ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўл ёзма ҳуқуқида

УДК 004.056

ҚУРБОНОВ ХУРШИД АБДИРАУПОВИЧ

Ахборотни криптографик ҳимоялашнинг аппарат-дастурий воситалари тадқиқи

5А330301 – Криптография ва криптоанализ

Магистр академик даражасини олиш учун ёзилган

диссертация

Илмий раҳбар:

Асадов О.

Тошкент – 2013

МУНДАРИЖА

КИРИШ

Диссертация мавзусининг асосланиши ва унинг долзарблиги. “XXI аср – ахборот технологиялари асри” - деб бежизга айтмаганлар Президентимиз И. А.Каримов. Бу аср остида одамзот тасаввур қила олмаган сунъий интеллект роботлари, технологиялар ва бошқа техник қурулмалар яратилишига ҳеч ким шубҳа қилмаса керак. Ахборот технологияларни ривожланиши ҳар бир мамлакат учун иш унумдорлигини ошиши, сифати ва энг асосийси иш самарадорлиги юқори даражада бўлишини таъминлаб беради. Ўзбекистон Республикаси мустақиллик йиллари ахборотлаштириш соҳасида инқилобий ўзгаришлар даврини бошдан кечирмоқда. Замонавий ахборот-коммуникация технологиялари қулайликлар яратиш билан бир қаторда янги муаммоларни ҳам ўртага қўймоқда.

Мустақиллик йиллари мамлакатимизда ахборот телекоммуникация технологияларининг жадал суръатлар билан ривожланиб бориши глобал ахборот жамиятида Ўзбекистон Республикаси ҳам муносиб ўрин эгаллашига катта таъсир кўрсатди.

Ҳозирги кунда ахборот базаларида сақланаётган ва телекоммуникация тизимларида айланаётган ахборот хавфсизлигига таҳдид кескин ошиб бормоқда. Натижада ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди.

Ҳозирги кунга қадар ахборот хавфсизлигини таъминлашда енг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Республикамизда бу йўналиш жадал суръатлар билан ривожланмоқда. Янгидан янги криптографик тизимлар, алгоритмлар, стандартлар ишлаб чиқилмоқда ва турли соҳаларга тадбиқ етилмоқда.

Ўзбекистон Республикасида криптография соҳасида илмий тадқиқотлар бошланганига ҳали кўп (10 йил ҳам) бўлгани йўқ.

Республикада Ўзбекистон алоқа ва ахборотлаштириш агентлигининг Фан-техника ва маркетинг тадқиқотлари маркази олимлари биринчилардан бўлиб, криптография йўналиши бўйича илмий тадқиқотларни бошлаб юбордилар.

1974-йилда ўзбек олими Ўзбекистонда хизмат кўрсатган фан арбоби, профессор Хасанов Пўлат Фаттохович томонидан таклиф етилган диаматрицалар алгебрасини марказимиз директор ўринбосари Хасанов Хислат Пўлатович томонидан криптография масалаларини ечиш учун такомиллаштирилиб топилган параметрли алгебра ишлаб чиқилди. Бунинг натижасида Фан-техника ва маркетинг тадқиқотлари марказининг бош илмий ходими Хасанов П. Ф. раҳбарлигида 2002-йилда криптография бўйича биринчи патентга талабнома берилди. Бу патент 2006-йилда Ўзбекистон Республикаси давлат патент идораси томонидан рўйхатга олинди ва “Рақамли имзони шакллантириш ва аутентификация усули” ихтироси учун 03070-сонли патент берилди.

03070-сонли “Рақамли имзони шакллантириш ва аутентификация усули” патенти ғоялари Фан-техника ва маркетинг тадқиқотлари маркази ходимлари томонидан ишлаб чиқилган Ўзбекистон Республикасининг криптография соҳасидаги дастлабки давлат стандартларига асос бўлди. O`z DSt 1092:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси, Електрон рақамли имзони шакллантириш ва текшириш жараёнлари”, O`z DSt 1105:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми”, O`z DSt 1106:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функсияси” шулар жумласидандир. Криптография йўналишини ривожлантиришга давлатимиз томонидан ҳам катта аҳамият берилмоқда. Бунга кейинги йилларда қабул қилинган бир нечта қонун ва меъёрий ҳужжатлар, жумладан, “Электрон рақамли имзо”, “Электрон ҳужжат айланиши” тўғрисидаги қонунлар, Президентимизнинг 2007-йил 3-апрелда қабул қилган “Ўзбекистон Республикасида ахборотнинг

криптографик ҳимоясини ташкил етиш чора-тадбирлари” тўғрисидаги қарори мисол бўлиши мумкин.

03070-сонли “Рақамли имзони шакллантириш ва аутентификация усули” патенти ғоялари Ўзбекистон Республикасининг қонун ва қарорларини амалга татбиқ етишда муҳим аҳамият касб етмоқда. Сўнгги йилларда миллий стандартларга асосланиб e-HUJJAT - електрон ҳужжат алмашиш тизими, e-ХАТ электрон хат алмашиш тизими, ҳимояланган файл “HIMFAYL” тизими ва масофавий солиқ ҳисоботи топшириш тизими учун криптопровайдерлар ишлаб чиқилди. Ҳозирги кунда кўпгина корхоналарда, жумладан - Ўзбекистон алоқа, ахборотлаштириш ва телекоммуникация давлат қўмитаси, Давлат солиқ қўмитаси, Ташқи ишлар вазирлиги, Давлат алоқа инспексияси, Фан-техника ва маркетинг тадқиқотлари маркази, Ўзимпексалоқа корхонаси, Ўзбектелеком АК ва бошқаларда миллий тизимлардан фойдаланилмоқда.

Ўзбекистон Республикасининг миллий криптографик алгоритмларини яратиш, уларни такомиллаштириш ва ахборотни криптографик муҳофазалашнинг миллий дастурий ва аппарат-дастурий воситаларини ишлаб чиқиш Ўзбекистон Республикаси Президентининг 2007 йил 3-апрелдаги “Ўзбекистон Республикасида ахборотнинг криптографик муҳофазасини ташкил етишга оид чора-тадбирлар тўғрисидаги” 614-сонли қарорида биринчи галдаги вазифа қилиб қўйилганлигини ҳисобга олсак, мазкур ихтиро бу қарорнинг бажарилишини таъминлашда муҳим аҳамиятга эгадир.

Ҳозирги замон криптографиясида қўлланилувчи воситалар аппарат, дастурий ва аппарат-дастурий воситаларга бўлинади. Дастурий воситалар нисбатан арзон бўлсада, ишончлилик даражаси паст. Аппарат воситалар ишончли бўлибгина қолмасдан нархи ҳам қиммматдир. Шунинг учун ҳозирда буларнинг комплекс бирикмаси фойдаланиляпти. Аппарат-

дастурий воситалар ахборотни химоялашда муҳим ахамиятга эга, сабаби уни янгилаш осон, нархи ҳам аппарат воситаларга қараганда арзонроқ.

Илмий тадқиқот ишининг объекти ва предметининг белгиланиши. Тадқиқотнинг объекти ахборотни ҳимоялашнинг асосий воситаларидан бири бўлмиш криптографик ҳимоя воситалардир.

Криптобардошли апарат-дастурий воситаларни ишлаб чиқиш усуллари, криптотизимни бардошлилигини ошириш методлари тадқиқотнинг предмети ҳисобланади.

Илмий тадқиқот ишининг мақсади ва вазифалари. Ушбу магистирлик диссертациясида олиб борилган илмий тадқиқот ишининг мақсади мавжуд апарат-воситаларни ўрганиб чиқиб, шулар асосида янги криптобардошли ҳимоя воситасини ишлаб чиқиш.

Тадқиқот мақсадини амалга ошириш учун диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

- Апарат-дастурий воситаларга қўйилган умумий талабларни аниқлаш;
- Мавжуд апарат-дастурий воситаларни ишлаш принсипини ўрганиш ва у ҳақда маълумотга эга бўлиш;
- Мавжуд криптографик аппарат-дастурий воситаларини қуриш усулларини классификацияси ва қиёсий таҳлили;
- Криптографик аппарат-дастурий воситаларнинг криптобардошлигини ошириш принципларини ишлаб чиқиш;
- Юқори криптобардошли криптографик дастурий модулни ишлаб чиқиш.

Илмий тадқиқотнинг асосий масалалари ва фаразлари. Ахборот-коммуникацион тизимларида ахборот хавфсизлигини таъминлашда фойдаланилаётган криптографик аппарат-дастурий ҳимоя воситаларини тадқиқ этиш, уларни криптобардошлигини баҳолаш ва ушбу талаблар асосида криптографик дастурий ҳимоя воситаси алгоритмини яратиш масалалари ечимига эришиш.

Мавзу бўйича қисқача адабиётлар таҳлили. Ахборот-коммуникацион тизимларида, ахборотни ҳимоялаш тизимларида замонавий компьютерларнинг фойдаланилиши, электрон маълумот айланишида ахборот муҳофазасини криптографик усулларини кенг қўлланилишига сабаб бўлмоқда.

Криптографик аппарат-дастурий воситалар яратиш ва тадқиқ қилиш соҳасидаги манбалар сифатида Шнайер Б., Варлатая С.К., Шаханова М.В., Жданов О.Н., Золотарев В.В., Шеннон К.Е., Петров А.А. томонидан олиб борилган тадқиқот ишларини келтириш мумкин. Ушбу олиб борилган тадқиқот ишлари шуни кўрсатдики аппарат-дастурий воситаларнинг криптобардошлиги унда фойдаланилган криптографик алгоритмга ва алгоритмнинг амалга ошириш усулига боғлиқ бўлар экан. Шифрлаш алгоритлари асосида аппарат ва аппарат-дастурий воситаларни яратиш устида дунёнинг кўплаб етакчи илмий тадқиқот институтлари компаниялари (“Crypto AG” Швейцария, “Анкад”, “КриптоПро”, “Аладдин” Россия, “Global Crypto”, “RSA Data Security” АҚШ ва бошқа.) томонидан инжинерлик тадқиқот ишлари олиб борилмоқда.

Илмий тадқиқот ишида қўлланилган услубларнинг қисқача тавсифи. Ушбу илмий тадқиқот ишида ахборотни криптографик ҳимоялаш тизимлари назарияси, эҳтимоллар назарияси, сонлар назарияси, математик мантиқ ва комбинаторика методларидан фойдаланилган. Булардан ташқари солиштириш, тестлаш ва қиёсий таҳлил усулларидан фойдаланилди.

Тадқиқот натижаларининг назарий ва амалий аҳамияти. Мавжуд криптографик аппарат-дастурий воситаларни таҳлил этиш, уларни қуриш усулларини ўрганиш, криптобардошлигини баҳолаш ва ҳозирда ушбу воситаларда фойдаланилган криптографик алгоритмларни таҳлил қилиш ва тадқиқлаш магистрлик диссертациясининг назарий аҳамияти ҳисобланади.

Магистрлик диссертациясининг амалий аҳамияти – яратилган дискдаги маълумот хавфсизлигини таъминловчи дастурий модул алгоритми ва дастурий таъминотни Ўзбекистон шароитида ишлаб чиқарилган ишончли ва тезкор ишловчи аппарат-дастурий криптографик воситаларда, компьютер тизимларида маълумотларни махфийлигини таъминлашда фойдаланиш мумкин.

Илмий тадқиқот ишининг илмий янгилиги. Ушбу тадқиқот ишининг янгилиги мавжуд криптографик воситаларнинг ишлаш прициплари ўрганилиб, криптобардошли методлар орқали янги криптобардошли дастурий модулни ишлаб чиқиш.

Диссертация таркибининг қисқача тавсифи. Ушбу тадқиқот иши қуйидаги: кириш, 3 та бўлим, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат. Ушбу тадқиқот ишида 14 та жадвал, 18 та расмдан иборат. Илмий тадқиқот ишининг умумий ҳажми 81 саҳифани ташкил этади.

I боб. Мавжуд криптографик аппарат-дастурий воситаларининг қиёсий таҳлили

1.1. Криптографик аппарат-дастурий воситаларга қўйиладиган умумий талаблар

Криптография - ахборотни аслидан ўзгартирилган ҳолатга акслантириш услубларини топиш ва такомиллаштириш билан шуғулланади. Дастлабки системалашган криптографик услублар эрамиз бошида, Юлий Цезарнинг иш юритиш ёзишмаларида учрайди. У, бирор маълумотни маҳфий ҳолда бирор кишига етказмоқчи бўлса, алфбонинг биринчи ҳарфини тўртинчи ҳарфи билан, иккинчи ҳарфини бешинчиси билан ва ҳоказо тартибда алмаштириб матнни асл ҳолатидан шифрланган матн ҳолатига ўтказган [6].

Криптографик системалар йўналишидаги изланишлар айниқса биринчи ва иккинчи жаҳон уруши йиллари даврида муҳим аҳамият касб этди ва жадал ривожланди. Урушдан кейинги йилларда, ҳисоблаш техникаларининг яратилиши, уларнинг такомиллашиб, инсоният фаолиятининг барча соҳаларига чуқур ва кенг маънода кириб бориши, криптографик услубларни табиий равишда ривожланиб ва такомиллашиб боришини таъқозо этмоқда.

Криптографик услубларнинг ахборот тизими муҳофазаси масалаларида қўлланилиши, айниқса, ҳозирги кунда фаоллашиб бормоқда. Ҳақиқатан ҳам, бир томондан компьютер тизимларида интернет тармоқларидан фойдаланган ҳолда катта ҳажмдаги давлат ва ҳарбий аҳамиятга эга бўлган, ҳамда, иқтисодий, шаҳсий ва бошқа турдаги ахборотни тез ва сифатли узатиш, қабул қилиш кенгайиб бормоқда. Иккинчи томондан эса бундай ахборотларнинг муҳофаза қилиниши таъминлаш масалалари муҳимлашиб бормоқда.

Ахборотни мухофаза қилиш масалалари билан *криптология* (kryptos-маҳфий, logos- илм) фани шуғулланади. Криптология мақсадлари ўзаро

қарама-қарши иккита йўналишига эга бўлган – *криптография* ва *криптоанализ* [6].

Криптографиянинг очиқ маълумотларни шифрлаш масалаларининг математик услублари билан шуғулланиши тўғрисида юқорида айтиб ўтилди.

Криптоанализ эса шифрлаш услуби (калити ёки алгоритми)ни билмаган ҳолда шифрланган маълумотни асл ҳолатини (мос келувчи очиқ маълумотни) топиш масалаларини ечиш билан шуғулланади.

Ҳозирги замон криптографияси қуйидаги тўртта бўлимни ўз ичига олади:

1. Симметрик криптотизимлар.
2. Очиқ услубга ёки яна бошқача айтганда очиқ калитлар алгоритмига асосланган криптотизимлар.
3. Электрон рақамли имзо криптографик тизимлари.
4. Криптотизимлар учун криптобардошли калитларни ишлаб чиқиш ва улардан фойдаланишни бошқариш.

Криптографик услублардан фойдаланишнинг асосий йўналишлари: маҳфий маълумотларни очиқ алоқа канали бўйича муҳофаза қилиш ҳолда узатиш, уларнинг хақиқийлигини таъминлаш, ахборотларни (электрон хужжатларни, электрон маълумотлар жамғармасини) компьютерлар тизими хотирасида шифрланган ҳолда сақлаш ва шу каби масалаларнинг ечимларини ўз ичига олади.

Такидлаш жоизки, крипография узоқ вақт давомида давлат органлари алоқа тармоқларида алмашинадиган маълумотлар муҳофазасининг таҳминланишида қўлланиб келинди. Компьютер тармоқлари ва электрон ҳужжат алмашинуви технологияларининг ривожланиши молия, банк ишлари, савдо-сотиқ каби соҳаларда қўлланилиши ахборот муҳофазасининг криптографик усулларини умумжамият фаолиятининг турли соҳаларига кенг кириб боришига сабаб бўлди. Ҳақиқатан ҳам, алоқа тармоқларида ахборотни муҳофаза

қилиниши, криптографик усулда таъминлаш умумжамият тараққиётининг ривожланиш босқичлари билан боғлиқ бўлган узоқ тарихий манбаларига эга бўлиб, умуминсоният жамиятига хҳизмат қилмаслиги (яъни криптографик усулларни кенг омма томонидан фойдаланилишининг чекланиши) таажубланарли ҳолат бўлар эди.

Ахборотлар тизими муҳофазасининг замонавий криптографик услубларига қуйидаги умумий талаблар қўйилади [6]:

- шифрланган маълумотни асл нусҳасига эга бўлиш имконияти фақат дешифрлаш калити маълум бўлгандагина мумкин бўлсин;
- фойдаланилган шифрлаш калитини шифрматннинг бирор маълум қисми бўйича ёки унга мос келувчи очиқ қисми бўйича аниқлаш учун, бажарилиши зарур бўлган амаллар сони калитни аниқ топиш учун бажарилиши керак бўлган барча амаллар сонидан кам бўлмаслиги керак, яъни калит танлаб олиниши керак бўлган тўплам элементларининг сонидан кам бўлмаслиги керак;
- шифрлаш алгоритмининг маълумлиги унинг бардошлилигига салбий таъсир кўрсатмаслиги керак;
- калитнинг ҳар қандай даражадаги (озми, кўпми) ўзгариши шифрланган маълумотнинг жиддий ўзгаришига олиб келиши керак;
- шифрлаш алгоритми таркибидаги элементлар ўзгармас бўлиши керак;
- шифрлаш жараёни давомида маълумотларга киритиладиган қўшимча битлар (элементлар) шифрланган матнда (маълумотда) тўла ва ишончли холда қўлланилган бўлиши керак;
- шифрлаш жараёнида қўлланиладиган калитлар орасида содда ва осонлик билан ўрнатиладиган боғлиқликлар бўлмаслиги керак;
- калитлар таркиби тўпламидан олинган ихтиёрий калит ахборотнинг ишончли муҳофазасини таъминлаши керак;

- криптоалгоритм дастурий ҳамда техник жиҳатдан амалий қўлланишга қулай бўлиб, калит узунлигининг ўзгариши шифрлаш алгоритмининг сифатсизлигига олиб келмаслиги керак.

