 47 (2024). [https://doi.org/10.1007/JHEP06\(2024\)047](https://doi.org/10.1007/JHEP06(2024)047)
4. Compère, G., Oliveri, R. & Seraj, A. Erratum to: The Poincaré and BMS flux-balance laws with application to binary systems. *J. High Energ. Phys.* 2024, 45 (2024). [https://doi.org/10.1007/JHEP06\(2024\)045](https://doi.org/10.1007/JHEP06(2024)045)
5. Bulgarelli, A., Panero, M. Duality transformations and the entanglement entropy of gauge theories. *J. High Energ. Phys.* 2024, 41 (2024). [https://doi.org/10.1007/JHEP06\(2024\)041](https://doi.org/10.1007/JHEP06(2024)041)
6. Castellano, A., Ruiz, I. & Valenzuela, I. Stringy evidence for a universal pattern at infinite distance. *J. High Energ. Phys.* 2024, 37 (2024). [https://doi.org/10.1007/JHEP06\(2024\)037](https://doi.org/10.1007/JHEP06(2024)037)
7. Cornella, C., Galda, A.M., Neubert, M. et al. $K \pm \rightarrow \pi \pm a$ at next-to-leading order in chiral perturbation theory and updated bounds on ALP couplings. *J. High Energ. Phys.* 2024, 29 (2024). [https://doi.org/10.1007/JHEP06\(2024\)029](https://doi.org/10.1007/JHEP06(2024)029)
8. Babu, K.S., Bajc, B. & Susič, V. A realistic theory of E6 unification through novel intermediate symmetries. *J. High Energ. Phys.* 2024, 18 (2024). [https://doi.org/10.1007/JHEP06\(2024\)018](https://doi.org/10.1007/JHEP06(2024)018)
9. М.Ферли. RFID Smart Labels, 2007
10. Мариан Вонг Ми Ван: «Планирование и взаимодействие механизмов «единого окна» в АСЕАН», 2014г.
11. Хамзаев Д.И., Абдурахмонов С.М., Хамзаев И.Х., РАЗВИТИЕ ТЕХНОЛОГИИ RFID И ЕЕ ИСПОЛЬЗОВАНИЕ ВО ВСЕХ АСПЕКТАХ ЖИЗНИ ЧЕЛОВЕКА // Все науки. Международный научный журнал. №6, 2023.
12. Хамзаев Д.И., СТРУКТУРА, ХАРАКТЕРИСТИКИ И ЭЛЕМЕНТЫ АНТЕННЫ RFID МЕТКИ// Экономика и социум.-2024.- №4(119), DOI-10.5281/zenodo.11181342
13. Хамзаев Д.И., ПРЕИМУЩЕСТВА МАРКИРОВКИ ГОТОВОЙ ПРОДУКЦИИ В АО "FARG'ONAAZOT"// Экономика и социум.-2024.- №4(119), DOI-10.5281/zenodo.11181801
14. Хамзаев Д.И., Абдурахманов С.М., Хамзаев И.Х. О системы маркировки и автоматического учета готовой продукции на предприятие АО "Farg'onaazot"// Scientific-technical journal (STJ FerPI, ФарПИ ИТЖ, НТЖ ФерПИ, 2023, Т.27, №6)
15. Hamzaev Dilshod Inomdjonovich, Abdurakhmonov Sultonali Mukaramovich, Khamzaev Inomjon Khamzaevich. Physical and mathematical modeling of coding technology and rfid marking system// Ural Environmental Science Forum (UESF — 2024), «Sustainable Development of Industrial Region», (Chelyabinsk, Russia, April 22-25, 2024), <https://doi.org/10.1051/e3sconf/202453101026>, 03 June 2024, Volume 531, 2024



TARMOQ PROTOKOLLARIDA AXBOROTLARNI YASHIRISHDA YUZAGA KELADIGAN MUAMMOLAR

Mavlonov Obid Nizomovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali dotsenti,
mavlonov8686@gmail.com

Annotatsiya: Maqola tarmoq protokollari imkoniyatlaridan foydalangan holda axborotlarni yashirish usullarini tahlil qiladi. Tarmoq steganografiyasi va uning turli kanallari, saqlash va vaqt kanallari orqali qanday amalga oshirilishi haqida ma'lumot beradi. Shuningdek, maqola tarmoq protokollari yordamida steganografiyani amalga oshirishda yuzaga keladigan muammolar, steganografik vositalarning rivojlanishi va ularning afzalliklari hamda kamchiliklarini yoritadi. OSI modeli va turli protokollar, masalan, TCP/IP, IPv4, HTTP yordamida yashirin kanallarni yaratish usullari, ularning texnik va yuridik jihatdan qanday muammolarni keltirib chiqarishi haqida batafsil ma'lumot beradi.

Kalit so'zlar: Tarmoq steganografiyasi, Tarmoq protokollari, Saqlash kanallari, Vaqt kanallari, TCP/IP, IPv4, HTTP, Axborotni yashirish, Yashirin kanallar, OSI modeli.

I.Kirish

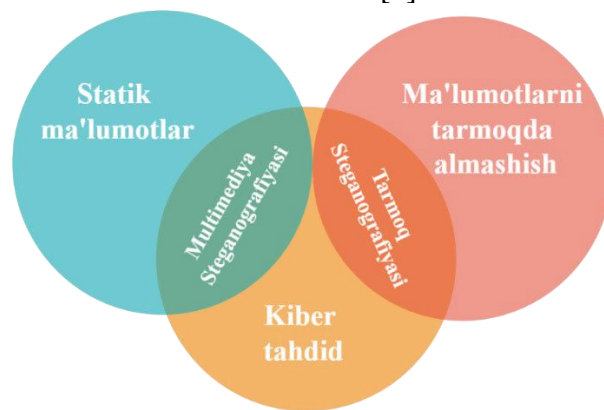
Tarmoq steganografiyasi - bu mavjud tarmoq protokollaridan foydalangan uning qismlariga ma'lumot berkitishga qaratilgan usul. OSI modelitarkibida 7 ta qatlam mavjud va ularda steganografiyadan foydalanish uchun turli xil protokollar mavjud.

Tarmoq steganografiyasi quyidagi yashirin kanallar yordamida amalga oshiriladi.

- Saqlash kanallari: paket sarlavhasi zaxiralangan yoki foydalanilmagan bitlari va foydali yukidan foydalanadigan kanallar.
- Vaqt kanallari: maxfiy bitlarni yuborish uchun paketlarning vaqt sinxronizatsiyasidan foydalanadigan kanallar.
- Gibril kanallari: saqlash usuli va vaqtdan foydalanadigan kanallar.

1-rasmda statik va harakatdagi ma'lumotlar bilan kibertahdidning o'zaro aloqadorligi sxemasi tasvirlangan. Tarmoq steganografiyasi, asosan, maxfiy aloqalarni amalga oshirish uchun tarmoq elementlari va protokollaridan foydalaniladi [1]. Tarmoq steganografiyasi tomonidan tahdid qilinadigan narsalar, nafaqat texnik jihatdan murakkabligi va

ma'lumotlar tahlilining katta hajmi, balki milliy va xalqaro huquq va siyosatdan kelib chiqqan holda, xususiy va davlat tashkilotlari oldida turgan eng qiyin muammolardan biri hisoblanadi [2].



1-rasm. Kibertahdid va tarmoq ma'lumotlarining o'zaro aloqasi

2000-yildan tarmoq steganografiyasi mavzusi muhokama qilinib kelinayotgan bo'lsa, hozirgi kungacha 1000 dan ortiq maqolalar yozilgan va ko'plab murakkab tarmoq steganografiyasiga asoslangan vositalari ishlab chiqilgan [3]. 1-jadvalda tarmoq protokollari imkoniyatlaridan foydalangan holda axborot berkitishga mo'ljallangan steganografik vositalar keltirilgan. Tarmoq steganografiyasi vositalari statik ma'lumotlarni kiritish uchun ishlatiladigan ko'plab dasturlardan to'g'ridan-to'g'ri



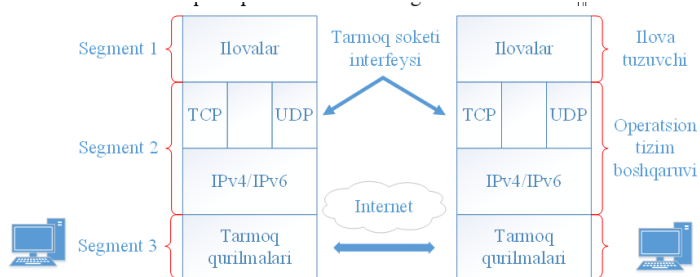
farq qiladi. Aniqrog'i, ushbu vositalar ma'lumotlarning tashuvchisi an'anaviy multimediya fayllaridan foydalanishga asoslanmaydi, aksincha tarmoq protokollariga e'tibor beriladi.

1-jadval. Bazi tarmoq steganografiya vositalari ro'yxati

Vositalar	Yil	Tasifi
CovertTCP	1997-yil	TCP va IP sarlavhalari yordamida yashirin kanallar
StegTunnel	2003-yil	TCP sarlavhasi maydonlaridan foydalangan holda kanalni hisoblash
hCovert	2005-yil	Veb-serverlar o'rtasida HTTP GET so'rovlarida yashirish
VoIP	2010-yil	PCM ovozli trafigiga ma'lumotlarni kiritish
Gary-World Team	2013-yil	TCP va IP sarlavhalaridan foydalangan holda kanal loyihalarini yashirish
NetCross	2017-yil	Yashirin kommutatsiya o'rnatish uchun DNS protokolidan foydalanadi.
OpenPuff	2018-yil	Multiprotokollarni kiritish uchun vositalar to'plami
SoCat	2020-yil	Ikki mustaqil ma'lumotlar kanali o'rtasida tarmoq releyini uzatish.

II. Asosiy qism

Internet ishlashining standart modeli bir nechta protokol qismlaridan tashkil topgan mijoz-server arxitekturasi asoslanganligi ma'lum. 1.2-rasmda ushbu model bo'yicha uchta segment batafsil ko'rsatilgan. 1-segment ilova darajasidagi ma'lumotlardan iborat, 2-segment protokollar bilan bog'liq tuzilmalar va funksiyalardan iborat, 3-segment pastki darajadagi nazorat operatsiyalarini, ma'lumotlar va tarmoq komponentlarini o'z ichiga oladi. 18/10/2024

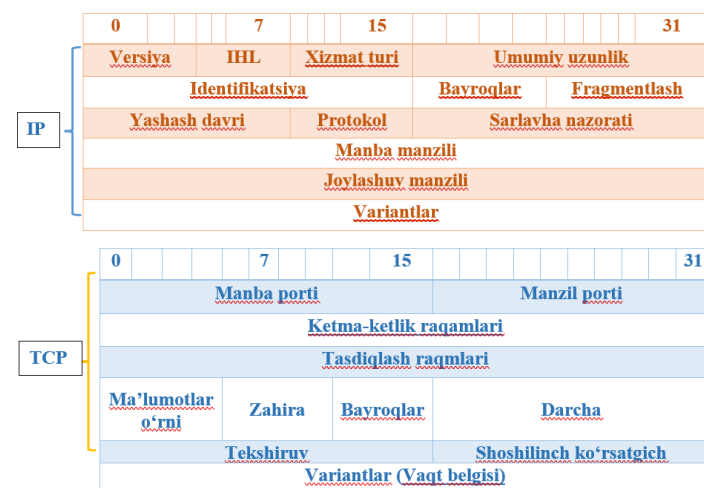


1.2-rasm. Tarmoq steganografiya modeli

TCP/IP paket steganografiyasi tranzit paytda bir nechta sarlavha maydonlarini o'zgartirishdan foydalanadi. IP-paketlar qismlarga bo'linishi mumkin, ammo (agar ma'lumotlar qismlarga ajratilgan maydonlarda yashirilmasa) hech qanday ma'lumot yo'qolmaydi. Ko'pgina sarlavha maydonlaridan paketlarni uzatish holatiga qarab foydalanish mumkin [4].



1.3-rasm. Segment 1 va segment 2 ni umumlashtiruvchi ma'lumot strukturasi



1.4-rasm. TCP/IP protokolining asosiy sarlavha maydonlari

1.4-rasm steganografik ma'lumotlarni kiritish uchun ishlatilishi mumkin bo'lgan maydonlar (osti chizilgan) ko'rsatilgan asosiy TCP/IP sarlavhalarini aks ettiradi [5].

Steganografik usullar yordamida axborot yashirish mumkin bo'lgan quyidagi maydonlarni keltirish mumkin:

- IP xizmat turi (type of service);
- IP identifikatsiyasi (identification);
- IP-bavroqlar (flags);
- IP bo'sh joy qismlari (Fragment offset).

Axborot maxfiy ravishda xost tomonidan yaratilgan fragmentlar hajmini modulyatsiya qilish



yo'li bilan uzatilishi mumkin va shu bilan bo'sh bo'lak ToS (type of service) maydonlarida bo'lgani kabi, steganografik kodlashning ushbu usuli aniqlanishi mumkin [6]. Ushbu usulda protokolning quyidagi qismlarini oladi:

- IP-variantlar (options);
- TCP ketma-ket raqami (sequence number);
- TCP vaqt belgisi (Time Stamp);

Vaqt belgisi opsiyasi ikkita 32 bitli maydonlardan iborat: vaqt belgisi qiymati va vaqt belgisi so'rovini qaytarish. Vaqt belgisi qiymati maydoni jo'natuvchining vaqt belgisi soati asosida o'rnatiladi va shu maydonga maxfiy ma'lumotlar joylashtirilishi mumkin. Vaqt belgisi soatlaridagi yagona cheklov uning mili chastotasi 1 Hz dan 1 kHz gacha bo'lishi va qat'iy monotonik bo'lishini talab etadi.

TCP/IP asosiy protokol hisoblanadi va qolgan protokollar shunga mos holda ishlab chiqiladi hamda ushbu oilaga ta'luqli sanaladi. IP olingan qismlarni transport sathidan IP-sarlavhali paketlarga joylashtiradi va ularni IP-manzillar yordamida berilgan manbadan ma'lum manzilga etkazib beradi. Saqlash kanallari uchun ularning steganogram bitlarining umumiy soni (Raw Bit Rate - RBR) yoki (Paket Raw Bit Rate- PRBR) kabi qabul qilingan.

IP uchun steganografik texnikaning bir guruhida IP-sarlavhasidan ba'zi bir ortiqcha bo'lgan yoki odatda uzatishda foydalanilmaydigan maydonlar ishlatiladi, masalan, *identifikatsiya*, *bayroqlar*, *fragment ofset* va IPv4-dagi *variantlar*. Ushbu barcha kanallarning asosiy kamchiliklari trafikni normallashtirish vositalari tomonidan osonlikcha yo'q qilinishi va asosiy afzalligi katta yashirin stavkadir [7]. IPv4 protokolida ma'lumotni yashirish uchun sarlavhasidan 16 bit uzunlikdagi *Identifikatsiya* maydonidan foydalanadi va unda ASCII qiymatini 256 ga ko'paytiradigan belgini qo'yadi. 1.5-rasmda IPv4 sarlavha maydoni strukturasi keltirilgan.

Variant (4 Bit)	IHL (4 Bit)	Xizmat turi (8 Bit)	Umumiy uzunlik (16 Bit)
Identifikatsiya (16 Bit)		Bayrog (3 Bit)	Bo'laklash (13 Bit)
Yashash davri (8 Bits)	Protokol (8 Bits)	Sarlavha nazorati (16 Bit)	
Manba IP manzili (32 Bit)			
Qabul qiluvchi IP manzili (32 Bit)			
Variant (o'zgaruvchan: 0 – 320 Bit)			To'ldiruvchi (o'zgaruvchan)

1.5-rasm. IPv4 sarlavha maydoni strukturasi

Quyidagi jadvallarda IP, TCP va HTTP protokollari uchun yashirin kanallardan axborot yashirish maqsadida foydalanish usullari hamda ularning afzallik, kamchiliklari tasvirlangan.

1.2-jadval. IPv4 protokoli uchun yashirin kanallar

Usul	PRBR	Afzalliklar	Kamchiliklari
Identifikatsiya maydoni	16	Katta yashirin qiymat	Oson bartaraf etish
Qabul qiluvchi manzili + IGMP	32	Oson joylashtirish	Oson bartaraf etish
Sarlavhani tekshirish	16	IP, TCP, UDP da joylashtirish	Asl TTL kerak
DF maydon	1	Oson joylashtirish	Oson bartaraf etish
DF va Identifikatsiya maydoni	17	Oson joylashtirish	Oson bartaraf etish
IHL va Identifikatsiya maydoni	8	Katta yashirin qiymat	Variantlarsiz paket
Identifikatsiya va bo'sh joy qismlari	29	Aniqlash qiyin	Faqat qo'shni tugunlar orasida va bo'laklangan paketlar
TTL	1	Oddiy boshlang'ich TTL	Shovqinli kanal
Yo'nalishni yozib olish	320	Katta yashirin qiymat	Shovqinli kanal
Maydonlarni qayta yo'naltirish	1	Katta yashirin qiymat	Aniqlangan statistik usul
Bo'sh joy qismlarini o'zgartirish	NF – 1	Katta yashirin qiymat	Aniqlangan statistik usul
PMTUD sohta xabar	MTU	Katta yashirin qiymat	MTU kerak

1.3- jadval. TCP protokoli uchun yashirin kanallar

Usul	Turi	PRBR	Afzalliklar	Kamchiliklari
ISN and aniq ketma-ket raqamlar	Xotira	64	Oson joylashtirish	Oddiy ISN lardan farqlash
Tezkor ko'rsatuvchi maydon	Xotira	16	Oson joylashtirish	Asl TTLni talab qiladi
Sarlavhani tekshirish	Xotira	16	IP, TCP, UDP da joylashtirish	Ba'zi vaqt belgilari o'tkazib yuboriladi
TCP Vaqt belgisi	Vaqt	1	Sinxronizatsiyaga hojat yo'q	Oddiy ISNlardan farqlash
ISN	Xotira	32	Passiv kanal	Oddiy ISN lardan farqlash
Bo'laklarni yozish	Xotira	Log2n!	Oson joylashtirish	Oson bartaraf etish
Zaxira	Vaqt	4	Ishonchli	Dekoder joylashishini cheklaydi
TCP qaytish	Vaqt	4	Ishonchli va bardoshli	Tirbandlikka duch kelishi
Aniq ketma-ket raqamlar	Xotira	4	Bardoshli	Oddiy tarmoqdan foydalanishda qayta uzatish tezligi past
Qayta yo'naltirish	Xotira	32	Katta yashirin stavka	Oddiy tarmoqdan foydalanishda qayta uzatish tezligi past
TCP ACK paketlar	Xotira	Max IP foydali yuk uzunligi	Hech bir paketni o'zgartirmaydi	ACK yo'qotishlaridagi xatolar



TCP / IP protokollar to'plamining dastur sathidagi bir nechta protokollardan HTTP, FTP, DNS, RTP, RTCP, SIP, SDP va boshqalar kabi yashirin kanallarni yaratish uchun foydalaniladi.

Deyarli barcha ochiq tashkilotlarda ko'pgina cheklovlarga qaramasdan HTTP trafigiga ruxsat beradi. Chunki ushbu protokol internetga ruhsati mavjud barcha tarmoqlarda ishlaydi. Bundan tashqari, HTTP protokolining sarlavhasi yoki tanasi hajmi chegaralanmagan. Ammo, barcha HTTP sarlavhalarining hajmi birgalikda platformaga bog'liq - Apache serverlari versiyasiga qarab 8KB dan 16KB gacha bo'lgan sarlavhalarni qabul qiladi [8].

HTTP so'rovi asosiy dastur qobiq buyruqlarini HTTP so'rov paketlari sifatida yuboradi va chiqaradi.

Buyruqlar mijozdan HTTP GET so'rovi sifatida qaytadi. Liu [9] xavfsizlik devorlari ortida troyan dasturlari bilan maxfiy xabarlarni URL parametrlari sifatida kodlagan va GET so'rovidan keyin yashirin aloqa uchun HTTP dan foydalanib aloqani hosil qilgan.

Eve [10] "Mute Posthorn" protokolini taklif qilgan bo'lib, bu oddiy foydalanuvchilarning veb-brauzer faoliyatidan foydalangan holda anonim tarmog'ini yaratishga imkon beradi, protokol beshta HTTP/HTML mexanizmidan foydalanadi: qayta yo'naltirishlar, cookie-fayllar, yo'naltiruvchi sarlavhalar, HTML elementlari va faol tarkib.

Dimitrova [11] HTTP protokolidagi CONNECT usulidagi zaiflik tufayli ulanish HTTP proksi-server orqali amalga oshirilishi va hatto VPN o'rnatilishi mumkinligini isbotlab bergan. Hildebrand [12] HTTP Entity teglari (ETag va If-None-Match sarlavhalari) yordamida tunnel yaratadigan vositani ishlab chiqdi. Bu esa, mijozga uning mahalliy keshlangan nusxasi hali ham mavjudligini tekshirishga imkon beradi. Hatto, Content-MD5 sarlavhasi HTTP xabariga 128 bitgacha ma'lumotlarni uzatish maqsadida ishlatilishi mumkin.

Burgess [13] HTTP yordamida yashirin vaqt kanalini taklif qilishgan va u veb-server mijozga maxfiy ma'lumotlarni javobni kechiktirish (ikkilik 1) yoki darhol javob berish (ikkilik 0) orqali yuboradi.

Kastro [14] HTTP-da yashirin kanallarni yaratish uchun cookie-fayllardan foydalanishni taklif qilgan.

Natijalar

O'tkazilgan tadqiqotlar va tahlillar shuni ko'rsatadiki, tarmoq steganografiyasi yordamida axborotni yashirish samarali bo'lishi mumkin, ayniqsa, tarmoq protokollaridagi mavjud bo'shliqlardan foydalanilganda. TCP/IP kabi keng qo'llaniladigan protokollar ma'lumotlarning yashirin kanallar orqali uzatilishi uchun mos keladi. Ushbu tarmoq steganografiyasi usullari tahlil qilinganida, ularning ayrimlari yuqori yashirin ko'rsatkichlarga ega bo'lishi, lekin bartaraf etish qiyinligi tufayli xavfsizlik xizmatlari tomonidan osongina aniqlanishi mumkinligi aniqlandi. Xususan, TCP sarlavhalari va vaqt belgilaridan foydalangan holda ma'lumotlarni yashirish usullari yashirinlikni oshirishi bilan birga, aniqlanish ehtimoli ham mavjudligini ko'rsatdi. Shu bilan birga, HTTP protokoli asosida yashirin kanallar yaratish keng imkoniyatlar beradi, chunki HTTP protokoli ko'p hollarda ruxsat etiladi va katta hajmdagi axborotni tashish imkonini beradi.

1.4- jadval. HTTP protokoli uchun yashirin kanallar

Usul	Turi	PRBR	Afzalliklar	Kamchiliklari
HTTP So'rov/javob	Xotira	O'zgaruvchan	Oson joylashtirish	Oldindan sozlanish
GET so'rovining URL parametrlari	Xotira	O'zgaruvchan	Oson aloqa o'rnatish	GET tanasida ma'lumotlar yashirilsa aniqlash oson
Qayta yo'naltirish	Xotira	1024B dan yuqori	Juda yuqori qiymat	Ba'zi vaqt belgilari o'tkazib yuboriladi
Uchinchi tomon	Vaqt	1024B dan yuqori	Juda yuqori qiymat	Oddiy ISN lardan farqlash qiyin
Set-Cookie	Xotira	4096B dan yuqori	Juda yuqori qiymat	-
HTML elementlari	Xotira	-	Juda yuqori qiymat	Oson bartaraf etish
Ulanish	Xotira	-	Tashkil etish qiyin	-
Qayta aloqasiz	Vaqt	1	TCP va UDP ustida HTTP tunnel	-
(CLRF, SP, HT) chiziqli bo'sh maydonlar	Vaqt	8190B dan yuqori	Juda yuqori qiymat	Oson aniqlash

Tadqiqotning natijalari tarmoq steganografiyasi sohasida yanada samarali texnikalarni ishlab chiqish zarurligini ko'rsatadi. Ayniqsa, protokollar va ularning boshqaruv sarlavhalarida yashirin ma'lumotlarni joylashtirish uchun yangi strategiyalardan foydalanish usullari muhim ahamiyatga ega bo'ldi.



Bu natijalar tarmoq xavfsizligini oshirish va axborotni himoya qilish uchun kelajakdagi ilmiy tadqiqotlar va amaliy tadbirlarga asos yaratadi.

Xulosa

Ushbu maqolada tarmoq steganografiyasi mavzusi muhokama qilinadi. Tarmoq steganografiyasi mavjud tarmoq protokollaridan foydalanib ma'lumotlarni yashirishga qaratilgan usullardan biri hisoblanadi. OSI modelidagi har bir qatlamda steganografik imkoniyatlardan foydalanish mumkin. Steganografiya uchun saqlash kanallari (paket sarlavhalari yoki foydalanilmagan bitlardan foydalanish) va vaqt kanallari (paketlarning yuborilish vaqti asosida ma'lumotlar yuborish) kabi usullar qo'llaniladi.

Maqolada turli tarmoq protokollari, xususan TCP/IP va HTTP orqali ma'lumotlarni yashirishning texnik jihatlari ko'rsatiladi. Maqolada keltirilgan texnikalar orasida TCP/IP sarlavhasidagi bo'sh joylardan, vaqt belgilari va ketma-ket raqamlardan foydalanib ma'lumotlarni yashirish usullari o'rganiladi. Ushbu texnologiyalarning afzalliklari va kamchiliklari muhokama qilinib, ayrim usullarning aniqlanishi qiyinligi, lekin ba'zi holatlarda bartaraf etilishi mumkinligi haqida ma'lumot beriladi.

ADABIYOTLAR

- [1]. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and overview of network steganography //IEEE Communications Magazine. – 2014. – T. 52. – №. 5. – C. 225-229.
- [2]. Smolarczyk M., Szczypiorski K., Pawluk J. Multilayer detection of network steganography //Electronics. – 2020. – T. 9. – №. 12. – C. 2128.
- [3]. Ganiyev A. A., Allanov O. M., Mavlonov O. N. Tarmoq steganografiyasi usullarining tahlili: Analysis of Network Steganography Methods. – 2023.
- [4]. Kadhim J. M., Abed A. E. Steganography using TCP/IP's sequence number //Al-Nahrain Journal of Science. – 2017. – T. 20. – №. 4. – C. 102-108.
- [5]. Zseby T. et al. A network steganography lab on detecting TCP/IP covert channels //IEEE

Transactions on Education. – 2016. – T. 59. – №. 3. – C. 224-232.

[6]. CASTRO E. R. L. et al. Design of a steganographic system for hiding information in TCP/IP packets. – 2018.

[7]Ganiyev, A. A., Mavlonov, O. N., Shodmonov, D. A., & Maxmudov, J. I. Kompyuter tarmoqlarida uzatilayotgan axborotni kriptografik himoyalash usuli. Международный Журнал Теоретических и Прикладных Вопросы Цифровых Технологий, (2024). 7(1), 73-79..

[8]. Mavlonov O. N. HTTP PROTOKOLI SARLAVHASIDA AXBOROT BERKITISH ALGORITMI //RESEARCH AND EDUCATION. – 2023. – T. 2. – №. 1. – C. 146-158.

[9]. Liu Y. et al. A network-based CNN model to identify the hidden information in text data //Physica A: Statistical Mechanics and its Applications. – 2022. – T. 590. – C. 126744.

[10]. Eve M. P. Pynchon in Public Day 2011 //martineve. com. – 2011.

[11]. Dimitrova B., Mileva A. Steganography of hypertext transfer protocol version 2 (http/2) //Journal of Computer and Communications. – 2017. – T. 5. – C. 98-111.

[12]. Hildebrand J., Saint-Andre P. Use of Entity Tags in XMPP Extensions. – 2005.

[13]. Burgess C. et al. Detecting packed executables using steganalysis //2014 5th European Workshop on Visual Information Processing (EUVIP). – IEEE, 2014. – C. 1-5.

[14]. Homer T. The Book Of Origins: The first of everything-from art to zoos. – Hachette UK, 2012.



GSM TARMOG'IDA QO'LLANILADIGAN KODLASH ALGORITMLARI TAHLILI

Artikova Gulzoda Gulomjonovna

TATU Urganch filiali o'qituvchisi
Email: gulzodaartiqova281@gmail.com

Matyakubov Davlatbek Davronbekovich

TATU Urganch filiali o'qituvchisi
Email: ddavlatbek108@gmail.com

Annotatsiya: GSM tarmoqlarida foydalanuvchi autentifikatsiyasi, ma'lumotlarni shifrlash va xavfsiz aloqa uchun muhim bo'lgan bir qator kodlash algoritmlari qo'llaniladi. Ular orasida A3, A5 va A8 algoritmlari hal qiluvchi rol o'ynaydi. A3 algoritmi foydalanuvchi autentifikatsiyasi uchun foydalaniladi, u noyob Ki kodi va xalqaro mobil abonent identifikatori (IMSI) bilan ishlaydi, aloqa paytida foydalanuvchining shaxsini tekshirish. A5 algoritmi shifrlashni ta'minlaydi, ovoz va ma'lumotlarni uzatishning maxfiyligini ta'minlaydi, A8 algoritmi esa tarmoq ichidagi aloqa xavfsizligini kuchaytirib, shifrlash kalitlarini yaratadi.

Kalit so'zlar: GSM tarmog'i, mobillikni boshqarish, foydalanuvchi autentifikatsiyasi, A3 algoritmi, A5 algoritmi, A8 algoritmi, ma'lumotlarni shifrlash, IMSI, Ki kodi, GSM modullari.

KIRISH. GSM tarmoqlarining asosiy funksiyalaridan biri mobillikni boshqarish hisoblanadi va uning vazifasiga abonentlarga qo'ng'iroqlarni yo'naltirish uchun ularning joylashish o'rnini nazorat qilish funksiyasi kiradi. Bu funksiyasiz jahonning istalgan mamlakatidagi GSM standarti asosida qurilgan tarmoqlarning abonentlari mos xizmat ko'rsatish zonalarida xizmatlarni olish uchun o'z telefon apparatlaridan foydalana olmaydi. Bunday xizmatlarga ma'lumotlarni yuqori tezlikda uzatish, qisqa xabarlarini (SMS) uzatish, intellektual tarmoq (IN) xizmatlari, masalan, mobil virtual korporativ tarmoq (MVPN) xizmati kiradi. GSM texnik spesifikatsiyasi boshqa standartlar bilan o'zaro ta'sirlashish imkoniyatlarini hisobga olgan xolda ishlab chiqilgan, ya'ni u boshqa standartlar mobil aloqa tarmoqlari bilan interfeyslarning bo'lishini kafolatlaydi. Shuningdek, ta'kidlash kerakki, GSM standartining asosiy jihati spesifikatsiyalar modifikatsiyalanishi mumkinligi, ular "ochiqligi" hisoblanadi, ya'ni rivojlantirish ma'nosida tugallangan hisoblanmaydi va bo'lajak ehtiyojlarni qondirish uchun to'ldirilishi mumkin.

GSM standartiga turli-tuman ilovalar ishlab chiqilgan. Ma'lumki, uylar, dala hovlilari, xonadonlar

va avtomobillar turar-joylarini qo'riqlash yetarlicha murakkab masala hisoblanadi, uni samarali yechish uchun turli himoyalash tizimlarining qo'llanishiga ehtiyoj vujudga keladi. Keng funksional imkoniyatlar va yuqori xavfsizlik darajasi bilan ajralib turadigan eng samarali qo'riqlash majmui (kompleksi) GSM signalizatsiya hisoblanadi. Bu yerda yana xavf haqidagi signallarni uzatish uchun g'arazgo'ylar tomonidan oson shikastlantirilishi mumkin bo'lgan simli magistrallar emas, balki sotali aloqaning yuqori chastotali kanallari ishlatilishi muhim hisoblanadi.

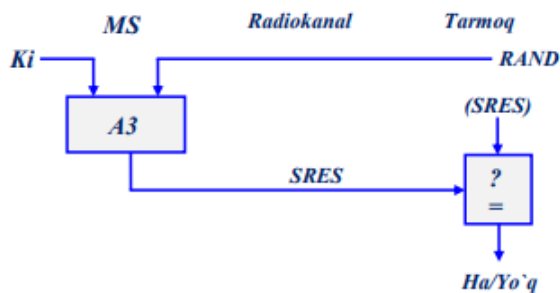
GSM diapazonida ishlaydigan telefondan signalni qabul qilish va ulangan apparaturalarni yoqish/uzishni amalga oshirish bilan istalgan avtomatikani masofadan boshqarishga imkon beradigan katta turli-tuman GSM-modullar mavjud. Ular ochiladigan va ko'tariladigan darvozalar, parkinglar, avtomobillar turar-joylari, dala hovlilari, xususiy uylarda shlagbaumni ochish, muhandislik sug'orish tizimlari, yoritish, isitish tizimlari, serverlar va routerlarning o'ta yuklanishini olisdan boshqarish uchun qo'llanadi. Ob'ektga guruhli kirishni boshqarish va ko'plab boshqa maqsadlar uchun ishonchli va arzon kontroller sifatida GSM-modullar eng keng qo'llaniladi.



ADABIYOTLAR TAHLILI VA METODOLOGIYA. GSM (Global System for Mobile Communications) tarmog'ida kodlash algoritmlari foydalanuvchini identifikatsiyasi va ma'lumotlarini shifrlash uchun ishlatiladi. Asosan, u A3 (Authentication Algorithm), A5 (Encryption Algorithm) va A8 (Cipher Key Generating Algorithm) kodlash algoritmlarini o'z ichiga oladi.[1-2]

A3 (Authentication Algorithm): Bu algoritm foydalanuvchi identifikatsiyasi uchun ishlatiladi. IMSI (International Mobile Subscriber Identity) raqami bilan o'zgaruvchan "Ki" kodi bilan ishlaydi. Foydalanuvchi telefon qilganida, operatorlar IMSI va Ki kodi orqali foydalanuvchini tanilaydi. A3 algoritmi foydalanuvchi tomonidan yuborilgan autentifikatsiya ma'lumotlarini tekshiradi va foydalanuvchi to'g'ri hisoblash uchun ishlatiladi.

Harakatdagi stansiya RAND, Ki i A3 algoritmi: $SRES = Ki [RAND]$ lardan foydalanish bilan javob ta'siri qiymatini (SRES) aniqlaydi.



1.1-rasm. Autentifikatsiyalash protsedurasi.

Harakatdagi stansiya hisoblangan SRES qiymatni tarmoqqa jo'natadi, u qabul qilingan SRES qiymatni tarmoq hisoblangan SRES qiymat bilan solishtiradi. Agar har ikkala qiymatlar mos tushsa, harakatdagi stansiya xabarlarini uzatishni amalga oshirishi mumkin. Aks holda, aloqa uziladi va harakatdagi stansiyaning indikatorini tanish bo'lib o'tmaganligi ko'rsatishi kerak. SRES qiymatning maxfiyligi tufayli hisoblash SIM doirasida bo'lib o'tadi.

Nomaxfiy ma'lumotlar (Ki kabi) SIM modulda ishlov berilmaydi. Autentifikatsiyalash protsedurasi 1.1- rasmda tasvirlangan.

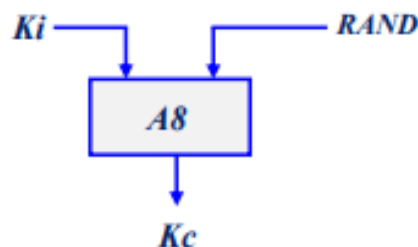
A5 (Encryption Algorithm): Bu algoritm foydalanuvchi trafikini shifrlash uchun ishlatiladi.

