MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

4-SON 1(4)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

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

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №4
Vol.1, Iss.4, 2023 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

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

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

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

FARG’ONA - 2023 YIL

Jurnal quyidagi bazalarda indekslanadi:

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · DRJI Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Muxtarov Farrux Muhammadovich, TARMOQ TRAFIGI ANOMALIYALARINI IDENTIFIKATSIYA QILISHNING STATIK USULI	4-7
Daliyev Baxtiyor Sirojiddinovich, Abelning umumlashgan integral tenglamasini yechish uchun Sobolev fazosida optimal kvadratur formulalar	8-14
Umarov Shuxratjon Azizjonovich, KRIPTOBARDOSHLI KRIPTOGRAFIK TIZIMLAR VA ULARNING KLASSIFIKATSIYASI	15-21
Zulunov Ravshanbek Mamatovich, PYTHONDA NEYRON TARMOQNI QURISH VA BASHORAT QILISH	22-26
Djalilov Mamatisa Latibdjanovich, IKKI QATLAMLI NOELASTIK PLASTINKANING KO‘NDALANG TEBRANISHI UMUMIY TENGLAMASINI TAHLIL QILISH	27-30
Erkin Uljaev, Azizjon Abdulkhamidov, Utkirjon Ubaydullayev, A Convolutional Neural Network For Classification Cotton Boll Opening Degree	31-36
Seytov Aybek Jumabayevich, Xusanov Azimjon Mamadaliyevich, Magistral kanallarda suv resurslarini boshqarish jarayonlarini modellashtirish algoritmini ishlab chiqish	37-43
Abdullayev Temurbek Marufjonovich, Algorithm of functioning of intellectual information-measuring system	44-49
Odinakhon Sadikovna Rayimjanova, Usmonali Umarovich Iskandarov, Reaserch of highly sensitive deformation semiconductor sensors based on AFV	50-53
S.S.Radjabov, G.R.Mirzayeva, A.O.Tillavoldiyev, J.A.Allayorov, BARG TASVIRI BO‘YICHA MADANIY O‘SIMLIKLARNING FITOSANITAR HOLATINI ANIQLASH ALGORITMLARI	54-59
Эргашев Отабек Мирзапулатович, Интеллектуальный оптоэлектронный прибор для учета и контроля расходом воды в открытых каналах	60-65
Xomidov Xushnudbek Rapiqjon o‘g‘li, Nurmatov Sardorbek Xasanboy o‘g‘li, Yo’ldashev Bilol Iqboljon o‘g‘li, O‘lmasov Farrux Yorqinjon o‘g‘li, Konus setkali chang tozalovchi qurilma uchun chang namunalarining dispers tarkibi tahlili	66-69
Akhundjanov Umidjon Yunus ugli, VERIFICATION OF STATIC SIGNATURE USING CONVOLUTIONAL NEURAL NETWORK	70-74
Лазарева Марина Викторовна, Горовик Александр Альфредович, Цифровизация и цифровой менеджмент в современном управлении	75-81
D.X.Tojimatov, KIBERTAHDIDLARNI OLDINI OLISHDA KIBERRAZVEDKA AMALIYOTI VA UNING USTUVOR VAZIFALARI	82-85
Muxtarov Farrux Muhammadovich, Rasulov Akbarali Maxamatovich, Ibroximov Nodirbek Ikromjonovich, Kompyuter eksperimenti orqali kam atomli mis klasterlarining geometrik tuzilishini o‘rganish	86-89
Umurzakova Dilnoza Maxamadjanovna, BOSHQARISH QONUNLARINI ADAPTATSIYALASH ALGORITMLARINI ISHLAB CHIQISH	90-94
Muxamedieva Dildora Kabilovna, Muxtarov Farrux Muhammadovich, Sotvoldiev Dilshodbek Marifjonovich, JAMOAT TRANSPORTI MARSHRUTLARINI QURISH INTELLEKTUAL ALGORITMLARI	95-103
Нурдинова Разияхон Абдихаликовна, Перспективы применения элементов с аномальными фотовольтаическими напряжениями	104-108
Bozarov Baxromjon Ilxomovich, UCH O‘LCHOVLI FAZODAGI SFERADAANIQLANGAN FUNKSIYALARNI TAQRIBIY INTEGRALLASH UCHUN OPTIMAL KUBATUR FORMULALAR	109-113
Улжаев Эркин, Худойбердиев Элёр Фахриддин угли, Нарзуллаев Шохрух Нурали угли, РАЗРАБОТКА КОНСТРУКЦИИ И ФУНКЦИОНАЛЬНОЙ СХЕМЫ ПОЛУЦИЛИНДРИЧЕСКОГО ЁМКОСТНОГО ПОТОЧНОГО ВЛАГОМЕРА	114-122
Mamirov Uktam Farkhodovich, Buronov Bunyod Mamurjon ugli, ALGORITHMS FOR FORMATION OF CONTROL EFFECTS IN CONDITIONS OF UNOBSERVABLE DISTURBANCES	123-127
Sharibayev Nosirjon Yusubjanovich, Jabborov Anvar Mansurjonovich, YURAK-QON TOMIR KASALLIKLARI DIAGNOSTIKASI UCHUN TEXNOLOGIYALAR, ALGORITMLAR VA VOSITALAR	128-136
Marina Lazareva, Estimating development time and complexity of programs	137-141
Asrayev Muhammadmullo, ONLINE HANDWRITING RECOGNITION	142-146
Norinov Muhammadyunus Usibjonovich, SPEKTR ZONALI TASVIRLARGA INTELLEKTUAL ISHLOV BERISH USULLARI TAHLILI	147-152
Xudoynazarov Umidjon Umarjon o‘g‘li, PARAMETRLI ALGEBRAGA ASOSLANGAN EL-GAMAL SHIFRLASH ALGORITMLARINI GOMOMORFIK XUSUSIYATINI TADQIQ ETISH	153-157
D.M.Okhunov, M.Okhunov, THE ERA OF THE DIGITAL ECONOMY IS AN ERA OF NEW OPPORTUNITIES AND PROSPECTS FOR BUSINESS DEVELOPMENT BASED ON CROWDSOURCING TECHNOLOGIES	158-165