Криптографик ҳимоя тизимлари орқали қуйидаги ишларни амалга ошириш мумкин:

- маълумот сақловчи воситаларда калит маълумотларни ҳосил қилиш ва улардан фойдаланиш;
- сақловчи воситалардаги маълумотларни, малумотлар базаларидаги ёки барча турдаги маълумотларни шифрлаш орқали ҳимоялаш;
- фойдаланувчиларни аутентификация ва идентификациядан ўтказиш;
- маълумотларни ҳақиқийлигини таъминлаш;
- криптобардошли калитларни ишлаб чиқариш ва уларни бошқариш.

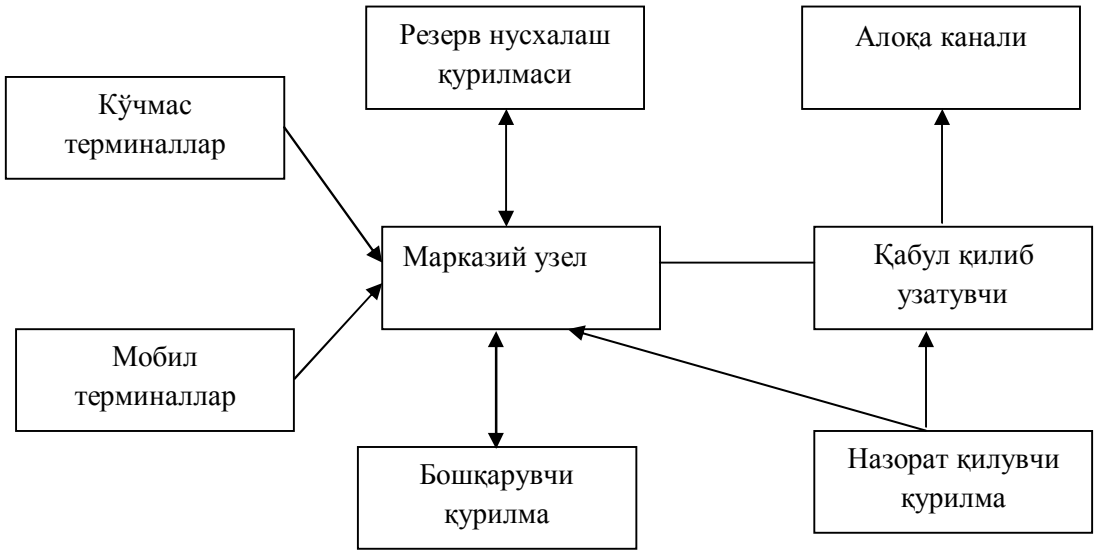
Ахборотларнинг криптографик ҳимоя воситалари (АКҲВ) – аппарат, дастурий ва аппарат-дастурий воситалар кўринишида бўлиши мумкин ва улар ўзида бир ёки бир нечта криптографик усулларни қамраб олган бўлиши мумкин.

Юқорида айтиб ўтилганидек, АКҲВ қуйидаги асосий воситалардан ташкил топган [8]:

- криптографик дастурий воситалар - бир ёки бир нечта криптографик усулларни ўзида мужассам этган, юқори ёки қуйи дастурлаш тилларида ёзилган алоҳида библотекалар ёки белгиланган дастурлар тўплами;
- криптографик аппарат воситалар – криптографик усулларни махсус микросхемалар, процессорлар, махсус блоклар ёки дастурий модулларда амалга оширилган кўриниши бўлиб, автоматик равишда ишлайди;
- криптографик аппарат-дастурий воситалар – криптографик ҳимоя усулларини комплекс, яъни ҳам аппарат ҳам дастурий воситалар орқали амалга оширилади.

Юқорида келтирилган криптографик ҳимоя воситалари орасида принципиал фарқ мавжуд эмас. Улар ягона, яъни криптографик усулларни турлича амалга оширишлари билан бир-биридан фарқ қилади. Аппарат воситаларда барча амаллар махсус микросхема хотирасида амалга оширилса, дастурий воситалар эса ҳисоблаш воситалари хотирасида амалга оширилади.

Криптографик ҳимоя воситалари принципиал фарқ қиласада, ахборот-коммуникацион тизимларида ахборот хавфсизлиги сиёсатига кўра қўлланилади. Умумий ҳолда криптографик ҳимоя воситалари ахборот-текоммуникация тизимларида қуйидаги тарзда фойдаланилади [8]:



1- расм. АКҲВнинг ахборот-телеккомуникация технологияларида қўллашдаги ўрни

Умумий ҳолда АКҲВ ахборот-телекоммуникацион тизимларида қуйидаги режимларда ишлайди [7,8]:

- фойдаланувчиларга оид шифрлаш;
- тўғридан-тўғри шифрлаш;
- оқимли шифрлаш;
- электрон рақамли имзо;
- идентификация ва аутентификация.

Барча хавфсизлик воситалари сингари криптографик ҳимоя воситаларни ҳам яратилиш асосига кўра ва тузилишига кўра учта гуруҳга ажратиш мумкин [7,8]:

- дастурий криптографик воситалар;
- аппарат криптографик воситалар;
- аппарат-дастурий криптографик воситалар.

Ушбу криптографик воситаларда амалларни бажариш тезлиги ва бажариш жараёнида фойдаланилган ресурслар хусусиятлари билан фарқ қилса, асосидаги криптографик тизимлар эса ўзгармайди. Қуйида ушбу воситалар ҳақида маълумотлар берилган.

Аппарат криптографик ҳимоя воситалар. Криптографик аппарат ҳимоя воситалар – махсус блок бўлиб, бу блок малумотларни шифрлаш учун фойдаланиладиган иккилик сановчи қурилмалардан ёки алоҳида қўшимча қурилмалардан ташкил топган.

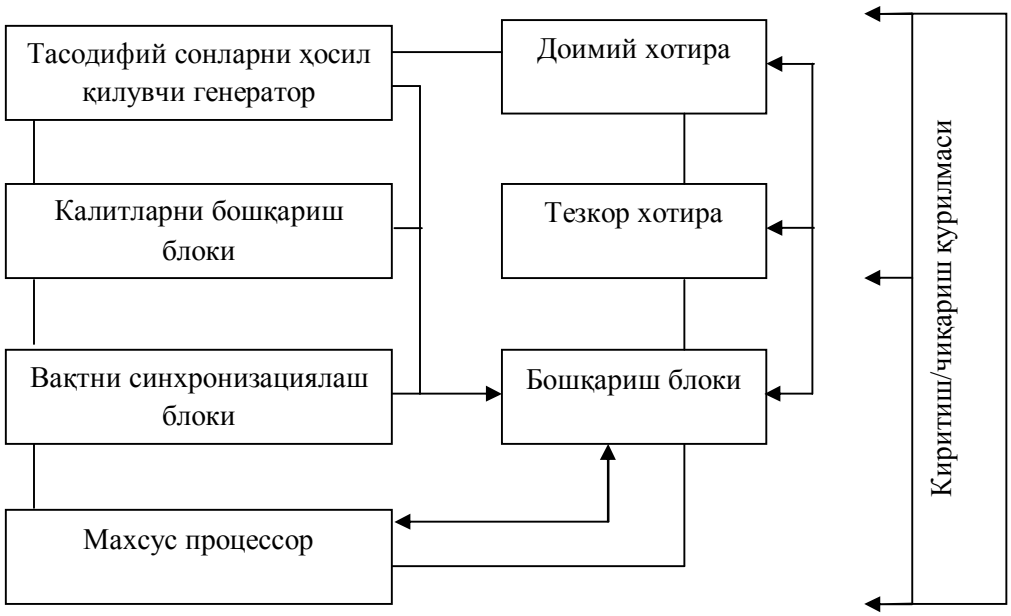
Криптографик аппарат ҳимоя воситалари шунингдек қўшимча ҳимоя функциялардан иборат. Масалан, рухсатсиз фойдаланишлардан ҳимояловчи функцияси.

Бундан ташқари криптографик аппарат воситалар дастурий воситаларга талаб этилмайдиган қуйидаги қўшимча блоклардан иборат[8]:

- криптографик калитларни бошқариш блоки;
- тасодифий сонларни ҳосил қилувчи генератор;
- хотира, доимий ва тезкор хотира;
- вақтни синхронизациялаш блоки;
- хэш қийматни сақловчи ва назорат қилувчи блок.

Шунингдек, аппарат-криптографик ҳимоя воситалари қўшимча махсус шифрловчи процессорлардан, идентификация, аутентификация ва авторизацияни текширувчи блоклардан иборат бўлиши мумкин. Ҳаттоки, аппарат воситалар махсус ҳисобловчи компютер ҳам бўлиши мумкин. Бунда у марказий процессор билан махсус шина (тизим шинаси) орқали боғланади.

Криптографик аппарат ҳимоя воситалар одатда компьютерга уланадиган плата кўринишида бўлади ва у қуйидаги блоклардан иборат бўлади [8]:



2 - расм. Криптографик аппарат ҳимоя воситаларининг асосий схемаси

Бошқариш блоки криптографик аппарат химоя воситасиниг турли хил блокларини бир-бирига боғлаш вазифасини бажаради, қурилмаларни ташқи оқимни бир-бирига боғлайди, малумотларни бошқаради ва тизим шинаси орқали узатилишини таъминлайди.

Апппаратнинг хотираси икки блокдан ташкил топган [7,8]:

- тезкор хотира - криптогрпфик ҳимоя воситасининг дастурий таъминотини, дастур ташкил этувчиларини, ўзгарувчи параметрларни ўзида сақлайди;
- доимий хотира - махсус буйруқлар, ҳимояни амалга оширувчи функциялар ва аппрат АКҲВ дастурий таъминоти юкланишлари йиғиндиси.

Булардан ташқари қолган манбалар қўшимча икки хотира блокида сақланади [8]:

- журнал учун хотира;
- калитларни сақлаш учун хотира.

Тасодифий сонлар генератори аппарат АКҲВ учун тасодифий сонлар кетма-кетлигини ҳосил қилиб беради. Тасодифий сонлар генераторининг аппарат кўригишида физик жараёнлар орқали тасодифий кетма-кетликлар олинади.

Вақтни синхрогизациялаш блоки аппрат АКҲВ да амаллар бажарилишини назорат қилади, малумот узатилишини вақт синхронизациясида амалга оширади.

Киритиш/чиқариш блоки ташқаридан кирувчи сигналнн ички сигналга айлантириб беради. Аппарат АКҲВ киритиш/чиқариш блоки қуйидаги қурилмалар билан боғлиқ муҳим боғланишларни амалга оширади:

- компьютернинг тизимли шинаси ёки маълумотларни узатувчи линиядарда қабул қилувчи/узутувчи қурилма, бу тўғридан-тўғри шифрлаш учун фойдаланилади;
- калит маълумотларни сақловчи қурилма, улар идентификация/аутентификация жараёнларига ёрдам беради, шунингдек аппрат АКҲВ вазифаларини назорат қилишга ёрдам беради;
- қаттиқ диск бошқарувчиси ва маълумотларни захирада сақлаш қурилмаси, булар маълумотларни хавфсизлигини таъминлашда ва захирада сақлашда ишлатилади.

Шундай қилиб, аппарат криптографик ҳимоя воситалар ўзида мураккаб бўлган кўп функцияларни қамраб олган. Криптографик аппарат воситалар қуйидаги афзалликларга эга:

- шифрлаш алгоритмини ўзгартириб бўлмаслик;
- криптографик калитларни ҳосил қилишда тасодифий сонлар генераторидан фойдаланишлик;

- шахсий идентификаторлар (смарт-карта ёки Touch Memory)даги калитлар билан шифрлаш тўғридан-тўғри аппаратнинг махсус процессорида амалга оширилиши;
- калитларни компьютернинг хотирасида эмас балки шифрловчи процессор хотирасида сақланилиши;
- тизим юклангунга қадар фойдаланувчиларни идентификация ва аутентификациядан ўтказиш имконяти;
- маълумотларни шифрлаш юқори тезликда амалга оширилиши.

Криптографик дастурий ҳимоя воситалари (КДҲВ). Криптографик дастурий воситаларда криптографик алгоритмлар юқори ёки қуйи даражадаги дастурлаш тилларида амалга оширилади. Дастурий воситалардаги амаллар одатда компьютер хотирасида бажарилади.

Дастурий воситани криптобардошлилиги криптоалгоритмни қанчалик аниқлик билан амалга оширилганига боғлиқ. Криптографик дастурий воситаларга аппарат воситалар каби кенг қамровли шартлар қўйилмасада, қуйидаги муҳим ўзига хос хусусиятларга ега бўлиши шарт [8]:

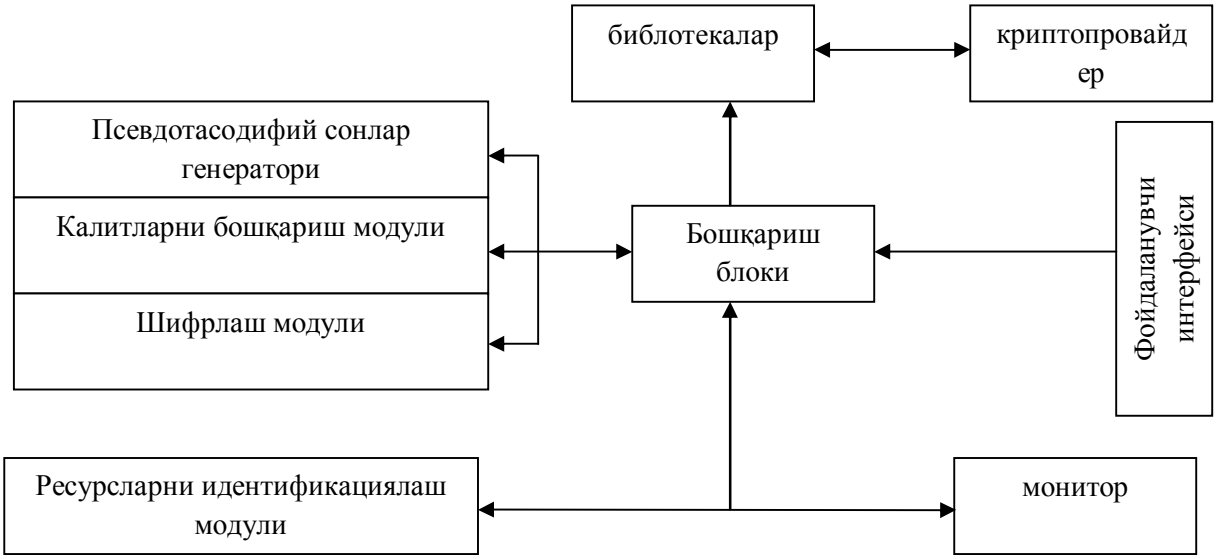
- вазифаларни қўшимча назорат қилиш имконяти мавжудлиги, чунки кўп ҳолларда дастуриф воситалар аппарат воситаларга қараганда анча суст ишлаши кузатилади;
- ёпиқ матнларда хатоларни назорат қилиш имконяти мавжудлиги;
- калитларни ишончли сақланилишини таъминлаш имконяти;
- мавжуд дастурий воситани ўзгартириш имконяти ва қўшимчалар қўшиш имконяти мавжудлиги;

Криптографик дастурий воситалар қуйидаги вазифаларни бажаради:

- фойдаланувчиларни идентификация/аутентификациядан ўтказиш;
- операцион тизим ва дастурий воситаларни криптографик ҳимоясини таъминлашда;
- псевдотасодифий кетма-кетликларни ҳосил қилишда;
- дискдаги маълумотларни шифрлашда;

- маълумотларни аниқ шифрлаш;
- маълумотларни фойдаланучили шифрлаш;
- калитларни ташкил этиш, текшириш, электрон рақамли имзо ва дастурий кодларни кўчиришдан ҳимоялаш учун;
- калит узатилишида хавфсизликни таъминлашда.

Криптографик дастурий воситаларнинг тузулиши қуйидаги кўринишга эга [8]:



3 - расм. Криптографик дастурий воситаларнинг умумий схемаси

Бошқариш блоки дастурий воситанинг алоҳида қисмларини бирлаштиради, ташқаридан кирувчи буйруқларни ичми модул билан боғлайди.

Калитларни бошқариш модули калит маълумотларни ҳосил қилишда, фойдаланувчини идентификация/аутентификациядан ўтказишда фойдаланилади.

Псевдотасодифий кетма-кетлик генератори тасодифий бўлган битлар кетма-кетлигини ҳосил қилишда фойдаланилади.

Криптографик дастурий модул библотекалари амалий вазифаларни ҳал этади ва дастурий воситани созлашда фойдаланилади.