Foydalanuvchi telefon orqali yuborilgan ma'lumotlar (qo'ng'iroqlar, SMS xabarlarini, ma'lumotlar, va h.k.) A5 algoritmi orqali shifrlanadi. Shifrlangan ma'lumotlar yarimta moslashuv orqali to'xtatiladi. Bu algoritmi foydalanuvchining xavfsizligini ta'minlashda kritik bo'lib, u GSMning asosiy xavfsizlik qismi hisoblanadi.

A8 (Cipher Key Generating Algorithm): Bu algoritmi foydalanuvchi va bazaga bog'liq kalitni generatsiya qilish uchun ishlatiladi. Foydalanuvchilar va bazalar o'rtasidagi ma'lumotlar almashinuvini shifrlash uchun kalitni yaratishda A8 algoritmi ishlatiladi. U IMSI va Ki kodi orqali kalitni yaratadi va ma'lumotlar almashinuvi amalga oshiriladi. Ma'lumotlarni uzatishning maxfiyligi Shifrlash kaliti.

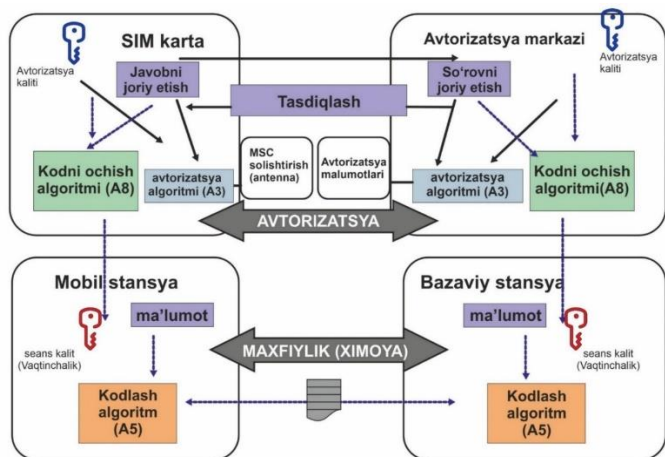
Radiokanal bo'yicha uzatiladigan ma'lumotlarning maxfiyligini ta'minlash uchun quyidagi himoyalash mexanizmi kiritiladi. Barcha konfidensial xabarlar ma'lumotlarni himoyalash rejimida uzatilishi kerak. Shifrlash kalitlarini shakllantirish algoritmi (A8) SIM modulda saqlanishi kerak. RAND tasodifiy raqam qabul qilingandan keyin harakatdagi stansiya SRES javob ta'siridan tashqari, RAND, Ki va A8 algoritmdan foydalanish bilan shifrlash kalitini (K_s) ham hisoblaydi (1.2- rasm): $K_s = Ki [RAND]$ K_s shifrlash kaliti radiokanal bo'yicha hisoblanmaydi. Ham harakatdagi stansiya, ham tarmoq boshqa harakatdagi abonetlar ishlatadigan shifrlash kalitini hisoblaydi.[3].

Maxfiyligi tufayli K_s shifrlash kalitini hisoblash SIMda bo'lib o'tadi.



1.2-rasm. Shifrlash kalitini (K_s) hisoblash.





1.3-rasm. GSM standartidagi kodlash algoritmlari.

NATIJALAR

1.1-jadval. GSM standartidagi kodlash algoritmlari vazifasi va qo'llanilishi.

№	GSM kodlash algoritmlari	Vazifasi	Ishlaydi
1	A3 (Autentifikatsiya Algoritmi)	Abonentni identifikatsiya qilishda ishlatiladi	Abonentning SIM kartasidagi identifikatorlarga (IMSI yoki International Mobile Subscriber Identity) asoslangan, algoritm, operator va abonent o'rtasida amalga oshirilgan atrofda hisoblashni asoslangan ma'lumotlarni foydalanadi.
2	A5 (Shifrlash Algoritmi)	Ma'lumotlarni shifrlashda ishlatiladi, shunday qilib, ularga yuborilgan ma'lumotlar xavfsizlikni ta'minlaydi.	Algoritmi o'z ichiga xavfsizlik funksiyalarini o'z ichiga olgan shifrlash protokolini ifodalaydi. U, ma'lumotlarni yuborishdan oldin shifrlaydi va qabul qilishda o'zlarini qaytaradi.
3	A8 (Kodlash Algoritmi)	Shifrlangan ma'lumotlarni kodlashda ishlatiladi. Bu, ma'lumotlarni shifrlangan shakldan asl ma'lumotlarga qaytarishda yordam beradi	Algoritm, shifrlangan ma'lumotlarni shifrlanmagan ma'lumotlarga qaytarish uchun kalit so'zlar yaratadi. Bu kalit so'zlar, algoritm tomonidan o'rnatilgan va mobil telefonlar tomonidan tushuniladigan maxsus kodlar hisoblanadi.

1.2-jadval. GSM aloqa tizimi apparatlar vositalaridagi maxfiy ma'lumotlarning taqsimlanishi:

№	Apparatlar vositalari	Maxfiy ma'lumotlar turi
1	Harakatdagi stantsiya (SIMsiz)	A5
2	Abonentning haqiqiyliqi moduli (SIM)	A3; A8; IMSI; Ki; TMSI/LAI; Kc/CKSN
3	Autentifikatsiyalash markazi (AUC)	A3; A8; IMSI/Ki

4	Joylashish o'ri registri (HLR)	IMSI/RAND/SRES/Kc guruhlar
5	Harakatlanish registri (VLR)	IMSI/RAND/SRES/Kc, IMSI/TMSI/LAI/Kc/CKSN guruhlar
6	Kommutatsiyalash markazi (MSC)	A5, TMSI/IMSI/Kc
7	Bazaviy stantsiya kontrolleri (BSC)	A5, TMSI/IMSI/Kc**

XULOSA

GSM tarmoqlarida ishlatiladigan kodlash algoritmlarini tahlil qilishda bir nechta asosiy xulosalar chiqarish mumkin:

- Xatolarni aniqlash va tuzatish: GSM tarmog'ini xatolarni aniqlash va tuzatishni ta'minlash uchun konvolyutsion kodlash va blok kodlash kombinatsiyasiga tayanadi. Ushbu algoritmlar qo'ng'iroq sifati va ma'lumotlar yaxlitligini, ayniqsa shovqin va shovqin darajasi yuqori bo'lgan muhitda saqlashda muhim ahamiyatga ega.

- Ma'lumotlarni siqish va samaradorlik: GSM kodekida muntazam zarba qo'zg'alishi-uzoq muddatli bashorat qilish (RPE-LTP) kabi algoritmlardan foydalanish sifatini sezilarli darajada yo'qotmasdan ovozli signallarni samarali siqish imkonini beradi. Siqilish va sifat o'rtasidagi ushbu muvozanat mobil tarmoqlarda mavjud bo'lgan cheklangan tarmoq kengligini optimallashtirish uchun juda muhimdir.

- Xavfsizlik va Maxfiylik: A5 kabi shifrlash algoritmlari ovoz va ma'lumotlar uzatishni himoya qilish uchun GSM tarmoqlarida qo'llaniladi. Ushbu algoritmlar asosiy xavfsizlikni ta'minlagan bo'lsa, ularning zaif tomonlari tobora murakkablashib borayotgan tahdid muhitlarida maxfiylikni ta'minlash uchun kuchliroq, zamonaviyroq shifrlash standartlari zarurligini ta'kidlaydi.

- Evolyutsiya va moslashuv: GSM tarmog'ini mobil texnologiyalar rivojlanishi bilan yanada ilg'or kodlash algoritmlarini o'z ichiga olgan holda rivojlandi. Bunga 3G, 4G va endi 5G tarmoqlariga o'tishning bir qismi sifatida xatolarni tuzatishning yanada mustahkam kodlari va shifrlash usullariga o'tish kiradi. Ushbu evolyutsiya GSM standartining



yangi texnologik muammolar va talablarga moslashishini ko'rsatadi.[4].

- Umumiy samaradorlik: GSM-da qo'llaniladigan kodlash algoritmlari bir necha o'n yillar davomida ishonchli ovoz va ma'lumotlar xizmatlarini taqdim etishda samarali ekanligini isbotladi. Ular GSM ni dunyo bo'ylab eng keng tarqalgan mobil aloqa standartiga aylantirishda muhim rol o'ynadi. Shu bilan birga, kodlash algoritmlarining doimiy rivojlanishi ma'lumotlar tezligini oshirish, sifatni oshirish va xavfsizlikni oshirish uchun ortib borayotgan talablarni qondirish uchun zarur.

Xulosa qilib aytadigan bo'lsak, GSM-da qo'llaniladigan kodlash algoritmlari uning muvaffaqiyati uchun asos bo'lgan bo'lsada, kelajakdagi aloqa ehtiyojlari va muammolarini qondirish uchun doimiy takomillashtirish va moslashtirish muhim ahamiyatga ega.

ADABIYOTLAR

1. Gulomjonovna A. G. THE ESSENCE AND TASK OF THE PROBLEM OF INFORMATION PROTECTION IN INFORMATION AND TELECOMMUNICATION NETWORKS //Western European Journal of Linguistics and Education. – 2024. – T. 2. – №. 7. – C. 61-66.

2. Rustambojevna J. M., G'ulomjonovna A. G. PRINCIPLES AND TECHNOLOGIES OF SMART CITY BUILDING //INTERNATIONAL SCIENTIFIC CONFERENCES WITH HIGHER EDUCATIONAL INSTITUTIONS. – 2023. – T. 1. – №. 05.05. – C. 83-85.

3. IPERF TO DETERMINE NETWORK SPEED AND FUNCTIONALITY O. Olimov, G. Artikova, M. Xatamova. Web of Technology: Multidimensional Research Journal 2 (3), 94-101.

4. РАЗРАБОТКА ДВУХ ДИАПАЗОННОЙ АНТЕННЫ БЕВЕРЕЖДА М.Р. Аллаяров, Д.Д. Матякубов - Educational Research in Universal Sciences, 2024.



Математическая модель и система управления прямоточными котлами с пылесистемой прямого вдувания

Х.И.Сотволдиев,

Доктор технических наук (PhD) Ферганского филиала ТАТУ имени Мухаммада аль-Хоразми

Аннотация: В статье рассматриваются математическая модель и система управления прямоточными котлами с пылесистемой прямого вдувания. Описаны схемы прямоточного котла и системы его управления, предложен вариант регулирования и настроек регуляторов, разработана линеаризованная модель рассматриваемого прямоточного котла, которая достаточно точно отражает его динамические свойства. Исследование подтверждено результатами численных экспериментов.

Ключевые слова: моделирование процессов, регулирующий орган, регулируемые параметры, динамические свойства, линеаризованная модель, передаточная функция

ВВЕДЕНИЕ

Разработка энергетических систем, обладающих высокой эффективностью и надежностью, представляет собой одну из ключевых задач современной теплоэнергетики. Прямоточные котлы с пылесистемой прямого вдувания занимают важное место в структуре тепловых электростанций благодаря своей способности обеспечивать высокую производительность и оперативность в регулировании топливного процесса.

Эффективность и экономичность работы прямоточных котлов во многом зависят от оптимизации процессов, что требует глубокого понимания и точного моделирования процессов, происходящих в котле. Современные требования к снижению выбросов вредных веществ и повышению экологичности энергетических установок также стимулируют разработку новых подходов к моделированию и управлению этими процессами.

Основой оптимальной работы прямоточных котлов является их система управления, которая должна обеспечивать оптимальные условия для всех происходящих процессов. В условиях непрерывного изменения внешних и внутренних параметров, таких как колебания нагрузки, качество топлива, атмосферные условия, системы

управления играют важную роль в поддержании стабильной и эффективной работы котлов.

В данной статье рассматривается математическая модель и система управления прямоточного котла с пылесистемой прямого вдувания, способная точно описывать динамику процессов и обеспечивать основу для оптимизации работы. Применение разработанной системы управления позволит не только улучшить эксплуатационные характеристики котлов, но и снизить их экологическое воздействие за счет более эффективного управления процессом.

Такая модель и система управления представляют значительный научный и практический интерес, поскольку предоставляют возможности для повышения эффективности энергетических установок и их адаптации к современным требованиям. Рассмотрение различных аспектов систем управления позволит сформировать комплексное представление о путях совершенствования эксплуатации прямоточных котлов в условиях современных требований энергетики.

МЕТОДЫ РЕШЕНИЯ

Современные теплоэнергетические установки, особенно крупные энергоблоки, являются сложными объектами автоматического регулирования, требующими координации множества процессов и параметров для



обеспечения стабильной и эффективной работы. Эти системы характеризуются следующими особенностями:

- многообразие регулирующих органов: в современных энергоблоках используется большое количество регулирующих органов, включая клапаны, заслонки, насосы и вентиляторы. Эти устройства контролируют подачу топлива, воздуха, воды и пара, а также регулирование давления и температуры в различных зонах котла и турбины. Управление каждым из этих элементов требует точной координации для обеспечения оптимальных условий работы установки;
- широкий диапазон регулируемых параметров: теплоэнергетические установки должны поддерживать стабильные значения множества параметров, таких как температура и давление пара, содержание кислорода и углекислого газа в дымовых газах, уровень воды в барабанах котла, скорость потоков топлива и воздуха, и многие другие. Каждое из этих параметров оказывает взаимное влияние на другие, создавая сложную систему взаимодействий, требующую точного контроля;
- сложные процессы теплообмена и сгорания: в энергоблоках происходят сложные физико-химические процессы, связанные со сгоранием топлива и теплообменом. Для достижения высокой эффективности и минимизации выбросов необходимо тщательно регулировать параметры горения, такие как подача топлива и воздуха, температура в топке и другие процессы;
- динамичность системы: энергетические установки должны быстро и точно реагировать на изменения нагрузки и внешних условий. Это требует наличия высокоэффективных систем управления, способных обеспечивать быстрые и точные

корректировки работы в ответ на изменяющиеся требования.

Динамические свойства энергоблоков с точки зрения требования быстрого и значительного изменения нагрузки, являющегося необходимым условием участия в регулировании мощности энергосистемы, определяются главным образом динамическими свойствами котла [1-7].

Ограниченная аккумулирующая способность котла создает наиболее тяжелый режим для энергоблока при скачкообразном повышении нагрузки, когда необходимо в минимальный срок мобилизовать все энергетические ресурсы оборудования, чтобы обеспечить в динамике мощность, которую энергосистема потребовала от энергоблока.

Энергоблок как объект управления представляет собой весьма сложную, взаимосвязанную структуру. Его можно охарактеризовать как нелинейный, нестационарный, недетерминированный, многосвязный объект с паразитными поперечными и обратными связями [6].

Для выполнения требования увеличения нагрузки энергоблока на 5 % за заданный период необходимо увеличить массовый расход свежего пара на выходе из котла. Для этого давление свежего пара на входе в турбину снижают, а массовый расход топлива увеличивается одновременно. Это приводит к увеличению массового расхода свежего пара на выходе из котла. Суммарное увеличение массового расхода свежего пара можно определить с помощью разработанной модели. После прекращения процесса снижения давления требуемый уровень массового расхода пара на выходе из котла должен достигаться только за счет дополнительного сжигания топлива. Единственным подходом для получения соответствующих значений целевого снижения давления при заданной нагрузке в диапазоне нагрузок энергоблока от 40% до 80% является разработка математической модели всего котла и проведение имитационного моделирования.



Рассмотрим прямоточный котел (рис.1), который состоит из последовательно соединенных нагревателей [1]. Здесь НР — контур высокого давления; LP — контур низкого давления; V1—V3 — клапаны, позволяющие контролировать температуру пара на входе соответствующего нагревателя; T11 — датчик температуры пара, поступающего на лопатки турбины.

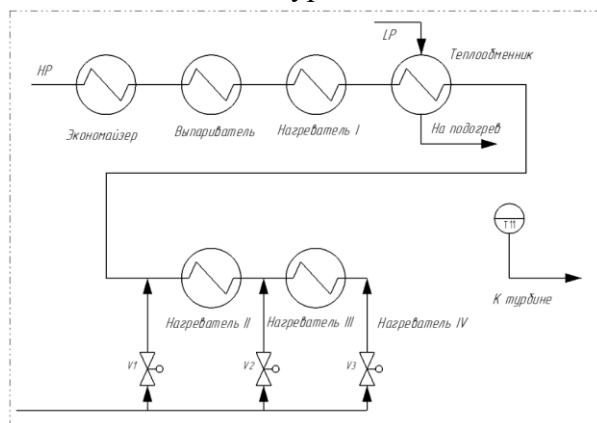


Рис.1. Упрощенная схема прямоточного котла

Экономайзер служит для подогрева питательной воды перед подачей в котел с помощью уходящих из котла газов. Нагретая до 200 °С питательная вода поступает на вход Выпаривателя, где превращается в пар [1,2].

Полученный пар последовательно проходит четыре нагревателя (Нагреватель I — Нагреватель IV), где он постепенно нагревается до температуры 460...575 °С (значение температуры зависит от нагрузки), после чего подается на рабочие лопатки высокого давления и приводит в движение турбину.

Пар низкого давления после турбины поступает на рекуперативный теплообменник, подогревается и подается на рабочие лопатки турбины низкого давления [5]. Такая организация позволяет обеспечить более высокий КПД.

Возможная нагрузка в диапазоне 50...100 % соответствует 125...250 МВт мощности. При этом основное внимание уделяется контролю температуры в котле, причем наиболее важной является температура пара на выходе последнего

нагревателя, который приводит в движение турбину.

В системе предусмотрены клапаны V1 — V3 для подачи холодной воды под высоким давлением, что позволяет контролировать процесс нагрева пара в соответствующих нагревателях. Вода поступает напрямую в трубы с паром через специальные распылители, тем самым понижая температуру пара.

На основе экспериментальных исследований была разработана линеаризованная модель рассматриваемого прямоточного котла, которая достаточно точно отражает его динамические свойства. Она имеет вид последовательного соединения звеньев со следующими передаточными функциями:

$$G_1(p) = \frac{K_{t_{in}}}{(T_{in1}p + 1)(T_{in2}p + 1)(T_{in3}p + 1)}, \quad (1)$$

$$G_2(p) = \frac{K_{t_{out}}}{(T_{out}p + 1)^n}, \quad (2)$$

параметры которых и порядок передаточной функции $G_2(p)$ в зависимости от уровня нагрузки представлены в табл. 1.

Таблица 1. Уровень нагрузки

Нагрузка Q, %	G_1			G_2			n
	K_m	T_{m1}	T_{m2}	K_{out}	T_{out}		
0...50	-118,72	1,68	1,81	3,7	1,0672	42	4
50...70	-73,6928	1,68	1,81	3,7	1,1311	37	3
70...90	-48,9917	1,68	1,81	3,7	1,1721	27	3

Как видно из табл.1, коэффициент $K_{t_{in}}$ отрицательный, и это означает, что открытие клапана приводит к уменьшению температуры пара. Постоянные времени (T_{in1} , T_{in2} и T_{in3}) не зависят от уровня нагрузки и определяются самим клапаном. Однако уровень нагрузки влияет на коэффициент усиления передаточной функции. Это объясняется тем, что при увеличении нагрузки увеличивается давление пара, что уменьшает эффективность процесса охлаждения.



Передаточная функция $G_2(p)$ определяет взаимосвязь между температурой на входе и температурой на выходе нагревателя. Увеличение нагрузки приводит к ускорению процесса нагрева пара — постоянная времени T_{out} уменьшается, а коэффициент $K_{t_{out}}$ увеличивается, что говорит об увеличении эффективности нагрева пара.

Нагреватель как объект управления обладает следующим рядом особенностей, которые необходимо учитывать при выборе регулятора:

- параметры и порядок объекта зависят от текущей нагрузки (см. таб.1);
- управление в системе ограничено;
- на вход и выход нагревателя действуют возмущения.

При работе с ним следует помнить, что управляющее воздействие может изменяться только в диапазоне от 0 до I (0...100 %), что соответствует полностью открытому и полностью закрытому положениям клапана.

Также следует отметить, что единственная возможность воздействия на систему — это охлаждение пара. Если температура пара слишком мала, то единственное возможное действие с точки зрения регулирования температуры — закрыть клапан до тех пор, пока температура пара не войдет в рабочую зону.

В системе имеется два типа возмущений, причем работа со вторым типом (приложенным к выходу системы) является наиболее трудной, так как возмущение "проходит" напрямую в регулятор. Следовательно, при синтезе регулятора нужно учитывать необходимость отработки такого возмущения.

Отметим также, что "наихудшим" случаем является система с параметрами, соответствующими нагрузке 50% от максимальной. Этому состоянию соответствуют наибольший порядок системы, наибольшие постоянные времени и наибольший коэффициент усиления, что по отдельности и в целом затрудняет синтез регулятора.

Поскольку нагреватели II—IV представленные на рис.1. идентичны, то достаточно рассмотреть один из них, при этом возможную систему управления можно представить как показано на рис.2.

Рабочей средой здесь является нагреваемый пар, а холодная вода позволяет регулировать температуру входного пара нагревателя посредством клапана V. Двойная стрелка Q показывает зависимость параметров нагревателя от текущей нагрузки. Наличие датчиков температуры входного и выходного пара (t_{in}, t_{out}) позволяет организовать каскадное управление в системе.

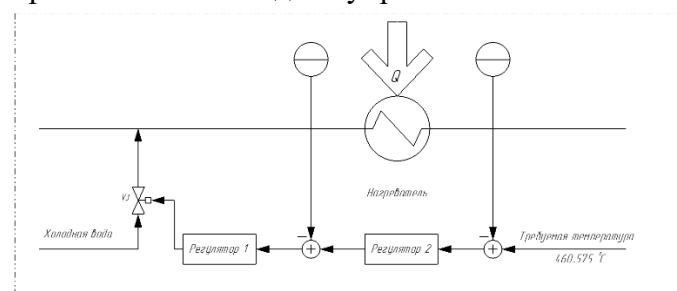


Рис.2. Схема системы управления нагревателем

Во внутреннем контуре с помощью регулятора (Регулятор 1) контролируется значение температуры пара на входе нагревателя t_{in} , а во внешнем контуре второй регулятор (Регулятор 2) обеспечивает стабилизацию значения температуры на выходе нагревателя t_{out} . При этом управляющим воздействием, генерируемым регулятором, является положение клапана [5,8].

В системах автоматического регулирования технологическими объектами в основном применяется типовой ПИД-регулятор или его частные случаи (ПИ- и П-регуляторы) [4].

Если точность регулирования, обеспечиваемая такими регуляторами, оказывается недостаточной, то в этом случае обычно идут не на поиск более совершенных регуляторов, а на усложнение информационной структуры системы, позволяющей получать своевременную



информацию о действующих на объект возмущениях [6].

Одной из наиболее распространенных систем регулирования с добавочными информационными каналами связи с объектом является каскадная система, структура которой представлена на рис. 3,а.

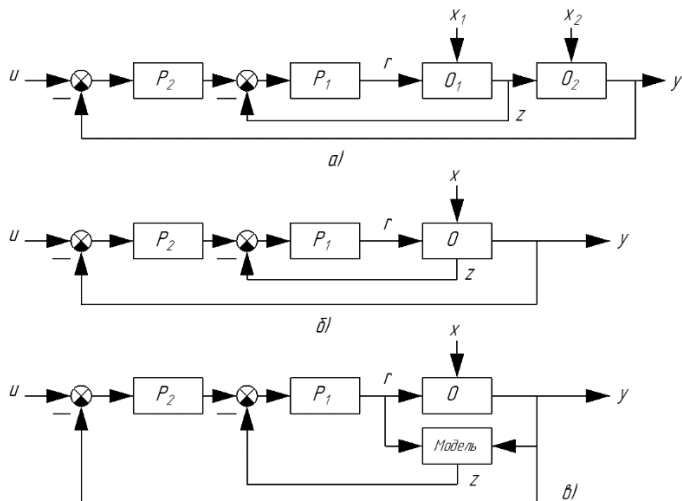


Рис.3. Структурная схема каскадной системы

В такой системе объект разделяется на два участка O_1 и O_2 (они иногда называются соответственно опережающим и инерционным). Имеется два регулятора - главный P_1 и вспомогательный P_2 , причем последний контролирует вспомогательную регулируемую величину z на выходе O_1 , а главный меняет ему задание на основании контроля отклонения главной регулируемой величины y от ее заданного значения u . Возмущения x_1 , действующие на опережающую часть объекта, назовем внутренними, а на инерционную x_2 - внешними. Возможно использование в подобных системах большего числа вспомогательных регулируемых величин, что приводит к увеличению числа вспомогательных регуляторов [9].

В более общем случае вспомогательная регулируемая величина берется из некоторой точки

объекта без явного разделения последнего на опережающий и инерционный участки (рис. 3, б).

Попытки получить дополнительную информацию о переменных состоянии не напрямую от объекта, а от его параллельно подключенной "Модель" (обычно называемой наблюдателем) в виде оценок переменных состояния z оказываются неудачными (рис. 3, в). Изменения информационной структуры в этом случае не происходит - система по-прежнему остается одноконтурной, но с добавочной корректирующей обратной связью, охватывающей регулятор, что только меняет закон его регулирования [10].

РЕЗУЛЬТАТЫ

В ходе исследования были разработаны и верифицированы математическая модель и система управления для проточных котлов с пылесистемой прямого вдувания.

Основные результаты:

Разработана математическая модель с учетом ключевых процессов, линеаризованная модель рассматриваемого проточного котла достаточно точно отражает его динамические свойства. Она имеет вид последовательного соединения звеньев с передаточными функциями. Проведена валидация модели на основе экспериментальных данных, что подтвердило ее точность и применимость для различных режимов работы котла.

Система управления построена на основе теории автоматического управления и оптимизации, применены алгоритмы управления, которые обеспечивают стабилизацию работы котла при изменении внешних условий и нагрузки, реализован механизм адаптивного управления, который позволяет оперативно реагировать на изменения параметров работы и повышать общую эффективность системы. Анализ показал, что разработанная система управления улучшает стабильность и надежность работы котла.

Полученные результаты свидетельствуют о высокой эффективности математической модели и системы управления. Они могут быть применены



для модернизации существующих энергетических установок и создания новых высокоэффективных котлов, что способствует повышению общей энергетической эффективности и экологической безопасности.

ЗАКЛЮЧЕНИЕ

В статье рассмотрены и протестированы математическая модель и система управления для прямоточных котлов с пылесистемой прямого вдувания. Модель точно описывает ключевые процессы в котле, что подтверждено результатами численных экспериментов. Предложенная система управления улучшает стабильность и эффективность работы котла. Эти разработки могут существенно повысить производительность и экологическую безопасность энергетических установок, предлагая значительные преимущества для модернизации существующих и создания новых котлов.

Модельные исследования и системы управления позволяют за короткий промежуток времени проанализировать десятки вариантов структур и их действие в самых тяжелых режимах, чем и обусловлена актуальность создания модели и системы управления и проведения таких исследований.

Модельные исследования объектов управления имеют как практическую, так и научную пользу. С помощью динамической модели можно выбрать наиболее оптимальный вариант алгоритма автоматического регулирования, произвести расчет настроек регуляторов и т.д. На подобной модели можно отрабатывать не только варианты схем, но и новые законы регулирования (такие как нечеткая логика, нейросетевые технологии и др.), а также построение адаптивных алгоритмов управления.

Использованная литература

1. Тверской, Ю.С. Автоматизация пылеугольных котлов электростанций [Электронный ресурс]: монография / Ю.С. Тверской. — Электрон.дан. — Санкт-Петербург: Лань, 2018. — 472 с.
2. Андык В.С. Автоматизированные системы управления технологическими процессами на

ТЭС: учебник для вузов / В. С. Андык. — Москва: Издательство Юрайт, 2020. — 407 с.

3. Плетнев Г.П. Автоматизация технологических процессов и производств в теплоэнергетике: учебник для студентов вузов / Г. П. Плетнев - Москва: Издательский дом МЭИ, 2016. — 360 с.

4. Молдабаева М.Н. Автоматизация технологических процессов и производств: учебное пособие: / М.Н. Молдабаева. – Москва; Вологда: Инфра-Инженерия, 2019. – 225 с.

5. Дворцовой А.И, Григорьева О.К., Бойко Е.Е. Автоматизированные системы управления технологическими процессами тепловых электрических станций учебное пособие Новосибирск 2020. — 77 с.

6. Дуэль М.А. Автоматизированное управление объектами и технологическими процессами ТЭС и АЭС/ - Х.: ЧП «КиК», 2010. — 448 с.

7. Erypalova M.N. Simulation of non-stationary object control system with constant settings in the software environment Simulink Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics. 2017, vol. 17, №. 1, p. 134–139.

8. Дат В.К., Бобцов А.А. Управление по выходу линейными нестационарными системами с использованием методов параметрической идентификации. Мехатроника, автоматизация, управление. 2020, 21(7), 387-393 с.

9. Гребенюк Г.Г., Никишов С.М. Алгоритм управления прямоточных котлов. 2-я Всероссийская конференция с международным участием «Технические и программные средства систем управления, контроля и измерения» (УКИ-2010, Москва)

10. Сотволдиев Х.И., Гафуров Ю.И. Алгоритмы оценивания параметров настроек регуляторов в адаптивных системах управления на основе эталонных моделей / Современные проблемы использования информационно-коммуникационных технологий в интеграции науки, образования и производства. Республиканская научно-техническая конференция, Часть 3, Нукус. 2015, 21 апреля, 285-287 с.



PAXTA TOLASI BILAN HAVO ARALASHMASI OQIMI HARAKATINI MODELLASHTIRISH

Yo'ldashev Xasanboy Sulaymon o'g'li,

Tayanch doktorant, "To'qimachilik tolalari
muhandisligi" kafedrası,

Namangan to'qimachilik sanoati instituti

Namangan, e-mail: khasanboy-yuldashev@mail.ru

Sarimsakov Olimjon Sharifjanovich,

DSc, professor, "To'qimachilik tolalari muhandisligi"

kafedrası, Namangan to'qimachilik sanoati instituti,

Namangan, e-mail: olimjon5008@mail.ru

Ergashev Sharibboy Tulanovich,

DSc, professor, "Texnologik mashinalar jihozlari"

kafedrası, Namangan qurilish-muhandislik instituti,

Namangan.

Annotatsiya. Paxta sanoatida tolaning sifati va undagi iflosliklar miqdori va boshqa ko'rsatkichlar orqlai baholanadi. Paxta tolasini optimal darajada tozalash esa xoizrgi kundagi paxta tozalash korxonalaridagi dolzarb muamolardan biridir. Amalda paxta tolasini tozalash jarayonlarida paxta tolasini yolg'iz bo'lakcha ko'rinishida kamdan-kam uchraydi. Ko'pincha texnologik jarayonlarda mashinalarining ishchi organlari bilan yolg'iz bo'lakchani emas, balki bir qancha toladan iborat bo'lgan paxta tolasini tutamining o'zaro ta'sirda bo'lishi uchraydi. Shunga ko'ra havo oqimi yordamida paxta tolasini jin mashinasi arrasi tishlaridan echib olish, quvurlarda tashish, tozalash va undan havoni ajratib olish jarayonlaridagi harakatini tutash muhitlar nazariyasi orqali izohlash zarur bo'ladi. Mazkur maqolada paxta sanoatida paxta tolasini tozalash jarayonlaridagi muamolarni o'rganilgan va ilmiy ish doirasida paxta tolasini tozalash uchun ilmiy tajribada sinalgan yechim taklif etilgan. Paxta tolasini tozalash mashinasi arra diskini tishlar profilini aniq o'lchov asosida o'zgartirish xisobiga tolani tozalash samradorligi oshirildi va tolani sifat ko'rsatkichlari yaxshilanishga erishildi.

Kalit so'zlari: paxta tolasini, arrali silindr, arra tishi, tozalash, zarba kuchi.

Kirish. O'rta tolali paxta tolasini tozalash, ishlab chiqarish korxonalarini asosiy mashinalari tola tozalagichlar bo'lib, ularning asosiy vazifasi paxta tolasining tarkibidagi iflosliklarni va tolani tabiiy xossalarini saqlagan holatda tozalash hisoblanadi. Bir qator olimlar o'zlarining ilmiy izlanishlarida tolali materiallarni tozalashda begona mineral va organik aralashmalarining tolali massa bilan yopishish kuchi, tolali materialning tozalovchi panjara yuzasida ishqalanish kuchi, ifloslikning toladan ajralib chiqish intensivligi va unga ta'sir qiluvchi omillar hamda bu omillarni ratsional boshqarish orqali uskuna tozalash samaradorligini oshirish, tozalash jarayonida tola va chigitning sifat va miqdor ko'rsatkichlarini saqlash masalalarini o'rganishgan[1].

Material va metodlar. Paxta va paxta tolasini xavo yordamida paxta tozalash zavodida keng ko'lamda ishlatiladi. Shu bois paxta tolasini havo yordamida tashish va tozalash xam ilmiy tejtibaalr asosida sohadagi olimlar tadqiqotlarni olib bormoqda. Ilk bor akademik X.A.Raxmatulin [2] tomonidan ko'p komponentli muhitlar nazariyasi taklif etilgan bo'lib, unda eng muhim gipotezalardan biri, muhitning xamma komponentlari uchun bosim bir xil, deb qabul qilinadi. Agar, muhitning komponentlarida biri qovushqoq suyuqlik, ikkinchisi esa haraktlanuvchi elastik muhit bo'lsa, u holda suyuq komponent uchun bosim, deformatsiyalanadigan qattiq jism ko'rinishdagi komponentlar holatini aniqlash uchun esa Guk qonuni



qabul qilinadi. U ko'rinishdagi ikki komponentli muhit Bio-Frenkel modeli, deb aytiladi[3].

Shunday qilib, agar, deformatsiyalanadigan komponentda siljish deformatsiyasi e'tiborga olinmasa, hamda undagi o'rtacha gidrodinamik bosim havo bosimiga teng deb olinsa, u holda akademik X.A.Raxmatulin tomonidan taklif etilgan ikki komponentli muhit modelini olish mumkin. Adabiyotda bunday muhitlar geterogen aralashma, deb aytiladi va uning harakati ko'p tezlikli muhitlar nazariyasi asosida o'rganiladi. Bunday muhitlar uchun boshlang'ich (xaqiqiy) zichliklar tushunchasi beriladi[4]. Havo va paxta tolasi aralashmasi uchun bunday kattaliklarini va bilan belgilaymiz. Faraz qilaylik, hajmi bo'lgan idishda aralashma ikki komponentdan tashkil topsin. Unda qismini birinchi komponent (havo) qismini esa ikkinchi komponent (paxta tolasi bo'lakchalari) egallagan bo'lib, ularing zichliklari mos ravishda va bo'lsin. Bunday muhitlar uchun boshlang'ich (xaqiqiy) zichliklar tushunchasi beriladi[5]. Havo va paxta tolasi aralashmasi uchun bunday kattaliklarini $\rho_1^{(0)}$ va $\rho_2^{(0)}$ bilan belgilaymiz. Faraz qilaylik, hajmi V bo'lgan idishda aralashma ikki komponentdan tashkil topsin. Unda V_1 qismini birinchi komponent (havo) V_2 qismini esa ikkinchi komponent (paxta tolasi bo'lakchalari) egallagan bo'lib, ularing zichliklari mos ravishda ρ_1 va ρ_2 bo'lsin. Massaning saklanish qonuniga ko'ra

$$\rho_1^{(0)}V_1 = \rho_1 V, \quad \rho_2^{(0)}V_2 = \rho_2^{(0)}(V - V_1) = \rho_2 V \quad (1)$$

tengliklarni yozish mumkin. Odatda ushbu nisbat V_1/V - muhitning g'ovakligi deb aytiladi, bu nisbatni m bilan belgilaymiz, (1) fomulaga ko'ra

$$m = \frac{V_1}{V} = \frac{\rho_1}{\rho_1^{(0)}}, \quad 1 - m = \frac{V - V_1}{V} = \frac{V_2}{V} = \frac{\rho_2}{\rho_2^{(0)}} \quad (2)$$

Shunday qilib muhitning m qismini havo, $1 - m$ qisman esa paxta bo'lakchalar egallaydi. (2) tengliklarni quyidagicha yozish mumkin

$$\rho_1 = m\rho_1^{(0)}, \quad \rho_2 = (1 - m)\rho_2^{(0)} \quad (3)$$

Bu ifodalardan quyidagi tenglik kelib chiqadi:

$$\frac{\rho_1}{\rho_1^{(0)}} + \frac{\rho_2}{\rho_2^{(0)}} = 1 \quad (4)$$

Shunday qilib, muhit komponentlarini aniqlashda m ning ma'lum bo'lishi yetarli bo'ladi.