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Солиев Бахромжон Набиджонович, Путеводитель по построению веб-API на Django - Шаг за шагом с Django REST framework — от моделей до проверки работоспособности	166-171
Sevinov Jasur Usmonovich, Boborayimov Okhunjon Khushmurod ogli, ALGORITHMS FOR SYNTHESIS OF ADAPTIVE CONTROL SYSTEMS WITH IMPLICIT REFERENCE MODELS BASED ON THE SPEED GRADIENT METHOD	172-176
Mamatov Narzullo Solidjonovich, Jalelova Malika Moyatdin qizi, Tojiboyeva Shaxzoda Xoldorjon qizi, Samijonov Boymirzo Narzullo o'g'li, SUN'IY YO'LDOSHDAN OLINGAN TASVIRDAGI DALA MAYDONI CHEGARALARINI ANIQLASH USULLARI	177-181
Обухов Вадим Анатольевич, Криптография на основе эллиптических кривых (ECC)	182-188
Turdimatov Mamirjon Mirzayevich, Sadirova Xursanoy Xusanboy qizi, AXBOROTNI HIMOYALASHDA CHETLAB O'TISHNING MUMKIN BO'LGAN EHTIMOLLIK XOLATINI BAHOLASH USULLARI	189-193
Musayev Xurshid Sharifjonovich, TRIKOTAJ MAHSULOTLARIDA NUQSONLI TO'QIMALARNING ANIQLASHNING MATEMATIK MODELI VA UNING ALGORITMLARI	194-196
Kodirov Ahkhmadkhon, Umarov Abdumukhtar, Rozaliyev Abdumalikjon, ANALYSIS OF FACIAL RECOGNITION ALGORITHMS IN THE PYTHON PROGRAMMING LANGUAGE	197-205
Suyumov Jorabek Yunusalievich, METHODOLOGICAL PROBLEMS OF QUALIMETRY IN CONDUCT OF PEDAGOGICAL EXPERIMENT-EXAMINATION	206-211
Хаджаев Саидакбар Исмоил угли, АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МАЛОГО И СРЕДНЕГО БИЗНЕСА ОТ КИБЕРАТАК	212-217
M.M.Khalilov, Effect of Heat Treatment on the Photosensitivity of Polycrystalline PbTe Films AND PbS	218-221
Тажибаев Илхом Бахтиёрович, ПОЛНОСТЬЮ ВОЛОКОННЫЙ СЕНСОР, ОСНОВАННЫЙ НА КОНСТРУКЦИИ ИЗ МАЛОМОДОВОГО ВОЛОКОННОГО СМЕЩЕНИЯ С КАСКАДНЫМ СОЕДИНЕНИЕМ ВОЛОКОННОЙ РЕШЕТКИ С БОЛЬШИМ ИНТЕРВАЛОМ, ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ИСКРИВЛЕНИЯ И ПРОВЕДЕНИЯ АКУСТИЧЕСКИХ ИЗМЕРЕНИЙ	222-225
Sharibaev Nosir Yusubjanovich, Djuraev Sherzod Sobirjanovich, To'xtasinov Davronbek Xoshimjon o'g'li, PRIORITIES IN DETERMINING ELECTRIC MOTOR VIBRATION WITH ADXL345 ACCELEROMETER SENSOR	226-230
Mukhammadjonov A.G., ANALYSIS OF AUTOMATION THROUGH SENSORS OF HEAT AND HUMIDITY OF DIFFERENT DIRECTIONS	231-236
Эрматова Зарина Кахрамоновна, АКТУАЛЬНОСТЬ ПРЕПОДАВАНИЯ ЯЗЫКА ПРОГРАММИРОВАНИЯ C++ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ	237-241
Saparbaev Rakhmon, ANALOG TO DIGITAL CONVERSION PROCESS BY MATLAB SIMULINK	242-245
Садикова М.А., Авазова Н.К., САМООБУЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, БАЗОВЫЕ ПРИНЦИПЫ РАБОТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТ НА ПРОСТОМ ПРИМЕРЕ	246-250
Abduhafizov Tohirjon Ubaydullo o'g'li, Abdurasulova Dilnoza Botirali kizi, DEVELOPMENT OF ALGORITHMS IN THE ANALYSIS OF DEMAND AND SUPPLY PROCESSES IN ECONOMIC SYSTEMS	251-256
Kayumov Ahror Muminjonovich, CREATING MATHEMATICAL MODELS TO IDENTIFY DEFECTS IN TEXTILE MACHINERY FABRIC	257-261
Mirzakarimov Baxtiyor Abdusalomovich, Xayitov Azizjon Mo'minjon o'g'li, BIOMETRIC METHODS SECURE COMPUTER DATA FROM UNAUTHORIZED ACCESS	262-266
Soliyev B., Odilov A., Abdurasulova Sh., Leveraging Python for Enhanced Excel Functionality: A Practical Exploration	267-271
Жураев Нурмахамад Маматович, Системы Электроснабжения Оборудования Предприятий Связи: Надежность и Эффективность	272-276
Rasulova Feruzaxon Xoshimjon qizi, Isroilov Sharobiddin Mahammadyusufovich, OLIY TA'LIM MUASSASALARIDA MUTAXASISILIK FANLARINI O'QITISHDA MULTIMEDIALI MOBIL ILOVADANDAN FOYDALANISHNING STATISTIK TAHLILI	277-280
Muxtarov Farrux Muxammadovich, Toshpulatov Sherali Muxamadaliyevich, SUN'IY INTELLEKT YORDAMIDA IJTIMOIY TARMOQ MONITORINGI TIZIMINI YARATISH, AFZALLIKLARI VA MUHIM JIXATLARI	281-285
Sadikova Munira Alisherovna, APPLICATION OF ARTIFICIAL INTELLIGENCE DEVICES IN MANUFACTURING	286-290
Mamatov Narzullo Solidjonovich, Ibroximov Sanjar Rustam o'g'li, Fayziyev Voxid Orzumurod o'g'li, Samijonov Abdurashid Narzullo o'g'li, SUN'IY INTELLEKT VOSITALARINI TA'LIMNI NAZORAT QILISH VA BAHOLASHDA QO'LLASH	291-297