Фойдаланувчи интерфейси фойдаланувчига дастурий муҳитдан фойдаланишга қулайлик туғдиради ва ички модулга маълумот критишда ва натижани фойдаланувчига кўрсатиш учун фойдаланилади.

Шундай қилиб, дастурий криптографик ҳимоя воситалари қуйидаги ўзига хос хусусиятларга эга:

- ушбу дастурий криптографик ҳимоя воситалари бошқа қурилмаларда сақланган бўлиши мумкин;
- блокли шифрлаш алгоритмларида блок ўлчами файл сегменти ўлчамини ошириши мумкин, натижада эса файл ўлчами ортиши мумкин;
- дастурий криптографик ҳимоя воситаларининг шифрлаш тезлиги аппарат воситалар тезлигига қараганда паст бўлиши мумкин, чунки барча ҳисоблашлар марказий процессорда амалга оширилади.

Қуйидаги жадвалда дастурий криптографик ҳимоя воситаларига мисоллар келтирилган [23].

1-жадвал

ДКҲВ мисоллар

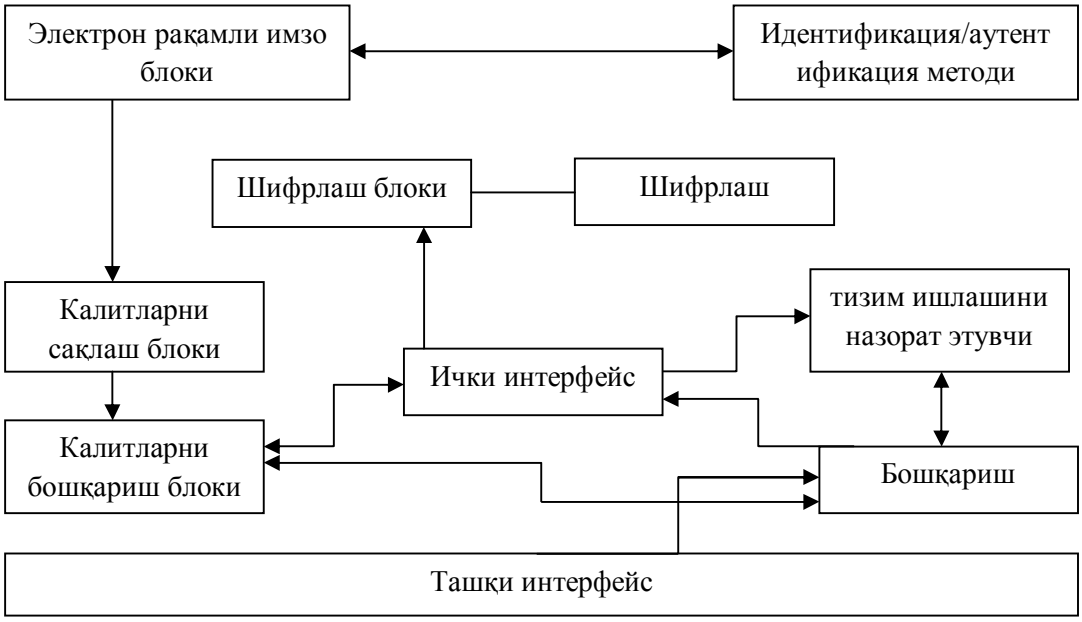
КДҲВ гуруҳлари	**Мисоллар**
Фойдаланувчиларни аутентификация ва идентифиядан ўтказиш	ОТ дастурий воситалари
Дискдаги маълумотларни шифрлаш тизимлари	ОТнинг дастурий воситалари, PGP, Secret Disk
Тармоқда маълумотларни шифрлаш тизимлари	ЗАСТАВА комплекси (VPN + дастурий КҲВ)
Электрон ҳужжатларни ҳақиқийлигини аниқлаш тизимлари	PGP
Калитларни бошқариш тизимлари	ЗАСТАВА сервер сертификатлари

Юқоридаги фикрлардан келиб чиққан ҳолда шуни айтиш мумкинки, дастурий криптографик ҳимоя воситалари криптографик ҳимоялашда амалий вазифаларни бажаради. Криптографик дастурий воситалар

ҳимоянинг тўлиқлигига кафолат бермасада, иқтисодий томондан фойдали бўлиб, ихтиёрий қийинликка эга бўлган тизимларда қўлланилиш имконини беради.

Криптографик аппарат-дастурий ҳимоя воситалари (КАДҲВ). Аппарат-дастурий ҳимоя воситалар аппарат ва дастурий ташкил этувчилар йиғиндисидан ташкил топ ган бўлиб, улар қуйидаги таянч модуллардан ташкил топган [8]:

- шифрлаш блоки(асимметрик шифрлаш тизимлари дастурий модуллар, симметрик шифрлашла аппарат модуллар учун), дастурий, аппарат кўринишида ёки уларнинг комбинацияси асосида амалга оширилади;
- электрон рақамли имзо блоки;
- калитларни бошқариш блоки;
- идентификация/аутентификация модули;
- ташқи интерфейсни бошқариш модули;
- тизим ишлашини назорат этувчи модул;



4- расм. Критографик аппарат-дастурий воситларнинг таянч схемаси

Шуни айтиб ўтиш керакка аппарат-дастурий криптографик воситаларни қуришда намунавий таянч схема мавжуд емас, чунки ушбу тизимни қуришда ва самарадорлигини оширишда доим янги усуллар қидирилади ва тизим схемаси ўзгариб туради. Қуйида умумий ҳолда аппарат-дастурий криптографик модулнинг таянч схемаси келтирилган [8].

2-жадвал

КАДҲВ га мисоллар

КАДҲВ гуруҳлари	**Мисоллар**
Фойдаланувчиларни аутентификация ва идентифиядан ўтказиш	АККОРД
Дискдаги маълумотларни шифрлаш тизимлари	Crypton Soft, ГРЯДА
Тармоқда маълумотларни шифрлаш тизимлари	Crypton ArcMail (КРИПТОН платасида)
Электрон ҳужжатларни ҳақиқийлигини аниқлаш тизимлари	Crypton Sign, Crypton ArcMail (КРИПТОН платасида)
Калитларни бошқариш тизимлари	Crypton Tools(КРИПТОН платасида)

Ушбу криптографик ҳимоя воситалари хавфсизлик сиёсати ва ҳимояланадиган тизимга қўйилган талаблардан келиб чиққан танланади. Қуйидаги жадвалга ушбу криптографик ҳимоя воситаларининг умумий хусусиятлари берилган.

3-жадвал

КҲВ умумий хусусиятлари

Номи/ хусусияти	**Дастурий КҲВ**	**Аппарат КҲВ**	**Аппарат-дастурий КҲВ**
Амал бажариш тезлиги	секин	тезкор	тезкор
Қўлланиш соҳаси	ЭРИ ва ассиметрик шифрлашда	Симметрик шифрлашда	Симметрик ва ассиметрик шифрлашда, ЭРИ
Амалларни бажарилиш манбаси	ШК марказий процессори	Махсус микропроцессор (КҲВ хотираси)	Махсус микропроцессор (КҲВ хотираси)
Воситани янгилаш имконияти	Мавжуд, осон	Мавжуд емас	Мавжуд, мураккаб
Бардошлилиги	Паст	Юқори	Юқори
Нархи	Арзон	Қиммат	Қиммат

1.2. Криптографик аппарат-дастурий воситалар

Криптографик аппарат-дастурий воситаларнинг ахборот хавфсизлигида муҳим аҳамиятга эга еканлиги ҳақида юқоридаги бўлимларда айтиб ўтилди. Шуни ҳисобга олган ҳолда ҳозирда кўплаб давлат аҳамиятига эга бўлган, шунингдек тижорат ва корхоналар хавфсизлигини таъминлашда криптографик ҳимоя воситалари қўлланиляпти. Ҳозирда кўплаб ҳимоя воситаларини ишлаб чиқарувчи ташкилотлар томонидан айнан криптографик ҳимоя воситаларини ишлаб чиқаришда катта аҳамият берилмоқда. Ушбу бобда криптографик ҳимоя воситаларини ишлаб чиқарувчи этакчи ташкилотлар ишлаб чиқарган воситалар таҳлили келтирилган.

АНКАД 20 йилдан бери ахборот хавфсизлиги соҳасида ишлаб келадиган машҳур фирмалардан биридир. Ушбу фирма кенг кўламдаги хавфсизлик воситаларини(ахборотнинг криптографик ҳимоя воситаларини, электрон рақамли имзо қурилмаларини, рухсатсиз

фойдаланишни олдини олиш учун мўлжалланган воситаларни, комьпютер ресурсларига рухсатни чеклаш ва ҳ.к.) ишлаб чиқаради.

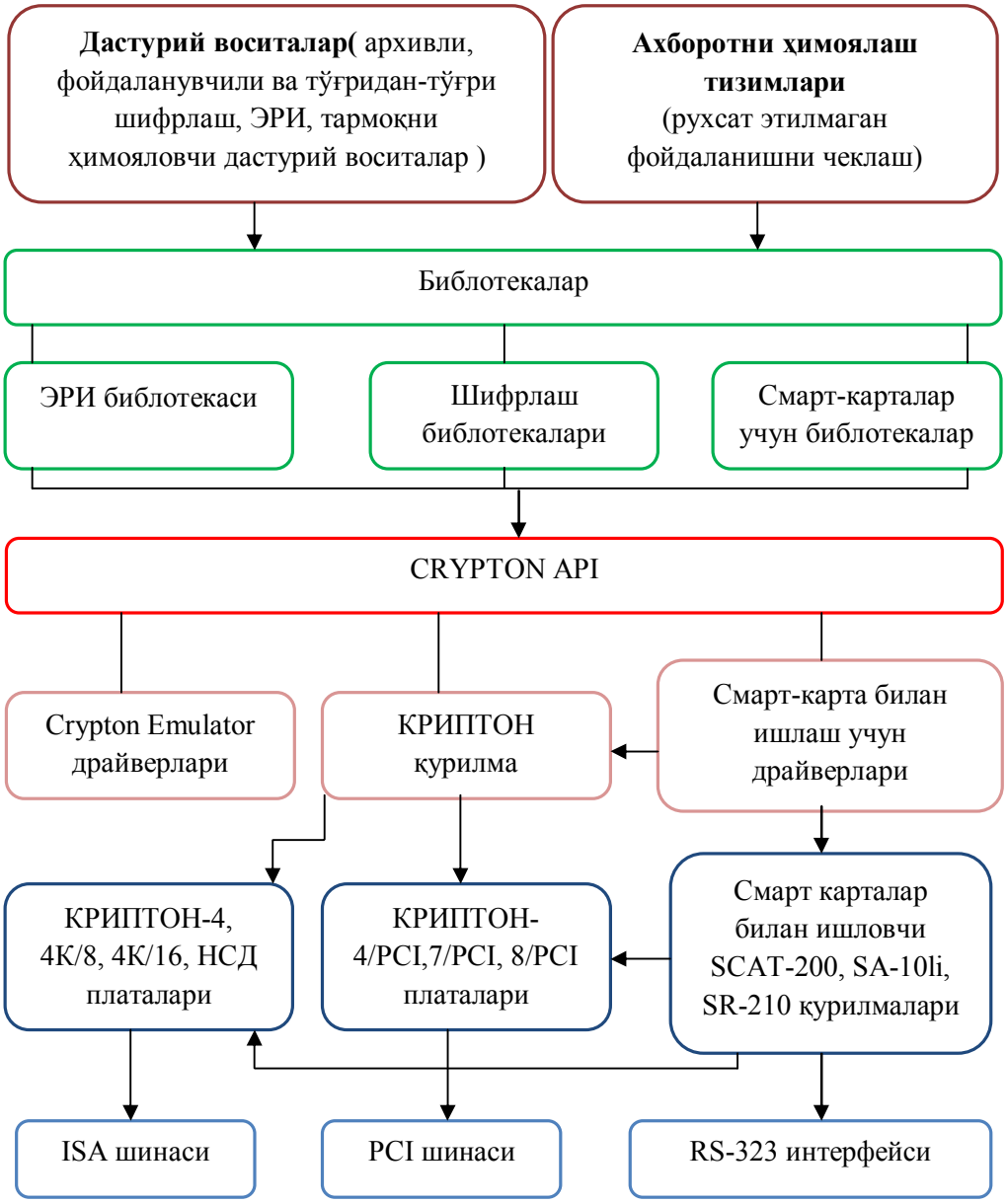
АНКАД фирмасининг ҳимоя воситалари орқали қуйидаги турдаги ахборотларни ҳимоялаш мумкин [25]:

- давлат сирларини ҳимоялашда;
- шахсий маълумотларни ҳимоялашда;
- конфиденциал маълумотларни ҳимоялашда;
- тижоратга оид маълумотларни ҳимоялашда.

Ушбу фирма КРИПТОН/Crypton савдо белгиси билан ўз маҳсулотларини ишлаб чиқаради. АНКАД фирмаси қуйидаги соҳалар бўйича ўз ҳимоя воситаларини ишлаб чиқаради [23,25]:

- ҳимоянинг криптографик аппарат ва дастурий воситаларини;
- электрон рақамли имзо;
- рухсатни чеклаш ва назорат қилиш;
- тармоқда маълумотларни узутишда хавфсизликни таъминлаш;
- симсиз алоқа каналларида хавфсизликни таъминлаш;
- талабга кўра хавфсизлик воситаларини ишлаб чиқиш.

Дискни шифрловчи қурилмалар. М-544(“КРИПТОН-IDE”, М-590 модел), М-591(“КРИПТОН-ПШФД/USB”), М-575(“КРИПТОН-ПШД/SATA”) ва М-623(“КРИПТОН-ИНТЕГРАЛ”) крпитографик аппарат-дастурий воситалари компьютер дискидаги ахборотларни сақлаш ва рухсатсиз киришларни олдини олиш учун ишлатилади. Бу модуллар шифрловчи криптографик аппарат восита “КРИПТОН” ва рухсатсиз киришларни олдини олишга мўлжалланган аппарат-дастурий восита “КРИПТОН-ЗАМОК” модулларини ўзида бирлаштирган [25].

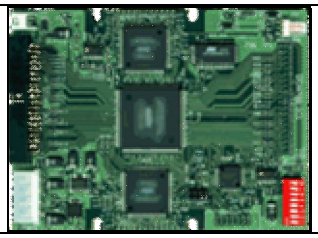
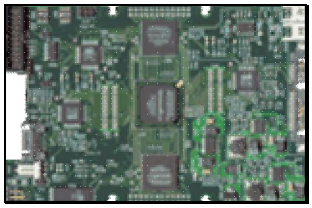
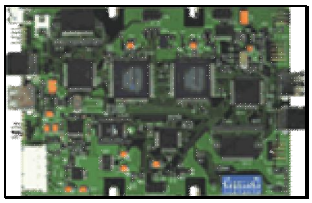


5 - расм. АНКАД фирмаси криптографик фимоя воситаларининг тузулиши

4-жадвал

Диск шифрловчи криптографик аппарат-дастурий воситалар

М-590 («КРИПТОН-ПШД/IDE»)	
Асосий хусусятлари Интерфейс: IDE ва ANSIx3.298-1997 ларга мўлжалланган ATA/ATAPI-6; Ҳимоя усули: блокли шифрлаш; Қувват манбаи: Компьютер қувват манбаи	

орқали; Шифрлаш алгоритми: ГОСТ-28147-89; Шифрлаш тезлиги: 70 Мбит/с; Калит маълумотларни сақловчи: Touch Memory	
М-575 («КРИПТОН-ПШД/SATA»)	
Асосий хусусятлари Интерфейс: Serial ATA 1/0; Ҳимоя усули: блокли шифрлаш; Қувват манбаи: Компьютер қувват манбаи орқали; Шифрлаш алгоритми: ГОСТ-28147-89; Шифрлаш тезлиги: 240 Мбит/с; Калит маълумотларни сақловчи: Touch Memory	
М-591 («КРИПТОН-ПШФД/USB»)	
Асосий хусусятлари Интерфейс USB: Universal Serial Bus Rev. 2.0; Маълумотларни жўнатиш тезлиги: 1.5 Мбита/с и 12 Мбит/с; Қувват манбаи: Компьютер қувват манбаи орқали +5В, +12В; Истемол қилиш қуввати: 5Ваттдан кам Шифрлаш алгоритми: ГОСТ-28147-89; Шифрлаш тезлиги: 48 Мбит/с; Калит маълумотларни сақловчи: Touch Memory	
М-623 («КРИПТОН-ИНТЕГРАЛ»)	
Асосий хусусятлари Интерфейс: Serial ATA 1/0; Ҳимоя усули: блокли шифрлаш; Қувват манбаи: Компьютер қувват манбаи орқали; Шифрлаш алгоритми: ГОСТ-28147-89; Шифрлаш тезлиги: 240 Мбит/с; Калит маълумотларни сақловчи: Touch Memory	

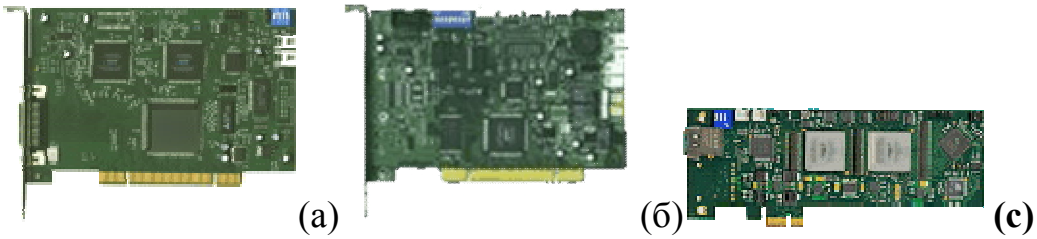
КРИПТОН AncNet Pro. М-524 ва М-525(КРИПТОН AncNet Pro) криптографик аппарат-дастурий воситалар тармоқда юборилаётган маълумотларни ҳимоялашда ва рухсатсиз киришларни олдини олиш учун

мўлжалланган. М-524 ва М-525(КРИПТОН AncNet Pro) модуллари қуйидаги вазифаларни бажаради [25]:

- Ethernet II кўринишидаги TCP/IP нинг 4 варианти билан пакетларни жўнатиш ва қабул қилиш;
- ГОСТ 28147-89 шифрлаш стандарти билан маълумотларни шифрлаш;
- Жўнатилаётган маълумотларни тўлиқлигини назорат қилиш;
- Компьюютернинг аппарат-дастурий ресурсларига бўладиган рухсатсиз фойдаланишларни олдини олиш;
- BIOS тизими юклангунга қадар фойдаланувчини идунтификация ва аутентификациядан ўтказиш;
- Юкланаётган операцион тизимни тўлиқлигини назорат қилиш;
- Рухсат этилмаган киришларда копьмютерни қулфллаш;
- Рухсат этилмаган киришларни рўйхатга олиш;
- CD-ROM ва бошқа турдаги қаттиқ дисклар орқали рухсатсиз компьютерни юклаганда қурилмали қулфлаш.