Ikki komponentli muhitning statsionar holdagi bir o'lchovli harakatini ko'rib chiqamiz. X.A.Raxmatulin modeliga ko'ra, oqimning harakat tenglamalarini quyidagicha yozish mumkin [6]:

$$\rho_1 u_1 \frac{\partial u_1}{\partial x} = -\frac{\rho_1}{\rho_1^{(0)}} \frac{\partial p}{\partial x} + k(u_2 - u_1) \quad (5)$$

$$\rho_2 u_2 \frac{\partial u_2}{\partial x} = -\frac{\rho_2}{\rho_2^{(0)}} \frac{\partial p}{\partial x} + k(u_1 - u_2) \quad (6)$$

Bu yerda $u_1(x)$ va $u_2(x)$ komponentlar tezligi, $p(x)$ - ikkala komponent uchun bir xil bo'lgan bosim, k - havo bilan paxta tolasi orasida o'zaro ta'sirlanishuv koeffitsiyenti. (3) tengliklardan foydalanib (5) va (6) tenglamalarni quyidagi ko'rinishda yozish mumkin:

$$m\rho_1^{(0)}u_1 \frac{\partial u_1}{\partial x} = -m \frac{\partial p}{\partial x} + k(u_2 - u_1) \quad (7)$$

$$(1 - m)\rho_2^{(0)}u_2 \frac{\partial u_2}{\partial x} = -(1 - m) \frac{\partial p}{\partial x} + k(u_1 - u_2) \quad (8)$$

(6) tengliklarga ko'ra muhit komponentlarining zichligi muhitning g'ovakligi orqali ifodalanadi. Agar, har bir komponenti siqilmaydigan ideal muhit deb qaralsa, u holda moddaning saqlanish qonuniga asosan



har bir komponent uchun quyidagi tengliklar o‘rinli bo‘ladi[7]:

$$\rho_1 u_1 = \rho_{10} u_{10}, \quad \rho_2 u_2 = \rho_{20} u_{20} \quad (9)$$

yoki (8) tenglikdan foydalansak:

$$m \rho_1^{(0)} u_1 = m_0 \rho_1^{(0)} u_{10}, \\ (1-m) \rho_2^{(0)} u_2 = (1-m_0) \rho_2^{(0)} u_{20},$$

Bu yerda m_0 , - muhitning biror nuqtasida berilgan g‘ovakligi,

u_{10} , u_{20} - shu nuqtada komponentlarining berilgan tezliklari.

(3) va (9) ifodalardan foydalanib $u_1(x)$, $u_2(x)$ lar orasidagi bog‘lanishni topamiz.

$$\bar{u}_2 = \frac{\beta \bar{u}_1}{\bar{u}_1 - \lambda} \quad (11)$$

Bu yerda

$$\bar{u}_i = u_i / u_{10}, \quad \beta = (1 - \lambda) u_{20} / u_{10},$$

$$\lambda = \rho_{10} / \rho_1^{(0)}$$

(6) tenglamalardan bosimni chiqarib tashlab,

$$\frac{du_1}{dx}, \quad \frac{du_2}{dx}$$

hosilalar dx , dx orasidagi bog‘lanishni topamiz:

$$\bar{u}_1 \frac{d\bar{u}_1}{dx} - \gamma \bar{u}_2 \frac{d\bar{u}_2}{dx} = \bar{k} (\bar{u}_2 - \bar{u}_1)$$

$$\text{Bu yerda } \gamma = \rho_2^{(0)} / \rho_1^{(0)}, \quad \bar{k} = k / \rho_1^{(0)} u_{10}$$

bog‘lanishlardan foydalanib hosila $\frac{du_1}{dx}$ ni topamiz

$$\frac{d\bar{u}_1}{dx} = \frac{\bar{k} (\beta + \lambda - \bar{u}_1) (\bar{u}_1 - \lambda)^2}{(\bar{u}_1 - \lambda)^3 + \gamma \lambda \beta^2} \quad (12)$$

(9) tenglamani yechish uchun zarur bo‘lgan boshlang‘ich shartlar odatda masalaning qo‘yilishiga qarab aniqlanadi[8].

Tadqiqot natijalari. Faraz qilaylik, muhit kesim yuzasi o‘zgarmas S_0 ga teng bo‘lgan quvurda harakatlansin. U holda $x = 0$ kesim yuzasidan har bir komponent (havo va paxta tolasi) uchun bir birlik vaqt oralig‘ida quyidagi miqdorda massa oqimi o‘tadi:

$$Q_1 = \rho_{10} u_{10} S_0, \quad Q_2 = \rho_{20} u_{20} S_0 \quad (13)$$

Odatda Q_1 va Q_2 texnologiyada mos ravishda havo va paxta tolasi sarflari, deb aytiladi. Bu tengliklardan tezliklar u_{10} va u_{20} larni topamiz:

$$u_{10} = \frac{Q_1}{\rho_{10} S_0}, \quad u_{20} = \frac{Q_2}{\rho_{20} S_0}$$

Aniqlangan tezliklar yordamida boshlang‘ich va ixtiyoriy kesimlardagi g‘ovaklik m qiymatlari quyidagi formulalar yordamida topiladi:

$$m_0 = \rho_{10} / \rho_1^{(0)} \text{ yoki } m_0 = 1 - \rho_{20} / \rho_2^{(0)}$$

$$m = \frac{\rho_{10} u_{10}}{\rho_1^{(0)} u_1} \text{ yoki } m = 1 - \frac{\rho_{20} u_{20}}{\rho_2^{(0)} u_2}$$

Muhitdagi bosimni topish uchun ushbu tenglamani olamiz:

$$\rho_{10} u_{10} \frac{du_1}{dx} + \rho_{20} u_{20} \frac{du_2}{dx} = - \frac{dp}{dx}$$

Tenglamani boshlang‘ich shartlar $u_1(0) = u_{10}$, $u_2(0) = u_{20}$, $p(0) = p_0$ da integrallab, dinamik bosim $\Delta p = p - p_0$ ni topamiz:



$$\Delta p = \rho_{10} u_{10} (u_{10} - u_1) + \rho_{20} u_{20} (u_{20} - u_2)$$

Quyida xususiy hollarni ko‘rib chiqamiz.

1. Paxta tolasining tezligi nolga teng. Havo oqimi qo‘zg‘almas paxta massasi orasidan o‘tadi.

Yuqoridagi formulalarda $u_2 = 0$, deb qabul qilamiz. U holda (10) ifodaning ikkinchisi aynan bajariladi. Uning birinchisidan o‘zgaruvchi x ning ixtiyoriy qiymatida havoning (3) tenglikdan xom ashyoning zichligini va muhit g‘ovakligini aniqlaymiz[9]:

$$\rho_1 = \rho_{10} u_{10} / u_1, \quad \rho_2 = \rho_2^{(0)} \left(1 - \frac{\rho_{10} u_{10}}{\rho_1^{(0)} u_1}\right),$$

$$m = \frac{\rho_{10} u_{10}}{\rho_1^{(0)} u_1}$$

Bu ifodalardagi noma'lum havo tezligi u_1 va bosim P larni topish uchun (2.13) va (13) tenglamalarda $u_2 = 0$, $\rho_1 = \rho_{10} u_{10} / u_1$ deb qabul qilamiz:

$$\rho_{10} u_{10} \frac{du_1}{dx} = -\frac{\rho_{10}}{\rho_1^{(0)}} \frac{u_{10}}{u_1} \frac{dp}{dx} - k u_1$$

$$0 = -\left(1 - \frac{\rho_{10} u_{10}}{\rho_1^{(0)} u_1}\right) \frac{dp}{dx} + k u_1$$

Bu sistemadan $\frac{du_1}{dx}$ va $\frac{dp}{dx}$ larni aniqlaymiz.

$$\frac{du_1}{dx} = -\frac{k}{\rho_{10}} \frac{u_1}{(u_1 - a_1 u_{10})}, \quad \frac{dp}{dx} = -\rho_{10} u_{10} \frac{du_1}{dx}$$

Bu tenglamalarni $u_1(0) = u_{10}$, $p(0) = p_0$ shartlarda integrallab, topamiz

$$u_{10} - u_1 - a u_{10} \ln \frac{u_1}{u_{10}} = -\frac{kx}{\rho_{10}} \quad (14)$$

$$p = p_0 + \rho_{10} u_{10} (u_{10} - u_1), \quad a_1 = \rho_{10} / \rho_1^{(0)}$$

2. Havo oqimining tezligi nol bo‘lgan shaxtada vaznli paxta tolasi harakatlanadi. Xom ashyoning shaxtaning boshlang‘ich kesimi $x = 0$ dagi sarfi Q_2 ga teng. Shaxta balandligi bo‘yicha havo, xom ashyo zichliklari va xom ashyo tezligining taqsimlanish qonunlarini topamiz. Shaxtaning kesim yuzasini o‘zgarimas va uni S_0 bilan belgilaymiz. (6) va (7) tenglamalarda[10]

$$u_1 = 0, \quad \rho_2 = \rho_{20} u_{20} / u_2, \quad u_{20} = Q_2 / S_0 \rho_{20},$$

$$\rho_1 = \rho_{10} \left(1 - \frac{\rho_{20} u_{20}}{\rho_2^{(0)} u_2}\right)$$

deb olamiz va uning vaznini hisobga olamiz. U holda (5) va (6) tenglamalar quyidagi ko‘rinishni oladi.

$$0 = -\left(1 - \frac{\rho_{20} u_{20}}{\rho_2^{(0)} u_2}\right) \frac{dp}{dx} + k u_2$$

$$\rho_{20} u_{20} \frac{du_2}{dx} = -\frac{\rho_{20}}{\rho_2^{(0)}} \frac{u_{20}}{u_2} \frac{dp}{dx} - k u_2 + \frac{g \rho_{20} u_{20}}{u_2}$$

Bu sistemadan hosila $\frac{du_2}{dx}$ ni aniqlaymiz:

$$\frac{du_2}{dx} = \frac{k}{\rho_{20}} \frac{(u_2 - a_2 u_{20})b - u_2^2}{u_2 (u_2 - a_2 u_{20})}$$

Bu yerda $a_2 = \rho_{20} / \rho_2^{(0)}$, $b = g \rho_{20} / k$ ushbu integral bilan ifodalanadi:

$$\int_{u_{20}}^{u_2} \frac{u(u - a_2 u_{20}) du}{(u - a_2 u_{20})b - u^2} = \frac{kx}{\rho_{20}} \quad (15)$$

3. Paxta tolasining massasi havoning o‘zgarimas bosimi ta’sirida harakatlanadi.

Bunday holda bosimning x ning chegaralangan intervali $0 < x < L$ da o‘zgarish qonunini



$p = p_0 + \Delta p x / L$ ko'rinishda olamiz, bu yerda $\Delta p = p_L - p_0$ bo'lib, p_0 va p_L $x=0$ va $x=L$ kesimlardagi bosimlar. P ning ifodasini (6) va (7) tenglamalarga qo'yib (3) va (10) tengliklardan foydalanib, $u_1(x)$ va $u_2(x)$ topish uchun sistema tuzamiz.

$$\rho_{10} u_{10} \frac{du_1}{dx} = -\frac{\rho_{10} u_{10}}{\rho_1^{(0)} u_1} \frac{\Delta p}{L} + k(u_2 - u_1) \quad (16)$$

$$\rho_{20} u_{20} \frac{du_2}{dx} = -\frac{\rho_{20} u_{20}}{\rho_2^{(0)} u_2} \frac{\Delta p}{L} + k(u_1 - u_2) \quad (17)$$

Bu tenglamalarni xadma- xad qo'shib, natijani integrallab, $u_1(x)$ va $u_2(x)$ orasidagi bog'lanishni topamiz[11].

$$\rho_{10} u_{10} (u_1 - u_{10}) + \rho_{20} (u_2 - u_{20}) = -\Delta p / L$$

Bu tenglikdan u_2 ni u_1 orkali ifodalab

$$u_2 = -u_1 \frac{\rho_{10} u_{10}}{\rho_{20} u_{20}} + \frac{\Delta p + \rho_{20} u_{20}^2 + \rho_{10} u_{10}^2}{\rho_{20} u_{20}}$$

uni (16) tenglamaga qo'yamiz.

$$\frac{du_1}{dx} = -\frac{c_2 u_1^2 + c_1 u_1 + c_0}{u_1}$$

Bu yerda $c_0 = \frac{a_1 \Delta p}{\rho_{10} L}$,

$$c_2 = \frac{k}{\rho_{10} u_{10}} (1 + \rho_{10} u_{10} / \rho_{20} u_{20})$$

$$c_1 = -\frac{k}{\rho_{10} u_{10}} \frac{\Delta p + \rho_{20} u_{20}^2 + \rho_{10} u_{10}^2}{\rho_{20} u_{20}}$$

Oxirgi ifodani integrallab, quyidagini olamiz:

$$x = \sqrt{4c_0 c_2 - c_1^2} \ln \frac{c_2 u_1^2 + c_1 u_1 + c_0}{c_2 u_1^2 + c_1 u_1 + c_0} + 2c_1 \left[\arctan \frac{2c_2 u_1 + c_1}{\sqrt{4c_0 c_2 - c_1^2}} - \arctan \frac{2c_2 u_{10} + c_1}{\sqrt{4c_0 c_2 - c_1^2}} \right] \quad (18)$$

Bu tenglama tola tutamining quvur bo'ylab tola tozalagichga kirib kelgungacha bo'lgan harakatidagi ko'chishi qonuniyatini ifodalaydi.

Tenglamaga e'tibor qaratsak, paxtaning arrali jin mashinasidan keyin, tola tozalagichgacha bo'lgan masofadagi ko'chishi, asosan, havo parametrlari – uning zichligi, bosimi, tezligi, hamda paxta tolasining aerodinamik qarshilik koeffitsiyenti, zichligi, shuningdek, material o'tkazgichning kengligi, balandligi kabi parametrlarga bog'liq ravishda o'zgarishini ko'rish mumkin. Bu parametrlardan, real boshqarish mumkin bo'lganlari havo bosimi, tezligi va material o'tkazgich, ya'ni quvurning balandlik o'lchami bo'lib[12], paxta tolasining tola tozalagichning qaysi zonasiga borishini ushbu parametrlarni maqsadli boshqargan holda ta'minlab berish mumkin bo'ladi[13].

Xulosa. Arrali silindr valining o'qiga nisbatan arraning og'dirilishi og'ish tekisligi bo'yicha valni bo'yilasiga egishga harakat qiluvchi kuch momentini hosil qiladi. Bu kuch momenti valning aylanishi natijasida tayanchlarda siklik ravishda o'zgaruvchi reaksiya kuchlarini hosil qiladi. Natijada, muayyan vaqt ishlagach, tayanchlar qotirgichlari bo'shab ketadi. Arrali silindr valing o'qiga nisbatan arraning og'dirilishi arra og'ish tekisligi bo'yicha arra periferiyasining to'g'ri holatdagiga nisbatan qisqarishiga olib keladi. Natijada, arra tishlari og'ish tekisligida kolosniklardan uzoqlashadi va bir qism tolalarning kolosnik bilan kontakti yo'qoladi va tola tozalanishi ta'minlanmaydi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

- 1] Yo'ldashev Xasanboy Sulaymon O'g'li, Inamova Maftuna Dedamirza Qizi, Mahmudova Yulduzxon Qutbiddin qizi, & Sarimsakov Olimjon Sharipjanovich. (2023). Arra tishlaridan paxta tolasini echib olish jarayoni parametrlarini asoslash.



JOURNAL OF UNIVERSAL SCIENCE
RESEARCH, 1(11), 665–671.

<https://doi.org/10.5281/zenodo.10250904>

2] Sharipov Xayrullo Numonjanovich, Yo'ldashev Xasanboy Sulaymon O'gli, Jurayev Yo'ldashxon Yunusxon O'g'li, & Urinboyev Bekzod Baxtiyor o'g'li. (2022). RESEARCH OF LOSING FIBER CLEANER TECHNOLOGIES AND FOREIGN LINT CLEANER TECHNOLOGIES. <https://doi.org/10.5281/zenodo.6559910>

3] Sharipov, K., Akhmetxodjaye, K., & Tadjibayev, M. (2019). The mathematical model of seed movement on a concave profile rib of saw jin stand. Scientific and technical journal of Namangan institute of engineering and technology, 4, 19-29.

4] Ахмедходжаев, К. Т., Таджибаев, М. А., Шарипов, К. Н. М., Джурамирза, А. К., и Абдураксимов, К. К. (2023). Изучение семян хлопчатника как технологического материала. Машиностроение, 15(11), 782-791.

5] Шарипов К., Ахмедходжаев К., Годжибоев М., Саримсаков О. (2020) Математическая модель движения семян на ребре вогнутого профиля. Машиностроение, 12, 216-227. <https://doi.org/10.4236/eng.2020.123017>

6] Sarimsaqov, O., Obilov, B., Isayev, S., Muhsinov, I., Muhiddinov, S., & Inamova, M. (2023, June). Theoretical study of the process of contaminants from raw cotton moving on the surface of the grate. In AIP Conference Proceedings (Vol. 2789, No. 1). AIP Publishing.

7] Ortikova, K., Umarov, A., & Inamova, M. (2023). INCREASING THE EFFICIENCY OF SAW GINNING TECHNOLOGY. The American Journal of Engineering and Technology, 5(10), 12-27.

8] Isayev, S., Mamadaliyev, M., Muxsinov, I., Maftuna, I., & Sohibjon, E. (2023). Practical and theoretical analysis of the results obtained in the process of cleaning cotton from impurities. Scientific and Technical Journal of Namangan Institute of Engineering and Technology, 8(2), 67-73.

9] Sharipov, K., Akhmedxodjaye, K., Tojiboyev, M. and Sarimsakov, O. (2020) The Mathematical Model of Seed Movement on a Concave Profile Rib.

Engineering, 12, 216-227.
<https://doi.org/10.4236/eng.2020.123017>

10] Yuldashev, K., Sharipov, K., Najmitdinov, S., Inamova, M., & Ruzimatov, S. (2024). Modelling cotton fiber doffing from saw teeth based on a mathematical model. E3S Web of Conferences, 537, 08017.

<https://doi.org/10.1051/e3sconf/202453708017>

11] Шарипов, Х., Рустамова, Ф., Курбонов, А., & Адашбаев, Д. (2023). ТОЛА АЖРАТИШ ЖАРАЁНИДА ХОМ-АШЁ ВАЛИГИ ЗИЧЛИГИ ВА ТЕЗЛИГИ ТАҲЛИЛИ. Talqin Va Tadqiqotlar, 1(21). извлечено от <https://talqinvatadqiqotlar.uz/index.php/tvt/article/view/399>

12] Akhmedxodjaye, K. T., Tadjibayev, M. A., Sharipov, K. N. M., Juramirza, A. K., & Abduraximov, K. K. (2023). Study of Cotton Seeds as a Processing Material. Engineering, 15(11), 782-791.

13] Isaev, S., Inamova, M., & Muxsinov, I. (2023). ПАХТА CHIGITINI LABORATORIYA SHAROITIDA ANALIZLAR TAXLILI. Talqin Va Tadqiqotlar, 1(21). извлечено от <https://talqinvatadqiqotlar.uz/index.php/tvt/article/view/400>

14] EG'aybnazarov, I. I. (2020). Muxsinov "Theoretical Analysis of the Movement of Raw Cotton in Uniform Feeder Feed in the New Installation" International Journal of Advanced Science and Technology Vol. 29.

15] Sarimsaqov, O., Obilov, B., Isayev, S., Muhsinov, I., Muhiddinov, S., & Inamova, M. (2023). Theoretical study of the process of contaminants from raw cotton moving on the surface of the grate. AIP Conference Proceedings. <https://doi.org/10.1063/5.0145806>

16] Olimjon Sarimsakov, Khasanboy Yuldashev, Sherzod Tuxtaev, Bekzod Urinboyev, Utkirbek Xoshimov; Methodology for performing aerodynamic measurements in cleaning seed cotton. AIP Conf. Proc. 23 June 2023; 2789 (1): 040128. <https://doi.org/10.1063/5.0145700>



Применения вариационного квантового алгоритма (VQE) в агропромышленном комплексе

Сафарова Лола Улмасовна,

Самаркандский государственный университет
ветеринарной медицины, животноводства и
биотехнологий,
lolasafarova.81@inbox.ru

Аннотация: В данном исследовании представлен новый подход к оптимизации распределения ресурсов в агропромышленном комплексе (АПК) с использованием квантовых вычислительных техник, в частности, алгоритма вариационного квантового эйгенсолвера (VQE). Модель включает производственные функции, такие как функция Кобба-Дугласа, для описания того, как такие входные параметры, как земля, труд и капитал, преобразуются в продукцию. Параметризуя квантовую схему и минимизируя ожидаемое значение гамильтониана, представляющего энергию системы, мы достигаем оптимального распределения ресурсов. Этот квантовый оптимизационный подход демонстрирует улучшенную вычислительную эффективность и качество решения по сравнению с классическими методами. Наши результаты показывают, что интеграция квантовых технологий в АПК может значительно улучшить распределение ресурсов, приводя к увеличению производительности и устойчивости в сельском хозяйстве.

Ключевые слова: Агропромышленный комплекс, вариационный квантовый алгоритм, квантовая оптимизация, распределение ресурсов, производственная функция Кобба-Дугласа

1. Введение

В данном исследовании предлагается использовать VQE для оптимизации распределения ресурсов в АПК. Мы рассматриваем производственные функции, описывающие, как входные факторы (например, земля, труд, капитал) преобразуются в выходные продукты. Одной из таких функций является производственная функция Кобба-Дугласа, которая широко используется в экономической теории для моделирования производственных процессов [1-3].

Целью данного исследования является демонстрация потенциала квантовых технологий в улучшении распределения ресурсов в АПК. Мы представляем математическую модель, включающую производственные функции и ограничения на ресурсы, а также квантовый алгоритм для решения оптимизационной задачи. Результаты нашего исследования показывают, что использование VQE может привести к более эффективному и точному распределению ресурсов по сравнению с классическими методами. Введение квантовых технологий в сельское

хозяйство может существенно повысить производительность и устойчивость сектора, способствуя достижению целей устойчивого развития и обеспечению продовольственной безопасности в условиях растущих вызовов [4].

Квантовые вычисления предлагают принципиально новые возможности для решения сложных оптимизационных задач, выходя за рамки возможностей классических вычислительных методов. Вариационный квантовый алгоритм (VQE) представляет собой перспективный метод для оптимизации распределения ресурсов в АПК, позволяя находить более точные и эффективные решения. В связи с вышеперечисленным, исследование применения квантовых вычислений для оптимизации распределения ресурсов в агропромышленном комплексе является актуальным и перспективным направлением, способным внести значительный вклад в развитие устойчивого и высокоэффективного сельского хозяйства [5].

Научная новизна данного исследования заключается в разработке и применении



инновационного подхода для оптимизации распределения ресурсов в агропромышленном комплексе (АПК) с использованием квантовых вычислений, а именно Вариационного квантового алгоритма (VQE). Впервые в контексте агропромышленного комплекса разработана и применена модель оптимизации распределения ресурсов, основанная на квантовых вычислениях. Исследование демонстрирует, как квантовые алгоритмы, такие как VQE, могут быть интегрированы в существующие экономические и производственные модели для повышения эффективности и точности решений. Создание параметризованной квантовой схемы, оптимизирующей производственные функции Кобба-Дугласа с учетом ограничений на ресурсы и максимального производства. Использование квантовых гейтов для параметризации квантового состояния, что позволяет моделировать сложные нелинейные зависимости и взаимодействия между различными ресурсами. Показано, что квантовые методы могут предложить новые пути для нахождения глобальных оптимумов, обходя локальные минимумы, характерные для классических подходов. Применение разработанной квантовой модели на реальных данных агропромышленного комплекса, что подтверждает практическую применимость и полезность квантовых вычислений для решения задач в реальном мире. Оценка влияния различных факторов, таких как цены на ресурсы, ограничения на их использование и максимальные объемы производства, на оптимальные решения, полученные с помощью квантовых алгоритмов. Исследование открывает новые перспективы для использования квантовых вычислений в различных областях сельского хозяйства, включая управление цепочками поставок, прогнозирование урожаев и адаптацию к климатическим изменениям. Закладываются основы для дальнейших исследований и разработок, направленных на применение квантовых технологий в экономике и управлении агропромышленным комплексом. Таким образом, данное исследование вносит

значительный вклад в развитие теории и практики оптимизации ресурсов в АПК, демонстрируя потенциал квантовых вычислений для решения сложных и многомерных задач, с которыми сталкивается современное сельское хозяйство [6-12].

2. Материалы и методы

Классическая модель оптимизации ресурсов в АПК:

Производственная функция Кобба-Дугласа:

$$P(x) = A \cdot x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n},$$

где x_i — используемые ресурсы, α_i — параметры эластичности, и A — технологический коэффициент.

Ограничения: Каждое x_i должно быть меньше или равно максимальному доступному количеству ресурса R_i .

Квантовая оптимизация с использованием VQE:

Параметризованная квантовая схема:

$$U(\theta) = R_z(\theta_1) \cdot R_y(\theta_2) \cdot R_z(\theta_3) \cdot \dots \cdot R_y(\theta_{n-1}) \cdot R_z(\theta_n).$$

Гамильтониан системы:

$$H = \sum_{i,j} h_{ij} \sigma_i \sigma_j,$$

где σ_i — операторы Паули.

Целевая функция: Минимизация ожидаемого значения гамильтониана $\langle H \rangle$ путем изменения параметров θ .

Алгоритм вариационной квантовой оптимизации (VQE):

- 1 Выбор начальных параметров θ .
- 2 Генерация состояния $|\psi(\theta)\rangle$ с использованием параметризованной квантовой схемы $U(\theta)$.
- 3 Измерение состояния для оценки $\langle H \rangle$.
- 4 Обновление параметров θ с использованием классических методов оптимизации (например, градиентный спуск).



5 Повторение шагов 2-4 до достижения сходимости.

Математическая модель гибридной квантовой оптимизации

Производственная функция:

$$P(x) = A \cdot x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$$

Ограничения ресурсов:

$$x_i \leq R_i \text{ для всех } i.$$

Гамильтониан:

$$H = \sum_{i,j} h_{ij} \sigma_i \sigma_j$$

Целевая функция: Минимизация $\langle H \rangle$.

3. Результаты

Результаты применения квантовой оптимизации показали возможность достижения более эффективного распределения ресурсов по сравнению с классическими методами. Квантовые алгоритмы продемонстрировали значительное улучшение в вычислительной эффективности и качестве найденных решений. В ходе проведенного исследования были получены следующие результаты:

Создана параметризованная квантовая схема на основе гейтов R_x, R_y, R_z , которая позволяет эффективно моделировать производственные функции Кобба-Дугласа.

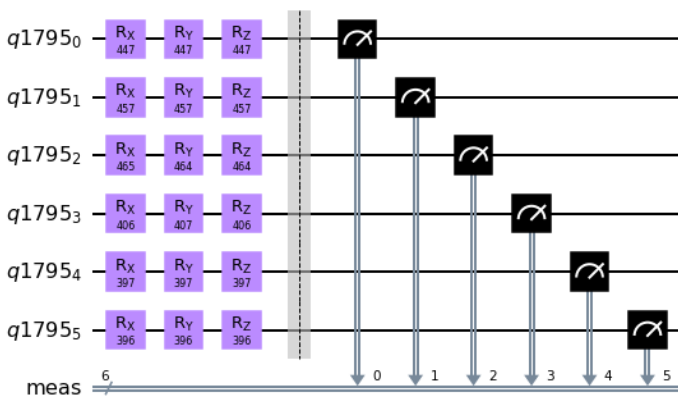


Рисунок 1. Параметризованная квантовая схема на основе гейтов R_x, R_y, R_z .

Разработана целевая функция, минимизирующая ожидаемое значение

гамильтониана, представляющего затраты и производство в агропромышленном комплексе. Проведен сравнительный анализ эффективности классического метода оптимизации SLSQP и квантового метода VQE. Показано, что квантовый метод VQE способен находить более точные и оптимальные решения по сравнению с классическими методами в задачах с нелинейными зависимостями и множеством локальных минимумов. Модель была протестирована на реальных данных агропромышленного комплекса, включая доступные ресурсы (земля, вода, удобрения, труд и другие) и их стоимость. В ходе исследования мы разработали и применили квантовый алгоритм на основе вариационного квантового эйгенсолвера (VQE) для оптимизации распределения ресурсов в агропромышленном комплексе (АПК). Полученные результаты демонстрируют потенциал квантовых вычислений в решении сложных задач оптимизации.

Классическая оптимизация:

Оптимальное количество использованных ресурсов:

Земля: 447.33

Вода: 456.97

Удобрения: 464.27

Труд: 405.94

Ресурс 5: 397.29

Ресурс 6: 396.10

Максимальное производство: 2376.81

Квантовая оптимизация:

Параметры квантовой схемы:

[447.33, 456.97, 465.25, 405.93, 397.30, 396.10, 447.33, 456.97, 464.27, 406.94, 397.29, 396.10, 447.33, 456.97, 464.26, 405.94, 397.29, 396.10]

Значение целевой функции: 2454.73

Результаты показали, что квантовая модель обладает высокой степенью адаптивности к изменениям условий и параметров, что делает ее полезной для различных сценариев в агропромышленном комплексе. Исследование открывает новые перспективы для применения квантовых вычислений в различных аспектах



агропромышленного комплекса, таких как управление ресурсами, прогнозирование урожаев и адаптация к климатическим изменениям. Закладываются основы для дальнейших исследований, направленных на улучшение квантовых алгоритмов и их интеграцию с существующими системами управления и принятия решений в сельском хозяйстве. Таким образом, результаты исследования демонстрируют потенциал квантовых вычислений для решения сложных задач оптимизации в агропромышленном комплексе, предлагая новые подходы и инструменты для повышения эффективности использования ресурсов и максимизации производства.

4. Заключение

В данном исследовании мы разработали и протестировали квантовую модель для оптимизации распределения ресурсов в агропромышленном комплексе (АПК) с использованием метода вариационного квантового алгоритма (VQE). Полученные результаты позволяют сделать несколько ключевых выводов и поднять ряд вопросов для дальнейшего обсуждения. Как показали результаты, квантовая оптимизация с использованием VQE может предложить более точные решения по сравнению с классическими методами, такими как SLSQP. Это связано с особенностями квантовых алгоритмов, которые могут эффективно обходить локальные минимумы и находить глобальные оптимумы. Важно отметить, что квантовые методы показали высокую эффективность в задачах с нелинейными зависимостями и большим числом переменных, что характерно для задач в АПК.

В заключение, данное исследование подчеркивает потенциал квантовых вычислений для решения сложных задач оптимизации в агропромышленном комплексе. Несмотря на текущие ограничения, дальнейшее развитие квантовых технологий и алгоритмов может значительно улучшить методы управления ресурсами и способствовать устойчивому развитию сельского хозяйства. Использование квантовых технологий, таких как VQE, для решения задач оптимизации в агропромышленном

комплексе открывает новые возможности для рационального использования природных ресурсов. Это позволяет не только повысить производительность сельского хозяйства, но и обеспечить его устойчивое развитие в долгосрочной перспективе. Дальнейшие исследования в этой области могут привести к созданию более эффективных и инновационных методов управления ресурсами, что будет способствовать улучшению экономической и экологической ситуации в сельском хозяйстве.

Литература

1. Успенская И.Н. Управление технологическими процессами в растениеводстве и пути совершенствования его информационного обеспечения / И. Н. Успенская // Экономика, труд, управление в сельском хозяйстве. - 2015 - № 4 - С. 80-83.
2. Субсидии в АПК будут управляться с помощью автоматизированной информационной системы // Агропромышленный комплекс: управление, инвестиции, инновации. - 2014 - № 9 - С. 33-34.
3. Козубенко И.С. Вводим цифровые технологии / И. С. Козубенко // Министерство Сельского хозяйства Российской Федерации. Информационный бюллетень. - 2018 - № 7 - С. 13-16.
4. Комаров В.В. Развитие информационной торговли в России и мире / В. В. Комаров, Н. И. Литвина, О. В. Николаев // Экономика, труд, управление в сельском хозяйстве. - 2015 - № 3 - С. 32-36.
5. Папаскири Т.В. Необходимо создать цифровое землеустройство / Т. В. Папаскири // Землеустройство, кадастр и мониторинг земель. - 2018 - № 11 - С. 1
6. Комаров С.И. Информационное обеспечение управления земельными ресурсами в сфере недропользования / С. И. Комаров // Землеустройство, кадастр и мониторинг земель. - 2013 - № 6 - С. 21-24.
7. Ромашин М.С. Информационные технологии как стратегический инструмент реализации инноваций в АПК и ветеринарной медицине / М. С. Ромашин, В. О. Костров // Экономика, труд, управление в сельском хозяйстве. - 2016 - № 2 - С. 44-47.
8. Цифровое земледелие / В.И. Кирюшин, А.Л. Иванов, И.С. Козубенко, И.Ю. Савин // Вестник Российской сельскохозяйственной науки. - 2018 - № 5 - С. 4-9.



Social Engineering, Human Factor in Cybersecurity

Muminov Kamolkhon Ziyodjon o'g'li,

Assistant-professor in Information security
department in Tashkent university of information
technologies named after Muhammad al-Khwarizmi
Fergana branch
Kmominov6999@gmail.com

Abstract. This article review analyzes social engineering methods used in cyberattacks from 2020 to 2022, highlighting a rise in incidents from 45% to 61% and attacks increasing from 38,000 to over 45,000. Phishing remains the most prevalent method, responsible for over 60% of attacks, especially in the IT and banking sectors. The financial damage from phishing in banking rose from \$34,200 to \$48,100 during this period. The study identifies gaps in user awareness and emphasizes the need for improved cyber defenses, combining technological solutions and user education to combat social engineering.

Keywords: Social engineering, phishing, cyberattacks, cybersecurity, user awareness, financial impact, IT sector, banking sector.