KRIPTOBARDOSHLI KRIPTOGRAFIK TIZIMLAR VA ULARNING KLASSIFIKATSIYASI

Umarov Shuxratjon Azizjonovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali Axborot xavfsizligi kafedrasi dotsenti, Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD)
e-mail: sh.umarov81@mail.ru

Annotatsiya: Maqolada kriptografik tizimlarni kriptobardoshliligi bo‘yicha tasniflangan, bu ularning ma’lumotlarni ishonchli himoya qilish imkoniyatini baholash imkonini beradi. Kriptografik bardoshlilik tushunchasi berilgan. Kriptografik bardoshli (mutlaqo, nisbatan, vaqtinchalik) tizimlarning mavjudligi shartlari va bardoshli kriptografik tizimlarga qo‘yiladigan talablar aniqlangan. Shuningdek, bardoshli kriptografik tizimlarning talablari keltirilgan. Shu bilan bir qatorda, bardoshli kriptografik tizimlarning kamchiliklari ham ko‘rsatib o‘tilgan.

Kalit so‘zlar: kriptobardoshlilik, kriptotizim, entropiya, kriptogramma, RSA algoritmi,kriptoanalitik, shifrlash, deshifrlash, kriptoalgoritm.

KIRISH. Kriptografik usullar qo‘llaniladigan asosiy yo‘nalishlardan biri axborot tizimlarining xavfsizligi hisoblanadi. Kriptografik usullardan ma’lumotlarni himoya qilish va ma’lumotlarning maxfiyligini, haqiqiyligini ta’minlash uchun foydalaniladi. Hozirgi kunda insoniyat faoliyatining barcha sohalarida kriptografik usullardan foydalanishni ko‘rish mumkin. Masalan, Internet orqali ma’lumotlarni uzatishda ma’lumotlarni ruxsatsiz kirishdan himoya qilish uchun SSL/TLS kabi kriptografik protokollar qo‘llaniladi. Bank va moliya sohasida to‘lov kartalarini himoya qilish va xavfsiz moliyaviy operatsiyalarni amalga oshirish uchun kriptografik usullardan foydalanish bir qator xavfsizlikni ta’minlaydi. Korxona va tashkilotlar o‘zlarining ichki tarmoqlaridagi maxfiy ma’lumotlarni himoya qilish uchun kriptografiyadan ham foydalanishlari mumkin bo‘ladi. Shuningdek, kriptografik usullardan elektron tijoratda xarid ma’lumotlari va foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilish uchun ham qo‘llaniladi. Bu xaridor va sotuvchi o‘rtasida ma’lumot uzatishda xavfsizlikni ta’minlaydi. O‘z navbatida, foydalanuvchilarni autentifikatsiya qilish va turli onlayn xizmatlardan foydalanishda xavfsizlikni ta’minlash uchun ham qo‘llanilishi mumkin. Ular klientlarning ma’lumotlarini ruxsatsiz kirishdan himoya qilishga va xakerlik hujumlarining oldini olishga yordam beradi. Davlat va korporativ tizimlar sohasida maxfiy axborotni himoya qilish, uning xavfsizligi va yaxlitligini ta’minlash uchun kriptografik usullar qo‘llaniladi. Kriptografik usullar tibbiyot (tibbiy ma’lumotlar va tibbiy hujjatlarni himoya qilish), huquq (yuridik ahamiyatga ega hujjatlar uchun elektron imzo), sun’iy yo‘ldosh va kabel televideniyasi (kontentni kodlash va himoya qilish) va boshqa ko‘plab boshqa sohalarda ham qo‘llaniladi [1].

Axborot muhofazasining kriptografik usullarini yaratishning asosiy vositasi matematik modellar bilan aniqlanuvchi akslantirishlardan iborat shifrlash algoritmlari hisoblanadi. Axborot muhofazasini ta’minlashda shifrlash algoritmlaridan foydalanish qulay va samarali hisoblanadi [2].

Shu bilan birga shifrlash algoritmlari akslantirishlarining matematik modellardan iboratligi shifrma’lumotlarni tahlil qilish natijasida shifrlash algoritmini aniqlash, shifrlash algoritmi ma’lum bo‘lganda esa kalitni topish, kalit noma’lum bo‘lganda ham shifrma’lumotni deshifrlashga erishish kabi urinishlarni matematik usullarini amalga oshirish imkoniyatlariga manbaa bo‘ladi. Bunday urinishlar kriptohujum deb ataladi.

Kriptohujumning maqsadi kalit noma’lum bo‘lganda shifrma’lumotga mos ochiq ma’lumotni topishga erishishdan iborat. Kriptohujumni amalga oshiruvchini kriptoanalitik deb yuritiladi. Kriptoanalitik tomonidan kriptohujum biror vosita orqali amalga oshiriladi. Bunday vositalar kriptoalgoritmlar akslantirishlarining xossalaridan kelib chiqqan holda matematik modellar ko‘rinishida

yaratilib, kriptotahlil usullarining asosi sifatida foydalaniladi [3].

