TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

OCHILOV NIZOMIDDIN NAJMIDDIN O‘G‘LI

OCHIQ KODLI OPERATSION TIZIMLARDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent-2023

UDK: 004.451.8(09)

Texnika fanlari doktori (DSc) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора (DSc) по техническим наукам

Contents of dissertation abstract of the doctor (DSc) on technical sciences

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

OCHILOV NIZOMIDDIN NAJMIDDIN O‘G‘LI

OCHIQ KODLI OPERATSION TIZIMLARDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent-2023

Texnika fanlari doktori (DSc) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2022.3.DSc/T541 raqam bilan ro‘yxatga olingan.

Dissertatsiya Toshkent axborot texnologiyalari universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasida (www.tuit.uz) va "Ziyonet" Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy maslahatchi:	**Karimov Madjit Malikovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Irgasheva Durdona Yakubdjanovna** texnika fanlari doktori, professor
	Kerimov Kamil Fikratovich texnika fanlari doktori, dotsent
	Kuryazov Davlatyor Matyakubovich fizika-matematika fanlari doktori.
Yetakchi tashkilot:	**Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti.**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.01 Ilmiy kengashning 2023 yil ___ _____ soat __ dagi majlisida bo‘lib o‘tadi. (Manzil: 100202, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43, faks: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Dissertatsiya bilan Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (_____ raqam bilan ro‘yxatga olingan.). (Manzil: 100202, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-65-44).

Dissertatsiya avtoreferati 2023 yil ___ _____ da tarqatildi.
(2023 yil ___ _____ dagi ___ raqamli reyestr bayonnomasi.)

B.SH. Maxkamov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, i.f.d., professor

E.SH. Nazirova
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, t.f.d., professor

S.K. Ganiyev
Ilmiy darajalar beruvchi Ilmiy kengash qoshidagi Ilmiy seminar raisi, t.f.d., professor

KIRISH (fan doktori (DSc) dissertatsiyasining annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahonda axborot xavfsizligi (AX) tizimlarini ishlab chiqishga va ularni takomillashtirishga alohida e'tibor qaratilmoqda. Axborot-kommunikatsiya tizimlari rivojining hozirgi darajasida samarali AXni ta'minlashning birmuncha muhim mexanizmlaridan biri bo'lgan operatsion tizimlarni himoyalash masalasi ayniqsa dolzarb bo'lib qolmoqda. "Kasperskiy laboratoriyasi ma'lumotlariga ko'ra, 2022-yilda Hindistonda kiberhujumlar soni 2020-yilga nisbatan 1,23 barobarga (23,7 foiz) oshgan. Qozog'iston Respublikasi (14,38 foiz) va Rossiya Federatsiyasida (18,45 foiz) ham bunday hujumlarni aniqlash 2021-yilga nisbatan 1,3 barobarga oshgan".[1] Shu munosabat bilan Gollandiya, Germaniya, Buyuk Britaniya, Shvetsiya, Fransiya va boshqalar kabi Yevropa Ittifoqining bir qancha davlatlari kiberhujumlarga qarshi kurashish sohasida ish boshladi. Axborot tizimlari xavfsizligini va tizim fayllarini himoya qilishni yuqori darajada ta'minlovchi dasturiy-texnik vositalar hamda shifrlash mexanizmlarini ishlab chiqishga alohida e'tibor qaratilmoqda.

Jahonda ma'lumotlarni shifrlashning zamonaviy algoritmlari samaradorligini oshirish va operatsion tizimlarning (OT) himoyalanish darajasini oshirishga alohida e'tibor qaratilmoqda. Bu yo'nalishda olib borilayotgan ilmiy-tadqiqot ishlarida quyidagi jihatlarga alohida e'tibor qaratilmoqda: kompyuter tizimlarining ishonchli himoyasini ta'minlash maqsadida ma'lum toifadagi resurslarga shifrlash algoritmlariga asoslangan cheklash usullarini ishlab chiqish. Bunga zamonaviy shifrlash usullari va tizim fayllarini shifrlash kabi himoya vositalari majmuasidan foydalanish orqali erishiladi. OTlarda axborot tizimlarini himoya qilish uchun dasturiy ta'minotlarini ishlab chiqish ham davom etib kelmoqda. Bu kabi o'zgarishlarning barchasi yuqori darajadagi xavfsizlikni ta'minlashga qaratilgan.

Respublikamiz davlat va xo'jalik boshqaruvi organlarida axborot texnologiyalarini rivojlantirish bilan bir qatorda, kompyuter tizimlarida ma'lumotlarni himoyalash vositalari va usullarini keng qo'llashga va ma'lumotlarni OTlardagi tahdidlardan himoyalashga alohida e'tibor qaratilgan. Shu munosabat bilan kompyuter tizimlaridagi tahdidlar va hujumlarni aniqlash va ularni bartaraf etish borasida sezilarli natijalarga erishilgan. Jumladan, kompyuter tizimlarining himoyalanganligini ta'minlash maqsadida axborot xavfsizligining monitoringi tizimini, hujumlarni aniqlash va ularni bartaraf etish tizimini ishlab chiqish yo'lga qo'yilgan.

O'zbekiston Respublikasi Prezidentining «2022-2026 yillarga mo'ljallangan Yangi O'zbekistonning Taraqqiyot strategiyasi to'g'risida»gi, 2022 yil 28 yanvardagi PF-60-son, «Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to'g'risida» gi Farmonlari, 2018 yil 21 noyabrdagi PQ-4024-son «Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to'g'risida» gi va 2019 yil 14 sentabrdagi PQ-4452-son «Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar

[1] https://securelist.ru/it-threat-evolution-in-q1-2022-non-mobile-statistics/105173/

to‘g‘risida» gi Qarorlari hamda mazkur faoliyatga tegishli boshqa meyoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya tadqiqoti ma’lum darajada xizmat qiladi.

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

Dissertatsiya mavzusi bo‘yicha xorijiy ilmiy-tadqiqotlar sharhi.

Jahondagi ko‘plab mamlakatlarda ochiq kodli operatsion tizimlarda axborot xavfsizligini ta’minlash borasida ishlar olib borilmoqda. Linux, FreeBSD va boshqalar kabi ochiq kodli operatsion tizimlar va ularning rivojlanishi va xavfsizligiga hissa qo‘shadigan ishlab chiquvchilar va xavfsizlik bo‘yicha ekspertlarning global hamjamiyati mavjud. Ochiq kodli operatsion tizimlarda axborot xavfsizligini ta’minlash borasida ishlar olib borayotgan ayrim mamlakatlarni e’tirof etish joiz.

AQShda ochiq kodli operatsion tizimlarda axborot xavfsizligi sohasida tadqiqot olib boruvchi ko‘plab tashkilotlar, institutlar va universitetlar mavjud. NSA (Milliy xavfsizlik agentligi), NIST (Milliy standartlar va texnologiyalar instituti) va CERT (kompyuter favqulodda vaziyatlariga javob beruvchi guruh) kabi tashkilotlar tadqiqot va operatsion tizimlar xavfsizligini ta’minlash usullari va algoritmlarini ishlab chiqish bilan faol shug‘ullanmoqda.

Yevropaning Germaniya, Fransiya, Buyuk Britaniya, Italiya va boshqa mamlakatlarida ochiq kodli operatsion tizimlarda axborot xavfsizligini ta’minlash usullarini tadqiq qilish va ishlab chiqish ishlari olib borilmoqda. Boxum shahridagi Rur universiteti (Germaniya), ENISA (Yevropa Ittifoqining tarmoq va axborot xavfsizligi agentligi) va OWASP (web-ilovalarning ochiq xavfsizlik loyihasi) kabi ayrim universitetlar va tadqiqot markazlari mazkur yo‘nalishda tadqiqotlar olib bormoqda. Shuningdek, Kanadada ham ochiq kodli operatsion tizimlarda axborot xavfsizligi bo‘yicha faoliyat yurituvchi ishlab chiquvchilar va tadqiqotchilarning faol hamjamiyati mavjud. Ayrim universitetlar, jumladan Vaterloo va Kalgari kabi universitetlar kiberxavfsizlik sohasidagi tadqiqot va ishlanmalarda faol ishtirok etib kelmoqda.

Rossiya Federasiyasi ham ochiq kodli operatsion tizimlarda axborot xavfsizligini ta’minlash ustida ishlar olib bormoqda. Turli tashkilotlar, jumladan, Rossiya kompaniyalari, universitetlari va tadqiqot markazlari universitetlar, institutlar va xususiy kompaniyalarda operatsion tizimlar xavfsizligini oshirish va ishlab chiqish bo‘yicha faol tadqiqot olib bormoqdalar. Rossiya Federasiyasida maxsus xizmat vakillari buyurtmasiga muvofiq ROSA Labs kompaniyasi tomonidan ishlab chiqilgan va qo‘llab-quvvatlanuvchi ochiq kodli “ROSA Linux” operatsion tizimi ishlab chiqilib, amaliyotga joriy etilgan.

Shu munosabat bilan, mazkur mavzu bo‘yicha ilmiy ishlarning aksariyat qismi maxfiy bo‘lgani sababli, Internet tarmoqlarida qator yetakchi mamlakatlar tomonidan ishlab chiqilgan va ishga tushirilgan ochiq kodli operatsion tizimlar bilan yaqindan tanishish va ma’lumotlarni tahlil qilish va ulardan foydalanish imkoniyati mavjud emas. Bu esa, o‘z navbatida, mazkur yo‘nalishda ish olib borayotgan

tadqiqotchilar uchun qiyinchiliklar tug‘diradi.

Muammoning o‘rganilganlik darajasi. L.Torvalds, R.Xersog, B.Kernigan kabi olimlar Linux oilasiga mansub bo‘lgan operatsion tizimlarni ishlab chiqish borasida tadqiqotlar olib borganlar. R.Payk, B.Uord, D.Barrett, S.Alapati, A.Robachevskiy, D.N.Kolesnichenko, M.Flenov, S.Nemnyugin, O.Stesik, T.Adelshtayn, B.Lyubanovich, S.L.Sklovskaya kabi xorijlik va mamlakatimiz olimlarining Linux OT dagi ma’lumotlarni himoyalash tizimini yaratish sohasidagi ilmiy-tadqiqot ishlari o‘rganib chiqilgan. MDH davlatlari hamda O‘zbekiston Respublikasi ilmiy ishlanmalarida algoritmlarni shifrlash, himoyalash vositalarining turli usullari, modellari va algoritmlari, axborotni himoyalashning nazariy va amaliy tamoyillari, axborotni himoyalash vositalari va usullarini ishlab chiqish bo‘yicha «Astra Linux», «Zarya» OT lari, «Alt Linux», «ROSA» kabi operatsion tizimlar o‘rganib chiqilgan. Turli davlat muassasalarida qo‘llaniluvchi «Doppix» grafik qobiqlari o‘rganilgan.

M.M. Karimov, X.A.Muzaffarov, G‘.U. Jo‘rayev va A.Ikromovlar ilmiy maqolalarida GOST 28147-89 algoritmi bilan shifrlash va himoya tizimlarini yaratish usullari o‘rganib chiqilgan. D.N.Kolesnichenko va V.Allenlar ilmiy ishlarida, Linux Format jurnalining 2014, 2015 va 2016 yillaridagi barcha sonlarida Linux OT yadrosi algoritmlari va tuzilmasi, paket ma’lumotlarga ishlov berish tezligi, xavfsizlik modellari, xavfsizlikni ta’minlash vositalari tadqiq qilingan.

Shu bilan birga, tarmoqdagi tahdidlardan himoyalash vositalari va usullari to‘la tahlil qilinmagan, mavjud algoritmlardagi kamchiliklar aniqlangan hamda noqonuniy ta’sirlardan himoyalovchi qurilmalarni boshqarish vositalari yetarli darajada o‘rganilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan muassasaning ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Davlat test markazining innovatsion faoliyat sohasida uch yilga mo‘ljallangan “Yo‘l xaritasi”ning 2022 yil uchun mo‘ljallangan dasturiga muvofiq “Axborot tizimlari uchun himolangan tizim va vositalarni ishlab chiqish” mavzusidagi loyihalari doirasida bajarilgan.

Tadqiqotning maqsadi ochiq kodli OT larda milliy shifrlash algoritmlari asosida xavfsizlik talablariga muvofiq, shuningdek, maxfiy ish yuritish sohasidagi standartlar talablarini qondiruvchi maxsus usullar va algoritmlarni ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

zamonaviy ochiq kodli OT larda shifrlash algoritmlarining sifat ko‘rsatkichlarini baholashning tasnifi va parallellashtirish masalalari yordamida shifrlash rejimlarini tahlil etish;

himoyalangan fayllar tizimini (HFT) ishlab chiqishda B+ fayllar strukturasidan foydalanishga qo‘yiladigan talablar va HFT tizimlarini yaratish algoritmlari, HFTlarda katalog va jurnallarni tashkil etish;

ochiq kodli OT yadrosi tarkibida shifrlashni tashkillashtirish usullari va ishlash algoritmlarini yaratish;

ochiq kodli OT larda arxivlash yordamida GOST 28147-89 va O‘zDSt 1105:2009 algoritmi asosida shifrlash usullarini va ruxsat etilgan tashqi qurilmalarni

ro‘yxatga olish, o‘chirish va formatlash algoritmi va mexanizmlarini ishlab chiqish, ularga shifrlangan ma’lumotlarni yozish algoritmini yaratish;

GOST 28147-89 algoritmi yordamida shifrlash va arxivlash orqali OT dagi ma’lumotlarning himoyalanganligini tashkillashtirish, initsializatsiya jarayonida tizim fayllarini shifrlash va rasshifrlashni tashkil etish, OT ning fayl tizimi uchun shifrlashning grafik dasturiy ta’minotini ishlab chiqish va grafikli dasturiy majmuasining ishlashining samaradorligini baholashdan iborat.

Tadqiqot obyekti sifatida ochiq kodli OT larda mahalliy shifrlash algoritmlari va ular yordamida yaratilgan himoyalangan fayl tizimlari olingan.

Tadqiqot predmeti sifatida ochiq kodli OT dagi mahalliy standartlar asosida shifrlash usullari va algoritmlari olingan.

Tadqiqot usullari. Tadqiqot jarayonida axborotni himoyalash usullaridan, algoritmlar nazariyasidan, matematik usullaridan hamda tartibli va obyektga yo‘naltirilgan dasturlashdan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat**:**

ochiq kodli OT larda shifrlash algoritmlarining samaradorligini ta’minlashda parallel hisoblash texnologiyasi yordamida kriptobardoshliligi baholandi;

ext3/4 fayl tizimlari bilan ishlash uchun optimallashtirilgan algoritmlar taklif qilingan va HFTda, yadroda shifrlash algoritmlari turli o‘lchamdagi fayllar uchun sinovdan o‘tkazilgan shuningdek, fayllarni o‘qish va yozishnin zamonaviy usullari taklif etilgan;

milliy shifrlash algoritmlari asosida xavfsizlik talablariga muvofiq va maxfiy ish yuritish sohasidagi maxsus usullar va algoritmlari taklif etildi hamda O‘zDSt 1105:2009 standartining kriptobardoshliligi statistik tahlillar yordamida baholandi;

ruxsat etilgan tashqi qurilmalarga shifrlangan ma’lumotlarni yozishni ta’minlash OT tomonidan amal oshirilishi natijasida, tashqi kiruvchi/chiquvchi qurilmalarni OT yadrosi darajasida ro‘yxatga olishning majburiy va ulardagi ma’lumotlarni xavfsizligini ta’minlash uchun shifrlash amalini bajarish usuli ishlab chiqilgan;

GOST 28147-89 algoritmi yordamida shifrlash va arxivlash orqali OTdagi ma’lumotlarning maxfiyligini ta’minlash maqsadida butun initsializatsiya zanjirini shifrlash UEFI Secure Boot (UEFI dasturlarda elektron raqamli imzolarni tekshiruvchi protokol) va GPG (ma’lumotlarni shifrlash va elektron raqamli imzolarni yaratish dasturi) dan foydalangan holda, tizimni almashtirishdan va tizim dasturlarini buzishdan samarali himoya usuli taklif etilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

O‘zDSt 1105:2009 shifrlash algoritmiga almashtirish jadvallarining har biri uchun chiziqli va differensial usul yordamida avtomatik ravishda sifatni baholash funksiyasini qo‘llagan holda, hujumlar uyushtirildi va ularning kriptobardoshliligi aniqlangan;

himoyalangan fayllar tizimida fayl bloklari va inodlar algoritmlari va ularning ishlash blok-sxemasi sinov tariqasida turli xil o‘lchamdagi fayllarda testlar o‘tkazilib, baholangan va HFT laridan fayllarni o‘qish va yozishda taklif etilayotgan algoritm ext3/4 da ishlovchi tizimlarda ishlash samaradorligi o‘rtacha 0.5 baravarga oshirilgan;

ochiq kodli OT larda O‘zDSt 1105:2009 standarti asosida kalitlar yordamida shifrlash dasturi exe faylari faqat bitta seans kaliti bilan shifrlashda 10%dan kam bo‘lmagan zichlash samaradorligiga erishilgan;

tajribalar yordamida maxsus yaratilgan arxivlash hamda mahalliy standart yordamida shifrlash dasturida lug‘at hajmi 256 Mbdan oshmasligini inobatga olib, maksimal rejimda arxivlash tezligi fayl parametrlarini kamaytirish orqali o‘rtacha 2-3 martagacha oshirish mumkinligi isbotlangan;

yaratilgan kriptografik modul mahalliy standartga javob berishi uchun sinovdan o‘tkazilgan va mahalliy standartlar asosida shifrlash/rasshifrlash algoritmini amalga oshirishi tasdiqlangan.

Tadqiqot natijalarining ishonchliligi. Natijalarni miqdor va sifat jihatdan baholashni qo‘llagan holda, tadqiqotning maqsadi va vazifalari, predmetga mos bo‘lgan usullarda nazariy va amaliy darajada tadqiqot o‘tkazish orqali tadqiqot metodologiyasining asoslanganligi ta’minlangan.

Tadqiqot natijalarining ilmiy ahamiyati. Ma’lumotlarni jismoniy va mantiqiy himoyalash usullarida hamkorlikdan foydalanish va ajratish tamoyilini joriy qilish asosida AX tizimlarining funksional imkoniyatlarini kengaytirishga imkon beruvchi algoritmlar va dasturiy vositalar ishida tavsiya etilgan amaliy aprobatsiyalardan iborat. Axborotni himoyalash va unga ishlov berish uchun universal mexanizmlar tavsiya etilgan va algoritmlar ishlab chiqilgan. Tavsiya etilgan algoritmlar O‘zbekiston Respublikasi qonunchiligiga muvofiq, ochiq kodli OT lar uchun xavfsizlik talablariga muvofiq algoritmlar va usullarni ishlab chiqish imkonini beradi.

Tadqiqot natijasining amaliy ahamiyati. O‘zDSt 1105:2009 hamda GOST 28147-89 shifrlash algoritmlari talablariga muvofiq va maxfiy ish yuritish sohasidagi axborotni himoyalashni ta’minlash uchun davlat va huquqiy organlar tomonidan uning xulosalaridan foydalanish bilan bog‘liq bo‘lgan davlat yoki tijorat muassasalarida qo‘llash mumkin bo‘lgan axborot xavfsizligini ta’minlash tizimini ishlab chiqishdan iborat. Tadqiqot natijalarining amalda joriy qilinishi O‘zbekiston Respublikasi vazirliklari va idoralarida foydalanuvchi axborot tizimlari va texnologiyalarini qo‘llash bilan bog‘liq bo‘lgan AXning birmuncha asoslangan va maqsadga yo‘naltirilgan siyosatini ta’minlashga imkon beradi.

Tadqiqot natijalarining joriy qilinishi. Ishlab chiqilgan AXni ta’minlash vositalari va usullari hamda yaratilgan algoritmlari bo‘yicha olingan natijalar asosida:

ochiq kodli tizimlarda O‘zDSt 1105:2009 standarti asosida kalitlar yordamida shifrlash dasturi “exe” faylari faqat bitta seans kaliti bilan shifrlashda 10% kam bo‘lmagan zichlash samaradorligini ko‘rsatgan. Shuningdek, ruxsat etilgan tashqi qurilmalarga shifrlangan ma’lumotlarni yozishni ta’minlash OT tomonidan bir qator cheklovlar orqali amal oshirilgan. Natijada, tashqi kiruvchi/chiquvchi qurilmalarni OT yadrosi darajasida ro‘yxatga olish va ulardagi ma’lumotlarning xavfsizligini ta’minlashda shifrlash amalini bajarishning majburiy usuli tufayli qurilmalardagi ma’lumotlarning chiqib ketishining oldi olingan (O‘zbekiston Respublikasi Qurilish vazirligining 2022 yil 17 noyabrdagi 11-06/13043-son ma’lumotnomasi). Ilmiy tadqiqot natijasida “Kiberxavfsizlik to‘g‘risidagi qonun” talablariga mos keluvchi

dasturiy ta’minot hamda mazkur dasturiy ta’minotni amaliyotga tatbiq etish natijasida tashkilotning 1,2 mlrd. so‘m mablag‘lari tejab qolingan;

ochiq kodli OT larda arxivlash yordamida GOST 28147-89 algoritmi asosida shifrlash usuli va ruxsat etilgan tashqi qurilmalarni ro‘yxatga olish, o‘chirish va formatlarining algoritm va mexanizmlari, ularga shifrlangan ma’lumotlarni yozish algoritmlarini ishlab chiqilgan. GOST 28147-89 algoritmi yordamida shifrlash va arxivlash orqali OT dagi ma’lumotlarning himoyalanganligini tashkillashtirish, initsializatsiya jarayonida tizim fayllarini shifrlash va rasshifrlashni tashkil etish, OT ning fayl tizimi uchun shifrlashning grafik dasturiy ta’minotini ishlab chiqilgan (O‘zbekiston Respublikasi Iqtisodiy taraqqiyot va kambag‘allikni qisqartirish vazirligi huzuridagi “Loyihalar va import kontraktlarini kompleks ekspertiza qilish markazi” DUKning 2022 yil 23 noyabrdagi 45/01-08-7954-son ma’lumotnomasi). Natijada ochiq kodli OT da dasturiy majmualar va ma’lumotlarning xavfsizligini ta’minlash usullarini qo‘llash obyektlarga qayd qilinmagan murojatlardan himoya qilish va ularning himoyalangan OT larini yaratishdagi samaradorlikni aniqlash imkonini bergan;

yaratilgan kriptografik modul mahalliy standartga javob berishi uchun sinovdan o‘tkazilgan va tasdiqlangan. Himoya vositalarining ishlash samaradorligi aniqlangan va OT ning hisoblash resurslari yuklanishiga ta’siri o‘rganilgan hamda ilovani ishga tushirish rejimida protsessorning qo‘shimcha yuklanishi 23% dan, oddiy dasturning ishlash rejimida esa, 17% dan oshmasligi ko‘rsatilgan. Shu bilan birga, dasturni ishga tushirish vaqti 4 soniyadan oshmasligi ham ko‘rsatilgan. Olingan natijalarning adekvatligi tajribani statistik qayta ishlanishi bilan isbotlangan. Shuningdek, himoyalangan fayllar tizimida fayl bloklari va inodlar algoritmlari va ularning ishlash blok-sxemasi, sinov tariqasida turli xil o‘lchamli fayllarda testlar o‘tkazilgan va baholangan. (O‘zbekiston Respublikasi Transport vazirligining 2022 yil 24 noyabrdagi 4/7271-son ma’lumotnomasi). Natijalar shuni ko‘rsatadiki, ma’lumotlar hajmidan qat’iy nazar, HFT laridan fayllarni o‘qish va yozishda taklif etilayotgan algoritm ext3/4 da ishlovchi tizimlarda ishlash samaradorligi qariyb 0.5 baravarga oshirilgan.