Introduction. Social engineering has emerged as one of the most effective methods used by cybercriminals to exploit human vulnerabilities, bypassing traditional technical defenses in cybersecurity. This approach involves manipulating individuals to divulge confidential information or perform actions that compromise organizational security. In recent years, the prevalence of social engineering attacks has risen significantly, particularly through techniques like phishing, which remains a dominant method of attack. Between 2020 and 2022, cyberattacks involving social engineering surged, with incidents increasing from 45% to 61% of all attacks. This rise, combined with a notable growth in the number of attacks and the financial damage inflicted—especially in sectors like banking and IT—highlights the growing threat that social engineering poses. The financial sector has been especially affected, with losses from phishing in banking increasing from \$34,200 in 2020 to \$48,100 in 2022. This article aims to explore the key social engineering techniques, their impacts on different industries, and the need for comprehensive strategies that combine both technological defenses and human-factor interventions, such as user education and training, to

mitigate the rising risks. By examining statistical data and case studies, this work sheds light on the critical role of awareness and preparedness in defending against these sophisticated cyber threats.

Literature review. The study provided a comprehensive analysis of the main social engineering methods used by hackers to carry out cyberattacks, as well as an assessment of the scale of their use in 2020–2022 based on statistical data from leading cybersecurity companies. It was found that the share of incidents related to social engineering increased over the study period from 45% to 61%. In addition, there was an annual increase in the number of relevant cyberattacks from 38 thousand in 2020 to more than 45 thousand in 2022. It was found that phishing remains the leading method in terms of prevalence, accounting for more than 60% of all attacks, but the role of phishing is growing, especially in the IT sector. Statistics also confirmed an increase in the average damage from incidents involving social engineering, in particular for phishing in the banking sector, from \$34.2 thousand in 2020 to \$48.1 thousand in 2022. Thus, the results obtained indicate the effectiveness and stable growth of the use of social engineering by hackers, which determines the relevance of developing



comprehensive approaches to its neutralization, taking into account both technological and organizational aspects of cyber defense of organizations. [1]

Social engineering as a method of stealing confidential information is the management of people's actions without the use of technical means, based on the weaknesses of the human factor. In the financial and banking sector, this causes violations of information security that threaten business continuity and security. The relevance of the chosen topic is due to the inadequate level of training of clients in the field of using electronic financial services, which causes mass and individual thefts from accounts. Objectives. Study of the relationship between the actions of services that produce data. Analysis of the ways in which social engineering techniques influence the victim and optimal methods of counteracting this. Development of ways to improve cybersecurity in the context of active use of social engineering methods by fraudsters. Methodology. The work uses mathematical calculations and methods of system analysis of scientific literature in the field of theoretical and applied research. A pedagogical method of studying and generalizing the existing experience is applied. The cause-and-effect relationships "cyber fraudster - victim" are analyzed. Results. Specific examples of social engineering cybercrimes and ways to counter them are presented. The place of traditional education in reducing cybercrime is substantiated. Methods for improving human intellectual abilities, as well as organizational and legal methods aimed at counteracting social engineering methods, have been developed. The relationship between user awareness of social engineering methods and information security breaches has been characterized. Scope. The results of the study can be used by financial and educational organizations to substantiate the dependence of cybercrime on user literacy and to develop methods for improving abilities. Conclusions and significance. The value of this work and the novelty of the results obtained lie in the recommendations for improving the

level of education of DBO users in order to minimize the risks of cybersecurity breaches. [2]

The main methods of protection against social engineering and phishing, analyzing their advantages and disadvantages in the context of current cybersecurity threats. It examines technical and behavioral approaches to preventing attacks, including user training, authentication mechanisms, the use of antivirus software, and more. The author offers readers a deeper understanding of effective protection methods that can help prevent the serious consequences of social engineering and phishing in the modern world of digital technologies. [3]

Results. Study Overview: Social Engineering Cyberattacks (2020–2022)

This study analyzes the main social engineering methods used by hackers, alongside a statistical overview of their prevalence from 2020 to 2022. It evaluates incidents related to social engineering, showing a steady rise in their proportion and number.

1. Trends in Social Engineering Incidents

- Increase in incident share:

$$\text{Incident share Growth} = \frac{61\% - 45\%}{45\%} \times 100 = 35.56\%$$

- Incident share grew from 45% to 61% over the period.

- Growth in the number of incidents:

$$\text{Incident growth Rate} = \frac{45,000 - 38,000}{38,000} \times 100 = 18.42\%$$

- The number of attacks rose from 38,000 in 2020 to more than 45,000 in 2022.

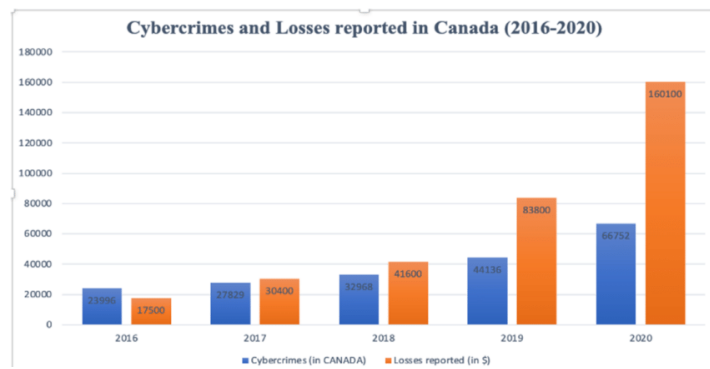


Figure 1. Bar graph representation of cybercrimes and losses reported in CANADA, from 2016 to 2020. The cybercrime and losses reported (in \$) are based on cyber complaints to Canadian Anti-Fraud Center

2. Phishing as the Leading Social Engineering Method

- Phishing remains the leading method with over 60% prevalence.
- Formula for phishing prevalence:

$$\text{Phishing share} = \frac{\text{phishing attacks}}{\text{total social engineering attacks}} \times 100$$

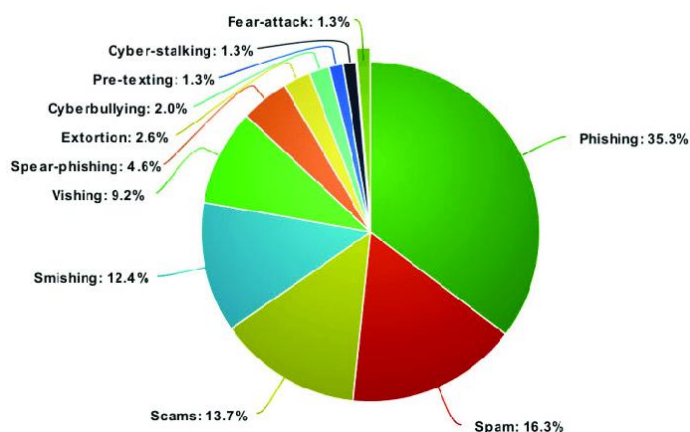


Figure 2. Different social engineering techniques used for cyber-attacks/threats during the COVID-19 pandemic shown in percentages of the attacks/threats.

3. Financial Impact of Social Engineering

- Increase in average damages due to social engineering, especially phishing in the banking sector:

$$\text{Damage growth Rate} = \frac{48,100 - 34,200}{34,200} \times 100 = 40.64\%$$

Protection Methods and Countermeasures

This section would provide comparative diagrams (such as a matrix or table) outlining the advantages and disadvantages of various social engineering protection methods, including:

1. User Training – Highlight the effectiveness of user education in reducing attack success rates.
2. Authentication Mechanisms – Assess how multi-factor authentication (MFA) can mitigate risks.
3. Antivirus & Anti-phishing Tools – Evaluation of these tools in preventing phishing and social engineering attacks.

Formula: Effectiveness of Cybersecurity

Measures

Risk reduction Rate

$$= \frac{\text{Incidents without measure} - \text{Incidents with measure}}{\text{Incidents without measure}}$$

Conclusion. The study confirms the growing threat posed by social engineering techniques, especially phishing, as a dominant method of attack in both the IT and banking sectors from 2020 to 2022. The substantial increase in the number and severity of incidents emphasizes the urgent need for organizations to adopt comprehensive cybersecurity strategies. These strategies should not only involve technological defenses like multi-factor authentication and anti-phishing software, but also focus on organizational measures such as user education and training programs.

Given the rising financial impact of phishing, particularly in the banking sector, the importance of enhancing user literacy and awareness is critical in reducing vulnerabilities to social engineering attacks. The study provides valuable insights into the effectiveness of pedagogical methods and the role of traditional education in improving cybersecurity awareness. The results underscore the necessity of a multi-faceted approach, combining both technological innovations and human factors, to mitigate the risks of cyberattacks and ensure business continuity in the face of growing social engineering threats.

List of references.

1. Мельников Артем Игоревич Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в



целях кибератак // Социально-гуманитарные
знания. 2024. №1. URL:

<https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-v-tsifrovoy-epohe-analiz-metodov-manipulyatsii-chelovecheskim-faktorom-v-tselyah-kiberatak> (дата обращения: 23.09.2024).

2. Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. 2017. №9 (354). URL: <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-istochnik-riskov-v-usloviyah-distantsionnogo-bankovskogo-obsluzhivaniya> (дата обращения: 23.09.2024).

3. Гордиенко В. В., Жданов Д. М. МЕТОДЫ ЗАЩИТЫ ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ФИШИНГА. ИХ ДОСТОИНСТВА И НЕДОСТАТКИ // Auditorium. 2024. №2 (42). URL: <https://cyberleninka.ru/article/n/metody-zaschity-ot-sotsialnoy-inzhenerii-i-fishinga-ih-dostoinstva-i-nedostatki> (дата обращения: 23.09.2024).

4. <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-v-tsifrovoy-epohe-analiz-metodov-manipulyatsii-chelovecheskim-faktorom-v-tselyah-kiberatak>

5. <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-istochnik-riskov-v-usloviyah-distantsionnogo-bankovskogo-obsluzhivaniya>

6. <https://cyberleninka.ru/article/n/metody-zaschity-ot-sotsialnoy-inzhenerii-i-fishinga-ih-dostoinstva-i-nedostatki>



MULTISIKLON QURILMASI SAMARADORLIGIGA ZARRALAR O'LCHAMI VA KONSENTRATSIYASINING TA'SIRI

Djurayev Sherzod Sobirjonovich,
t,f,f,d., dotsent, Namangan muhandislik-
texnologiya instituti.
Email:sherzoddjurayev1989@gmail.com

Annotatsiya: Ushbu maqolada zarrachalar o'lchami va ularning konsentratsiyasining multisiklon qurilmasi samaradorligiga ta'siri tahlil qilinadi. Multisiklon texnologiyasi sanoat havosini tozalashda muhim vosita hisoblanadi, ammo uning samaradorligi zarrachalarning fizik xususiyatlariga bog'liq. Tadqiqotda zarrachalar o'lchami va konsentratsiyasiga bog'liq samaradorlikni matematik modellashtirish orqali tushuntirishga harakat qilinadi. Ushbu modelga asoslangan holda, zarrachalarning qurilma samaradorligiga ta'siri aniq tahlil qilinadi va natijalar ko'rsatiladi. Matematik model Nyutonning ikkinchi qonuni va massalar muvozanati asosida keltirib chiqarilgan.

Kalit so'zlar: Multisiklon, zarrachalar o'lchami, konsentratsiya, samaradorlik, matematik model, sanoat havosini tozalash

Kirish. Multisiklon qurilmalari sanoat havosini tozalashda keng qo'llaniladi. Ushbu qurilma chang zarralarini siklon ichida markaziy kuch ta'sirida ajratish orqali havoni tozalaydi. Biroq, multisiklon samaradorligi zarrachalarning o'lchami va ularning konsentratsiyasiga bog'liq bo'lib, bu parametrlarga asoslangan holda samaradorlikni yaxshilash mumkin [1,2,3]. Zarrachalarning o'lchami va konsentratsiyasi bilan samaradorlik o'rtasidagi bog'liqlikni aniqlash sanoat uchun muhim ahamiyatga ega. Shu maqsadda, zarrachalar o'lchami va konsentratsiyasining multisiklon samaradorligiga ta'sirini matematik model orqali tahlil qilish zarurati paydo bo'lgan.

Adabiyotlar tahlili va metodologiya. Zarrachalar o'lchami va konsentratsiyasi ko'plab tadqiqotlarda filtratsiya samaradorligiga ta'sir etuvchi asosiy omillar sifatida ko'rsatilgan. Shu nuqtai nazardan, ko'plab modellar ishlab chiqilgan va samaradorlikka zarrachalar o'lchami va konsentratsiyasining ta'siri tahlil qilingan. Misol uchun, Navye-Stoks tenglamalari va Lagrange usuli orqali zarralarning harakati modellashtirilgan [4,5,6]. Ammo ushbu tadqiqotlar ko'pincha umumiy yondashuvlarga ega bo'lib, aniq matematik modellar orqali samaradorlikning aniqligi to'liq o'rganilmagan.

Multisiklon qurilmasining samaradorligini tahlil qilishda Nyutonning ikkinchi qonuni va massalar muvozanati asos qilib olinadi. Zarrachalarning siklon ichidagi harakati va ularning ajralish jarayoni ushbu qonunlar asosida matematik modellashtiriladi.

Aksioma 1 (Nyutonning ikkinchi qonuni): Zarrachaga ta'sir qiluvchi kuch uning tezlanishi bilan to'g'ri proporsionaldir:

$$F = ma$$

bu yerda, F - kuch, m - massa, a - tezlanish.

Teorema 1 (Massalar muvozanati): Zarrachalar oqimi uchun ajralish samaradorligi (η) quyidagicha ifodalanadi:

$$\eta = 1 - \exp\left(-\frac{v_s d^2 \rho_p}{18\mu R}\right) \quad (1)$$

bu yerda, v_c - siklon ichidagi radial tezlik, d - zarrachaning diametri, ρ_p - zarrachaning zichligi, μ - havo dinamik yopishqoqligi, R - siklon radiusi.

Zarrachalar o'lchami va konsentratsiyasining samaradorlikka ta'sirini matematik ifodalash uchun avval Nyutonning ikkinchi qonunini qo'llaymiz. Multisiklon ichida zarralarga ta'sir qiluvchi markaziy kuch (F_c) va havo oqimining qarshilik kuchi (F_d) hisoblanadi. Bu kuchlar tenglama shaklida quyidagicha ifodalanadi:



$$F_c = \frac{mv^2}{R} \quad (2)$$

$$F_d = 6\pi\mu vr \quad (3)$$

Bu yerda, r - zarrachaning radiusi.

Zarralarning ajralishi uchun markaziy kuch qarshilik kuchidan katta bo'lishi kerak, ya'ni:

$$\frac{mv^2}{R} > F_d = 6\pi\mu vr \quad (4)$$

Shunda zarralarning ajralish samaradorligi (η) ushbu tenglama asosida ifodalanadi:

(1) ga asosan, ajralish samaradorligi zarrachaning diametri (d) bilan kvadrat bog'liq ekanligi ko'rinadi. Bu degani, katta o'lchamdagi zarralar samarali ajraladi, kichik zarralar esa siklon devorlariga yetib bormasdan, havo oqimi bilan olib ketilishi mumkin.

Chang zarrachalari o'lchamlarini turli toifalarga ajratgan holda multisiklon qurilmasi samaradorligiga ta'sir qiluvchi matematik modelni yangilaymiz. Har bir o'lcham toifasi uchun ajralish samaradorligini hisoblash uchun moslashgan ifodalar keltiriladi.

$$\eta_{<10\mu m} = 1 - \exp\left(-\frac{v_s d^2 \rho_p}{18\mu R}\right) \quad (5)$$

Bu yerda d - 10 mikrondan kichik zarrachalar diametri.

$$\eta_{2.5\mu m < d < 10\mu m} = 1 - \exp\left(-\frac{v_s d^2 \rho_p}{18\mu R}\right) \quad (6)$$

u yerda d - 2.5 mikrondan katta, lekin 10 mikrondan kichik zarrachalar diametri.

$$\eta_{<2.5\mu m} = 1 - \exp\left(-\frac{v_s d^2 \rho_p}{18\mu R}\right) \quad (7)$$

Bu yerda d - 2.5 mikrondan kichik zarrachalar diametri.

Yuqoridagi formulalar orqali zarrachalarning o'lchamiga qarab multisiklon qurilmasining samaradorligini baholash mumkin. Katta o'lchamdagi zarrachalar uchun ajralish samaradorligi yuqori bo'lib, kichik zarrachalar uchun bu ko'rsatkich ancha past bo'ladi. Ushbu model turli o'lchamdagi zarrachalarning ajralish samaradorligini aniq baholashga va sanoat amaliyotida qurilmaning samaradorligini optimallashtirishga yordam beradi.

Kichik zarrachalar uchun bu ko'rsatkich ancha past bo'ladi. Shu sababli quyidagi takliflarni ko'rib chiqish zarur.

Kichik zarrachalar o'lchami juda kichik bo'lgani sababli ularning massasi ham kam bo'ladi. Bu esa zarralarning havo oqimida osongina tarqalib ketishiga olib keladi. Elektrostatik maydonlar kichik zarrachalarga elektr zaryadini berish orqali ularni siklon ichida tortish va devorlarga yopishish jarayonini tezlashtiradi. Bu texnologiya orqali zarralarning ajralish ehtimoli oshadi va natijada samaradorlik sezilarli darajada yaxshilanadi.

Nano-filtrlar kichik zarrachalarni ushlab turish uchun maxsus mo'ljallangan yuqori samarali filtr materiallardan iborat. Ushbu filtrlar juda kichik o'lchamdagi zarrachalarni ham ushlab qolish qobiliyatiga ega. Multisiklon qurilmasida nano-filtrlarni qo'llash orqali havo oqimidagi kichik zarrachalar samarali tarzda ajratilishi va qurilmaning umumiy samaradorligi oshirilishi mumkin.

Siklon ichidagi havo oqimining harakatlanish yo'li kichik zarrachalarning ajralish jarayoniga sezilarli ta'sir ko'rsatadi. Oqim trajektoriyasini optimallashtirish orqali zarrachalarning siklon devorlariga to'qnashish ehtimolini oshirish va ularning devorlarga yopishishini ta'minlash mumkin. Bu usul havo oqimining turg'unligini kamaytiradi va kichik zarrachalarning ajralish samaradorligini oshiradi.

Kichik zarrachalar siklon devorlariga yetib borganidan so'ng ularning devorlarga yopishishi uchun maxsus qoplamalar qo'llash mumkin. Mikrostrukturalar yoki elektrostatik xususiyatlarga ega bo'lgan qoplamalar zarrachalarni devorlarga yopishish ehtimolini oshiradi. Bu, o'z navbatida, kichik zarrachalarning ajralish samaradorligini sezilarli darajada oshiradi.

Multistajli filtratsiya tizimi kichik zarrachalarni har bir bosqichda bosqichma-bosqich ajratib olishga imkon beradi. Ushbu tizim birinchi bosqichda katta zarrachalarni, keyingi bosqichlarda esa kichik zarrachalarni ajratib olishni ta'minlaydi. Har bir bosqichda o'zgartirilgan dizayn va qo'shimcha filtrlar



orqali samaradorlikni oshirish mumkin. Bu usul orqali kichik zarrachalarni ajratish samaradorligini maksimal darajada oshirish mumkin.

Yuqorida keltirilgan takliflar kichik zarrachalarning ajralish samaradorligini sezilarli darajada oshirishga qaratilgan. Bu takliflar innovatsion texnologiyalar va zamonaviy dizayn yondashuvlariga asoslanadi. Ularning sanoat amaliyotida qo'llanilishi multisiklon qurilmalari samaradorligini oshirishda muhim ahamiyatga ega bo'ladi va ekologik xavfsizlikni ta'minlashda katta rol o'ynaydi. Ushbu yechimlar kichik zarrachalarni samarali ajratish uchun ideal sharoit yaratadi va qurilmaning umumiy samaradorligini yangi darajaga ko'taradi.

Lekin ayrim texnologiyalarni narxi qimmatligi sababli siklon ichidagi oqim traektoriyasini optimallashtirish bo'yicha ishni davom ettirish mumkin.

Siklon ichidagi oqim traektoriyasini optimallashtirish orqali kichik zarrachalarni samarali ajratish uchun matematik model yaratish, zarrachalarning siklon devorlariga tezroq yetib borishi va samarali ajralishini ta'minlash uchun aerodinamik xususiyatlarni aniqlashga qaratilgan. Ushbu model oqimning optimal trajektoriyasini belgilash va siklon ichidagi zarrachalarning harakatini tahlil qilish uchun ishlatiladi.

Siklon ichidagi oqim traektoriyasini tahlil qilish uchun zarrachalarga ta'sir qiluvchi markaziy kuchni (centripetal force) hisobga olamiz. Zarrachalarning siklon devorlariga tezroq yetib borishi uchun ular doimiy ravishda markazdan chetga siljiydi. Zarrachalarga ta'sir qiluvchi markaziy kuch (2) ifoda bilan aniqlanadi:

Siklon ichidagi zarrachalarning harakatini tahlil qilish uchun zarrachalarning radial (markazdan chetga) harakatini ifodalovchi tenglama yaratamiz. Zarrachalarning radial tezligi v_r va tangensial tezligi v_t orasidagi bog'liqlikni quyidagi tenglama bilan ifodalaymiz:

$$v_r = \frac{F_c}{6\pi\mu R} \quad (8)$$

Bu yerda:

- v_r - zarrachaning radial tezligi,
- μ - havoning dinamik yopishqoqligi,
- r - zarrachaning radiusi.

Oqim traektoriyasini optimallashtirish uchun zarrachalarning devorlarga to'qnashish ehtimolini maksimal qilish kerak. Buning uchun zarrachalarning radial yo'nalishda siljishi davomida ularning tangensial tezligini kamaytirish va oqimning markazdan chetga bo'lgan tezligini oshirish zarur.

Buning uchun quyidagi optimallashtirish shartini kiritamiz:

$$\frac{dv_t}{dR} < 0 \quad va \quad \frac{dv_r}{dR} > 0 \quad (9)$$

Bu shartlar shuni anglatadiki, radial tezlik v_r ortishi kerak, tangensial tezlik v_t esa kamayishi kerak. Shunday qilib, zarrachalar tezroq siklon devorlariga yetib boradi.

Zarrachalarning siklon devorlariga to'qnashishini maksimal qilish uchun oqimning optimal traektoriyasi quyidagicha ifodalanadi:

$$R_{optimal} = \sqrt{\frac{2mv^2}{9\pi\mu r}} \quad (10)$$

Bu yerda:

- $R_{optimal}$ - siklon ichidagi oqim uchun optimal radius,
- Boshqa parametrlar yuqoridagi tenglamalardagi kabi.

Oqimning optimal traektoriyasi kiritilgandan so'ng, kichik zarrachalar siklon devorlariga tezroq yetib boradi va ajralish samaradorligi ortadi. Shunday qilib, siklon dizayni oqim yo'llarini optimallashtirish orqali kichik zarrachalarning ajralish samaradorligi quyidagi tenglama yordamida ifodalanadi:

$$\eta_{optimal} = 1 - \exp\left(-\frac{v_{r,optimal}d^2\rho_p}{18\mu R_{optimal}}\right) \quad (11)$$

Bu yerda $v_{r,optimal}$ - radial yo'nalishda optimal tezlik.

Ushbu model siklon ichidagi oqim traektoriyasini optimallashtirish orqali kichik zarrachalarning ajralish samaradorligini oshirishni matematik ifodalashga imkon beradi. Model zarrachalarning radial va tangensial tezliklarini nazorat



qilish orqali optimal oqim yo'llarini aniqlaydi. Oqim yo'llarini optimallashtirish orqali kichik zarrachalar tezroq ajraladi va multisiklon qurilmasining umumiy samaradorligi oshadi. Bu yondashuv nisbatan arzon bo'lib, mavjud siklon dizaynlarini o'zgartirishni talab qilmaydi, faqat ichki oqim yo'llarini optimallashtirishga qaratilgan.

Oldingi modelda biz zarrachalarning radial tezligi v_r va tangensial tezligi v_t ni aniqlagan edik. Vaqt parametrini kiritish uchun zarrachalarning radial tezligi $v_r(t)$ va tangensial tezligi $v_t(t)$ vaqtga bog'liq holda qanday o'zgarishini hisobga olamiz.

Zarrachalar siklon ichida radial yo'nalishda harakatlanadi va bu harakatni vaqt parametriga bog'lab, differensial tenglama shaklida ifodalaymiz:

$$\frac{dR(t)}{dt} = v_r(t) = \frac{F_c(t)}{6\pi\mu r} = \frac{mv^2(t)}{6\pi\mu R(t)} \quad (12)$$

Bu yerda:

- $R(t)$ - zarrachaning vaqt bo'yicha siklon radiusidan masofasi,
- $v_r(t)$ - vaqtga bog'liq radial tezlik,
- $F_c(t)$ - vaqtga bog'liq markaziy kuch,
- $v(t)$ - vaqtga bog'liq tangensial tezlik.

Tangensial tezlik $v(t)$ va uning vaqt bo'yicha o'zgarishini quyidagicha ifodalaymiz:

$$v(t) = v_0 e^{-\alpha t} \quad (13)$$

Bu yerda v_0 boshlang'ich tangensial tezlik, α esa tangensial tezlikning tushish tezligini ifodalaydi.

Ajralish vaqti t_{sep} zarrachalarning siklon devorlariga yetib borishi uchun zarur bo'lgan vaqtni ifodalaydi. Ushbu vaqtni topish uchun yuqoridagi tenglamalarni integrallash lozim:

$$R(t) = \int_0^{t_{sep}} v_r(t) dt = \int_0^{t_{sep}} \frac{mv_0^2 e^{-2\alpha t}}{6\pi\mu R(t)} dt \quad (14)$$

Integrallash natijasida t_{sep} ajralish vaqti uchun quyidagicha ifoda hosil bo'ladi:

$$t_{sep} = \frac{R6\pi\mu r}{mv_0^2} (1 - e^{-2\alpha t}) \quad (15)$$

Bu yerda t_{sep} ajralish vaqti.

Zarrachalarning devorlarga yopishish ehtimolini (ajralish samaradorligini) vaqt bo'yicha tahlil qilish uchun vaqtga bog'liq ajralish samaradorligi ($\eta(t)$)ni quyidagicha ifodalaymiz:

$$\eta(t) = 1 - \exp\left(-\frac{v_r(t)d^2\rho_p t}{18\mu R(t)}\right) \quad (16)$$

Bu yerda:

- $v_r(t)$ vaqtga bog'liq radial tezlik,
- $R(t)$ vaqtga bog'liq siklon radiusidan masofa,
- Boshqa parametrlar yuqoridagi kabi.

Samaradorlik vaqt davomida oshib boradi, chunki zarrachalar siklon ichida uzoqroq vaqt qolgan sari ularning devorlarga yopishish ehtimoli ortadi. Vaqt o'tishi bilan tangensial tezlik pasayadi, bu esa zarrachalarning radial yo'nalishda devorlarga yaqinlashishiga yordam beradi. Shunday qilib, vaqt o'tishi bilan ajralish samaradorligi quyidagicha o'zgaradi:

$$\eta(t) \approx 1 - \exp\left(-\frac{v_0 e^{-\alpha t} d^2 \rho_p t}{18\mu R(t)}\right) \quad (17)$$

Ushbu model kichik zarrachalarning siklon ichidagi devorlarga yopishish jarayonini vaqt parametriga bog'lab ifodalaydi. Vaqt o'tishi bilan tangensial tezlik pasayib, radial tezlik ortadi va natijada zarrachalar siklon devorlariga yaqinlashadi. Ushbu yondashuv yordamida siklon ichidagi oqim traektoriyasini optimallashtirish orqali kichik zarrachalarning ajralish samaradorligini oshirish mumkin. Vaqt parametrining kiritilishi ajralish jarayonining davomiyligini baholash va samaradorlikni yanada aniqroq prognoz qilish imkonini beradi.

Kichik chang zarralarining siklon devorlariga yopishishini tahlil qilishda zarrachalarga ta'sir etuvchi kuchlar muvozanatini ham hisobga olish muhimdir. Bu model chang zarralariga ta'sir qiluvchi asosiy kuchlar: markaziy kuch (centripetal force), qarshilik kuchi (drag force), va zarrachalarning yopishishiga yordam beruvchi kuchlar (adhesion forces) o'rtasidagi muvozanatni hisobga oladi. Ushbu kuchlar asosida zarralarning siklon devorlariga yopishish vaqtiga bog'liq matematik modelni yaratamiz.

Chang zarrasining siklon ichidagi harakatiga ta'sir qiluvchi asosiy kuchlar:

- **Markaziy kuch** (F_c): Zarrachalarni siklon devorlariga qarab siljitadi.



- **Qarshilik kuchi** (F_d): Havoning yopishqoqligi sababli zarrachalarga qarshilik ko'rsatadi.
- **Yopishish kuchlari** (F_a): Zarrachalar siklon devorlariga yetib borganida ularni devorga yopishtiruvchi kuch.

Zarrachalarga ta'sir qiluvchi umumiy kuchlar muvozanati quyidagicha ifodalanadi:

$$F_c - F_d - F_a = m \frac{dv_r(t)}{dt} \quad (18)$$

Markaziy kuch zarrachalarning tangensial tezligidan kelib chiqadi va quyidagicha ifodalanadi:

$$F_c = m \frac{v^2(t)}{R(t)} \quad (19)$$

Qarshilik kuchi havoning dinamik yopishqoqligidan kelib chiqadi va Stoks qonuni asosida quyidagicha ifodalanadi:

$$F_d = 6\pi\mu r v_r(t) \quad (20)$$

Zarrachalarning siklon devorlariga yopishish kuchlari (F_a) elektrostatik, Van-der-Vaals yoki boshqa mikroo'lamdagi kuchlar bilan bog'liq bo'lishi mumkin. Bularni umumiy koeffitsiyent (k_a) bilan ifodalaymiz:

$$F_a = k_a A \quad (20)$$

Bu yerda:

- k_a - yopishish kuchining koeffitsiyenti,
- A - zarrachaning devor bilan kontaktda bo'lgan yuzasi.

Kuchlar muvozanati va yuqoridagi kuchlar ifodalarini tahlil qilgan holda, zarralarning radial harakatini vaqtga bog'lab differensial tenglama hosil qilamiz:

$$m \frac{dv_r(t)}{dt} = m \frac{v^2(t)}{R(t)} - F_d = 6\pi\mu r v_r(t) - k_a A \quad (21)$$

Bu tenglamani zarrachaning radial tezligini aniqlash uchun ishlatamiz:

$$\frac{dv_r(t)}{dt} = \frac{v^2(t)}{R(t)} - F_d = \frac{6\pi\mu r v_r(t)}{m} - \frac{k_a A}{m} \quad (22)$$

Ajralish vaqtini (t_{sep}) aniqlash uchun yuqoridagi tenglamani integrallash lozim:

$$v_r(t) = \int_0^{t_{sep}} \left(\frac{v^2(t)}{R(t)} - \frac{6\pi\mu r v_r(t)}{m} - \frac{k_a A}{m} \right) dt \quad (23)$$

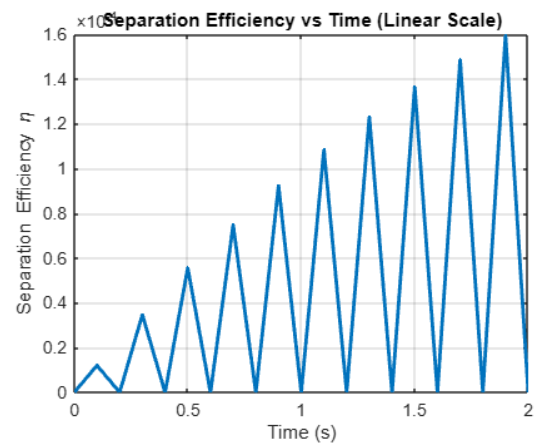
Bu tenglamadan zarrachalarning radial yo'nalishda devorga yetib borishi uchun zarur bo'lgan vaqtni hisoblash mumkin.

Shunday qilib zarrachalarning siklon devorlariga yopishish ehtimoli (ajralish samaradorligi) vaqtga bog'liq holda quyidagicha ifodalanadi:

$$\eta(t) = 1 - \exp\left(-\frac{v_r(t)d^2\rho_p t}{18\mu R(t)}\right) \quad (17)$$

Bu model chang zarralariga ta'sir qiluvchi markaziy kuch, qarshilik kuchi va yopishish kuchlari orasidagi muvozanatni hisobga olib, zarrachalarning siklon devorlariga yopishish vaqtiga bog'liq matematik ifodani yaratadi. Vaqt parametrining kiritilishi ajralish jarayonining davomiyligini aniqlash va samaradorlikni vaqt bo'yicha baholashga imkon beradi. Ushbu model kichik zarrachalarning ajralish jarayonini aniqroq tahlil qilish va siklon dizaynini optimallashtirish uchun ilmiy asos yaratadi.

Quyidagi MATLAB kodini ishlatib, kichik zarrachalar uchun ajralish samaradorligini vaqtga bog'liq holda grafik tarzda ko'rish mumkin (1-rasm).



1-rasm. kichik zarrachalar uchun ajralish samaradorligini vaqtga bog'liq holda grafigi

Natijalar. Tadqiqot davomida kichik zarrachalarning multisiklon qurilmasidagi ajralish samaradorligini matematik modellashtirish orqali tahlil qilindi.

Zarrachalarga ta'sir qiluvchi kuchlar, jumladan markaziy kuch, qarshilik kuchi va yopishish kuchlari o'rtasidagi muvozanat zarrachalarning siklon devorlariga yetib borishi va yopishishini aniqladi.



Markaziy kuchning ta'siri bilan zarralar siklon devorlariga qarab harakatlandi, qarshilik kuchi esa bu harakatni sekinlashtirdi. Yopishish kuchlari zarralarning devorlarga yopishishini ta'minladi. Matematik model orqali zarralarning radial harakati vaqtga bog'liq holda tahlil qilindi.

Vaqt parametrini kiritish orqali ajralish samaradorligining vaqt o'tishi bilan qanday o'zgarishi aniqlandi. Modellashtirish natijalari ko'rsatdiki, vaqt o'tishi bilan tangensial tezlik pasayib, radial tezlik oshdi, bu esa zarralarning siklon devorlariga tezroq yetib borishiga olib keldi. Shu bilan birga, samaradorlikning vaqt bo'yicha oshishi kuzatildi, bu kichik zarrachalarning samarali ajralishini ta'minladi.

Siklon ichidagi oqim traektoriyasini optimallashtirish orqali kichik zarrachalarning ajralish samaradorligini sezilarli darajada oshirish mumkinligi aniqlandi. Optimal traektoriya zarralarning devorlarga tezroq yetib borishini ta'minlab, ajralish samaradorligini oshirdi. Modellashtirish natijalari zarralarning radial tezligini oshirish orqali oqim yo'llarini optimallashtirish mumkinligini ko'rsatdi.

MATLABda chizilgan grafiklar ajralish samaradorligining vaqtga bog'liq o'zgarishini aniq ko'rsatdi. Bu grafiklar orqali vaqt o'tishi bilan zarralarning ajralish samaradorligining qanday o'zgarishini vizual tarzda baholash imkoniyati yaratildi. Grafik tahlillari zarralarning radial tezligi va samaradorlik orasidagi bog'liqlikni aniqlashga yordam berdi.

Muhokama. Natijalar asosida, multisiklon qurilmalarining samaradorligini oshirish uchun ikkita asosiy yo'nalish taklif qilindi: birinchisi, aeroelektrik maydonlardan foydalanish, ikkinchisi esa siklon dizaynini optimallashtirishdir. Matematik isbotlar va eksperimentlar natijalari bu usullar yordamida havo tozalash samaradorligini sezilarli darajada oshirish mumkinligini ko'rsatadi. Yangi yondashuvlar sanoat korxonalarida qo'llanilishi mumkin va ular ekologik jihatdan muhim ijobiy ta'sirga ega bo'ladi.