MASALANING QO‘YILISHI. Axborotni kriptografik muhofazasini ta’minlash sohasidagi mutaxassislar fikricha, muhofaza vositalarini – kriptoalgoritmlarni ishlab chiqishdan ko‘ra, ularning kriptografik samaradorligini – kriptohujumlarga bardoshli yoki bardoshli emasligini kriptografik tahlili qiyin masala hisoblanadi. Chunki, kriptotahlil masalalari kriptografik algoritmlar akslantirishlarining samaradorligini tahlil qilish bilan bog‘liq hisoblashlarning ratsional matematik modellarini qurish, elektron hisoblash qurilmalari hamda tarmoqlarida ularning amalga oshirishning dasturiy ta’minotlarini vaqt va xotira bilan bog‘liq murakkabliklarini yechish kabi keng qamrovli (kompleks) muammolarni yuqori ilmiy saviyada tizimli hal etishni talab etadi [4].

Foydalanuvchilar uchun kriptografik vositalarni yaratilishiga va ulardan foydalanishga ehtiyojlar ortib bormoqda. Odatda, axborot muhofazasini ta’minlashning kriptografik vositalari algoritmlari barcha foydalanuvchilarga ma’lum bo‘lib, uning kriptobardoshliligi faqat algoritmda ishlatiladigan kalitning maxfiy saqlanishini o‘ziga bog‘liq bo‘lishi Kirxgof tamoyili sifatida ta’kidlanadi. Yangi yaratilayotgan kriptogrfik vositalarni sifat va samaradorligini ilmiy asoslangan holda baholab borish uchun ular negizidagi algoritmlar akslantirishlari xususiyatlariga ko‘ra sinflarga ajratish, kriptografik algoritmlarga qo‘llanadigan kriptohujum vositalarining yaratilishini nazariy va amaliy ilmiy asoslarini tizimli tahlil etib borish dolzarbdir.

Ko‘p jihatdan kriptografik usullardan amaliy foydalanish ularning kriptobardoshliligiga bog‘liq. Kriptobardoshlilik - bu kriptografik tizimning uni matematik tahlil qilish orqali buzishlariga dosh bera olish qobiliyatidir. Darhaqiqat, kriptografik usullarning kriptobardoshliligi ulardan amaliy foydalanishning asosiy jihatlaridan biridir. Agar kriptografik tizim yetarli darajada bardoshli bo‘lmasa, uni buzish mumkin va tizim tomonidan himoyalangan ma’lumotlar ruxsatsiz olinishi va ishlatilishi mumkin. Kriptogrammadan ma’lumot olishning o‘zi kriptografik tizimlarning bardoshliliga bog‘liq. Agar qarshilik zaif bo‘lsa, u holda ushlangan xabarlardan ishonchli ma’lumot olish imkoniyati mavjud bo‘ladi. Kriptografik tizimning zaifligiga misol sifatida nemis Enigma shifrlash mashinasi haqidagi ma’lumotni keltirish mumkin [2]. Ikkinchi jahon urushi boshida Enigma xabarlarni shifrlashda tengsiz va ishonchli hisoblangan. Biroq, Polsha va Britaniya kriptoanalitiklari tomonidan shifr matnini o‘qish mumkin bo‘ldi. Bu urush jarayonida sezilarli burilishga olib kelgan. Ushbu misol kriptografik tizimlarning kriptobardoshliligi qanchalik muhimligini aniq ko‘rsatib turibdi. Zamonaviy shifrlash usullari murakkab matematik algoritmlarga asoslanadi va ularning kriptobardoshliligini ta’minlash uchun muntazam ravishda sinovdan o‘tkaziladi va tekshiriladi. Biroq, hisoblash texnikasi va kriptoanalizning doimiy rivojlanishi tufayli kriptografik usullarning mustahkamligi va ishonchliligini saqlab qolish uchun ularni doimiy ravishda yangilash va takomillashtirish muhim ahamiyatga ega.

MASALANING YECHILISHI. Kriptografik tizimning kriptobardoshliligini baholash juda qiyin vazifadir, chunki bunday baholash uchun hech qanday mezon yo‘q [5]. Buning o‘rniga kriptotizimning shifrlash shartlarini aniqlash va uning kriptobardoshliligini baholash uchun turli usullar qo‘llaniladi. Yondashuvlardan biri shifrlash algoritmining matematik murakkabligini tahlil qilishdir. Agar shifrlash usuli faktorizatsiya yoki diskret logarifm kabi ma’lum matematik masalalarga asoslangan bo‘lsa va bu muammolarni hal qilish uchun faqat murakkab algoritmlar ma’lum bo‘lsa, kriptotizim xavfsiz hisoblanadi. RSA, Diffi-Hellman yoki elliptik egri chiziq kabi kriptografik algoritmlar ana shunday matematik masalalarga asoslangan. Yana bir yondashuv - kriptografik tizimni har xil turdagi hujumlarga qarshilik ko‘rsatish uchun sinovdan o‘tkazish hisoblanadi. Buning uchun turli usullar qo‘llaniladi, jumladan, qo‘pol kuch hujumlari, statistik hujumlar, kriptoanaliz va boshqalar. Agar tizim ushbu hujumlarga muvaffaqiyatli dosh bersa va chegaralangan vaqt ichida buzib bo‘lmaydigan bo‘lsa, u kriptobardoshli hisoblanadi. Bundan tashqari, kriptografik tizimning mustahkamligini tegishli tashkilotlar va standartlarni mustaqil tekshirish, audit va sertifikatlash orqali tasdiqlash mumkin. Masalan, Elektr va elektronika muhandislari instituti (IEEE), Milliy standartlar va texnologiyalar instituti (NIST) va Xalqaro standartlashtirish tashkiloti (ISO) kriptografik algoritmlarni yaratadi va ulardan foydalanish bo‘yicha ham standartlar va ko‘rsatmalarni ishlab chiqadilar.

