**O‘ZBEKISTON MILLIY UNIVERSITETI
HUZURIDAGI ILMIY DARAJALAR BERUVCHI
DSc.03/30.12.2019.FM.01.02 RAQAMLI ILMIY KENGASH**

O‘ZBEKISTON MILLIY UNIVERSITETI

SAYMANOV ISLAMBEK MIRZABAEVICH

EKOLOGIK MA’LUMOTLARNI QAYTA ISHLASH VA HIMOYA QILISHNING ALGORITMIK VA MANTIQIY USULLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi (fizika-matematika fanlari)

FIZIKA-MATEMATIKA FANLARNI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2023

УДК: 004.056

Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора философии (PhD) по физико-математическим наукам

Contents of dissertation abstract of doctor of philosophy (PhD) on physical-mathematical sciences

**O‘ZBEKISTON MILLIY UNIVERSITETI
HUZURIDAGI ILMIY DARAJALAR BERUVCHI
DSc.03/30.12.2019.FM.01.02 RAQAMLI ILMIY KENGASH**

O‘ZBEKISTON MILLIY UNIVERSITETI

SAYMANOV ISLAMBEK MIRZABAEVICH

EKOLOGIK MA’LUMOTLARNI QAYTA ISHLASH VA HIMOYA QILISHNING ALGORITMIK VA MANTIQIY USULLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi (fizika-matematika fanlari)

FIZIKA-MATEMATIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Тошкент – 2023

Fizika-matematika fanlari bo‘yicha falsafa doktori (Doctor of Philosophy) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasida №B2022.2.PhD/FM739 raqam bilan ro‘yxatga olingan.

Dissertatsiya Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasi (http://ik-fizmat.nuu.uz/) va «ZiyoNet» Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Kabulov Anvar Vasilovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Abduraximov Baxtiyor Fayziyevich** fizika-matematika doktori, professor
	Saidov Abdusobirjon Abduraxmonovich texnika fanlari doktori, professor
Yetakchi tashkilot:	**Berdaq nomidagi Qoraqalpoq davlat universiteti**

Dissertatsiya himoyasi O‘zbekiston Milliy universiteti huzuridagi DSc.03/30.12.2019.FM.01.02 raqamli Ilmiy kengashning «___»_____2023 yil soat____ dagi majlisida bo‘lib o‘tadi. (Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 227-12-24, faks: (+99871) 246-53-21, 246-02-24, e-mail: nauka@nuu.uz).

Dissertatsiya bilan O‘zbekiston Milliy universitetining Axborot-resurs markazida tanishish mumkin (___ raqami bilan ro‘yxatga olingan). (Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 246-02-24).

Dissertatsiya avtoreferati 2023 yil «____» _____kuni tarqatildi.
(2023 yil «____» _____ dagi _____ raqamli reestr bayonnomasi).

M.M. Aripov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, f.-m.f.d. professor

Z.R. Raxmonov
Ilmiy darajalar beruvchi Ilmiy kengash ilmiy kotibi, f.-m.f.d.

G.U. Jo‘rayev
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, f.-m.f.d.

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon miqyosida turli sohalarda axborot texnologiyalaridan foydalanishga, ayniqsa, ulardan davlat boshqaruvi va o‘z-o‘zini boshqarish tizimida qo‘llash sohasida alohida e’tibor qaratilmoqda. Shunga ko‘ra, jismoniy va yuridik shaxslarga turli davlat interaktiv xizmatlarini ko‘rsatishda ma’lumotlarning maxfiyligini ta’minlash texnologiyalari va usullaridan foydalanish, iqtisodiy tizimlarni global miqyosda integratsiyalash imkoniyatlarini kengaytirish dolzarb muammo hisoblanadi. Xalqaro ma’lumotlar korporatsiyasi (IDC)ning yangi bashoratlariga ko‘ra, 2025 yilda 41,6 milliard IoT-qurilmalari yoki 79,4 zetabayt (Zb) ma’lumotlarni umumlashtiruvchi “buyumlar”ning ulanishi rejalashtirilgan. Ko‘plab mamlakatlarda, jumladan, AQSh, Yevropa, Osiyo va MDH davlatlari, shuningdek, arab mamlakatlari tomonidan axborotning kompleks himoyasini ta’minlash bo‘yicha ilmiy tadqiqotlar olib borilmoqda.

Hozirgi kunda jahonda nashrlarning tahlili, raqamli texnologiyalarga kompleks yondashuvga asoslangan ekotizimlar misolida IoT axborot tizimlarini himoyalash modellari va usullarini ishlab chiqish zarurligini ko‘rsatmoqda. Ekotizimlarning axborot xavfsizligini boshqarish tizimining asosiy funktsiyalari ekotizim axborot xavfsizligining buzilishi bilan bog‘liq vaziyatning keskinlik darajasini baholash, axborot xavfsizligining buzilish xavfi darajasini baholash va ushbu vaziyatda harakatlar bo‘yicha qarorlarni qabul qilishni qo‘llab-quvvatlashdan iborat bo‘lishi lozim. Boshqacha qilib aytganda, asosiy muammo ko‘p hollarda axborot xavfsizligi tizimining holati, ehtimoliy tahdidlar, beqarorlashtiruvchi omillar to‘g‘risidagi to‘liq bo‘lmagan va noaniq dastlabki ma’lumotlarga bog‘liq.

Mamlakatimizda fundamental fanlarning ilmiy va amaliy tadbiqiga ega bo‘lgan kriptologiyaning dolzarb yo‘nalishlariga e’tibor ko‘chaytirildi. Jumladan, kriptografik akslantirishlar va algoritmlarni ishlab chiqish sohasida ma’lum yutuqlarga erishilib, axborotlarni uzatish va qayta ishlashning himoyalangan tizimlarini yaratishga alohida e’tibor qaratildi. “Amaliy matematika va matematik modellashtirish” fanlarining ustuvor yo‘nalishlari bo‘yicha xalqaro standartlar darajasida ilmiy tadqiqotlar olib borish asosiy vazifalar va faoliyat yo‘nalishlari etib belgilandi. “Funksional analiz, algebra, differensial tenglamalar, matematik fizika, matematik modellashtirish, hisoblash matematikasi va diskret matematika, ehtimollar nazariyasi va matematik statistika” ustuvor yo‘nalishlar bo‘yicha xalqaro standartlar darajasidagi ilmiy izlanishlar olib borish O‘zR FA V.I.Romanovskiy nomidagi Matematika instituti faoliyatining asosiy vazifalaridan biri hisoblanadi. Qaror ijrosini ta’minlashda steganografiya algoritmlarini amalga oshirish, algoritmlar va mantiqiy algebra funktsiyalari tizimlarining graf-sxemalari asosida timsollarni aniqlash va tanib olish uchun IoT tizimida ekologik ma'lumotlarini qayta ishlash va himoya qilishning algoritmik va mantiqiy usullarini ishlab chiqish muhim ahamiyatga ega.

O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevraldagi PF-4947 “O‘zbekiston Respublikasini yanada rivojlantrish bo‘yicha harakatlar strategiyasi to‘g‘risida”gi Farmoni, 2017-yil 17-fevraldagi PQ-2789-son “Fanlar akademiyasi

faoliyati, ilmiy-tadqiqot ishlarini tashkil etish, boshqarish va moliyalashtirishni yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi, 2017-yil 20-apreldagi PQ-2909-son “Oliy ta’lim tizimini yanada rivojlantirish chora-tadbirlari to‘g‘risida”gi va 2018 yil 27 apreldagi PQ-3682 “Innovatsion g‘oyalar, texnologiyalar va loyihalarni amaliyotga joriy qilish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risidagi” qarorlari hamda mazkur faoliyatga tegishli boshqa normativ-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Dissertatsiya respublika fan va texnologiyalar rivojlanishining IV. «Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish» ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Kriptografiya, steganografiya, identifikatsiya va tasvirlarni tanib olish algoritmlarini amalga oshirish uchun ekotizimlar va ekologik ma’lumotlarini qayta ishlash va himoya qilishning algoritmik va mantiqiy usullari, shuningdek, maxfiy ekologik ma’lumotlarni himoya qilishni ta’minlash usullarining mantiqiy, matematik yechimlari misolida IoT axborot tizimlarining ishlashi va himoyasi modellari va usullarini yaratishning nazariy va amaliy vazifalari bo‘yicha ilmiy-tadqiqot ishlari va adabiyot manbalarining tahlili quyidagi olimlarning ishlarida ko‘rib chiqilgan: L. Zhou, M. Pavanil, S. Goel, R. Nagalakshmi, J. Ahamed, Bento A. Ganzaga, O.Y. Abdulhammed, R. Mohandas, Ю.И. Журавлев, О. Евсютин, А. Шелупанов, А. Тихомиров, В.В. Мельников, С.С. Корт, А.Г. Корченко, И.В. Котенко, М.В. Степашкин va boshqalar.

Ekotizimlarning axborot xavfsizligi nazariyasi va amaliyotini rivojlantirishga G. Fischer, И.И. Быстров, В.А. Герасименко, О.Ю. Гаценко, А.А. Грушо, В.С. Заборовский, П.Д. Зегжда, Д.П. Зегжда, В.А. Конявский, А.А. Малюк, А.А. Молдовян, Л.Г. Осовецкий, В.П. Шерстюк, А.Ю. Щербаков va boshqalar salmoqli hissa qo‘shishgan. So‘nggi bir necha yil ichida ushbu mualliflar tomonidan texnik va qonunchilik nuqtai nazaridan IoT ilovalari va qurilmalarining xavfsizligi va maxfiyligi masalalari bo‘yicha ko‘plab ishlar amalga oshirilgan.

O‘zbekistonda ko‘rib chiqilayotgan muammo axborot xavfsizligi va ma’lumotlar maxfiyligini ta’minlash algoritmlari va modellarini yaratishga katta hissa qo‘shgan yetakchi olimlar: T.F. Bekmuratov, M. Aripov, S. Ganiev, X.A. Muzaffarov, B.F. Abduraximov, R.J. Aloev, N.A. Ignatev va boshqalar rahbarligida yaratilgan ilmiy maktablar tomonidan ishlab chiqilmoqda.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti O’zbekiston Milliy universitetining ilmiy-tadqiqot ishlari rejalariga muvofiq FZ-201906117 “Orolbo‘yi qishloq xo‘jaligi ishlab chiqarishida ekologik vaziyatlar ta’sirini aniqlash monitoringini yuritishning dasturiy ta’minoti” (2020-2022), F-OT-2021-248 “Funtsional jadvallar asosida axborotlarni himoyalash uchun xavf-xatarlarni aniqlash, identifikatsiya va bartaraf qilishning intellektual usullari va texnologiyalarini ishlab chiqish” (2021-2022), AL-18245120 – “Orol mintaqasi misolida IoT qurilmalari tomonidan ishlab chiqarilgan ekologik ma’lumotlar

oqimlarini qayta ishlash va himoya qilishning intellektual usullari va texnologiyalari (2022-2023) loyihalari doirasida bajarilgan.

Tadqiqotning maqsadi algoritmik va mantiqiy algebraik funktsional tizimlarning graf-sxemalari asosida steganografiya, identifikatsiya va tanib olish algoritmlarini amalga oshirish uchun IoT tizimida atrof-muhit ma’lumotlarini qayta ishlash va himoyalashning algoritmik va mantiqiy usullarini ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

IoT texnologiyalariga asoslangan ekotizimda axborotni himoya qilish ob’ektining tavsiflarini tadqiq etish, hamda sensor va boshqa qurilmalarda ma’lumotlarni saqlash va uzatishni xavfsiz amalga oshirish uchun IoT infratuzilmasini tahlil qilish;

ma’lumotlarni kiritish va foydalanuvchilardan foydalanishni nazorat qilish jarayonida sub’ektlar va ob’ektlarning optimal mosligini ta’minlash uchun funktsional jadvallari (FJ) asosida algoritmik modelni ishlab chiqish;

IoT texnologiyalari asosida ekotizimda tasvirlarni saqlash va uzatishni xavfsiz amalga oshirish uchun steganografik kodlash usullari va algoritmlarini ishlab chiqish;

baholashlarning hisoblash modelini chiziqli qisqa tutashuv (yopilish)dan to‘g‘ri (korrekt) modelga asoslangan holda bir-biriga mos kelmaydigan sinflar bilan tanib olish masalalarini yechishning algebraik usulini va to‘g‘ri (korrekt) algoritmni ishlab chiqish;

etalon jadvalini hamma joyda ham aniqlanmagan mantiqiy funktsiya sifatida ko‘rib chiqish va sinflarning butun fazoga kengayishini aniqlaydigan butun belgilar fazosida mantiqiy funktsiyaning optimal davomini qurish asosida ob‘ektlarni tanib olishning mantiqiy usulini ishlab chiqish;

mikrokontrollerlar va dasturlashtiriladigan mantiqiy kontrollerlarni loyihalash uchun CAD tizimiga asoslangan disyunktiv normal shakllar sinfida bul’ funktsiyalari asosida tasvirlarni xavfsiz saqlash va uzatish uchun steganografik kodlash va El Gamal assimetrik shifrlash algoritmlarini amalga oshirish;

ekologiyada IoT texnologiyalaridan foydalanish asosida Orolbo‘yi ekotizimida identifikatsiya qilish muammosini hal qilish uchun baholashlarning hisoblash modellarini joriy etish.

Tadqiqotning ob’ekti sifatida IoT qurilmalari tomonidan yaratilgan ekologik ma'lumotlarini boshqarish, aniqlash, qayta ishlash va himoya qilish uchun o‘rnatilgan tizimlaridan iborat.