Xulosa. Ushbu tadqiqotda kichik chang zarrachalarining multisiklon qurilmasidagi ajralish samaradorligini matematik modellashtirish orqali tahlil qilindi. Modellashtirish natijasida zarrachalarning siklon devorlariga yopishishiga ta'sir qiluvchi asosiy kuchlar muvozanati, vaqt parametriga bog'liq ajralish

samaradorligi, va oqim traektoriyasining optimallashtirilishi kabi omillar o'rganildi.

Umumiy xulosa sifatida aytish mumkinki, kichik zarrachalarning multisiklon qurilmasida samarali ajralishini ta'minlash uchun oqim traektoriyasini optimallashtirish, vaqt parametrini hisobga olish va kuchlar muvozanatini tahlil qilish juda muhimdir. Ushbu tadqiqotda keltirilgan matematik model va natijalar sanoat amaliyotida multisiklon qurilmalarining samaradorligini oshirish uchun zarur ilmiy asos yaratadi. Bundan tashqari, bu yondashuvlar havoni tozalash texnologiyalarini yanada samarali qilishda va kichik zarrachalarni ajratishda yangi imkoniyatlar yaratadi.

Foydalanilgan adabiyotlar

1. Sharibaev, N., Tursunov, A., & Djuraev, S. (2022). Mathematical modeling of the laws of airborne distribution of dust particles generated in manufacturing plants. In *Journal of Physics: Conference Series* (Vol. 2373). Institute of Physics. <https://doi.org/10.1088/1742-6596/2373/7/072043>
2. Ochiyev, B. S., & Jumayev, T. Y. (2019). "Multisiklon qurilmalar samaradorligini oshirish usullari." *O'zbekiston Fanlar Akademiyasi axborotnomasi*, 47(2), 112-118.
3. Guliaev, A. A., & Ivanov, V. K. (2018). "Industrial chang tutgichlarining samaradorligini oshirish usullari." *Chang va gaz tutish texnologiyalari jurnali*, 29(3), 56-61.
4. Smith, J. D. (2017). "Particle Size and Concentration Effects on Cyclone Separators." *Chemical Engineering Science*, 64(10), 230-242.
5. Kim, S. K., & Lee, J. H. (2016). "Influence of Particle Size on Multicyclone Efficiency in Industrial Applications." *Journal of Environmental Engineering*, 142(4), 04016010.
6. Xolmatov, U. N., & Shamsiev, D. K. (2015). "Gazli aralashmalardagi chang zarralarining o'lchami va konsentratsiyasining multisiklonli qurilmalarga ta'siri." *Toshkent Davlat Texnika Universiteti ilmiy axborotlari*, 63(3), 27-34.



HUE MOMENTLARIGA ASOSLANGAN QO'LYOZMA MATNI TASVIRI BELGILARINI AJRATIB OLISH ALGORITMI

Mirzayev Nomaz,

Texnika fanlari doktori, professor,
Yetakchi ilmiy xodim, RTCIR ITI
e-mail: nomazmirza@rambler.ru

Radjabov Sobirjon Sattorovich,

Texnika fanlari doktori,
Laboratoriya mudiri, «TIQXMMI» MTU
huzuridagi FATI
e-mail: s_radjabov@yahoo.com

Rabbimov Ilyos Mehridinovich,

Texnika fanlari bo'yicha falsafa doktori (PhD),
Yetakchi ilmiy xodim,
O'zbekiston Respublikasi Prezidenti
Administratsiyasi huzuridagi Iqtisodiy
tadqiqotlar va islohotlar markazi
e-mail: ilyos.rabbimov91@gmail.com

Asrayev Muhammadmullo Abdullajon o'g'li

Texnika fanlari bo'yicha falsafa doktori (PhD),
Katta o'qituvchi, Muhammad al-Xorazmiy nomidagi
«TATU» Farg'ona filiali
e-mail: asrayevmuhammaddullo@gmail.com

Mardiyev Azamat Shakar o'g'li,

Tayanch doktorant, «TIQXMMI» MTU
huzuridagi FATI
e-mail: herr.azamat7@gmail.com

Annotatsiya: Qo'lyozma matn tasvirlarini tahlil qilish asosida shaxsni identifikatsiyalash masalasi ko'rib chiqilgan. Qo'lyozma so'zning tasvirini ushbu so'zni tashkil etuvchi obyektlarga ajratish algoritmi taklif etilgan. Ushbu algoritm uchun kirish ma'lumotlari qo'lyozma so'z skeletining binar normallashtirilgan tasviri bo'lsa, chiqish ma'lumotlari esa segmentlangan so'zni tashkil etuvchi qo'lyozma obyektlarning tasvirlaridir. Qo'lyozma obyektlarning belgilarini ajratib olish algoritmi ham taklif etilgan. Ushbu algoritm obyekt tasvirining affin almastirishlariga invariant bo'lgan Hue momentlariga asoslangan. Eng keng tarqalgan tanib olish algoritmlaridan foydalangan holda qo'lyozma matn tasvirini tahlil qilish asosida shaxs identifikatsiyasi natijalari keltirilgan.

Kalit so'zlar: qo'lyozma matn, shaxs identifikatsiyasi, tasvirni segmentlarga ajratish, belgilarni ajratib olish.

Kirish. Hozirgi kunda shaxsni tanib olish biometrik texnologiyalari, xususan, qo'lyozma matni tasvirlarini tahlil qilishga asoslangan texnologiyalar yuqori tezlikda rivojlanib bormoqda, chunki bu texnologiyalar inson faoliyatining qo'lyozma matni muallifini tanibni olish talab qilinuvchi ko'pgina sohalarida keng qo'llanilmoqda. Ushbu yo'nalishda o'tkazilgan tahlil qo'lyozma matni tasvirlarini



segmentatsiya qilish, belgilar fazosini shakllantirish hamda ushbu belgilar asosida tanib olish masalalarini hal qilish bunday tizimlarni yaratishda eng muhim hisoblanishini ko'rsatdi. Hozirgi vaqtga keltirilgan masalalarni hal qiluvchi bir qator usullar va algoritmlar ishlab chiqilganligiga qaramasdan qo'lyozma matni tasvirlarini tahlil qilish asosida shaxsni identifikatsiya qilish aniqligini oshirishni ta'minlovchi mavjudlarini usullar va algoritmlarni takomillashtirish hamda yangilarini ishlab chiqish muammosi yetarlicha o'rganilmagan.

So'nggi yillarda qo'lyozma matn muallifini aniqlash sohasidagi tadqiqotlar asosan matnning statistik xususiyatlarini ajratib olishga qaratilgan. Natijada, qo'lyozma matn tasvirlarining yo'l uzunligi va yozuv qiyaliklari taqsimoti, hattoki, entropiya xarakteristikalarini kabi xususiyatlarini ajratib olish uchun algoritmlar ishlab chiqilgan. [1] da taklif qilingan algoritmi kabi bir qator algoritmlar muallif yozuvining global va mahalliy xususiyatlarini birlashtiradi, ammo bu xususiyatlar asosida tasniflash natijalari hali ham oddiy. [2] da xat mualliflari klassifikatsiyasi uchun shablonlar ishlatilgan va bu klassifikatsiya masalasi matnda ushbu shablonlarning paydo bo'lish chastotasiga asoslangan. [3] da qo'lda yozilgan matnning makro va mikro xususiyatlarini aniqlash algoritmi taklif qilingan va individual xususiyatlar xat muallifini farqlash uchun turli qobiliyatlarga ega ekanligi ko'rsatilgan. [4] qo'lyozma matn tasvirlari Gabor filtrlari va birgalikdagi matritsani qo'llash orqali olingan turli teksturalar sifatida ko'rib chiqiladigan xolistik yondashuvni taqdim etadi. [5] da qo'l yozuvi matnning har bir satrining strukturaviy xususiyatlaridan kelib chiqqan holda ajratilgan va [6] da bu maqsadda bog'langan komponentlar konturidan foydalanilgan. [7] da qo'l yozuvi xususiyati fazosi qo'lda yozilgan matn tasvirlarining tashqi konturining minimallarini tahlil qilish natijasida olingan lokal xususiyatlardan shakllanadi.

Bu ishda [8] da keltirilgan algoritmlar yordamida qo'lda yozilgan matnning asl tasviriga oldindan ishlov berish (sifatni oshirish, binarlashtirish,

qator va so'zlarni segmentlash, skeletizatsiya, yozuv qiyaligini to'g'irlash) amalga oshiriladi. Keyin tanlangan so'z tasvirlari ushbu ishda taklif qilingan obyektlar bo'yicha tasvir etikasi segmentatsiyasi algoritmi yordamida segmentlarga bo'lingan. Ushbu obyektlarning xususiyatlarini ajratib olish uchun obyekt tasvirining affin almashtirishlariga invariant Hue momentlariga asoslangan algoritmi taklif etiladi. Yaratilgan belgi maydoniga asoslanib, xat muallifi eng keng tarqalgan tanib olish algoritmlari yordamida aniqlandi.

Taklif etilayotgan algoritmlar. Ma'lumki, qo'lyozma matn tasviridan shaxsni aniqlash vazifasi asl tasvirni tahlil qilish asosida yozuv muallifini aniqlashdan iborat bo'lib, qo'lyozma matnning asl tasvirini olish, oldindan ishlov berish, segmentatsiya qilish, xususiyatlarni ajratib olish va tanib olish bosqichlaridan iborat.

Ushbu maqola qo'lyozma so'zning tasvirini obyektlarga bo'lish va yozuv muallifini keyinchalik aniqlash uchun ushbu obyektlarning xususiyatlarini ajratib olish algoritmlarini taklif qiladi.

Qo'lyozma so'z tasvirini ushbu so'zni tashkil qiluvchi obyektlarga segmentatsiyalash uchun ushbu tasvirdagi yozuvni tahliliga asoslangan algoritmi taklif etilmoqda. Ushbu algoritmi uchun kiruvchi ma'lumotlar sifatida qo'lyozma so'z skeletining normallashtirilgan binar tasviri, chiquvchi ma'lumotlar esa – segmentlangan so'zni tashkil qiluvchi qo'lyozma obyektlarining tasvirlari O_1, O_2, \dots, O_k hisoblanadi.

Aytaylik, (x_1, y_1) va (x_2, y_2) – qo'lyozma so'zi I tasvirining mos holda yuqori chap va quyi o'ng koordinatalari berilgan bo'lsin.

Taklif etilayotgan segmentatsiyalash algoritmi quyidagi qadamlardan tashkil topadi.

1-qadam. Boshlang'ich qiymatlarni berish:

$k := 1;$

$lX := x_1; rX := x_1;$

$cRow := x_1; nRow := cRow + 1; Up :=$

$True,$



bu yerda (lX, y_1) va $(rX, y_2) - O_k$ qo'lyozma obyekti tasvirining mos holda yuqori chap va quyi o'ng koordinatalari.

2-qadam. Ko'rib chiqilayotgan ustundagi qora piksellar to'plami C aniqlansin:

$$C := \{b(cRow, c) \mid b(cRow, c) \in I \text{ va } c \in [y_1, y_2]\}.$$

3-qadam. Agar $nRow > x_2$ bo'lsa, 10-qadamga o'tilsin.

4-qadam. $nRow$ ustundagi qora piksellar to'plami N aniqlansin:

$$N := \{b(nRow, n) \mid b(nRow, n) \in I \text{ va } n \in [y_1, y_2]\}.$$

5-qadam. Agar $|N| = 0$ bo'lsa, 8-qadamga o'tilsin.

6-qadam. Agar $|N| = 1$ va $|n - c| \leq 1$ bo'lsa, agar $c > n$ va $Up == True$ bo'lsa,

8-qadamga o'tilsin,

aks holda,

agar $c < n$ bo'lsa, $Up := True$

9-qadamga o'tilsin.

Bu yerda n va c shunday tanlanganki, $b(cRow, c)$ va $b(nRow, n)$ qora piksellar o'zaro bog'langan.

7-qadam. Agar $\min_{\substack{b(nRow, n_j) \in N \\ b(cRow, c_j) \in C}} |n_j - c_j| \leq 1$

bo'lsa,

agar $c > n$ va $Up == True$ bo'lsa,

8-qadamga o'tilsin,

aks holda,

agar $c < n$ bo'lsa, $Up := True$

9-qadamga o'tilsin.

Bu yerda n va c shunday tanlanganki, $b(cRow, c)$ va $b(nRow, n)$ qora piksellar o'zaro bog'langan.

8-qadam. O_k qo'lyozma obyektining tasviri ajratib olinsin:

$$rX := nRow;$$

$$O_k :=$$

$$\{o(i, j) \mid o(i, j) \in I, i \in [lX, rX], j \in [y_1, y_2]\};$$

$$lX := rX + 1; Up := False; k := k + 1.$$

9-qadam. Qiymatlar o'zgartirilsin:

$$cRow := nRow; C := N$$

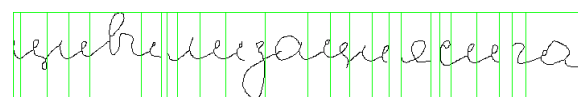
va 3-qadamga o'tilsin.

10-qadam. Tamom.

Quyidagi rasmda qo'lyozma so'z tasvirini ushbu so'zni tashkil qiluvchi obyektlarga segmentatsiyalash algoritmining ish natijasi keltirilgan.



a)



b)

1-rasm. Berilgan tasvir (a) va taklif etilayotgan algoritmdan foydalanib uni segmentatsiyalash natijalari (b)

Segmentatsiyalash natijasida olingan qo'lyozma obyektlari tasvirining statistik belgilarini ajratish algoritmi taklif etilmoqda. Tasvirning statistik belgilari sifatida Hue momentlarini hisoblash qaralgan.

Taklif etilayotgan algoritm qo'lyozma obyektlar tasvirlarining affin almashtirishlarga invariant bo'lgan Hue momentlarini hisoblash, obyektlarni aniqlangan belgilari bo'yicha yaqinligi (o'xshashligi) asosida guruhlash va har bir hosil bo'lgan guruhdan bitta etalon obyektini ajratib olishga asoslangan. Ushbu algoritm uchun kiruvchi ma'lumotlar bo'lib yuqorida keltirilgan algoritmi yordamida segmentatsiya qilingan qo'lyozma obyektlari tasvirlari O_1, O_2, \dots, O_k , chiquvchi ma'lumotlar bo'lib esa – ushbu obyektlarning belgilardagi ifodalari hisoblanadi.

Taklif etilayotgan qo'lyozma matni tasvirining xarakterli belgilarini ajratib olish algoritmi quyidagi bosqichlardan tashkil topadi.

1-bosqich. Qo'lyozma obyektlarining xarakteristik belgilarini hisoblash. Ushbu bosqichda har bir qo'lyozma obyekt O_i ($i = \overline{1, k}$) uchun Hue momentlari hisoblanadi:



$$\begin{aligned}
 h_0 &:= \eta_{20} + \eta_{02}; \\
 h_1 &:= (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^2; \\
 h_2 &:= (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2; \\
 h_3 &:= (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2; \\
 h_4 &:= (\eta_{30} - 3\eta_{12})(\eta_{30} \\
 &\quad + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2] \\
 &\quad + \\
 &\quad + (3\eta_{21} - \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \\
 &\quad \eta_{03})^2]; \\
 h_5 &:= (\eta_{20} - \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \\
 &\quad \eta_{03})^2 + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03})]; \\
 h_6 &:= (3\eta_{21} - \eta_{03})(\eta_{30} \\
 &\quad + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2] \\
 &\quad + \\
 &\quad + (\eta_{30} - 3\eta_{12})(\eta_{21} + \eta_{03})[3(\eta_{30} + \\
 &\quad \eta_{12})^2 - (\eta_{21} + \eta_{03})^2].
 \end{aligned}$$

Bu yerda:

$$\begin{aligned}
 \eta_{ij} &:= \frac{\mu_{ij}}{\frac{i+j}{2} + 1}; \\
 \mu_{ij} &:= \sum_x \sum_y (x - \bar{x})^i (y - \bar{y})^j I(x, y); \\
 \bar{x} &:= \frac{M_{10}}{M_{00}}; \\
 \bar{y} &:= \frac{M_{01}}{M_{00}}; \\
 M_{ij} &:= \sum_x \sum_y x^i y^j I(x, y).
 \end{aligned}$$

2-bosqich. O'xshash qo'lyozma obyektlari qism-to'plamini shakllantirish. Ushbu bosqichda qo'lyozma obyektlari to'plami O_1, O_2, \dots, O_k ni ularning yaqinliklari (o'xshashliklari) bo'yicha qism-to'plamlarga bo'lish amalga oshiriladi.

Aytaylik, G_q ($q = \overline{1, k}$) – o'xshash obyektlar qism-to'plamlari bo'lsin. G_p va G_q qism-to'plamlar o'rtasidagi yaqinlik o'lchovi $L(G_p, G_q)$ ularning belgilarining normasi L2 bo'yicha aniqlanadi.

O'xshash obyektlar qism-to'plamlarini shakllantirish quyidagicha amalga oshiriladi.

2.1-qadam. Boshlang'ich qiymatlarni berish:

$$G_1 := \{O_1\}, G_2 := \{O_2\}, \dots, G_k := \{O_k\},$$

$$L(G_i, G_j) := b_{ij}, t := k.$$

2.u-qadam ($u > 1$). Toki $t > n$:

– G_p va G_q bitta qism-to'plamga birlashtirilsin,

agar

$$L(G_p, G_q) :=$$

$$\min \left\| L_{ij}^{(u-1)} \right\|_{(k-u+1) \times (k-u+1)}, (i, j \in [1, k-u+1], i \neq j)$$

bo'lsa;

– $\|L_{ij}^u\|$ -tartibdagi yangi yaqinlik matrisasi

shakllantirilsin;

– $t := t - 1$.

Belgilarni birlashtirish jarayoni har bir obyekti o'z qism-to'plamida yaqinroq bo'lgan G_1, G_2, \dots, G_n obyektlarning n ta qism-to'plami olinmagunicha davom ettiriladi.

3-bosqich. Etalon qo'lyozma obyektlarini aniqlash. Ushbu bosqichda o'xshash qo'lyozma obyektlarining har bir qism-to'plami G_q ($q = \overline{1, n}$) dan bittadan obyekt ajratib olinadi va etalon obyektlar to'pdami shakllantiriladi.

Aytaylik, $\mathfrak{C}_q = |G_q|$ – o'xshash obyektlar qism to'plami G_q ning quvvati, \mathbb{E}_0 – etalon obyektlar to'plami bo'lsin.

Etalon qo'lyozma obyektlarini aniqlash quyidagicha amalga oshiriladi.

3.1-qadam. $\mathbb{E}_0 := \emptyset$.

3.2-qadam. Barcha q ($q = \overline{1, n}$) uchun, agar $\mathfrak{C}_q = 1$ bo'lsa, u holda $\mathbb{E}_0 := \mathbb{E}_0 \cup G_q$.

3.3-qadam. Barcha q ($q = \overline{1, n}$) uchun, agar $\mathfrak{C}_q > 2$ bo'lsa, u holda:

– har bir $O_i \in G_q$ ($i = \overline{1, \mathfrak{C}_q}$) obyektning G_q qism-to'plamning boshqa obyektlariga yaqinlik bahosi $\rho(O_i)$ hisoblansin:

$$\rho(O_i) := \sum_{j=1}^{i-1} L(O_i, O_j) + \sum_{j=i+1}^{\mathfrak{C}_q} L(O_i, O_j);$$

– G_q qism-to'plamning G_q boshqa obyektlariga maksimal darajada yaqin bo'lgan obyekti aniqlansin:



$$O_{i_q} := \arg \min_{O_i \in G_q} \rho(O_i);$$

$-O_{i_q}$ obyekt etalon obyektlar to'plamiga
qo'shilsin:

$$\mathbb{E}_0 := \mathbb{E}_0 \cup O_{i_q}.$$

3.4-qadam. Barcha q ($q = \overline{1, n}$) uchun, agar
 $\mathbb{C}_q = 2$ bo'lsa, u holda:

– har bir $O_i \in G_q$ obyektning etalon obyektlarga
yaqinligi bahosi $\rho(O_i)$ hisoblansin:

$$\rho(O_i) := \sum_{j=1}^{|\mathbb{E}_0|} L(O_i, O_j^E);$$

– G_q qism-to'plamining \mathbb{E}_0 obyektlaridan
sezilarli farq qiluvchi obyektini aniqlansin:

$$O_{i_q} := \arg \max_{O_i \in G_q} \rho(O_i);$$

$-O_{i_q}$ obyekt etalon obyektlar to'plamiga
qo'shilsin:

$$\mathbb{E}_0 := \mathbb{E}_0 \cup O_{i_q}.$$

Ishlab chiqilgan algoritmlarni eksperimental o'rganish. Tajribaviy tadqiqotlar IAM [9] va IUHT [10] qo'lyozma matni tasvirlari bazalari asosida o'tkazildi. IAM bazasida ingliz tilidagi 657 ta muallifga tegishli bo'lgan skanerlangan 1539 ta qo'lyozma matni sahifasi mavjud. IUHT bazasi o'zbek tilidagi (lotin va kirill grafikasi) 373 ta muallifga tegishli bo'lgan skanerlangan 2242 ta qo'lyozma matni sahifasidan tashkil topgan. Bunda har ikkala bazada ham sahifalar 600 dpi tasvir aniqligi bilan skanergangan va kulrang tasvirlar ko'rinishida JPEG formatida saqlangan, sinflarga ajratish kerak bo'lgan obyektlarning sinflari esa muvozanatlashgan.

Qo'lyozma matni tasvirlarini tahlil qilish asosida shaxsni identifikatsiya qilish masalasi ishda taklif qilingan belgilarni ajratib olish va taniqli tanib olish algoritmlaridan foydalangan holda hal qilindi. Qiyosiy tahlil qilish uchun ushbu masala kiruvchi va yashirin qatlamlarda ReLU faollashtirish funksiyalariga, chiquvchi qatlamda esa – SoftMax faollashtirish funksiyalariga ega bo'lgan uch qatlamli to'liq bog'lanishli sun'iy neyron tarmog'idan foydalanib ham hal qilindi. Bunday arxitekturadan

klassik hollarda obyektlarni sinflarga ajratish masalalarini hal qilishda foydalaniladi. Ta'kidlab o'tamizki, taklif qilingan belgilarni ajratib olish algoritmini qo'llanishi natijasida tanib olish obyektlari soni kichik bo'lganligi uchun neyron tarmog'ini o'qitish uchun berilgan ma'lumotlarni augmentatsiya qilish amalga oshirildi.

Sanab o'tilgan algoritmlar sifatini baholash berilgan tanlanmaning 20% ni tashkil qiluvchi nazorat tanlanmasi obyektlarini tanib olish aniqligi bo'yicha hamda 10×10 karrali sirpanuvchi nazoratda foydalangan holda o'tkazildi.

IAM va IUHT tasvirlar bazalaridan olingan nazorat tanlanma obyektlarini sinflarga ajratish natijalari mos tarzda 1- va 2-jadvallarda keltirilgan.

1-jadval.

IAM tasvirlar bazasi qo'lyozma obyektlarini sinflarga ajratish natijalari

t/r	Tanib olish algoritmi	Tanib olish aniqligi (% da)
1.	Minimal masofa	84,82
2.	Qaror qabul qilish daraxti	84,19
3.	Tasodifiy o'rmon	87,13
4.	k ta eng yaqin qo'shnilar	77,81
5.	Uch qatlamli SNT	88,69

Shuni ta'kidlab o'tamizki, berilgan tasvirlarga dastlabki ishlov berish, satrlar va so'zlarni segmentatsiya qilish [8] da taklif qilingan algoritmlardan foydalanib o'tkazildi, qo'lyozma obyektlari esa ushbu ishda taklif qilingan segmentatsiyalash algoritmidan foydalanib ajratib olindi.

2-jadval.

IUHT tasvirlar bazasi qo'lyozma obyektlarini sinflarga ajratish natijalari

t/r	Tanib olish algoritmi	Tanib olish aniqligi (% da)
1.	Minimal masofa	86,34
2.	Qaror qabul qilish daraxti	85,21



3.	Tasodifiy o'rmon	88,42
4.	<i>k</i> ta eng yaqin qo'shnilar	79,78
5.	Uch qatlamli SNT	88,71

Olingan natijalarni solishtirish (1-, 2-jadvallarga qarang) taklif qilingan qo'lyozma matni belgilarini ajratib olish algoritmi asosida tanib olish algoritmlardan aniqlik nuqtai-nazaridan eng samaralisi bo'lib uch qatlamli sun'iy neyron tarmoqqa asoslangan algoritmi ekanligini ko'rsatdi.

Xulosa. Tajribalar natijalari qo'lyozma so'z tasvirini uning tarkibiy obyektlariga bo'lish va ushbu obyektlarning xususiyatlarini aniqlash uchun taklif qilingan algoritmlarning ishlashini ko'rsatdi. Taklif etilgan algoritmlar qo'lyozma matnli tasvirlarni tahlil qilish uchun turli tizimlarni yaratish uchun ishlatilishi mumkin.

Adabiyotlar

1. Siddiqi I., Vincent N. Combining global and local features for writer identification //In Proc. of the 11 Int. Conf. on Frontiers in Handwriting Recognition, Montreal, 2008.

2. Niels R., Grootjen F., Vuurpijl L. Writer identification through information retrieval: the allograph weight vector //In Proc. of the 11 Int. Conf. on Frontiers in Handwriting Recognition, Montreal, 2008.

3. Srihari S., Arora H., Lee S. Individuality of handwriting //Journal of Forensic Sciences, 47(4):1.17, July 2002.

4. Said H.E.S., Tan T.N., Baker K.D. Personal Identification Based on Handwriting //Pattern Recognition, vol. 33, 2000, pp.149-160.

5. Marti U.V., Messerli R., Bunke H. Writer Identification Using Text Line Based Features //In Proc. of the 6th Int. Conf. on Document Analysis and Recognition, Seattle, USA, 2001, pp. 101-105.

6. Schomaker L., Bulacu M. Automatic Writer Identification Using Connected-Component Contours and Edge-Based Features of Uppercase Western Script

//In IEEE Transactions of Pattern Analysis and Machine Intelligence, vol. 26, no. 6, pp. 787-798, 2004.

7. Bensefia A., Paquet T., Heutte L. A writer identification and verification system //Pattern Recognition Letters, vol. 26, issue 13, 2080-2092, 2005.

8. Дадаханов М.Х. Қўлэзма матни тасвирига дастлабки ишлов бериш алгоритмлари: Техн. фанлари бўйича фалсафа докт. (PhD) илм. дар. олиш учун ёзилган дис. – Тошкент: АКТ ИИМ, 2021. – 105 б.

9. Marti U.V., Bunke H. The IAM-Database: An English Sentence Database for Offline Handwriting Recognition //Int. J. Document Analysis and Recognition, 2002, vol. 5, no. 1, pp. 39-46.

10. Раджабов С.С., Дадаханов М.Х., Асраев М.А., Маматов А.А. Қўлэзмали матн тасвирларини сегментациялаш алгоритмлари //Информатика ва энергетика муаммолари. – Тошкент, 2020. – №3. – 137-142 б.



ZOLDIR PROKATLASH STANI ISHCHI ELEMENTLARINING KONSTRUKSIYALARINI ISHLAB CHIQISH MASALASI

Shaxobutdinov Rustam Erkinbayevich

Islom Karimov nomidagi Toshkent davlat texnika
universiteti Nazariy mexanika va mashina va
mexanizmlar nazariyasi kafedrasida texnika fanlari
bo'yicha falsafa doktori, PhD, dotsent
E-mail: rus-0373@mail.ru

Karimova Anorgul Ruzimovna

Islom Karimov nomidagi Toshkent davlat texnika
universiteti Nazariy mexanika va mashina va
mexanizmlar nazariyasi kafedrasida katta o'qituvchi
E-mail: kanorgul@gmail.com

Nosirov To'lqin Narzulla o'g'li

"O'zmetkombinat" AJ, Zoldir prokatlash sexi
boshlig'i o'rinbosari
E-mail: t.nosirov@uzbeksteel.uz

Annotatsiya: Maqolada zoldir prokatlash stanining eng muhim va zaruriy ishchi elementlaridan hisoblangan zoldir prokatlash valoklari va yo'naltiruvchi lineyklarining konstruksiyalarini ishlab chiqish masalasi o'rganilgan. Ariqchalarining markazlari o'zgaruvchan vintli kalibrga ega bo'lgan zoldir prokatlash valoklarini va zoldir prokatlash stani yo'naltiruvchi lineyklarining konstruksiyalarini loyihalash maqsadida, ularning geometrik parametrlarini matematik ifodalar orqali nazariy asoslash uchun algoritmlar ishlab chiqilgan. Olingan matematik ifodalarnig yechimlarini MatCAD 15 dasturida tahlil qilingan va KOMPAS 3d dasturi yordamida zoldir prokatlash valoklari va yo'naltiruvchi lineyklarining modeli ishlab chiqilgan.

Kalit so'zlar: maydalovchi po'lat zoldir, zoldir prokatlash stani, zoldir prokatlash valogi, yo'naltiruvchi lineyka, kulachok, vintli kalibr.

Kirish. Ko'ndalang vintli prokatlash bu metallarga ishlov berish jarayonining bir turi bo'lib, unda ma'lum o'lchamlarga ega bo'lgan va belgilangan yuqori haroratda qizdirilgan metall xom-ashyo bir xil yo'nalishda aylanadigan valoklar hamda ularni prokatlash o'qi bo'yicha ravon ilgarilanma, aylanma harakatini ta'minlovchi yo'naltiruvchi lineyklar orasidan o'tadi Bu texnologik jarayon yordamida kalta o'lchamli aylanma shakldagi mahsulotlarni ishlab chiqarishda foydalaniladi [1-5].

Ko'ndalang vintli prokatlash usuli yordamida maxsus shakldagi vallar, tog'-kon sanoatida qo'llaniladigan vintli mahkamlagichlar, temir yo'llarda qo'llaniladigan vagon o'qlari, tog'-kon sanoati va

ko'mir ishlab chiqarish va boshqa sanoat sohalarida qo'llaniladigan maydalovchi po'lat zoldirlar va boshqa mahsulotlar ishlab chiqariladi.

Zoldir prokatlash stanlarida bajariladigan ko'ndalang vintli prokatlash jarayoni asosiy texnologik jarayon hisoblanib, bunda zoldir prokatlash valoklarini hamda yo'naltiruvchi lineyklarini loyihalash o'ta yuqori aniqlikda tayyorlashni talab etadi (1-rasm). 1-rasmda 1 – quyi yo'naltiruvchi lineyka, 2 – o'ng valok, 3 – chap valok tasvirlangan.





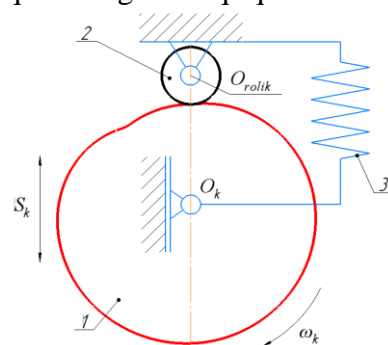
1-rasm. Quyi yo'naltiruvchi lineyka va prokatlash valoklarining metall xom-ashyoning kirish tomonidan ko'rinishi.

Zoldirlarni prokatlash usuli bilan ishlab chiqarish uchun mo'ljallangan stanning muhim elementlarining konstruksiyalarini ishlab chiqish bugungi kunda maydalovchi po'lat zoldirlarni ishlab chiqarish texnologiyasining rivoji uchun eng muhim talablardan biridir. Ushbu masalani yechish uchun zoldir prokatlash valoklari va yo'naltiruvchi lineyklarini loyihalash maqsadida, ularning geometrik parametrlarini aniqlashning nazariy asoslarini ishlab chiqish bo'yicha algoritmlar va hisoblash dasturlarini tuzish ishlarini amalga oshirish maqsadga muvofiq hisoblanadi.

Adabiyotlar tahlili va metodologiya. Zoldir prokatlash valoklari va yo'naltiruvchi lineyklar maydalovchi po'lat zoldirlarni prokatlash uchun mo'ljallangan stanning muhim ishchi elementlari hisoblanadi. Zoldirlarni prokatlash jarayonida vintli kalibrli valoklarning o'z o'qiga nisbatan aylanma harakat qilishi natijasida, belgilangan aniq o'lchamlarga ega bo'lgan metall xom-ashyoning ishchi qismi prokatlash o'qi bo'ylab harakatlanadi. Zoldir prokatlash stani yo'naltiruvchi lineykalari prokatlanayotgan metall xom-ashyo uchun tayanch vazifasini bajarishi bilan bir vaqtning o'zida uning prokatlash o'qiga nisbatan aylanma va prokatlash o'qi bo'ylab ilgariylanma harakatini ta'minlash vazifalarini amalga oshiradi [6].

RT117 markali tokarlik vint qirqish dastgohida ariqchalarining markazlari o'zgaruvchan vintli kalibrli olti kirimli zoldir prokatlash valoklarini qirqishda eng

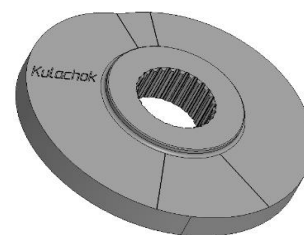
asosiy vazifalardan birini bajaruvchi zveno kulachoklar hisoblanadi. Shuning uchun olti kirimli zoldir prokatlash valoklarini qirqishda profili nazariy asoslangan kulachoklarni loyihalashda eng yuqori samaradorlikka ega bo'lish uchun hisoblash ishlarini o'ta yuqori aniqlikda bajarish zarur bo'ladi. Bu esa asosan, kulachokka qo'yilgan talablarning bajarilishini ta'minlash masalasi bilan bog'liq. Matematik hisoblashlar yordamida ma'lum aniqlikdagi o'lchamlar bo'yicha tayyorlangan kulachoklar yordamida zoldir prokatlash valoklarining o'zgaruvchan markazli ariqchalarga ega vintli kalibrlarini kesish uchun maxsus nusxa ko'chirish moslamasi bilan jihozlangan tokarlik vint qirqish dastgohida qirqiladi.



2-rasm. Zoldir prokatlash valoklarini qirqishda qo'llaniladigan kulachokli mexanizmning kinematik sxemasi.

2-rasmda zoldir prokatlash valoklarini qirqishda qo'llaniladigan kulachokli mexanizmning kinematik sxemasi keltirilgan bo'lib, bu sxemada 1 – kulachok, 2 – rolik, 3 – prujina tasvirlangan.

Zoldir prokatlash valoklarini qirqishda qo'llaniladigan kulachoklar raqamli dasturlash bilan boshqariladigan (RDB) frezalash dastgohida tayyorlanadi.



3-rasm. Zoldir prokatlash stani valoklarini qirqishda ishlatiladigan kulachokning umumiy ko'rinishi.



Buning uchun zoldir prokatlash valoklarini kesishda vintli kalibrning qadamini ta'minlab beruvchi profili nazariy asoslangan kulachoklarning konstruksiyalari ishlab chiqiladi. Shu bilan birga, RDB dastgohiga mos bo'lishi uchun kompyuterda dasturlar tuziladi va kulachoklar tayyorlanadi (3-rasm).