Tarixga nazar solsak, Klod Shennon o‘zining "Maxfiy aloqa nazariyasi" (1949) asarida kriptografik himoyalangan tizimlarning mavjudligi shartlarini belgilab berdi va bu bilan kriptografiyaga katta hissa qo‘shdi [6]. U ochiq matnda mavjud bo‘lgan ma’lumotlar miqdorini baholashga imkon beruvchi axborot entropiyasi tushunchasini kiritdi va kriptografik tizimlarning kriptobardoshliligini baholash usullarini keltirdi. Shennon teoremasiga ko‘ra, agar shifrlangan xabar (kriptogramma) tarkibidagi ma’lumotlarning miqdori ushlab qoluvchi tajovuzkorga kalit yoki ochiq matnni olish uchun yetarli ma’lumot bermasa, demak, kriptotizim kriptobardoshli bo‘ladi. Agar tajovuzkor cheksiz hisoblash kuchiga va katta hajmdagi shifrlangan xabarlarga kirish huquqiga ega bo‘lsa ham, kriptogrammaning maxfiyligi buzilmasa, kriptotizim mutlaqo kriptobardoshli hisoblanadi. Biroq, kriptografik tizimlarning mutlaqo kriptobardoshliligini amaliy amalga oshirish qiyin, chunki bu teng uzunlikdagi kalitlardan foydalanishni va juda katta hisoblash resurslarini talab qiladi. Shu sababli, real hayotda nisbatan kriptobardoshlilikka ega kriptografik tizimlar keng qo‘llaniladi. K.E.Shennon ta’rifiga ko‘ra kriptoalgoritm va kriptotizimlarning nazariy bardoshliligi - kriptoanalitik (kriptotahlilchi) kriptografik tizimning tahlili uchun yetarli darajadagi ilmiy hamda texnik va boshqa kerakli vositalarga ega bo‘lganda shuningdek kriptotahlil muddati chegaralanmaganda uning bardoshliligi qanday bo‘lishini aniqlashdan iborat. Nazariy bardoshlikning bunday ta’rifi mutlaqo bardoshli kriptoalgoritm kaliti uzunligining cheksiz bo‘lishini yoki shifrlash alfaviti belgilari to‘plamining quvvatini sanoqli bo‘lishi (ya’ni natural sonlar to‘plamiga ekvivalent bo‘lishi) shartlaridan birining bajarilishini talab etadi. Bu shartlar kriptoalgoritmning mutlaqo bardoshli bo‘lishi uchun zarur va yetarlidir. Amalda ko‘plab hollarda nazariy bardoshli kriptotizimlarning yaratilishi maxfiy kalit hajmining cheksiz katta bo‘lib ketishi masalasi bilan bog‘liq. Shunday qilib, kriptografik tizimning nazariy bardoshliligi tushunchasi kriptografik tizimlarni baholashga aniqlik kiritadi, ammo mutlaqo bardoshli bo‘lgan kriptotizimlarning yaratilishi va ulardan amalda foydalanishning qulay hamda samarali bo‘lishi nuqtai nazardan mumkin bo‘lmaydi. Bundan kelib chiqib, E.K.Shennon kriptografik algoritm va kriptotizimlarning tatbiqlarida foydalanuvchilarga qulay va samarali bo‘lib, zamonaviy ilm-fan hamda texnika yutuqlarining real istiqbolli yuqori imkoniyatlariga tayangan holda kriptotahlil uchun qancha vaqt va moddiy xarajatlarni sarf bo‘lishini hisobga olgan holda amaliy bardoshlikning ta’rifini ifodaladi. Kriptoalgoritm va kriptotizimlarning amaliy bardoshliligi - kriptoanalitik (kriptotahlilchi) kriptografik tizimning tahlili uchun yetarli darajadagi ilmiy hamda texnik va boshqa kerakli vositalarga ega bo‘lmaganda, shuningdek kriptotahlil muddati chegaralanganda uning bardoshliligi qanday bo‘lishini aniqlashdan iborat [7].

Shunday qilib, K.Shennonning kriptografiyaga qo‘shgan hissasi entropiya yondashuviga asoslangan kriptografik tizimlarning mustahkamligi uchun asosiy tamoyillar va shartlarni kiritishdan iborat bo‘ldi. Bunda quyidagicha tartibda entropiya hisoblanishi keltiriladi. Diskret signalning N ta mumkin bo‘lgan holatga ega entropiyasi quyidagicha hisoblanadi [8]:

$$H(x) = -\sum_{i=1}^{N} p(i)\log p \qquad (1)$$

bu yerda $p(1), p(2),..., p(N)$ qiymatlar $x_1, x_2,..., x_N$ alifbo elementlarining paydo bo‘lish ehtimoli.

Alifboning barcha elementlari uchun yuzaga kelish ehtimoli bir xil bo‘lgan holatlar uchun

$$p(1) = p(2) = ... = p(N) = \frac{1}{N} \qquad (2)$$

bu yerda

$$H(x) = -\sum_{i=1}^{n}\left(\frac{1}{N}\right)\log\left(\frac{1}{N}\right) = \log N \qquad (3)$$

Ideal kriptobardoshli (mutlaqo, nazariy jihatdan aniqlab bo‘lmaydigan) tizim mavjudligi uchun zarur shartlar [9]:

1. Agar biron bir kriptogramma ushbu kriptogrammada shifrlangan ma’lumotni haqidagi ma’lumotni qo‘shmasa, tizim mutlaqo xavfsizdir.

$$I(E, M) = 0, \qquad (4)$$

bu yerda I – ma’lumotlar soni, E – kritogramma, M – xabar matni.