Асосий техник хусусятлари:

- Тармоқда маълумотларни узутиш тезлиги: 10/100 Мбит/сек.
- Қўлланилувчи протоколлар: Fast Ethernet 802.3, 2000Edition; 802.3U; 802.3X.
- Тармоқ қурилмалари: 100 Base-FX, 10/100 Base-TX, 10 Base-T, 10 Base-FL.
- Тармоқда ишлаш режими: Full/Half duplex(160/80 Мбит/с).
- Ҳимоялаш усули: IP пакетларни блокли шифрлаш.
- Тизимли шина стандарти: PCI Local bus Rev. 2.1, 2.2.
- PCI шинасида маълумотларни алмашиниш режими: Bus Master.
- Шифрлаш алгоритми: ГОСТ 28147-89.
- Шифрлаш тезлиги: 9Мбит/с.
- Калит маълумотларни сақловчи: Touch Memory.



6-расм. а-М-524, б-М-525 ва с- PCI Express воситаси

КРИПТОН. Криптон номли криптографик ҳимоя воситаси IBM PC замонавий компьютерларига мўлжалланган шифрлаш аппарати бўлиб, давлат ва савдо тизимларида маълумотларни хавфсизлигини таъминлашда қўлланилади [25].

Криптон номли қурилмалар қуйидаги афзалликларга ега:

- Криптографик алгоритмларни аппарат кўринишда амалга оширилганлига орқали алгоритмни тўлиқлигини таъминлайди;
- Шифрлаш калити компьютернингтезкор хотирасида емас балки қурилма хотирасида сақланади;
- Қасодифий сонлар аппарат кўрсаткичи;
- Шифрлаш калитини смарт-карта ёки Touch Memory орқали юклаш;
- Криптон қурилмаси ёрдамида компьютерни рухсатсиз киришларни олдини олишда ва рухсатни чеклашда фойдаланиш имкони мавжудлиги;
- Махсус шифрлаш процессори компьютернинг марказий процессорини юклайди.

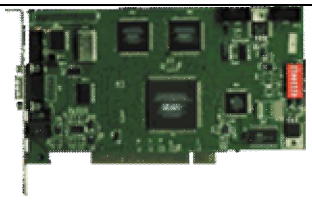
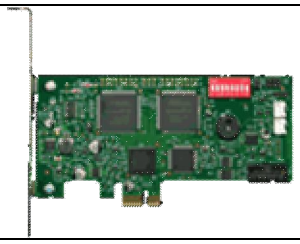
Криптон қурилмаси учун дастурий воситалар қуйидаги вазифаларни бажаради:

- Компьютердаги маълумотларни(файллар, папкалар, диск қисмлари) шифрлаш ва уларни хавфсизлигини таъминлаш;
- Маълумотларни ҳақиқийлигини тасдиқлашда электрон рақамли имзодан фойдаланиш;

- Маълумотларни тармоқ орқали узатишда хавфсизликни таъминлаш учун вертуал тармоқлардан қойдаланиш, IP пакетларни шифрлаб жўнатиш;
- Компьютерда рухсатсиз киришларни олдини олиш ва фойдаланишларни чеклаш.

5-жадвал

Асосий техник хусусиятлар

Шифрлаш алгоритми Шифрлаш калити узунлиги, бит Калит тизими даражалари сони Тасодифий сонлар кўрсаткичи Калитларни қайтарилаш даражаси Қўллаб-қуватловчи операцион тизим	ГОСТ 28147-89 256 3 (асосий калит, фойдаланувчи / тармоқ калити), сеанс калити) Аппаратли 0.0005 дан кўп бўлмаган MS-DOS, Windows 95(98)/ME/NT 4.0/2000/XP/2003 UNIX(Solaries/Intel)
КРИПТОН-8	
Шифрлаш алгоритмини амалга ошириш тури: аппаратли; Шифрлаш тезлиги: 8,5 Мбайт/с гача; Тизим шина стандарти: PCI	
КРИПТОН-10	
Шифрлаш алгоритмини амалга ошириш тури: аппаратли; Шифрлаш тезлиги: 27 Мбайт/с гача; Тизим шина стандарти: PCI Express x1 Rev. 1.1	

РУТОКЕН. РУТОКЕН – аутентификациялаш ва маълумотларни ҳимоялаш тизими бўлиб, россияда ишлаб чиқилган ёки халқаро стандартларини қўллайди. У USB занжир кўринишида бўлиб, компюьтернинг USB портига улунади. Ҳозирда РУТОКЕНнинг 32Кбайт ва ундан юқори хотирали турлари қўлланилмоқда [22,25].

РУТОКЕН қуйидаги вазифаларни бажаради:

Аутентификациялаш:

- Маълумотлар базаси, WEB-серверларда, VPN-тармоқларда парол орқали бўладиган аутентификацияни аппарат-дастурий аутентификацияга алмаштириш;
- Почта серверлари, маълумотлар базаси сервери, Web-серверлар, файл серверлар билан бўладиган тўғридан-тўғри алоқа ҳимоялаш.

Маълумотларни ҳимоялаш:

- Маълумотларни ГОСТ 28147-89 стандарти орқали шифрлаш;
- Электрон почтани шифрлаш, электрон рақамли имзо орқали ҳимоялаш;
- Компьютерга бўладиган рухсатларни ҳимоялаш.

Корпаратив фойдаланишда:

- Амалий дастурлар орқали электрон савдо-сотиқ тизимида хизмат маълумотларини, шахсий маълумотларни, паролларни, рақамли сертификатларни, шифрлаш паролларини сақлашди;
- РУТОКЕН корпаратив тизимларда ҳар хил турдаги ахборотларга бўладиган рухсатларни берувчи ягона идентификатор сифатида қўллаш.

РУТОКЕНнинг асосий хусусятлари:

- ГОСТ 28147-89 стандарти бўйича аппаратли шифрлаш;
- ISO 7819 да мавжуд файл тизимлари;
- 8, 16 ёки 32 Кбайтли мустақил энергия манбаига эга бўлган хоитра;
- PC/SC, PKCS#11, MS CryptoAPI, X.509 ларни қўллаш.

Умумий техник хусусятлар[25]*:*

- Ҳимояланган микроконтроллер асосида ишлаши;
- USB(USB 1.1/USB 2.0) интерфейсга егалиги;
- 8, 16 ва 32 Кбли EEPROM хотира;
- Икки факторли аутентификация(РУТОКЕН фактории ва PIN код орқали);
- 32 битли такрорланмас серия рақамига эгалиги;

- Windows 98/ME/2000/XP/2003 операцион тизимларига ишлатиш имконяти мавжудлиги;
- ISO/IEC 7816, PC/SC, ГОСТ 28147-89, MS CryptoAPI ва SmartCardAPI, PKCS#11 стандартларини қўллаб-қуватлаши.

Қўшимча имконятлари [25]*:*

- X.509 стандарти ва RSA, DES(3DES), RS2, RC4, MD4, MD5, SHA-1 алгоритмларини қўллаб-қуватлаши;
- Ассиметрик шифрлаш алгоритмлари ва ЭРИ алгоритмлари калитларини сақлаш;
- E-mail мижозлар: MS Outlook, MS Outlook Express ва Microsoft ва Verisign сетификат марказларини ишлашини тестлаш;
- Windows 2000/XP/2003 операцион тизимида PKI Logon орқали аутентификациялаш.

КриптоПРО – криптографик ҳимоя воситаларини ишлаб чиқарувчи ташкилоти бўлиб, 2000 йилда ташкил топган. Ушбу ташкилот криптографик ҳимоя воситалари, асосан ЭРИ воситаларини ишлаб чиқариб, жаҳон бозорида КриптоПРО номи остида ўз маҳсулотлари билан машҳур. Ушбу ташкилот криптографик ҳимоя воситалари асосида асосан россида ишлаб чиқарилган стандартлар ва жаҳонда тан олинган стандартлар ётади [24].

КриптоПРО HSM –криптографик аппарат-дастурий модул ҳисобланиб, КриптоCSP модули билан биргаликда фойдаланилади [14, 24].

7-расм. КриптоПРО HSM аппарат-дастурий воситаси кўриниши

КриптоПРО HSM криптографик аппарат-дастурий воситаси қуйидаги вазифаларни бажаради [14,24]:

- ЭРИ ташкил этиш ва текшириш;
- хэш қийматни ҳисоблаш;
- маълумотлар блокини шифрлаш ва дешифрлаш;
- калитларни ҳосил қилиш ва уларни сақлаш;
- криптографик хизматлар учун фойдаланувчиларни бошқариш;

КриптоПРО HSM криптографик аппарат-дастурий воситасида қуйидаги криптографик стандартлар фойдаланилган [24]:

- ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 ва RSA алгоритмлари учун калитларни ҳосил қилиш;
- ГОСТ 28147-89 стандарти бўйича маълумотларни шифрлаш ва дешифрлаш;
- ГОСТ Р 34.11-94 стандарти бўйича хэш қийматларни ҳисоблаш;
- ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 ва RSA ЭРИ алгоритмларини ҳосил қилиш ва текшириш;
- ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 стандарти учун калитларни очиқ тақсимлаш алгоритми, Диффи-Хеллмандан фойдаланиш.

CISCO – дунёда тармоқ қурилмаларини ишлаб чиқарувчи этакчи ташкилит ҳисобланиб, 1984 йилда ташкил топган. CISCO тармоқ воситалари ўзида хавфсизликни таъминлаш мақсадида криптографик тизимлардан фойдаланади [29].

CISCO компанияси ишлаб чиқарадиган қурилмаларда хавфсизлик воситаларида криптографик тизимлардан кенг фойдаланилади. CISCO ҳимоя воситаларида хавфсизлик беш қисмга бўлиниб, қуйида ҳар бир қисмда фойдаланиладиган криптографик тизимлар ҳақида маълумот берилган [9][10].

Authentication, Authorization, and Accounting (AAA). Ушбу қисмда тизимда фойдаланувчиларни ҳақиқийлигини тасдиқлаш усуллари кўрилиб,

ушбу усуллар албатта криптографик протоколлар асосида амалга оширилади.

Security Server Protocols. Ушбу қисмда биринчи қисм ташкил этувчиси(Authorization) таркибида фойдаланилган протоколлар асосида хавфсизлик ташкил этилади. Ушбу криптографик протоколлар қуйидагилар [29]:

- Radius;
- TACACS+;
- Kerberos

Ушбу протоколлар маълумот узатишда ва фойдаланувчиларни ҳақиқийлигини таъминлашда фойдаланилади.

Traffic Filtering and Firewalls. Ушбу қисмда асосан хавфсизлик сиёсатига асосан қурилмадан ўтаётган пакетларни анализ қилиш амалга оширилади. Бу анализ асосан IP- адресслар ва киритилган қоидалар асосида амалга оширилади.

IP Security and Encryption. Ушбу қисмда тармоқ сатҳида хавфсизликни таъминлаш амалга оширилади ва қуйидаги стандартлардан фойдаланади [29]:

- IPSec;
- Internet Key Exchange (IKE);
- Data Encryption Standard (DES);
- MD5 (HMAC variant);
- SHA (HMAC variant);
- Authentication Header (AH);
- Encapsulating Security Payload (ESP).

Ушбу криптографик тизимлар CISCO қурилмаларида оддий ҳолда ишлатилади. Ушбу тизимларни ўзгартириш ёки бошқасиги алмаштириш махсус буйруқлар асосида амалга оширилади.

Other Security Features. Ушбу қисмда пароллар сиёсати ўрнатилиб, парольларни сақлаш, ўрнатиш, ҳимоялаш ва шифрлаш орқали ҳимоялаш каби вазифалар амалга оширилади.

6-жадвалда CISCO тармоқ воситаларига қўлланилган криптографик тизимлар келтирилган.

6-жадвал

CISCO тармоқ қурилмаларида қўлланилган криптографик тизимлар

ID	Алгоритм	Ўлчами	Изоҳ
RNG Seed	X9.31	64-бит	Тасодифий калитлар ишлаб чиқаради.
Diffie Hellman	DH	1024-2048бит	Калит узатишда қўлланилади.
Skeyid	SHA-1	160-бит	Калит алмашинувида фойдаланилади.
IKE session encrypt key	Triple-DES/AES	168/256 бит	Маълумотларни шифрлашда.
IKE RSA Authentication private Key	RSA	1024-2048 бит	Аутентификация жараёнида.
GDOI Key encryption Key (KEK)	AES (128, 192 ва 256 bits)	168-256 бит	Калитларни ҳосил қилишда.

КРИПТОПРОЦЕСОР “ГРЯДА-41”. Ушбу криптографик аппарат-дастурий ҳимоя воситаси Украина давлат хавфсизлик хизмати томонидан давлат органлари ва тижорат ташкилотларида хавфсизликни таъминлаш мақсадида фойдаланилади. Ушбу восита ахборот хавфсизлигини таъминлашда криптографик тизимлар, калитларни генерация қилиш алгоритмлари, шифрлаш, хэш-функцияни ҳисоблаш, ЭРИ шакллантириш ва текшириш ва криптографик протоколларни шакллантириш каби тизимлардан фойдаланилган [37].

Ушбу ҳимоя воситаси орқали қуйидаги имкониятларга эга бўлинади [37]:

- ГОСТ 28147-89, FIPS 197 алгоритмлари билан шифрлаш;
- ДСТУ 4145-2002, ISO/IEC 15946-2, ГОСТ 34.310-95 алгоритмлари орқали ЭРИ шакллантириш ва текшириш;
- ГОСТ 34.311-95 (SHA-1, SHA-2) бўйича хэш-функцияни ҳисоблаш;
- Диффи-Хелман (X9.42 и X9.63) протоколи асосида калитларни тақсимлаш алгоритми;
- ГОСТ 34.310-95, ДСТУ 4145-2002 ЭРИ стандарти ва Диффи-Хелман ISO/IEC 15946-3 протоколи учун очиқ ва ёпиқ калитларни ҳосил қилиш;
- ГОСТ 28147-89 учун сеанс калитини, ГОСТ 34.310-95 ва ДСТУ 4145-2002 учун псевдотасодифий кетма-кетликни ҳосил қилиш;
- Маълумотларни ҳимояланган шаклда ташқи хотира қурилмаларида сақлаш;
- Дастурий таъминотларни тўлиқлигини ва ишлаш режимини тўғрилигини таъминлаш.

Ушбу аппарат-дастурий таъминот орқали қуйидаги натижаларни олиш мумкин [37]:

- ДСТУ 28147-89 – 108 МБит/с, FIPS 197 бўйича 100 МБит/с билан шифрлаш ва дешифрлаш;
- ДСТУ 34.311-95 бўйича 3,8 МБит/с билан хэш функцияни ҳисоблаш;
- ДСТУ 34.311-95 бўйича 0,03 с давомида ЭРИ шакллантириш;
- ДСТУ 34.311-95 бўйича 0,07 с давомида ЭРИ текшириш;
- ДСТУ 4145-2002 бўйича 0,001 с давомида ЭРИ шакллантириш;
- ДСТУ 4145-2002 бўйича 0,32 с давомида ЭРИ текшириш.