Tadqiqotning predmeti algoritmik avtomatik modellar, steganografik algoritmlar va axborot xavfsizligi funksional jadvallari, mantiqiy jadvallar va steganografiya algoritmlarining funksiyalari.

Tadqiqotning usullari. Tadqiqot ishida tizimli tahlil, avtomatlar nazariyasi, optimal boshqaruv nazariyasi, algoritmik modellar va vositalar, axborot resurslarining maxfiyligini ta’minlash algoritmlari va usullari, boshqaruv monitorlarini qurish, imitatsion modellashtirish, Petri tarmoqlari, algebra va matematik mantiq, tasvirlarni aniqlash usullaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

ma’lumotlarni kiritish va foydalanuvchi kirishini boshqarish jarayonida sub’ektlar va ob’ektlarning optimal mosligini ta’minlash uchun algoritmik model algoritmlashtirish tamoyillarini tadqiq qilish va funksional jadvallarni yaratish asosida ishlab chiqilgan;

mikrokontrollerlar va dasturlanadigan mantiqiy kontrollerlarni CAD loyihalashtirish tizimlari bazasida diz’yunktiv normal shakllar sinfida bul funksiyalari asosida steganografik kodlashning mantiqiy avtomat algoritmi tasvirlarni saqlash va uzatishni xavfsiz tashkil etish uchun ishlab chiqilgan;

mantiqiy funktsiyaning optimal davomini qurishga va to‘g‘ri modelga asoslangan o‘zaro kesishmaydigan sinflar bilan tanib olish masalalarini yechishning algebraik va mantiqiy usullari baholarni hisoblash algoritmlarini chiziqli tutashuv va butun alomatlar fazosi uchun ishlab chiqilgan;

IoT tizimida tasvirlarni identifikatsiya qilish, qayta ishlash va himoyalashning mantiqiy tanib olish algoritmining polinimial murakkabligi isbotlangan;

IoT tizimida ekologik ma’lumotlarini identifikatsiya qilish, qayta ishlash va himoyalashning algebraik tanib olish algoritmining korrektligi isbotlangan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

ekotizimning ob’ekti va sub’ekti o‘rtasidagi muvofiqlik jadvali asosida boshqaruv va xavfsizlik axborot tizimlari uchun IoT texnologiyalarini qo‘llash maqsadida ekotizimlarning dasturiy-texnik majmuasi ishlab chiqildi. Steganografiya algoritmlarining bul jadval graf-sxemalarini tashkil etuvchi mantiqiy formulalar ko’rinishidagi mantiqiy munosabatlar qurilgan;

ekologiyada Internet-narsalar texnologiyalaridan foydalanish asosida Orolbo‘yi ekotizimida identifikatsiya qilish muammosini hal qilish uchun baholarni hisoblash modeli taklif etilgan;

steganografiya va assimetrik shifrlash El Gamal algoritmlarning graf-sxemalari va dizyunktiv normal shakllar sinfidagi optimal bul’ funktsiyalari asosida amalga oshirilgan.

Tadqiqot natijalarining ishonchliligi himoya jarayonining yagona va standart tavsifi asosida, murakkab tizimlarni algoritmlashning asosli usullari nazariyasi va amaliyoti, avtomat modellar, bul funktsiyalari, kriptoalgoritmlar va stegoalgoritmlarni taqdim etish uchun o‘rnatilgan mikroprotsessorli tizimlardan foydalangan holda axborotni kompleks himoya qilish muammolarini qat’iy shakllantirish bilan asoslangan.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati agregat tizimlarni himoya qilish jarayonini tanib olish uchun algebraik va mantiqiy usullar bilan identifikatsiya algoritmlarini ishlab chiqish, avtomat modellar hamda xavfsizlikning faoliyat ko‘rsatishi va ta’minlanishida o‘rnatilgan IoT ekotizimini yaratish usullari bilan izohlanadi.

Tadqiqot natijalarning amaliy ahamiyati IoT ekotizimlarini yaratish imkoniyati, axborot xavfsizligi va kriptografiya uchun kriptoalgoritmlarning graf-sxemalarini amalga oshiradigan bul funktsiyalarning diz’yunktiv normal shakllariga asoslangan kriptotizimlar va kriptoalgoritmlarni optimal taqdim etish bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Axborot tizimlarini boshqarishda interaktiv xizmatlar axborot resurslarining maxfiyligini ta’minlash maqsadida ishlab chiqilgan usullar va modellari asosida bir qator xo‘jalik sub’ektlarida joriy etilgan:

steganografiya algoritmining optimal matematik modelidan Uzb-Ind-2021-94 “CRN asosida IoT infratuzilmasidan foydalangan holda aqlli shahardagi energiya samaradorligi va ma’lumotlarning oqimi” loyihasida shifrlash algoritmlarini mikrokontrollerlarga yozishda mikrobuyruqlarning bul funksiya shakllarini tahlil qilish va yozishda qo’llanilgan (Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining 2022 yil 25 maydagi №1596-15/01-son ma’lumotnomasi). Ilmiy natijalarni qo‘llash mikrokontrollerga steganografik algoritmini optimal yozish va tahlil qilish imkonini bergan;

suv va tuproqni interaktiv tahlil qilish usuli va vositalari, shuningdek, Orol dengizi bo‘yidagi qishloq xo‘jaligi sanoatida suv va tuproqni interaktiv tahlili natijalaridan atrof-muhit sharoitining ta’sirini aniqlash uchun monitoring dasturiy ta’minotini ishlab chiqishda qo’llanilgan (Qoraqalpog‘iston Respublikasi Suv xo‘jaligi vazirligining 2022 yil 6 maydagi №03/08-3-148-son ma’lumotnomasi). Ilmiy natijalarni qo‘llash texnologik jarayonda ishlab chiqarish samaradorligini 7-8% oshirish imkonini bergan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 11 ta Ilmiy-amaliy anjumanlarda, jumladan 7 ta xalqaro va 4 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha 26 ta ilmiy ish chop etilgan, shulardan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining falsafa doktori dissertatsiyalari asosiy Ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarda 11 ta maqola, jumladan 5 tasi xorijiy (5 ta scopus) va 6 tasi Respublika jurnallarida chop etilgan. Shuningdek, 4 ta EHM uchun yaratilgan dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, uchta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovadan tashkil topgan. Dissertatsiyaning hajmi 104 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi, tadqiqot maqsadi va vazifalari, tadqiqot ob’ekti va predmeti tavsiflanadi, tadqiqotning respublikada fan va texnologiyalarni rivojlanishining ustuvor yo‘nalishlariga muvofiqligi ko‘rsatiladi. Izlanishning ilmiy yangiligi va amaliy natijalari aniqlangan, olingan natijalarning ishonchliligi asoslangan, olingan natijalarning ilmiy-amaliy ahamiyati ko‘rsatilgan. Natijalar, ularni amaliyotga tatbiq etish, nashr etilgan ishlar va dissertatsiya tuzilishi to‘g‘risida ma’lumotlar berilgan.

Dissertatsiyaning “**Ekotizimlar misolida IoT axborot tizimlarining faoliyat ko‘rsatishi va himoyasi modellari va usullari**” deb nomlangan birinchi bobida IoT texnologiyalari asosida ekologik tizimdagi sensorlar, datchiklar va boshqalardan ma’lumotlarni xavfsiz saqlash va uzatish uchun “internet buyumlari” infratuzilmasining tahlili amalga oshirilgan. “Internet buyumlari” infratuzilmasining

himoyasini oshirish uchun IoT texnologiyalar asosida ekologik tizimdagi tasvirlarni saqlash va uzatishni xavfsiz tashkil etish uchun steganografik kodlash usullari va algoritmlari ishlab chiqilgan.

§1.1-paragrafda IoT texnologiyalari asosida ekologik tizimdagi ma'lumotlarni himoya qilish ob'ektining tavsifi keltirilgan.

§1.2-paragrafda "internet buyumlari" infratuzilmasining himoyasini oshirish maqsadida IoT texnologiyalar asosida ekologik tizimdagi tasvirlarni saqlash va uzatishni xavfsiz tashkil etish uchun steganografik kodlash usullari va algoritmlari ishlab chiqilgan.

Aytaylik I - muqova sirti $R*C$ piksel bilan tasvirlangan matritsa, S -bu x - qiymatli pikselga ega bo'lgan maxfiy xabar bo'lsin, unda I - matritsa (1) ko'rinishda, S - maxfiy xabar (2) ko'rinishda hamda L - xabar uzunligi esa (3) ifoda ko'rinishda tasvirlanadi:

$$I = \{x_{ij} \mid 1 \le i \le R, 1 \le j \le C, x_{ij} \in \{0,1,...,255\}\} \quad (1)$$

$$S = \{S_N \mid 1 \le N \le n, S_N \in \{0,1,...,255\}\} \quad (2)$$

$$L = \{255 * l_w + l_r \mid 0 \le l_w \le 255, 0 \le l_r \le 255\} \quad (3)$$

Aytaylik S - yashirin bo'lishi kerak bo'lgan xabar, E va D lar mos ravishda qo'yish va ekstraktlar (kiritish va chiqarish) algoritmlari, Y' - stego fayli bo'lsin. Qo'yish (kiritish) jarayoni $Y' = E(S, I, L)$ tenglama orqali berilishi mumkin.

Xabar muqova tasviridan quyidagi $X = D(Y', L)$ tenglama yordamida ajratiladi.

Steganografik algoritmning samaradorligi quyidagi ikkita parametr asosida tekshiriladi:

PSNR (signal/shovqin munosabatlar cho'qqisi) va MSE (o'rta kvadratik xatolik). Eng samarali kul rang tasvirni aniqlash usuli quyidagi ifoda orqali berilishi mumkin: $MSE = \frac{1}{R \times C} \sum_{i=1}^{R} \sum_{j=1}^{C} (x_{ij} - x'_{ij})^2$, $PSNR = 10\log[\frac{255^2}{MSE}]$, bu yerda R va C x_{ij} dastlabki ko'rinishda tasvirlangan matritsa o'lchovini, hamda x'_{ij} ko'rinishdagi yashirin tasvirini ifodalaydi.

§1.3-paragrafda, funktsional jadvallar (FJ) asosida ma'lumotlarni kiritish va foydalanuvchini kirishni boshqarish jarayonida sub'ektlar va ob'ektlarning optimal muvofiqligi ta'minlanadi. Algoritmik model quyidagi ko'rinishda ifodalaniladi: $T\Phi = \{S, O, Type, Q, H, L, n, A, B, \Theta, t, U, G, F, P\}$ - bu yerda avtomatlashtirilgan boshqaruv tizimi (АСУ) samarali funktsional axborot tizimi (AT) bilan ta'minlangan, shuningdek FJ asosida AT ga kirish quyidagi parametrlar orqali boshqarilgan: S to'plam $S\{A_j\}$ sub'ektlar to'plami; O to'plam $O\{B_i\}$ ob'ektlar to'plami; A – ma'lum sub'ekt; B – ma'lum ob'ekt; X – ma'lum qoidalar; Θ – «A_i » va «B_i» orasidagi koordinatalar; t – vaqt; $Type$ – sub'ektlar turining to'plami; Q – quduqlar to'plami; H – quduq suvlarining chuqurlik qiymatlari to'plami (metrlarda); L – bir texnik tamonidan bosib o'tgan to'liq yo'li; n – bir texnikga biriktirilgan nazorat quduqlari soni; U – tashqi ta'sir ($\Theta_{ij}\{A_i, B_j\}$); F – o'tish jarayoni; G –graflarning o'tishi (Θ_{ij} dan $\Theta_{i+n, j+m}$ ga o'tish);

M – ruxsat berish (kirish) matritsasi; V – kirish imtiyozlari to‘plami; P – hisoblash va mantiqiy kiritish, chiqarish va boshqarish operatsiyalari.

Qism quduqlari quyidagi bir necha quduqlardan iborat:

$Q=\{\mathrm{Q}_1,\mathrm{Q}_2,\mathrm{Q}_3,\ldots,\mathrm{Q}_m\},\forall \mathrm{Q}_i,Q_j\in Q$ va $i\neq j, Q_i\cap Q_j=\varnothing$, $\|Q\|=m$

bu yerda Q_i qism quduqlarning elementlari bo‘lgan quduqlar va k_i – Q_i qism quduqlarining elementlari soni bo‘lib, quyidagi $Q_i=\{\mathrm{q}_1^i,\mathrm{q}_2^i,\ldots,\mathrm{q}_{k_i}^i\}$, $\forall \mathrm{q}_a,q_b\in Q_i$ ko‘rinishga ega, agar $a\neq b$ bo‘lgan holda $q_a=q_b$ bo‘ladi, $\|Q_i\|=k_i$ ga teng, shuning uchun quduqlarning umumiy soni quyidagi $\sum_{i=1}^{m}k_i=k_1+k_2+k_3+\ldots+k_m$ ko‘rinishda bo‘ladi, D_e – sho‘rlanishiga qarab taqsimlangan yer maydoni, $O=Q\bigcup D_e$, T – texniklar to‘plami ($T=\{\mathrm{T}_1,\mathrm{T}_2,\mathrm{T}_3,\ldots,\mathrm{T}_k\}$)

Quyidagi $F:T\to Q$ akslantirishni ko‘rib chiqamiz. Diskret vaqtdagi FJ ning o‘zgarishi quyidagi shartlarga ko‘ra dinamik holda amalga oshiriladi: agar t_i diskret vaqtda quduqlar soni $\|Q_i\|=n$ ga teng, t_{i+1} diskret vaqtda esa quduqlar soni $\|Q_i\|=n'$ ga teng bo‘lsa hamda agar quduqlar soni o‘z-aro teng bo‘lsa, ya’ni $n=n'$, u holda F_{t_i} FJ dan $F_{t_{i+1}}$ FJ holatiga o‘tiladi.