“Ochiq kodli operatsion tizimlarda AXni ta’minlashning zamonaviy usullari va algoritmlari” mavzusida dissertatsiya tadqiqotida himoyalangan fayllar tizimlaridan fayllarni o‘qish va yozishda taklif etilayotgan algoritm ext3/4 da ishlovchi tizimlarda ishlash samaradorligi qariyb 0.5 baravarga oshirilgan (O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Davlat test markazining 2022 yil 21 dekabrdagi 40-son ma’lumotnomasi). Natijada mazkur ilmiy tadqiqot doirasida milliy shifrlash algoritmlari asosida xavfsizlik talablariga muvofiq va maxfiy ish yuritish sohasidagi standartlar talablarini qondiruvchi maxsus usullar va xavfsizlik vositalari hamda algoritmlari ishlab chiqilgan va amaliyotga keng joriy etilgan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari jami 8 ta, jumladan, 5 ta xalqaro va 3 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 26 ta ilmiy ish e’lon qilingan, shulardan 12 ta maqola Oliy attestatsiya komissiyasining doktorlik dissertatsiyalari asosiy natijalarini chop etishga tavsiya

qilingan, 3 tasi xorijiy ilmiy jurnal nashrlarida chop etilgan hamda EHM uchun yaratilgan dasturiy mahsulotlarni qayd etish to‘g‘risida 3 ta guvohnoma olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiyaning hajmi 182 betdan iborat.

DISSERTATSIYANING ASOSIY MAZMUNI

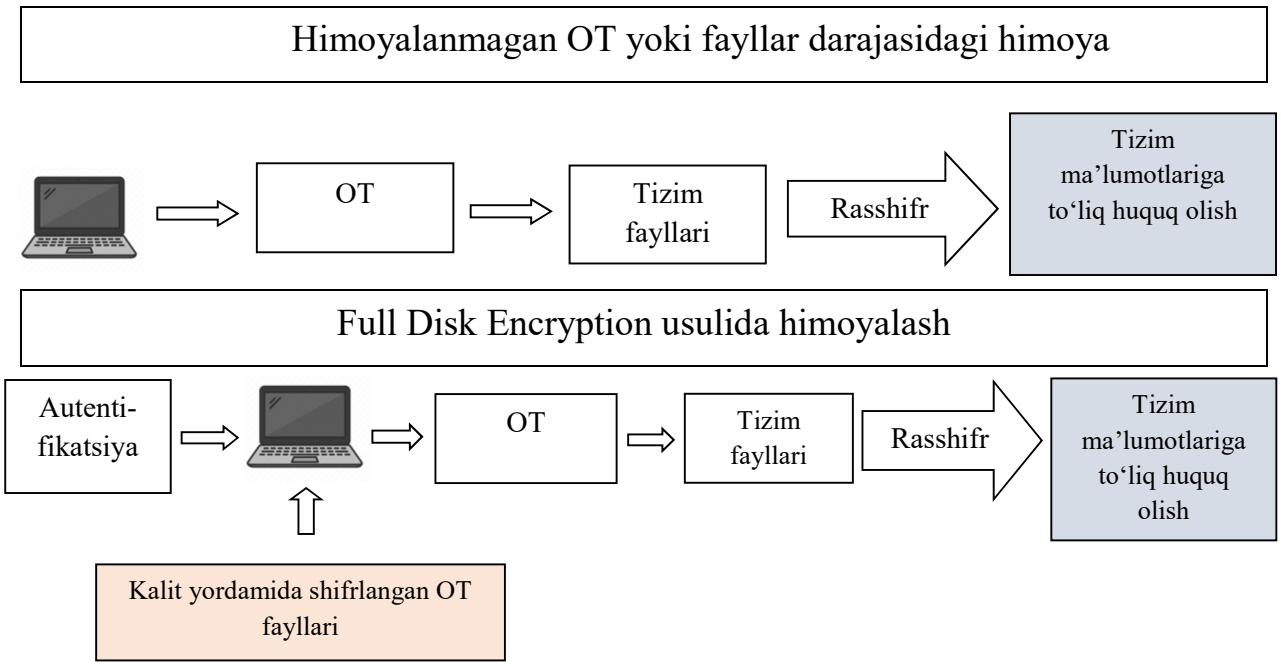
Kirish qismida dissertatsiya mavzusining dolzarbligi va zarurati keltirilib, tadqiqotning O‘zbekiston Respublikasi fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, maqsad va vazifalari belgilab olingan hamda tadqiqot obyekti va predmeti aniqlangan, olingan natijalarning ishonchliligi asoslab berilgan. Ularning nazariy va amaliy ahamiyati ochib berilgan, tadqiqot natijalarini amalga tatbiq etish ro‘yxati taqdim qilingan, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **«Ochiq kodli operatsion tizimlarda shifrlash algoritmlarining samaradorligini ta’minlash muammolari»** deya nomlanuvchi birinchi bobi ochiq kodli OT larda hozirgi vaqtda qo‘llanilib kelinayotgan xalqaro standartlar asosida yaratilgan shifrlash algoritmlarinig samaradorligi, shifrlash algoritmlarining xususiyatlari tadqiqi va himoyalangan fayl tizimlari tahliliga bag‘ishlangan. OT larda shifrlash algoritmlari asosida AXni ta’minlash maqsadida ushbu sohadagi xalqaro va mahalliy standartlar tahlil qilingan. Bunday standartlarga misol qilib GOST 28147-89 va O‘zDSt 1105:2009 larini keltirish mumkin. Ochiq kodli OT larda asosan blok shifrlash algoritmlari keng tatbiq etilgan. Ular orasida AQSH MXA (Milliy xavfsizlik agentligi) va Rossiya Federatsiyasining TK-26 (2-GOST) shifrlash algoritmlari o‘rganib chiqilgan. Ko‘plab operatsion tizimlarda fayllar tizimida shifrlash yoki tizim fayllarini shifrlash maqsadida shifrlash amallari bajariladi. Linux oilasidagi OT larda diskni to‘liq shifrlash (FDE-Full Disk Encryption) usuli mavjud bo‘lib, bu kompyuter va tashqi qurilmalardan ma’lumotlarning o‘g‘irlanishidan himoya qilishning eng samarali usullaridan biri bo‘lib kelmoqda. FDE tizimi OT yuklanishidan oldin ishga tushadi (1-rasm). Bu o‘z navbatida shuni anglatadiki, tizim ishga tushganidan so‘ng operatsion tizimning kodi shifrlangan muhitga yuklana boshlaydi. Shifrlash tizimi o‘z navbatida OTning ishlashni sekinlashtiradi.

Barcha shifrlash/rasshifrlash amallari foydalanuvchiga ko‘rinmas holda amalga oshiriladi. Butun qattiq disk shifrlanganda virtual xotira fayllari, vaqtinchalik fayllar, muhimlilik darajasidan qat’iy nazar, shifrlanadi.

Agar tizim foydalanuvchisi shifrlangan qattiq diskning shifrlash parolini yo‘qotib qo‘ygan taqdirda, tizim administratorining yopiq kaliti yordamida ma’lumotlar qayta tiklanadi.

AXni ta’minlash xalqaro hamjamiyatning ustuvor vazifalaridan biridir. Ushbu sohada davlatlar o‘rtasida hamkorliklar hozirgi davrda yanada rivojlanib bormoqda. O‘zbekiston Respublikasida ham davlat sirlari va maxfiy ma’lumotlari muhofazasiga alohida e’tibor qaratilmoqda.



1-rasm. FDE usulida himoyalash va himoyalanmagan OT fayllar himoyasi o‘rasidagi tafovut.

O‘zbekiston Respublikasida blok shifrlash algoritmini tavsiflovchi O‘zDSt 1105:2009 standarti asosida yaratilgan shirlash/rasshifrlash algoritmi ishlab turibdi. Dissertatsiya ishining ushbu bo‘limida O‘zDSt 1105:2009 standarti asosida olingan nazariy natijalar keltirib o‘tilgan. O‘zDSt 1105:2009 kriptografik standartida jadval almashinishi 256 qiymatni almashtirishdan iborat va keltirilgan formulaga muvofiq *d, L, R* argumentlari bo‘yicha bit kengaytirilgan k_{se} kalitiga qarab hosil bo‘ladi.

O‘zDSt 1105:2009 shifrlash standartining tahlili natijasida quyidagilar aniqlandi:

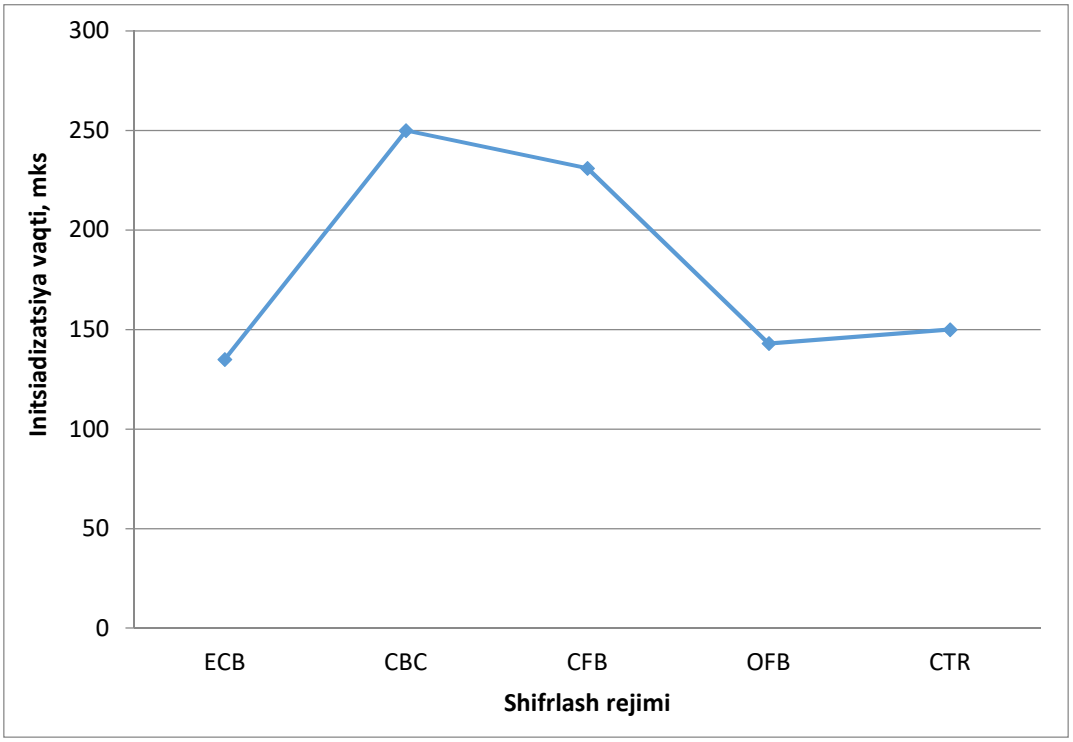
- O‘zDSt 1105:2009 shifrlash algoritmida 2 ta – shifrlash kaliti va funksional kalit ishlatiladi, ularning har biri 256 bitli ketma-ketlikni tashkil etadi. Ushbu kalitlarning birgalikda ishlashi, shifrlash algoritmida 512 bitli shifrlash kalitidan foydalanish bilan barobardir. Bu esa o‘z navbatida, ma’lumotlarni ruxsatsiz rasshifrlash imkoniyatini oldini oladi;
- agar yuqori darajadagi havfsizlik elementlari qo‘llanilsa, funksional kalit har bir seansda almashadi;
- O‘zDSt 1105:2009 shifrlash standarti chiziqli va differensial tahlilga chidamli ekanligi tasdiqlandi, buning uchun raundlar soni 4 tadan yuqori bo‘lishi kifoya.

Ushbu parametrlarning turli xil qiymatlari asosida hosil qilingan almashtirish jadvallarining umumiy soni 4 161 600 ni tashkil qiladi. Shuning uchun asosiy maqsadimiz O‘zDSt 1105:2009 standartining shifrlash algoritmida qo‘llaniladigan almashtirish jadvallari sifatini avtomatik ravishda tekshirish usulini tahlil qilishdan iborat. O‘zbekiston Respublikasining O‘zDSt 1105:2009 kriptografik standartida qo‘llaniladigan algoritm nisbatan yangi bo‘lganligi sababli kam o‘rganilgan. O‘zDSt 1105:2009 kriptografik standartini tahlil qilish jarayonida uning almashtirish

jadvallarini avtomatik ravishda baholashga imkon beradigan parallel algoritmdan foydalaniladi.

Yaratilgan algoritm asosida ixtiyoriy almashtirish jadvallarini tahlil qilish imkoniyatini yaratildi. Masalan, barcha 4-bitlik almashtirish jadvallarini yoki aniq funksiyalar sinflarining barqarorligini tekshirishda bu algoritmni takomillashtirish mumkin bo‘ladi. S-blok butun kriptotizimning “yuragi” bo‘lganligi sababli, uning ustida olib boriluvchi tadqiqot natijalari muhim amaliy ahamiyat kasb etadi.

Tahlillar jarayonida shifrlash rejimlarida tizimning initsializatsiya vaqti ham o‘rganilib chiqilgan.



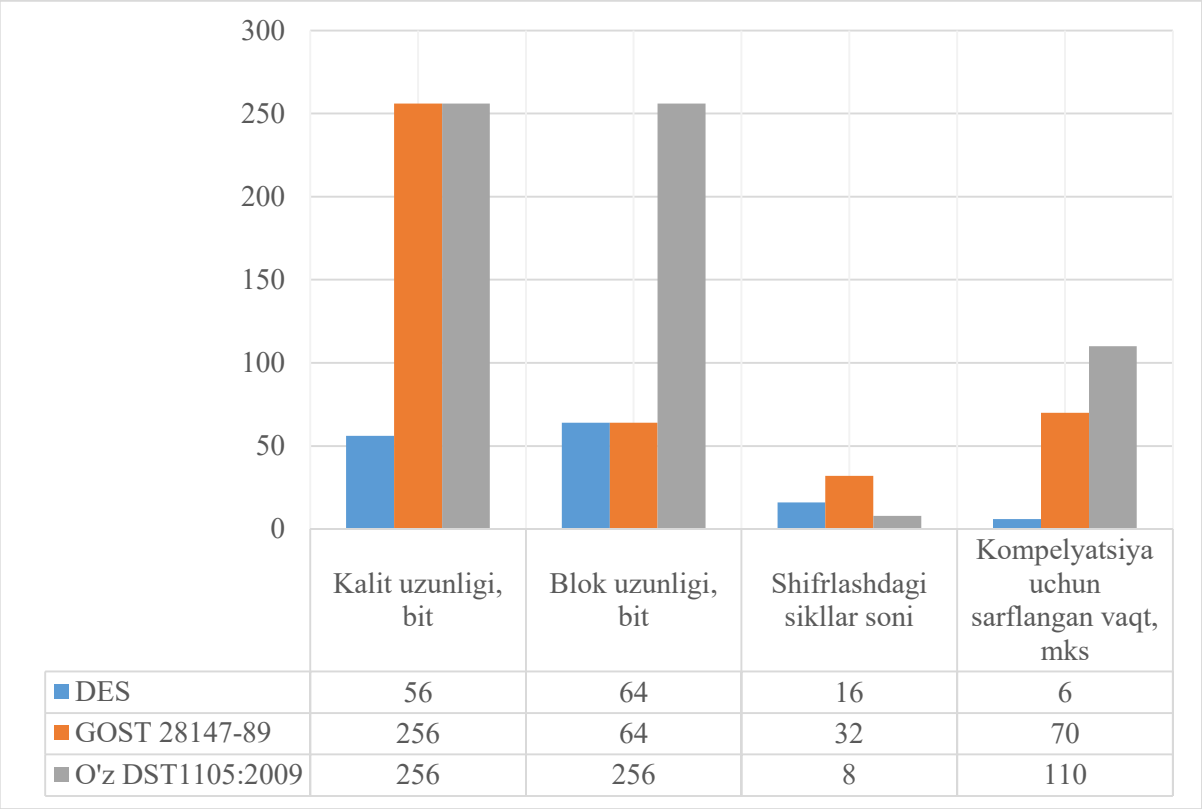
2-rasm. Shifrlash rejimlarining initsializatsiya vaqti

Aksariyat hollarda, tanlangan rejimga qarab shifrlashning boshlang‘ich vaqtlardagi og‘ishlari ahamiyatga ega emas. CBC (Cipher Block Chaining) va CFB (Cipher Feedback Mode) rejimlarida initsializatsiya vaqti ortadi. CBC rejimida shifrlash algoritmining kritobardoshliligi ortadi (2-rasm).

Tahlillar asosida O‘zDSt 1105:2009 standarti uchun axborotni himoyalanganligi va shifr matnlarining kriptobardoshliligini inobatga olib CBC rejimini tanlab olamiz va mazkur rejimida shifrlashda insializatsiya vaqti 0,00025 sek vaqtda bajarilganligini ma’lumot sifatida qabul qilish maqsadga muvofiq. Ortib borayotgan davlat tashkilotlari va tijorat firmalari bepul muqobil dasturiy ta’minotlardan foydalanmoqdalar. Xususan, aksariyat korxona va tashkilotlar pullik Windows OT o‘rniga bepul Linux OT dan foydalanishni ma’qul ko‘rmoqdalar.

GOST 28147-89 va O‘zDSt 1105:2009 shifrlash algoritmlarida, almashtirish bloklari, DES (Data Encryption Standard) dagi kabi o‘rnatilmagan va maxfiydir. Shifrlashda qo‘llaniluvchi kalit ham – 256 bitdan iborat bo‘lib, bu kriptobardoshlilikni oshiradi (3-rasm).

Hujjatlar yaratish va turli operatsiyalarni bajarishda OT ning bir qismi bo‘lgan fayllar tizimidan foydalaniladi. Linux OT larining xususiyatlaridan biri – qattiq disklarning katta qismlarida ishlaydigan, minglab fayllarni osonlik bilan o‘lchaydigan va turli o‘lchamdagi fayllar bilan samarali ishlaydigan fayllar tizimini qo‘llab-quvvatlashidir.



	Kalit uzunligi, bit	Blok uzunligi, bit	Shifrlashdagi sikllar soni	Kompelyatsiya uchun sarflangan vaqt, mks
DES	56	64	16	6
GOST 28147-89	256	64	32	70
O'z DST1105:2009	256	256	8	110

3-rasm. Ochiq kodli OT larda shifrlash algoritmlari tahlili

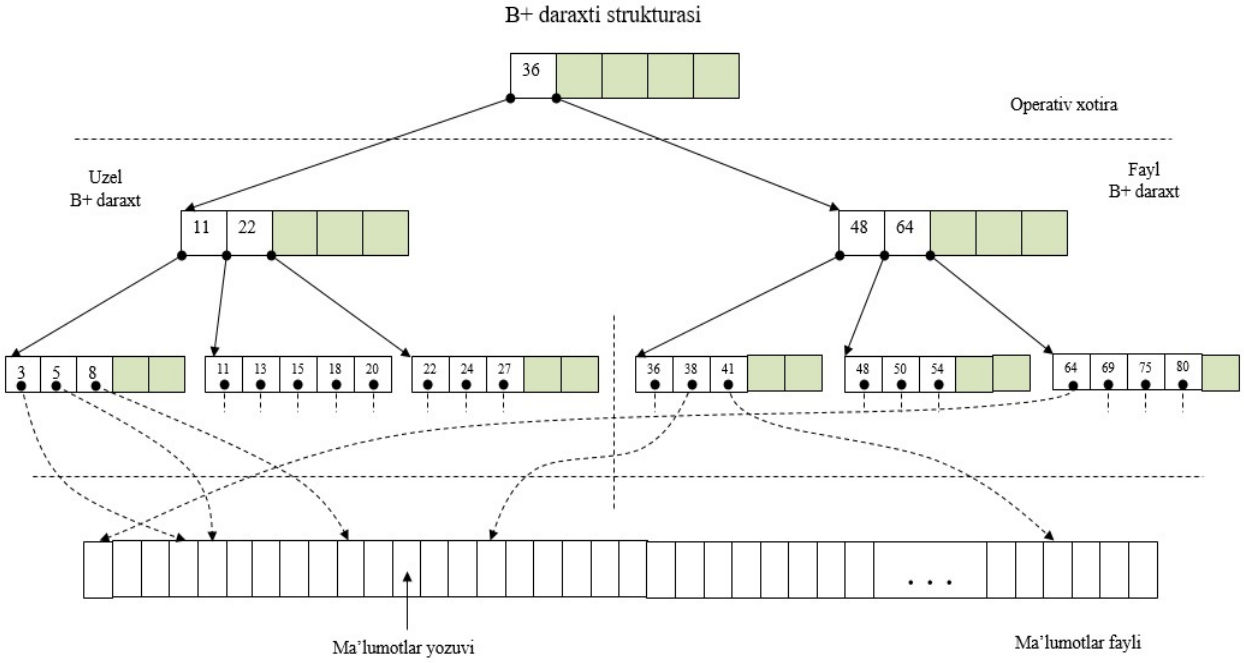
OT foydalanuvchilari asosan tizim tomonidan taqdim etilgan fayl tizimlari bilan ishlaydilar. Ular kamdan-kam hollarda yangi disk bo‘limlarini yaratadilar va ularning sozlamalari haqida kamroq o‘ylagan holda, faqat tavsiya etilgan parametrlardan yoki oldindan formatlangan tayyor tashqi xotiralardan foydalanadilar.

Shifrlash algoritmlarining sifat ko‘rsatkichlarini baholashning tasnifi taklif etilgan va parallellashtirish masalalari yordamida shifrlash rejimlarining tahlili o‘tkazilgan. Zamonaviy OT larda va ochiq kodli OT dan ishlovchi ma’lumotlarni shifrlash/rasshifrlash standartlari qiyoslanilib, ishlash tezligi va kriptotahlillariga baho berilgan. HFT ni ishlab chiqish va yaratish uchun XFS fayl tizimidan foydalanish maqsadga muvofiq. XFS fayl tizimi katta hajmli fayllarni qo‘llab-quvvatlaydi va yaxshi oqimli I/O (kirish/chiqish) ishlashini ta’minlay oladi.