Kalitni bilmagan holda kriptogrammani ushlab olishda ma’lumot miqdori nolga teng.

$$I(E, M) = H(M) - H(M / E), \qquad (5)$$

bu yerda $H(M)$ – xabar manbasining entropiyasi, $H(M/E)$ – kriptogramma ushlangan bo‘lsa, xabarning shartli entropiyasi.

Shuni aytish mumkinki, $P(M) = P(M/E)$ kriptogrammani bilish xabarni bilish ehtimolini o‘zgartirmaydi.

2. Kalitlar soni xabarlar sonidan kam bo‘lmasligi kerak

$$L^N \geq m^n \quad (6)$$

bu yerda L – kalit ma’lumotining alifbo hajmi, N – kalit uzunligi, m – xabar alifbo hajmi, n – xabar uzunligi.

3. Kalit uzunligi xabar uzunligidan kam bo‘lmasligi kerak. (6) tengsizlikning har ikki tarafi logarifmlab yuboriladi:

$$\log L^N \geq \log m^n \quad (7)$$

Bundan kalit uzunligi ushbu ifoda bilan hisoblanadi

$$N \geq \frac{n \log m}{\log L} \quad (8)$$

Yuqoridagi (8) tengsizlik – mutlaqo maxfiy tizimlar uchun Shennon chegarasini aniqlaydi, ya’ni maxfiy kalitning qiymati shu kalit bilan shifrlanadigan ma’lumotning qiymatidan kichik bo‘lmasligi kerak. Agarda maxfiy kalit L_Z bo‘lgan alifboning belgilaridan tuzilgan bo‘lib, uning hajmi K ga teng bo‘lsa, u holda maxfiy kalitning qiymati bahosi

$$H(Z) \leq \log(L_Z^K) = K \log L_Z \quad (9)$$

tengsizlik bilan, ochiq ma’lumot elementlari soni L_X alifboning belgilaridan tuzilgan bo‘lib, uni tashkil etuvchi belgilar M bo‘lsa, u holda ochiq ma’lumot qiymatining bahosi

$$H(X) \leq M \log L_X \quad (10)$$

bilan hisoblanadi.

Shunday qilib, agarda $L_X = L_Z$ bo‘lib, ochiq ma’lumot butunlay tasodifiy bo‘lsa, (9) va (10) ifodalardan $K \geq M$ tengsizlikka ega bo‘linadi. Bu munosabat esa kalitning hajmi (uzunligi) ochiq ma’lumot hajmidan kam bo‘lmasligi kerakligini ko‘rsatadi [10].

Mutlaqo kriptobardoshli kriptografik tizimlarning afzalliklari :

1. Qo‘llaniladigan tizimlarning mutlaqo (nazariy) kriptobardoshliligi ixtiyoriy ma’lumotlarni shifrlanmaslik kafolati bilan uzatish va saqlash imkonini berishi kerak.

2. Tizimni ishlab chiqish va amaliyotda qo‘llash juda oddiy bo‘lishi zarur.

3. Ishonchlilik: mutlaqo kriptobardoshli kriptografik tizimlar ishonchlilikning yuqori darajasiga ega, ya’ni ularni zamonaviy hisoblash resurslari bilan buzish qiyin yoki amalda imkonsizdir.

4. Axborotni himoya qilish: kriptobardoshli kriptografik tizimlar axborotni yuqori darajada himoya qiladi. Ular murakkab matematik algoritmlar va shifrlash usullaridan foydalanib hujumlarga bardoshli hisoblanadi va ma’lumotlarning konfidensialligini saqlash imkonini beradi [11].

3. Masshtablilik: kriptobardoshli kriptografik tizimlar faoliyatning turli sohalarida qo‘llanilishi hamda turli tarmoq va kompyuter tizimlariga moslashtirilishi mumkin. Ularning yangi variantlarini ishlab chiqib, kengaytirish mumkin.

5. Standartlarni qo‘llab-quvvatlash: kriptobardoshli kriptografik tizimlar odatda belgilangan xalqaro standartlar va protokollarga mos keladi. Bu ularning muvofiqligini va ushbu standartlarga amal qiladigan boshqa tizimlar bilan ma’lumot almashishini ta’minlaydi.

6. Hujumlarga qarshilik: Mutlaqo kriptobardoshli kriptografik tizimlar qo‘pol kuch hujumlari, kriptotahlil yoki zaifliklar kabi har xil turdagi hujumlarga dosh berishga mo‘ljallangan bo‘ladi.

Kriptobardoshli kriptografik tizimlarning kamchiliklari [12]:

1. Asosiy ma’lumotlarning katta miqdori

2. Asosiy ma’lumotlarni yetkazib berish uchun tashkiliy tuzilmaning murakkabligi.

Kriptografik tizimlarning kriptobardoshli bo‘lishi uchun talablar [13]:

1. Kalitlar soni cheksiz katta bo‘lishi kerak.

Agar 256 bit uzunlikdagi kalit bo‘lsa, unda kalitlarning umumiy soni 2256 = 1,16·1077 bo‘ladi, sekundiga 106 bit sig‘imli kompyuterda ishlaganda, umumiy qidirish vaqti 3,67·1063 yilni tashkil qiladi. Agar kompyuter tezligi 3 darajaga, ya’ni sekundiga 109 bit ishlashga oshirilsa, u holda kalit uzunligini 10 bitga oshirish kerak (1-jadval).