Prokatlash jarayonida zoldir prokatlash valoklarining xom-ashyoga ishlov beruvchi qismi shakl hosil qiluvchi va shaklga ishlov beruvchi qismlarga ajralishi bilan farqlanadi. Kulachoklarning profilini aniqlash maqsadida bir qator hisoblash ishlari bajariladi va kinematik hamda dinamik talablarga javob beradigan texnologiya ishlab chiqiladi. Bunda

s_T - turtkichning ko'chishi, φ_k - kulachokning burilish burchagi, s_T' - turtkichning tezlik analogi, s_T'' - turtkichning tezlanish analogi, h_{max} - turtkichning maksimal ko'chishi, φ_u - uzoqlashish faza burchagi, $\varphi_{u,t}$ - uzoqda turish faza burchagi, φ_y - yaqinlashish faza burchagi va $\varphi_{y,t}$ - yaqinda turish faza burchagi kabi parametrlar qiymatlarining o'zgarishi asos qilib olinadi (zoldir prokatlash valoklarini qirqishda ishlatiladigan kulachoklarda uzoqda turish faza burchagi nolga teng: $\varphi_{u,t} = 0$). [7] da kulachokning to'rt harakatlanish fazalari uchun turtkichning siljishi, tezligi va tezlanishlarini aniqlashning matematik modellari siljish parametrlarining o'zgarish dinamikasi asosida ishlab chiqilgan.

Zoldir prokatlash stanining mahsuldorligini oshirish maqsadida esa, valoklardagi kirimlarning soni oshiriladi. Bu esa valoklarning har bir aylanishida oltitagacha bo'lgan maydalovchi po'lat zoldirlarni olish imkoniyatini beradi.

Ushbu texnologik jarayonni soddalashtirish maqsadida, zoldir prokatlash stani valoklarini loyihalash algoritmini ishlab chiqish va shu asosda raqamli dastur bilan boshqariladigan dastgoh yordamida valoklarni yuqori aniqlikda qirqish texnologiyasini joriy qilish samaralidir.

Zoldir prokatlash valoklarni qirqish jarayonida metall xom-ashyoning deformatsiyalanishini hisobga olish bilan bir qatorda vintli kalibr geometriyasining murakkab ishlanmasini ishlab chiqish va bunda eng muhim hisoblangan vintli kalibr gardishlarining qalinligi, balandligi va boshqa parametrlarini aniqlagan holda loyihalash hamda vintli kalibrni qirqish texnologiyasini amalga oshirish zarur bo'ladi. Zoldir prokatlash stanining yana bir muhim elementlaridan biri bo'lgan yo'naltiruvchi lineyklarining asosiy geometrik parametrlarini nazariy asoslash va uni loyihalashda zoldir prokatlash valoklarining diametri, prokatlash valogi ishchi qismining uzunligi, prokatlash valogi rebordalarining balandligi, prokatlanayotgan zoldirning diametri, prokatlash valoklari orasidagi o'qlararo masofa kabi parametrlarning qiymatlarini o'rganish muhimdir.

Natijalar. Masalani aniq misollarda tahlil qilish uchun olti kirimli diametri 50mm bo'gan maydalovchi po'lat zoldirlarni ishlab chiqarish uchun mo'ljallangan stanning valoklarini loyihalash ishlari bajarildi.

$X(\psi)$	347,117	347,06413	346,90555	346,64129	346,27144	345,79612	...
$Y(\psi)$	0	0,949389	1,898755	2,848097	3,797415	4,746709	...
$Z1(\psi)$	0	6,058027	12,114209	18,1667	24,213658	30,25324	...

1-jadval. Zoldir prokatlash valoklarining vint chiziqlarini hosil qilish uchun koordinata o'qlari bo'yicha dastlabki qiymatlar.

Loyihalash yuqori aniqlikda bajarilishi uchun KOMPAS 3d dasturi imkoniyatlaridan kelib chiqqan holda, vintli kalibrning uzunligi bo'yicha 823 ta qiymatlar orqali X, Y, Z o'qlari bo'yicha koordinatalarining sonli natijalari olindi (jadvalda X, Y, Z dekart koordinata o'qlari bo'yicha qiymatlardan dastlabki 6 ta qiymat keltirilgan).

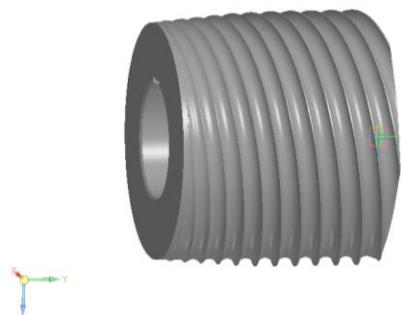
Vintli kalibrning uzunligi bo'yicha olingan 823 ta qiymatlar bo'yicha jadval asosida vintli kalibrni qirqish texnologiyasini amalga oshirish uchun dastlab quyidagi asosiy ketma-ketlik bo'yicha ish olib boriladi:



$$\begin{cases} \psi_1 := 0 \dots \psi_{umumiy}, & \alpha(\psi_1) := \psi_1 \cdot \text{deg}, \\ X(\psi_1) := R_{\text{prok.o'qi}} \cos(\alpha(\psi_1)) \\ Y(\psi) := Z(\psi) \\ Z_1(\psi_1) := R_{\text{prok.o'qi}} \sin(\alpha(\psi_1)). \end{cases} \quad (1)$$

bu yerda ψ_1 – valok uzunligiga mos bo'lgan vintli kalibrning uzunligi; ψ_{umumiy} – vintli kalibrning umumiy uzunligi; $R_{\text{prok.o'qi}}$ – prokatlash o'qidan vintli kalibr markazigacha bo'lgan masofa.

X, Y, Z dekart koordinata o'qlarining har biri bo'yicha vintli kalibrning uzunligida belgilangan qiymatlar asosida zoldir prokatlash stani valoklarining vint chiziqlari hosil qilinadi. Olti kirimli diametri 50mm bo'gan maydalovchi po'lat zoldirlarni prokatlash maqsadida, zoldir prokatlash valoklarining modeli ishlab chiqildi (4-rasm).



4-rasm. Olti kirimli diametri 50mm bo'gan maydalovchi po'lat zoldirlar uchun zoldir prokatlash valogining umumiy ko'rinishi.

Turli diametrdagi maydalovchi po'lat zoldirlarni prokatlash uchun prokatlash valoklarining kalibrovkalarini ishlab chiqish bir-biridan farq qiladi va ularni tayyorlash imkoniyatlari nazariy jihatdan ilmiy asoslashni talab etadi. Zoldir prokatlash stani yo'naltiruvchi lineyklarining asosiy geometrik parametrlarini hisoblashda ularning ishchi qismining qalinligini aniqlash uchun prokatlash valoklarning o'qlararo masofasi o'zgarmas qiymatga ega ekanligiga alohida ahamiyat berish lozim.

Yuqori va quyi yo'naltiruvchi lineyklarining balandligi quyidagicha aniqlanadi:

$$\begin{aligned} h_{yu.} &= h_1 - \frac{d_{zoldir}}{2} \\ h_q. &= h_2 - \frac{d_{zoldir}}{2} \end{aligned} \quad (2)$$

bu yerda h_1 – prokatlash o'qidan yuqori yo'naltiruvchi lineykaning asosigacha bo'lgan masofa, h_2 – prokatlash o'qidan quyi yo'naltiruvchi lineykaning asosigacha bo'lgan masofa. Bu h_1 va h_2 masofalarning qiymati prokatlash stani konstruktiv o'lchamlariga asosan olinadi.

Turli diametrdagi zoldirlar uchun yo'naltiruvchi lineyklarining balandigi ham har xil qiymatlarni qabul qiladi. Prokatlanayotgan zoldirning diametriga bog'liq ravishda, ZPS 40-80 va ZPS 80-120 stanlari uchun konstruktiv o'lchamlar har xil bo'ladi.

Yuqori va quyi yo'naltiruvchi lineyklar uchun matematik ifodalarni aniqlashda zoldirning diametrik va zoldir prokatlash valoklari vintli ariqchalari uchun vintli kalibr uzunligining qiymatlarlarini inobatga olish zarur. Zoldirlarning hosil bo'lishda yo'naltiruvchi lineyklarining ishchi qismi alohida ahamiyatga ega. Prokatlash stanida yo'naltiruvchi lineykaning ishchi qismini konstruktiv joylashish doimiysi k ga farq qilgan holda prokatlash valoklarining shakl hosil qiluvchi va shaklga ishlov beruvchi qismlariga mos bo'lgan 2 ta asosiy ishchi qismga ajratish mumkin. Buni esa yo'naltiruvchi lineykani prokatlash staniga o'rnatish davomida aniqlash mumkin bo'ladi.

Yo'naltiruvchi lineyka ishchi qismining umumiy uzunligi quyidagicha aniqlanadi:

$$l_{lineyka} = k + l_{valok} \quad (3)$$

bu yerda k – yo'naltiruvchi lineykaning prokatlash staniga konstruktiv joylashish doimiysi, l_{valok} – zoldir prokatlash valogining umumiy uzunligi.

Yo'naltiruvchi lineyka ishchi qismining uzunligini prokatlash valogining zoldir chiqish tomonidan boshlab hisoblaganda, vintli kalibr uzunligiga bog'liq holda quyidagicha aniqlanadi:

$$l(\varphi) = Z_{k_1}(\varphi) + T_{\text{dastgoh}}(\varphi) - R_{\text{kalibr}} \quad (4)$$

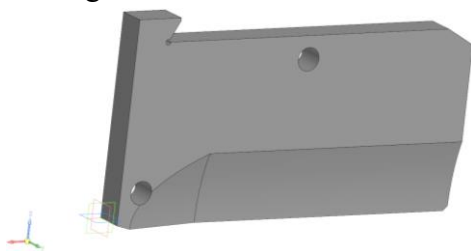


bu yerda $Z_{k1}(\varphi)$ – zoldir prokatlash valogi vintli kalibrining mm o‘lchov birligidagi uzunligi, $T_{dastgoh}(\varphi)$ – dastgoh qadaming mm o‘lchov birligidagi uzunligi.

Prokatlash valoklarining β burchakka burilishini hisobga olgan holda, valok markazining siljish balandligi quyidagicha aniqlanadi [1]:

$$h_{\beta} = l_{\beta} \cdot \operatorname{tg} \beta \quad (5)$$

bu yerda l_{β} – prokatlash valogining yon tomonidan valokning burilish nuqtasigacha bo‘lgan masofa, β – valokning burilish burchagi $0^{\circ} - 7^{\circ}$ oralig‘ida o‘zgaradi.



5-rasm. Zoldir prokatlash stani yo‘naltiruvchi lineykasining umumiy ko‘rinishi.

Nazariy asoslashlar bo‘yicha, DSt 7520-2015 bo‘yicha diametri 50mm bo‘lgan maydalovchi po‘lat zoldirlarni prokatlash uchun, zoldir prokatlash stani yo‘naltiruvchi lineykasi ishlab chiqildi [8].

Zoldir prokatlash stani valoklari hamda yo‘naltiruvchi lineykalari konstruksiyalarini loyihalash asosida, standart talablarga mos bo‘lgan diametrdagi zoldirlarni prokatlash imkoniyatlari yaratildi (5-rasm).

Xulosa. Zoldir prokatlash stanlarida qo‘llaniladigan prokatlash valoklari va yo‘naltiruvchi lineyklarining asosiy geometrik parametrlarini nazariy asoslash va ularni loyihalash maqsadida matematik ifodalarni ishlab chiqildi. Aniqlangan matematik ifodalarning yechimlarini MathCAD 15 dasturida tahlil qilindi va zaruriy grafiklar olindi. Hisoblash ishlari asosida, KOMPAS 3d dasturi yordamida diametri 50 mm bo‘lgan maydalovchi po‘lat zoldirlarni prokatlash valoklari va yo‘naltiruvchi lineyklarining konstruksiyalari ishlab chiqildi.

Foydalanilgan adabiyotlar

1. Целиков А.И., Барбарич М.В., Васильчиков М.В., Грановский С.П., Жукевич-Стоша Е.А. Специальные прокатные станы. // –М.: Металлургия, 1971. – 336 с.
2. Котенок В.И. Развитие теории формообразования профилей винтовых калибрах и создание высокоэффективных процессов и оборудования для прокатки деталей машин: Дис. ... д-ра техн. наук. : 05.03.05 / Котенок Владимир Иванович — Москва, 2005. – 342 с.
3. Фастыковский А.Р., Савельев А.Н. Конструкции и расчеты оборудования прокатных клетей сортовых и листовых станов: учеб. пособие / Сиб. гос. индуст ун-т. – Новокузнецк, 2008. – 316 с.
4. Перетятко В.П., Климов А.С., Филиппова М.Ф. Калибровка валков шаропркатного стана. “Известия высших учебных заведений. Чёрная металлургия”, Том 56, № 6, 2013, стр. 16-20.
5. Филиппова М.В. Математическое моделирование прокатки шаров / М.В. Филиппова, М.В. Темлянцев, В.Н. Перетятко, Е.Е. Прудский // Изв. Вуз. Черная металлургия. – 2017. – Т.60. - №7. – стр. 516-521.
6. Shaxobutdinov R.E., Karimova A.R., Nosirov T.N. Import o‘rnini bosuvchi mahsulot – maydalovchi po‘lat zoldirlarni ishlab chiqarishni o‘zlashtirish masalalari. “Im-fan va innovatsion rivojlanish” ilmiy-texnikaviy jurnal 7-jild / 3, 2024, 36-44 b.
7. Шахобутдинов Р.Э. Теоретические и прикладные основы кулачковых механизмов, применяемых в шаропркатном производстве. Монография / Ташкент, 2024. – 152 с.
8. Межгосударственный стандарт ГОСТ 7524-2015 «Шары, мелющие стальные для шаровых мельниц» Технические условия. Издание официальное. // Москва, Стандартинформ, 2016.



ANTENNANI QAYTA SOZLASHDA P-I-N DIODLARDAN FOYDALANISH, NAZARIY VA AMALIY QO'LLANISHLAR

B.O.Djalilov
Raqamli texnologiyalar markazi direktori,
"Telekommunikatsiya injiniringi"
kafedrası dotsenti.

A.G'.Muhammadjonov
TATU Farg'ona filiali "Dasturiy injiniring"
kafedrası assistenti.
m.azamatjon0212@gmail.

Annotatsiya: P-i-n diodlar yordamida antennalarni qayta sozlash texnologiyasi radioelektron va mikroto'lqinli tizimlarda antennalarning dinamik xususiyatlarini o'zgartirish uchun samarali usuldir. P-i-n diodlarning elektr fazasi va sig'im-induktiv xususiyatlarini nazorat qilish orqali antennaga tushayotgan yoki tarqalayotgan elektromagnit to'lqinlarning moslashuvchanligi ta'minlanadi. Bu usul antennalarning keng polosali diapazonlarini dinamik boshqarishga, shuningdek, garmonik filtrlash va fazali massivlar yaratish imkoniyatini beradi. P-i-n diodlardan foydalanish texnologiyasi yuqori tezlikdagi jo'natish va qabul qilish tizimlarini optimallashtirishda muhim ahamiyat kasb etadi. Tadqiqotlar shuni ko'rsatmoqdaki, antennalarni qayta sozlash orqali yuqori samaradorlikka erishish, signal yoyilishining moslashuvchanligi va chastota doiralarini kengaytirish mumkin. Mazkur usul kommunikatsiya, radiolokatsiya va simsiz aloqa sohalarida yangilik yaratish imkoniyatini ochib beradi.

Kalit so'zlar: Antenna, diodlar, texnologiya, simsiz aloqa, kommunikatsiya.

Kirish. Zamonaviy radioelektron, mikroto'lqinli tizimlarda antennalarning samaradorligi va moslashuvchanligi juda muhim ahamiyatga ega. Radioaloqa, radiolokatsiya, simsiz tarmoqlarda yuqori sifatli signal uzatish va qabul qilishga bo'lgan talab kun sayin ortib borayotgani sababli, antennalarning dinamik sozlanishiga ehtiyoj yuqori hisoblanadi. Bu jarayonda p-i-n diodlar muhim rol o'ynaydi, chunki ular elektromagnit to'lqinlar diapazonini avtomatik ravishda o'zgartirish va dinamik nazorat qilish imkonini beradi.

P-i-n diodlar o'zlarining maxsus elektr-kimyoviy tuzilishi tufayli induktiv va sig'imli xususiyatlarni o'zgartira oladi, bu esa antennalarning qo'llash diapazonini kengaytirish va ularning moslashuvchanligini oshirishga yordam beradi. Hozirgi kunda p-i-n diodlar asosida antennalarni qayta sozlash nafaqat signallarni uzatish sifatini oshiradi, balki foydalaniladigan chastotalarni kengaytirish,

signalga halaqit qiluvchi elementlarni kamaytirish va fazali antenna massivlarini optimallashtirish imkonini beradi. Mazkur texnologiyaning dolzarbligi radio to'lqinlarni boshqarish imkoniyatlarini kengaytirish va yangicha aloqa tizimlarini yaratish bilan bog'liq hisoblanadi. P-i-n diodlarning tezkor va aniq boshqarish xususiyatlari sababli, ular antennalarning qayta sozlanishiga zamonaviy yechim sifatida ko'riladi.

Adabiyotlar tahlili va metodlar.

Antennalarni qayta sozlash sohasidagi tadqiqotlar va texnologiyalar keng qamrovli bo'lib, turli usul va elementlardan foydalanish orqali antennalarni moslashtirishga yo'naltirilgan. P-i-n diodlar yordamida qayta sozlanuvchi antennalar bo'yicha ilmiy tadqiqotlar uzoq vaqtdan beri davom etib keladi va bu diodlarning yuqori tezlikdagi kommutatsiya xususiyati ularni antennalarni dinamik sozlashda keng qo'llanilishini ta'minlamoqda.



Klassik tadqiqotlarda p-i-n diodlar asosan mikroto'qimli sxemalarda signalni bloklash yoki o'tkazish vazifasini bajargan (Johnson, 1999). Keyinchalik p-i-n diodlar fazali antenna massivlarini qayta sozlash va signallar fazasini boshqarish uchun ham qo'llanila boshlandi (Gupta, 2005). Shu bilan birga, Qosimov (2011) hamkasblari bilan olib borgan tadqiqotlari antennalarni dinamik sozlash imkoniyatlarini tadqiq qilib, diapazon kengligi va samaradorligini oshirishni ko'rsatdi.

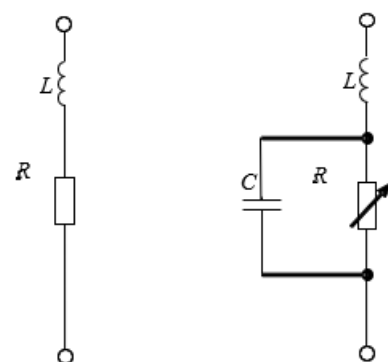
Oliyov (2017) o'z tadqiqotida p-i-n diodlar yordamida qayta sozlanuvchi antennalarning to'qinlarni qabul qilish xususiyatlarini tahlil qildi va bu usulning kommunikatsiya tizimlaridagi samaradorligini oshirishini ta'kidladi. Boshqa tadqiqotlar esa p-i-n diodlar asosida antennalarning garmonik filtrlash xususiyatlariga bag'ishlangan bo'lib, ular interferensiyani kamaytirishda muvaffaqiyatli qo'llanilishi mumkinligini ko'rsatiladi (Kang, 2019).

Natija: PIN-diod elektron (n) va teshik (p) o'tkazuvchanlik sohalari o'rtasida o'z ichki (legirlanmagan, inglizcha intrinsic) yarim o'tkazgich (i-soha) joylashgan diodning bir turi hisoblanadi. p va n sohalar odatda kuchli legirlanadi, chunki ular metall bilan omik kontakt uchun ishlatiladi. p-i-n diodning o'ziga xos xususiyatlari i-soha kuchli legirlangan n+ va p+ sohalardan zaryad tashuvchilar bilan to'ldirilganda kuchli in'eksiya rejimida ishlashida namoyon bo'ladi, bunda ularga to'g'ri siljitish kuchlanishi qo'yiladi. i-sohada zaryad tashuvchilarning konsentratsiyasi juda past bo'lganligi sababli, bu yerda in'eksiya paytida deyarli hech qanday rekombinatsiyalanish jarayonlari bo'lib o'tmaydi. Ammo to'g'ri siljitish rejimida zaryad tashuvchilarning konsentra-siyasi ichki konsentratsiyadan bir necha marta yuqori bo'ladi.

Past chastotalarda o'sha bir xil tenglamalar oddiy diodlarda bo'lganidek, p-i-n diodlariga ham amal qiladi. Yuqori chastotalarda to'g'ri siljitishda p-i-n diod deyarli ideal rezistor kabi ishlaydi, uning volt-amper xarakteristikasi (VAX) hatto juda katta kuchlanishlar qiymatlarida ham chiziqli bo'ladi.

Shunday qilib, siljitish kuchlanishini o'zgartirish bilan diodning qarshiligini 0,1 Omdan 10 KOMgacha keng diapazonda o'zgar-tirish mumkin. i-sohaning katta kengligi p-i-n diodning teskari yo'nalishda kichik sig'imga ega ekanligini ham anglatadi.

Bu ishda qayta sozlash elementlari sifatida Hawlett Packard kompani-yasining HSMP4820 turdagi ikkita p-i-n diodlari ishlatilgan [37]. 1-rasmda diodlarning ochiq holatda (a) va yopiq holatdagi (b) ekvivalent zan-jirlari keltirilgan. Ekvivalent sxema parametrlarining qiymatlari 1-jadvalda keltirilgan.



1-rasm. Diodning (a) ochiq holatda va (b) yopiq holatdagi ekvivalent sxemalari.

1-jadval. p-i-n diod elementlarining qiymatlari

Parametr	p-i-n diod holati	
	Ochiq	Yopiq
	Qiymat	
L , nГH	0.75	0.75
C , пФ	-	0.8
R_s , Ом	0.6	2500

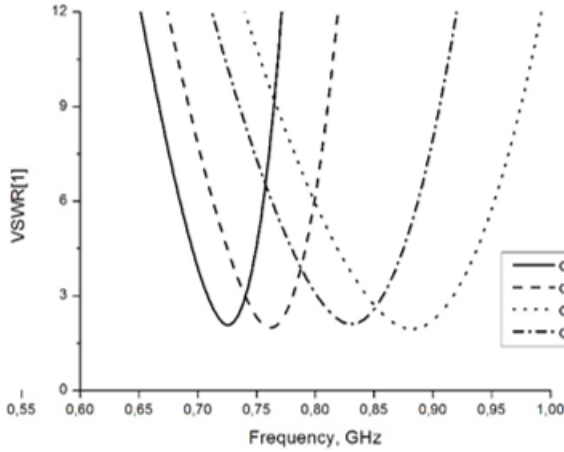
2-jadval. Qayta sozlashda diodlarning holatlari

Egri chiziq (4-rasm)	Diodlarning holatlari	
	1-diod	2-diod
1	Ochiq	Ochiq
2	Yopiq	Ochiq
3	Ochiq	Ochiq
4	Yopiq	Yopiq

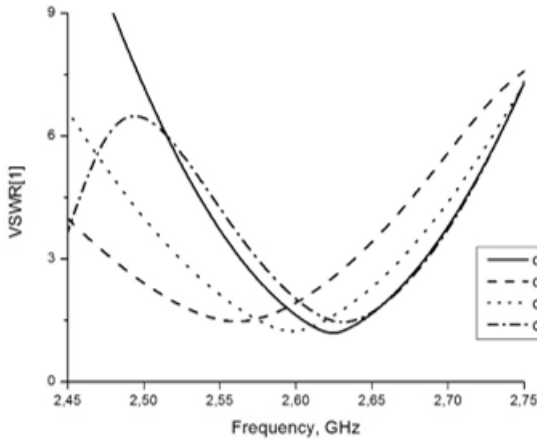


Past chastotali diapazonlarni qayta ulash uchun 11 pF (1-diod) va 15 pF (2-diod) kondensatorlari bilan ketma-ket ulangan ikkita p-i-n diodlar ishlatiladi.

Antenna KTTKni chastotaga bog‘liqligi 2-rasmda keltirilgan. 2-rasmdagi egri chiziq-larga mos keladigan sozlamalardagi diodlarning ho-latlari 2-jadvalda berilgan.



a)



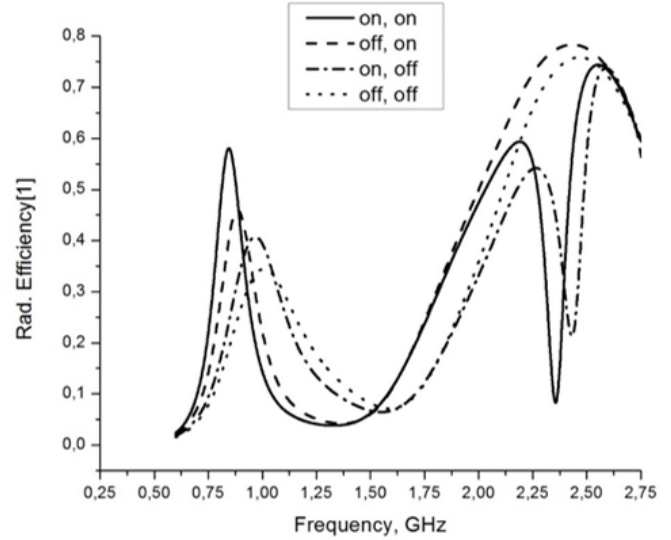
b)

2-rasm. Turg‘un to‘lqin koefitsiyentining (a) past chastotalar diapazoni va (b) yuqori chastotalar diapazonidagi bog‘liqligi.

Past chastotalar diapazonidagi polosa kengligi 12...19,4%ni, yuqori chastotalar diapazonida - 12,2%ni tashkil etadi, bu LTE standartiga mos keladi.

p-i-n diodli zanjirda olingan FIK qiymatlari 3-rasmda keltirilgan. Antennaning foydali ish koefitsenti PCH sohada 36...60% dan YUCH sohada

78% gacha oshish bilan ortadi (alohida egri chiziq-lar uchun diodlarning holatlari 2-jadvalga mos keladi).



3-rasm. Antenna foydali ish koefitsiyentining bog‘liqligi.

Past chastotalar diapazonida qayta sozlanadigan antennaning yo‘naltirilganlik diagrammasi 4-rasmda tasvirlangan.

3-jadvalda PCH va YUCH diapazonlari uchun antenna yo‘naltirilganlik diagrammalarining mos qiymatlari keltirilgan.

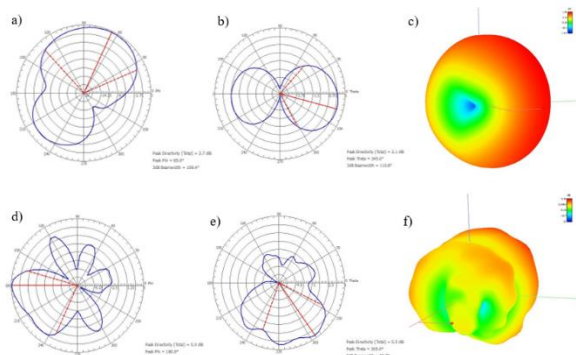
3-jadval

Antenna yo‘naltirilganlik diagrammasining xarakteristikalari

Parametrlar	azimutal burchak		Ko‘tarilish burchagi	
	PCH diapazon	YUCH diapazon	PCH diapazon	YUCH diapazon
Maksimal yo‘naltirilganlik, dB	2.7	5	2.1	5.5
Maksimal burchak, grad	65	180	345	305
Diagrammaning kengligi, grad	109.4	81.7	110.8	82.5



P-i-n diodlar yordamida olib borilgan tadqiqotlar natijalari doimo tahlil qilinib kerakli xulosalarga kelinadi. Antennalarni qayta sozlash sohasidagi tadqiqotlar va texnologiyalar keng qamrovli bo'lib, barcha natija va metodlar yordamida kerakli xulosalarga kelish zarur hisoblanadi.



4-rasm. PCH va YUCH diapazonlaridagi 2D va 3D antenalar yo'naltirilganlik diagrammalari.

- PCH-diapazon azimutal burchagi,
- PCH-diapazon ko'tarilish burchagi,
- PCH-diapazon uch o'lchovli ko'rinishdagi yo'naltirilganlik diagrammasi,
- YUCH diapazonining azimutal burchagi,
- YUCH-diapazon ko'tarilish burchagi,
- YUCH-diapazon uch o'lchovli ko'rinishdagi yo'naltirilganlik diagrammasi

Xulosa. P-i-n diodlar yordamida antennalarni qayta sozlash texnologiyasi radio va mikroto'lqinli tizimlar uchun yuqori samaradorlik va moslashuvchanlikni ta'minlaydi. Tadqiqot davomida p-i-n diodlarning antennalarni qayta sozlashdagi fazaviy, sig'imli xususiyatlari har tomonlama o'rganildi va ularning elektr moslashuvchanligi orqali antennalarning diapazonlarini dinamik tarzda o'zgartirish imkoniyati mavjudligi tasdiqlandi. Bu jarayon antennalarning o'tkazuvchanlik va qabul qilish xususiyatlarini optimallashtirishda muhim rol o'ynadi.

Simulyatsiya va tajribalar natijalari shundan dalolat beradiki, p-i-n diodlar asosida qayta sozlanuvchi antenalar yuqori tezlikdagi signal almashinuvida interferensiyani kamaytiradi, garmonik

filtrlash orqali diapazonni kengaytirish imkonini beradi va fazali massivlarni boshqarishda aniqlikni oshiradi. Tadqiqotning amaliy qo'llaniluvchi samsiz aloqa, radiolokatsiya, fazaviy antenalar va yuqori tezlikdagi ma'lumot uzatish tizimlarini optimallashtirishga imkon beradi. Shu bilan birga, qayta sozlanuvchi antennalarning p-i-n diodlar yordamida tezkor va samarali boshqarilishi yuqori samaradorlikka erishishning uzviy qismi sifatida qaraldi.

Yakuniy natijalar shundan dalolat beradiki, antennalarni qayta sozlash texnologiyalari kelajakda radio va mikroto'lqinli aloqa sohasidagi innovatsiyalar uchun yangi imkoniyatlar eshigini ochib beradi.

Foydalanilgan adabiyotlar ro'yhati.

- Johnson, R. C. (1999). "Microwave PIN Diodes: Application in Switching and Tuning Circuits." *Microwave Journal*, 42(12), 22-30.
- Gupta, K. C., & Singh, A. (2005). "Smart Antennas and Their Applications." *IEEE Transactions on Antennas and Propagation*, 53(5), 1625-1635.
- Қосимов, А. Ж. (2011). "Антенналарнинг қайта созланиши: p-i-n диодлардан фойдаланиш имкониятлари." *Техника ва Инновация*, 23(7), 45-51.
- Kang, S. H. (2019). "Harmonic Filtering in Reconfigurable Antennas Using PIN Diodes." *Journal of Electromagnetic Waves and Applications*, 33(18), 2341-2352.
- Олийнов, И. Х. (2017). "Қайта созланувчи антенналар ва уларнинг фазавий бошқаруви." *Микротўлқинли техника журнали*, 55(3), 79-85.



HONEYPOT TEXNOLOGIYASINING FUNKSIONAL IMKONIYATLARINI TADQIQ ETISH

Xudoyqulov Zarif Turaqulovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti, "Kriptologiya" kafedrasini
mudiri, Toshkent, O'zbekiston
e-mail zarif.khudoykulov@tuit.uz

Qurbonaliyeva Dilshoda Vali qizi,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti, "Kriptologiya" kafedrasini
assistenti, Toshkent, O'zbekiston
e-mail dilshodavaliyevna@gmail.com

Bozorov Suhrobjon Mumin o'g'li,

Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti, "Kriptologiya" kafedrasini
assistenti, Toshkent, O'zbekiston
e-mail mr.bozorov95@gmail.com

Annotatsiya: Honeypot - spam, fishing, DDoS yoki boshqa zararli usullardan foydalangan holda kompyuter tarmoqlariga hujum qilishga urinayotgan zararli hujumchilarni yolg'on zaifliklar orqali jalb qilish uchun yaratilgan tuzoq sifatidagi kompyuter tizimi yoki ilovasi. Xaker ushbu tuzoqqa tushib qolsa, honeypot tizimi administratorlarga tajovuzkorning turi, u amalga oshirayotgan harakatlar va ko'p hollarda hujumchini aniqlash haqidagi qimmatli ma'lumotlarni olish imkonini beradi. Ushbu maqolada Honeypot vositalarining funksional imkoniyatlari va algoritmlarining tahlili amalga oshirilgan. Olingan natijalar asosida tarmoqdagi hujumchilarning hatti-harakatlarini aniqlovchi va haqiqiy tizimni hujumlardan himoya qila oluvchi yordamchi dasturlarning qiyosiy tahlili keltirilgan.

Kalit so'zlar: Honeypot server, honeypotlar klassifikatsiyasi, virtual honeypot, fizik honeypot, honeynet, hujum, xaker harakatlari, zaiflik, monitoring, DMZ.

Kirish. Kiber tahdidlarning kompyuter tarmoqlariga ta'sirining jiddiyligiga ko'ra, tarmoq himoyachilari noma'lum tahdidlarni aniqlash va tahlil qilish va xavfli tahdidlarni oldini olish uchun vositalarni ishlab chiqishga harakat qilishadi. Tahdidlarni kuzatish tizimlari, xavfsizlik devorlari, IPsec va bosqinlarni aniqlash tizimlari (IDS) kabi hujumlarni aniqlash va oldini olish uchun turli xil xavfsizlik mexanizmlari ishlab chiqilgan bo'lsa-da, ular birinchidan nol kunlik va noma'lum tahdidlarni aniqlash uchun yetarlicha samarali emas. Ikkinchidan raqibning hatti-harakatlarini yaqindan tahlil qilishning imkoni yo'q. Biroq, honeypotlar tarmoq himoyachisiga

ikkala yuqorida aytib o'tilgan maqsadga erishishga yordam beradigan aldamchi vositadir.

Adabiyotlar tahlili va metodologiya.

Kiberxavfsizlik dunyosida honeypot tushunchasi odatda tizimning haqiqiy hatti-harakatlariga ega bo'lgan, qasddan xavfsizlik bo'shlig'ini qoldiradigan va ularga kirishni istagan kiber jinoyatchilar haqida ma'lumot to'plashni maqsad qilgan tuzoq tizimlari deb ataladi [1]. Bu zaifliklar orqali kiberhujumlarni jalb qilishni maqsad qilib qo'ygan kompyuter tizimi. U kiberhujumchilar kabi nishonga taqlid qilish va hujumga urinishlar, ishlash usullari haqida bilish yoki ularni boshqa nishonlardan chalg'itish uchun ishlatiladi [2].