Dissertatsiyaning **«Himoyalangan fayllar tizimi va yadro tarkibida shifrlashni amalga oshirishning zamonaviy usullari va algoritmlari»** deya nomlanuvchi ikkinchi bobida himoyalangan fayllar tizimini yaratishda B+ fayllar strukturasidan foydalangan holda, qo‘yiladigan talablar va HFT tizmilarini yaratish algoritmlari, HFTlarda katalog va jurnallarni tashkil etish taklif etilib, ochiq kodli

operatsion tizimining yadrosi tarkibida shifrlashni tashkillashtirish usullari va ishlash algoritmlariga bag‘ishlangan.

HFT barcha vaziyatlarda B+ fayllar strukturasidan foydalangan. Ular inodlar paketlarini, erkin ro‘yxatlar, katalog yozuvlari va fayl xaritasi yozuvlarini indekslash uchun foydalanilgan. HFTlarning B+ fayllar strukturasidagi (4-rasm) ichki uzellarida faqat kalitlar va ko‘rsatkichlar, barglarida esa kalit ma’lumotlari saqlanadi. HFTda bir nechta fayl strukturalari bo‘lganligi uchun, umumiy kod faqat standart blok sarlavhalari bilan ishlaydi.



4-rasm. HFTlarining B+ daraxtsimon fayllar strukturasi

B+ daraxtining har bir ichki uzeli p_0, key_1, p_1, key_2, p_2 , . . . ,key_n, p_n , bu yerda p_i i-bargining ko‘rsatkichi, $0 \le i \le n$, key_i – kalit, uzeldagi kalitlar o‘sish tartibida joylashgan $key_1 < key_2 < \ldots < key_n$. Kichik daraxtdagi barcha kalitlar p_0 ko‘rsatkichli $k_1$dan kichik. $0 \le i \le n$ holat uchun barcha kalitlar p_i ko‘rsatkichli k_i va k_{i+1} dan kichik. p_n ko‘rsatkichli barcha kalitlar $k_n$dan kichik.

Har bir fayl sarlavhalaridan keyin ma’lumotlar massivlari mavjud. Kalitlar va yozuvlar formati shunga qarab daraxt turi bilan belgilanadi. HFT tizimi 64-bitlik fayl tizimi sifatida qo‘llaniladi. Bunday fayl tizimini yaratishda ko‘rsatkichlarning 64-bitlik bo‘lishi shart emas. Ko‘rsatkichlarning 32-bitli qiymat ichida saqlash ajratish guruhlaridan foydalanishning asosiy mexanizmlaridan biridir. O‘rtacha har bir ajratish guruhlari hajmi 0.5-4 Gb ni tashkil qiladi va o‘z chegaralarida inodlar va bloklarning joylashishini boshqarish uchun o‘z ma’lumot tuzilmalariga ega.

Almashtirish guruhlarining cheklangan kattaligi ular ichida nisbatan 32-bitli inodli raqamlardan foydalanish imkonini yaratadi, bu esa o‘z navbatida ma’lumotlar tuzilmalarining o‘lchamlarini maqbul qiymatlar darajasida saqlaydi.

Strukuturalarda almashtirish guruhlari tarkibidagi ma’lumotlarga 32-bitli raqamlardan foydalanilsa, global ma’lumotlar tuzilmalarida 64-bitli

ko‘rsatkichlardan foydalanib, fayl tizimining istalgan joyida blok va inodlarga murojat qilishi mumkin.

Bundan tashqari, qisqa muddatga ega bo‘lgan fayllar diskda umuman jismonan saqlanmasligi mumkin. HFT ularni o‘chirishdan oldin joylashtirish to‘g‘risida qaror qabul qilishga ulgurmaydi.

Almashtirish guruhlari odatda ma’lumotlarni guruhlashtirish uchun kamdan-kam qo‘llaniladi, ular juda katta fayllar yoki kataloglar HFT tizimida ma’lumotlar markazi bo‘lib (fragmentatsiyani kamaytirish va o‘qish qobiliyatini yaxshilash maqsadida) xizmat qiladi.

HFT tizimlarini yaratish o‘ta murakkab jarayon bo‘lib, bu dasturchilardan o‘ylangan disk maydonlarini ajratish, algoritmlardan foydalanish va foydalanuvchining so‘rovlarini samarali parallel-lashtirishni talab qiladi. Dasturchi esa ushbu usullar orqali boshqarishni amalga oshirish vositasida katta va o‘rtacha hajmdagi fayllarni qayta ishlash jarayonida ijobiy natijalarga erishishi mumkin.

HFT tizimlarida har bir inod – yadro, keyingi bog‘langan adres, u va a kabi to‘rt qismli parametrlardan iborat. Yadroda barcha turdagi inodlarga xos doimiy ma’lumotlar mavjud. Yadrodan ajratilgan keyingi bog‘langan adres maydoni bilan ajratishlar guruhi funksional ravishda bog‘langan va blok-sxema ko‘rinishida quyidagicha tasvirlangan (1-blok sxema).

HFT fayl tizimidagi katalogning tarkibi to‘g‘ridan-to‘g‘ri inodda saqlanadi yoki faylning daraxti orqali manzillanadi. Katalog tuzilmalaridagi barcha amallar mantiqiy, ya’ni ba’zi elementlarning fizik holatini topish uchun fayl tizimi fayllar xaritasiga murojaat qiladi va tegishli o‘zgarishlarni amalga oshiradi.

Agar katalog bitta yagona blokka mos kelmasa, HFTda saqlash uchun daraxt tuzilishini kengaytiradi, bu esa katalog elementlarining ma’lumotlaridan iborat. Fayl nomlari va ularning inodlari va ma’lumotlar bloklaridagi indeks ma’lumotlarini o‘z ichiga olgan bloklari hamda katalog ichidagi mos elementlarning nomlari va xesh qiymatlaridan iborat.

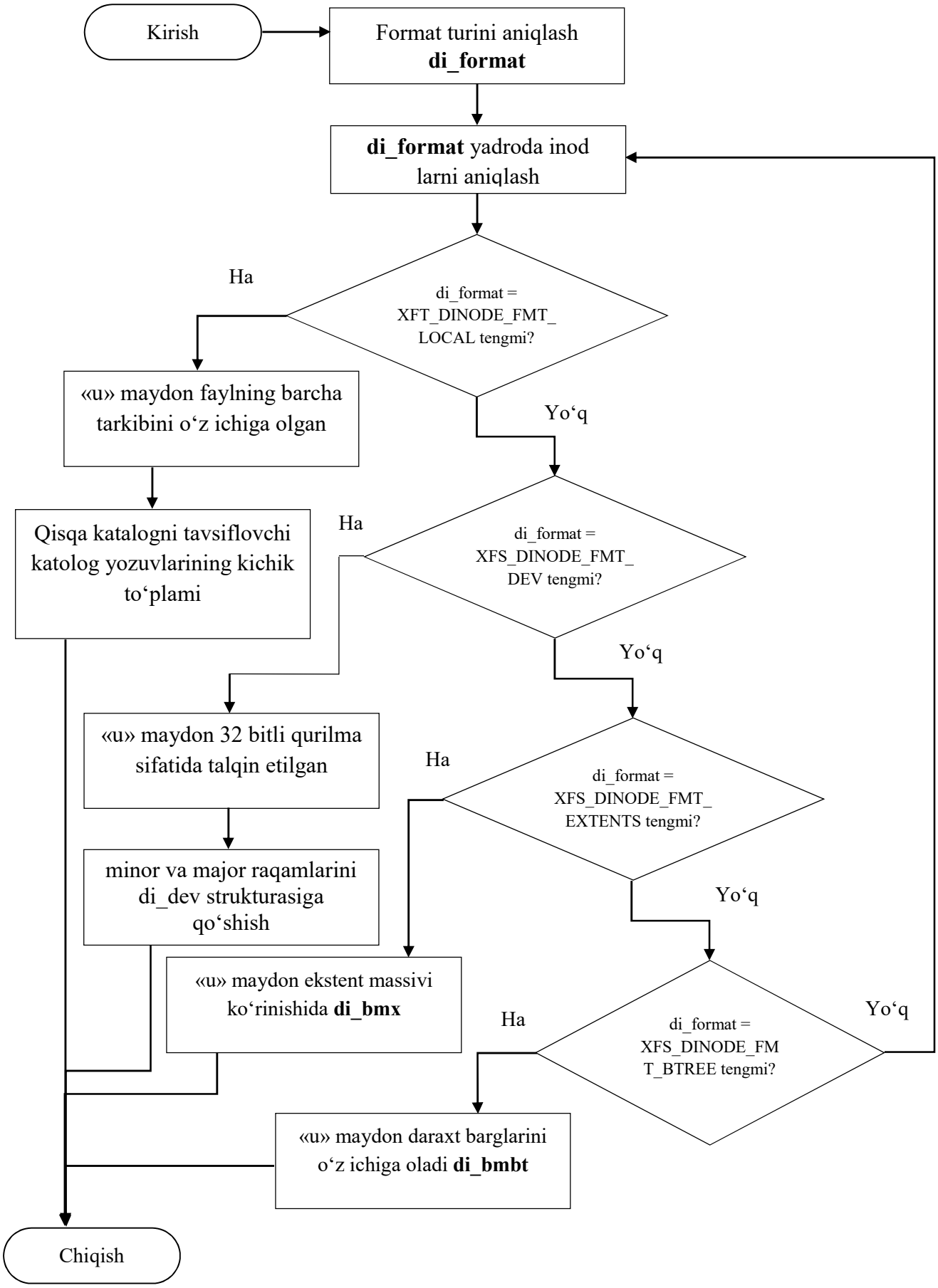
Ushbu tuzilmalarga bo‘sh bloklar biriktiriladi. Katalog fayli ichidagi mantiqiy bo‘sh joy 8 bitli so‘zlar hisoblanadi.Ushbu struktura-larni faqat daraxt strukturali tizimlar deya atash ham mumkin.

Aslida HFT tizimida kataloglar xeshlash yordamida indekslanadi.

Bularning barchasi HFTni reiserfs kabi kengaytirilgan fayl tizimlaridan funksional orqada qolishiga sabab bo‘lib keladi.

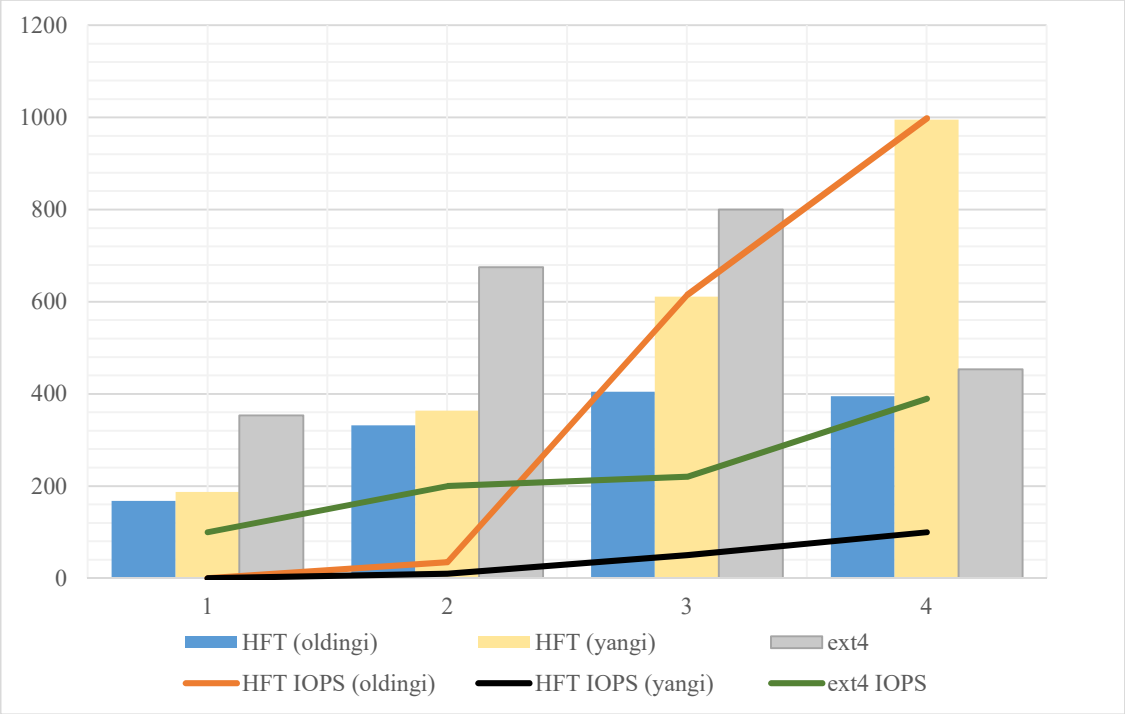
Tizim fayllarining yaxlitligini tekshirish dasturi OT ning xavfsizligini ta’minlashning qo‘shimcha mexanizmi hisoblangan. Bunday tizimlar fayllar va kataloglardagi o‘zgarishlarni real vaqt jarayonida tekshirish imkoniyatini yaratgan.

Tizim fayllarining yaxlitligini ta’minlash uchun xesh summani tekshirish amalga oshirilgan. Bunda GOST R 34.11-2012 xeshlash algoritmi qo‘llanilgan. Shuningdek, bu mexanizm tizim kataloglarida ortiqcha fayllarning paydo bo‘lishi va OT fayllari atributlarining o‘zgarishini nazorat qilgan. O‘zDSt 1106:2009 xesh funksiyalari orqali ham xeshlashlarni amalga oshirishi mumkin, lekin kriptobardoshlilik darajasi pastligi kuzatilgan.



1-Blok-sxema. inodlarni yaratish algoritmi.

Sinov tariqasida HFTning oldingi varianti, yangi taklif etilgani va ext3/4 fayl tizimi bilan qiyoslaganda bir yoki ikkita oqim bilan ishlashda ext3/4 HFTga nisbatan sekinroq, ammo oqimlar soni sakkiztaga yetganida esa, tizimning ishlash tezligi chiziqli oshgan (5-rasm).



5-rasm. Fayl tizimlarini qiyoslash grafigi.

Yuqoridagi muammolarni hal etish uchun Thunar fayl menejerining thunar-enum-types.c va thunar-list-model.c fayllari o‘zgartirilgan. Standart fayl ma’lumotlari orasida kirish darajalarini o‘z ichiga oladigan qiymat mavjud emas.

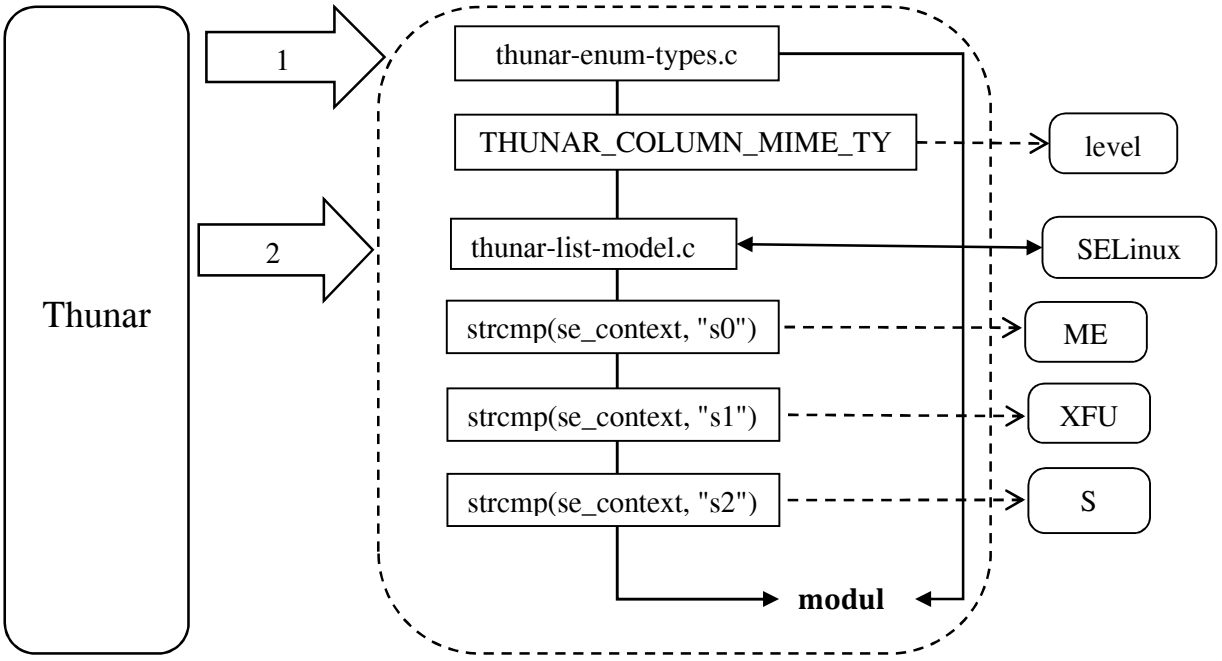
OT foydalanuvchilariga fayllar tizimi bilan ishlash va fayllar bilan ishlash darajalarini ko‘rishda qulaylik yaratish uchun Thunar fayl menejeriga qo‘shimcha o‘zgartirishlar va imkoniyatlar yaratilgan. Mazkur vazifani bajarish uchun ikki turdagi masalani yechish talab etiladi.

Birinchidan, jadvaldagi ustun (fayl tizimi tomonidan qo‘llanil-mayotgan) aniqlangan va unda ishlash darajasi to‘g‘risidagi ma’lumot ko‘rsatilgan. Ikkinchidan, fayl menejeriga kerakli ma’lumotlarni qayerdan va qanday olish kerakligi haqida ko‘rsatma beradigan modulni ishlab chiqish kerak.

Mazkur vazifalarni bajarish uchun OT ning standart kutubxonalari va funksiyalaridan foydalanilgan.

Yuqoridagi muammolarni hal etish uchun Thunar fayl menejerining thunar-enum-types.c va thunar-list-model.c fayllari o‘zgartirilgan. Standart fayl ma’lumotlari orasida kirish darajalarini o‘z ichiga oladigan qiymat mavjud emas.

Quyidagi modul fayl menedjeri interfeysidagi fayllarga kirish darajalarini ko‘rsatgan (6-rasm). Katta strelkalar ichidagi raqamlar murojaatlar ketma-ketligini belgilagan.



6-rasm. Fayl menejeri interfeysidagi fayllarga kirish darajalari

Himoyalangan fayllar tizimida fayl bloklari va inodlar algoritmlari va ularning ishlash blok-sxemasi, sinov tariqasida turli xil o‘lchamdagi fayllarda testlar o‘tkazilib, baholangan. Natijalar shuni ko‘rsatadiki, ma’lumotlar hajmidan qat’iy nazar, HFTlaridan fayllarni o‘qish va yozishda taklif etilayotgan algoritm ext3/4 da ishlovchi tizimlarda ishlash samaradorligi o‘rtacha 0.5 baravarga oshirgan. OT foydalanuvchilariga himoyalangan fayllar tizimi bilan ishlash va fayllar bilan ishlash darajalarini ko‘rishda qulaylik yaratish uchun Thunar fayl menejeri yordamida qo‘shimcha imkoniyatlar yaratilgan.

Dissertatsiyaning **«Mahalliy standartlar asosida shifrlash va arxivlashning zamonaviy usullari va algoritmlari»** deya nomlanuvchi uchinchi bobida mahalliy standartlar asosida shirflash/rasshifrlash usullari va algoritmlari ishlab chiqilgan. Mahalliy shifrlash standartlaridan O‘zDSt 1105:2009 shifrlash algoritmininig kriptotahlili hamda GOST 28147-89 shifrlash algoritmininig statistik tahlili keltirib o‘tilgan. Ochiq kodli OT larda arxivlash yordamida GOST 28147-89 alogoritmi asosida shifrlash usuli taklif etilgan.

Katta strelkalar ichidagi raqamlar murojaatlar ketma-ketligini belgilagan:

Ruxsat etilgan tashqi qurilmalarni ro‘yxatga olish, o‘chirish va formatlash algoritmi va mexnaizmlari ishlab chiqilib, ularga shifrlangan ma’lumotlarni yozish algoritmi yaratilgan. Tashqi qurilmalar bilan ishlashni avtomatlashtirish maqsadida grafik interfeys yaratilgan.

Mazkur bo‘limda shifrning psevdokodi va almashtirishlari hamda shifrlash algoritmi almashtirishlari va amaliy kriptografik bardoshliligining bahosi (O‘zDSt 1105:2009 ma’lumotlarni shifrlash algoritmi misolida) keltirilgan. Ushbu natijalar asosida shuni aytish mumkinki, O‘zDSt 1105:2009 simmetrik blokli shifrlash algoritmi chiziqli va differensial kriptotahlil usullariga bardoshliligi yuqori darajada.

Hozirgi O‘zDSt 1105:2009 simmetrik blokli shifrlash algoritmidan axborotlarni himoyalashda foydalanilganda yuqori kriptobardoshli himoyani ta’minlaydi, deyish mumkin.

Bir tomondan, oddiy matnda bitning bir vaqtning o‘zida siklning barcha chiquvchi bitlariga o‘zgartirish ta’sirining matematik dalillari bir tekis farq qiladigan to‘g‘ri matnga mos keladigan juft shifr matnlarining ortogonalligidir (o‘zaro bog‘liq bo‘lmaganligi) $m_w = 32$.

Agar mutlaqo tasodifiy 64-bitli blokka (mustaqil ikkilik belgilaridan iborat) e’tibor qaratilsa, u holda bunday bloklardagi nolga teng bo‘lmagan bitlar soni uchun taqsimot qonuni parametrlarga ega binomial hisoblanishini ko‘rish mumkin.

$$m_w = np_0 = 64 \cdot \frac{1}{2} = 32,$$

$$\sigma_w^2 = np_0(1- p_0) = 64 \cdot \left(\frac{1}{2}\right)^2 = 16 .$$

$np_0(1- p_0) \geq 10$ qiymatida, taxminiy yaqinlashish darajasi yuqori bo‘lgan binomial taqsimot, ehtimollik taqsimotining normal qonuni bilan qiyoslanadi (Muavr-Laplas formulasi asosida). m_w qiymatning hosil bo‘lgan qiymatlari esa tasodifiy va 32 ga teng.