Аккорд-У. Ушбу аппарат-дастурий криптографик ҳимоя воситаси бўлиб, асосан Microsoft Windows 2000/XP/2003/Vista/2008/7 тизими учун ишлаб чиқилган. Ушбу ҳимоя воситаси россия хавфсизлик хизмати

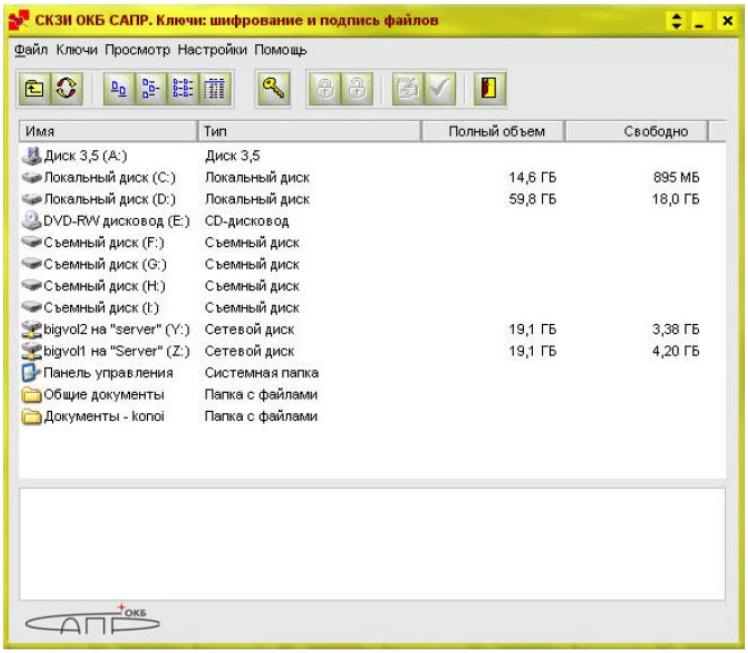
томонидан яратилган бўлиб, асосан ушбу давлат криптотизимлари асосида шакллантирилган [13].

Ушбу восита қуйидагилар учун фойдланилиши мумкин [13]:

- ШК хотирасидаги ва ташқи хотира қурилмаларида маълумотларни шифрлаш ва ЭРИ амалларини бажариш. Ушбу амал бажарилишида амаллар ва ҳисоблашлар қурилма хотирасида амалга оширилади ва сақланади. Буларни бошқариш еса дастурий интерфейс орқали амалга оширилади.
- Операцион тизимни ишончли юкланишини таъминлаш;
- Аутентификациядан ўтказиш;
- Шифрлашда ва ЭРИ текширишда фойдаланилган калитларни аппарат шаклда ҳосил қилиш.

Аккорд-У қуйидаги имкониятларга эга [13]:

1. Қуйидаги алгоритмларнинг аппарат шаклида ҳисоблаш:
   - ГОСТ 28147-89 бўйича шифрлаш;
   - ГОСТ Р 34.11-94 бўйича хэш-функцияни ҳисоблаш;
   - ГОСТ Р 34.10-2001 бўйича ЭРИ шакллантириш ва текшириш;
   - Парол орқали аутентификация жараёнида паролларни ҳосил қилиш ва текшириш.
2. 3 тагача ташқи қурилмаларни улаш имконияти.
3. Криптографик тизимлар калит маълумотларини сақлаш учун 4 байт ҳажмдаги ички хотира.
4. Криптографик тизимларда калит, сертификат ва калит маълумотларни сақлаш учун алоҳида 512 Кбайтли хотира.
5. Аппарат шаклдаги тасодифий калит генератори.



8-расм. Шифрлаш/ЭРИ дастури ойнасининг кўриниши

“Crypto AG”. Crypto AG Швейцария компаняси бўлиб, алоқа ва ахборот технологиялари тизимида криптографик ҳимоя воситаларини ишлаб чиқариш билан шуғулланади.

9-расм. Crypto AG компанияси белгиси

Ушбу компания асосан алоқа каналларида хафвсизликни таъминлаш масаласи билан шуғулланади ва OSI нинг 1,2,3 босқичларида ишловчи тармоқ қурилмаларини ҳамда, радио, ethernet, STM, GSM, телефон ва факс қурилмалари учун шифрлаш воситалари ишлаб чиқаради [27].

Ушбу компания ҳимоя воситаларида швейцария ва халқаро стандартларидан фойдаланади.

“RSA Data Security”. Ушбу АҚШ давлат компанияси компьютер ва тармоқ хавфсизлиги доирасида криптографик ҳимоя воситаларини ишлаб чиқаради. Ушбу компания ҳимоя воситалари RSA BSAFE криптографик кутубхона ва SecurID аутентификация токенларига асосланган.

Ушбу компания ҳимоя воситалари асосан АҚШ давлати стандартлари асосида ишлаб чиқилади. Ҳозирда кенг фойдаланилаётган воситалар қуйидагилар [28]:

1. Аутентификация воситалари:
   6. RSA Adaptive Authentication
   7. RSA Digital Certificate Manager
   8. RSA Identity Verification from LexisNexis
   9. RSA SecurID
2. Маълумотни ёқолишини олдини олишга мўлжалланган:
   10. RSA Data Loss Prevention (DLP)
   11. RSA Data Loss Prevention (DLP) Datacenter
   12. RSA Data Loss Prevention (DLP) Endpoint
   13. RSA Data Loss Prevention (DLP) Network
3. Маълумотлар ҳимояси:
   14. RSA BSAFE
   15. RSA Data Protection Manager
4. Тармоқ мониторинги ва анализи:
   16. RSA Security Analytics
5. Хавфсизлик анализи:
   17. RSA Security Analytics

ва бошқа хавфсизлик соҳасига доир ҳимоя воситаларини ишлаб чиқаради.

1.3. Мавжуд криптографик аппарат-дастурий воситаларини қуриш усулларининг қиёсий таҳлили

Ҳозирги кунда келиб ахборот технологияларини ўсиши ва унда хавф-хатарларнинг ортиши натижасида ахборот хавфсизлини ҳимоя воситаларига, хусусан КҲВ бўлган талабларнинг ортишига олиб келди. Ғарбда КҲВ ишлаб чиқариш 80-йиллардан бошлаб ривожлани бошлади. Умуман олганда ҳозирги кунда КҲВ қуриш йўлида қуйидаги муаммоларга дуч келинади [23]:

- криптографик алгоритмларни компьютер тизимларида амалга оширишда мавжуд бўлган ресурслар муаммоси;
- яратилган криптоалгоритмни дастурий таъминотини яратишда ва бу алгоритмнинг компьютер тилида ҳисоблашда қанчалик мослигида;
- яратилган криптографик воситалар ўзи мустақил равишда ишлай олмайди, масалан операцион тизимда ишлайди ёки қандайдир қўшимча дастурий восита керак бўлади. Демак, маълумотни чиқиб кетиш хафи мавжуд бўлади;

КҲВ қуришда тўсқинлик қиладиган юқоридаги муаммоларни бартараф этишда ва самарали КҲВ ишлаб чиқишда қуйидаги вазифалар қўйилади [7,8,23]:

- криптографик алгоритмларни компьтер тизимларида дастурий кўринишда ва алоҳида аппарат кўринишда яратишда оптимал йўлни топиш;
- КҲВ ташқи тасирлардан ҳимолаш;
- КҲВ ташкил этувчи қисмларини ва калит маълумотларни рухсатсиз киришлардан, фойдаланишлардан сақлаш;
- КҲВ операцион тизим билан ишлашда ишончли алоқа ўрнатишни ва фойдаланувчидан мукаммал фойдаланиш талаб этилади.

Албатта, юқори ишончли КҲВ ишлаб чиқиш техник вазифани яратишдан бошланади. Шунга кўра КҲВ қуришда қуйидаги техник вазифалар ишлаб чиқили шарт:

- яратилаётган КҲВ нинг аниқ мақсади;
- КҲВ функциядарини тўғри ишлаб чиқилганлиги;
- маълумотларни ҳимоялаш даражаси учун талаблар;
- криптографик алгоритмни криптографик дастурий ёки дастурий-аппарат тарзда амалга ошириш учун талаблар;
- рухсатсиз фойдаланишдан ҳимоялашга бўлган талаблар;
- тизим ресурсларидан ва бошқа дастурий таминотдан фойдаланишда қаттиқ талаблар;

- махсус талаблар;
- дастурий тиллардан фойдаланишда мавжуд талаблар.

КАДҲВни қуриш усуллари. КҲВ қуришда абстракция усулларига мувофиқ яратувчилар икки йўлдан боришади: аппарат қисмдан(юқори поғонадан) дастурий восита қисмига, фойдаланувчи интерфейсини яратиш ёки тескариси дастурий қисмдан(қуйи поғонадан) аппарат қисмга ўтиш орқали [23].

Шуларга асосланиб, КАДҲВ қуришда икки усулдан: юқоридан-пастга ва пастдан юқорига усулларидан фойдаланилади. Қолган усуллар ушбу усулларга асосланади ёки уларни биргаликдаги кўринишидан иборат [23].

Пастдан-юқорига усули. Ушбу усулда асосан яратувчи аппарат восита асосида ҳосил қилишни мақсад қилади. Ушбу усулда ҳар бир вазифалар қатламларга бўлиниб амалга оширилади. Энг қуйи қатламда аппарат қисм жойлашиб, янги қўшимча функция қўшиш орқали кейинги қатлам ҳосил қилинади. Энг юқори қатлам орқали пастдаги барча қатламларни бошқариш имкони мавжуд бўлиб, барча талабларга жавоб беради ва барча бошқаришлар ушбу қатламда амалга оширилади.

Ушбу усулнинг камчиликлари қуйидагидардан иборат:

- киритилган буйруқни бажаришни дастлабки, энг қуйи босқич орқали амалга оширилиши, ўз-ўзидан бу жуда мураккаб ва унга мос келсагина бажарилади;
- дастурий қисмини яратиш имконияти фақатгина аппарат қисми(микросхема) яратилгандан сўнг амалга оширилиши;
- техник вазифада қўйилган мақсад ва якуний олинган восита орасида фарқни мавжудлиги.

Ушбу усулда криптографик алгоритмни дастурий воситага айлантиришда, дастурчи фақат яратилган қурилма элементлариг мос келадиган усуллар ва буйруқлардан фойдаланиши талаб этилади. Қисқа

қилиб айтганда, аппарат қурилма имконятидан келиб чиққан ҳолда криптографик алгоритмларни ёзиш амалга оширилади.

Юқоридан-пастга усули(иерархик усул). Ушбу усул пастдан-юқорига усулига тескари бўлиб, бунда яратилган дастурий таъминот асосида қуйига қараб аппарат қатламгача амалга оширилади. Бу усулда жараён ундан кейинги(пастки) қисмга узатиш орқали бажарилади [23].

Ушбу иерархик усулни ташкил этишда модулли ва структурали усуллардан фойдаланилади.

Ташкил этишнинг модулли усули дастурлашнинг қуйидаги мустақил қисмларидан: алмаштирувчи қисм, кодификация, ўчириш ва қўшимча ташкил этувчи қисмлардан иборат.

Модулли усулдан фойдаланиш қуйидаги афзалликларни беради:

- дастурни созлашни осонлаштиради;
- биргаликда ишловчи дастур ва қурилма яратувчиларга бир-бири билан шерикликда ишлашга имкон беради;
- дастур сифатини оширишда.

Ташкил этишнинг структурали усули фундаментал билимлар ва асосан амалга оширилишдан иборат. Ушбу усулдан фойдаланиб дастур яратишда асосий учта функционал қисмни қуриш керак, улар қуйидагилар:

- функционал блок;
- умумлашган жараён тузиш блоки;
- икки томонлама йечим қабул қилувчи тузилмали блок.

Структурали усул жараён қурилишини рўйхатга олади, яратувчига операцион тизим ёки аппарат билан биргаликда ишлаши учун имконият яратади.

КАДҲВ ишончлилигини таъминлаш. Ҳозирги замон талабларидан бири шуки, ҳар бир ишлаб чиқариладиган аппарат-дастурий ҳимоя воситалари тизимда фойдаланишда хавфсизликни таъминлаши керак ёки бошқача айтганда, ишончли бўлиши керак [23].

Умумий ҳолда КАДҲВ да ишончлилик деганда, вақт бўйича барча параметрларни сақланиши, техник томондан хавфсизликни таъминлаш, тизим ишлаш режими, ундаги функцияларни махфий тутилиши каби вазифаларни тушуниш мумкин.

Бошқа томондан, ҳар қандай криптографик тизимни шакллантиришда дастурий воситани тўғри шакллантириш муҳим аҳамиятга ега. Чунки ҳозирда замонавий дастурий тизимларда алгоритмни шунчаки амалга ошириш эмас балки, қўйилган техник вазифа ва хавфсизлик талабларидан келиб чиқиб амалга ошириш талаб этилади.

Умумий ҳолда КАДҲВ ишончлиликни таъминлаш икки турдаги хатоликни бартараф этиш билан амалга оширилади. Булар тизим ишлашидаги хатолик (fault tolerance) ва тизимни қуришдаги мавжуд хатоликлар (fault avoidance).

Биринчи турдаги хатолик, бу шундай хатоликларки, улар дастурий таъминотни яратиш босқичларидаги хатоликлар бўлмасдан, тизимни иш жараёнида вужудга келиб одатда, дастурий, ахборотли ва вақтинчалик ортиқча ресурсдан фойдаланиш орқали вужудга келади [23].

Ушбу хатоликлар ЭҲМ да амаллар бажариж жараёнида ёки маълумотларни рестрда ёзиш ва ўқиш жараёнларига вужудга келади.

Тизимни яратишда криптографик алгоритмларни қуриш босқичларида вужудга келадиган хатоликларни бартараф этиш дастлаб криптографик алгоритмни тўғри амалга оширилганлигига, уни анализдан ўтганлигига ишонч ҳосил қилиш орқали амалга оширилади. Буларни амалга оширишда дастлаб тизимни қуришда қўйилган талаблар, хавфсизлик талаблари ва бошқа талабларга амал қилган ҳолда ёндошиш талаб этилади.

I боб бўйича хулосалар

Магистрлик диссертациясининг биринчи бўлими криптографик аппартат-дастурий воситаларнинг қиёсий таҳлилига бағишланган бўлиб, дастлаб ушбу воситаларга қўйилган талаблар келтирилди.

Ушбу келтирилган талаблардан келиб чиқиб, криптографик аппарат-дастурий воситаларнинг криптобардошлиги қуйидагиларга боғлиқлиги аниқланди:

- воситанинг амалга ошириш шаклига;
- воситанинг қуриш усулига;
- дастурий қисмининг амалга оширилиш даражасига;
- воситада ишлатилган криптотизимларнинг бардошлигига.

Криптографик ҳимоя воситаларининг хусусиятларидан келиб чиқиб, улар ҳақида, ишлаш усули тўғрисида маълумот берилди ва улар таҳлил қилинди. Ушбу таҳлил натижаларидан келиб чиқиб аппарат воситалар бардошли бўлишига қарамасдан нарх ва янгиланиш имконияти томонидан камчиликка ега еканлиги, дастурий воситалар еса бардошлилик даражаси пастлиги аниқланди. Аппарат-дастурий воситалар еса ушбу икки воситалар камчиликларини бартараф етгани ва бунинг натижасига криптобардошли еканлиги аниқланди.

Ҳозирда криптографик аппарат-дастурий воситалар ишлаб чиқарувчи фирмалар воситалари кўриб ўтилиб, АНКАД фирмасининг КРИПТОН/Crypto номи остидаги воситалари ва бошқа фирмаларда ишлаб чиқилган воситалар таҳлил қилинди.

Барча криптографик аппарат-дастурий воситалар икки усулда яъни, юқоридан-пастга ва пастдан-юқорига усуллари бўйича амалга оиширилиши ва юқоридан-пастга усули бошқа усулга қараганда қулай ва ўринли еканлиги аниқланди.

II боб. Криптографик аппарат-дастурий воситаларида фойдаланилган криптобардошли тизимлар

2.1. Шифрлаш алгоритмлари

Симметрик блокли шифрлаш алгоритмлари бир нечта босқичлардан (раундлардан) иборат бўлиб, ҳар бир раунд аралаштирувчи ва тарқатувчи акслантиришлардан тузилган. Бундай асосда тузилиш тамоили, ҳар бир раунд шифрлаш жараёнини ҳар хил калитлар билан бир хил турдаги акслантиришларни амалга оширишга, ҳамда, дешифрлаш жараёнини раунд акслантиришлари ва калитларини тескари тартибда қўллашнинг самарали имконини беради. Алгоритм асосини ташкил этувчи, раунд шифрлаш жараёнини амалга оширувчи, аралаштириш ва тарқатиш хусусиятларига эга бўлган функциялар асосий акслатиришлар дейилади. Асосий акслантиришларнинг аппарат-техник жиҳатдан қулай қўлланиш модели сифатида тескари боғлиқликка эга бўлган силжитиш регистларини келтириш мумкин. Бунда тарқатувчи акслантириш тескари боғлиқликни таъминловчи функция билан, аралаштирувчи акслантириш эса, регистрдаги маълумотларни силжитиш билан амалга оширилади [6].

Шифрланиши керак бўлган маълумот блокини силжитиш регистрларига киритиб (юклаб), регистрдаги маълумотни шартли равишда чап ва ўнг қисмблок векторларига бўлиб, улар устида ҳар хил калитлар билан бир хил турдаги акслантиришларни босқичма-босқич амалга оширишга асосланган – Фейстел тармоғи деб аталувчи шифрлаш жараёни функционал қурилмасига асосланган, 8 ва 32-битли векторлар устида амаллар бажаришга ва параметрли алгебрага асосланган алгоритмлар кенг тарқалган [6].