Misol uchun, bitlari soni 2^n tadan iborat bo‘lgan ochiq matnni juftliklarga ajratilsa, ular soni n ta bo‘ladi. Bunday jadvalli akslantirishning, kalitni bilmagan holda ochish murakkabligi $4^n=2^{2n}$ bo‘ladi. Bu esa barcha mumkin bo‘lgan ochiq matnlarni tahlil qilish zaruriyligini ta’minlaydi va bunday jadvalli akslantirishning maksimal kriptobardoshli ekanligini ko‘rsatadi.

1-jadvaldan ko‘rinib turibdiki, kalit uzunligi 1 bitga oshganda, kalitni sanab o‘tishga urinishlar soni taxminan 2 baravar ortadi.

2. Xabarlar statistikasi kriptogramma statistikasidan chiqarib tashlanishi kerak.

Masalan, rus alifbosida oddiy almashtirish shifrlashdan foydalanilganda mumkin bo‘lgan kombinatsiyalar soni 32! =2,63·1035. Biroq, rus alifbosidagi harflarning paydo bo‘lish chastotasiga ko‘ra, uzatilgan xabarni osongina hisoblash mumkin. Rus harflarining paydo bo‘lish chastotasi avvaldan berilgan (2-jadvalda). Buning uchun kriptogrammadagi harflarning takrorlanish chastotasini hisoblash kerak bo‘ladi. Kriptogramma matni bo‘ylab eng yuqori chastotali harf bo‘sh joy yoki tinish belgisi sifatida qabul qilinadi, bir oz pastroq chastotasi "o", eng past chastotasi "e" yoki "щ" va shunga o‘xshash. Kriptogrammaning hajmi qanchalik katta bo‘lsa, statistik ma’lumotlar shunchalik ko‘p bo‘ladi va bu kriptogrammani ochish osonroq bo‘ladi. Bundan tashqari, rus tilida sodda so‘zlar ko‘p, masalan, ko‘p so‘zlar unlilarsiz ifodalasa ham bo‘ladi va ularni topish mumkin bo‘ladi.

1-jadval

Kalitni topishga urinishlar sonining kalit uzunligiga bog‘liqligi

Kalit uzunligi	Urinishlar soni
58	288 230 376 151 711 000
59	576 460 752 303 423 488
60	1 152 921 504 606 846 976
61	2 305 843 009 213 693 952
62	4 611 686 018 427 387 904
63	9 223 372 036 854 775 808
64	18 446 744 073 709 551 616
65	36 893 488 147 419 103 232

2-jadval

Rus alifbosining chastotaviy qiymatlari

Xarf	Chastota	Xarf	Chastota	Xarf	Chastota	Xarf	Chastota
о	0,09	в	0,038	з	0,016	ж	0,007
е	0,072	л	0,035	ы	0,016	ш	0,006
а	0,062	к	0,028	б	0,014	ю	0,006
и	0,062	м	0,026	ь, ъ	0,014	ц	0,004
н	0,053	л	0,025	г	0,013	щ	0,003
т	0,053	п	0,023	ч	0,012	э	0,003
с	0,045	у	0,021	й	0,01	ф	0,003
р	0,04	я	0,018	х	0,009		

Bo‘sh joy va tinish belgilarining paydo bo‘lish ehtimoli 0,174 ga teng.

3. Tutib olingan kriptogrammada ochiq ma’lumotning ba’zi qismlari ma’lum bo‘lgan taqdirda ham shifrni ochish imkoni bo‘lmasligi kerak.

Kriptogrammada shifrlangan ma’lumotlarning bir qismini bilish kriptogrammaning keyingi qismini parolini ochish uchun ba’zi asosiy ma’lumotlarni ochishga ta’sir qilmasligi kerak. Ushbu talabga rioya qilmaslik kriptotizimning kriptografik bardoshliligini sezilarli darajada kamaytiradi [14].

Kriptografik tizimlar bardoshliligiga qarab uch sinfga ajraladi:

1) Mutlaqo bardoshli kriptografik tizimlar: Bu tizimlar shifrlashni mutlaqo ochib bo‘lmaydigan, ya’ni nazariy jihatdan shifrni ochib bo‘lmaydigan hisoblanadi. Ular hatto cheksiz hisoblash resurslaridan foydalangan holda ham buzilmaydigan matematik tamoyillarga asoslanadi. Masalan, Shennon shifrlash bilan bog‘liq axborot nazariyasi.

2) Nisbatan bardoshli kriptografik tizimlar: Mutlaqo bardoshli tizimlardan farqli ravishda nisbatan bardoshli tizimlar muayyan hisoblash yoki matematik tahlillarga asoslanadi. Agar ular katta sonlarni faktorlash yoki murakkab matematik muammolarni hal qilish kabi muayyan hisoblash vazifalarini bajara olmasalar ham mustahkam hisoblanadi. Nisbatan bardoshli kriptografik tizimga misol sifatida RSA algoritmini keltirish mumkin.

3) Vaqtincha bardoshli kriptografik tizimlar: Bu tizimlar vaqt o‘tishi bilan kriptoanalitik texnika va hisoblash resurslari yaxshilanadi degan ma’lumotga asoslanadi. Shuning uchun ular faqat ma’lum vaqt davomida yoki ma’lum hisoblash qobiliyatlari doirasida qat’iylikni ta’minlaydi. Bunday tizimlar o‘zgaruvchan hisoblash quvvatiga rioya qilish uchun davriy yangilanishlar va almashtirishlarni talab qiladi [15].