Yuqorida keltirilgan savolga aniq javob olish uchun, ishonch oralig‘i usullaridan foydalanilgan. ya’ni, ehtimollik taqsimoti noma’lum parametrlarining taxminiy qiymatlari to‘plamini tuzish uchun maxsus ishlab chiqilgan matematik statistika usuli mohiyati quyidagicha:

$X_1, X_2, \ldots, X_n, n \geq 2$ noma’lum parametrlarga ega bo‘lgan bir xil normal qonunga bo‘ysunadigan mustaqil tasodifiy o‘zgaruvchilarning $EX_i = \theta_1$ va $DX_i = \theta_2$ interval baholashni $u(\theta) = \theta_1$ tuzish talab etilgan.

$$\bar{X} = \frac{1}{n} \cdot \sum_{i=1}^{n} X_i ; \quad s^2 = \frac{1}{n-1} \cdot \sum_{i=1}^{n} (X - \bar{X})^2 \qquad (1)$$

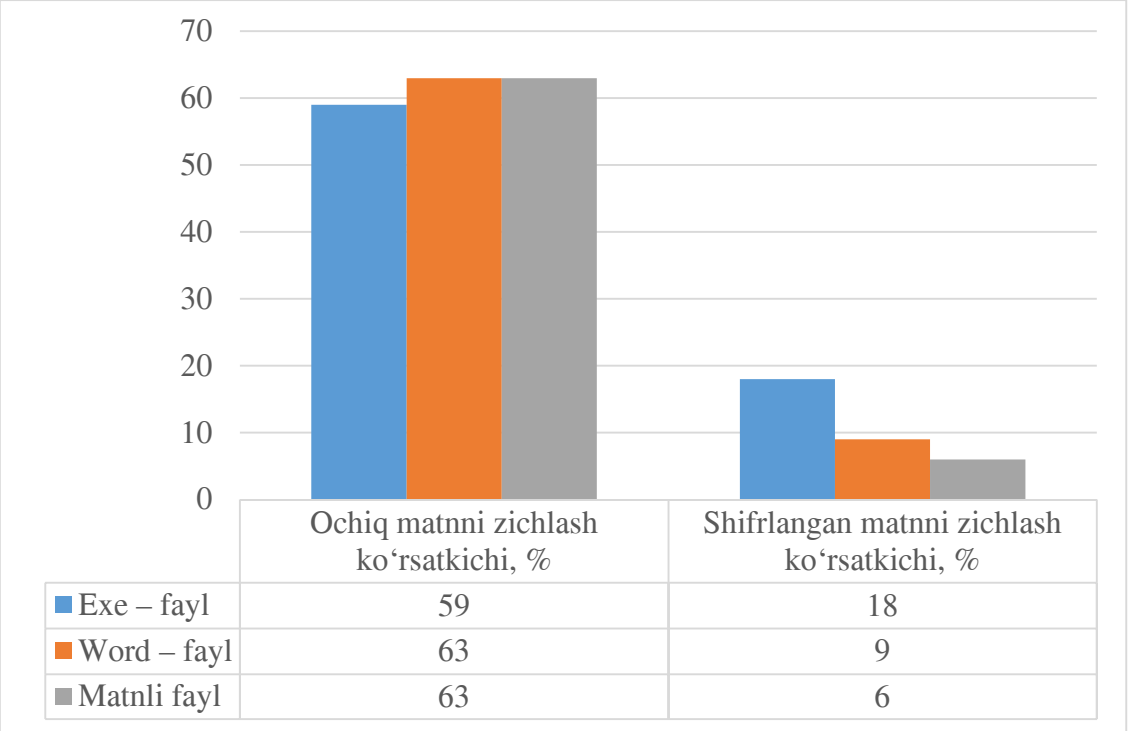
Tasodifiy o‘zgaruvchi $T = \frac{\sqrt{n}(\bar{X}-\theta)}{s}$ Styudent taqsimlanishining c_{n-1} darajasiga bo‘ysunadi va noma’lum q_1 va $q_2(|\theta_1| \leq \infty, \theta_2 > 0)$ parametrlariga bog‘liq bo‘lmaganligi sababli, har qanday t uchun hodisaning ehtimolliligi faqat t ga bog‘liq bo‘lib qolaveradi.

$$\left\{\bar{X} - \frac{t \cdot s}{\sqrt{n}} < \theta_1 < \bar{X} + \frac{t \cdot s}{\sqrt{n}}\right\} \qquad (2)$$

Agar, ko‘rsatilgan intervalda baholash c uchun q_1 qabul qilinsa, u $\theta = \{\theta_1, \theta_2\}$ ga bog‘liq bo‘lmagan quyidagi $P_c(\theta_1, \theta_2) = P\{|T| < t\} = 1 - \alpha$ ehtimollik intervaliga mos keladi. Bunday intervallar oralig‘i ishonch ehtimolliklar oralig‘i va uning chegaralari ishonch intervali chegaralari deb ataladi.

Yuqorida keltirilgan ta’riflarga muvofiq, ishonch ehtimolliligi intervali sifatida $P_c(\theta_1, \theta_2) = 0,999 \longrightarrow (\alpha = 0,001)$, yuqorida keltirilgan Styudent jadvali asosida n ning son qiymati $n = 1024$ (tajribalar asosida) $t = 3,291$ va $\frac{t \cdot s}{\sqrt{n}} = \frac{3,291 \cdot 4}{\sqrt{1024}} = 0,4$ ni

olamiz. Shu bilan birga m_w ni ishonch intervaliga mos kelishligini taxmin qilish mumkin va u quyidagi shartni qanoatlantiradi: $32-0,4 \leq m_w \leq 32+0,4$.



	Ochiq matnni zichlash ko‘rsatkichi, %	Shifrlangan matnni zichlash ko‘rsatkichi, %
Exe – fayl	59	18
Word – fayl	63	9
Matnli fayl	63	6

7-rasm**.** Shifrlangan matnlar va ochiq matnlarning zichlash algoritmi o‘rtasidagi tafovut.

Ochiq kodli OTlarda GOST 28147-89 standarti asosida ochiq kalitlar yordamida shifrlash dasturi “exe” faylari faqat bitta sean kaliti bilan shifrlashda, 10% kam bo‘lmagan zichlash samaradorligini ko‘rsatadi (7 - rasm). Bu esa shunday fayllarda bir xil matnlarning mavjudligi ko‘pligi bilan tushuntiriladi, qolgan barcha fayllarda esa xar xil seans kalitlarida yaxshiroq natijalarga erishish mumkin.

GOST algoritmida uning asl almashtirish jadvalidan va nolga teng bo‘lmagan sessiya kalitidan $\vec{K} \neq 0$ foydalanilganida, barcha chiquvchi bitlarning har qanday kirish bitlariga bog‘liqligini ta’minlash uchun algoritmning 8-9 siklini qo‘llash maqsadga muvofiq. Natijada, GOST algoritmi uchun sikllar sonini hisoblash, unda kirish bitidagi o‘zgarish deyarli barcha chiquvchi bitlarga ta’sir qilmaydi. 1 – va 64 – bitlar uchun berilgan natijalar boshqa bitlarning natijalari bilan bir xil. Nolga teng bo‘lgan sessiya kaliti $\vec{K} = 0$ bilan yana bitta ko‘shimcha sikl paydo bo‘ladi. Umuman olganda, statistik tomondan almashtirish usulining xarakteristikalari (o‘zgarish bitta sikl bo‘lganligi sababli) sessiya kalitiga $\vec{K}$ deyarli bog‘liq emas.

Sinov tariqasida uch turdagi matnli fayllar tanlab olingan. O‘zDSt 1105:2009 standartining kriptobardoshligini ta’minlovchi xususiyatlari: kriptografik akslantirishlarning muvozanatlashganlik (balanslashganlik va muntazamlik) va qat’iy keskin o‘zgarish samaradorlik shartlarini qanoatlantirishini ta’minlash masalasi o‘rganib chiqildi va muvozanatdan og‘ishi o‘rtacha 1.1% teng ekanligi hamda 99.1% chiziqsiz ekanligi aniqlangan.

Ishlab chiqilgan modulda 4 baytli ketma-ketlikni 32 bit belgisiz songa va 32 bit belgisiz sonni navbati bilan 4 bayt ketma-ketlikka aylantiruvchi get va set usullaridan foydalanilgan. Bu usullar ishlab chiqilgan bo‘lib, modulda ham qo‘llanilgan, binobarin ular tashqi funksiyalar emas. 32 bitlik raqamda baytlarni yozish ketma-ketligi GOST 28147-89 ga to‘liq mos keladi. 32 bitli belgisiz raqamga baytlardan ma’lumot kiritish uchun 8 bitga siljishlar qo‘llaniladi. Ruxsat etilgan tashqi qurilmalarga shifrlangan ma’lumotlarni yozishni ta’minlash OT tomonidan bir qator cheklovlar qo‘yish orqali amalga oshirilgan. Natijada, tashqi kiruvchi/chiquvchi qurilmalarni OT yadrosi darajasida ro‘yxatga olish va ulardagi ma’lumotlarning xavfsizligini ta’minlashda shifrlash amalini bajarishning majburiy usuli tufayli, qurilmalardagi ma’lumotlar chiqib ketishining oldi olingan.

Dissertatsiyaning **«GOST 28147-89 algoritmi yordamida shifrlash va arxivlash orqali operatsion tizimdagi ma’lumotlarning himoyalanganligini ta’minlash usullari»** deya nomlanuvchi to‘rtinchi bobi ochiq kodli OT larda GOST 28147-89 algoritmi yordamida shifrlash va arxivlash orqali OT dagi ma’lumotlarning himoyalanganligini tashkillashtirish, initsializatsiya jarayonida tizim fayllarini shifrlash va rasshifrlashni tashkil etishga hamda OT ning fayl tizimi uchun shifrlashning grafik dasturiy ta’minotini ishlab chiqish va grafikli dasturiy majmuasi ishlashining samaradorligini baholashga bag‘ishlangan.

Initsializatsiya bo‘limi uchun ma’lumotlarning yaxlitligi, ularniing maxfiyligidan muhimroq. LUKS (Linux Unified Key Setup) shifrlash usuli shu kabi kamchiliklarni bartaraf etish uchun xizmat qiladi (8-rasm). Asosiy afzalliklaridan biri shuki, shifrlangan bo‘limni soxtalashtirish qiyin.

Shifrlash kalitini saqlash va xavfsiz yuklash muhitini tekshirish uchun TPM (Trusted Platform Module) dan foydalanishni ko‘rib chiqish mumkin. TPM aslida tizimdagi kriptoprotsessor hisoblanadi. Mazkur texnologiya kalitni kiritishni talab qilmasdan tizimda xavfsiz shifrlashni amalga oshirishga (masalan, barmoq izi bilan tizimga kirish yoki shifrlash usuliga bog‘liq bo‘lmagan autentifikatsiya usulidan foydalanish) imkon beradi.

Ideal holda, u UEFI Secure Boot bilan ishlashi kerak, bu o‘z navbatida, tizim sozlamalariga zarar yetganida shifrni ochishga ruxsat bermaydi.

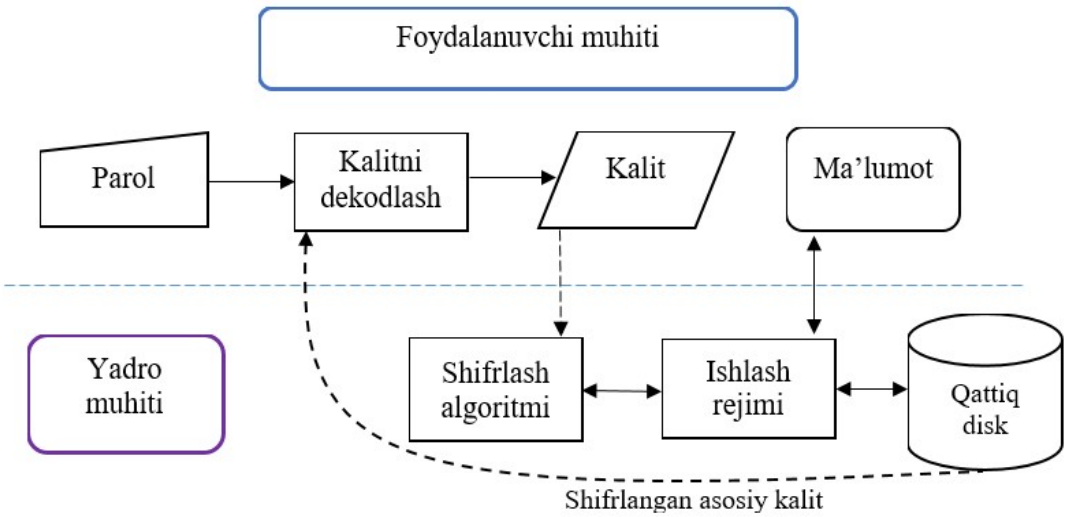
Biroq, Linuxda TPM ni qo‘llab-quvvatlash – hali boshlang‘ich bosqichda. Initsializatsiya zanjirini elektron imzo bilan to‘liq qoplash uchun UEFI Secure Bootdan foydalanilgan.

Mahalliy shifrlash standarti O‘zDSt 1105:2009 AES-256 bilan bir xil kalit o‘lchamiga ega bo‘lganligi sababli, parollar ketma-ketligidan kalit yaratish tartibini o‘zgartirmaslikka qaror qilingan. Buning uchun 7zip SHA-2 xeshlar algoritmidan foydalanilgan va uning yaxshi statistik kriptotahlilga egaligi tufayli undan, psevdotasodifiy ketma-ketlik generatori sifatida qo‘llanilgan.

Biroq, kalitni kengaytirish tartibi AES va mahalliy standart uchun keskin farq qilgan. Shuning uchun AES.c faylida joylashgan butun modul encrytp.c (5-ilova va 6-ilova) o‘zgartirilgan. 7 zip matnni 128 bitli bloklarga bo‘lish va qoidalarga muvofiq kerakli uzunlikka to‘ldirishni amalga oshirilgan. encrytp.c moduli blokning o‘lchamini 64 bitga o‘zgartirgan.

128 soni 64 ga karrali bo‘lganligi sababli, bu o‘zgartirish faqat konstantalarni

o‘zgartirish, shuningdek, bloklar sonini ikki baravar oshirish orqali amalga oshirilgan.



8-rasm. LUKS (Linux Unified Key Setup) shifrlash ketma-ketligi

7 zip CBC rejimidagi shifrlashdan foydalangan (shifrlangan matn bloklarini birlashtirish rejimi), ammo hisoblagich rejimini ham qo‘llashi mumkin. Xuddi shu usul encrytp.c modulini yaratishda inobatga olib ketilgan. Kalitni kengaytirish funksiyasi dastlab 7zip tomonidan yaratilgan maxsus massivni ichki noyob xususiyatidan foydalangan holda, raund kalitlar bilan to‘ldirilganligi sababli, faqat bitta raund shifrlash funksiyasi yaratilgan (shifrlash va rasshifrlash vaqtida amalga oshirilgan).

Ushbu usul turli xil rejimlarda qo‘llanilgan. Ko‘pgina hollarda, tanlangan rejimga qarab ishga tushirish vaqtidagi og‘ishlar ahamiyatsiz. CBC va CFB rejimlarida (shifr matnlarining qayta aloqa rejimi) ishga tushirish vaqti ortgan. CBC rejimida shifrlashni tanlashda ushbu usul uchun kriptobardoshlilik ta’minlangan.

AX tizimining samaradorligini baholash uchun berilgan chastotali protsessorda soniyasiga 1, 2, 5 va 10 martalab “exe” kengaytmali faylni bajarishni tajribadan o‘tkazishda axborot xavfsizligi tizimi o‘rnatilgan va o‘rnatilmagan rejimlarda ko‘rilgan. Faylni bajarish chastotasining har bir qiymati uchun 10 ta tajriba o‘tkazilgan, shundan so‘ng o‘lchov natijasining xatosi hisoblab chiqilgan.

Tajriba natijalarini qayta ishlashda quyidagi amallar bajarilgan:

1) 10 ta sinovning o‘rtacha qiymati quyidagi formula yordamida hisoblab chiqilgan:

$$x_{o'} = \frac{\sum_{i=1}^{N} x_i}{N}$$

2) xatolik quyidagi formula bilan hisoblangan:

$$\Delta x_i = |x_{o'} - x_i|$$

3) o‘lchovlarning kvadratik xatoliklar hisoblab chiqilgan.

4) o‘rta arifmetikning o‘rtacha kvadratik xatoligi quyidagi formula yordamida hisoblangan:

$$S_{x_{o'}} = \sqrt{\frac{\sum(\Delta x_i)^2}{n(n-1)}}$$

5) o‘lchovning ishonchliligi qiymati 0.95 ga tenglashtirilgan;
6) o‘lchov ishonchliligi va o‘tkazilgan tajribalar sonidan berilgan qiymat uchun Styudent koeffitsiyenti $t = 2.262$ aniqlangan;
7) ishonch oralig‘i (o‘lchov xatosi) quyidagi formula yordamida aniqlangan:

$$\Delta x = S_{x_{o'}} \times t$$

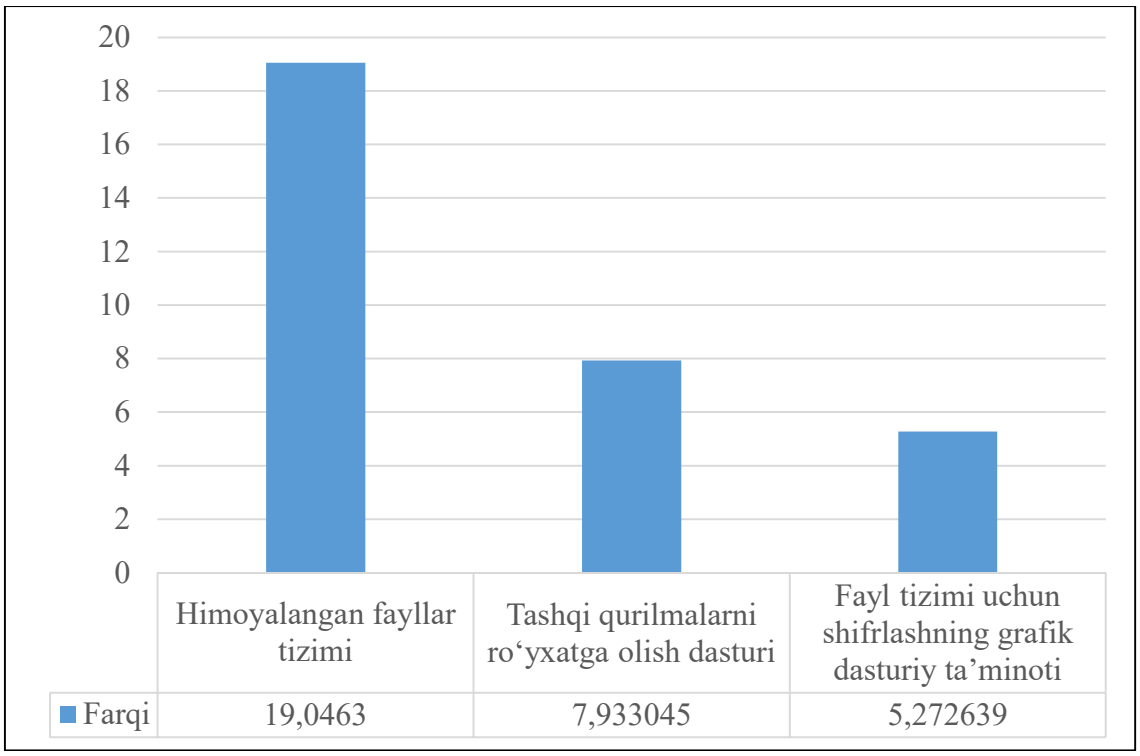
Ilovalarda markaziy protsessorning qo‘shimcha yuklanishi 19% dan oshmaganligini ko‘rish mumkin. Birinchi tajribada bu qiymat 23% dan oshmagan edi. Bundan xulosa qilish mumkinki, olingan model va natijalar to‘g‘ri, markaziy protsessordan foydalanishni esa, yuqorida keltirigan natijalar asosida taxmin qilish mumkin. Shu bilan birga himoyalangan fayllar tizimi uchun yuklash vaqti 5 soniyadan 8 soniyagacha, tashqi qurilmalarni ro‘yxatga olish dasturi uchun – 4 soniyadan 8 soniyagacha, fayl tizimi uchun shifrlashning grafik dasturiy ta’minoti uchun esa – 5 soniyadan 7 soniyagacha oshgan. To‘liq AHTning ishga tushish vaqti 4 soniyaga oshganini ko‘rish mumkin.

Himoya vositalarining ishlash samaradorligi aniqlanib, OT ning hisoblash resurslarining yuklanishiga ta’siri o‘rganilgan hamda ilovani ishga tushirish rejimida protsessorning qo‘shimcha yuklanishi 23% dan oshmasligi va oddiy dastur ishlash rejimidi 17% dan oshmasligi ko‘rsatilgan. Shuningdek dasturni ishga tushirish vaqti 4 soniyadan oshmasligi ko‘rsatilgan (9-rasm). Olingan natijalarning adekvatligi tajribani statistik qayta ishlash bilan isbotlangan.

7zip arxivlash dasturi AES algoritmi bilan shifrlashni amalga oshirib, shifrlashdan oldin ma’lumotlar uchun barcha kerakli tayyorgarliklarni amalga oshirgan (paroldan kalit yaratish, kengaytirilgan ketma-ketlikdan foydalangan holda, shifrni ochishning to‘g‘riligini tekshirish bilan blok uzunligiga karrali xabar qo‘shish, initsializatsiya vektorini yaratish va b.). Shuningdek, AES blokining o‘lchami GOST 28147-89 blokining o‘lchamidan 2 baravarga ko‘pligi sababli GOST 28147-89 dan foydalanish shifrlash tezligini ham birmuncha oshirilishi o‘rganilgan.

Disk shifrlash – ma’lumotlar maxfiyligini ta'minlash uchun etarli emasligining sababi shundaki, diskni shifrlashning o'zi butun tizimni almashtirish va tizim dasturlarini buzishni oldini olmaydi. Biroq, butun ishga tushirish zanjirini UEFI Secure Boot va GPG bilan shifrlash bunday hujumlardan yuqori darajadagi himoyani ta'minlaydi.

Kriptografik modulga kirish uchun juda qulay grafik interfeys ishlab chiqilgan bo‘lib, buning natijasida foydalanuvchi buyruq qatoriga murojaat qilishiga va p7zip dasturiga murojaat qilishiga hamda buyruqlarning ketma-ketligini eslab qolishiga hojat qolmagan.



9-rasm. Ishlab chiqilgan dasturlarning o‘rtacha kvadratik ishlash natijalari

Maksimal rejimda arxivlash tezligi fayl parametrlarini kamaytirish orqali 2-3 martagacha oshirilishi mumkin va mazkur testlar yordamida maxsus yaratilgan arxivlash hamda mahalliy standart yordamida shifrlash dasturidan lug‘at hajmi 256 Mb dan oshmasligini inobatga olib, deyarli har qanday kompyuterda foydalanish mumkinligi isbotlangan.

Hozirgi vaqtda mazkur tadqiqot doirasida ochiq kodli OT larda himoyalangan fayllar tizimi, tashqi qurilmalarni ro‘yxatga olish dasturi, fayl tizimi uchun shifrlashning grafik dasturiy ta’minotlarini amaliyotga joriy etish natijasida ochiq kodli OT larda dasturiy majmualar va ma’lumotlarning xavfsizligini ta’minlash metodlarini qo‘llash obyektlarga qayd qilinmagan murojatlardan himoya qilish va ularning himoyalangan vositalarini qurishdagi samaradorligini aniqlash imkonini beradi.