Dissertatsiyaning “**Tahdidlarni aniqlash va identifikatsiya qilish uchun tanib olish usullari va algoritmlari**” deb nomlangan ikkinchi bobida chekli sonli kesishuvchi sinflar bilan tanib olish masalalarini yechishning algebraik usullari takomillashtirilgan. Har bir Z tanib olish topshirig‘i uchun evristik algoritmlar oilasi bo‘yicha algebra atamalarida to‘g‘ri algoritm, ya’ni har bir sinf bo‘yicha ob’ektlarning cheklangan tanlovini namunasini to‘g‘ri tasniflaydigan algoritm qurilgan.

Yuqorida keltirilgan ishlarda qurilgan, kesishuvchan sinflar bilan bog‘liq topshiriqlar ko‘rib chiqilganligi sababli algoritm yetarli darajada murakkab hisoblanadi. Algoritm tavsifining o‘zi katta xotiradan foydalanishni talab etadi/xotira hajmi proportsional ortadi $q^2\cdot l^2$ – bu yerda q ushbu topshiriqdagi tanib olish ob’ektlari soni, l - sinflar soni. Ma’lum bo‘lishicha, agar faqatgina kesishmaydigan sinflar bilan bog‘liq topshiriqlar ko‘rib chiqilsa, an’anaviy algebraik usullar bilan tavsifiga ko‘ra soddaroq va sezilarli darajada samarali hisoblash algoritmini hosil qilish mumkin.

§2.1-paragrafda kesishmaydigan sinflar bilan tanib olish masalalarini yechish uchun algebraik usullar ko‘rib chiqilgan. Baholarni hisoblash modelining chiziqli tamomlashdan iborat to‘g‘ri modellar taklif etilgan.

§2.2-paragrafda baholarni hisoblash va to‘g‘ri algoritm modelining chiziqli tamomlanishini qurish keltirilgan.

§2.3-paragrafda ob’ektlarni tanib olishning mantiqiy usuli taklif etilgan. Usul sinflarni butun makon bo‘ylab kengayishini belgilovchi, hamma joyda aniqlanmagan mantiqiy funktsiya va xususiyatlarning butun makonida mantiqiy funktsiyaning optimal davomini qurish sifatida mos jadvalni ko‘rib chiqishdan iborat.

Biz bir-biriga mos kelmaydigan $K_1,\ldots,K_l$ sinflari bilan bog‘liq masalani ko‘rib chiqamiz va $J_0\left(K_1,K_2,\ldots,K_l\right)$ ma'lumotlari T_{nml} o‘quv jadvali shaklida berilgan deb hisoblaymiz.

Maqsad, ko‘rib chiqilayotgan baholashlarni hisoblash modelining asosiy operatorlari to‘plamini ajratib ko'rsatish, ularning chiziqli yopilishini qurish va $\breve{S}_q$ tanlanmasidagi har bir $\tilde{K}_j$ sinf ob’ekti uchun ushbu operatorlar yetarlicha katta Γ_j bahosini va $u \neq j$ da etarlicha kichik Γ_u baholarini shakllantirishni isbotlashdan iborat.

Barcha asosiy operatorlar, shuningdek, chiziqli tutashuv operatorlari oshkor ko‘rinishda quriladi.

Aytaylik o‘rganiladigan ma’lumotlar T_{nml} - o’quv jadval shaklida berilgan bo’lsin.

Jadval satrlari $S_1,\ldots,S_m,\ S_i=\left(a_{i1},\ldots,a_{in}\right),\ i=\overline{1,n}$ ob’ektlarining standart tavsiflari bo’ladi.

$S_{m_{j-1}+1},\ldots,S_{m_j},\ m_0=0,\ m_l=m$ ob’ektlar o‘zaro kesishmaydigan $K_j,\ j=\overline{1,l}$ sinfiga tegishli bo‘lsin deb hisoblaymiz.

Agar S satr $K_j,\ j=1,2,\ldots,l$ sinfga tegishli bo‘lsa, unda l - o‘lchovli $P\left(S\right)=j$ predikat kiritamiz, u holda masala P predikat qiymatining $S^1,S^2,\ldots,S^q$ chekli ob’ektlar to‘plami uchun hisobdagi masala uchun o‘rganiladigan ma’lumotlaridan tuzilgan.

$S^1,S^2,\ldots,S^q,\ S^i=\left(b_{i1},\ldots,b_{in}\right),\ j=\overline{1,l},\ \ i=\overline{1,q}$ ob’ektlar yakuniy tanlanmani hosil qiladi, bu erda $S^{q_{j-1}+1},\ldots,S^{q_j}$, $q_0=0,\ q_l=q$ ob’ektlar faqat K_j sinfiga tegishli bo‘ladi.

Quyidagi $\left\{S_1,\ldots,S_m\right\}\cap K_j=K,\ \left\{S_1,\ldots,S_m\right\}\setminus\tilde{K}_j=C\tilde{K}_j,$

$$S^1,\ldots,S^q\cap K_j=K_j^1,\ \left\{S^1,\ldots,S^q\right\}\setminus K_j^1=CK_j^1$$

belgilashlar orqali $B_j,\ j=\overline{1,l}.$ operatorlarni shakllantirish mumkin.

Aytaylik A algoritm l – sinfli Z tanib olish masalani o‘tkazuvchi ixtiyoriy algoritmi, $Z=\left\{J,S^q\right\}$ - esa $\left\|\beta_{ij}\right\|_{q\times l}$ matritsaning natijasi va $A\left(J,S^q\right)=\left\|\beta_{ij}\right\|_{q\times l},\ \beta_{ij}\in\{0,1,\Delta\}$ bo‘lsin. Quyidagi $\beta_{ij}=1,\ \beta_{ij}=0,\ \beta_{ij}=\Delta$ tengliklar esa A algoritm S^i ob’ektlarni K_j sinflarga tegishlilik hisobini inkor etib, mos ravishda $S^i:\ S^i\in K_j,\ S^i\notin K_j$ ob’ekt uchun hisoblaydi.

Bunday algoritmlar Z masala uchun korrekt emas va ixtiyoriy korrekt bo‘lmagan algoritm korrekt dep ataladi.

Teorema 1. Har bir A - algoritmni $A = B \times C$ ko‘rinishda ifodalash mumkin ($\times$ - ko’paytma ketma-ket bajarilishni anglatadi), bu yerda, agar $A(Z) = \|\beta_{ij}\|_{q\times l}$, $\beta_{ij} \in \{0,1,\Delta\}$ bo‘lsa, u holda $B(Z) = \|\alpha_{ij}\|$, $C\left(\|\alpha_{ij}\|_{q\times l}\right) = \|\beta_{ij}\|_{q\times l}$ bo‘ladi.

Teorema 1 har bir A algoritmni ikkita ketma-ket bosqichlarga bo‘lish mumkinligini ko‘rsatadi. 1 - bosqichda Z masala (q,l) - o‘lchamli sonli matritsaga o‘tkaziladi, bu yerda q - matritsa satri bo‘lib ob’ektlarni tanib olishlar soniga teng, l - esa matritsa ustuni bo‘lib sinflar soniga teng.

2 - bosqichda esa sonli matritsaga asosan $S^i,\ldots,S^q$ ob’ektlarning $K_1,\ldots,K_l$ sinflarga mansubligi haqidagi savollarga javoblar shakllantiriladi.

α_{ij} - qiymat tabiiy ravishda $S^i, i = \overline{1,q}$ ob’ektlarning K_j, $j = \overline{1,l}$ sinflarga tegishlilik o’lchovlarining qiymatlari sifatida talqin qilinadi. B - bosqich tanib oluvchi operator, C - esa hal qiluvchi qoida deb ataladi.

Keyinchalik, faqat chegaraviy hal qiluvchi $C^*\left(\|\alpha_{ij}\|_{q\times l}\right) = \|C(a_{ij})\|_{q\times l}$ qoidalar ko’rib chiqiladi.

Qoida elementma-element qo’llaniladi. a - son, shuningdek d_1, d_2 - chegaraviy sonlar va $0 < d_1 < d_2$ bo‘lsin, u holda

$$C^*(a) = \begin{cases} 1, & agar\ \ a > d_2 \\ 0, & agar\ \ a < d_1 \\ \Delta, & agar\ \ d_1 < a < d_2 \end{cases}$$

Operatorlarni tanib oluvchi algebra. Aytaylik $Z = \left(J, \tilde{S}^2\right)$ - l ta sinfli $K_1,\ldots,K_l$ fiksirlangan tanib olish masalasi bo‘lsin, shuningdek $B_i, i = 1,2$ ovozlar matritsasiga ega $B_i(Z) = \|\Gamma^i_{uv}\|_{q\times l}$ ko‘rinishdagi operatorlarni tanib olish bo‘lsin.

So‘ngra

$$(B_1 + B_2)(Z) = \|\Gamma^1_{uv} + \Gamma^2_{uv}\|_{q\times l},$$

$$(B_1 \times B_2)(Z) = \|\Gamma^1_{uv} \times \Gamma^2_{uv}\|_{q\times l},\ (cB)(Z) = \|c\cdot\Gamma\|_{q\times l} \quad i = 1,2$$

operatorlar ustida yig‘indi, ko‘paytirish va songa ko‘paytirishning algebraik amallari kiritiladi.

$\{B\}$ da kiritilgan amallarga nisbatan (B) - algebraik yopilmalar oilasi quyidagi

$$\sum b_{i_1},\ldots,b_{i_k},\ B_{i_1}\cdot B_{i_2}\cdot\ldots\cdot B_{i_k}$$

ko‘rinishdagi operatorli polinomlar sifatida ifodalash mumkin.

Dissertatsiyada $L\{A\}$ chiziqli kengaytmali $L\{B\}\cdot C(d_1,d_2)$ algoritmlar oilasini ko’rib chiqamiz.

Ta'rif 1. $(S^u, j), S^u \in \tilde{S}^q, S^u \in K_j, 1 \le j \le l$ juftlik B operatorda belgilangan dep ataladi, agar barcha $S^r \in \tilde{S}^q$, $S^r \notin K_w$, $w = 1,2,\ldots,l$ satrlar uchun $B_v(Z) = \|a_{tv}\|_{q \times l}$, $a_{uj} \ge 1$, $0 < |a_{rw}| < \delta < 1$ o'rinli bo'lsa.

Teorema 2. Aytaylik biror modellarda $B_1,\ldots,B_w$ operatorlar berilgan bo'lsinki, har bir $\left(S^u, j\right), \breve{S}^u \in K_j$ juftlik kamida bitta B_i, $i = \overline{1, w}$ operator bilan belgilanadi. Shunday $\sum_{i=1}^{n} \alpha_i B_i = \tilde{B} \in \tilde{L}\{\mathrm{B}\}$ chiziqli kombinatsiya topiladiki, $\tilde{A} = \breve{B} \times C$ (bu erda C - chegaraviy hal qiluvchi qoida) algoritm Z masala uchun korrekt (to'g'ri) algoritm bo'ladi.

Teorema 3. Aytaylik $B \in B(j)$ - ixtiyoriy operator va $S = (\alpha_1,\ldots,\alpha_n)$ - ixtiyoriy mumkin bo'lgan ob'ekt bo'lsin. Shuningdek

$$B(\mathrm{S}) = \left(\Gamma_1^j(S),\ldots,\Gamma_j^j(S),\ldots,\Gamma_l^j(S)\right)$$

ifoda quyidagi

$$0 \le \Gamma_t^j(S) < m \cdot n \cdot \varepsilon,\ t = 1,2,\ldots,\ j-1,\ j+1,\ldots,l$$

tengsizlikka ega bo'lsin.

Endi quyidagi (u,v) juflikni ko'rib chiqamiz, bu yerda $1 \le v \le n$, boshqacha qilib aytganda sinflarga tegishli ob'ektlar satrlari $S_u \in \tilde{K}_j$ ni ko'rib chiqamiz.

Bu (u,v) juftlik o'qitish jadvalining a_{uv} elementiga mos keladi.

Quyidagi $\rho_v(a_{uv}, b_{tv})$, $t = \overline{1,q}$ qiymatni, ya'ni S_u ob'ektdagi v - alomatlar masofasini, T_{nml} o'qitish jadvalida S^t ning S^q dagi ushbu alomat qiymatigacha bo'lgan masofasini ko'rib chiqamiz.

$\tilde{S}^q$ dagi ob'ektlarni tartiblaymiz, bu erda $\tilde{S}^q = \left\{S^1,\ldots,S^q\right\}$ satr $p_v(a_{uv}, b_{uv})$, $t = \overline{1,q}$ qiymatlarning o'sishi bo'yicha, ob'ektlar esa ixtiyoriy tarzda o'zaro element miqdori bilan tenglashtirilgan.

Quyidagi tariblangan satrlarni olamiz:

$$S^{r_1}, S^{r_2},\ldots,S^{r_i},\ldots,S^{r_q}\ 0 \le \rho_v\left(a_{uv}, b_{r_1 v}\right) \le \rho\left(a_{uv}, b_{r_2 v}\right) \le \ldots \le \rho_v\left(a_{uv}, b_{r_i v}\right) \le \rho\left(a_{uv}, b_{r_q v}\right).$$

Agar ob'ektlar K_j sinfga tegishli bo'lsa «+» belgisini, aks holda esa «-» belgisi bilan almashtirib yozib chiqamiz.