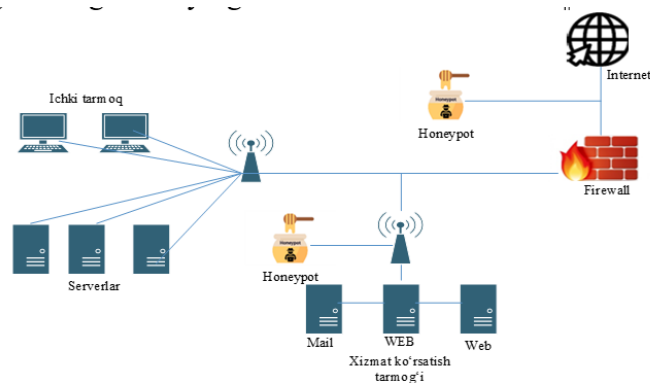


Barcha honeypotlarning asosiy maqsadi har xil turdagi dasturiy ta'minotga qarshi paydo bo'ladigan hujumlarni aniqlash va razvedka ma'lumotlarini tahlil qilish va yaratish uchun hisobotlarni to'plashdan iborat. Yig'ilgan hisobotlardan keyinchalik tarmoq tahdidlariga qarshi profilaktika usullarini yaratishda foydalaniladi [3]. Yuqorida aytib o'tilganidek, honeypot tuzoq tizimidir [4]. Ushbu tuzoq tizimlari ko'pincha tarmoqqa ulangan virtual mashina yoki bulut serverida o'rnatiladi. Shu bilan birga tizim va tarmoq ishtirokchilari tomonidan izolyatsiya qilingan bo'lib, qat'iy nazorat qilinadi [5]. Hujumchilarning e'tiboriga tushish uchun, honeypot maqsadli himoyasiz bo'lishi zarur. Shu holatda uning zaif tomonlarini tajovuzkor aniqlaydi va ulardan foydalanishga harakat qiladi [6]. Ushbu zaifliklar ilova ichidagi xavfsizlik tizimining bir qismi bo'lishi mumkin. Keraksiz ochiq portlar, eskirgan dasturiy ta'minot versiyalari, zaif parol yoki eskirgan yadro kabilar ham tizim zaifliklaridan biri bo'lishi mumkin [7].

Honeypot tavsifi. Honeypotlar ma'lum replikatsiya vektorlari va zararli dastur hujumlari signaturalaridan foydalanish orqali zararli dasturlarni aniqlash uchun ishlatiladi. USB xotira yoki flesh-disklar kabi replikatsiya vektorlaridagi o'zgarish belgilarini qo'lda yoki drayverlardan nusxa oluvchi maxsus honeypotlar yordamida osongina tekshirish mumkin.

Hujumchi o'zining zaif nishonini topgandan so'ng, u tizim yoki ilova ustidan ma'lum nazoratni qo'lga kiritmaguncha hujumni boshlashga va imtiyozlarni oshirishga harakat qiladi. Xakerlarning ko'pchiligi bilmaydigan narsa shundaki, honeypot ma'muri ularning har bir qadamini diqqat bilan kuzatib, hujumchidan joriy xavfsizlik siyosatini kuchaytirishga yordam beradigan ma'lumotlarni to'playdi. Shuningdek, administrator, hodisa haqida darhol yuridik organlarga xabar berishi mumkin bo'lib, bu ko'pincha yuqori darajadagi korporativ tarmoqlarda sodir bo'ladi. Aksariyat honeypotlar hujumchilarni haqiqiy tarmoqlarda joylashgan muhim ma'lumotlardan chalg'itadigan tuzoq sifatida ishlaydi.

Yana bir umumiy jihat shundaki, honeypotga ulanishning deyarli barcha urinishlari dushman deb hisoblanishi mumkin, chunki, odatda qonuniy foydalanuvchini ushbu turdagi tizimlar bilan bog'lanishga undaydigan sabablar kam bo'ladi.



1-rasm. Honeypot arxitekturasi.

Honeypotni yaratilishida e'tibor qaratish lozim bo'lgan muhim jihatlardan biri - ma'mur qanday qilib hujumchiga xakerlik qilish qiyin bo'lishini bilishi kerak. Agar honeypotni buzish juda oson bo'lsa ya'ni himoya qismiga e'tibor berilmasa, buzg'unchi yoki Xakerlar qiziqishlarini yo'qotishlari, hatto haqiqiy ishlab chiqarish tizimi bilan shug'ullanmayotganliklarini tushunishlari ham mumkin. Bunday holda honeypot o'z vazifasini bajara olmaydi. Boshqa tomondan, agar tizim juda kuchli himoyalangan bo'lsa, har qanday hujumlarni to'xtatish va hech qanday ma'lumot to'play olmaslik holati yuzaga keladi. Shunday qilib, qiyinchilik nuqtai nazaridan, hujumchilarni osonlik va qiyinchilik o'rtasidagi muvozanatni saqlagan holda jalb qilish haqiqiy vaziyatni simulyatsiya qilish uchun eng yaxshi kafolat bo'ladi.

Honeypotning afzalliklari va kamchiliklari.

Quyida honeypotlarning asosiy afzalliklari keltirilgan [8].

Yig'iladigan ma'lumotlar. Honeypotning qiymati uning hujumchilarning usullari va hatti-harakatlari haqida to'plagan ma'lumotlari, tajovuzkor esa uni kuzatib borilmayotganiga ishonishiga bog'liq. Boshqa tarmoq monitoringi vositalari, masalan, hujumlarni aniqlash tizimlari (IDS) honeypot kabi bir



xil darajadagi ma'lumotni taqdim etmaydi. Misol uchun, IDS shubhali faoliyatni aniqlash, ogohlantirishlarni yuborish va buzg'unchilarni imkon qadar tezroq to'xtatish uchun tarmoqlarni kuzatib boradi. IDS buzg'unchilar haqida ma'lumot to'plash va tahlil qilishiga qaramasdan, bu uning asosiy vazifasi emas.

Hujum modellarini aniqlash. Xavfsizlik bo'yicha tadqiqotchilar, sotuvchilar, korxonalar va boshqa tashkilotlar honeypotdan to'plangan ma'lumotlardan kiberhujumlarning senariylarini aniqlash uchun foydalanishlari va keyin hujumlarga qarshi turish uchun o'z mahsulotlari va strategiyalarini moslashtirishlari mumkin.

Tuzatish kerak bo'lgan zaifliklar. Korxonalar tarmoqni qidirish va himoyalash hamda bartaraf etilishi kerak bo'lgan zaifliklarni aniqlash uchun "honeypot" dan foydalanishi mumkin.

Yuqoridagi afzalliklar bilan birga Honeypotning foydalanuvchilari bilishi kerak bo'lgan kamchiliklari ham bor:

Honeypot xakerlar tomonidan buziladi. Honeypot to'g'ri o'rnatilishi kerak. Tajribali xakerlar noto'g'ri sozlangan honeypotda bo'lganligini bilib, tarmoq ma'muriga yolg'on ma'lumot berish uchun uni to'xtatib qo'yishi mumkin. Masalan, tizimni honeypot sifatida aniqlagan tajovuzkor administratorning e'tiborini xizmat ko'rsatish tizimida sodir bo'layotgan haqiqiy zararli hujumdan chalg'itish uchun yolg'on tizimda harakat qilishi mumkin.

Xizmat ko'rsatish tarmog'iga kirish. Honeypot DMZda bo'lsa-da, ular bir nuqtada ichki tarmoqqa ulanadi; malakali xaker ichki tarmoqqa kirish nuqtasi sifatida noto'g'ri sozlangan "honeypot" dan foydalanishi mumkin.

Zararli honeypotlarni joylashtirish. Xakerlar o'zlarining honeypotlarini ham yaratishlari mumkin. Soxta veb-sayt yaratadigan yoki Wi-Fi tarmog'ini aldaydigan va trafikni kuzatadigan xaker mohiyatan honeypotdan foydalanadi.

Ishlash prinsipi. Honeypotning ishlash prinsipi quyidagilardan iborat:

- *Sozlash*
- *Jalb qilish*
- *Monitoring*
- *Ma'lumotlarni yig'ish*
- *Tahlil:*
- *Ogohlantirish*

Honeypot *sozlashning* dastlabki bosqichida haqiqiy tizim yoki xizmatga o'xshash qilib tayyorlanadi. Tizim talabidan kelib chiqib, Linux Operatsion Tizimi (Ubuntu, Debian, CentOS) va dasturlar (Python, Git, pip) o'rnatiladi. Internet orqali kerakli paketlar yuklab olinadi, konfiguratsiya fallari tahrirlangandan so'ng honeypot ishga tushiriladi. Shu bilan birga Honeypotni izolyatsiya qilish uchun firewall texnologiyasi bilan birga, shubhali faoliyat aniqlanganda ogohlantirish berishi uchun Alert tizimlarini ham o'rnatish yuqori va o'rta darajali honeypotlarda tizim konfidensial ma'lumotlari xavfsizligini ta'minlaydi. Honeypot samarali ishlashi uchun sozlash jarayonining har bir bosqichga e'tibor qaratish zarur.

Hujumchilarni *jalb qilish* bosqichida Honeypot konfiguratsiyasida ma'lum zaifliklar yoki ochiq portlar kiberhujumchilarni e'tiborini tortish uchun qo'shiladi. U haqiqiy xizmatlarning hatti-harakatlarini taqlid qilib, qiziqarli ko'rinishga ega bo'ladi. Masalan Kippo asosan SSH (22-port) da ishlaydi. Hujumchilarni jalb qilish uchun esa boshqa portlarni (2222-port bo'lishi mumkin) ochiq qilib qo'yish mumkin. Va bu ochiq portlarda zaif lekin haqiqiy xizmatlar joylashtiriladi. Bundan tashqari, tizimda kuchsiz parollarni simulyatsiya qilish yoki mavjud bo'lgan foydalanuvchilar ro'yhatini yaratish va ularga zaif parollarni sozlash ham Xakerlarni jalb qilishi mumkin. Bularning asosi esa Honeypotning internetga bog'langanligi. Honeypotga simulyatsiya qilingan tizimning internet manbalaridagi reklamalar ijtimoiy tarmoqlarda qiziquvchilar sonining ortishiga sabab bo'ladi. SSH dan tashqari boshqa protokollarni (masalan, FTP yoki HTTP) ham simulyatsiya qilish mumkin. Bu ham yanada ko'proq hujumchilarni jalb qiladi.



Bundan tashqari honeypotga samarali jalb qilish uchun to'g'ri sozlash, ochiq portlarni tashkil etish va hujumchilarni qiziqtiradigan muhit yaratish zarur. Ushbu tavsiyalarni amalga oshirish orqali hujumchilarning harakatlarini yaxshiroq tushunish imkoniyatiga ega bo'linadi.

Monitoring bosqichida hujumchilar honeypot bilan o'zaro aloqaga kirganda, ularning harakatlari kuzatiladi va yozib olinadi. Bu quyidagilarni o'z ichiga oladi:

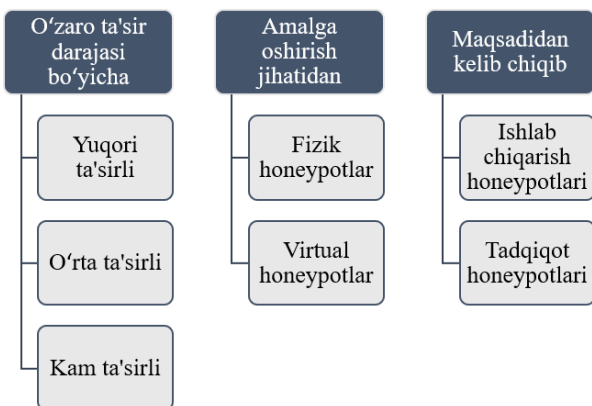
- Hujumchilarning IP manzillari
- Qanday hujumlar amalga oshirilgan
- Ishlatilgan vositalar va usullar

Ma'lumotlarni yig'ish: Har bir o'zaro aloqa yoziladi va bu qimmatli ma'lumotlar tahlil uchun xizmat qiladi. Bu ma'lumotlar kiberhujumchilarning hatti-harakatlarini va strategiyalarini aniqlashda yordam beradi.

Tahlil: Yig'ilgan ma'lumotlar tahlil qilinadi, bu esa kiberxavfsizlik choralarini yaxshilashga yordam beradi. Bu tashkilotlarga yangi tahdidlarni tushunishga yordam beradi.

Ogohlantirish: Ko'pgina honeypotlar shubhali faoliyat aniqlanganda xavfsizlik jamoasini tezkor xabardor qilish tizimlariga ega. Tizim xavfsizlik hodimlarining o'z vaqtida hujumlardan habardor bo'lishi ularning oqibatlarini bartaraf etish bilan birga, moddiy va boshqa turdagi yo'qotishlarga qarshi chora hisoblaniladi.

Klassifikatsiyalanishi.



2-rasm. Honeypotlar klassifikatsiyasi

Yuqori ta'sirli honeypotlar. Ular OTning barcha jihatlarini simulyatsiya qiluvchi haqiqiy tizimlardir. Ular yuqori xavf ostida bo'lishi mumkin.

O'rta ta'sirli honeypotlar. O'rta ta'sirli honeypotlarda simulyatsiya yuqori darajada bo'lmaydi. Haqiqiy ma'lumotlar xavfsizligi yetarli darajada ta'minlangan bo'ladi.

Kam ta'sirli honeypotlar. Bu turdagi honeypotlar tizimning ba'zi jihatlarini simulyatsiya qiladi. Ularni joylashtirish oson, xavf darajasi juda past bo'ladi. Ular uchun cheklangan ma'lumotlardan foydalaniladi.

Fizik honeypotlar. Ular haqiqiy mashinalar bo'lib, fizik honeypotlarga shaxsiy IP manzil beriladi. Odatda tarmoqda Firewall texnologiyalari bilan ketma ketlikda qo'llaniladi.

Virtual honeypotlar. Bu turdagi honeypotlar boshqa mashinalar tomonidan simulyatsiya qilinadi. Honeypotga yuborilgan tarmoq trafigiga javob qaytariladi. Bir vaqtning o'zida bir nechta mashinalarni o'rganishi mumkin.

Ishlab chiqarish honeypotlari. Bu xususiy va davlat muassasalari, kompaniyalar va korporatsiyalar tomonidan Internetdagi tarmoqlarga hujum qilishga intilayotgan Xakerlarning hatti-harakatlari va usullarini tekshirish uchun foydalaniladi.

Tadqiqot honeypotlari. Bu turdagi tuzoqlar universitetlar, kollejlarda, maktablar va boshqa tegishli muassasalarda ishlaydigan dasturchilar, tizim ma'murlari va loyiha jamoalarining menejerlari tomonidan qo'llaniladi.

Natijalar. Maqsadi va qo'llanilishi bo'yicha, hamda, tizimga va konfidensial ma'lumotlarga raqibning ta'sir doirasidan kelib chiqib honeypotlarning to'liq tavsifi quyidagi jadvallarda keltirilgan.

1-jadval. Foydalanish maqsadiga ko'ra

Tavsifi	Honeypot (xizmat ko'rsatish)	Honeypot (tadqiqot)
Asosiy tavsiflar (ta'rif)	Odatda, tashkilot xavfsizlikni yaxshilash uchun	U turli tarmoqlarda blackhatni



	uni boshqa xizmat ko'rsatish serverlari bilan birga xizmat ko'rsatish tarmog'ida joylashtiradi.	nishonga olish sabablari va taktikasi haqida ma'lumot to'plash uchun ishlatiladi.
Ilova maydonlari	Ulardan foydalanish oson va asosan korporatsiyalar tomonidan qo'llaniladi.	Asosan harbiy, davlat tashkilotlari va tadqiqot maqsadlarida foydalaniladi.
O'zaro ta'sir darajasi	Bular o'zaro ta'siri past bo'lgan honeypotlar bo'lib, ular tadqiqot honeypotlariga qaraganda kamroq ma'lumot beradi.	Ular odatda xakerlarning harakatlarini sinchkovlik bilan tahlil qilish va shunga mos ravishda tizimni himoya qilish uchun ishlatiladi.
Xavf darajasi	Bu tajovuzkorlar tomonidan tashkilot resurslarini yo'qotishning yuqori xavfi bilan bog'liq.	Bu kamroq xavf bilan bog'liq, chunki u tadqiqot maqsadlari uchun mo'ljallangan.
Axborotni joylashtirish va yig'ish	Ularni joylashtirish va faqat cheklangan ma'lumotlarni yig'ish oson.	Ularni joylashtirish va saqlash qiyin, chunki katta hajmdagi ma'lumotlarni to'playdi.

Yuqoridagi jadvalda Honeypotlarning foydalanish maqsadiga ko'ra turlarining to'liq tavsifi keltirilgan. Unga ko'ra ishlab chiqarish Honeypotlarida risk yuqori. Chunki ular tizimni simulyatsiya qiladi. Katta ma'lumotlar bilan ishlash esa tadqiqot Honeypotlarida ba'zi qiyinchiliklarni keltirib chiqarishi mumkin.

2-jadval: O'zaro ta'siriga ko'ra

Terminlar	Past darajadagi o'zaro ta'sir	Yuqori darajadagi o'zaro ta'sir
Ta'rif	Blackhat tizim bilan o'zaro aloqasi cheklangan va oz vaqt talab etadi, shuning uchun Blackhat tizimga kira olmaydi.	Maksimal darajada "blackhat" dan ma'lumot ola oladi, bu ularga butun tizimga kirishga yoki hatto uni buzishga imkon beradi.
Virtual mashinalar bilan ishlash	Bir nechta virtual mashinalarni bitta jismoniy tizimda osongina joylashtirish mumkin, virtual tizim qisqa javob vaqtiga ega, kamroq kod talab qilinadi, bu tizimning murakkabligini kamaytiradi.	Virtual tizimlarda ishlashi mumkin
Misollar	Honeyd, HoneyBOT va b.	Honeynet va b.
Tahdidlar	Xost tizimiga hujum qilish uchun juda kam zaifliklar mavjud va ba'zida ular allaqachon ma'lum.	Ilgari aniqlanmagan yangi hujumlar va anomaliyalarni aniqlaydi
Xavfsizlik	Tashkiliy nuqtai nazardan xavfsiz va xavfsiz.	Yuqori darajadagi himoya
Amalga oshirish uchun bilim	Past	Yuqori
Xizmat vaqti	Past	Juda yuqori
Rivojlanish bilimlari	Past	Yuqori
Qayta loyihalash va rivojlantirish	Oson	Oson
Texnik xizmat ko'rsatish	Oson bajariladi	Juda qiyin
O'zaro ta'sir	Cheklangan	Keng imkoniyatli
Aniqlash	Tuzoq sifatida oson aniqlanadi	Aniqlash qiyin
Modellashtirish	OTni va unga aloqador xizmatlarni simulyatsiya qiladi	Haqiqiy xizmatlar, ilovalar yoki qurilmalarni simulyatsiya qiladi
Xatarlar ehtimoli	Juda kam	Juda yuqori

2-jadvalda past va yuqori darajadagi o'zaro ta'sirli Honeypotlarning farqlanishi misollar bilan keltirilgan. O'rta ta'sirli Honeypotlarni xususiyatlaridan kelib chiqib past yoki yuqori ta'sirligiga qo'shish mumkin. Past ta'sirli Honeypotlarning eng sodd ko'rinishi dasturiy ilova (HoneyBot) bo'lishi mumkin. Honeynetlar esa ko'p xizmat vaqtini talab etadi va ularga texnik xizmat ko'rsatish juda qiyin. Bunga sabab ularda bir emas bir nechta serverlarni Honeypot sifatida bog'lashdir.

O'zaro ta'sir darajasiga ko'ra o'rnatilgan Honeypotlarni ko'rsatilayotgan xizmatlar, ma'lumotlarning yozib olinishi, qo'llanilish platformalari va ogohlantirish ehtimolliklariga ko'ra o'rganildi va 3,4- jadvallarga natijalar joylashtirildi.



3-jadval: Past o'zaro ta'sirli honeypot (LIH)
dasturi doirasida o'rnatilgan vositalar

Terminlar / Vositalar	Xizmatlar	Log faylga yozish	Platformalar	Ogohlantirish ehtimolligi
KFsensor	Ochiq proksi-serverlarni sinab ko'rish, Dameware, myDoom va blaster qurtlarini aniqlash [3].	Ha	Windows OS	Ro'yxatga olish va xabar berish mexanizmi qo'llaniladi
BackOfficer friendly	HTTP, FTP, Telnet yoki pochta - jami 7 xizmat	Yo'q	Windows OT (windows 95 va windows 98)	Masofaviy ro'yxatga olish, ogohlantirishlar yo'q
Labrea Tarpit	Tarmoqda foydalanilmagan IP manzillarni skanerlash, ularni yozib olish va spam sifatida belgilash orqali avtomatlashtirilgan hujumni to'xtadi.	Ha	Ubuntu	Ro'yxatga olish, shuningdek, bildirishnoma mexanizmi qo'llaniladi
Honeyd	Qurtlar va spamlarga qarshi nusxalash	Ha	Windows va Linux	O'rnatilgan bildirishnoma mexanizmi yo'q
HoneyRJ	Java interfeysi yordamida protokollarni qo'shish bilan kengaytirilishi mumkin.	Ha	Microsoft Windows XP Professional, Java Runtime Environment Version 1.5, Eclipse 3.4	Yuborilgan yoki qabul qilingan har bir paket alohida qatorda qayd etiladi.

4-jadval: Yuqori o'zaro ta'sirli honeypot (HIH)
dasturi doirasida o'rnatilgan vositalar [7]

Terminlar / Vositalar	Xizmatlar	Log faylga yozish	Platformalar	Ogohlantirish ehtimolligi
Mantrap	U asosiy OTning dublikatlarini yaratish uchun ishlatiladigan blokirovkalash xizmatlaridan foydalanadi	Ha	Virtual tizimda ishlaydi	Yaxshi tashkillashtirilgan xabar berish qobiliyati bilan yashirin kuzatuvni ta'minlaydi
Deception toolkit	Noodatiy trafikni blokirovka qilish uchun TCP ning himoyalash xizmatidan foydalanadi	Ha	Linux va Windows	Ogohlantirishlar bilan bir qatorda jurnallardan ham foydalanadi
Sebek	Linux nusxalarida ishlaydi	Ha	OC Linux	Tarmoq darajasida xabardor qiladi
Honeynets	Blackhat vositalari, strategiya va kontseptsiyani to'plash uchun mo'ljallangan.	Ha (Swatch jurnal faylini real vaqtda kuzatib boradi)	Bir vaqtning o'zida bir nechta tizimlardan foydalanadi, masalan, Solaris, Linux, Windows NT, Cisco router, Alteon switch	Kelishilgan nuqta bloklanganligi haqida xabar beradi.

5-jadval. Hujumlar bo'yicha honeypotlar tasnifi [20]

Xizmat turi	Amazon Services	Web	Google cloud	Microsoft Azure
Honeypot				
Dionaea	228075		162570	308102
Gutton	11878		84375	17256
Cowrie	4503		297818	9012
Heralding	1885		12255	3370
Mailoney	720		9419	146
Adbhoney	413		2497	442
Ciscoasa	260		750	134
Honeyppy	172		2149	497

Xulosa sifatida aytish mumkinki dinamik kiberxavfsizlik vositalari sifatida Honeypotlar ko'p hollarda namoyon bo'ladi, ularning turlari har biri o'ziga xos tarzda ajralib turadi va o'ziga xos maqsadlarga xizmat qiladi. Ushbu farqlar ko'pincha turli mezonlardan kelib chiqadi, bu ularning maqsadi, ularni amalga oshirish metodologiyasi yoki ular qarshi turish uchun mo'ljallangan o'ziga xos tahdid landshafti bilan bog'liq. Binobarin, eng mos honeypot turini tanlash muhim qaror bo'lib, bir nechta muhim omillarni diqqat bilan ko'rib chiqqandan keyin qabul qilinishi kerak. Taroziga soladigan birinchi omil tarmoqning hozirgi holatidir. Chunki tarmoq topologiyasini, masshtabini va u joylashgan muhim aktivlarini baholash muhim ahamiyatga ega.

Foydalanilgan adabiyotlar

1. Душода Курбаналиева, 2023. "Тarmoq xujumlarini aniqlash vositalari tahlili". Ж: Информатика и инженерные технологии.
2. A. Javadpour, F. Ja'Fari, T. Taleb and C. Benzaïd, "A Mathematical Model for Analyzing Honeynets and Their Cyber Deception Techniques," 2023 27th International Conference on Engineering of Complex Computer Systems (ICECCS), Toulouse, France, 2023, pp. 81-88, doi: 10.1109/ICECCS59891.2023.00019
3. Pawlick, J., Colbert, E., Zhu, Q., 2018. Modeling and analysis of leaky deception using



signaling games with evidence. *IEEE Trans. Inf. Forensics Secur.* 14 (7), 1871–1886.

4. *Shanto Roy, Nazia Sharmin, Mohammad Sujan Miah, Jaime C Acosta, Christopher Kiekintveld, And Aron Laszka.* Adversarial Reconnaissance Mitigation and Modeling. arXiv:2306.06769v1 [cs.CR].
5. *Lance Spitzner* (2002). Honeypots tracking hackers. Addison-Wesley. pp. 68–70. ISBN 0-321-10895-7.
6. *Katakoglu, Onur* (2017-04-03). "Attacks Landscape in the Dark Side of the Web" (PDF). acm.org. Retrieved 2017-08-09.
7. *Suhrobjon Bozorov, Nozima Akhmedova, Dilshoda Qurbonaliyeva and Kader Gultekin* 2024. "Survey on honeypot: detection, countermeasures and future with ML", AIP Conference Proceedings (ISSN:0094-243X; E-ISSN:1551-7616).



IOT TEXNOLOGIYASIDA BLOKCHEYN ASOSIDA MA'LUMOTLARNI XAVFSIZ ALMASHISHNING TAKOMILLASHGAN USULI

Xudoyqulov Z.T.,

Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti,
PhD, dotsent
zarif.khudoykulov@tuit.uz

Seidullayev M.K.

Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti,
katta o'qituvchi
mr.madiyar95@gmail.com

Annotatsiya: Hozirgi kunga kelib IoT texnologiyasi juda tez rivojlanayotgan texnologiyalarning biri hisoblanadi. IoT texnologiyasi yordamida juda ko'plab ma'lumotlar uzatiladi, qabul qilinadi va qayta ishlanadi. IoT texnologiyasiga qaratilgan kiberhujumlar soni ortib bormoqda, natijada xavfsizlikni ta'minlash dolzarb masallardan biriga aylandi. Ushbu maqalada IoT texnologiyasida qo'llaniladigan protokollar tahlil qilingan. Blokcheyn yordamida IoT ilovalari uchun xavfsiz autentifikatsiya va ma'lumot almashish tizimi arxitekturasi ishlab chiqildi. Taklif etilayotgan tizim ko'p qatlamli arxitektura bo'lib, uchta qatlamdan iborat: qurilma qatlami, boshqaruvchi qatlami va saqlash qatlami. Tizimda autentifikatsiya algoritmi blokcheyn (aqli shartnoma) yordamida algoritmi takomillashtirildi. Ikki to'plam a'zolari o'rtasidagi aloqa xavfsizligini ta'minlash uchun AES simmetrik va Elliptik egri chiziq murakkabligiga asoslangan elektron raqamli imzo algoritmlari yordamida takomillashtirildi.

Kalit so'zlar: Buyumlar Interneti (IoT), REST, CoAP, MQTT, xavfsizlik, Blokcheyn.

I.Kirish

IoT atamasi dastlab Massachusetts texnologiya instituti qoshidagi Auto-ID Labs tadqiqot guruhi xodimi Kevin Eshton tomidan 1999-yilgi taqdimotda RFID texnologiyasini keng qamrovli tatbiq etishda paydo bo'lgan. IoT-bu fizik obyektlar o'rtasida Internet orqali ma'lumotlarni uzatish tarmog'i tushunchasi. Fizik va raqamli muhitlarni o'zaro bog'lash va integratsiyalash orqali aqli shaharlar, aqli uylar va Sanoat 4.0 kabi yangi tizimlarni taqdim etmoqda [1].

IoT texnologiyasining asosiy qurilmalarining hisoblash, quvvat va tarmoq imkoniyatlarini cheklanganligi bois, ularni amaliyotda qo'llashda alohida yondashuvni talab etadi. IoT texnologiyasini amaliyotda qo'llashda quyidagi keltirilgan protokollardan keng qo'llaniladi [2]:

- MQTT;

- CoAP;
- AMQP;
- Rest;
- XMPP;
- Stomp.

IoT texnologiyasida foydalanilgan protokollar REST. REST (Representational State Transfer) tarmoqdagi taqsimlangan dastur komponentlarining o'zaro ta'siri asosida quriladigan tarmoqning bir turi hisoblanadi. REST tarmog'ida asosan ma'lumotlarni almashishda CoAP protokolidan foydalanadi. REST tarmog'iga misol sifatida, agar mijoz X (harorat sensori) bo'lsa, X resursning Y holatini yaratib, uni tarmoq orqali uzatadi [3].

REST tarmog'ining asosiy talablari quyidagilar [3]:

1. Yagona interfeys (Uniform interface). Bitta resurs uchun so'rovning qayerdan kelganidan



qat'i nazar bir xil shaklda bo'lishi. REST tarmog'ida mijoz nomi yoki elektron pochta manzili kabi bir xil ma'lumotlar faqat bitta yagona resurs identifikatoriga (uniform resource identifier, URI) tegishli bo'lishi kerak.

2. Mijoz-server ajratish. REST tarmog'ida mijoz va server ilovalari bir-biridan butunlay mustaqil bo'lishi talab etiladi. Mijoz ilovasi faqatgina so'ralgan resursning URI bilishi kerak, ya'ni server ilovasi bilan aloqada bo'lmasligi kerak. Xuddi shunday server ilovasi ham so'ralgan ma'lumotlarni uzatishdan tashqari mijoz ilovasini o'zgartirmasligi kerak.

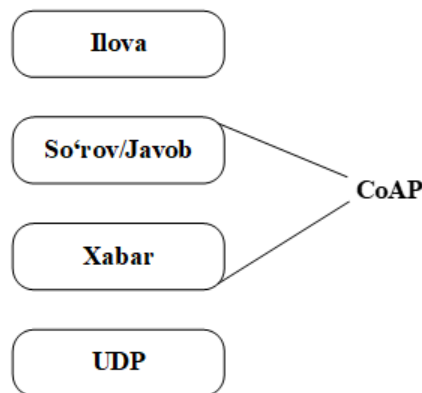
3. Makonsiz (Statelessness). Mijoz va server o'rtasidagi o'zaro aloqa protokoli quyidagi shartning bajarilishini talab qiladi: mijoz so'rovlari orasidagi davrda serverda mijozning holati to'g'risida hech qanday ma'lumot saqlanmaydi. Mijozning har bir so'rovi uni qayta ishlash uchun zarur bo'lgan barcha ma'lumotlarni o'z ichiga olishi kerak. Boshqacha qilib aytganda, REST serveri bu so'rovni boshqa serverga jo'nata olishi kerak.

4. Kesh xotiraga yozish (Cacheable). Internet tarmog'ida bo'lgani kabi, REST tarmog'ida ham mijoz serverdan kelgan javoblarni kesh xotirga saqlashi mumkin. Server javoblarida mijozlar javoblarni kesh xotiraga saqlashi mumkin yoki mumkin emasligi haqidagi ma'lumotlarni ham o'z ichiga olishi kerak. Sababi eskirgan yoki noto'g'ri ma'lumotlarni saqlashga yo'l qo'ymaslik. Kesh xotiraga saqlash ba'zi bir mijoz-server aloqa muammolarini qisman bartaraf etishi va tizimning ishlashi tezligini samarali oshirish mumkin.

5. Ko'p qatlamli tizim arxitekturasi. Mijoz, odatda tarmoqlarning ierarxik tuzilishi (bunday tuzilma qatlamlarni tashkil etishini nazarda tutadi) tufayli to'g'ridan-to'g'ri server bilan yoki oraliq tugun bilan bog'langanini aniqlay olmaydi. Oraliq tugunlardan foydalanish tarmoq yuklanishini teng taqsimlashga va taqsimlangan kesh xotiralar sababli tizimning ishlash tezligini samarali oshirish mumkin.

CoAP (cheklangan dastur protokoli). Cheklangan dastur protokoli (Constrained application protocol, CoAP) - hisoblash, quvvat va tarmoq imkoniyatlari cheklangan qurilmalardan tuzilgan

tizimlar uchun mo'ljallangan protokollardan biri. IoT texnologiyalarida CoAP protokoli juda keng qo'llaniladi. CoAP protokoli odatda "Aqlli energiya" va "Aqlli shahar" kabi mashinadan mashinaga (M2M) ilovalar uchun mos keladi. CoAP protokoli strukturasi quyidagi 1-rasmda tasvirlangan.



1-rasm. CoAP protokli strukturasi

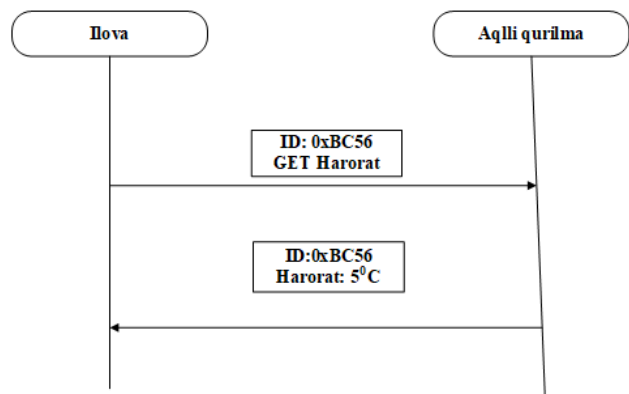
CoAP protokolining ishlash prinsipi HTTP protokoliga juda yaqin. CoAP protokoli yuqori yuklanish va cheklangan ulanish kabi xusiyatlarga ega tarmoqlarda samarali ma'lumot almashishni ta'minlaydi. CoAP protokoli xavfsizlik nuqtai nazaridan 128-bitli RSA kalitli shifrlash algoritmidan foydalanadi [4].

CoAP protokoli takroriy xabarlarini aniqlash uchun noyab identifikatordan (unique ID) foydalanadi. CoAP protokoli xabari quyidagi qismlardan iborat:

- Ikkilik sarlavha;
- Token;
- Foydali yuk.

CoAP protokolida ma'lumotning butunligini ta'minlash uchun tasdiqlangan xabar turidan foydalaniladi. Ushbu turdagi aloqada mijoz va server orasidagi xabarlar ikkinchi tomon tasdiq xabarini(ACK) jo'natmaguncha doimiy ravishda qayta yuboriladi. Agarda mijoz va server orasidagi xabarlar ikkinchi tomon tasdiqlashini talab qilmasa tasdiqlanmagan xabar(NON) turidan foydalaniladi. Ushbu turdagi xabarlarda ma'lumotning butunligini ta'minlash darajasi past hisoblanadi. CoAP protoklida ma'lumotlar almashish jarayoni quyidagi 2-rasmda tasvirlangan.





2-rasm. CoAP protoklida ma'lumotlar almashish jarayoni

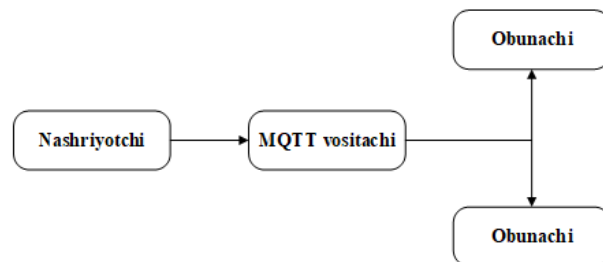
CoAP protokolida quyidagi so'rovi turlari mavjud:

- GET - resurslarni qidiradi va URI havolasida ko'rsatilgan manbaga mos keladigan ma'lumotlarni taqdim etadi;
- POST - resursdagi harakatni o'zgartirish uchun javobgardir;
- PUT - resursda yangi amalni o'rnatadi;
- DELETE - faollashtirilgan resurs imkoniyatlarini o'chirishga xizmat qiladi.