Natijada mazkur ilmiy tadqiqot doirasida milliy shifrlash algoritmlari asosida xavfsizlik talablariga muvofiq va maxfiy ish yuritish sohasidagi standartlar talablarini qondiruvchi maxsus usullar va xavfsizlik vositalari hamda algoritmlari ishlab chiqilgan va amaliyotga keng joriy etilgan.

XULOSA

«Ochiq kodli operatsion tizimlarda mahalliy standartlar asosida shifrlash usullari va algoritmlari» mavzusidagi dissertatsiya bo‘yicha quyidagi xulosalar taqdim etilgan:

1. Ochiq kodli OT larda shifrlash algoritmlarining samaradorligini ta’minlashda parallel hisoblash texnologiyasi asosida parallel algoritmlar yaratilib,

ularning kriptobardoshliligi aniqlandi va natijada O‘zDSt 1105:2009 shifrlash algoritmiga almashtirish jadvallarining (bayt almashtirish) sifatni baholash funksiyasini qo‘llagan holda, hujumlar uyushtirildi va kriptobardoshliligi aniqlangdi.

2. Himoyalangan fayllar tizimida fayl bloklari va inodlar algoritmlari va ularning ishlash blok-sxemasi, sinov tariqasida turli xil o‘lchamli fayllarda testlar o‘tkazilib, ma’lumotlar hajmidan qat’iy nazar, HFTdan fayllarni o‘qish va yozishda taklif etilayotgan algoritm ext3/4 da ishlovchi tizimlarda ishlash samaradorligini o‘rtacha 0.5 baravarga oshirgan.

3. Milliy shifrlash algoritmlari asosida xavfsizlik talablariga muvofiq va maxfiy ish yuritish sohasidagi maxsus usullar va algoritmlar ishlab chiqildi hamda GOST 28147-89 va O‘zDSt 1105:2009 standartlarining kribtobardoshliligi statistik usullar yordamida aniqlandi va natijada ochiq kodli OT larda O‘zDSt 1105:2009 standarti asosida kalitlar yordamida shifrlash dasturi exe faylarini faqat bitta seans kaliti bilan shifrlashda 10%dan kam bo‘lmagan zichlash samaradorligiga erishilgan.

4. Ruxsat etilgan tashqi qurilmalarga shifrlangan ma’lumotlarni yozishni ta’minlash OT tomonidan bir qator cheklovlar orqali amal oshirilish natijasida, tashqi kiruvchi/chiquvchi qurilmalarni operatsion tizim yadrosi darajasida ro‘yxatga olish va ulardagi ma’lumotlarning xavfsizligini ta’minlashda shifrlash amalini bajarishning majburiy usuli tufayli, qurilmalardagi ma’lumotlar chiqib ketishining oldi olingan.

5. Kriptografik modulga kirish uchun qulay grafik interfeys ishlab chiqilgan bo‘lib, buning natijasida foydalanuvchi buyruq qatoriga murojaat qilish va p7zip dasturiga murojaat qilishmaslik imkoniyati yaratilgan.

6. Diskni shifrlash ma’lumotlarning maxfiyligini ta’minlash uchun yetarli emasligi sababli, UEFI Secure Boot va GPG dan foydalangan holda, butun initsializatsiya zanjirini shifrlash, butun tizimni almashtirishdan va tizim dasturlarini buzishdan himoyalash darajasiga erishilgan.

7. Tajribalar yordamida maxsus yaratilgan arxivlash hamda mahalliy standart yordamida shifrlash dasturida lug‘at hajmi 256 Mb dan oshmasligini inobatga olib maksimal rejimda arxivlash tezligi arxivlash parametrlarini kamaytirish orqali o‘rtacha 2-3 martagacha oshirish mumkinligi isbotlangan.

8. Ilovalarni ishga tushirish rejimida protsessorning qo‘shimcha yuklanishi 23% dan oshmasligi va oddiy dasturda ishlash rejimida 17% dan oshmasligi ko‘rsatildi, shu bilan birga dasturni ishga tushirish vaqti o‘rtacha 4 soniyadan oshmasligi natijasida himoya vositalarining ishlash samaradorligini aniqlangan hamda olingan natijalarning adekvatligi statistik tajribalar asosida isbotlangan.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.02
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ОЧИЛОВ НИЗОМИДДИН НАЖМИДДИН УГЛИ

СОВРЕМЕННЫЕ МЕТОДЫ И АЛГОРИТМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ ОТКРЫТЫМ КОДОМ

05.01.05 - Методы и системы защиты информации. Информационная безопасность

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ТЕХНИЧЕСКИХ НАУК (DSc)**

Ташкент-2023

Тема диссертации доктора технических наук (DSc) зарегистрирована в Высшая аттестационная комиссия при Министерстве высшего образования, науки и инноваций Республики Узбекистан за № B2022.3.DSc/T541

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещён на веб-сайт Научного совета (www.tuit.uz) и на информационно-образовательный портал (www.ziyonet.uz) «ZiyoNet».

Научный консультант:	**Каримов Маджит Маликович,** доктор технических наук, профессор.
Официальные оппоненты:	**Иргашева Дурдона Якубджановна** доктор технических наук, профессор.
	Керимов Камил Фикратович доктор технических наук, доцент.
	Курязов Давлатёр Матякубович доктор физико-математических наук.
Ведущая организация:	**Национальный университет Узбекистана имени Мирзо Улугбека.**

Защита диссертации состоится ___ _____2023 года в __ часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №___). (Адрес: 100202, г.Ташкент, ул. Амир Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан ____ _____ 2023 года.
(протокол рассылки №__ от ____ _____ 2023 года)

Б.Ш. Махкамов
Председатель Научного совета по присуждению ученых степеней, д.э.н., профессор

Э.Ш. Назирова
Ученый секретарь Научного совета по присуждению ученых степеней, д.т.н., профессор

С.К. Ганиев
Председатель Научного семинара при Научном совете по присуждению ученых степеней, д.т.н., профессор

ВВЕДЕНИЕ (аннотация докторской диссертации (DSc))

Актуальность и востребованность темы диссертации. Особое внимание в мире уделяется развитию и совершенствованию систем информационной безопасности (ИБ). На современном уровне развития информационных и коммуникационных систем вопросы защиты операционных систем (ОС), которые являются одними из важнейших механизмов обеспечения эффективной ИБ, остаются особенно актуальными. «Согласно данным "Лаборатории Касперского", количество кибератак в Индии в 2022 году увеличилось на 1,23 раза (23,7%) по сравнению с 2020 годом. В Республике Казахстан (14,38%) и Российской Федерации (18,45%) обнаружение таких атак также увеличилось на 1,3 раза по сравнению с 2021 годом»[1]. В связи с этим, несколько стран Евросоюза, таких как Нидерланды, Германия, Великобритания, Швеция, Франция и другие, приступили к работе в области противодействия кибератакам. Особое внимание уделяется разработке программно-аппаратных средств и механизмов шифрования, которые обеспечивают высокий уровень безопасности информационных систем и защиту системных файлов.

Особое значение в мире придается улучшению эффективности современных алгоритмов шифрования данных и повышению уровня защиты ОС. В научно-исследовательских работах, проводимых в этой области, особое внимание уделяется следующим аспектам: разработка ограничительных методов, основанных на алгоритмах шифрования определенных категорий ресурсов, с целью обеспечения надежной защиты компьютерных систем. Это достигается путем использования комплекса средств защиты, таких как современные методы шифрования и шифрование системных файлов. Также ведется разработка программных комплексов для защиты информационных систем в ОС. Все эти усовершенствования направлены на обеспечение более высокого уровня безопасности.

В Республике Узбекистан особое внимание уделяется наряду с развитием информационных технологий в государственном и хозяйственном управлении широкому использованию средств и методов защиты данных в компьютерных системах и защите данных от угроз в ОС. В связи с этим достигнуты значительные результаты в обнаружении и устранении угроз и атак на компьютерные системы, в том числе разработка системы мониторинга информационной безопасности, системы обнаружения и реагирования на атаки в целях обеспечения защиты компьютерных системах.

В определенной степени данное диссертационное исследование служит реализации решений указов и постановлений Президента Республики Узбекистан "О стратегии развития нового Узбекистана на 2022-2026 годы", №УП-60 "О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций" от 28 января 2022 года, №УП-4024 "О мерах по контролю за внедрением информационных технологий и

[1] https://securelist.ru/it-threat-evolution-in-q1-2022-non-mobile-statistics/105173/

коммуникаций, организации их защиты" от 21 ноября 2018 года и №УП-4452 “О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты” от 14 сентября 2019, а также задач, поставленных в других нормативно-правовых актах, связанных с этой деятельностью.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в рамках приоритетного направления развития науки и технологий республики IV. «Развитие информатизации и информационно-коммуникационных технологий».

Обзор зарубежных исследований по теме диссертации.

Во многих странах предпринимаются усилия по обеспечению информационной безопасности в операционных системах с открытым исходным кодом. Операционные системы с открытым исходным кодом, такие как Linux, FreeBSD и другие, имеют глобальное сообщество разработчиков и экспертов по безопасности, которые вносят свой вклад в их разработку и безопасность. Можно назвать некоторые страны, где ведутся работы по обеспечению информационной безопасности в операционных системах с открытым исходным кодом.

В США существует множество организаций, институтов и университетов, которые проводят исследования в области информационной безопасности в операционных системах с открытым исходным кодом. Такие организации, как АНБ (Агентство национальной безопасности), NIST (Национальный институт стандартов и технологий) и CERT (Группа реагирования на компьютерные чрезвычайные ситуации), активно занимаются исследованиями и разработкой методов и алгоритмов для обеспечения безопасности операционных систем.

В Германии, Франции, Великобритании, Италии и других странах Европы ведутся исследования и разработки методов обеспечения информационной безопасности в операционных системах с открытым исходным кодом. Некоторые университеты и исследовательские центры, такие как Рурский университет Бохума (Германия), ENISA (Европейское агентство по сетевой и информационной безопасности) и OWASP (Открытый проект безопасности веб-приложений), проводят исследования в этом направлении.

В Канаде также есть активное сообщество разработчиков и исследователей, работающих в области информационной безопасности в операционных системах с открытым исходным кодом. Некоторые университеты, в том числе Университет Ватерлоо и Университет Калгари, активно занимаются исследованиями и разработками в области кибербезопасности.

Российская Федерация также работает над обеспечением информационной безопасности в операционных системах с открытым исходным кодом. Различные организации, в том числе российские компании, университеты и исследовательские центры, активно проводят исследования по

разработке и повышению безопасности операционных систем в университетах, институтах и частных компаниях. В Российской Федерации по заказу представителей спецслужб была разработана и внедрена в практику операционная система с открытым исходным кодом «РОСА Линукс», разработанная и поддерживаемая компанией РОСА Лабс.

В связи с тем, что большая часть научных работ по данной теме является конфиденциальной, нет возможности анализировать данные в сети Интернет и знакомиться и использовать операционные системы с открытым исходным кодом, разработанные и выпущенные рядом ведущих стран. Это, в свою очередь, создает трудности для исследователей, работающих в этом направлении.

Степень изученности проблемы. Такие ученые, как Л. Торвальдс, Р. Херцог, Б. Керниган проводили исследования по разработке ОС, принадлежащих к семейству Linux. Были изучены научно-исследовательские работы таких зарубежных и отечественных ученых, как Р.Пайк, Б.Уорд, Д.Барретт, С.Алапати, А.Робачевский, Д.Н. Колеснеченко, М.Фленов, С.Немнюгин, О.Стесик, Т.Адельштайн, Б.Любанович, С.Л.Скловская в области создания системы защиты информации в операционной системе Linux.

В научных разработках стран СНГ и Республики Узбекистан были изучены операционные системы (ОС) «Astra Linux», «Заря» для разработки средств и методов защиты информации, различных методов, моделей и алгоритмов шифрования, средств защиты, теоретических и практических основ защиты информации, а также ОС «Альт Linux» и «РОСА». Исследованы графические оболочки Doppix, используемые в разных государственных учреждениях.

В научных статьях М.М. Каримова, Х.А.Музаффарова, Г.У. Жураева и А.Икрамова были изучены методы создания систем шифрования и защиты с алгоритмом ГОСТ 28147-89. В научных работах Д.Н. Колесниченко и В. Аллена, во всех выпусках журнала Linux Format за 2014 - 2016 годы внедрялись алгоритмы и структура ядра ОС Linux, скорость обработки пакетных данных, модели безопасности, средства защиты.

В то же время средства и методы защиты от угроз в сети до конца не проанализированы, выявлены недостатки в существующих алгоритмах, недостаточно изучены средства управления устройствами для защиты от неправомерных воздействий.

Связь диссертационного исследования с планами научно-исследовательских работ учреждения, в котором выполнена диссертация. Диссертационное исследование выполнено в рамках проектов Государственного центра тестирования при Кабинете Министров Республики Узбекистан по теме «Разработка систем и инструментов защиты для информационных систем» в соответствии с программой до 2022 года «Дорожной карты» на три года в сфере инновационной деятельности.

Целью исследования является используемая в Республике Узбекистан разработка специальных методов и средств защиты на основе отечественных

алгоритмов шифрования, отвечающих требованиям безопасности и стандартов в области конфиденциальности.

Целью исследования является разработка специальных методов и алгоритмов, а также алгоритмов на основе национальных алгоритмов шифрования, отвечающих требованиям безопасности и удовлетворяющих требованиям стандартов в области конфиденциальности в ОС с открытым исходным кодом.

Задачи исследования:

классификация оценки качественных показателей алгоритмов шифрования в современных ОС с открытым исходным кодом и анализ режимов шифрования с помощью задач распараллеливания;

создание требования к использованию файловых структур B+ при разработке защищенных файловых систем (ЗФС) и алгоритмов предложено создания ЗФС-систем для организации каталогов и журналов в ЗФС;

создание методов и алгоритмов организации шифрования в структуре ядра открытой ОС;

разработка технологии шифрования в структуре ядра на основе алгоритмов ГОСТ 28147-89 и O‘zDSt 1105:2009 с использованием архивации в открытых ОС, а также разработка алгоритмов и механизмов регистрации, удаления и форматирования допустимых внешних устройств, создание алгоритмов записи на них зашифрованных данных;

организация защиты данных в ОС путем шифрования и архивирования с помощью алгоритма ГОСТ 28147-89, организация шифрования и расшифрования системных файлов при процессе инициализации, разработка программного обеспечения для шифрования файловой системы ОС и оценка эффективности работы графического программного комплекса;

В качестве **объекта исследования** были взяты отечественные алгоритмы шифрования и созданные с их помощью защищенные файловые системы в ОС с открытым исходным кодом.

В качестве **предмета исследования** - методы и алгоритмы шифрования, основанные на отечественных стандартах в ОС с открытым кодом.

Методы исследования. В ходе исследования были использованы методы защиты информации, теория алгоритмов, математические методы а также упорядоченное и объектно-ориентированное программирование.

Научная новизна исследования заключается в:

на основе технологии параллельных вычислений и определении криптостойкости для обеспечения эффективности алгоритмов шифрования в ОС с открытым кодом;

предложены алгоритмы, оптимизированные для работы с файловыми системами ext3/4 и проверена функциональность шифрования в защищенной файловой системе и в ядре для файлов различных размеров, а также представлены современные подходы к чтению и записи файлов;

на основе национальных алгоритмов шифрования разработаны специальные методы и алгоритмы в области конфиденциальной работы, отвечающие требованиям безопасности, а также были определены

криптостойкость с помощью статистических методов стандарта O‘zDSt 1105:2009;

в результате реализации ОС, обеспечивающих запись зашифрованных данных на разрешенные внешние устройства, были разработаны методы обязательный регистрации внешних устройств ввода-вывода на уровне ядра ОС и выполнения шифрования для обеспечения безопасности данных;

были предложены эффективные способы защиты от взлома системных программ и замены системы путём шифрования всей цепочки инициализации с помощью UEFI Secure Boot (протокол UEFI для проверки электронной цифровой подписи в приложениях) и GPG (программа для шифрования данных и создания электронной цифровой подписи) путем шифрования и архивирования по алгоритму ГОСТ 28147-89 с целью обеспечения конфиденциальности данных в ОС.

Практические результаты исследования заключаются в следующем:

были организованы атаки и определена криптостойкость для каждой из таблиц подстановки алгоритма шифрования O‘zDSt 1105:2009 с использованием функции автоматической оценки качества линейным и дифференциальным методом;

разработаны алгоритмы файловых блоков и inodов в защищенной файловой системе и блок-схема их работы, были проведены тесты на файлах разного размера и оценены, а предложенный алгоритм чтения и записи файлов из ЗФС увеличил эффективность систем ext3/4 в среднем на 0,5 разы;

была достигнута эффективность сжатия не менее 10% при шифровании только одним сеансовым ключом стандарта O‘zDSt 1105:2009 в ОС шифрования исполняемых файлов программ “exe” расширением;

с помощью экспериментов доказано, что скорость архивирования в максимальном режиме может быть увеличена в среднем до 2-3 раз за счет уменьшения параметров файла с учетом того, что размер словаря не превышает 256 Мб в специально созданное программное обеспечение для архивирования и шифрования с использованием местного стандарта;

созданный криптографический модуль был протестирован на соответствие отечественному стандарту, и было подтверждено, что он реализует алгоритм шифрования/расшифрования, основанный на отечественных стандартах.

Достоверность результатов исследования. Используя количественную и качественную оценку результатов методами, цели и задачи исследования соответствующими предмету через исследования на теоретическом и практическом уровнях обеспечена достоверность методологии исследования.

Научная значимость результатов исследования. Она состоит из алгоритмов и практических апробаций, предлагаемых в работе программных средств, позволяющих расширить функциональные возможности систем защиты информации на основе внедрения принципа совместного использования и разделения в физической и логической защите данных. Предложены универсальные механизмы защиты и обработки информации и разработаны алгоритмы, позволяющие разработать алгоритмы и методы,

отвечающие требованиям безопасности для ОС с открытым кодом в соответствии с законодательством Республики Узбекистан.

Практическая значимость результатов исследования. Оно заключается в разработке системы защиты информации, отвечающей требованиям собственных алгоритмов шифрования O‘zDSt 1105:2009 и ГОСТ 28147-89 и допускающей применение в государственных или коммерческих учреждениях, связанных с использованием ее выводов государственными и юридическими органами для обеспечения защиты конфиденциальной информации. Внедрение результатов исследования обеспечит переход к более обоснованной и целенаправленной политике информационной безопасности, связанной с использованием пользовательских информационных систем и технологий в министерствах и ведомствах Республики Узбекистан. Практическая значимость результатов исследования обеспечит переход к более обоснованной и целенаправленной политике ИБ, связанной с использованием пользовательских информационных систем и технологий в министерствах и ведомствах Республики Узбекистан.

Внедрение результатов исследования. Разработанные средства и методы защиты информации, основанные на результатах, полученных по разработанным алгоритмам:

программное обеспечение для шифрования с использованием открытых ключей на основе стандарта O‘zDSt 1105:2009 в системах с открытым исходным кодом показало эффективность сжатия не менее 10% при шифровании файлов “exe” только одним сеансовым ключом. Также, ОС обеспечивала запись зашифрованных данных на разрешенные периферийные устройства через ряд ограничений. В результате утечка данных на устройствах была предотвращена из-за обязательного метода регистрации внешних входящих/исходящих устройств на уровне ядра ОС и выполнения операции шифрования при сохранении данных на них (Справка № 11- № 06/13043 от 17 ноября 2022 года Министерства строительства Республики Узбекистан). В результате научного исследования программного обеспечения, соответствующего требованиям “Закона о кибербезопасности”, а также внедрения данного программного обеспечения в практику, сэкономлены 1,2 миллиарда сумов организации;

разработан метод шифрования на основе алгоритма ГОСТ 28147-89 с использованием архивирования в ОС с открытым кодом и алгоритмы и механизмы регистрации, выключения и форматирования разрешенных внешних устройств, алгоритмы записи в них зашифрованных данных. Организация защиты информации в ОС путем шифрования и архивирования по алгоритму ГОСТ 28147-89, организация шифрования и расшифрования системных файлов в процессе инициализации, разработала графическое программное обеспечение шифрования для файловой системы ОС (Справка № 45/01-08-7954 от 23 ноября 2022 года ГУП “Центр комплексной экспертизы проектов и импортных контрактов” при Министерстве экономического развития и сокращения бедности Республики Узбекистан). В результате применение программных комплексов и методов обеспечения безопасности

информации в ОС с открытым кодом позволило защитить объекты от незарегистрированных обращений и определить их эффективность при построении защищенных ОС;

созданный криптографический модуль был протестирован и проверен на соответствие локальному стандарту. Определена эффективность работы средств защиты и изучено влияние на загрузку вычислительных ресурсов ОС, а также показано, что в режиме запуска приложения дополнительная загрузка процессора не превышает 23%, а в режиме нормальной работы приложения не превышает 17%. Также показано, что время запуска программы не превышает 4 секунды. Адекватность полученных результатов доказывается статистической обработкой эксперимента. Также были протестированы и оценены алгоритмы файловых блоков и inodов в защищенной файловой системе и блок-схема их работы на файлах разного размера (Справка № 4/7271 от 24 ноября 2022 года Министерства транспорта Республики Узбекистан). Результаты показывают, что независимо от размера данных эффективность работы в системах, работающих на ext3/4, алгоритме, предлагаемом при чтении и записи файлов ЗФС, была увеличена почти в 0,5 раза.

Предложенный алгоритм чтения и записи файлов из защищенных файловых систем, использованный в нашем в диссертационном исследовании на тему «Современные методы и алгоритмы обеспечения информационной безопасности в операционных системах с открытым кодом» повышает эффективность работы в системах, работающих на ext3/4, почти в 0,5 раза (Справка № 40 от 21 декабрья 2022 г. Государственного центра тестирования при Кабинете Министров Республики Узбекистан). В результате, в рамках данного научного исследования были разработаны и широко внедрены в практику специальные методы и средства и алгоритмы защиты, отвечающие требованиям безопасности и отвечающие требованиям стандартов в области конфиденциального делопроизводства на основе национальных алгоритмов шифрования.

Апробация результатов исследования. Результаты данного исследования апробированы в 8 научных статьях, в том числе, на 3-х международных и 5-х республиканских научных конференциях.

Публикация результатов исследований. Всего по теме исследования опубликовано 26 научных статьи. Из них 12 статей рекомендованы к публикации по основным результатам докторских диссертаций ВАК, 3 опубликованы в зарубежных научных журналах, в том числе на регистрацию продуктов программного обеспечения для ЭВМ получено 3 сертификата.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 182 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении приводятся актуальность и востребованность темы диссертации, обосновано соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, определены цель и задачи исследования, степень изученности проблемы, обоснована достоверность полученных результатов и раскрыто теоретико-практическое значение исследования. Приведена информация о внедрении в практику результатов исследования, представлены сведения по опубликованным работам, структуре и объему диссертации, дан перечень результатов выполнения, опубликованных работ и сведения о структуре диссертации.