ГОСТ 28147-89 стандарт симметрик блокли шифрлаш алгоритми. ГОСТ 28147-89 криптоалгоритми ҳозирда Россия Федерацияси давлат стандарт шифрлаш алгоритми ҳисобланади. Бу алгоритм аппарат ва дастурий таъминот учун мўлжалланган бўлиб,

ҳимояланадиган маълумотнинг махфийлик даражасига чегаралаш йўқ . Алгоритмнинг калит узунлиги 256 битга шифрлашни 64 бит узунликдаги блокларда амалга оширади ва раундлар сони 32 га тенг [6,8,21,22].

Бирор маълумотни ГОСТ 28147-89 криптоалгоритми билан шифрлаш учун дастлаб 256 битли калитдан 32 та 32 битли рунд калитлари K_i генерация қилинади ва очиқ маълумот 64 битли $X_i, i = 1,2,...$ блокларга бўлинади. Бу 64 битли X_i блок 32 битли чап L_i ва ўнг R_i қисмларга бўлинади

$$X_i = L_i \| R_i \text{ ва } \begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i). \end{cases}$$

формула ёрдамида алмаштирилади, яъни шифрланади.

Криптоалгоритмнинг F функцияси қуйидаги амал ва алмаштиришлардан ташкил топган:

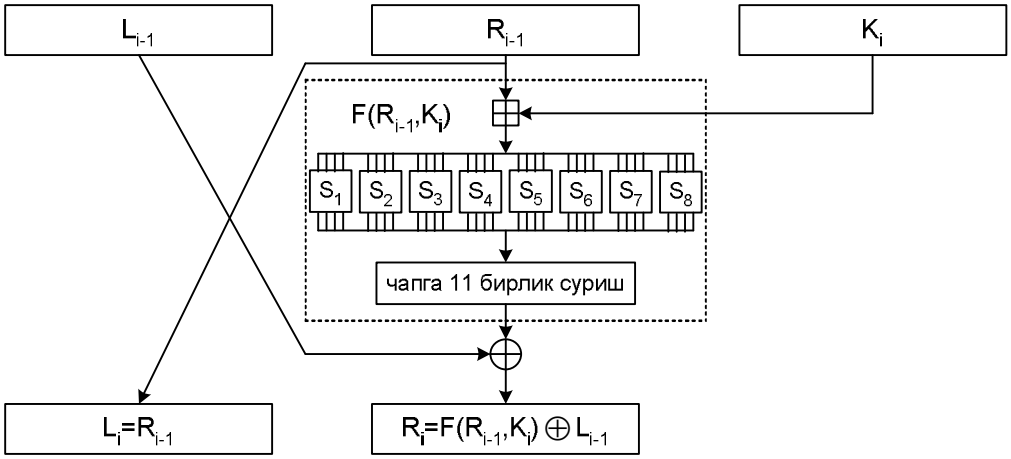
1) блокни 32 битли ўнг қисми ва 32 битли раунд калитини $\bmod 2^{32}$ бўйича қўшиш: $C_i = (R_{i-1} + K_i) \bmod 2^{32}$;

2) 32 битли C_i натижа саккизта махфий S-блокларда ўрнига қўйиш акслантириши орқали аксланади ;

3) S-блокларда чиқувчи 32 битли блок чапга 11 бирлик циклик сурилади;

Очиқ маълумот 32 раунд итератив шифрлашдан сўнг, чап L_{32} ва ўнг R_{32} қисмлар бирлаштирилади ва $Y_i = R_{32} \| L_{32}$ шифрмаълумот, яъни Y_i шифрмаълумот ҳосил қилинади [6].

ГОСТ 28147-89 криптоалгоритмининг і-раунди қуйидаги функцинал схемада келтирилган:



10-расм. ГОСТ 28147-89 криптоалгоритмининг i-раунди

ГОСТ 28147-89 криптоалгоритмида 8 та S-блоклар қўлланилади, S-блоклар махфий ва бу алгоритмдаги ягона чизиқли бўлмаган акслантиришдир. Бу S-блокларнинг кириш ва чиқиш битлари тўртга тенг бўлиб, нолдан ўн бешгача бўлган сонлар қатнашади. Масалан, биринчи S-блок қуйидагича бўлиши мумкин(8- жадвал):

8 - жадвал

S-блок кўриниши

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11	7	13	0	7	9	14	1	6	15	3	4	10	2	5	12

Биринчи S-блокка кирувчи қиймат 4 га тенг бўлса, S-блокдан чиқувчи қиймат 7 га тенг. 4 ва 7 сонлари орасида чизиқли боғланиш мавжуд эмас.

ГОСТ 28147-89 криптоалгоритмида блокнинг 32 битли ўнг қисми R_i 32 битли раунд калити K_{i+1} га $\mathrm{mod}2^{32}$ амали бўйича қўшилади. Криптоалгоритм K_{i+1} раунд калити махфийлигини ҳисобга олганда, R_i ёки K_{i+1} ни битта бити ўзгариши натижанинг камида битта битини ўзгаришига олиб келади, шунингдек бу амал умумлашган тўлдириш хусусиятига эга.

Бунинг учун калит билан қўшишда ҳосил бўладиган коллизияни кўрсатиш етарли. φ_x-32 битли блокни шифрлаш акслантириши, φ_k- калит акслантириши, F-шифрлаш раунд функцияси, L-чап блок, R-ўнг блок бўлсин. Тўлдириш хусусияти қуйидаги тенглик бўйича аниқланади:

$$\varphi_x(L \oplus F(R+k)) = \varphi_x(L \oplus F(\varphi_x(R)+\varphi_k(k))).$$

φ_x ва F акслантиришлар тескариси ҳам ўзига тенглиги хоссасидан фойдалансак, қуйидаги шифр автоморфизмлик шарти ҳосил бўлади:

$$R + k = \varphi_x(R) + \varphi_k(k) (\mathrm{mod}\, 2^{32})$$

Хусусан бу шартни $\varphi_x(X) = X + 2^{31} (\mathrm{mod}\, 2^{32})$ ва $\varphi_k(k) = k + 2^{31} (\mathrm{mod}\, 2^{32})$ операторлари ҳам қаноатлантиради. Бу эса катта битнинг инверсияси раунд калити ёки 32 битли блокда пайдо бўлишини билдиради.

Криптоалгоритмнинг S-блоклари махфийлиги алгоритм бардошлилигини янада оширади. Ҳар бир S-блокда 16 та бир хил бўлмаган сонлар қатнашади ва бу сонларни тўлиқ танлаш 16! ни ва саккизта S-блокларни танлаш $C_{16!}^{8} = \frac{(16!)!}{8!(16!-8)!}$ ни ташкил этади. Криптоалгоритм дифференциал ва чизиқли криптотаҳлил усулларига ҳам бардошли бўлиб, бу криптотаҳлил усулларини алгоритмга қўллаш учун 2^{64}, яъни мумкин бўлган барча блоклар сонидан ҳам кўп очиқ маълумот талаб этилади. Алгоритмда S-блоклардан сўнг 11 бит чапга циклик суриш акслантириши қўлланилаган. 11 сони 33 га каррали, 32 га каррали эмас ва алгоритмга кирувчи блокдаги ҳар бир элемент тўлиқ аралашишини таъминлайди, яъни алгоритмга кирувчи блокнинг бирор x_i элементи, масалан 4- ўринда x_4 бўлса, 1 -раунддан сўнг 30 -ўринда x_{30} бўлиб, 2 -раунддан сўнг 17 -ўринда x_{17} бўлиб ва ҳоказо ўринларда учрайди. Ҳеч қачон бирор раунддан сўнг жойлашган ўрни қайтарилмайди, яъни $x_i \neq x_j, i \neq j$, $1 \leq i, j \leq 32$. Бу стандарт шифрлаш алгоритми ҳозирги кунда ҳам кўп жиҳатдан бошқа алгоритмларга нисбатан ўзининг кириптографик самарадорлигини сақлаб келмоқда.

Мисол тариқасида бугунги кунда ҳам ўзининг самарадорлиги ва бардошлилиги билан ишончли криптографик хусусиятларга эга бўлган Фейстел тармоғига асосланган ГОСТ 28147-89 стандарт симметрик блокли шифрлаш алгоритми такомиллашган вариантини келтирамиз.

1. Калит узунлиги: $|k| = 256 \cdot n$ бит =$32 \cdot n$ байт.
2. Блок узунлиги: $|B| = 64 \cdot n$ бит=$8 \cdot n$ байт.
3. R – ўнг ва L – чап қисмлари узунликлари: $|L| = |R| = 32 \cdot n$ бит= $4 \cdot n$ байт.
4. Такомиллашган алгоритм калити: $k(256 \cdot n) = k_1 \ldots k_{8 \cdot 32 \cdot n}$ = $k_1 \ldots k_{32 \cdot n}\, k_{32 \cdot n+1} \ldots k_{2 \cdot 32 \cdot n}$ $k_{2 \cdot 32 \cdot n+1} \ldots k_{3 \cdot 32 \cdot n}\, k_{3 \cdot 32 \cdot n+1} \ldots k_{4 \cdot 32 \cdot n}\, k_{4 \cdot 32 \cdot n+1} \ldots k_{5 \cdot 32 \cdot n}\, k_{5 \cdot 32 \cdot n+1} \ldots k_{6 \cdot 32 \cdot n}\, k_{6 \cdot 32 \cdot n+1} \ldots k_{7 \cdot 32 \cdot n}\, k_{7 \cdot 32 \cdot n+1} \ldots k_{8 \cdot 32 \cdot n}$.
5. Раунд калитлари: $k(i) = k_{(i-1) \cdot 32 \cdot n+1} \ldots k_{i \cdot 32 \cdot n}$, i=1,…8.
6. S-блоклар сони: $8 \cdot n$ (дона.)
7. Раунд калитлари узунлиги: $|k_{raund}(i)| = 32 \cdot n$ бит.

Фейстел тармоғига асосланган такомиллашган ва такомиллашмаган алгоритмларнинг шифрлаш ва дешифрлаш тезлиги тенг, чунки $n = 1$ да алгоритм блок узунлиги 64 га тенг бўлиб, алгоритм тезлиги 20 тактдан иборат бўлса, $n = 2$ да такомиллашган алгоритм блок узунлиги 128 бит бўлиб, тезлиги 40 тактдан иборат бўлади.

Демак, такомиллашган Фейстел тармоғи қуйидаги афзалликларга эга:

1. Такомиллаштириш параметри n га боғлиқ бўлган ҳолда шифрлаш алгоритми хоссалари ва бардошлилигини сақлаб қолган ҳолда алгоритм калит узунлигини ошириб бориш имконияти мавжуд. Бу эса ўз навбатида ҳисоблаш техникаси қурилмаларининг такомиллашуви натижасида алгоритм калит узунлиги тўлиқ танлаш усулига бардошсиз бўлиб қолишини олдини олади.
2. Алгорим тезлиги такомиллаштириш параметри n га боғлиқ эмас, яъни Фейстел тармоғига асосланган такомиллашган ва такомиллашмаган

алгоритм тезликлари тенг. Бу хосса, ўз навбатида, алгоритм тезлигини сақлаб қолган ҳолда такомиллаштириш имкониятини беради.

AES-FIPS 197 стандарт симметрик блокли шифрлаш алгоритми. DES блокли шифрлаш алгоритми 1999 йилгача АҚШда стандарт шифрлаш алгоритмлари сифатида ишлатиб келинган.

1974 йилдан Америка қўшма штатларининг стандарт шифрлаш алгоритми сифатида қабул қилинган DES шифрлаш алгоритми қуйидаги :

- калит узунлигининг кичиглиги (56 бит);

- S-блок акслантиришларининг дифференциал криптотаҳлил усулига бардошсизлиги ва бошқа сабабларга кўра эскирган деб саналади.

Айниқса 1999 йилда DES шифрлаш алгоритми ёрдамида шифрланган маьлумотнинг Internet тармоғига уланган 300 та паралел компьютер томонидан йигирма тўрт соат давомида очилиши ҳақидаги маьлумотнинг тасдиқланиши бундан кейин мазкур стандарт алгоритми ёрдамида маьлумотларни криптографик муҳофаза қилиш масаласини қайтадан кўриб чиқиш ва янги стандарт қабул қилиш заруратини келтириб чиқарди.

Америка қўшма штатларининг “Стандартлар ва Техналогиялар Миллий Институти (NIST)” 1997 йилда XXI асрнинг маълумотларни криптографик муҳофазаловчи янги шифрлаш алгоритми стандартини қабул қилиш мақсадида танлов эълон қилди. 2000 йилда стандарт шифрлаш алгоритми қилиб, RIJNDAEL шифрлаш алгоритми асос қилиб олинган AES (Advanced Encryption Standard) (FIPS 197) қабул қилинди. Алгоритмнинг яратувчилари Белгиялик мутахассислар Йон Дэмен (Joan Daemen) ва Винсент Рюмен (Vincent Rijmen)ларнинг фамилияларидан RIJNDAEL номи олинган [6, 21].

AES FIPS 197 блокли шифрлаш алгоритмида 8 ва 32-битли (1-байтли ва 4-байтли) векторлар устида амаллар бажарилади. AES FIPS 197 шифрлаш алгоритми XXI асрнинг энг барқарор шифрлаш алгоритми деб ҳисобланади. Бу алгоритм бошқа мавжуд стандарт симметрик шифрлаш

алгоритмларидан фарқли ўлароқ, Фейстел тармоғига асосланмаган блокли шифрлаш алгоритмлари қаторига киради [6].

Квадрат архитектурага эга AES блокли шифрлаш алгоритми ўзгарувчан узунликдаги калитлар орқали шифрланади. Калит ва блок узунликлари бир – бирига боғлиқ бўлмаган ҳолда 128, 192 ёки 256 бит бўлади. Биз мазкур ўқув қўлланма ишида AES шифрлаш алгоритмини блоклар узунлиги 128 бит бўлган ҳоли учун кўриб чиқамиз.

Блок ўлчами 128 битга тенг кириш , бу 16 байтли массив 4 та қатор ва 4 та устундан иборатдир (ҳар бир сатр ва ҳар бир устун бу ҳолда 32 разрядли (битли) сўз деб қаралади.)

Шифрлаш учун кираётган маълумот байтлари:

s_{00} , s_{10} , s_{20} , s_{30} , s_{01} , s_{11}, s_{21}, s_{31}, s_{02} , s_{12} , s_{22} , s_{32} , s_{03} , s_{13} , s_{23} , s_{33} ,

кўринишида белгиланади.

Кираётган маълумот қуйидаги 2.2 – жадвалдаги квадрат массив кўринишида киритилади. Яъни, байтларни тартиб билан устун бўйича тўлдириб борилади. Биринчи тўртта байт (s_{00} , s_{10} , s_{20} , s_{30}) биринчи устунга мос тушади, иккинчи тўртта байт (s_{01} , s_{11}, s_{21}, s_{31}) иккинчи устунга мос тушади, учинчи тўртта байт (s_{02} , s_{12} , s_{22} , s_{32}) учинчи устунга мос тушади, тўртинчи тўртта байт (s_{03} , s_{13} , s_{23} , s_{33}) тўртинчи устунга мос тушади.

9 – жадвал

Кираётган маълумотларнинг ҳолат жадвали

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	S_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

Худди шундай тартибда шифрлаш калити ҳам квадрат жадвал шаклида киритилади. Улар 128 бит = 16 байт = 4 сўз (тўртта 32 битлик блок) дан иборат:

$k_{00}, k_{10}, k_{20}, k_{30}, k_{01}, k_{11}, k_{21}, k_{31}, k_{02}, k_{12}, k_{22}, k_{32}, k_{03}, k_{13}, k_{23}, k_{33}$.

10 – жадвал

Шифрлаш калити ҳолат жадвали

K_{00}	k_{01}	k_{02}	k_{03}
K_{10}	k_{11}	k_{12}	k_{13}
K_{20}	k_{21}	k_{22}	k_{23}
K_{30}	k_{31}	k_{32}	k_{33}

Шунингдек, AES шифрлаш алгоритми раундлар сони N_r, кириш блоклар ўлчами N_b ва калит узунлиги N_k ларга боғлиқ ҳолда қуйидаги 2.4-жадвалга мос ҳолда қўлланилади.

11 – жадвал

Шифрлаш калити узунликлари

N_r	**N_b=4 128 бит**	**N_b=6 192 бит**	**N_b=8 256 бит**
N_k=4 128 бит	*10*	*12*	*14*
N_k=6 192 бит	*12*	*12*	*14*
N_k=8 256 бит	*14*	*14*	*14*

Раунд акслантиришлари. Ҳар бир раунд шифрлаш жараёнлари қуйида келтирилган тўртта акслантиришлардан фойдаланилган ҳолда амалга оширилади [11, 21]:

1) SubBytes – алгоритмда қайд этилган 16x16 ўлчамли жадвал асосида байтларни алмаштириш, яъни S -блок акслантиришларини амалга ошириш;

2) ShiftRows – алгоритмда берилган жадвалга кўра ҳолат байтларини циклик суриш;

3) MixColumns – устун элементларини аралаштириш, яъни алгоритмда берилган матрица бўйича акслантиришни амалга ошириш;

4) AddRoundKey – раунд калитларини қўшиш, яъни блоклар мос битларни XOR амали билан қўшиш.

Дешифрлаш жараёни эса шифрлаш жараёнида фойдаланилган Sub Bytes(), ShiftRows(), MixColumns () ва AddRoundKey( ) алмаштиришларига мос равишда тескари:

- invSub Bytes(),
- invShiftRows(),
- invMixColumns (),
- AddRoundKey()

алмаштиришлар мавжуд бўлиб, бундай ҳолат қаралаётган симметрик шифрлаш алгритмининг аппарат-техник қурилмасини яратишда муҳим омиллардан ҳисобланади.