Natijada, masalan quyidagi ko'rinishdagi ketma-ketliklarni hosil qilamiz:

$$S^{+r_1}, S^{+r_2}, S^{-r_3}, S^{-r_4}, S^{+r_5},\ldots,\ \text{va h.k.}$$

Ta'rif 2. (u,v) juftlik statsionar deb ataladi, agar qurilgan «+, -» belgilar ketma ketligida bir o'zgaruvchi belgiga teng va elementlarda belgining $S^{r_i}, S^{r_{i+1}}$ o'zgarishi sodir bo'lib, $p_v\left(a_v, b_{r_i, v}\right) < p_v\left(a_{uv}, b_{r_{i+1}, v}\right)$ bajarilsa.

Teorema 4. Agar Z masalada har bir $j=\overline{1,l}$ raqam uchun statsionar juftlik mavjud bo‘lsa, u holda $A=\left(\left(C_1+C_2\right)\sum_{i=1}^{l}B^i\right)\cdot\left(C\left(C_1,C_2\right)\right)$ algoritm Z masala uchun korrekt (to‘g‘ri) bo‘ladi.

Optimal korrektorni tanib olish va qurishning mantiqiy usuli. Korrektorni qurishda quyidagicha mantiqiy usul shakllantiriladi – K_1,K_2 sinflari bilan kesishmaydigan ob’ektlarni tasniflovchi K - qiymatli mantiqning hamma yerda ham belgilanmagan optimal davomi.

Agar o‘qituvchi ma’lumot jadval $T_{n,m}^2$ ko‘rinishida taqdim etilgan bo‘lsa, barcha $\left(\tilde{\alpha},\tilde{\beta}\right)$ juftliklarga mos $\tilde{\gamma}$ to‘plamli $\tilde{T}$ jadval ko‘rib chiqiladi, bu yerda $\gamma_i=\begin{cases}1,\text{agar }\alpha_i\neq\beta_i\\0,\text{agar }\alpha_i=\beta_i\end{cases}$ ga teng bo‘lgan $\tilde{\alpha}\in K_1,\tilde{\beta}\in K_2$.

Ko‘rinib turibdiki, T intervallarini birlashtirish to‘plamlaridagi j qiymatni qabul qiluvchi va $F(\tilde{x})$ funktsiyaning davomi hisoblangan $a_{i_1}=b_{i_1},a_{i_2}=b_{i_2},\ldots,a_{i_k}=b_{i_k}$ ga ega $T_{n,m}^2$ jadvalning K_i sinfidan $\left(b_1,b_2,\ldots,b_n\right)$ topiladigan $\left(a_1,a_2,\ldots,a_n\right)$ to‘plamlarda i qiymatli qabul qiluvchi F^1 funktsiyasi.

Shu tarzda $F\left(x_1,x_2,\ldots,x_n\right)$ funktsiyasining optimal mantiqiy davomini quyidagicha shakllantirish mumkin.

1. T jadvalini shakllantirish.
2. “мин-max” (minimal normalarga ega ustunlar va maksimal birliklar soniga ega satrlarni tanlash) usuli yordamida qaytarilmas $\Pi_1,\ldots,\Pi_l$ satrli T ustunlar quriladi.
3. Har bir $\Pi_t,t=1,2,\ldots,l$ uchun F funktsiyasining ikkita F_t',F_t'' davomi quriladi:
4. Keltirilgan ob’ektlarning nazorat jadvali bo‘yicha F funktsiyasining har bir davomi uchun qoplash foizi aniqlanadi. Nazorat jadvalidagi ob’ektlarni qoplashning maksimal foizi bilan davom etish tanlanadi.

Algoritmning murakabligi elementar qadamlarning soni bilan ifodalanadi. Ko‘rinib turibdiki, $\tilde{T}$ shakllantirish uchun nm_1m_2 elementar qadamlar talab etiladi, bu yerda m_1 - K_1 dagi ob’ektlar soni, m_2 esa K_2 sinfidagi ob’ektlar soni. “min-max” usuli yordamida T satrlarning ustunlar bilan qaytarilmas qoplanishi quriladi. Buning uchun $m_1m_2n\left(m_1m_2+2\right)$ qadamlar zarur.

Keyingi bosqichda m_2 satrli va $2]\log m_1m_2\left(+\right)\log n[+4$ ustundan tashkil topgan jadval shakllantiriladi. Buning uchun $\left(2]\log m_1m_2\left(+\right)\log n[+4\right)m_1m_2$ qadam talab etiladi. Ko‘rish mumkinki, “min-max” algoritmi uchun $m_1m_2\left(m_2+2\right)\left(2]\log m_1m_2\left(+\right)\log n[+4\right)$ qadam mavjud. Shunga ko‘ra, algoritmning murakkabligi quyidagiga teng:

$$m_1 m_2 \left\{ n\left(m_1 m_2 + 3\right) + \left(m_2 + 3\right)\left(2\right]\log m_1 m_2 \left(+\right)\log n[+4\right)\right\}$$

Dissertatsiyaning “**Ekotizimlar misolida IoT axborot tizimining faoliyat ko‘rsatishi va himoyasi modellari va usullarini dasturiy tashkil etish**” deb nomlangan uchinchi bobida ekotizimda steganografik kodlash va identifikatsiya algoritmlarini tashkil etish taklif etilgan.

§3.1-paragrafda mikrokontrollerlar va dasturlanadigan mantiqiy kontrollerlarni CAD tizimlari bazasida diz’yunktiv normal shakllar sinfida bul funksiyalari asosida tasvirlarni saqlash va uzatishni xavfsiz tashkil etish uchun steganografik kodlash algoritmlarini mantiqiy avtomat tarzda tashkil etish taklif etilgan.

LSB usulining kodlash algoritmi algebraik ko‘rinishga quyidagicha o‘tkaziladi:

$Y_0 = 1;\quad Y_1 = 1;\quad Y_2 = X_1 X_2;\quad Y_3 = \overline{X_1};\quad Y_4 = \overline{X_1};\quad Y_5 = \overline{X_1} X_3;\quad Y_6 = \overline{X_1}\,\overline{X_3};$

$Y_7 = \overline{X_1}\,\overline{X_3} X_4 X_5;\quad Y_8 = \overline{X_1}\,\overline{X_3}\,\overline{X_4};\quad Y_9 = \overline{X_1}\,\overline{X_3}\,\overline{X_4} X_6 X_7;\quad Y_{10} = \overline{X_1}\,\overline{X_3}\,\overline{X_4} X_6 \overline{X_7} X_8;$

$Y_{11} = \overline{X_1}\,\overline{X_3}\,\overline{X_4} X_6 \overline{X_7}\,\overline{X_8};\quad Y_{12} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,\overline{X_6};\quad Y_{13} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,\overline{X_6} X_9;$

$Y_{14} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,\overline{X_6}\,\overline{X_9};\ Y_k = \overline{X_1}\,\overline{X_3}\,\overline{X_4} X_5 \overline{X_6} \vee; \overline{X_1}\,\overline{X_3} X_4 \overline{X_5}$

LSB usulining kodlashining GSA ga mos mikrokomandalarning matritsa ko‘rinishidagi sxemasi:

$Y_0 = Y_1;$

$Y_1 = X_1 X_2 Y_2 \vee \overline{X_1} Y_3;$

$Y_2 = X_1 X_2 Y_2 \vee \overline{X_1} Y_3;$

$Y_3 = Y_4;\quad Y_5 = Y_4;$

$Y_4 = X_3 Y_5 \vee \overline{X_3} Y_6;$

$Y_6 = X_4 X_5 Y_7 \vee \overline{X_4} Y_8;$

$Y_7 = X_5 Y_7;$

$Y_8 = X_6 X_7 Y_9 \vee X_6 \overline{X_7} X_8 Y_{10} \vee X_6 \overline{X_7}\,\overline{X_8} Y_{11} \vee \overline{X_6} Y_{12};$

$Y_9 = X_6 X_7 Y_9 \vee X_6 \overline{X_7} X_8 Y_{10} \vee X_6 \overline{X_7}\,\overline{X_8} Y_{11} \vee \overline{X_6} Y_{12};$

$Y_{10} = X_6 X_7 Y_9 \vee X_6 \overline{X_7} X_8 Y_{10} \vee X_6 \overline{X_7}\,\overline{X_8} Y_{11} \vee \overline{X_6} Y_{12};$

$Y_{11} = X_6 X_7 Y_9 \vee X_6 \overline{X_7} X_8 Y_{10} \vee X_6 \overline{X_7}\,\overline{X_8} Y_{11} \vee \overline{X_6} Y_{12};$

$Y_{12} = X_9 Y_{13} \vee \overline{X_9} Y_{13};$

$Y_{13} = X_9 Y_{13} \vee \overline{X_9} Y_{13};$

$Y_{14} = Y_k;$

El Gamal assimetrik shifrlash algoritmining algebraik shakliga o'tkazish quyidagicha amalga oshiriladi:

$Y_0 = Y_1 = 1 \qquad Y_2 = x_1 \qquad Y_3 = x_2$

$Y_4 = x_1 x_3 \qquad Y_5 = \overline{x}_1 \overline{x}_3 \overline{x}_4 \qquad Y_6 = \overline{x}_1 \overline{x}_3 \overline{x}_4 \overline{x}_5$

$Y_7 = \overline{x}_1 \overline{x}_3 \overline{x}_4 \overline{x}_5 \qquad Y_8 = \overline{x}_1 \overline{x}_3 \overline{x}_4 \overline{x}_5 \overline{x}_6 \qquad Y_K = \overline{x}_1 \overline{x}_3 \overline{x}_4 \overline{x}_5 \overline{x}_6$

El Gamal assimetrik shifrlash algoritmining GSA ga mos keladigan mikrokomanda matritsa sxemasi quyidagicha yaratilgan:

$Y_0 = Y_1 \qquad Y_1 = \overline{x_1} x_3 Y_1 \vee x_1 Y_2 \vee \overline{x_1}\,\overline{x_3} Y_4 \qquad Y_2 = Y_1$

$Y_3 = Y_2 \qquad Y_4 = x_4 Y_4 \vee \overline{x_4} Y_5 \qquad Y_5 = x_5 Y_4 \vee \overline{x_5} Y_6$

$Y_6 = Y_7 \qquad Y_7 = x_6 Y_7 \vee \overline{x_6} Y_8 \qquad Y_8 = Y_k$

§3.2-paragrafda IoT texnologiyalari asosida Orol mintaqasi ekotizimida identifikatsiya qilish muammolarini yechish uchun baholarni hisoblashga asoslangan modelni tashkil etish keltirilgan. Ushbu paragrafda faqatgina $A = B \times C$ ko‘rinishda taqdim etilgan algoritmlar ko‘rib chiqilgan, bu yerda B - algoritmning salmoqli qismi hisoblangan ixtiyoriy aniqlovchi operator; hal etuvchi operator – C

– barcha uchun standart hisoblangan algoritm va dasturlardan tashkil topgan bo‘lishi mumkin.

Har qanday ovoz berishni aniqlovchi operator Z topshirig‘ini ovozlarni raqamli matritsasida yoki $B(Z)=\|\Gamma_{ij}\|_{q\times l}$, $\Gamma_{ij}=\Gamma_j(S^i)$ baholarida aks ettiradi.

Agar $\left(\tilde{\alpha}-\tilde{\beta}\right)=\sum_{i=1}^{6}\sum_{j=1}^{10}|\alpha_i-\beta_i|\to\min$. α_i - datchik ma’lumotlari, β_j - sho‘rlanganlik sinfi parametrlari. Datchik ma’lumotlari: HCO_3 (gidrokarbonat), Cl (xlor), SO_4 (sulfat kislota), Ca (kaltsiy), Mg (magniy), Na (natriy). Sho‘rlanish 5 ta sinfga ajratiladi (sho‘rlanmagan, kam sho‘rlangan, o‘rtacha sho‘rlangan, yuqori sho‘rlangan, juda yuqori sho‘rlangan) va har bir sinf 10 ta banddan iborat.

Agar datchikdan α_i ma’lumotlari kelsa va u $a_i-b_i\to\min$ qiymatini tekshirganda berilgan shart bajarilsa va qaysi sho‘rlanish sinfiga mansubligini ko‘rsatib beradi. Agar qiymat $a_i-b_i\to\min$ teng bo‘lsa, ya’ni bir nechta sho‘rlanish sinfiga mos bo‘lsa, u holda ma’lumot ushlab qolingan hisoblanadi.

Baholarni hisoblash algoritmi asosida elektron resurslarda axborot xavfsizligi tahdidlarining taqqoslama tasnifi muammolarini yechish uchun to‘g‘ri algoritmdan foydalanilgan:

$$A=\left(\sum_{i=1}^{e}\sum_{S^t\in K_j}B(S^t)C(C_1,C_2)\right)$$

§ 3.3-paragrafda internet buyumlari texnologiyalarini ekologiyada (Orol bo‘yi misolida) tizim sifatida qo‘llash taklif etilgan. Tizim veb-sayt ko‘rinishida ishlab chiqilgan. Tizimning server qismini ishlab chiqishda Django freymvorki, GUI uchun Quasar freymvorki yordamida bir tomonlama ilova (SPA) sifatida mijoz qismi Vue js qo‘llanilgan. Tizimni ishga tushirish uchun zamonaviy brauzerlardan birida quyidagi saytni ecoaral.uz ochish zarur. Shundan so‘ng brauzer sahifasida tizimning bosh oynasi aks etadi.