Первая глава диссертации **«Проблемы обеспечения эффективности алгоритмов шифрования в операционных системах с открытым кодом»** посвящена исследованию эффективности алгоритмов шифрования на основе международных стандартов, используемых в настоящее время в операционных системах с открытым кодом, характеристикам алгоритмов шифрования и анализу защищенных файловых систем.

Были проанализированы международные и местные стандарты в этой области с целью обеспечения информационной безопасности на основе алгоритмов шифрования в операционных системах. Примерами таких стандартов являются ГОСТ 28147-89 и O‘zDSt 1105:2009. Алгоритмы блочного шифрования широко используются в операционных системах с открытым кодом.

Среди них алгоритмы шифрования MXA (Агентство национальной безопасности) США и ТК-26 (ГОСТ 2) Российской Федерации. Большинство операционных систем выполняют операции шифрования для шифрования файловой системы или системных файлов. В операционных системах семейства Linux существует метод полного шифрования диска (FDE-Full Disk Encryption) – он продолжает оставаться одним из наиболее эффективных способов защиты от кражи данных с компьютера и внешних устройств. Система FDE запускается перед загрузкой операционной системы (рис.1). Это, в свою очередь, означает, что после запуска системы код операционной системы начинает загружаться на зашифрованную среду. Система шифрования, в частности, замедляет работу операционной системы. Все операции шифрования/расшифрования выполняются незаметно для пользователя. Когда шифруется весь жесткий диск (файлы виртуальной памяти, временные файлы), он шифруется вне зависимости от уровня важности. Если пользователь системы теряет пароль шифрования зашифрованного жесткого диска, данные восстанавливаются с помощью закрытого ключа системного администратора.

Обеспечение информационной безопасности является одним из приоритетных задач международного сообщества. Сотрудничество между государствами в данной сфере все еще развивается. В Республике Узбекистан также особое внимание уделяется защите государственной тайны и

конфиденциальной информации. В нашей стране действует алгоритм шифрования/расшифрования, созданный на основе стандарта O‘zDSt 1105:2009, описывающий алгоритм блочного шифрования. В данном разделе диссертационной работы приведены теоретические результаты, полученные на основе стандарта O‘zDSt 1105:2009. В криптографическом стандарте O‘zDSt 1105:2009 обмен таблицами состоит из 256 значений и формируется в соответствии с приведенной формулой по аргументам d, L, R в зависимости от расширенного ключа CSE. В результате анализа стандарта шифрования O‘zDSt 1105:2009 было установлено, что:

в криптографическом стандарте O‘zDSt 1105:2009 обмен таблицами состоит из обмена 256 значениями, и по приведенной формуле бит на аргументах d, L, R формируется в зависимости от расширенного ключа k_{se}.

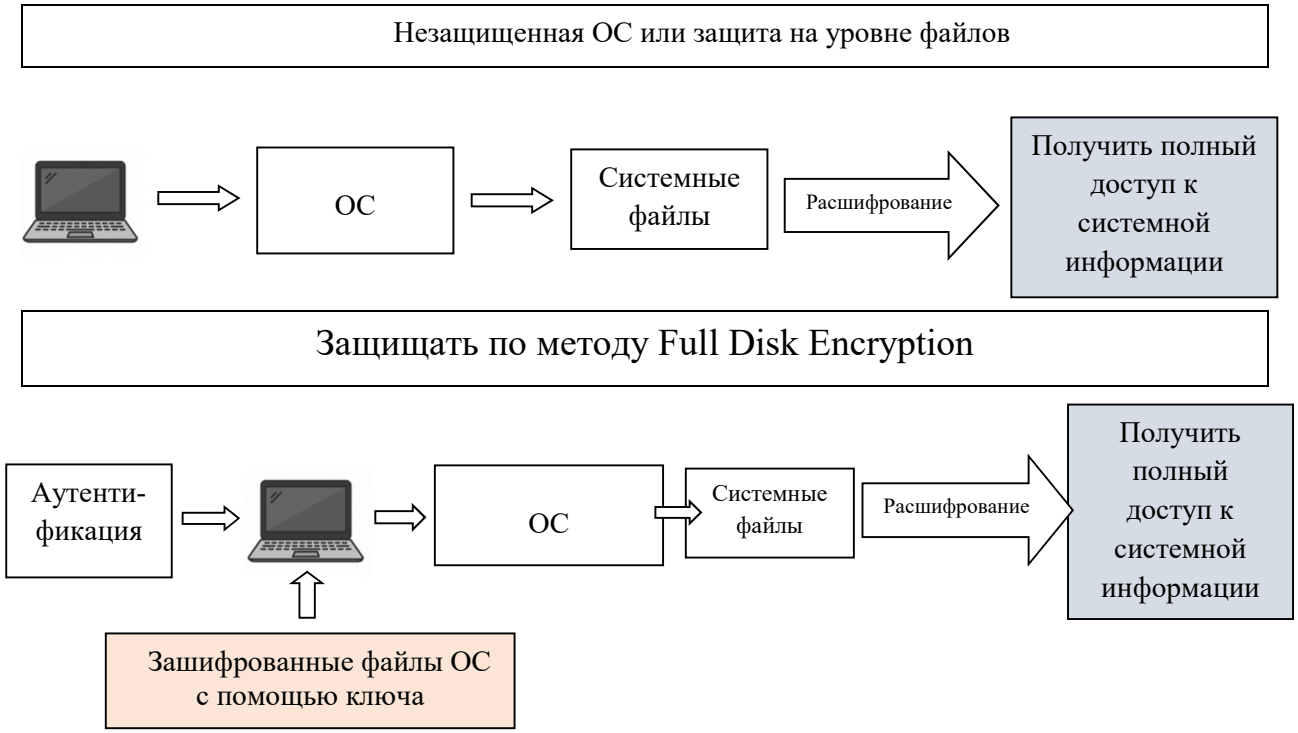


Рис. 1. Отличие защиты методом **FDE** от незащищенной защиты файлов операционной системы

В результате анализа стандарта шифрования O‘zDSt 1105:2009 выявлено следующее:

- алгоритм шифрования O‘zDSt 1105:2009 использует 2 ключа - ключ шифрования и функциональный ключ, каждый из которых представляет собой 256-битную последовательность.

Взаимодействие этих ключей эквивалентно использованиюв алгоритм е шифрования 512-битного ключа шифрования, что, в свою очередь, предотвращает возможность несанкционированного расшифрования данных;

- при использовании элементов повышенной безопасности функциональный ключ меняется в каждом сеансе;

- подтверждена устойчивость стандарта шифрования O‘zDSt 1105:2009 к линейному и дифференциальному анализу, для которого требуется более 4 раундов.

Общее количество таблиц замещения, сформированных на основе различных значений этих параметров, составляет 4 161 600. Поэтому нашей основной целью является анализ метода автоматической проверки качества замещающих таблиц, используемого в алгоритме шифрования стандарта O‘zDSt 1105:2009. Алгоритм, используемый в криптографическом стандарте O‘zDSt 1105:2009 Республики Узбекистан, является относительно новым поэтому данный стандарт относительно мало изучен.

В процессе анализа криптографического стандарта O‘zDSt 1105:2009 используется параллельный алгоритм, позволяющий автоматически оценивать таблицы замещения, что позволяет анализировать произвольные таблицы замещения на основе созданного алгоритма. Например, при проверке всех 4-битных таблиц замещений или стабильности конкретных классов функций становится возможным усовершенствовать этот алгоритм.

Поскольку S-блок является “сердцем” всей криптосистемы, результаты проводимых на нем исследований имеют большое практическое значение.

В ходе анализа также изучено время инициализации системы в режимах шифрования.

В большинстве случаев начальные временные отклонения шифрования в зависимости от выбранного режима не имеют значения. В режимах CBC и CFB время инициализации увеличивается.

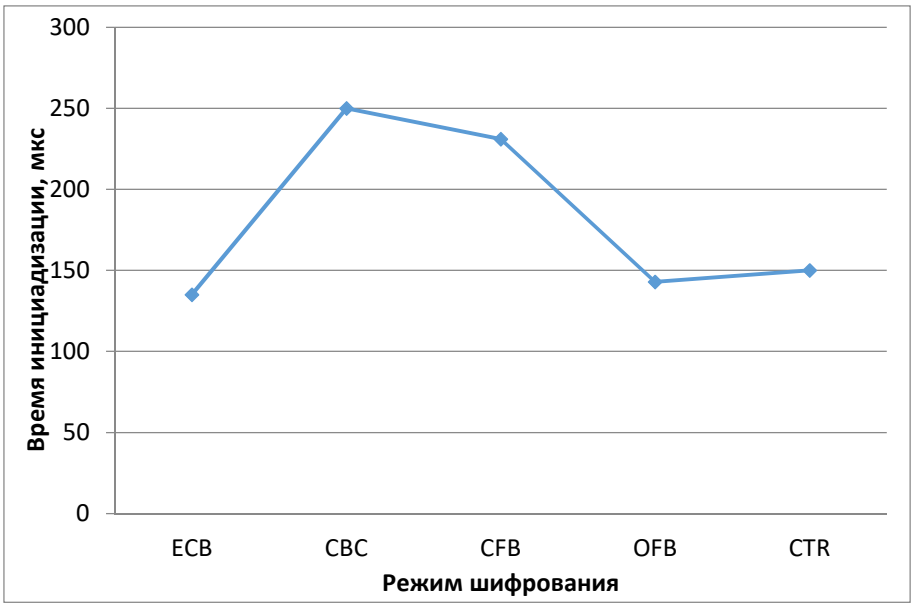
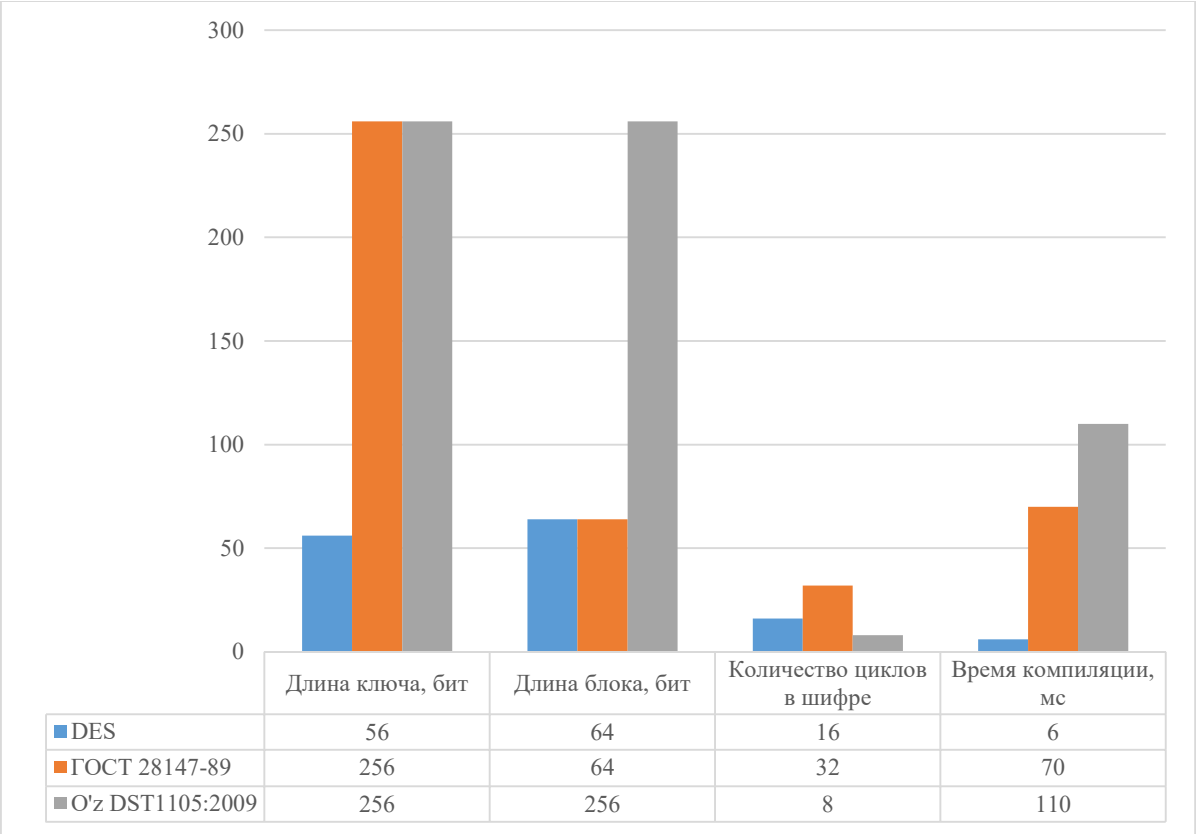


Рис.2. Время инициализации режимов шифрования

В режиме CBC повышается криптографическая устойчивость алгоритма шифрования (рис. 2). На основании анализа выбираем режим CBC для стандарта O‘zDSt 1105:2009 с учетом защищенности информации и криптостойкости шифротекстов, и разумно принять в качестве информации,

что время инициализации для шифрования в этом режиме составляет 0,00025 секунды.

В алгоритмах шифрования ГОСТ 28147-89 и O‘zDSt 1105:2009 замещающие блоки не устанавливаются, а скрываются, как в DES. Ключ, используемый в шифровании, имеет длину 256 бит, что повышает криптостойкость (рис. 3).



	Длина ключа, бит	Длина блока, бит	Количество циклов в шифре	Время компиляции, мс
DES	56	64	16	6
ГОСТ 28147-89	256	64	32	70
O'z DST1105:2009	256	256	8	110

Рис.3. Анализ алгоритмов шифрования в операционных системах с открытым исходным кодом

Все большее число государственных организаций и коммерческих фирм начинают использовать альтернативное бесплатное программное обеспечение. В частности, многие предприятия и организации начинают использовать бесплатные операционные системы Linux вместо платных операционных систем Windows.

Файловая система, входящая в состав операционной системы, используется для создания документов и выполнения различных операций.

Одной из особенностей операционных систем Linux является то, что они поддерживают файловую систему, которая работает на больших участках жестких дисков, легко измеряет тысячи файлов и эффективно работает с файлами разных размеров.

Предложена классификация оценки качественных показателей алгоритмов шифрования и проведен анализ режимов шифрования с использованием задач распараллеливания. Стандарты шифрования/

расшифрования данных для современных операционных систем и операционных систем с открытым исходным кодом сравнивались и оценивались по скорости обработки и криптоанализу. Для разработки и создания ЗФС (защищенная файловая система) рекомендуется использовать файловую систему ЗФС. Файловая система ЗФС может поддерживать большие объемы файлов и обеспечивать хорошую производительность потокового I/O (ввода/вывода).

Во второй главе диссертации **«Современные методы и алгоритмы шифрования в защищенной файловой системе и структуре ядра»** посвящена установлению требования и алгоритмов создания систем B+, протоколов ЗФС и журналов, использующих структуру файлов ЗФС при создании защищенной файловой системы, а также методам организации алгоритмов шифрования и обработки в структуре ядра защищенной файловой системы.

ЗФС использует файловую структуру B+ во всех ситуациях. Они используются для индексации пакетов inode, списков свободных мест, записей каталогов и записей карты файлов. В файловой структуре B+ ЗФС (рис. 4) во внутренних узлах хранятся только ключи и индикаторы, а в листьях — данные ключей. Поскольку ЗФС имеет несколько файловых структур, общий код работает только со стандартными заголовками блоков.

Каждый внутренний узел дерева B+ — это p_0, key_1, p_1, key_2, p_2,... , то p_n, где p_i — указатель i-листа, $0 \le i \le n$, то — ключ, ключи в узле расположены в порядке возрастания $key_1 < key_2 < \ldots < key_n$. Все ключи в маленьком дереве имеют индикатор p_0 показателем k_1 маленький. Для условия $0 \le i \le n$ все ключевые настройки являются ориентировочными k_i и k_i меньше +1. Все ключи с индикатором p_n имеют k_n малый размер.

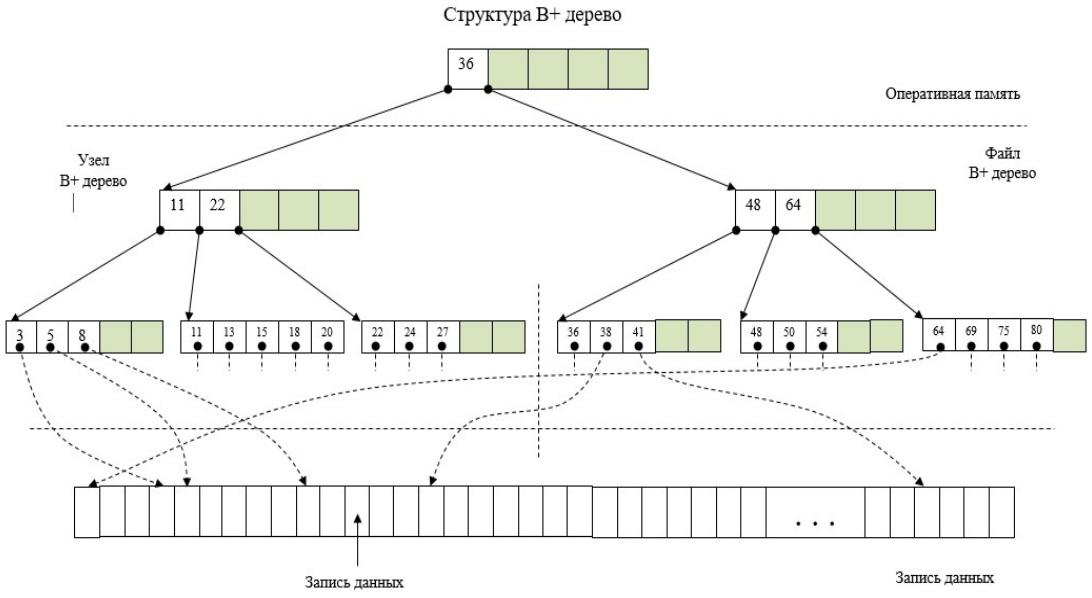


Рис. 4. B+ древообразная файловая структура ЗФС

После каждого заголовка файла существуют массивы данных. Формат ключей и записей определяется типом дерева соответственно. Система ЗФС используется как 64-битная файловая система.

При создании такой файловой системы индикаторы не обязательно должны быть 64-битными. Хранение указателей в пределах 32-битного значения является одним из основных механизмов использования групп разделения. В среднем размер каждой разделительной группы составляет 0,5-4 Гб и имеет шесть структур данных для управления расположением inodов и блоков в своих границах. Ограниченный размер взаимозаменяемых групп позволяет использовать внутри них относительно 32-битные номера inodов, а это, в свою очередь, содержит параметры структур данных на приемлемых уровнях.

В то время как группы обмена в структурах используют 32-битные числа для данных, содержащихся в них, глобальные структуры данных могут ссылаться на блоки и inod в любой точке файловой системы, используя 64-битные указатели.

Помимо этого, недолговечные файлы могут вообще физически не храниться на диске. ЗФС не успевает принять решение об их размещении, прежде чем закрыть их. Группы обмена редко используются для группировки данных, они служат центром обработки данных для очень больших файлов или каталогов ЗФС (с целью уменьшения фрагментации и улучшения читаемости).

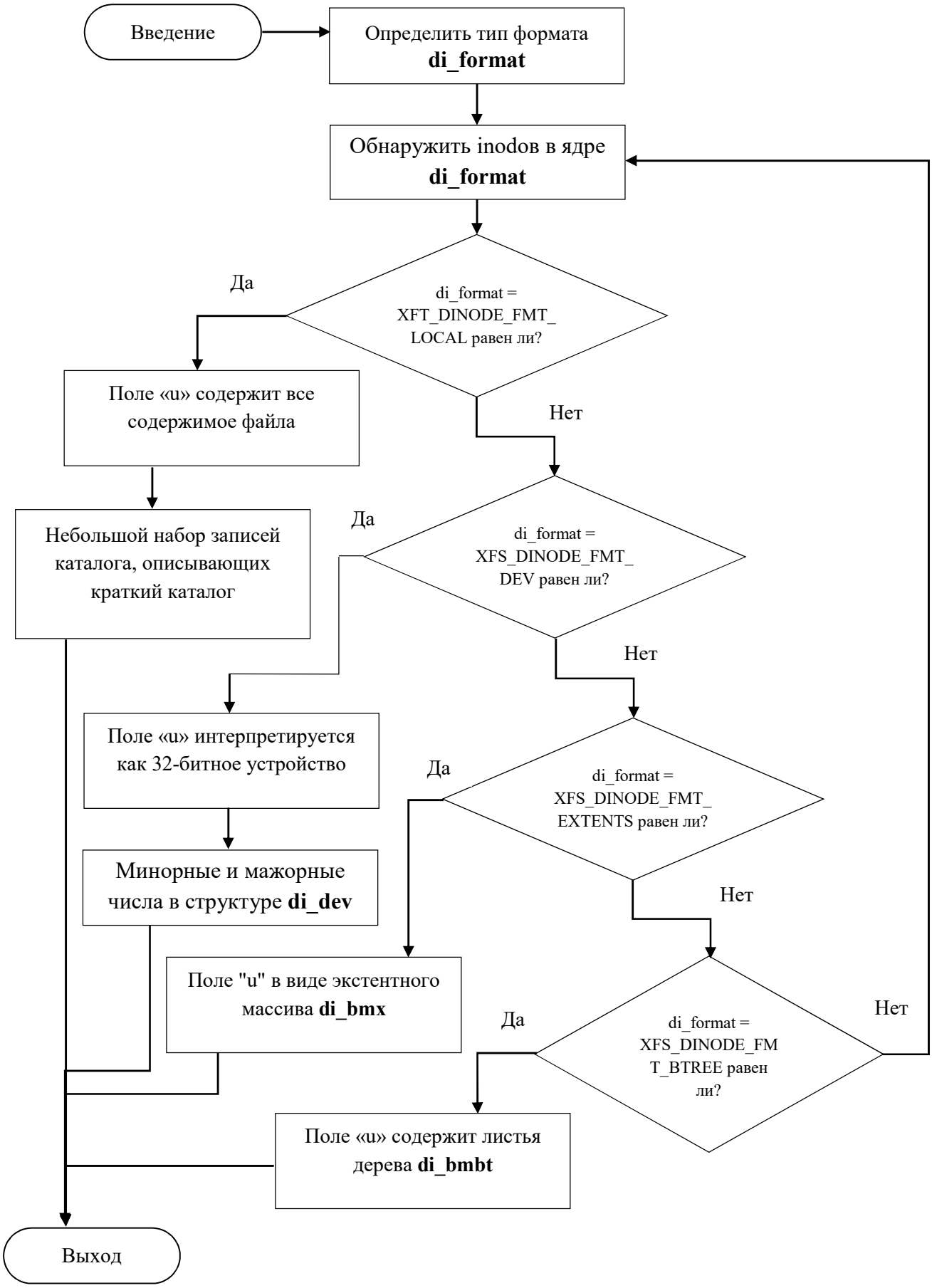
Создание ЗФС - систем является весьма сложным процессом, и хороших результатов можно добиться в процессе обработки больших и средних файлов, используя продуманные программистами алгоритмы разделения дискового пространства и управляя запросами пользователей с помощью эффективных методов параллелизма.