XULOSA. Kriptoalgoritmlar mutlaqo bardoshli yoki mutlaqo maxfiylikni ta’minlashi uchun quyidagi xususiyatlarga ega bo‘lishi kerak:

1) O‘rniga qo‘yish shifrlash algoritmlarining ko‘p alfavitli sinfiga tegishli bo‘lishi: shifrlash jarayoni

bosqichlarida ochiq ma’lumot alifbosi belgilarini shifrma’lumot alifbosi belgilariga almashtirish jadvalida shifrma’lumot alifbosi belgilarining joylashish tartibi o‘zgarib turishi lozim;

2) Kalit uzunligi yetarli katta (cheksiz bo‘lmasada) yoki shifrlash alfaviti belgilari to‘plamining quvvatini (sanoqli bo‘lmasada) yetarli katta bo‘lishi ta’minlangan bo‘lishi kerak;

3) Algoritmning akslantirishi amallari bajarilishida maxfiy kalitning bitta belgisini shifrlanishi kerak bo‘lgan ma’lumotning ham faqat bitta belgisiga bog‘liq bo‘lishi shart;

4) X - ochiq ma’lumot va Y – shifrma’lumotlarning statistik bog‘liq emasligi ta’minlangan bo‘lishi, ya’ni ixtiyoriy x - ochiq ma’lumot va y -shifrma’lumot uchun ularning ehtimolligi munosabatlari bilan aniqlanuvchi ushbu tenglik $P(X=x/Y=y)=P(X=x)$ o‘rinli bo‘lishi kerak;

5) Kalitning hajmi (uzunligi) K ochiq ma’lumot hajmidan (uzunligidan) M dan kam bo‘lmasligi kerak $K \geq M$;

6) Shifrlash kaliti faqat bir marta ishlatilishi kerak.

Bu keltirilgan shartlarni bajarilishi kriptoalgoritmlarning amaliy jihatdan mutlaqo bardoshli yoki mutlaqo maxfiylikni ta’minlovchi bo‘lishining yetarlilik shartlari-kriteriylari deb qabul qilinishi mumkin.

Kerakli bardoshlilik darajasiga va ma’lumotni himoya qilish kerak bo‘lgan vaqtga qarab tegishli kriptografik tizimdan foydalanish muhimdir.

Mutlaqo bardoshli va nisbatan bardoshli kriptografik tizimlar axborot xavfsizligining yuqori darajada ta’minlaydi va uzoq muddat himoya talab qilinadigan hollarda qo‘llanilishi mumkin.

Vaqtincha bardoshli kriptografik tizimlar ma’lumotlar qisqa vaqt davomida sir saqlanishi kerak bo‘lgan holatlarda foydali bo‘lishi mumkin. Ular, masalan, ma’lum vaqtdan keyin ahamiyatini yo‘qotadigan yoki ahamiyatini yo‘qotgan ma’lumotlarni uzatishda qulay bo‘lishi mumkin. Biroq, vaqtincha bardoshli kriptografik tizimlardan foydalanishda o‘ziga mos cheklovlar mavjud, chunki yuqorida ko‘rsatib o‘tilganidek, bunday kriptografik tizimlar zarur himoya darajasini saqlab turish uchun davriy yangilash va almashtirishni talab qiladi.

Taklif etilayotgan tasniflardan axborot tizimini loyihalashda kriptografik tizim sinfini tanlashda foydalanish mumkin. Tasniflash ma’lumotlarni himoya qilish darajasi, algoritmlar turlari, qo‘llab-quvvatlanadigan funksionallik va ishlash talablari kabi omillarni hisobga oladi. Ushbu mezonlarga asoslanib, axborot tizimidagi ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash uchun eng mos kriptografik tizimni tanlash mumkin.

ADABIYOTLAR

1. Калиновский, С. М. (2023). Классификация криптографических систем по стойкости.

2. Акбаров, Д. Е. (2009). Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. Ўзбекистон маркаси, 432.

3. Акбаров, Д. Е., Мухтаров, Ф. М., & Сиддиқов, А. А. (2014). Криптотаҳлил масалаларига тизимли ёндошув асослари ва уларни ечиш усуллари. Т.:—Фарғона, 142.

4. Гатченко, Н. А., Исаев, А. С., & Яковлев, А. Д. (2012). Криптографическая защита информации.

5. Салий, В. Н. (2017). Криптографические методы и средства защиты информации. Саратов–2017.

6. Шеннон, К. (2009). Теория связи в секретных системах [Электронный ресурс]. Режим доступа: http://www. enlight. ru/crypto/articles/shannon/shann__i. htm–свободный.–11.09.

7. Шурховецкий, Г. Н. (2018). Криптостойкость алгоритмов шифрования. Молодая наука Сибири: электрон. науч. журн, (2).

8. Курьязов, Д. М., Саттаров, А. Б., & Ахмедов, Б. Б. (2017). Блокли симметрик шифрлаш алгоритмлари бардошлилигини замонавий криптотаҳлил усуллари билан баҳолаш. Ўқув қўлланма. Тошкент:“Aloqachi, 228.

9. Калиновский, С. М. (2023). Классификация криптографических систем по стойкости.

10. Брауде-Золотарев, Ю. М. (2010). Абсолютно криптостойкие и самые простые шифраторы. Электросвязь, (3), 55-57.

11. Азизович, У. Б., & Азизжонович, У. Ш. (2021). Жадвалли алмаштиришлар асосидаги симметрик блокли шифрлаш алгоритмининг криптобардошлик критерийлари. Ахборот-

коммуникация технологиялари ва телекоммуникацияларнинг замонавий.

12. Акбаров, Д. Е., Кушматов, О. Э., Умаров, Ш. А., & Шаев, А. К. (2021). Исследование особенностей критерия стойкости алгоритма хеш-функции. CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES, 2(11), 60-64.

13. Азязова, Е. А., & Коровин, А. А. (2019). Криптостойкость шифров. Математическое и программное обеспечение вычис, 32.

14. Фомичёв, В. М., & Мельников, Д. А. (2019). Криптографические методы защиты информации.

15. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. (2022). Crypto-resistant methods and random number generators in internet of things (iot) devices. Innovative Technologies and Scientific Solutions for Industries, (2 (20)), 22-34.