XULOSA

IoT texnologiyalari asosida ekologik tizimdagi axborotni himoya qilish ob’ekti tavsifi va ekologik tizimda IoT texnologiyalari asosida sensorlar, datchiklar va h.k.lardan ma’lumotlarni uzatish va saqlashni xavfsiz tashkil etish uchun “internet buyumlari” infratuzilmasi tahlil qilindi;

internet buyumlari infratuzilmasining himoyasini oshirish shuningdek, IoT texnologiyalari asosida ekologik tizimdagi tasvirlarni saqlash va uzatishni xavfsiz tashkil etish uchun steganografik kodlash usullari va algoritmlarini ishlab chiqildi;

baholarni hisoblash va to‘g‘ri algoritm modelini chiziqli tamomlovchi to‘g‘ri model asosida kesishmaydigan sinflar bilan tanib olish muammolarini hal qilish uchun algebraik usul ishlab chiqildi;

mos jadvallarni ko‘rib chiqish asosida ob’ektlarni tanib olishning mantiqiy usulini sinflarni butun makon bo‘ylab kengayishini belgilovchi, hamma joyda aniqlanmagan mantiqiy funksiya va xususiyatlarning butun makonida mantiqiy funksiyaning optimal davomini qurish va har doim ham aniq bo‘lmagan mantiqiy funksiyasi ishlab chiqildi;

mikrokontrollerlar va dasturlanadigan mantiqiy kontrollerlarni CAD loyihalashtirish tizimlari bazasida diz’yunktiv normal shakllar sinfida bul funksiyalari asosida tasvirlarni saqlash va uzatishni xavfsiz tashkil etish uchun steganografik kodlash algoritmlarini mantiqiy avtomat tarzda tashkil etish amalga oshirildi;

internet buyumlari texnologiyasini ekologiyada qo‘llash asosida Orol mintaqasi ekotizimida identifikatsiya masalalarini hal etish uchun baholashni hisoblashga asoslangan modelni amalga oshirish taklif etildi.

НАУЧНЫЙ СОВЕТ DSc.03/30.12.2019.FM.01.02
ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ ПРИ
НАЦИОНАЛЬНОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

САЙМАНОВ ИСЛАМБЕК МИРЗАБАЕВИЧ

АЛГОРИТМИЧЕСКИЕ И ЛОГИЧЕСКИЕ МЕТОДЫ ОБРАБОТКИ И ЗАЩИТЫ ЭКОЛОГИЧЕСКИХ ДАННЫХ

05.01.05 – Методы и системы защиты информации. Информационная безопасность

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА ФИЛОСОФИИ (PhD)
ПО ФИЗИКО-МАТЕМАТИЧЕСКИМ НАУКАМ

Ташкент-2023

Тема диссертации доктора философии (PhD) по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2022.2.PhD/FM739.

Диссертация выполнена в Национальном Университете Узбекистана имени Мирзо Улугбека.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице Научного совета (http://ik-fizmat.nuu.uz) и на Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Кабулов Анвар Василович** доктор техническим наук, профессор
Официальные оппоненты:	**Абдурахимов Бахтиёр Файзиевич** доктор физико-математических наук, профессор
	Саидов Абдусобиржон Абдурахмонович доктор техническим наук, профессор
Ведущая организация:	**Каракалпакский государственный университет имени Бердаха**

Защита диссертации состоится «____» _____2023 года в ____ часов на заседании Научного совета DSc.03/30.12.2019.FM.01.02 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-12-24, факс: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за №____). (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 246-02-24).

Автореферат диссертации разослан «____» _____2023 года.
(протокол рассылки №_____ от «____» _____2023 года).

М.М.Арипов
Председатель Научного совета по присуждению ученых степеней, д.ф.-м.н., профессор

З.Р.Рахмонов
Ученый секретарь Научного совета по присуждению ученых степеней, д.ф.-м.н.

Г.У.Жураев
Председатель Научного семинара при научном совете по присуждению ученых степеней, д.ф.-м.н.

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В мире особое внимание уделяется к использованию в различных отраслях информационных технологий, в особенности в сфере применения их в государственном управлении и системе самоуправления, актуальной проблемой является применение технологий и методов обеспечения конфиденциальности информации при предоставлении физическим и юридическим лицам различных государственных интерактивных услуг, расширение возможностей интеграции хозяйственных систем в мировом масштабе. Согласно новому прогнозу Международной корпорации данных (IDC), в 2025 году будет подключено 41,6 миллиарда подключенных IoT-устройств или «вещей», генерирующих 79,4 зетабайта (ZB) данных. Многими странами мира, в том числе США, Европы, Азии и СНГ, а также арабских стран проводятся научные исследования по обеспечению комплексной защиты информации.

В настоящее время проведённый анализ публикаций последних лет свидетельствует о необходимости разработки моделей и методов защиты информационных систем IoT на примере экосистем основанных на комплексном подходе по цифровым технологиям. Основные функции системы управления информационной безопасностью экосистем должны состоять в оценке степени критичности ситуации, связанной с нарушением информационной безопасности экосистемы, оценке уровня риска нарушения информационной безопасности и в поддержке принятия решения относительно действий в данной ситуации. Другими словами, основная проблема заключается в зачастую неполных и неопределенных исходных данных о состоянии системы защиты информации, возможных угрозах, дестабилизирующих факторах.

В Республике Узбекистан наибольшее внимание уделяется современным направлениям защиты информации, требующим научного и практического применения фундаментальных наук. В частности, особая значимость придается созданию защищенных систем передачи и обработки информации, базирующейся на достижениях в области криптографии и системы разработки алгоритмов. Наряду с этим выполняется работы, направленные на определение основных задач по проведению на уровне международных стандартов научных исследований по приоритетным направлениям «Прикладная математика и математическое моделирование». Проведение научных исследований на уровне международных стандартов по приоритетным направлениям «Функциональный анализ, алгебра, дифференциальные уравнения, математическая физика, математическое моделирование, вычислительная математика и дискретная математика, теория вероятностей и математическая статистика» является одной из основных задач Института математики им. В.И.Романовского при Академии наук Республики Узбекистан. Для обеспечения ее реализации важное значение имеет разработка алгоритмических и логических методов обработки и защиты экологических данных в системе IoT для реализации алгоритмов

стеганографии, идентификации и распознавания образов на основе граф-схем алгоритмов и систем функций алгебры логики.

Настоящее диссертационное исследование в определенной степени служит выполнению задач, определенных в Указах Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-60 от 28 января 2022 г. «О Стратегии развития Нового Узбекистана на 2022–2026 годы», Постановлениях Президента Республики Узбекистан №ПП-2789 от 17 февраля 2017 г. «О мерах по дальнейшему совершенствованию деятельности Академии наук, организации, управления и финансирования научно-исследовательской деятельности», №ПП-2909 от 20 апреля 2017 г. «О мерах по дальнейшему развитию системы высшего образования», №ПП-3682 от 27 апреля 2018 г. «О мерах по дальнейшему совершенствованию системы практического внедрения инновационных идей, технологий и проектов», а также в других нормативно-правовых документах, принятых в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Настоящая работа выполнена в соответствии с приоритетным направлением развития науки и технологий Республики Узбекистан IV. «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. Проведённый анализ научно-исследовательских работ и литературных источников по теоретическим и практических задачам создания моделей и методов функционирования и защиты информационных систем IoT на примере экосистем и алгоритмических и логических методов обработки и защиты экологических данных для реализации алгоритмов криптографии, стеганографии, идентификации и распознавания образов а также логических, математических решений методов обеспечения защиты конфиденциальных экологических данных были рассмотрены в работах следующих ученых: L. Zhou, M. Pavanil, S. Goel, R. Nagalakshmi, J. Ahamed, Bento A. Ganzaga, O.Y. Abdulhammed, R. Mohandas, Ю.И. Журавлев, О. Евсютин, А. Шелупанов, А. Тихомиров, В.В. Мельников, С.С. Корт, А.Г. Корченко, И.В. Котенко, М.В. Степашкин и др.

Существенный вклад в развитие теории и практики информационной безопасности экосистем внесли G. Fischer, И.И. Быстров, В.А. Герасименко, О.Ю. Гаценко, А.А. Грушо, В.С. Заборовский, П.Д. Зегжда, Д.П. Зегжда, В.А. Конявский, А.А. Малюк, А.А. Молдовян, Л.Г. Осовецкий, В.П. Шерстюк, А.Ю. Щербаков и др. За последние несколько лет указанными авторами было проделано много работы по изучению вопросов безопасности и конфиденциальности приложений и устройств IoT как с технической, так и с законодательной точек зрения.

В Узбекистане рассматриваемая проблема разрабатывается научными школами, созданными под руководством ведущих учёных Т.Ф.Бекмуродова, М. Арипова, Б.Ф.Абдурахимова, С. Ганиева, Х.А. Музаффарова, Ғ.Туйчиева, А.А.Саидова, Н.А.Игнатьева и других, которые внесли большой вклад в

разработку алгоритмов и моделей обеспечения безопасности информации и конфиденциальности данных.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного исследовательского учреждения, где выполнена диссертация. Диссертация выполнена в соответствии с планом научных исследований Национального университета Узбекистана в рамках научно-исследовательских проектов Ф3-201906117 «Программное обеспечение проведения мониторинга определения влияния экологической ситуации на сельскохозяйственное производство Приаралья» (2020-2022 гг.), Ф-ОТ-2021-248 «Разработка интеллектуальных методов и технологий обнаружения, идентификации и обезвреживания угроз при обеспечении защиты информации на основе таблиц функционирования» (2021-2022гг.) и AL-18245120 - Интеллектуальные методы и технологии обработки и защиты потоков экологических данных, вырабатываемые IoT - устройствами на примере Аральского региона (2022-2023 гг.).

Целью исследования является разработка алгоритмических и логических методов обработки и защиты экологических данных в системе IoT для реализации алгоритмов стеганографии, идентификации и распознавания образов на основе граф-схем алгоритмов и систем функций алгебры логики.

Задачи исследования:

исследовать описания объекта защиты информации в экологической системе на основе IoT технологий и анализ инфраструктуры «интернета вещей» для безопасной реализации хранения и передачи информаций от сенсоров, датчиков и т.п. в экологической системе на основе IoT технологий;

разработать алгоритмическую модель на основе таблиц функционирования (ТФ) для обеспечения оптимальной совместимости субъектов и объектов в процессе ввода данных и управления доступом пользователей;

разработать методы и алгоритмы стеганографического кодирования для безопасной реализации хранения и передачи изображений в экологической системе на основе IoT технологий;

разработать алгебраический метод решения задач распознавания с непересекающимися классами на основе корректной модели из линейного замыкания модели вычисления оценок и корректного алгоритма;

разработать логический метод распознавания объектов на основе рассмотрения эталонной таблицы как невсюду определенной логической функции и построении оптимального продолжения логической функции на всю пространство признаков, что определяет расширение классов на все пространство;

реализовать алгоритмы стеганографического кодирования и ассиметричного шифрования El Gamal для безопасного хранения и передачи изображений на основе булевых функций в классе дизъюнктивных нормальных форм на базе микроконтроллеров и системы CAD проектирования программируемых логических контроллеров;

реализовать модели вычисления оценок для решения задачи

идентификации в экосистеме Аральского региона на основе применения технологий интернета вещей в экологии.

Объектом исследования являются встроенные системы управления, идентификации, обработки и защиты экологических данных, вырабатываемых IoT – устройствами.

Предметом исследования являются алгоритмические автоматные модели, стеганографические алгоритмы и таблицы функционирования защиты информации, булевые таблицы и функции алгоритмов стеганографии.

Методы исследования. При исследованиях применялись методы системного анализа, теории автоматов, теория оптимального управления, алгоритмические модели и средства, алгоритмы, методы обеспечения конфиденциальности информационных ресурсов, построения управляющих мониторов, имитационного моделирования, сетей Петри, алгебры и математической логики, распознавания образов.

Научная новизна исследования заключается в следущем:

разработана алгоритмическая модель на основе исследования алгоритмических принципов и синтеза таблиц функционирования для обеспечения оптимальной совместимости субъектов и объектов в процессе ввода данных и управления доступом пользователей;

разработан логический автоматный метод стеганографического кодирования для безопасной реализации хранения и передачи изображений на основе булевых функций в классе дизъюнктивных нормальных форм на базе микроконтроллеров и системы CAD проектирования программируемых логических контроллеров;

разработаны алгебраический и логический методы решения задач распознавания с непересекающимися классами на основе корректной модели из линейного замыкания алгоритмов вычисления оценок и построения оптимального продолжения логической функции на всё пространство признаков;

доказана полиномиальная сложность алгоритма логического распознавания для идентификации, обработки и защиты изображений в системе IoT;

доказана корректность алгоритма алгебраического распознавания для идентификации, обработки и защиты экологических данных в системе IoT.

Практическая результаты исследования заключается в следующем:

разработан программно-технический комплекс экосистем для применения IoT технологии для информационных систем управления и безопасности на основе таблиц соответствия между объектом и субъектом экосистемы, построено логическое отношение в виде логических формул, реализующих булевые таблицы граф-схем алгоритмов стеганографии.

предложена модель вычисления оценок для решения задачи идентификации в экосистеме Аральского региона на основе применения технологий интернета вещей в экологии;

реализован алгоритм стегонаграфии и ассиметричного шифрования El Gamal на основе граф-схем алгоритмов и оптимальных булевых функций в классе дизъюнктивных нормальных форм.