В ЗФС - системах каждый inod состоит из четырех частей - ядра, адреса следующего подключения, параметров u и a. Ядро содержит постоянные данные, специфичные для всех типов inodов. Группа распределений функционально связана со следующим связанным адресным полем, отделенным от ядра, и описывается следующим образом в виде блок-схемы (блок-схема 1).

Содержимое каталога в файловой системе ЗФС хранится непосредственно в inode или адресуется через файловое дерево.

Все операции в структурах каталога являются логическими, т.е. файловая система обращается к карте файлов, чтобы найти физическое состояние некоторых элементов и вносит соответствующие изменения.

Если каталог не помещается в единый блок, он расширяет древовидную структуру для хранения в ЗФС, которая содержит данные из элементов каталога. Состоит из имен файлов и их inodов и блоков, содержащих индексную информацию в блоках данных, а также имен и хеш-значений соответствующих элементов в каталоге. К этим конструкциям прикрепляются пустые блоки. Логическое пространство внутри файла каталога считается 8-битным словом.



Блок-схема - 1. Алгоритм создания inodов

Эти структуры можно назвать только древовидными структурными системами.

На самом деле в системе ЗФС каталоги индексируются с помощью хеширования. Все это заставляет ЗФС функционально отставать от расширенных файловых систем, таких как reiserfs.

Программа проверки целостности системных файлов была дополнительным механизмом обеспечения безопасности операционной системы.

Такие системы создают возможность в режиме реального времени проверять изменения в файлах и каталогах. Выполняется проверка суммы хеша для обеспечения целостности системных файлов. В ней используется алгоритм хеширования ГОСТ Р 34.11-2012. Этот механизм также контролирует появление избыточных файлов в системных каталогах и изменение атрибутов файлов ОС. Также возможно выполнение хеширования с использованием хеш-функций O‘zDSt 1106:2009, но уровень криптостойкости низкий.

В качестве теста, предыдущая версия ЗФС была относительно новой по сравнению с недавно предложенной и файловой системой ext3/4 при работе с одним или двумя потоками, ЗФС относительно медленнее, чем ext3/4, но когда количество потоков достигает восьми, скорость системы увеличивается линейно (Рис. 5).

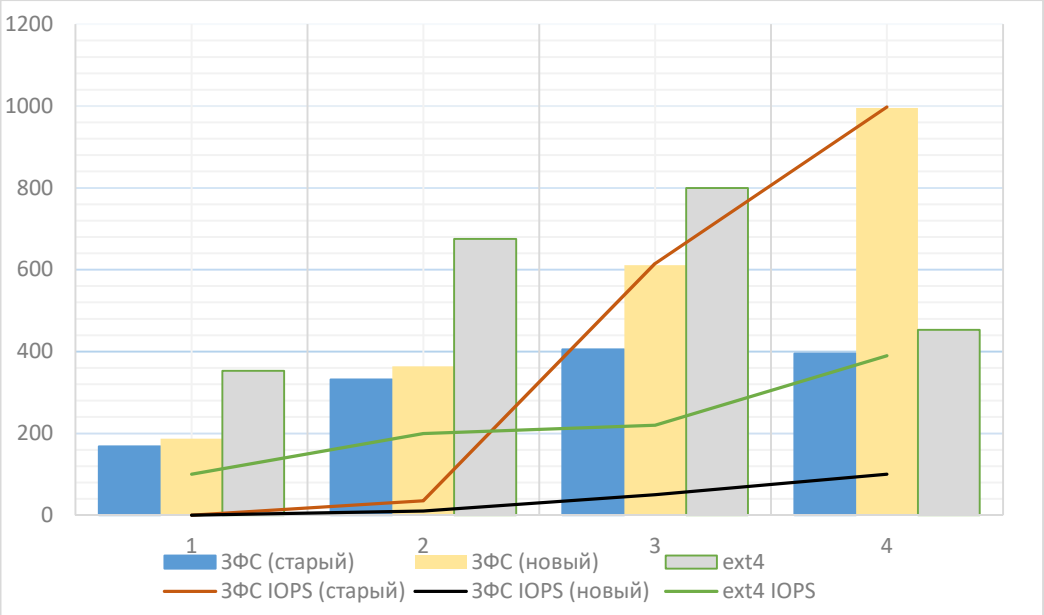


Рис.5. Сравнительный график файловых систем

Для решения вышеуказанных проблем были изменены файлы thunar-enum-types.c и thunar-list-model.c файлового менеджера Thunar. Среди стандартной информации о файле нет значения, включающего уровни доступа. Цифры внутри больших стрелок указывают на последовательность ссылок.

Создается дополнительные модификации и опции файлового менеджера

Thunar, чтобы пользователям ОС было удобно работать с файловой системой и видеть уровни обработки файлов. Для выполнения этой задачи требуется решить два типа задач.

Во-первых, определяется столбец в таблице (не используемый файловой системой) и в нем отображается информация об уровне производительности.

Во-вторых, следует разработать модуль, который инструктирует файловый менеджер о том, где и как получить нужную вам информацию. Для выполнения этих задач используются стандартные библиотеки и функции ОС.

Для решения вышеуказанных проблем были изменены файлы thunar-enum-types.c и thunar-list-model.c файлового менеджера Thunar. Среди стандартной информации о файле нет значения, включающего уровни доступа. В следующем модуле показаны уровни доступа к файлам в интерфейсе файлового менеджера (рис. 6). Цифры внутри больших стрелок указывают на последовательность ссылок.

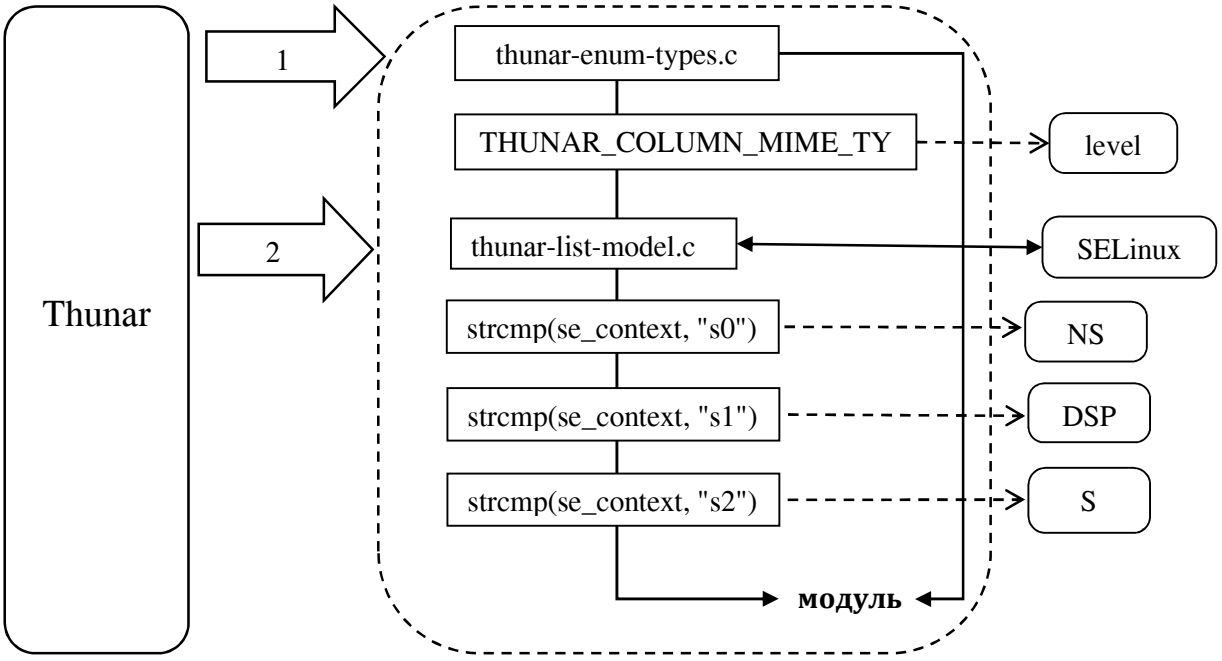


Рис. 6. Уровни доступа к файлам в интерфейсе файлового менеджера

В защищенной файловой системе алгоритмы файловых блоков и inodов и блок-схема их работы, как правило, тестировались в файлах разных размеров и оценивались по ним. Результаты показывают, что предложенный алгоритм чтения и записи файлов из фиксированных ЗФС в размер данных увеличивает эффективность работы на системах под управлением ext3/4 в среднем в 0,5 раза. С помощью файлового менеджера Thunar были созданы дополнительные функции, облегчающие пользователям ОС работу с защищенной файловой системой и просмотр уровней обработки файлов.

В третьей главе диссертации **«Современные методы и алгоритмы шифрования и архивирования на основе отечественных стандартов»**, разработаны методы и алгоритмы шифрования/расшифрования на основе

отечественных стандартов.

Приведен криптоанализ алгоритма шифрования O‘zDSt 1105:2009 по местным стандартам шифрования, а также статистический анализ алгоритма шифрования ГОСТ 28147-89.

Предложен метод шифрования на основе алгоритма ГОСТ 28147-89 с использованием архивации в ОС с открытым кодом. Разработаны алгоритмы и механизмы записи, удаления и форматирования фиксированных внешних устройств, создан алгоритм записи на них зашифрованных данных.

Создан графический интерфейс в целях автоматизации работы с внешними устройствами.

В данном разделе представлены псевдокод и замены шифра, а также замена алгоритма шифрования и оценка практической криптографической устойчивости (на примере алгоритма шифрования данных O‘zDSt 1105:2009).

На основании этих результатов мы можем констатировать, что алгоритм симметричного блочного шифрования O‘zDSt 1105:2009 отличается высокой устойчивостью к методам линейного и дифференциального криптоанализа. Можно сказать, что действующий алгоритм симметричного блочного шифрования O‘zDSt 1105:2009 обеспечивает высокую криптографическую защиту при использовании для защиты данных.

С одной стороны, математическим доказательством влияния одновременного изменения бита на все исходящие биты цикла в открытом тексте является ортогональность (не взаимосвязанность) пар шифровых текстов, соответствующих одинаково различному прямому тексту $m_w = 32$. Если рассматривать абсолютно случайный 64-битный блок (состоящий из независимых двоичных символов), то закон распределения для ненулевого числа битов в таких блоках является биномиальным с параметрами.

$$m_w = np_0 = 64 \cdot \frac{1}{2} = 32,$$

$$\sigma_w^2 = np_0(1 - p_0) = 64 \cdot \left(\frac{1}{2}\right)^2 = 16 .$$

При значении $np0\ (1\text{-}p_0) \geq 10$ биномиальное распределение с высокой степенью приближения сравнивается с нормальным законом распределения вероятностей (на основе формулы Муавра-Лапласа). Полученные значения m_w случайны и равны 32. Получить четкий ответ на поставленный выше вопрос можно, если использовать методы доверительного интервала. То есть суть математического статистического метода, специально разработанного для составления набора приближенных значений неизвестных параметров распределения вероятностей, заключается в следующем:

$EX_i = \theta_1$ независимые случайные величины $X_1, X_2, \ldots, X_n, n \geq 2$ подчиняются одному и тому же нормальному закону с неизвестными параметрами и для построения $u(\theta) = \theta_1$ требуется оценка интервала $DX_i = \theta_2$.

$$\bar{X} = \frac{1}{n} \cdot \sum_{i=1}^{n} X_i \; ; \quad s^2 = \frac{1}{n-1} \cdot \sum_{i=1}^{n} (X - \bar{X})^2 \qquad (1)$$

Поскольку случайная величина $T = \frac{\sqrt{n}(\bar{X}-\theta)}{s}$ подчиняется уровню c_{n-1} распределения Стьюдента и не зависит от неизвестных параметров q_1 и $q_2(|\theta_1| \leq \infty, \theta_2 > 0)$, вероятность события для любого t остается зависимым только от t.

$$\left\{\bar{X} - \frac{t \cdot s}{\sqrt{n}} < \theta_1 < \bar{X} + \frac{t \cdot s}{\sqrt{n}}\right\} \qquad (2)$$

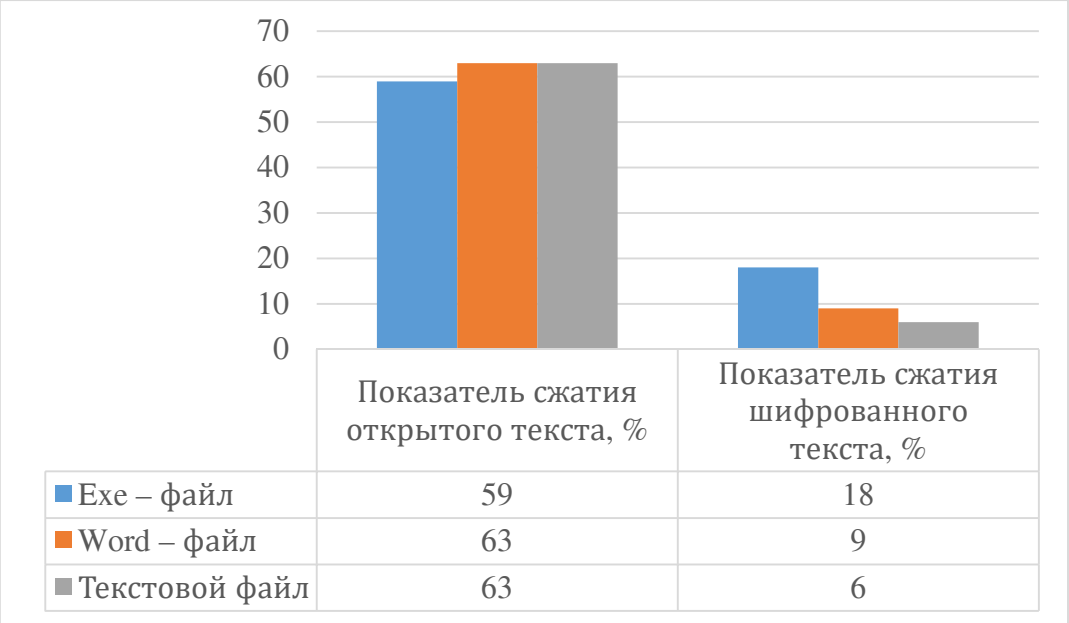
Если за оценку C в заданном интервале взять q_1, то u следующие $P_c(\theta_1, \theta_2) = P\{|T| < t\} = 1 - \alpha$ соответствуют вероятностному интервалу. Интервал таких значений является интервалом доверительных вероятностей, а его пределы называются пределами доверительного интервала.

Если, оценка в указанном интервале принимается за q_1, то следующий $P_c(\theta_1, \theta_2) = P\{|T| < t\} = 1 - \alpha$, не зависящий от $\theta = \{\theta_1, \theta_2\}$, соответствует вероятностному интервалу. Такой промежуток интервалов называется доверительным интервалом вероятностей, а его границы – границами доверительного интервала. Согласно приведенным выше тарифам, в качестве доверительного интервала $P_c(\theta_1, \theta_2) = 0{,}999 \longrightarrow (\alpha = 0{,}001)$, на основании приведенной выше таблицы Стьюдента числовое значение n составляет n = 1024 (на основе экспериментов) t = 3,291 и (t·s) получаем t = 3,291 ва $\frac{t \cdot s}{\sqrt{n}} = \frac{3{,}291 \cdot 4}{\sqrt{1024}} = 0{,}4$. Однако можно предположить, что m_w соответствует доверительному интервалу и удовлетворяет следующему условию: $32\text{-}0{,}4 \leq m_w \leq 32+0{,}4$. При использовании алгоритма ГОСТ 28147-89 из его исходной таблицы коммутации и ненулевого сеансового ключа $\vec{K} \neq 0$ целесообразно использовать 8-9 циклов алгоритма, чтобы все выходящие биты зависели от любых входящих битов. В результате расчет количества тактов по алгоритму ГОСТ 28147-89, при котором изменение входящего бита не влияет на все выходящие биты.

Результаты для битов 1 и 64 такие же, как и для других битов. При нулевом переключателе сеанса $\vec{K} = 0$ появляется еще один дополнительный цикл. В целом характеристики метода статистического переключения практически не зависят от сеансового ключа $\vec{K}$ (поскольку изменение происходит за один цикл).

В качестве теста были выбраны три типа текстовых файлов. В ОС с открытым кодом, шифрование с использованием открытых ключей на основе стандарта ГОСТ 28147-89, «exe» файлы показывают эффективность сжатия не менее 10% при шифровании только одним сеансовым ключом (рис. 7). Это объясняется тем, что в таких файлах много одинаковых текстов, а во всех

остальных файлах лучших результатов можно добиться с разными сеансовыми ключами.



	Показатель сжатия открытого текста, %	Показатель сжатия шифрованного текста, %
Exe – файл	59	18
Word – файл	63	9
Текстовой файл	63	6

Рис.7. Разница сжатия открытого текста между зашифрованными текстами и алгоритмами

Особенности криптостойчивости стандарта O‘zDSt 1105:2009 исследована проблемой обеспечения того, чтобы криптографические отражения удовлетворяли условиям (сбалансированности и регулярности) и строго резкой изменчивости эффективности, а также установлено, что отклонение от равновесия равно 1.1% и выявлена нелинейность 99,1%.

В разработанном модуле используются методы get и set, преобразующие 4-байтовую последовательность в 32-битное беззнаковое число и 32-битное беззнаковое число в 4-байтовую последовательность соответственно. Эти методы также использовались в разработанном модуле, они не являются внешними функциями. Последовательность записи байтов в 32-битном числе полностью соответствует ГОСТ 28147-89. 8-битные сдвиги используются для ввода данных из байтов в 32-битное число без знака. Обеспечение записи зашифрованных данных на фиксированные периферийные устройства было реализовано ОС через ряд ограничений. В результате утечка данных с устройств была предотвращена благодаря обязательному способу регистрации внешних входящих/исходящих устройств на уровне ядра ОС и выполнению операции шифрования для обеспечения безопасности содержащихся в них данных.

Глава четвертая диссертации **«Методы обеспечения защиты данных в операционной системе путем шифрования и архивирования с использованием алгоритма ГОСТ 28147-89»** посвящена организации защиты данных в ОС посредством шифрования и архивирования с использованием алгоритма ГОСТ 28147-89 в ОС с открытым кодом. А также она посвящена организации шифрования и расшифрования системных файлов

в процессе инициализации, разработке графических программных обеспечений шифрования для файловой системы и оценке эффективности функционирования графического программного комплекса. Для отдела инициализации целостность данных важнее, чем конфиденциальность ваших данных. Метод шифрования LUKS (Linux Unified Key Setup) служит для устранения таких недостатков (рис.8). Одним из основных преимуществ является то, что зашифрованный раздел трудно подделать.

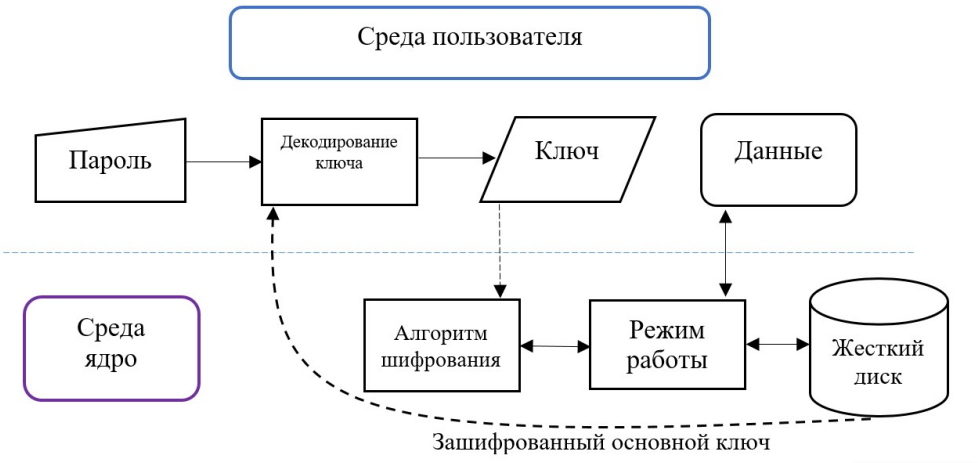


Рис.8. Последовательность метода шифрования LUKS (Linux Unified Key Setup)

Рассмотрим возможность использования TPM (Trusted Platform Module) для хранения ключа шифрования и проверки безопасной среды загрузки. TPM на самом деле является криптопроцессором в системе. Эта технология позволяет выполнять безопасное шифрование в системе без необходимости ввода ключа (например, используя вход по отпечатку пальца или метод аутентификации, не зависящий от метода шифрования). В идеале он должен работать с UEFI Secure Boot, который, в свою очередь, не позволяет выполнять расшифровку при повреждении системных настроек.

Однако поддержка TPM в Linux все еще находится в зачаточном состоянии. Мы используем UEFI Secure Boot, чтобы полностью покрыть цепочку инициализации электронной подписью.

Поскольку отечественный стандарт шифрования O‘zDSt 1105:2009 имеет тот же размер ключа, что и AES-256, было принято решение не менять порядок генерации ключей из последовательности паролей. Для этого 7zip использует алгоритм хеширования SHA-2. Причина, по которой он имеет хорошую статистическую криптостойкость заключается в том, что он используется в качестве генератора псевдослучайных последовательностей.

Однако, процедура расширения коммутатора кардинально отличается для AES и местного стандарта. Поэтому весь модуль, находящийся в файле AES.c, был модифицирован файл encrytp.c (Приложение 5 и Приложение 6). 7zip осуществляет разбиение текста на 128-битные блоки и заполнение их до нужной длины в соответствии с правилами. encryptp.c модуль изменяет

размер блока на 64 бита, поскольку число 128 является 64 кратным. А также это изменение не только осуществляет изменение константы, но и удваивает количество блоков.

7zip использует шифрование в режиме CBC (режим слияния зашифрованных текстовых блоков), но можно использовать и режим счетчика.

Этот же метод был учтен при создании модуля encryptp.c. Поскольку функция расширения ключа изначально была заполнена раундовыми ключами с использованием встроенного уникального свойства пользовательского массива, созданного 7zip, была создана только одна раундовая функция шифрования (осуществляется во время шифрования и расшифрования).

Этот метод используется в разных режимах. В большинстве случаев отклонения во времени запуска в зависимости от выбранного режима незначительны. В режимах CBC и CFB (режим обратной связи шифротекста) время запуска увеличивается. При выборе шифрования в режиме CBC для данного метода обеспечивается криптостойкость.