CoAP protokolida mavjud xavfsizlik muammolari. CoAP protokoli matnga asoslangan protokol bo'lib, tahdidlarni aniqlash va ulardan himoyalani usullari mavjud emas. Xavfsizlik nuqtayi nazaridan qo'shimcha DTLS xavfsizlik paketi ishlatishni talab qiladi. CoAP protokolida xabarlarini spoofing qilish muammosi ham mavjud. IoT texnologiyasida avtorizatsiya uchun CoAP protokolida qo'shimcha funktsiya mavjud emas. Protokolda xabar sarlavhasida token identifikatori mavjud bo'lib, u xabarni qaytadan o'zgaritib jo'natishga imkon beradi.

MQTT (cheklangan dastur protokoli). MQTT protokoli IoT texnologiyalarida keng qo'llaniladigan mashinadan mashinaga (M2M) protokollaridan biri hisoblanadi. Deyarli barcha IoT texnologiyalari qurilmalari MQTT protokolini qo'llab-quvatlaydi. MQTT protokoli ma'lumot almashish uchun nashriyotchi/obunachi (publish/subscribe) maxsus modelidan foydalanadi. U ma'lumot almashishning asosi sifatida TCP stekidan foydalanadi. MQTT protokoli ma'lumot hajmiga qaramasdan yuqori

o'tkazuvchanlik qobiliyatiga ega va doimiy seansni ta'minlaydi. Bu IoT texnologiyalarida qurilmalarga qo'yiladigan talablarni minimallashtirishga yordam beradi. MQTT protokolida ma'lumotlar almashish jarayoni quyidagi 3-rasmda tasvirlangan.



3-rasm. MQTT protoklida ma'lumotlar almashish jarayoni

MQTT vositachi – bu xabarlarini jo'natish va qabul qilishda filtrlash vazifasini bajaradigan server. Nashriyotchi – bu MQTT vositachiga ma'lumot jo'natuvchi mijoz hisoblanadi. Obunachi – bu MQTT vositachidan kerakli ma'lumotni qabul qiluvchi mijoz hisoblanadi.

MQTT protokolida xabarning muhimlik darajasini aniqlashda QoS (Xizmat sifati) bayroqlaridan foydalanadi. MQTT protokoli 3 xil QoS darajasini qo'llab-quvatlaydi [5]:

- QoS 0 - xabarni etkazib berish bir martadan ko'p bo'lmagan holda amalga oshiriladi. Muvaffaqiyatsiz bo'lsa, xabar yo'qoladi.
- QoS 1 - xabarni yetkazib berish kamida bir marta amalga oshiriladi. Yuborish qabul qiluvchi tomonidan tasdiqlanmaguncha takrorlanadi.
- QoS 2 - xabarni etkazib berish faqat bir marta amalga oshiriladi. MQTT protokoli aloqa kanalida muammo bo'lsa, etkazib berish kechiktiriladi. Biroq, har qanday holatda aloqa tiklanganda qabul qiluvchi xabar oladi.

MQTT protokolida bir qancha xavfsizlik xususiyatlari mavjud, bu CoAP protokoliga solishtirganda MQTT protokoli yordamida samarali xavfsizlikni ta'minlash mumkin. MQTT protokolida quyidagi xususiyatlari mavjud:

- chekka nuqta qurilmalarida shifrlash xususiyatiga ega va "o'rtadagi odam" (MITM) hujumlardan himoyalangan hisoblanadi;



- mijozlarni autentifikatsiya va avtorizatsiya qilish;

- server autentifikatsiyadan o'tgan qurilmaga faqatgina tegishli ma'lumotlarni jo'nata oladi, bu Ping of Death kabi hujumlarning oldini oladi;

- ikki tomonlama autentifikatsiyani qo'llab-quvvatlaydi, IP-spoofing hujumlarini bartaraf qilishga yordam beradi;

- MQTT vositachilar sertifikatlar asosida autentifikatsiyani ham o'z ichiga olishi mumkin.

IoT tizimining xavfsizlik muammolari.

Bugungi kunga kelib IoT texnologiyalari rivojlangan bo'lsada, xavfsizlik bilan bog'lik jiddiy muammolar mavjudligini ko'rish mumkin. Quyida bir qancha IoT texnologiyalaridagi xavfsizlik muammolari keltirib o'tamiz:

- ma'lumotlar yaxlitligini ta'minlash;
- yuqori markazlashgan boshqaruv usuli;
- turli kiberhujumlarga qarshi

himoyasizligi;

- markaziy nuqta nosozligi butun tizim nosozligiga sabab bo'lishi;

- boshqaruvsiz muhitlar.

II. Adabiyotlar tahlili

IoT xavfsizligini ta'minlashning an'anaviy usullari. Dunyo bo'ylab bir qancha olimlar tomonidan IoT uchun juda ko'p xavfsizlik tizimlari ishlab chiqilgan. Bu tizimlar hisoblash, quvvat va tarmoq imkoniyatlarini cheklangan qurilmalarga moslashtirilgan. Jain M.A. va boshqalar keltirgan maqolasida, IoT tizimida yangi qo'shilgan qurilmani autentifikatsiya qilish arxitekturasi taklif qilingan. Taklif qilingan arxitekturada qurilmalar bir-biri bilan aloqa qilish uchun CoAP protokolidan foydalanadi. Bu arxitekturaning boshqa arxitekturalardan farqi to'rt tomonlama autentifikatsiyadan foydalanadi. Arxitekturaning kamchiligi sifatida Sybil va qurilmaga qaratilgan hujumlarga nisbatan zaifligini ko'rsatish mumkin [6]. Yao X. va boshqalar tomonidan Elliptik egri chiziqqa asoslangan yengil sertifikatizatsiya ochiq kalitli kriptografiya tizimi taklif qilingan. Taklif qilingan tizimni mavjud sertifikatizatsiya ochiq kalitli kriptografiya tizimlariga solishtirganda hisoblash vaqti kam ekannin ko'rish mumkin. Maqolada

ma'lumotlarni xavfsiz saqlash va almashish to'g'risida ma'lumotlar keltirilmagan [7]. Roman R. va boshqalar, bulutli hisoblash va chekka nuqta kompyuterlarga asoslangan xavfsizlik tizimi taklif qilindi va bu tizimni "Virtual immunitet tizimi" deb nomlandi. Taklif qilingan tizimning tarkibiy qismlaridan biri tahdidlarni tahlil qilish. Bu tarkibiy qismning vazifasi yangi tahdidlarni aniqlash [8]. Alqahtani F. va boshqalar, IoT texnologiyasida bulutli hisoblash tizimiga asoslangan autentifikatsiya qilish usuli taklif qilindi. Taklif qilingan usulda IoT texnologiyalarida turli tahdidlarni aniqlash uchun monitoring sxemasi keltirilgan [9]. Wozid M. va boshqalar IoT texnologiyasi uchun bulutli hisoblashga asoslangan engil autentifikatsiya tizimini taklif qildi. Foydalanuvchilar IoT texnologiyasi kirish uchun autentifikatsiyadan o'tishi zarur [10]. Tahlil qilingan maqolardan xulosa qilib, taklif qilingan tizimlarda hisoblash, saqlash, aloqa yuklanishi va kiberhujum muammolari mavjud.

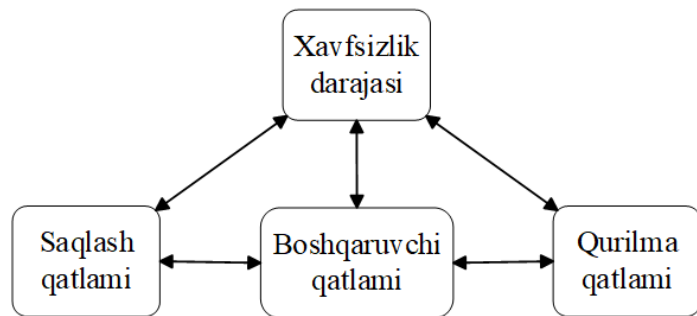
Blokcheyn yordamida IoT texnologiyasi xavfsizligi ta'minlash. Hozirgi kunga kelib IoT texnologiyalari uchun tadqiqotchilar tomonida bir qancha xavfsizlik tizimlari taklif qilishgan. Lekin markazlashtirilmagan boshqaruv, ma'lumotlarni xavfsiz saqlash, cheklangan qurilmalar uchun engil hisoblash, xavfsiz aloqa va qurilmalarni autentifikatsiya qilish kabi ba'zi takomillashtirilishi kerak bo'lgan sohalar mavjud. Ushbu sohalarni blokcheyn yordamida takomillashtirishda ba'zi chet el tadqiqotchilar taklif qilgan tizimlarni tahlil qilamiz. Shen M. va boshqalar tomonidan blokcheynga asoslangan xavfsiz SVM (vektor mashinasini qo'llab-quvvatlash) deb nomlangan tizim taklif qilindi. Taklif qilingan tizimning xavfsizligini ta'minlash uchun blokcheyn xususiyatlarida foydalanilgan [11]. Hammi M. va boshqalar, blokcheyn konsepsiyasi asosida qurilgan IoT ilovasi tizimini taklif qilishdi. Tizimda xavfsiz aloqani ta'minlash uchun dastlab xavfsizlik qabariqini yaratadi. Bu tizimning zaifliklaridan bir nechtasini ko'rish mumkin, yuqori hisoblashga asoslangan, DDoS va o'rtadagi odam (MitM) hujumlarini bartaraf qilish mumkin emas [12]. Tang B. va boshqalar, IoT texnologiyasi infratuzilmasida juda muhim bo'lgan platformalar aro aloqani



ta'minlaydigan IoT pasporti deb nomlangan tizimni taklif qilishdi. Taklif qilingan tizimda blokcheynga asoslangan autentifikatsiya va avtorizatsiya tizimlari keltirilgan. Tizim Sybil va Botnet hujumlariga zaif xisoblanadi [13]. Viriyasitavat W. va boshqalar tomonidan markazlashtirilmagan blokcheynga asoslangan IoT arxitekturasi taklif qilindi. Taklif qilingan tizim qurilmani xavfsiz ro'yxatdan o'tkazish va autentifikatsiya qilish uchun aqlli shartnomadan foydalanadi [14]. Beini Zhou va boshqalar identifikatsiya uchun shifrlash va blokcheyn kombinatsiyasidan foydalangan tizim taklif qildi. Ushbu tizimda har bir subyekt uchun Key Generation Center (KGC) tomonidan shaxsiy kalit beriladi. Tizimning asosiy kamchiliklaridan biri yuqori hisoblash va o'rtadagi odam (MitM) hujumini bartaraf qilish mumkin emas [15]. Ali Dorri va boshqalar blokcheynga asoslangan ikki qatlamli boshqarish tizimini taklif qildi. Ushbu tizimda markazlashtirilmagan boshqaruv, aloqa xavfsizligi va maxfiyligi uchun blokcheynda foydalanilgan. Bu tizimning asosiy kamchiligi hisoblash uchun katta resurslar kerak bo'lishi [16]. Lei Zhang va boshqalar tomonidan soxta xabarlarini aniqlash uchun Transport vositalari interneti (IoV) ni bir necha qismimlarga ajratish tizimi taklif qilindi. Bu qismimlar soxta xabar aniqlaganda ma'lumotni tekshirishga yordam beradi [17].

III. Materiallar va usullar

Taklif etilayotgan tizim ko'p qatlamli arxitektura bo'lib, uchta qatlamdan iborat: qurilma qatlami, boshqaruvchi qatlami va saqlash qatlami. Taklif etilayotgan tizim ko'p qatlamli arxitekturasi quyidagi 4-rasmda tasvirlangan. Qurilma qatlami IoT tizimidagi qurilmalarni o'z ichiga oladi. Boshqaruvchi qatlamida blokcheyn serverini yaratish uchun mas'ul bo'lgan to'plam boshqaruvchisi joylashgan bo'lib, uning asosiy vazifalari qurilmalarni autentifikatsiya qilish, blokklar va to'plamlarni yaratish, S_k maxfiy kalitini yaratish hisoblanadi [18].



4-rasm. Tizim arxitekturasi

Elliptik egri chiziq murakkabligiga asoslangan elektron raqamli imzo algoritmi (EECHERI)

Elliptik egri chiziq murakkabligiga asoslangan elektron raqamli imzo algoritmi (EECHERI) - bu ochiq kalitni shifrlash tizimining algoritmlarida biri hisoblanadi. EECHERI algoritmi DSA elektron raqamli imzo algoritmining modifikatsiyasi hisoblanadi. Agar M_i foydalanuvchi xabar yubormoqchi bo'lsa, u avval xabarga elektron raqamli imzo qo'yadi va uni M_j foydalanuvchiga ga yuboradi. M_j foydalanuvchi elektron raqamli imzoni tekshiradi, shundan so'ng agar elektron raqamli imzo haqiqiy bo'lsa ma'lumot almashuvni boshlaydi [19].

Burchak masofasi (BM)

Burchak masofasi (BM) - bu ikki obyekt orasidagi masofani hisoblash uchun ishlatiladi. Taklif etilayotgan tizimda to'plamga qo'shilishni istagan IoT qurilmasi va to'plam boshqaruvchisi orasidagi masofani hisoblash uchun BM dan foydalanilgan [20].

Burchak masofasini topish uchun

$$\begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ -\sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

burchak matritsasidan foydalaniladi. Agar to'plam a'zosi dastlabki koordinataga nisbatan α burchak ostida harakat qilsa, u holda to'plam a'zosining yangi koordinatalarini 1-tenglama yordamida hisoblash mumkin. Agar qurilma birinchi marta to'plamga kiritilgan bo'lsa, u holda burchak 0 daraja bo'ladi, chunki oldingi koordinata yo'q. To'plam a'zosining yangi koordinatasi hisoblagandan so'ng masofani 2-tenglama bo'yicha hisoblanadi. Endi IoT qurilmasi $P_i(X_i, Y_i)$ koordinatasida deylik, harakatdan so'ng, yangi koordinata $P_i'(X_i', Y_i')$ va to'plam boshqaruvchisi



koordinatasi $P_{TB}(X_{TB}, Y_{TB})$, burchak masofasi quyidagicha hisoblanadi:

$$\begin{bmatrix} X'_i \\ Y'_i \\ 1 \end{bmatrix} = \begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ -\sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_i \\ Y_i \\ 1 \end{bmatrix} \quad (1)$$

$$d_{i,j} = \|X_{TB} - X_i\| + \|Y_{TB} - Y_i\| \quad (2)$$

Bu erda $\| \|$ absolyut farqdir.

Merkle daraxti

Merkle daraxti - bu bloklardagi turli tranzaksiyalarning xeshlari yozilgan qaydnoma, ya'ni blokdagi barcha tranzaksiyalarning qisqacha mazmuni hisoblanadi. Shu sababli, u Xesh daraxti deb ham ataladi. Bu blok tarkibini samarali va xavfsiz tekshirishga yordam beradi. Bitkoin va Ethereum blokcheynlari tranzaksiyalar uchun Merkle daraxtidan foydalanadi. Taklif etilayotgan tizimda uzatilgan xabarlar tranzaksiyalar sifatida ko'rib chiqiladi. Tekshiruvchi ushbu barcha tranzaksiyalarni to'playdi va blokcheynga qo'shiladigan yangi blokni yaratish uchun Merkle daraxtini yaratadi [21-22].

Aqlli shartnoma

Aqlli shartnoma odatda ikki tomon o'rtasida raqamli aktivlar yoki ma'lumotlarning uzatilishini avtonom tarzda boshqaradigan if-then prinsipiga asoslangan shartli kompyuter dasturidir. Bu haqiqiy dunyo shartnomasiga juda o'xshaydi, lekin raqamli shaklda va blokcheyn ichida saqlanadi. Ular oldindan belgilangan muayyan shartlar yuzaga kelganda avtomatik ravishda amalga oshiriladi. Aqlli shartnomaning asosiy g'oyasi juda oddiy va uni quyidagicha tushuntirish mumkin [23-24]:

1. AGAR bu shart to'g'ri bo'lsa, unda bu harakatni bajarish kerak.
2. AGAR bu narsa mavjud bo'lsa, unda bu harakatni bajaring. Ya'ni, bu to'g'ri yoki noto'g'ri bo'lishi mumkin bo'lgan shartga muvofiq harakat qilinadigan shartli bayonotdir.

IV. Natija

Blokcheyn yordamida IoT ilovalari uchun xavfsiz autentifikatsiya tizimi

Taklif etilayotgan tizimda to'plamga qo'shilishdan oldin har bir qurilma xavfsiz autentifikatsiya mexanizmidan o'tishi kerak va

shundan keyingina u boshqa to'plam qurilmalari bilan aloqa o'rnatishi mumkin. Tizimda xavfsizlik mexanizmini ta'minlash uchun gibril kriptografiyadan foydalanilgan. To'plam a'zolari (TA) va to'plam boshqaruvchisi (TB) o'rtasidagi aloqa xavfsizligini ta'minlash uchun EECHERI dan foydalanilgan.

To'plamlar burchak masofasi (BM) asosida yaratiladi, ya'ni to'plamga qo'shilishni va TA bo'lishni xohlovchi qurilma birinchi navbatda TB dan ma'lum masofada bo'lishi kerak. Qurilma TB diapazoniga kirgach, u to'plamga qo'shilish uchun so'rov yuboradi (bu D_{id} qurilma identifikatorini o'z ichiga oladi). TB qurilmani tekshiradi va keyin ochiq kalit TK_{och} ni qurilmaga yuboradi. TB dan ochiq kalitni olgandan so'ng qurilma to'plam a'zosiga aylanadi. TB shuningdek, blokcheyn serverida qurilma identifikatorini o'z ichiga olgan blok yaratadi.

Algoritm-1 ikki koordinata nuqtasi orasidagi masofani aniqlaydi. Argument sifatida ikki nuqtaning koordinatalarini oladi va masofani aniqlaydi. $Nuqta_D$ qurilmasi (X_D, Y_D) koordinatalariga ega va TB ning $Nuqta_{TB}$ qurilmasi (X_{TB}, Y_{TB}) koordinatalariga ega.

1-jadval. Belgilar ta'rifi.

Belgi	Ta'rif
$E(K(X))$	X ni K kalit yordamida shifrlash
$D(K(X))$	X ni K kalit yordamida rasshifrlash
$H(X)$	X ni xesh qiymati
D_{id}	i -chi qurilmaning noyob identifikatori
n_i	i -komponentning psevd tasodifiy soni
R	To'plam radiusi
\oplus	XOR amali
$\ $	Birlashtirish operatsiyasi
S_k	Bir martalik maxfiy kalit
BK_{och}, BK_{sha}	Blokcheyn serverining ochiq va shaxsiy kalitlari
TB_{och}, TB_{sha}	To'plam boshqaruvchisining ochiq va shaxsiy kalitlari
$\Delta T_i, i=1,2,3...$	Vaqt chegarsi



k, ξ	Maxfiy ma'lumotlarni almashish uchun foydalaniladigan o'zgaruvchilar
$T_i, i=1,2,3...$	Vaqt
$T_i^*, i=1,2,3...$	Joriy vaqt
X_D, Y_D	Qurilmaning koordinatalari
X_{TB}, Y_{TB}	To'plam boshqaruvchisining koordinatalari
d_{ij}	i va j orasidagi masofa

Algoritm-1: Burchak masofasini topish algoritmi.

Kirish: $P_D, P'_D, P_{TB} : P_D, P_{TB}$ dastlabki koordinatlar va P'_D harakatdan keyingi koordinatalari.

Chiqish: d_{ij} : Bu ikkita qurilma orasidagi masofa (masalan, TA, TB)

- $P_D \leftarrow X_D, Y_D$ // qurilmaning koordinatalari
- $P_{TB} \leftarrow X_{TB}, Y_{TB}$ // to'plam boshqaruvchisining koordinatalari

$$3. \begin{bmatrix} X'_D \\ Y'_D \\ 1 \end{bmatrix} \leftarrow \begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ -\sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X_D \\ Y_D \\ 1 \end{bmatrix} // \text{bu}$$

tenglama qurilmaning yangi koordinatalarini hisoblash uchun ishlatiladi P_D va (X'_D, Y'_D) yangi koordinatalar.

- $d_{TB,D} \leftarrow \|X_{TB} - X'_D\| + \|Y_{TB} - Y'_D\|$ // Qurilma va to'plam boshqaruvchisi orasidagi masofa.

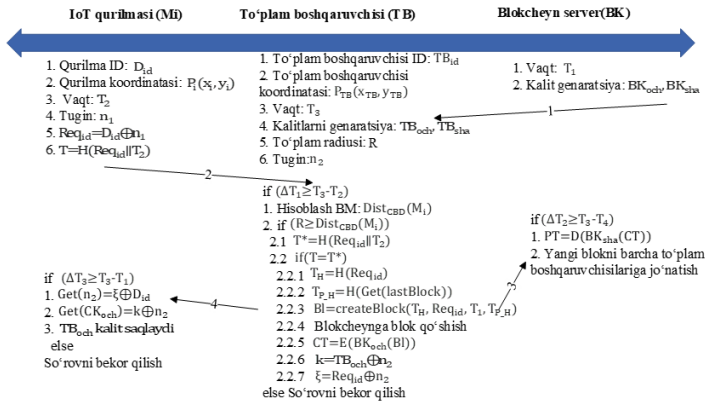
To'plam yaratish va qurilmani autentifikatsiya qilish jarayoni quyida keltirilgan 4 bosqichdan iborat:

- D_i qurilmasining D_{id} qurilma identifikatori, $P_i(X_i, Y_i)$ qurilma koordinatalari, T_2 vaqt aniqlanadi. Keyin $D_i, Req_{id} = D_{id} \oplus n_1 T = H(Req_{id} \| T_1)$ sifatida to'plamga qo'shilish so'rovini yaratish uchun hisob-kitoblarni amalga oshiradi va $(T, Req_{id} \| T_2)$ ni to'plam boshqaruvchisiga yuboradi.
- So'rovni olgandan so'ng, TB birinchi navbatda $\Delta T_1 \geq T_3 - T_2$ to'g'riligini tekshiradi, aks holda so'rov rad etiladi. Agar shart to'g'ri bo'lsa, boshqaruvchi burchak masofasidan foydalangan holda masofani hisoblab chiqadi (1-algoritm), agar qurilma boshqaruvchining to'g'ri diapazonida

bo'lsa, u harakat qiladi va $T^* = H(Req_{id} \| T_2)$ ni hisoblab chiqadi, keyin $T^* = T$ to'g'riligini tekshiradi va agar shunday bo'lsa, u $T_H = H(Req_{id}), T_{PH} = H(Get(lastBlock))$ sifatida hisoblashni amalga oshiradi (Merkle daraxti konsepsiyasidan foydalangan holda), so'ngra $Bl = T_H, Req_{id}, T_1, T_{PH}$ sifatida blokcheynda (PoS konsepsiyasidan foydalangan holda) blok yaratadi. Shundan so'ng, u yaratilgan blokni blokcheyn serverining BK_{och} ochiq kaliti yordamida shifrlaydi $CT = E(BK_{och}(Bl))$ va (CT, TB_{id}, T_3) ni boshqa to'plamlar bilan almashish uchun blokcheyn serveriga yuboradi. Bundan tashqari, TB umumiy kalitni so'ragan qurilma bilan almashish uchun $k = TB_{och} \oplus n_2, \xi = Req_{id} \oplus n_2$ sifatida k va ξ ni hisoblab chiqadi. Keyin D_i qurilmasiga (k, ξ, T_3) yuboradi.

- Blokcheyn serveri to'plam boshqaruvchisidan shifrlangan yangi blok oladi. U birinchi navbatda $\Delta T_2 \geq T_3 - T_4$ to'g'riligini tekshiradi, agar to'g'ri bo'lsa, u o'zining BK_{sha} shaxsiy kalitini $PT = D(BK_{sha}(CT))$ sifatida ishlatib, CT shifrini ochadi va keyin bu yangi blokni barcha to'plam boshqaruvchilarga xavfsiz tarzda uzatadi.
- To'plam boshqaruvchisidan javob olgandan so'ng, D_i birinchi navbatda $\Delta T_3 \geq T_3 - T_1$ to'g'riligini tekshiradi, agar to'g'ri bo'lsa, keyin D_i qabul qilingan javobdan $Get(n_2) = \xi \oplus D_{id}, Get(TB_{och}) = k \oplus n_2$ sifatida to'plam boshqaruvchisining ochiq kalitini hisoblaydi va keyingi aloqalar uchun TB_{och} ni saqlaydi. Ushbu protsedura boshqa qurilmalar tomonidan amalga oshiriladi va biz har bir qurilma TB dan autentifikatsiya qilingan xavfsiz qurilmalar to'plamini yaratamiz.





5-rasm. To'plam yaratish va qurilma autentifikatsiyasi qilish jarayoni

Maxfiy kalitni yaratish va M2M aloqasi

Ikki to'plam a'zolari o'rtasidagi aloqa xavfsizligini ta'minlash uchun 192 bitli AES simmetrik kriptografiya algoritmidan foydalanilgan. To'plam a'zolari bir-biri bilan aloqa qurishdan foydalanadigan simmetrik kalitni to'plam boshqaruvchisidan oladi. To'plam a'zosi va to'plam boshqaruvchisi o'rtasidagi aloqa uchun Elliptik egri chiziq murakkabligiga asoslangan elektron raqamli imzo algoritmidan foydalanilgan. Tepadagilarni umumiy qilib aytganda aloqa xavfsizligini ta'minlash uchun gibrid kriptotizimdan foydalanilgan. Taklif etilayotgan aloqa usuli quyida keltirilgan 7 da bosqichdan iborat:

- To'plam a'zosi M_i so'rov sifatida $Req[M_i||T_i]$ ni M_j (boshqa to'plam a'zosi) ga yuboradi.
- To'plam a'zosi M_j so'rovni qabul qiladi va birinchi navbatda tekshiradi $\Delta T_1 \geq T_i^* - T_i$ to'g'ri yoki noto'g'ri, agar to'g'ri bo'lsa, M_i to'plam a'zoning haqiqiylikini tekshirish va bir martalik maxfiy kalit yaratish uchun to'plam boshqaruvchisiga so'rov sifatida yuboradi $Req[E(TB_{och}(M_i||M_j||T_i||T_j))]$ yuboradi va javobni kutadi.
- To'plam boshqaruvchisi M_j dan so'rovni olgandan keyin, avval tekshiradi $\Delta T_2 \geq T_j^* - T_j$ agar to'g'ri bo'lsa, to'plam boshqaruvchisi ikkala a'zoni ham haqiqiylikini tekshiradi. Tekshirishdan so'ng, bir martalik maxfiy kalit S_k ni yaratadi, javobni ikkala a'zoga $Res[E(TB_{sha}(S_k \oplus M_i \oplus M_j)||T_j)]$, $Res[E(TB_{sha}(S_k \oplus M_i)||T_i)]$, M_j va

M_i a'zolariga mos ravishda yuboradi. Agar so'ragan a'zoldan biri to'plam boshqaruvchisi tomonidan topilmasa, boshqa to'plam boshqaruvchilar xabardor bo'lishi uchun ogohlantirish xabari ishlab chiqariladi.

- To'plam a'zosi M_i bir martalik maxfiy kalit S_k ni olish uchun qabul qilingan javobni $A = D(CKoch(E(TB_{sha}(S_k \oplus M_i)||T_i)))$ hisoblaydi va keyin $\Delta T_2 \geq T_i^* - T_i$ tekshiradi, agar to'g'ri bo'lsa $Get(S_k) = A \oplus M_i$ hisoblaydi va S_k ni aloqa uchun saqlab qo'yadi.
- To'plam a'zosi M_j javob sifatida $Res[T_i||T_j]$ ni M_i ga yuboradi, ya'ni u keyingi xabarni qabul qilishga tayyor.
- To'plam a'zosi M_i xabar yaratadi ($Xabr_1$) va uni bir martalik maxfiy kalit yordamida (AES shifrlash algoritmi) shifrlaydi $E(S_k(Xabr_1))$ va M_j ga yuboradi.
- To'plam a'zosi M_j qabul qiladi va xuddi shu kalit yordamida shifrnı ochadi, keyin u xabar yaratadi ($Xabr_2$) va uni shifrlagandan $E(S_k(Xabr_2))$ keyin M_i ga yuboradi, xuddi shunday qilib ikki to'plam a'zosi o'rtasida aloqa davom etadi.

Algoritm-2: Maxfiy kalitlarni yaratish.

Kirish: Q_n, R_n

Chiqish: S_k : bu bir martalik maxfiy kalit

1. $Q_n = randomNumber()$

2. $R_n = randomNumber()$

3. **agar** $Q_n = Tub\ son\ keyin$

agar $R_n = Tub\ son\ keyin$

$N = (Q_n - 1) * (R_n -$

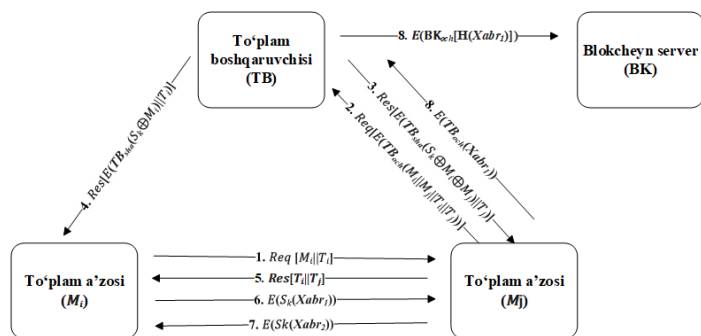
1)

$E =$

$randomNumber()\%1000$ // "% mod operatsiyasi

$S_k = N^E$





6-rasm. Maxfiy kalit yaratish va M2M aloqa jarayoni

Xulosa. Bugungi kunga kelib IoT texnologiyalari rivojlangan bo‘lsada, xavfsizlik bilan bog‘liq jiddiy muammolar mavjudligini ko‘rish mumkin. Ushbu maqolada IoT texnologiyasida qo‘llaniladigan REST, CoAP, MQTT protokollari tahlil qilindi. IoT texnologiyasidagi xavfsizlik muammolari ko‘rsatib o‘tilgan. Blokcheyn yordamida IoT ilovalari uchun xavfsiz autentifikatsiya va ma’lumot almashish tizimi arxitekturasi ishlab chiqildi. Taklif etilayotgan tizim ko‘p qatlamli arxitektura bo‘lib, uchta qatlamdan iborat: qurilma qatlami, boshqaruvchi qatlami va saqlash qatlami. Tizimda autentifikatsiya algoritmi blokcheyn (aqli shartnoma) yordamida takomillashtirildi va ikki to‘plam a‘zolari o‘rtasidagi aloqa xavfsizligini ta’minlash uchun AES simmetrik va Elliptik egri chiziq murakkabligiga asoslangan elektron raqamli imzo algoritmlari foydalanilgan.

Keyingi ilmiy tadqiqotlarimizda taklif etilayotgan tizimni turli xil xavfsizlik hujumlariga qarshi tahlil qilish va mavjud boshqa tizimlar bilan solishtirma tahlil o‘tkazish ko‘zda tutilgan.

Foydalanilgan adabiyotlar ro‘yxati

1. HaddadPajouh H. et al. A survey on internet of things security: Requirements, challenges, and solutions //Internet of Things. -2021. -T.14. -C. 100129
2. Srivastava, S., Chaurasia, B.K., Singh, D.: Blockchain-based IoT security solutions. In: Distributed Computing to Blockchain, pp. 327–339. Academic Press (2023)

3. Roy T. Fielding. Chapter 5 of dissertation “Representational State Transfer (REST)”. - 2020.
https://ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm
4. RFC 7252, Constrained Application Protocol (CoAP).
<https://datatracker.ietf.org/doc/html/rfc7252>
5. Bryan Boyd et al. Building Real-time Mobile Solutions with MQTT and IBM MessageSight. IBM Redbooks, 2014
6. Jan Mian Ahmad, Priyadarsi Nanda, Xiangjian He, Zhiyuan Tan, Ren Ping Liu. A robust authentication scheme for observing resources in the internet of things environment 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE (2014), pp. 205-211
7. Xuanxia Yao, Xiaoguang Han, Xiaojiang Du. A light-weight certificate-less public key cryptography scheme based on ECC. 2014 23rd International Conference on Computer Communication and Networks, ICCCN, IEEE (2014), pp. 1-8
8. Rodrigo Roman, Ruben Rios, Jose A. Onieva, Javier Lopez. Immune system for the internet of things using edge technologies. IEEE Int. Things J. (2018)
9. Fayez Alqahtani, Zafer Al-Makhadmeh, Amr Tolba, T.B.M. Omar Said. A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications. Comput. Commun., 150 (2020), pp. 216-225
10. Mohammad Wazid, Ashok Kumar Das, Vivekananda Bhat, Athanasios V. Vasilakos. LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment. J. Netw. Comput. Appl., 150 (2020), Article 102496
11. Meng Shen, Xiangyun Tang, Liehuang Zhu, Xiaojiang Du, Mohsen Guizani. Privacy-preserving support vector machine training



- over blockchain-based encrypted IoT data in smart cities. *IEEE Int. Things J.* (2019)
12. Hammi Mohamed Tahar, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni. Bubbles of Trust: a decentralized blockchain-based authentication system for IoT. *Comput. Secur.*, 78 (2018), pp. 126-142
 13. Bo Tang, Hongjuan Kang, Jingwen Fan, Qi Li, Ravi Sandhu. IoT passport: a blockchain-based trust framework for collaborative internet-of-things. *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, ACM (2019), pp. 83-92
 14. Wattana Viriyasitavat, Li Da Xu, Zhuming Bi, Assadaporn Sapsomboon. New blockchain-based architecture for service interoperations in Internet of Things. *IEEE Trans. Comput. Soc. Syst.*, 6 (4) (2019), pp. 739-748
 15. Beini Zhou, Hui Li, Li Xu. An authentication scheme using identity-based encryption & blockchain. *2018 IEEE Symposium on Computers and Communications, ISCC, IEEE* (2018), pp. 00556-00561
 16. Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. LSB: a lightweight scalable blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.*, 134 (2019), pp. 180-197
 17. Lei Zhang, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, Shengwei Tian. Blockchain based secure data sharing system for Internet of vehicles: a position paper. *Veh. Commun.*, 16 (2019), pp. 85-93
 18. N Akhmedov, H Khujamatov, A Lazarev, M Seidullayev. Application of LPWAN technologies for the implementation of IoT projects in the Republic of Uzbekistan. *2021 International Conference on Information Science and Communications Technologies (ICISCT)*.
 19. Nasrullayev, N., Seidullaev, M., Khudoykulov, Z., Abdjalilovich, G.A. (2024). Classification of Threats to Information Security of the “Smart Home” System. In: Aliev, R.A., et al. *12th World Conference “Intelligent System for Industrial Automation” (WCIS-2022)*. WCIS 2022. *Lecture Notes in Networks and Systems*, vol 718. Springer, Cham. https://doi.org/10.1007/978-3-031-51521-7_9.
 20. Madiyar Seidullayev. Internet of Things security based on blockchain technology. *Innovative Development in Educational Activities VOLUME 2 | ISSUE 11 | 2023*.
 21. Мадияр Сейдуллаев. Применение блокчейн-технологии в интернете вещей. *RESEARCH AND EDUCATION VOLUME 2 | ISSUE 1 | 2023*.
 22. Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. LSB: a lightweight scalable blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.*, 134 (2019), pp. 180-197
 23. Lei Zhang, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, Shengwei Tian. Blockchain based secure data sharing system for Internet of vehicles: a position paper. *Veh. Commun.*, 16 (2019), pp. 85-93
 24. Beini Zhou, Hui Li, Li Xu. An authentication scheme using identity-based encryption & blockchain. *2018 IEEE Symposium on Computers and Communications, ISCC, IEEE* (2018), pp. 00556-00561