Достоверность результатов исследования. Достоверность результатов исследования обосновывается строгой формализацией проблемы комплексной защиты информации на основе унифицированного и стандартного описания процесса защиты, использованием теоретически и практически обоснованных способов алгоритмизации сложных систем, автоматных моделей, булевых функций, встроенных микропроцессорных систем для представления криптоалгоритмов и стегоалгоритмов.

Научная и практическая значимость результатов исследования.

Научная значимость результатов проведенных исследований заключается в развитии алгоритмов идентификации алгебраическими и логическими методами распознавания процесса защиты агрегативных систем, автоматных моделей и методов создания встроенных IoT экосистем функционирования и обеспечения безопасности, построения оптимального представления алгоритмов стеганографии на основе логических формул булевых функций.

Практическая значимость результатов исследования заключается в возможности создания IoT экосистем, оптимального представления криптосистем и криптоалгоритмов на основе дизъюнктивных нормальных форм булевых функций, реализующих граф-схемы криптоалгоритмов информационной безопасности и криптографии.

Внедрение результатов исследования. На основании разработанных методов и моделей обеспечения конфиденциальности информационных ресурсов интерактивных услуг в управлении информационных систем были внедрены в ряде хозяйствующих субъектов:

оптимальная математическая модель алгоритма стеганографии была использована для анализа и записи функциональных форм микрокоманд при записи на микроконтроллеры в проекте Uzb-Ind-2021-94 «Энергоэффективность и поток данных в умном городе с использованием инфраструктуры IoT на основе CRN» (справка Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий от 25 мая 2022 года №1596-15/01). Использование научных результатов позволило оптимально реализовать микроконтроллер и проанализировать стеганографический алгоритм;

метод и средство интерактивного анализа воды и почвы использовались при разработке программного обеспечения для мониторинга определения влияния условий окружающей среды по результатам интерактивного анализа воды и почвы в сельском хозяйстве Приаралья (справка Министерство водного хозяйства Республики Каракалпакстан, от 6 мая 2022 года №03/08-3-148). Применение научных результатов позволило повысить эффективность производства в технологическом процессе на 7-8%.

Апробация результатов работы. Результаты данного исследования обсуждались на 11 научно-практических конференциях, в том числе 7 международных и 4 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По основным результатом исследования опубликовано всего 26 научных работ, из них 11 входят в перечень научных изданий, предложенных Высшей аттестационной комиссией Республики Узбекистан для защиты диссертаций доктора философии, из них 5 опубликована в зарубежных журналах (в базе Scopus) и 6 в республиканских научных изданиях. А также получены 4 свидетельства регистрации программных продуктов, созданных для ЭВМ.

Структура и объем диссертации. Структура диссертации состоит из введения, трёх глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 104 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обоснованы актуальность и востребованность темы диссертации, сформулированы цель и задачи исследования, охарактеризованы объект и предмет исследования, раскрыто соответствие исследования приоритетным направлениям развития науки и технологий республики, определены научная новизна и практические результаты исследования, обоснована достоверность полученнных результатов, показаны научная и практическая значимость полученных результатов, внедрение их в практику, даны сведения по опубликованным работам и структуре диссертации.

В первой главе диссертации под названием «**Модели и методы функционирования и защиты информационных систем IoT на примере экосистем**» проведен анализ инфраструктуры «интернета вещей» для безопасной реализации хранения и передачи информаций от сенсоров, датчиков и т.п в экологической системе на основе IoT технологий. Разработаны методы и алгоритмы стеганографического кодирования для безопасной реализации хранения и передачи изображений в экологической системе на основе IoT технологий для повышения защиты инфраструктуры «интернета вещей».

В §1.1-параграфе дано описание объекта защиты информации в экологической системе на основе IoT технологий.

В §1.2-параграфе для повышения защиты инфраструктуры «интернета вещей» разработаны методы и алгоритмы стеганографического кодирования для безопасной реализации хранения и передачи изображений в экологической системе на основе IoT технологий.

Пусть I будет изображением обложки из $R*C$ пикселей, S - секретным сообщением, x-значением пикселя, тогда матрица изображения может быть представлена как (1), и S как (2)

$$I = \{x_{ij} \mid 1 \le i \le R, 1 \le j \le C, x_{ij} \in \{0,1,...,255\}\} \quad (1)$$

$$S = \{S_N \mid 1 \le N \le n, S_N \in \{0,1,...,255\}\} \quad (2)$$

$$L = \{255 * l_w + l_r \mid 0 \le l_w \le 255, 0 \le l_r \le 255\} \quad (3)$$

Пусть S - это сообщение, которое должно быть скрыто, L - длина сообщения (3), E и D - алгоритмы вставки и извлечения соответственно, а Y'

- файл стего. Процесс вставки может быть задан следующим уравнением $Y' = E(S, I, L)$.

Сообщение отделяется от изображения обложки с помощью следующего уравнения $X = D(Y', L)$.

Эффективность стегонаграфического алгоритма проверяется на основе двух параметров: PSNR (пиковое отношение сигнал/шум) и MSE (среднеквадратичная ошибка). Наиболее эффективный метод оттенков серого должен быть определен: $MSE = \frac{1}{R \times C} \sum_{i=1}^{R} \sum_{j=1}^{C} (x_{ij} - x'_{ij})^2$; $PSNR = 10 \log[\frac{255^2}{MSE}]$, где R и C представляют размеры матрицы изображений, x_{ij} - исходное изображение, а x'_{ij} - изображение стего.

В §1.3-параграфе на основе таблиц функционирования (ТФ) обеспечивается оптимальная совместимость субъектов и объектов в процессе ввода данных и управления доступом пользователей.

Предлагается алгоритмическая модель **ТФ = {S, O,Type, Q, H, L, n, A, B, Θ, t, U, G, F, P}** – АСУ обеспечении эффективного функционирования ИС, а также управления доступа к информационной системе на основе ТФ:

S – множество субъектов S $\{A_j\}$; **O** – множество объектов O $\{B_i\}$; **A** – определенный субъект; **B** – определенный объект; **X** – определение прав; **Θ** – координаты между «A_i» и «B_i»; **t** – время; **Type** – множество типов субъектов; **Q** – подмножество скважин; H – набор значений глубины воды в скважинах (в метрах); L – полный путь, пройденный одним техником; n – количество наблюдательных скважин, закрепленных за одним техником; **U** – внешнее воздействие (на $\Theta_{ij}\{A_i, B_j\}$); **F** – процесс перехода; **G** –переходы графа (переход с одной Θ_{ij} на другую $\Theta_{i+n,\ j+m}$); **M** – матрица доступа; **V** – набор привилегий доступа; **P** – вычислительные и логические операции ввода, вывода и управления.

Подмножество скважин состоит из нескольких скважин:

$Q = \{Q_1, Q_2, Q_3, \ldots, Q_m\}, \forall Q_i, Q_j \in Q$ и $i \neq j, Q_i \cap Q_j = \varnothing$, $\|Q\| = m$;

Здесь приведены скважины, которые являются элементами подмножества Q_i и k_i – число элементов Q_i: $Q_i = \{q_1^i, q_2^i, \ldots, q_{k_i}^i\}, \forall q_a, q_b \in Q_i$ и когда $a \neq b$ состояние не $q_a = q_b$ существует. $\|Q_i\| = k_i$, поэтому общее число скважин имеет вид: $\sum_{i=1}^{m} k_i = k_1 + k_2 + k_3 + \ldots + k_m$, D_e – множество земель, распределенных на основе их засоленности, $O = Q \cup D_e$, T – множество техников ($T = \{T_1, T_2, T_3, \ldots, T_k\}$);

Рассматривается следующее отображение $F : T \to Q$. Изменение таблицы функционирования в дискретные моменты времени производится динамически на основе следующих условий: если в дискретные моменты времени t_i имеет место $\|Q_i\| = n$, в дискретные моменты времени t_{i+1} имеет

место $\|Q_i\| = n'$ и если $n = n'$, то из F_{t_i} таблица функционирование переходит в состояние $F_{t_{i+1}}$.

Во второй главе диссертации «**Методы и алгоритмы распознавания для обнаружения и идентификация угроз**» были развиты алгебраические методы решения задач распознавания с конечным числом непересекающихся классов. Для каждой задачи Z распознавания в терминах алгебры над семействами эвристических алгоритмов был построен корректный алгоритм, т.е. алгоритм правильно классифицирующий заданную конечную выборку объектов по каждому из классов.

В §2.1 рассматриваются алгебраические методы для решения задач распознавания с непересекающимися классами. Предлагаются корректные модели из линейного замыкания модели вычисления оценок.

В §2.2 дается построение линейного замыкания модели вычисления оценок и корректного алгоритма.

В §2.3 предлагается .логический метод распознавания объектов. Метод состоит в рассмотрении эталонной таблицы как невсюду определенной логической функции и построении оптимального продолжения логической функции на всю пространство признаков, что определяет расширение классов на все пространство.

Мы будем рассматривать задачу с непересекающимися классами $K_1,\ldots,K_l$ и считать, что информация $J_0\left(K_1,K_2,\ldots,K_l\right)$ задается в виде таблицы обучения T_{nml}. Целью является выделение набора базисных операторов рассматриваемой модели вычисления оценок, построение их линейного замыкания и доказательство того факта, что эти операторы для каждого объекта класса $\tilde{K}_j$ из выборки $\breve{S}_q$ формируют достаточно большую оценку Γ_j и достаточно малые оценки Γ_u при $u \neq j$.

Все базисные операторы, а также операторы из линейного замыкания будут построены в явном виде.

Пусть обучающая информация задана в виде таблицы обучения T_{nml}. Строками таблицы является стандартные описания объектов $S_1,\ldots,S_m,\ S_i = \left(a_{i1},\ldots,a_{in}\right),\ i = \overline{1,n}$. Будем считать, что объекты $S_{m_{j-1}+1},\ldots,S_{m_j}, m_0 = 0, m_l = m$ принадлежат классу $K_j,\ j = 1,2,\ldots,l$, классы попарно не пересекаются. Введем l - мерный предикат $P\left(S\right) = j$, если S принадлежит классу $K_j, j = 1,2,\ldots,l$, тогда задача состоит в вычислении по обучающей информации для некоторого конечного множества объекта $S^1,S^2,\ldots,S^q$ значения предиката P. Объекты $S^1,S^2,\ldots,S^q,S^i = \left(b_{i1},\ldots,b_{in}\right)$ образуют контрольную выборку, причем объекты $S^{q_{j-1}+1},\ldots,S^{q_j}$, $q_0 = 0$, $q_l = q$ принадлежат классу K_j и не принадлежат остальным классам.

Обозначим: $\{S_1,\ldots,S_m\}\cap K_j=\tilde{K}_j$, $\{S_1,\ldots,S_m\}\setminus\tilde{K}_j=C\tilde{K}_j$.
$\{S^1,\ldots,S^q\}\cap K_j=K_j^1$, $\{S^1,\ldots,S^q\}\setminus K_j^1=CK_j^1$.

Пусть A произвольный алгоритм переводящий задачу распознавания Z с l – классами, $Z=\{J,S^q\}$ в матрицу ответов $\|\beta_{ij}\|_{q\times l}$, $A(J,S^q)=\|\beta_{ij}\|_{q\times l}$, $\beta_{ij}\in\{0,1,\Delta\}$. Равенства $\beta_{ij}=1,\beta_{ij}=0,\beta_{ij}=\Delta$ означает, соответственно, что алгоритм A вычислил для объекта $S^i: S^i\in K_j, S^i\notin K_j$, отказывается от вычисления принадлежности объекта S^i классу K_j.

Такие алгоритмы называются некорректными для задачи Z и для произвольных некорректных алгоритмов имеет место.

Теорема 1. Каждый алгоритм A может быть представлен в виде $A=B\times C$ (умножение означает последовательное выполнение), причем если $A(Z)=\|\beta_{ij}\|_{q\times l}$, $\beta_{ij}\in\{0,1,\Delta\}$, то $B(Z)=\|\alpha_{ij}\|$-числовая матрица, $C\left(\|\alpha_{ij}\|_{q\times l}\right)=\|\beta_{ij}\|_{q\times l}$
.

Теорема 1 показывает, что каждый алгоритм A можно разделить на два последовательных этапа. На 1-этапе задача Z переводится в числовую матрицу стандартных размеров q - строк, l – столбцов, число строк равно числу распознаваемых объектов, число столбцов равно числу классов.

На 2-этапе по этой числовой матрице окончательно формируются ответы на вопросы о принадлежности объектов $S^i,\ldots,S^q$ к классам $K_1,\ldots,K_l$.

Значение α_{ij} естественным образом интерпретируются, как значения мер принадлежности объектов S^i классам K_j. Этап B называется распознающим оператором, этап C – решающим правилом.

В дальнейшем рассматриваются только пороговые решающие правила $C^*\left(\|\alpha_{ij}\|_{q\times l}\right)=\|C(a_{ij})\|_{q\times l}$.