O`z Dst 1105:2009 маълумотларни шифрлаш алгоритми. Ушбу «Маълумотларни шифрлаш алгоритми» (МША) стандарти электрон маълумотларни муҳофаза қилиш учун мўлжалланган криптографик алгоритмни ифодалайди. O‘z DSt 1105:2006 алгоритми ўрнига ишлаб чиқилган. МША - симметрик блокли шифр бўлиб, ахборотни шифрматнга ўгириш ва дастлабки матнга ўгириш учун фойдаланилади. МША 256 bit узунликдаги маълумотлар блокини шифрматнга ўгириш ва шифрматнни дастлабки матнга ўгириш учун 256 ёки 512 bit узунликдаги криптографик калитдан фойдаланиши мумкин [17].

Стандарт, электрон ҳисоблаш машиналари (ЭҲМ) тармоқларида, алоҳида ҳисоблаш комплекслари ва ЭҲМда ахборотга ишлов бериш

тизимларида ахборотни шифрлашнинг ягона алгоритмини ўрнатиб, маълумотларни шифрлаш қоидаларини белгилайди.

Маълумотларни шифрлаш алгоритми дастурий, аппарат ёки аппарат-дастурий криптографик модулларда амалга ошириш учун мўлжалланган.

Ташкилотлар, корхоналар ва муассасалар ЭҲМ тармоқларида, алоҳида ҳисоблаш комплексларида ёки ЭҲМда сақланувчи ва узатилувчи маълумотларнинг криптографик муҳофазасини амалга оширишда мазкур стандартдан фойдаланишлари мумкин.

МША устунларни аралаштириш ва байт бўйича алмаштириш ўзгартиришидан фойдаланишга асосланган ҳамда қуйидаги аломатлар билан тавсифланади [17]:

- босқич калитлари ахборот муҳофазасининг талаб қилинган даражасига боғлиқ ҳолда сеансларнинг маълум бир сонидан сўнг даврий равишда янгиланиб турадиган шифрлаш калити ва функционал калит асосида шаклланади. Муҳофазанинг энг юқори даражаси талаб қилинганда, функционал калит ҳар бир сеансда янгиланади;

- устунларни аралаштиришда махфий параметрлар иштирок этади.

Санаб ўтилган аломатлар маълумотларни шифрлаш алгоритмининг криптобардошлилигини ошишига ижобий таъсир кўрсатади.

Ушбу стандартда параметрли алгебра ва диамарицалар устида амаллардан фойдаланиш орқали криптобардошлилик таъминланган.

МШАда модуль арифметикасининг диаматрицалар алгебрасидан фойдаланилади, бунда, ҳисоблашнинг қийинлик даражаси матрицалар алгебрасидаги сингари бажарилади [17].

Шифрматнга ўгириш ва дастлабки матнга ўгириш процедураларида фойдаланиладиган диаматрицалар алгебрасининг асосий амали диаматрицани *p* модуль бўйича диаматрицага тескарилаш амали ҳисобланади. Бу амалларда икки ўлчамли сеанс калити массивининг махсус тузилмали *4*х*4* тартибли квадрат диаматрица билан акс эттирилувчи қисмлари иштирок этади; махсус тузилмали диаматрица учун

барча диагонал элементлар бир хиллиги, *1*-сатрдаги нодиагонал элементлар, шунингдек *2*-сатрнинг боши ва охиридаги элементлар ҳам бир хиллиги хосдир. *4*х*4* тартибли махсус тузилмали диаматрица байт даражасида ўнта элемент асосида шаклланади [17].

МШАда шунингдек бутун сонларни параметрли кўпайтириш, тескарилаш ва даражага ошириш деб аталган параметрли алгебра амалларидан фойдаланилади.

X ни *Y* га *p* модуль бўйича *R* параметрли кўпайтириш амали $X \circledR Y \ (mod\ p)$ кўринишда белгиланади ва қуйидаги кўринишда аниқланади:

$$X \circledR Y \ (mod\ p) \equiv X + Y\ (1 + R\ X)\ (mod\ p).$$

Ушбу амал коммутатив ва ассоциатив амалдир.

X ўзгарувчини *p* модуль бўйича *R* параметрли тескарилаш амали $X^{\backslash -1}\ (mod\ p)$ шаклида белгиланади ва қуйидаги кўринишда аниқланади:

$$X^{\backslash -1}\ (mod\ p) \equiv -X\ (1 + R\ X)^{-1}\ (mod\ p),$$

бу ерда $X^{\backslash -1} \circledR X \equiv 0\ (mod\ p)$, *0* – параметрли группанинг бирлик элементидир.

Асос *X* ни *p* модуль бўйича *R* параметр билан *d*-даражага ошириш амали $X^{\backslash d}\ (mod\ p)$ кўринишида ифодаланади. Масалан, $d = 37$ бўлганда *R* параметр билан $X^{\backslash d}$ қуйидагича ҳисобланади:

$$X^{\backslash 37} \Rightarrow X^{\backslash 32+4+1}\ (mod\ p) \equiv ((((X^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR (X^{\backslash 2})^{\backslash 2} \circledR X\ (mod\ p),$$

бу ерда: $X^{\backslash 2}\ (mod\ p) \equiv X\ (2 + X\ R)\ (mod\ p)$.

МШАда фойдаланиладиган сонларни параметрли даражага ошириш амали байт бўйича қайта алмаштириш талабини ҳисобга олган ҳолда амалга оширилган.

O’z DSt 1105:2009 стандартида қийидаги параметр ва функциялардан фойдаланилади [17]:

a)k – *256* ёки *512* bit узунликдаги шифрлаш калити;

b) k_f – *256* bit узунликдаги функционал калит;

c) K_e – *8*x*4 (*ёки *4*x*8)* тартибли икки ўлчамли массив шаклидаги босқич калити;

d) *b – 256* bit ли кириш блоклари сони;

e) *e* – босқичлар сони, *e=8*;

f) *p, (p +1)* – модуль, *p=256*;

g) *Aralash()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштириш учун диаматрицавий қисмлар устида амалга оширилади; мазкур шифралмаштириш кириши *Holat* массивининг диаматрицавий қисмлари ҳамда K_1 ва K_2 массивлари бўлиб, чиқиши *Holat* массивидир;

h) *BaytAlmash()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда *Holat* массиви элементларини алмаштириш массиви элементлари билан байт сатҳида алмаштириш учун фойдаланилади; мазкур шифралмаштириш кириши байт сатҳида *Holat* массиви, алмаштириш масиви чизиқли массив B_{sA} *[256]* ёки B_{sAD} *[256]* бўлиб, чиқиши байт сатҳида *Holat* массивидир;

i) *Sur()* – *Holat* массиви элементларини янада яхшироқ аралаштириш учун, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда фойдаланилади; мазкур алмаштириш кириши байт сатҳида *Holat* массиви, чиқиши устун бўйлаб шифрлашда пастга ва сатр бўйлаб ўнгга ёки шифрни очишда устун бўйлаб юқорига ва сатр бўйлаб чапга сурилган байт сатҳида *Holat* массивидир;

j) *ShaklSeansKalitBayt()* – сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *BaytAlmash()* шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши шифрлаш калити *k* ва функционал калит k_f бўлиб, чиқиши байт сатҳида чизиқли массивлар B_{sA} *[256]* ва B_{sAD} *[256]*;

k) *ShaklSeansKalit()* – сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Aralash()* шифралмаштиришини бажариш учун фойдаланилади; мазкур

шифралмаштириш кириши байтли элементлардан таркиб топган чизиқли массив $K_{st}=[32]$ бўлиб, чиқиши махсус тузилмали диаматрицалардан ташкил топган (K_{1t}, K_2) ёки (K_1, K_{2t}) массивлар жуфтликларидир;

l) *ShaklBosqichKalit()* – сеанс давомида сеанс-босқич калитидан босқич калитини шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Qo'shBosqichKalit()* алмаштиришини бажариш учун фойдаланилади; мазкур алмаштириш кириши чизиқли сеанс-босқич калити массиви k_{se}, чиқиши байт сатҳида берилган икки ўлчамли $K_e[8,4]$ массивидир;

m) *Qo'shBosqichKalit()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда *Holat* ва босқич калити массиви K_e элементлари устида истисноли ёки (*2* модули бўйича битлаб қўшиш) амалини бажаришдан иборат; мазкур шифралмаштириш кириши байт сатҳида *Holat* массиви, K_e массиви бўлиб, чиқиши байт сатҳида *Holat* массивидир;

n) *Qo'shHolat()* – оддий шифралмаштириш бўлиб, шифрлаш блоклари устида амалга ошириладиган электрон код китоби режимидан бошқа режимларда дастлабки матнни шифрматнга ва тескари йўналишда *XOR* амали иштирокида фойдаланиладиган алмаштириш.

2.2. ЭРИ алгоритмлари

Электрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таъминлайди [6], яъни:

- махфий калит фақат фойдаланувчи (А)нинг ўзигагина маълум бўлса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маълумотни фақат (А) томонидан жўнатилганлигини рад этиб бўлмайди;

- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда мадификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди;

- алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш юритиши муносабатидаги кўплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

ЭРИ ахборот коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани ечиш имконини беради [6][21]:

- электрон ҳужжат манбаининг ҳақиқийлигини аниқлаш;
- электрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш;
- электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлайди.

Ҳар қандай ЭРИ алгоритми иккита:

– имзо қўйиш;
– имзони текшириш;

қисмдан иборат бўлади. Имзо қўйиш муаллиф томонидан, фақат унга маълум бўлган махфий калит билан амалга оширилади. Имзонинг ҳақиқийлигини текшириш эса исталган шахс томонидан, имзо муаллифининг очиқ калити билан амалга оширилиши мумкин.

Ҳозирда ЭРИ тизимини яратишнинг бир нечта йўналишлари мавжуд. Бу йўналишларни учта гуруҳга бўлиш мумкин:

1. очиқ калитли шифрлаш алгоритмларига асосланган;
2. симметрик шифрлаш алгоритмларига асосланган;
3. имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидир.

DSA ЭРИ стандарти. 1991 йилда NIST (National Institute of Standard and Technology) томонидан DSA (Digital Signature Algorithm) алгоритмига асосланган DSS (Digital Signature Standard) ЭРИ стандартининг лойиҳаси муҳокамага қўйилди. Ушбу алгоритм бардошлилиги етарли катта туб характеристикага эга бўлган чекли майдонда дискрет логарифмлаш

масаласининг мураккаблигига асосланган. Қуйида алгоритм қадамлари кетма-кетлиги келтирилган [6, 21].

Имзони шакллантириш.

1. Маълумот жўнатувчи M -маълумотни ва қуйидаги параметрларни кенг доирадаги тизим фойдаланувчиларига очиқ эълон қилади:

p – туб сон, $2^{512} < p < 2^{1024}$, бит узунлиги 64 га каррали;

q - туб сон, $2^{159} < q < 2^{160}$, $p-1$ нинг бўлувчиси;

$g = h^{(p-1)/q} \bmod p$, бу ерда h ушбу $0 < h < p$ ва $h^{(p-1)/q} \bmod p > 1$ шартларни қаноатлантирувчи бутун сон;

y – очиқ калит бўлиб, $y = q^x \bmod p$ формула орқали аниқланади. Бу ерда x – махфий калит бўлиб, $0<x<q$ оралиқдан олинган ва фақат имзоловчининг ўзигагина маълум;

$H(M)$ – M маълумотдан $[1;q]$ оралиқдаги бутун сонни генерация қилувчи хеш-функция.

2. Маълумот жўнатувчи $0 < k < q$ оралиқдан тасодифий k сонни танлайди, уни махфий тутади ва имзо генерациясидан кейин дарҳол йўқотади.

3. Маълумот жўнатувчи r ва s қийматларни қуйидаги қонуният орқали ҳисоблайди:

$r = g^k \bmod p \bmod q,$

$s = k^{-1}(xr + H(M)) \bmod q.$

M - маълумотга қўйилган имзо (r, s) сонлар жуфтлигидан иборат.

Имзони текшириш. Қабул қилувчи M' маълумотни ва (r', s') имзони қабул қилиб олади. У M ва M' маълумотларнинг мос келишини текшириши лозим. Бунинг учун у қуйидаги қадамлар кетма-кетлигини бажаради:

1. $0 < s' < q$ ёки $0 < r' < q$ шартлардан бирортаси бажарилмаса, имзо қалбаки деб ҳисобланади ва имзони текшириш тугатилади.

2. $v = (s')^{-1} (\bmod q)$ топилади.

3. $z_1 = H(M') v \bmod q$, $z_2 = r' v \bmod q$ ҳисобланади.

4. Кейин $u = g^{z_1} y^{z_2} \ mod\ p\ mod\ q$ ҳисобланади.

5. Агар $r' = u$ тенглик ўринли бўлса, у ҳолда имзо ҳақиқий ва $M = M'$ тенглик тўғри.

Алгоритмнинг тўғрилиги. $M = M'$, $s' = s$ ва $r' = r$ бўлсин. У ҳолда $r = u$ тенглик ўринли бўлиши кўрсатилади.

Демак, $v = (s')^{-1} \ mod\ q$, $z_1 = H(M')\ v\ mod\ q$, $z_2 = r'\ v\ mod\ q$ эканлигидан, қуйидагини ёзиш мумкин:

$$u = g^{z1}\ y^{z1}\ \ mod\ p\ mod\ q = g^{H(M)s-1}\ g^{xrs-1}\ mod\ p\ mod\ q =$$

$$= g^{k(xr+H(M))-1(xr+H(M))}\ mod\ p\ mod\ q = g^{k}\ mod\ p\ mod\ q = r.$$

Бундан кўриш мумкинки, $r = u$ тенглик ўринли. Шундай қилиб, алгоритм тўғрилиги исботланди.

ГОСТ Р 34.10-2001 электрон рақамли имзо алгоритми.

Имзони генерация қилиш алгоритми. Бошланғич маълумотлар: M маълумот, берилган (эллиптик чизиққа алоқадор) параметрлар ва имзо махфий калити. Ушбу алгоритмда Эллиптик эгри чизиқ тенгламаси $p > 2^{255}$ шартни қаноатлантирувчи туб характеристикали F_p майдонда деб қаралди. Натижа, имзо (r, s).

Имзони генерация қилиш алгоритми қадамлари:

1. $1 \le k \le n-1$ интервалдан ихтиёрий k сони танлансин, бу ерда G нуқта тартиби $2^{254} < n < 2^{256}$ шартни қаноатлантирувчи сон.

2. $(x_1,y_1)= [k]G$ ҳисоблансин, яъни танланган эгри чизиққа тегишли G нуқтани k марта қўшилсин.

3. $r=x_1 \bmod n$ ҳисоблансин. Агар $r=0$ бўлса, 1-қадамга қайтилсин ва бошқа k сони танлансин.

4. M маълумотнинг хэш функцияси ҳисоблансин, яъни $e=H(M)$. Агар $H(M) \bmod n=0$ бўлса, у ҳолда $H(M) \bmod n=1$ деб олинсин.

5. $0< d <n$ интервалдан олинган d махфий калит асосида $s=(dr+ke) \bmod n$ ҳисоблаб топилсин.

6. Агар $s=0$ бўлса, 1-қадамга қайтилсин ва бошқа k сони танлансин.

7. Ҳосил бўлган (r,s) сонлар жуфтлиги M маълумотга қўйилган имзо ҳисобланади.

Имзони текшириш алгоритми. Бошланғич маълумотлар M маълумот, берилган (эллиптик чизиққа алоқадор) параметрлар, имзони текшириш калити ва M маълумот имзоси-(r,s). Натижа: имзо ҳақиқийлиги ёки қалбакилиги ҳақидаги тасдиқ .

Имзони текшириш алгоритми қадамлари:

1. Агар $1 \le r, s \le n-1$ бажарилмаса, у ҳолда имзо қалбаки ва текширишни шу ерда тўхтатиш мумкин.
2. $e = H(M)$ ҳисоблансин.
3. $w = H(M)^{(n-2)} \bmod n$ ҳисоблансин.
4. $u_1 = s\, w \bmod q$ ҳисоблансин.
5. $u_2 = (n-r)\, w \bmod n$ ҳисоблансин.
6. $X = [u_1]\, G + [u_2]\, Q = (x_1, y_1)$ ҳисоблансин.
7. Агар $x_1 \bmod n = r$ бўлса, имзо ҳақиқий, акс ҳолда имзо қалбаки ва алгоритм тўхтатилади [6].

O`z Dst 1092:2009 электрон рақамли имзони шакллантириш ва текшириш стандарти. Ушбу стандарт умумий фойдаланишдаги муҳофазаланмаган телекоммуникация каналлари орқали узатиладиган, берилган хабар (электрон ҳужжат) остига қўйилган электрон рақамли имзо (ЭРИ)ни шакллантириш ва унинг ҳақиқийлигини тасдиқлаш учун электрон рақамли имзо алгоритми (ЭРИА)ни белгилайди [18].

Стандарт электрон рақамли имзони шакллантириш ва унинг ҳақиқийлигини тасдиқлашда турли мақсадлар учун мўлжалланган ахборотларни қайта ишлаш тизимларида қўллаш учун мўлжалланган.