Для оценки эффективности работы системы информационной безопасности при проведении эксперимента по выполнению файла с расширением «exe» 1, 2, 5 и 10 раз в секунду на процессоре с заданной частотой система информационной безопасности строилась в встроенном и неустановленном режимах. Для каждого значения частоты выполнения файла выполнялось по 10 экспериментов, после чего вычислялась ошибка результата измерения.

Для обработки результатов эксперимента были предприняты следующие шаги:

1) среднее значение 10 тестов рассчитывается по следующей формуле:

$$x_{\text{o}} = \frac{\sum_{i=1}^{N} x_i}{N}$$

2) ошибка рассчитывалась по следующей формуле:

$$\Delta x_i = |x_{\text{o}} - x_i|$$

3) квадратичные ошибки вычислялись по следующей формуле.

4) средние квадратичные ошибки среднего арифметического рассчитываются по следующей формуле:

$$S_{x_{\text{o}}} = \sqrt{\frac{\sum(\Delta x_i)^2}{n(n-1)}}$$

5) значение надежности измерения было равно 0,95.

6) для значения, полученного из достоверности измерения и количества проведенных экспериментов, был определен коэффициент Стьюдента t = 2,262.

7) Доверительный интервал (ошибка измерения) определялся по следующей формуле:

$$\Delta x = S_{x_{\check{y}}} \times t$$

Дополнительная загрузка центрального процессора в приложениях не превышает 19%. В первом эксперименте это значение не превышало 23%. Из этого можно сделать вывод, что полученная модель и результаты верны, а использование центрального процессора можно предсказать на основании результатов, которые мы привели выше.

При этом время загрузки для защищенной файловой системы увеличилось с 5 до 8 секунд, для программы записи внешних устройств – с 4 до 8 секунд, а для графического программного обеспечения шифрования для файловой системы – с 5 до 7 секунд. Время запуска полной СИБ увеличилось до 4 секунд.

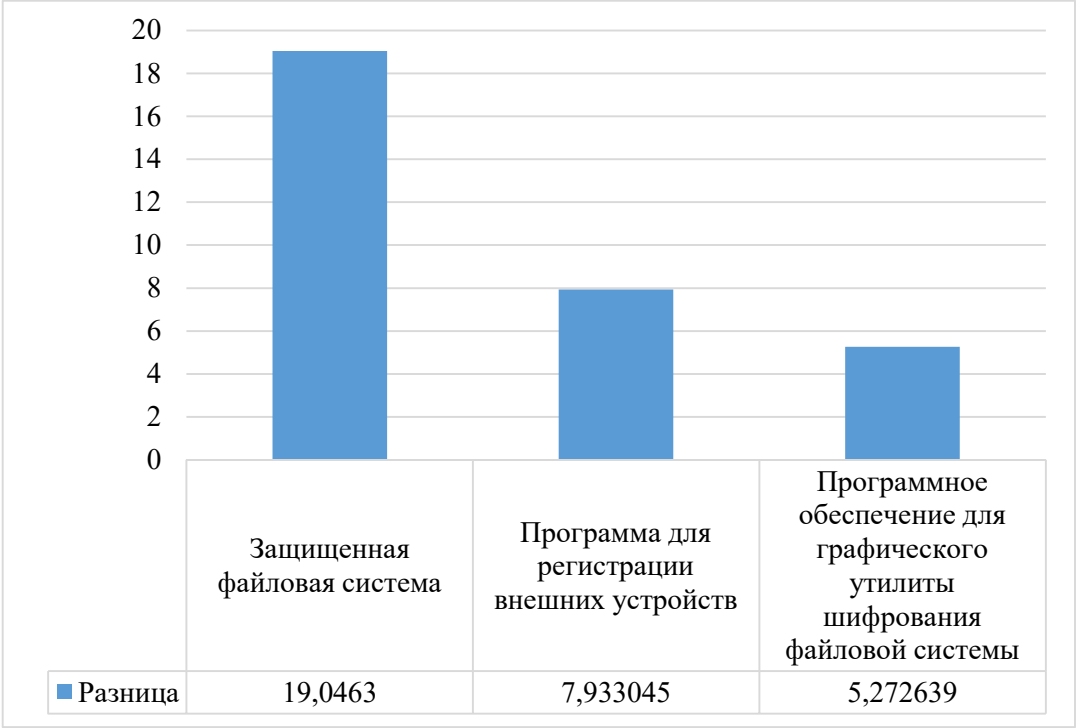


Рис.9. Средние квадратичные результаты производительности разработанных программ

Определена эффективность средств защиты и изучено влияние ОС на загрузку вычислительных ресурсов, при этом дополнительная загрузка процессора в режиме запуска приложений не превышала 23%, а в обычном режиме работы программ не превышала 17%, при этом время запуска программы не превышало 4 секунд (рис. 9.). Адекватность полученных результатов доказано статистической обработкой эксперимента.

Программное обеспечение для архивации 7zip выполняет шифрование алгоритмом AES и делает все необходимые приготовления данных перед шифрованием (создание ключа-пароля, добавление сообщения к длине блока путем проверки правильности расшифровки с помощью расширенной последовательности, создание вектора инициализации и т.д.). Также было изучено, что из-за того, что размер блока AES в 2 раза больше размера блока

ГОСТ 28147-89, использование ГОСТ 28147-89 также несколько увеличивает скорость шифрования на единицу.

Причина, по которой шифрование диска недостаточно для обеспечения конфиденциальности данных, заключается в том, что только шифрование диска не предотвращает замену всей системы и взлом системных программ. Однако шифрование всей цепочки инициализации с помощью UEFI Secure Boot и GPG позволяет достичь более высокого уровня защиты от таких атак.

Для доступа к криптографическому модулю был разработан очень удобный графический интерфейс, так что пользователь может получить доступ к командной строке и получить доступ к программе p7zip без необходимости запоминать последовательность команд.

В максимальном режиме скорость архивации можно увеличить до 2-3 раз за счет уменьшения параметров файла, и эти тесты доказали, что специально созданную архивацию, а также программу шифрования по местному стандарту можно использовать практически на любых компьютерах.

Предложенные в рамках данного исследования методы обеспечения сохранности программных комплексов и данных в ОС с открытым исходным кодом в результате практической реализации защищенных файловых систем, программного обеспечения для регистрации внешних устройств, графического программного обеспечения шифрования для файловой системы позволяет защитить объекты от незарегистрированных обращений и определить их эффективность при создании защищенных инструментов.

В результате были разработаны и широко внедрены на практике специальные методы и средства защиты, а также алгоритмы, соответствующие требованиям безопасности и удовлетворяющие требованиям стандартов в области конфиденциальной работы на основе национальных алгоритмов шифрования.

ЗАКЛЮЧЕНИЕ

В диссертации на тему «Методы и алгоритмы шифрования на основе отечественных стандартов в операционных системах с открытым кодом» представлены следующие выводы.

1. С целью обеспечения эффективности алгоритмов шифрования в ОС с открытым исходным кодом были созданы параллельные алгоритмы на основе технологии параллельных вычислений, определена криптостойкость, в результате которой были организованы атаки и определена криптостойкость с использованием функции оценки качества таблиц подстановки (замена байта) алгоритма шифрования O‘zDSt1105:2009.

2. В качестве теста были проведены тесты на различных размерах и оценены алгоритмы файловых блоков и inodов в защищенной файловой системе, что при чтении и записи файлов из ЗФС независимо от объема данных предлагаемый алгоритм повысил производительность в системах, работающих на ext3/4, в среднем в 0.5 раза.

3. На основе отечественных алгоритмов шифрования были разработаны специальные методы и алгоритмы в области секретного делопроизводства, а также с использованием статистических методов была определена криптостойкость стандартов ГОСТ 28147-89 и O‘zDSt1105:2009, и в результате в ОС с открытым исходным кодом был принят стандарт O‘zDSt1105:2009, на основе шифрования с открытым ключом была достигнута эффективность сжатия не менее 10% при шифровании exe - файлов только одним сеансовым ключом.

4. В результате обеспечения записи зашифрованных данных на стационарные внешние устройства, реализованных ОС с помощью ряда ограничений, утечка данных на устройствах была предотвращена за счет обязательного метода регистрации внешних входящих/исходящих устройств на уровне ядра ОС и выполнения шифрования для обеспечения безопасности данных в них.

5. Для доступа к криптографическому модулю разработан удобный графический интерфейс, благодаря которому пользователю не нужно обращаться к командной строке и программе p7zip, запоминая последовательность команд.

6. Причина отсутствия конфиденциальности данных шифрования диска в том, что шифрование всей цепочки инициализации с помощью UEFI Secure Boot и GPG позволило добиться уровня защиты от подмены всей системы и взлома системных программ.

7. Было доказано, что максимальная скорость архивации может быть увеличена до 2-3-х раз за счет уменьшения параметров архивации, и эти тесты доказали, что специально созданную архивацию, а также программу шифрования по местному стандарту можно использовать практически на любом компьютере, при условии, что размер словаря не превышает 256 МБ.

8. Определена эффективность работы средств защиты и изучено влияние ОС на загрузку вычислительных ресурсов, при этом дополнительная загрузка процессора в режиме запуска приложений не превышала 23%, а в обычном режиме работы программы не превышала 17%, а также адекватность полученных результатов подтверждалась с помощью статистических экспериментов.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

OCHILOV NIZOMIDDIN NAJMIDDIN UGLI

MODERN METHODS AND ALGORITHMS FOR ENSURING INFORMATION SECURITY IN OPERATING SYSTEMS OPEN CODE

05.01.05 – Methods and systems of information protection. Information Security

DISSERTATION ABSTRACT OF THE DOCTOR OF SCIENCE (DSc) ON TECHNICAL SCIENCES

Tashkent-2023

The theme of doctor of science (DSc) on technical sciences was registered at the Supreme attestation commission at the Ministry of higher education, science and innovation of the Republic of Uzbekistan under number B2022.3.DSc/T541.

The dissertation has been prepared at Tashkent University of Information Techologies.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website (www.tuit.uz) and on the website of «ZiyoNet» Information and educational portal (www.ziyonet.uz).

Scientific adviser:	**Karimov Madjit Malikovich** Doctor of Technical Sciences, Professor.
Official opponents:	**Irgasheva Durdona Yakubdjanovna** Doctor of Technical Sciences, Professor.
	Керимов Камил Фикратович Doctor of Technical Sciences, docent.
	Курязов Давлатёр Матякубович Doctor of Physical and Mathematical Sciences.
Leading organization:	**National University of Uzbekistan named after Mirzo Ulugbek**

The defense will take place "____" _____ 2023 at _____ the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No. _____). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on "____" _____ 2023 y.
(mailing report No. ___ on "____" _____ 2023 y.).

B.Sh. Makhkamov
Chairman of the Scientific Council
awarding scientific degrees,
Doctor of Economic Sciences, Professor

E.Sh. Nazirova
Scientific secretary of Scientific Council
awarding scientific degrees,
Doctor of Technical Sciences, Professor

S.K. Ganiyev
Chairman of the Academic seminar under the
Scientific council awarding scientific degrees,
Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is the development of special methods and algorithms, as well as algorithms based on national encryption algorithms that meet security requirements and meet the requirements of privacy standards in an open source OS.

The object of the research work domestic encryption algorithms and protected file systems created with their help in an open source OS were taken.

The scientific novelty of the research work is as follows:

based on the technology of parallel computing and the definition of cryptographic strength to ensure the effectiveness of encryption algorithms in an open source OS;

Algorithms optimized for working with ext3/4 file systems are proposed, encryption functionality in the secure file system and in the kernel is tested for files of various sizes, and modern approaches to reading and writing files are presented;

on the basis of national encryption algorithms, special methods and algorithms have been developed in the field of confidential work that meet security requirements, and cryptographic strength has also been determined using the statistical methods of the standard

O'zDSt 1105:2009;

as a result of the implementation of operating systems that ensure the recording of encrypted data on permitted external devices, methods have been developed for mandatory registration of external input-output devices at the OS kernel level and encryption to ensure data security;

effective methods have been proposed to protect against hacking of system programs and system replacement by encrypting the entire initialization chain using UEFI Secure Boot (UEFI protocol for verifying electronic digital signature in applications) and GPG (program for data encryption and creating electronic digital signature) by encryption and archiving according to the GOST 28147-89 algorithm in order to ensure the confidentiality of data in the OS. **Implementation of the research results.**

The developed means and methods of information protection, based on the results obtained by the developed algorithms:

public key encryption software based on the O'zDSt 1105:2009 standard in open source systems has shown a compression efficiency of at least 10% when encrypting "exe" files with only one session key. Also, the operating system provided the writing of encrypted data to permitted peripheral devices through a number of restrictions. As a result, data leakage on devices was prevented due to the mandatory method of registering external incoming / outgoing devices at the operating system kernel level and performing an encryption operation when saving data on them (Reference No. 11- No. 06/13043 of November 17, 2022 of the Ministry of Construction of the Republic Uzbekistan). As a result of a scientific study of software that meets the requirements of the “Cybersecurity Law”, as well as the implementation of this software in practice, 1.2 billion soums of the organization were saved;

developed an encryption method based on the GOST 28147-89 algorithm using archiving in open source operating systems and algorithms and mechanisms for registering, turning off and formatting allowed external devices, algorithms for writing encrypted data to them. Organization of information protection in the operating system by encryption and archiving according to the GOST 28147-89 algorithm, organization of encryption and decryption of system files during the initialization process, developed graphical encryption software for the operating system file system (Reference No. 45/01-08-7954 dated November 23 2022 State Unitary Enterprise “Center for Comprehensive Expertise of Projects and Import Contracts” under the Ministry of Economic Development and Poverty Reduction of the Republic of Uzbekistan). As a result, the use of software systems and methods for ensuring information security in an open source operating system made it possible to protect objects from unregistered accesses and determine their effectiveness in building secure operating systems;

the created cryptographic module has been tested and checked against the local standard. The effectiveness of the protection means was determined and the impact on the loading of the computing resources of the operating system was studied, and it was also shown that in the application startup mode, the additional processor load does not exceed 23%, and in the normal operation mode of the application does not exceed 17%. It is also shown that the program start time does not exceed 4 seconds. The adequacy of the obtained results is proved by statistical processing of the experiment. Also, the algorithms of file blocks and inodes in a secure file system and the block diagram of their work on files of different sizes were tested and evaluated (Reference No. 4/7271 dated November 24, 2022 of the Ministry of Transport of the Republic of Uzbekistan). The results show that regardless of the size of the data, the performance of the algorithm offered when reading and writing FSS files was increased by almost 0.5 times in systems running on ext3/4;

the proposed algorithm for reading and writing files from protected file systems in the dissertation research on the topic "Modern methods and algorithms for ensuring information security in open source operating systems" increases the efficiency of work in systems running on ext3 / 4 by almost 0.5 times (Reference No. 40 of December 21, 2022 of the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan). As a result, within the framework of this scientific study, special methods and means and algorithms of protection were developed and widely implemented in practice that meet security requirements and meet the requirements of standards in the field of confidential record keeping based on national encryption algorithms.

Structure and volume of the dissertation. The dissertation consists of an introduction, four chapters, a conclusion, a list of references and applications. The volume of the dissertation is 182 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo‘lim (I часть; I part)

1. Очилов Н.Н. Шифрлаш усуллари ва алгоритмлари таҳлили // Фан ва технологиялар тараққиёти. Бухоро ш., 2021. №6.-Б.160-165. (05.00.00; № 24)

2. Очилов Н.Н. Creating Secure File Systems in Open-Source Operating Systems // WSEAS Transactions on Systems. ISSN / E-ISSN: 1109-2777 / 2224-2678, Volume 21, 2022, Art. #24,-P.221-232 (Scopus, DOI: 10.37394/23202.2022.21.24; IF = 0.8).

3. Каримов М.М., Очилов Н.Н., Тангиров А. Е. Encryption Methods and Algorithms Based on Domestic Standards in Open-Source Operating Systems // WSEAS Transactions on Information Science and Applications. ISSN / E-ISSN: 1790-0832 / 2224-3402, Volume 20, 2023, Art. #6 - P.42-49 (Scopus, DOI: DOI: 10.37394/23209.2023.20.6; IF = 0.3).

4. Каримов М.М., Очилов Н.Н. Создание алгоритмов каталогов и журналирования в защищенных файловых системах // Узбекский журнал "Проблемы информатики и энергетики". Ташкент: Фан ва технология, 2021 №2.-Б.104-111 (05.00.00; № 5).

5. Очилов Н.Н. Шифрлаш усуллари ва алгоритмлари таҳлили // Инновацион технологиялар. Қарши ш., 2022/1(45) - сон. -Б.54-60 (05.00.00; № 38).

6. Очилов Н.Н. Analysis of international and local standards of information protection in modern operating systems // International Scientific Journal Theoretical & Applied Science. Philadelphia, USA., 2022. Vol - Issue: 105-01. -Б. 175-179. (Scientific Journal Impact Factor; № 23; IF = 7.184).

7. Очилов Н.Н. Ҳимояланган файллар тизимида файл блоклари ва Inod лар алгоритмларини яратиш // Муҳаммад ал-Хоразмий авлодлари. Ташкент ш., 2022. №2(20). -Б.105-110 (05.00.00; № 10).

8. Очилов Н.Н. Операцион тизимларни ҳимоялашда шифрлашнинг ўзига хос хусусиятлари // ТАТУ хабарлари. г. Ташкент, 2020. №4(56).-Б.149-154 (05.00.00; № 31).

9. Очилов Н.Н. Analysis of methods and algorithms of encryption on the basis of local standards // Technical Science and Innovation. г. Ташкент, 2021. №3.-Б.152-159. (05.00.00; № 16).

10. Очилов Н.Н. Ҳимояланган файллар тизимида катологлар ва журналлар алгоритмлари // Ахборот коммуникациялар: Тармоқлар-Технологиялар-Ечимлар. Ташкент ш., 2022. №2(62).-Б.60-66 (05.00.00; № 2).

11. Очилов Н.Н. Очиқ кодли операцион тизимларида ҳимояланган файл тизимлари таҳлили // Ахбороткоммуникациялар: Тармоқлар-Технологиялар-Ечимлар. Ташкент ш., 2022. №3(63).-Б.47-55 (05.00.00; № 2).

12. Очилов Н.Н. Очиқ кодли операцион тизимларида ҳимояланган файл тизимлари таҳлили // Фарғона политехника институти Илмий-техника журнали. Фарғона ш., 2022, Том 26. №5.-Б.124-130 (05.00.00; № 20).

13. Очилов Н.Н. Development of encryption and archiving algorithms according to local standards in open operating systems // Technical Science and Innovation. г. Ташкент, 2023. №1.-Б.145-153 (05.00.00; № 16).

14. Очилов Н.Н. Очиқ кодли операцион тизимларида шифрлаш алгоритмлари таҳлили // Ўзбекистон Республикаси Фанлар академиясининг маърузалари. Тошкент ш., 2022. №6.-Б.99-102 (05.00.00; № 9).

15. Очилов Н.Н. Analysis of Protected File Systems in Operation Systems with Open Source // International Journal of Advanced Research in Science, Engineering and Technology. Индия, 2022. Vol - Issue: 9-1. –Б. 18871- 18878. (Осиё мамлакатлари нашрлари. 05.00.00; № 8).

II bo‘lim (II часть; II part)

16. Очилов Н.Н. Обеспечение защиты данных в операционной системе путем шифрования и архивирования // Научный форум: Технические и физико-математические науки: сборник статей по материалам LVII международной научно-практической конференции – № 7(57). – 2022, октябрь, Россия, Москва. -С.4-10

17. Очилов Н.Н. Algorithms of encryption on the basis of local standards // X Международная научно-практическая конференция “Информационные технологии. Проблемы и решения.” 24-27 мая 2022 года, Россия, Республики Башкортостан, Уфа. № 2(19). -С.100-107

18. Очилов Н.Н. Проблемы обеспечения эффективности алгоритмов шифрования в операционных системах с открытым кодом // Proceedings of the XXXVIII International Multidisciplinary Conference «Recent Scientific Investigation». Primedia E-launch LLC. Shawnee, USA. 2022. -С.64-70

19.Очилов Н.Н. Ochiq kodli operatsion tizimlarda GOST 28147-89 yordamida shifrlash va arxivlashni tashkil etish // “Axborot texnologiyalari, tarmoqlar va telekommunikatsiyalar” xalqaro ilmiy-amaliy anjumani. Urganch, 29-30 aprel, 2022 – yil. - Б.561-566

20. Очилов Н.Н. GOST 28147-89 shifrlash standartining statistik tahlili // “Axborot texnologiyalari, tarmoqlar va telekommunikatsiyalar” xalqaro ilmiy-amaliy anjumani. Urganch, 29-30 aprel, 2022 – yil. -Б.566-571

21. Очилов Н.Н. Очиқ кодли операцион тизимларда шифрлаш ва архивлашни ташкил этиш // Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot kommunikatsiya texnologiyalarining ahamiyati. Respublika ilmiy-texnik anjumani Toshkent, 10-11-mart, 2022 – yil.-Б.307-310

22. Очилов Н.Н. ГОСТ 28147-89 стандарти асосида шифрлаш алгоритмини жадвал ёрдамида тасодифий қидириш усули // Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot kommunikatsiya texnologiyalarining ahamiyati. Respublika ilmiy-texnik anjumani. Toshkent, 10-11-mart, 2022 – yil. - Б.310-313.

23. Очилов Н.Н. Инициализация жараёнида тизим файлларини шифрлаш ва расшифрлашни ташкил этиш // Raqamli transformatsiya jarayoniga axborot texnologiyalarini joriy etishda ma’lumotlarni himoyalash muammolari va yechimlari. Respublika ilmiy-texnik anjumani. Qarshi, 13-may, 2022 – yil. - Б.192-198.

24. Очилов Н.Н. Очиқ кодли операцион тизимнинг файл тизими учун шифрлашнинг график дастурий таъминоти // Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги интелектуал мулк агентлиги. Электрон ҳисоблаш машиналари учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисида 2022 йил 8 январдаги № DGU 14328- гувоҳномаси.

25. Очилов Н.Н. Ташқи қурилмаларни Linux операцион тизимида рўйхатга олиш дастури // Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги интелектуал мулк агентлиги. Электрон ҳисоблаш машиналари учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисида 2022 йил 8 январдаги № DGU 14327- гувоҳномаси.

26. Очилов Н.Н. Очиқ кодли операцион тизимларида ҳимояланган файллар тизимини ташкиллаштириш // Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги интелектуал мулк агентлиги. Электрон ҳисоблаш машиналари учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисида 2022 йил 8 январдаги № DGU 14326- гувоҳномаси.

Avtoreferat “Muhammad al-Xorazmiy avlodlari” ilmiy jurnali tahririyatida tahrirdan o‘tkazildi va o‘zbek, rus va ingliz tillaridagi matnlarini mosligi tekshirildi.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 3,75. Adadi 100 dona. Buyurtma № 48/23.

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