Правило применяется поэлементно. Пусть a – число, d_1,d_2 – также числа / пороги/ и $0<d_1<d_2$, тогда

$$C^*(a)=\begin{cases}1, \text{ если } a>d_2\\ 0, \text{ если } a<d_1\\ \Delta, \text{ если } d_1<a<d_2\end{cases}$$

Алгебра распознающих операторов. Пусть $Z=\left(J,\tilde{S}^2\right)$ фиксированная задача распознавания с l классами $K_1,\ldots,K_l$, пусть также B_1 и B_2 распознающие операторы $B_i(Z)=\|\Gamma_{uv}^i\|_{q\times l}$ с матрицей голосов $i=1,2$. Тогда вводятся алгебраические операции суммы, умножения и умножение на число над операторами $(B_1+B_2)(Z)=\|\Gamma_{uv}^1+\Gamma_{uv}^2\|_{q\times l}$,
$(B_1\times B_2)(Z)=\|\Gamma_{uv}^1\times\Gamma_{uv}^2\|_{q\times l}$, $(cB)(Z)=\|c\cdot\Gamma\|_{q\times l}$ $\quad i=1,2.$

Алгебраическое замыкание семейства (B) относительно введенных операций из $\{B\}$ могут быть представлены в виде операторных полиномов $\sum b_{i_1},\ldots,b_{i_k}$, $B_{i_1}\cdot B_{i_2}\cdot\ldots\cdot B_{i_k}$.

Рассмотрим в диссертации семейство алгоритмов $L\{B\}\cdot C(d_1,d_2)$ с линейным расширением $L\{A\}$.

Определение 1. Пара $(S^u, j), S^u\in\tilde{S}^q, S^u\in K_j, 1\le j\le l$ называется отмеченной в операторе B, если $B_v(Z)=\|a_{tv}\|_{q\times l}$, $a_{uj}\ge 1$, $0<|a_{rw}|<\delta<1$ для всех $S^r\in\tilde{S}^q$ таких, что $S^r\notin K_w, w=1,2,\ldots,l.$

Теорема 2. Пусть в некоторой модели даны операторы $B_1,\ldots,B_w$ такие, что каждая пара $(S^u, j), \breve{S}^u\in K_j$ отмечены хотя бы одним оператором $B_1,\ldots,B_w$. Существует линейная комбинация $\sum_{i=1}^{w}\alpha_i B_i=\tilde{B}\in\tilde{L}\{\mathrm{B}\}$ такая, что алгоритм $\tilde{A}=\breve{B}\times C$, C - пороговое решающее правило является корректным для задачи Z.

Теорема 3. Пусть B произвольный оператор из $B(j)$ и $S=(\alpha_1,\ldots,\alpha_n)$ произвольный допустимый объект. Пусть также $B(\mathrm{S})=\left(\Gamma_1^j(S),\ldots,\Gamma_j^j(S),\ldots,\Gamma_l^j(S)\right)$ тогда имеет место следующее неравенство $0\le\Gamma_t^j(S)<m\cdot n\cdot\varepsilon, t=1,2,\ldots,j-1,j+1,\ldots,l.$

Рассмотрим теперь пару (u,v) такую, что $1\le v\le n$, другими словами, объект $S_u\in\tilde{K}_j$. Паре (u,v) соответствует в таблице обучения элемент a_{uv}. Рассмотрим величины $\rho_v(a_{uv},b_{tv}), t=\overline{1,q}$, то есть расстояние значения v-го признака на объекте S_u, в таблице обучения T_{nml} до значения того признака в S^t из S^q.

Упорядочим объекты из $\tilde{S}^q$, где $\tilde{S}^q=\{S^1,\ldots,S^q\}$ по возрастанию величины $p_v(a_{uv},b_{uv}), t=\overline{1,q},$ объекты с равными величинами элементов, упорядочим между собой произвольным образом. Получаем: $S^{r_1},S^{r_2},\ldots,S^{r_i},\ldots,S^{r_q}$
$0\le\rho_v(a_{uv},b_{r_1v})\le\rho(a_{uv},b_{r_2v})\le\ldots\le\rho_v(a_{uv},b_{r_iv})\le\rho(a_{uv},b_{r_qv})$

Припишем объектам последовательности знака «+», если они принадлежат классу K_j и знак «-» в противном случае. В результате может получиться, например, такая последовательность:

$S^{+r_1},S^{+r_2},S^{-r_3},S^{-r_4},S^{+r_5},\ldots,$ и т.д.

Определение 2: Пара (u,v) называется стационарной, если в построенной последовательности знаки «+, -» имеет место равно одна перемена знака, и если перемена знака происходит на элементах $S^{r_i},S^{r_{i+1}}$ то: $p_v(a_v,b_{r_i,v})<p_v(a_{uv},b_{r_{i+1},v})$

Теорема 4. Если в задаче Z для каждого номера $j=\overline{1,l}$ существует стационарная пара, то алгоритм $A=\left(\left(C_1+C_2\right)\sum_{i=1}^{l}B^i\right)\cdot\left(C\left(C_1,C_2\right)\right)$ является корректным для задачи Z.

Логический метод распознавания. Сформулируем следующий логический метод построения оптимального продолжения не всюду определённой функций k-значной логики – классифицирующего объекты по непересекающимися классы K_1,K_2.

Пусть обучающая информация задана в виде таблицы $T_{n,m,2}$. Рассмотрим таблицу $\tilde{T}$ набора $\tilde{\gamma}$, соответствующих всем парам $\left(\tilde{\alpha},\tilde{\beta}\right)$, где $\tilde{\alpha}\in K_1,\tilde{\beta}\in K_2$ таких, что $\gamma_i=\begin{cases}1, \text{если } \alpha_i\neq\beta_i\\ 0, \text{если } \alpha_i=\beta_i\end{cases}$

Нетрудно заметить, что функция F^1, принимающая значение j на наборах объединения интервалов T и значение i на наборах $\left(a_1,a_2,\ldots,a_n\right)$, для которых найдется $\left(b_1,b_2,\ldots,b_n\right)$ из K_i таблицы $T_{n,m,2}$ такое, что $a_{i_1}=b_{i_1},a_{i_2}=b_{i_2},\ldots,a_{i_k}=b_{i_k}$ будет продолжением функции $F(\tilde{x})$.

Таким образом, алгоритм оптимального логического продолжения функции $F\left(x_1,x_2,\ldots,x_n\right)$ сформулируем следующим образом.

1. Формируем таблицу T.
2. Методом “мин-мах” (выделение столбцов с минимальными нормами и строк с максимальным числом единиц) строим неприводимые покрытия $\Pi_1,\ldots,\Pi_l$ строк T столбцами.
3. Для каждого $\Pi_t,t=1,2,\ldots,l$ строим два продолжения F_t',F_t'' функции F.
4. По заданной контрольной таблице объектов определяем процент покрытия для каждого продолжения функции F. Выбираем продолжения с максимальным процентом покрытия объектов контрольной таблицы.

Трудоемкость алгоритма будем выражать через число элементарных шагов. Очевидно, что для формирования $\tilde{T}$ потребуется nm_1m_2 элементарных шагов, где m_1 число объектов в K_1, а m_2 в K_2. Методом “мин-мах” строим неприводимые покрытия строк T столбцами. Ясно, что для этого нужно $m_1m_2n\left(m_1m_2+2\right)$ шагов.

В следующем этапе формируем таблиц, составленных на m_2 строк и $2]\log m_1m_2\left(+\right)\log n[+4$ столбцов. Для этого потребуются $\left(2]\log m_1m_2\left(+\right)\log n[+4\right)m_1m_2$ шагов. Нетрудно заметить, что для алгоритма “мин-мах” имеем $m_1m_2\left(m_2+2\right)\left(2]\log m_1m_2\left(+\right)\log n[+4\right)$ шагов. Таким образом, сложность алгоритма равна:

$$m_1m_2\left\{n\left(m_1m_2+3\right)+\left(m_2+3\right)\left(2]\log m_1m_2\left(+\right)\log n[+4\right)\right\}$$

В главе III “Программная реализация моделей и методов функционирования и защиты информационной системы IoT на примере экосистем» предложена реализация алгоритмов стеганографического кодирования и идентификации в экосистеме.

В §3.1 предлагается логическая автоматная реализация алгоритмов стеганографического кодирования для безопасной реализации хранения и передачи изображений на основе булевых функций в классе дизъюнктивных нормальных форм на базе микроконтроллеров и системы CAD проектирования программируемых логических контроллеров. Производится преобразование к алгебраическому виду алгоритма кодирования метода LSB следующим образом**:**

$Y_0 = 1;\ Y_1 = 1;\ Y_2 = X_1X_2;\ Y_3 = \overline{X_1};\ Y_4 = \overline{X_1};\ Y_5 = \overline{X_1}X_3;\ Y_6 = \overline{X_1}\,\overline{X_3};\ Y_7 = \overline{X_1}\,\overline{X_3}X_4\,X_5;$

$Y_8 = \overline{X_1}\,\overline{X_3}\,\overline{X_4};\qquad Y_9 = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,X_6X_7;\qquad Y_{10} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,X_6\,\overline{X_7}\,X_8;$

$Y_{11} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,X_6\,\overline{X_7}\,\overline{X_8};\qquad Y_{12} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,\overline{X_6};\qquad Y_{13} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,\overline{X_6}X_9;$

$Y_{14} = \overline{X_1}\,\overline{X_3}\,\overline{X_4}\,\overline{X_6}\,\overline{X_9};\ Y_k = \overline{X_1}\,\overline{X_3}\,\overline{X_4}X_5\,\overline{X_6}\vee;\overline{X_1}\,\overline{X_3}X_4\,\overline{X_5}$

Создается матричная схема микрокоманд, соответствующая ГСА алгоритма кодирования метода LSB:

$Y_0 = Y_1;$ $\qquad Y_8 = X_6X_7Y_9 \vee X_6\overline{X_7}X_8Y_{10} \vee X_6\overline{X_7}\,\overline{X_8}Y_{11} \vee \overline{X_6}Y_{12};$

$Y_1 = X_1X_2Y_2 \vee \overline{X_1}Y_3;$ $\qquad Y_9 = X_6X_7Y_9 \vee X_6\overline{X_7}X_8Y_{10} \vee X_6\overline{X_7}\,\overline{X_8}Y_{11} \vee \overline{X_6}Y_{12};$

$Y_2 = X_1X_2Y_2 \vee \overline{X_1}Y_3;$ $\qquad Y_{10} = X_6X_7Y_9 \vee X_6\overline{X_7}X_8Y_{10} \vee X_6\overline{X_7}\,\overline{X_8}Y_{11} \vee \overline{X_6}Y_{12};$

$Y_3 = Y_4;\quad Y_5 = Y_4;$ $\qquad Y_{11} = X_6X_7Y_9 \vee X_6\overline{X_7}X_8Y_{10} \vee X_6\overline{X_7}\,\overline{X_8}Y_{11} \vee \overline{X_6}Y_{12};$

$Y_4 = X_3Y_5 \vee \overline{X_3}Y_6;$ $\qquad Y_{12} = X_9Y_{13} \vee \overline{X_9}Y_{13};$

$Y_6 = X_4X_5Y_7 \vee \overline{X_4}Y_8;$ $\qquad Y_{13} = X_9Y_{13} \vee \overline{X_9}Y_{13};$

$Y_7 = X_5Y_7;$ $\qquad Y_{14} = Y_k;$

Производится преобразование к алгебраическому виду алгоритма асимметричного шифрования El Gamal следующим образом**:**

$Y_0 = Y_1 = 1$ $\qquad Y_2 = x_1$ $\qquad Y_3 = x_2$

$Y_4 = x_1x_3$ $\qquad Y_5 = \overline{x}_1\overline{x}_3\overline{x}_4$ $\qquad Y_6 = \overline{x}_1\overline{x}_3\overline{x}_4\overline{x}_5$

$Y_7 = \overline{x}_1\overline{x}_3\overline{x}_4\overline{x}_5$ $\qquad Y_8 = \overline{x}_1\overline{x}_3\overline{x}_4\overline{x}_5\overline{x}_6$ $\qquad Y_K = \overline{x}_1\overline{x}_3\overline{x}_4\overline{x}_5\overline{x}_6$

Создается матричная схема микрокоманд, соответствующая ГСА алгоритма асимметричного шифрования El Gamal:

$Y_0 = Y_1$ $\qquad Y_1 = \overline{x_1}x_3Y_1 \vee x_1Y_2 \vee \overline{x_1}\,\overline{x_3}Y_4$ $\qquad Y_2 = Y_1$

$Y_3 = Y_2$ $\qquad Y_4 = x_4Y_4 \vee \overline{x_4}Y_5$ $\qquad Y_5 = x_5Y_4 \vee \overline{x_5}Y_6$

$Y_6 = Y_7$ $\qquad Y_7 = x_6Y_7 \vee \overline{x_6}Y_8$ $\qquad Y_8 = Y_k$

В §3.2 дается реализация модели, основанной на вычислении оценок для решения задачи идентификации в экосистеме Аральского региона на основе IoT технологии. Рассматриваются только алгоритмы представимые в виде $A = B*C$, где B – произвольный распознающий оператор, являющийся

существенной частью алгоритма; C-решающее правило, которое может быть сделано стандартным для всех алгоритмов и программ. Любой распознающий оператор голосования отображает задачу Z в числовую матрицу голосов или оценок $B(\mathrm{Z}) = \left\| \Gamma_{ij} \right\|_{q \cdot l}, \Gamma_{ij} = \Gamma_j \left(S^i \right)$. Пусть $\left(\tilde{\alpha} - \tilde{\beta} \right) = \sum_{i=1}^{6} \sum_{j=1}^{10} \left| \alpha_i - \beta_i \right| \to \min$ α_i - это данные датчика, β_j - параметры класса засолённости. Данные датчика: HCO_3 (гидрокарбонат), Cl (хлор), SO_4 (серный кислота), Ca (кальций), Mg (магний), Na (натрий). Соленость делится на 5 классов (незасолённое, слабозасолённое, среднезасолённое, сильнозасолённое, очень сильнозасолённое), и каждый класс состоит из 10 пунктов.

Когда от датчика поступают данные a_i, проверяется выполнение условия $a_i - b_i \to \min$. Если заданное условие выполнено, то указывает к какому классу солености оно относится. Если значения $a_i - b_i \to \min$ соответствуют более чем одному классу солености, то считается, что информация где-то перехвачена.

Для решения задачи сравнительной классификации угроз информационной безопасности в электронных ресурсах на основе алгоритма вычисления оценок использован корректный алгоритм:

$$A = \left(\sum_{i=1}^{e} \sum_{S^t \in K_j} B\left(S^t \right) C\left(C_1, C_2 \right) \right)$$

В § 3.3 предложено применение технологий интернета вещей в экологии (на примере Приаралья) в качестве системы. Система была разработана в виде вебсайта. Фреймворк Django использовался при разработке серверной части системы, а Vue js - клиентской части как одностраничное приложение (SPA) с использованием фреймворка Quasar для GUI. Для запуска системы необходимо открыть этот сайт ecoaral.uz в одном из современных браузеров. После этого на странице браузера отразиться главное окно системы.

ЗАКЛЮЧЕНИЕ

исследованы описания объекта защиты информации в экологической системе на основе IoT технологий и анализ инфраструктуры «интернета вещей» для безопасной реализации хранения и передачи информаций от сенсоров, датчиков и т.п. в экологической системе на основе IoT технологии;

для повышения защиты инфраструктуры «интернета вещей» разработаны методы и алгоритмы стеганографического кодирования для безопасной реализации хранения и передачи изображений в экологической системе на основе IoT технологий;

разработан алгебраический метод для решения задач распознавания с непересекающимися классами на основе корректной модели и алгоритма из линейного замыкания модели вычисления оценок;

разработан логический метод распознавания объектов на основе рассмотрения эталонной таблицы как невсюду определенной логической

функции и построении оптимального продолжения логической функции на всю пространство признаков, что определяет расширение классов на все пространство;

проведена логическая автоматная реализация алгоритмов стеганографического кодирования и ассиметричного шифрования El Gamal для безопасной реализации хранения и передачи изображений на основе булевых функций в классе дизъюнктивных нормальных форм на базе микроконтроллеров и системы CAD проектирования программируемых логических контроллеров;

предложена реализация модели основанной на вычислении оценок для решения задачи идентификации в экосистеме Аральского региона на основе применения технологии интернета вещей в экологии.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.03/30.12.2019.FM.01.02 NATIONAL UNIVERSITY OF UZBEKISTAN

NATIONAL UNIVERSITY OF UZBEKISTAN

SAYMANOV ISLAMBEK MIRZABAEVICH

ALGORITHMIC AND LOGICAL METHODS FOR PROCESSING AND PROTECTION OF ENVIRONMENTAL DATA

05.01.05 – Methods and systems of information protection. Information security (Physical and mathematical sciences)

ABSTRACT OF DISSERTATION OF THE DOCTOR OF PHILOSOPHY (PhD) ON PHYSICAL AND MATHEMATICAL SCIENCES

Tashkent-2023

The theme of dissertation of doctor of philosophy (PhD) on physical and mathematical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number № B2022.2.PhD/FM739.

Dissertation has been prepared at National University of Uzbekistan.

The abstract of the dissertation is posted in three languages (uzbek, russian, english (resume)) on the website (www.ik-fizmat.nuu.uz) and the "ZiyoNet" Information and educational portal (www.ziyonet.uz).

Scientific superviser:	**Kabulov Anvar Vasilovich** Doctor of Technical Sciences, Professor
Official opponents:	**Abdurakhimov Bakhtiyor Fayziyevich** Doctor of Physical and Mathematical Sciences, Professor
	Saidov Abdusobirzhon Abduraxmonovich Doctor of Technical Sciences, Professor
Leading organization:	**Karakalpak state University named after Berdakh**

Defense will take place «____» _____2023 at _____ at the meeting of Scientific Council number DSc.03/30.12.2019.FM.01.02 at National University of Uzbekistan. (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 227-12-24, fax: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

Dissertation is possible to review in Information-resource centre at National University of Uzbekistan (is registered №____) (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 246-02-24).

Abstract of dissertation sent out on «____» _____2023 year

(Mailing report № _____on «____» _____2023 year)

M.M. Aripov
Chairman of Scientific council
on award of scientific degrees,
D.F.-M.S., professor

Z.R. Rakhmonov
Scientific secretary of Scientific
Council on award of scientific
degrees, D.F.-M.S.

G.U. Juraev
Deputy Chairman of Scientific
Seminar under Scientific
Council on award of scientific
degrees, D.F.-M.S.

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is the development of algorithmic and logical methods for processing and protecting environmental data in the IoT system for the implementation of steganography algorithms, identification and pattern recognition based on graph diagrams of algorithms and systems of logic algebra functions.

The research objective are built-in systems for managing, identifying, processing and protecting environmental data generated by IoT devices.

Scientific novelty of research work is as follows:

an algorithmic model was developed based on the study of algorithmic principles and the synthesis of functioning tables to ensure optimal compatibility of subjects and objects in the process of data entry and user access control;

a logical automaton method of steganographic coding has been developed for the safe implementation of storage and transmission of images based on Boolean functions in the class of disjunctive normal forms based on microcontrollers and a CAD system for designing programmable logic controllers;

algebraic and logical methods for solving recognition problems with non-overlapping classes based on a correct model from a linear closure of algorithms for calculating estimates and constructing an optimal continuation of a logical function for the entire feature space have been developed;

the polynomial complexity of the logical recognition algorithm for identification, processing and protection of images in the IoT system was proved;

the correctness of the algebraic recognition algorithm for the identification, processing and protection of environmental data in the IoT system was proved.

Implementation of the research results. Based on the developed methods and models for ensuring the confidentiality of information resources, interactive services in the management of information systems have been introduced in a number of business entities:

the optimal mathematical model of the steganography algorithm was used to analyze and write the functional forms of microcommands when writing to microcontrollers in the Uzb-Ind-2021-94 project “Energy efficiency and data flow in a smart city using IoT infrastructure based on CRN” (certificate of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi dated May 25, 2022 No. 1596-15/01). The use of scientific results made it possible to optimally implement the microcontroller and analyze the steganographic algorithm;

the method and means of interactive analysis of water and soil were used in the development of software for monitoring the determination of the influence of environmental conditions based on the results of an interactive analysis of water and soil in agriculture in the Aral Sea region (certificate of the Ministry of Water Resources of the Republic of Karakalpakstan, dated May 6, 2022 No. 03 / 08-3 - 148). The application of scientific results made it possible to increase the efficiency of production in the technological process by 7-8%.

The structure and volume of the thesis: The dissertation work consists of an introduction, three chapters, a conclusion, a list of references and an appendix. The volume of the dissertation is 104 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (1 часть; part 1)

1. Kabulov A., Urunboev E., Saymanov I. Object recognition method based on logical correcting functions // 2020 International Conference on Information Science and Communications Technologies, 2020, – P. 1-4. (№3, Scopus. ОАК Раёсатининг 18.09.2020 йилдаги №3008/5-01–сон қарори)
2. Kabulov A. V., Saymanov I., Berdimurodov M.A. Minimum logical representation of microcommands of cryptographic algorithms (AES) // International conference on information science and communications technologies: applications, trends and opportunities, 2021, – P. 1-5. (№3, Scopus. ОАК Раёсатининг 30.10.2021 йилдаги №308/6–сон қарори)
3. Kabulov A., Saymanov I. Application of IoT technology in ecology (on the example of the Aral Sea region) // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, 2021, – P. 1-5. (№3, Scopus. ОАК Раёсатининг 30.10.2021 йилдаги №308/6–сон қарори)
4. Kabulov A., Saymanov I., Yarashov I., Muxammadiev F. Algorithmic method of security of the Internet of Things based on steganographic coding // 2021 IEEE International IOT, Electronics and Mechatronics Conference, 2021, 9422588, – P. 1-5. (№1, Web of Science)
5. Kabulov A.V., Normatov I.H., Boltaev Sh., Saymanov I. Logic method of classification of objects with non-joining classes // Advances in Mathematics: Scientific Journal, 2020, 9(10), –P. 8635–8646 (№3, Scopus IF=0.1)
6. Кабулов А.В., Бердимуродов М.А., Сайманов И.М. Криптографик алгоритм микробуйруқларининг мантиқий бул функция шакли (AES, Эл-Гамал) // Самарқанд давлат университети илмий ахборотномаси. №3(2021), – Б. 90-100. (01.00.00, №2)
7. Кабулов А.В., Сайманов И.М., Бердимуродов М.А. Хранение данных на основе архитектуры блокчейна для интернета вещей (IoT) // Научный вестник Самаркандского Государственного Университета. №5(2021), – С. 60-68. (01.00.00, №2)
8. Кабулов А.В., Бабаджанов А.Ф., Сайманов И.М. Построение линейного замыкания модели вычисления оценок и корректного алгоритма // Муҳаммад ал-Хоразмий авлодлари илмий-амалий ва ахборот-таҳлилий журнал, 1(19)/2022, – С. 19-25. (05.00.00, №10)
9. Кабулов А.В., Сайманов И.М., Ярашов И. Методы и алгоритмы стеганографического кодирования для безопасной реализации передачи изображений // Узбекский журнал Проблемы информатики и энергетики, №4, 2020, – С. 26-35. (05.00.00, №5)
10. Кабулов А.В. Сайманов И.М., Ашуров С. Логический метод распознавания объектов // Узбекский журнал Проблемы информатики и энергетики, №5,

2020, – С. 57-63. (05.00.00, №5)
11. Сайманов И.М. Интернет вещей (IOT): Литературный обзор // Наука и общество научно-методический журнал, №3, 2021, – С. 16-19. (01.00.00, №15)

II bo‘lim (II част; II part)

12. Kabulov A., Babadjanov A., Saymanov I. Completeness of the linear closure of the voting model // Международная научно-практическая конференция. – Фарғона, 2021, – С.203.
13. Kabulov A., Babadjanov A., Saymanov I. Correct models of families of algorithms for calculating estimates // Международная научно-практическая конференция. – Фарғона, 2021, – С.204.
14. Normatov I., Saymanov I. On the existence of majorant algorithms over control systems // Международная научно-практическая конференция. – Фарғона, 2021, – С.211.
15. Кабулов А.В., Норматов И.Х., Сайманов И.М. Алгоритмические методы управления сложными системами на основе таблиц функционирования // Международная научно-практическая конференция. – Фарғона, 2020, – С.101-107.
16. Сайманов И.М., Ашуров С. Безопасность в технологии интернет вещей // Международная научно-практическая конференция. – Бухара, 2021, – С.291-292.
17. Сайманов И.М., Ашуров С. Области применения IoT // Республиканская научно-практическая конференция. – Карши, 2021, – С.314-317.
18. Сайманов И.М., Исоқов Г.С. Технология интернет вещей // Международная научно-практическая конференция.– Қарши, 2022, – С.176-178.
19. Сайманов И.М., Мирзоодилов Б.Н., Жураев М.Т., Васиева Д.Д. Алгоритмическая технология защиты информационных систем на базе таблицы функционирования // Международная научно-практическая конференция. – Пенза, 2020, – С.38-45.
20. Сайманов И.М., Норматов Д. Применение искусственных нейронных сетей в архитектуре IoT // Международная научно-практическая конференция. – Фарғона, 2020, – С.340-341.
21. Сайманов И.М., Турсунов С.Ю. Архитектура IoT // Международная научно-практическая конференция. – Қарши, 2022, – С.174-175.
22. Сайманов И.М., Ярашов И. IoT архитектурасида функционал даражалари таҳлили // Халқаро илмий-амалий анжуман. – Қарши, 2020, – С.356-358.
23. Сайманов И.М., Бердимуродов М.А. AES(Rijndael) криптографик алгоритмидаги S чизиқсиз акслантиришнинг буль функциясининг алгебраик шакли. Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги интеллектуал мулк агентлиги. Тошкент, 2021, №DGU 12634. 10.09.2021.
24. Кабулов А.В., Норматов И.Х., Сайманов И.М., Ярашов И.К. Особенности обнаружения и анализ DDoS-атак. Ўзбекистон Республикаси Адлия

вазирлиги ҳузуридаги интеллектуал мулк агентлиги. Тошкент, 2021, №DGU 13974. 06.12.2021.
25. Кабулов А.В., Норматов И.Х., Лолаев М.Я., Сайманов И.М. Орол бўйи қишлоқ хўжалиги ишлаб чиқаришида экологик вазиятлар таъсирини аниқлаш мониторингини юритишнинг “ecoaral.uz” дастурий таъминоти. Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги интеллектуал мулк агентлиги. Тошкент, 2022, №DGU 18211. 27.07.2022.
26. Кабулов А.В., Норматов И.Х., Сайманов И.М., Ярашов И.К. Орол бўйи қишлоқ хўжалиги ишлаб чиқаришида экологик вазиятлар таъсирини аниқлаш мониторингини юритишнинг “ecoaral.uz” сайтининг маълумотлар базаси. Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги интеллектуал мулк агентлиги. Тошкент, 2022, №DGU 18211. 27.07.2022. Тошкент, 2022, №BGU 00740. 28.07.2022.

Автореферат Ўзбекистон Миллий университетининг «ЎзМУ хабарлари» журнали таҳририятида 2023 йил 31 майда таҳрирдан ўтказилди.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 2,75. Adadi 100 dona. Buyurtma № 45/23.

Guvohnoma № 851684.
«Tipograff» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko‘chasi, 83-uy.