Электрон рақамли имзонинг умумий тан олинган схемаси (модели) учта жараённи ўз ичига олади:

- ЭРИ калитларини генерациялаш;
- ЭРИни шакллантириш;

– ЭРИни текшириш (ҳақиқийлигини тасдиқлаш).

Ушбу стандарт ЭРИни шакллантириш ҳамда ЭРИнинг ҳақиқийлигини тасдиқлаш учун иккита алгоритм (1-алгоритм, 2-алгоритм) ни тавсифлайди. 1-алгоритм икки асосий режимда қўлланилади:

– сеанс калитсиз;

– сеанс калитли.

1-чи алгоритм бўйича қуйидаги жараёнлар шакллантирилади.

Электрон рақамли имзо ва сеанс калитини шакллантириш. M хабар остига қўйиладиган электрон рақамли имзо ва сеанс калитини яратиш учун қуйидаги амалларни (қадамларни) бажариш зарур [18]:

1-қадам: хабарнинг хэш-функциясини ҳисобланг: $m = H(M)$ ва $c=x$ ни қабул қилинг;

2-қадам: $k=H(m+(1+mR)c)$ ни ҳисобланг. Агар $k = 0$ бўлса, унда $c = c + 2$ ни қабул қилинг ва 2–қадамга қайтинг;

3-қадам: R параметр билан $T \equiv g^{\backslash -k} \pmod{p}$ ни ҳисобланг;

4-қадам: $r \equiv m + (1+ mR)T \pmod{p}$ ни ҳисобланг. Агар $r \pmod{q} = 0$ бўлса, унда $k \equiv k+1 \pmod{p}$ ни қабул қилинг ва 3-қадамга қайтинг;

5-қадам: $s_1 \equiv k - rx \pmod{q}$ ни ҳисобланг. Агар $s_1=0$ бўлса, унда $k \equiv k + 1 \pmod{p}$ ни қабул қилинг ва 3-қадамга қайтинг;

6-қадам: $s \equiv s_1 u^{-1} \pmod{q}$ ни ҳисобланг. Агар $\mu = 0$ бўлса, унда r, s ни чиқишга беринг ва ҳисоблашни тўхтатинг;

7-қадам: $r_1 \equiv R_1 + (1 + RR_1)r \pmod{q}$ ни ҳисобланг. Агар $r_1 = 0$ бўлса, унда $k \equiv k + 1 \pmod{p}$ ни қабул қилинг ва 3-қадамга қайтинг;

8-қадам: $x_1 \equiv (k - suR_1)r_1^{-1} \pmod{q}$ ни ҳисобланг. Агар $x_1=0$ бўлса, унда $k \equiv k + 1 \pmod{p}$ ни қабул қилинг ва 3-қадамга қайтинг;

9-қадам: RR_1 параметр билан $y_1 \equiv (gR_1^{-1})^{\backslash x1} \pmod{p}$ ни ҳисобланг ва r, s, y_1 ларни чиқишга беринг.

Бу жараён учун дастлабки (киришдаги) маълумотлар бўлиб режим $\mu \in \{1, 0\}$, хабар M, ЭРИнинг ёпиқ калити (x, u), параметр g, назорат калити R_1, модуль p ва q сони ҳисобланади. $\mu = 1$ режимда чиқиш натижаси бўлиб (s, r, y_1) ва k (ушбу стандартга хос протоколдан фойдаланилганда), режим $\mu = 0$ учун эса s, r ҳисобланади. Сеанс калитли режим учун $\mu = 1$, сеанс калитсиз режим учун эса $\mu = 0$ қабул қилинади [18].

Бундан кейин имзоланган хабар (хабар ва тўлдирувчи) қабул қилувчи томонга узатилади. Агар сеанс калитли режимдан фойдаланилса, у ҳолда қабул қилувчи томонга ҳам сеанс калити узатилади.

Иккала режимда, одатда, очиқ калитлар инфратузилмаларида (ОКИ) фойдаланиладиган хабарларни алмашувчи умумий қабул қилинган протоколлари қўлланилади. Сеанс калитли режимдан фойдаланилганда ушбу стандартга хос протоколдан фойдаланишга рухсат берилади.

Электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш. Олинган M хабар остига қўйилган ЭРИнинг ҳақиқийлигини тасдиқлаш учун 1.2-алгоритм бўйича қуйидаги амалларни (қадамларни) бажариш зарур:

1–қадам: $m = H(M)$ хэш – функцияни ҳисобланг;

2–қадам: агар $L(s) <= L(q)$ AND $L(r) <= L(p)$ бўлса, унда кейинги қадамга ўтинг, акс ҳолда «имзо ҳақиқий эмас» қабул қилинади;

3–қадам: R параметр билан $z_0 \equiv z^{\backslash s} \pmod{p}$ ни ҳисобланг;

4–қадам: $r' \equiv r \pmod{q}$ ни ҳисобланг;

5–қадам: R параметр билан $y_2 \equiv y^{\backslash r'} \pmod{p}$ ни ҳисобланг;

6–қадам: $z_1 \equiv z_0 + (1 + z_0 R) y_2 \pmod{p}$ ни ҳисобланг;

7–қадам: $y_3 \equiv z_1 + (1 + z_1 R) r \pmod{p}$ ни ҳисобланг;

8–қадам: агар $\mu = 0$ ва $m = y_3$ бўлса, унда чиқишга “имзо ҳақиқий” ни беринг; агар $\mu = 1$ ва $m = y_3$, унда кейинги қадамга ўтинг, агар $m \neq y_3$, унда «имзо ҳақиқий эмас» қабул қилинади;

9–қадам: $g_3 \equiv z_1 R_1^{-1} \pmod{p}$ ни ҳисобланг;

10–қадам: $s_1 \equiv sR_1 \ (\mathrm{mod}\ q)$ ни ҳисобланг;

11–қадам: $r_1 \equiv R_1 + r'(1 + RR_1) \ (\mathrm{mod}\ q)$ ни ҳисобланг;

12–қадам: $z_2 \equiv zR_1^{-1} \ (\mathrm{mod}\ p)$ ни ҳисобланг;

13–қадам: $y_4 \equiv y_1$ ни қабул қилинг;

14–қадам: RR_1 параметр билан $z_3 \equiv z_2^{\backslash s1} \ (\mathrm{mod}\ p)$ ни ҳисобланг;

15–қадам: RR_1 параметр билан $y_5 \equiv y_4^{\backslash r1} \ (\mathrm{mod}\ p)$ ни ҳисобланг;

16–қадам: $g_4 \equiv z_3 + (1 + z_3 RR_1) y_5 \ (\mathrm{mod}\ p)$ ни ҳисобланг;

17–қадам: агар $g_3 = g_4$, унда “имзо ҳақиқий” қабул қилинади, акс ҳолда “имзо ҳақиқий эмас” қабул қилинади.

Бу жараён учун дастлабки (киришдаги) маълумотлар бўлиб имзоланган M хабар, электрон рақамли имзо s, r, очиқ калитлар y, z, назорат калити R_1, сеанс калити y_1, модуль p ва q сони, чиқиш натижаси бўлиб эса, мазкур ЭРИнинг ҳақиқийлиги ёки ҳақиқий эмаслиги ҳақидаги ахборот ҳисобланади. ЭРИ қалбакилигини аниқлаш калити (R_1, y_1) фақат сеанс калитли режимда қўлланилади.

2.3. Хэшлаш алгоритмлари

Хэш функция деб ихтиёрий узунликдаги (бит ёки байт бирликларида) маълумотни бирор фиксирланган узунликдаги (бит ёки байт бирликларида) қийматга ўтказувчи функцияга айтилади. Хэш функциялар статистик тажрибаларни ўтказишда, мантиқий қурилмаларни текширишда, тез қидириб топиш алгоритмларини тузишда ва маълумотлар базасидаги маълумотларнинг тўлалигини текширишда қўлланилади. Масалан, ҳар хил узунликдаги маълумотларнинг катта рўйхатидан керакли маълумотни тез қидириб топишда бу маълумотларни бир-бири билан таққослашдан кўра, уларнинг назорат йиғиндиси вазифасини бажарувчи хэш қийматларини солиштириш қулайроқдир [6].

Криптографияда хэш функциялар қуйидаги масалаларни ҳал қилиш учун ишлатилади:

- маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун;
- маълумотнинг манбаини аутентификация қилиш учун.

Хэш функцияга қуйидаги талаблар қўйилади [6]:

1. Ихтиёрий узунликдаги матнга қўллаб бўлади.
2. Чиқишда тайинланган узунликдаги қийматни беради.
3. Ихтиёрий берилган x бўйича $h(x)$ осон ҳисобланади.
4. Ихтиёрий берилган H бўйича $h(x)= H$ тенгликдан x ни ҳисоблаб топиб бўлмайди. (Бир томонлилик хоссаси)
5. Олинган x ва $y \neq x$ матнлар учун $h(x) \neq h(y)$ бўлади. (Коллизияга бардошлилик хоссаси).

ГОСТ Р 34.11-94 хэш функцияси алгоритми. Россиянинг ГОСТ Р 34.11-94 хэш функция стандарти ахборотни криптографик усулда ҳимоя қилиш учун, хусусан ГОСТ Р 34.10-94 ва ГОСТ Р 34.10-2001 электрон рақамли имзо алгоритмларида ишлатиш учун мўлжалланган. Хэш функциянинг қийматини ҳисоблаш жараёнида ГОСТ 28147-89 шифрлаш стандартидан фойдаланилади [6, 20].

ГОСТ Р 34.11-94 хэш функция стандартида чиқиш узунлиги белгиланган қадамли хэшлаш функциясидан фойдаланувчи кетма-кет хэшлаш усулидан фойдаланилади. Хэш функция аргументининг узунлиги 256 бит бўлган функция бўлиб, хэш қиймат узунлиги 256 бит бўлади. Хэшланадиган маълумот узунлиги ихтиёрий бўлиб, маълумот узунлиги 256 бит бўлган блокларга ажратилади. Охирги блок узунлиги 256 битдан кичик бўлса, 256 битгача нол билан тўлдирилади. Ундан ташқари бу блокларнинг охирига маълумот узунлигининг кодини билдирувчи ва назорат йиғиндисини билдирувчи яна иккита 256 битлик блоклар қўшилади. Маълумот узунлигининг кодини билдирувчи блок хэшланадиган маълумотнинг бит узунлиги $\bmod 2^{256}$ бўйича ҳисобланиб (бу процедура MD кучайтириш дейилади) ҳосил қилинади. Назорат йиғиндисининг кодини билдирувчи блок эса охирги тўлиқмас блок нол

билан тўлдирилгандан кейин барча блокларнинг йиғиндиси mod 2^{256} бўйича ҳисобланиб ҳосил қилинади.

ГОСТ Р 34.11-94 хэш функциясини ҳисоблашда қуйидаги белгилашлардан фойдаланилади [6, 20]:

M – хэшланиши керак бўлган маълумот,

h – M маълумотни $h(\mathrm{M}) \in V_{256}(2)$ га акслантирувчи хэш функция, бу ерда $V_{256}(2)$ - узунлиги 256 бит бўлган барча иккилик сўзлар тўплами,

$E_K(A)$ - A ни ГОСТ 28147-89 шифрлаш алгоритмидан фойдаланиб K калитда шифрлаш натижаси,

$\mathrm{H} \in V_{256}(2)$ - берилган бошланғич вектор.

ГОСТ Р 34.11-94 хэш функциясини ҳисоблаш учун қуйидагилар зарур:

- қадамли хэшлаш функцияси $\chi : V_{256}(2) \times V_{256}(2) \to V_{256}(2)$ ни ҳисоблаш алгоритми;

- хэш қийматни итератив ҳисоблаш жараёни.

Қадамли хэшлаш функцияси уч босқичда ҳисобланади. Биринчи босқичда узунликлари 256 бит бўлган тўртта K_1, K_2, K_3, K_4 калит генерация қилинади. Иккинчи босқичда бошланғич H вектор ҳар бирининг узунлиги 64 бит бўлган тўртта блокка ажратилади ва бу блоклар мос K_1, K_2, K_3, K_4 калитлар билан ГОСТ 28147-89 алгоритми ёрдамида шифрланади. Учинчи босқичда шифрлаш натижасини аралаштирувчи акслантириш бажарилади.

O‘z DSt 1106 : 2009 хэшлаш функцияси. Ушбу стандарт ахборотни қайта ишлаш ва муҳофаза қилишнинг криптографик методларида, шу жумладан автоматлаштирилган тизимларда ахборот узатиш, қайта ишлаш ва сақлашда электрон рақамли имзо процедураларини амалга ошириш учун қўлланиладиган иккилик символларининг исталган кетма-кетлиги учун хэшлаш функциясининг алгоритмини ва ҳисоблаш процедурасини белгилайди [16].

Хэшлаш функциясида модуль арифметикасининг бир томонлама функцияси қўлланилади, у бўйича ҳисоблашлар даражага кўтариш амалларидаги каби айнан ўша меҳнат сарфи даражасида осон амалга оширилади, функцияни инвертирлаш (тескарилаш) эса, *(A, B)* номаълум параметрда дискрет логарифм муаммосини ечиш жараёнига нисбатан кўпроқ ҳисоблашлар сарфи ва вақтни талаб қилади. Кўпайтириш, даражага кўтариш ва тескарилаш каби асосий амаллар янги бир томонлама функцияда параметр билан кўпайтириш, даражага кўтариш ва тескарилаш деб номланган. Даражага кўтаришнинг бир томонлама функцияси ушбу бир томонлама функциянинг хусусий ҳолидир. Хэшлаш функциясида параметр (коэффициент) сифатида натурал сонлар учлигидан *(A, B, R)* фойдаланилади [16].

Ушбу хэшлаш функциясида кириш кетма-кетлигининг узунлиги *128* ёки *256* битга карралидир, чиқиш кетма-кетлиги ва хэшлаш калити қайд этилган *128* ёки *256* бит узунликка эга. Ушбу стандартда кириш, чиқиш ва хэшлаш калитининг бошқа узунликларига йўл қўйилмайди.

Хэшлаш функциясида қуйидаги параметр ва функциялар фойдаланилади [16]:

а) *к* – ярим байт (байт) даражасидаги чизиқли массиви кўринишидаги *128* ёки *256* bit узунликдаги хэшлаш калити;

b) k_e - *4*x*8* тартибдаги икки ўлчамли массив кўринишидаги босқич (раунд) калити;

c) *b* – дастлабки маълумотлардаги блоклар сони;

d) *uzunlik* – дастлабки маълумотларнинг битлардаги узунлигини ўз ичига олувчи хэшлаш функциясига кирувчи маълумотларнинг охиргидан олдинги блоки;

e) *NY* - ўнлик саноқ тизимида дастлабки маълумотлар қийматлари суммасини ўз ичига олувчи хэшлаш функциясига кирувчи маълумотларнинг охирги блоки;

f) p - модуль, $p \in \{16,256\}$;

g) e_0 - *128* ва *(256)* битли кириш блоклари учун *(b +2)10* га тенг бўлган хэшлаш процедураси босқичларининг умумий сони;

h) *Qo'sh (holat, holatn)* - *holat* массиви ва *holatn* массиви жорий қийматларининг ярим байт (байт) даражасидаги элементлари устида p модули бўйича *(A, B, R)* параметри билан даражага кўтариш амали асосида хэшлаш процедурасида фойдаланиладиган ўзгартириш;

i) *BaytZichlash (holat, holatn)* - *holat* массиви ва *holatn* массиви жорий қийматларининг ярим байт (байт) даражасидаги элементлари устида, агар модуль $p=16$ бўлса, *XOR* амалидан фойдаланилган ҳолда ёки агар модуль $p=256$ бўлса, битта массивга зичлаш чизиқли массиви асосида хэшлаш процедурасида фойдаланиладиган ўзгартириш;

j) *Aralash(holat, k_e)* – диаматрицаларни кўпайтириш амали асосида хэшлаш процедурасида фойдаланиладиган ўзгартириш. Бу ерда кўпайтириладиган диаматрицалар, мос равишда, *holat* ва k_e босқич калити икки ўлчамли массивларининг квадрат шаклидаги чап ва ўнг яримларига ўзаро мос келади;

k) *SurHolat(holat)* - *holat* массиви устида амалга ошириладиган, хэшлаш процедурасида фойдаланиладиган ўзгартириш, бу *holat* массивининг барча тўртта сатрини горизонтал ва вертикал бўйича сурилишларнинг турли қийматларига даврий суришлардан иборат;

l) *SurKalit(k_e)* - k_e массиви устида амалга ошириладиган хэшлаш процедурасида фойдаланиладиган ўзгартириш, бу k_e массивининг барча тўртта сатрини горизонтал ва вертикал бўйича сурилишларнинг турли қийматларига даврий суришлардан иборат;

m) *TuzilmaKalit(k_e, k)* - хэшлаш процедурасининг ҳар бир босқичи сўнгида фойдаланиладиган ўзгартириш, бу унинг структурасини дастлабки хэшлаш калити k структурасига келтириш мақсадида k_e массивининг ҳар бир ярим байти (байти) устида амалга оширилади; ушбу ўзгартириш

натижаси k_e массивининг квадрат қисмларидан ҳар бирини тескарилаш шартларини қаноатлантиради [16].

2.4. Криптографик тизимларнинг бардошлилигини баҳолаш

Ушбу бўлимда юқоридаги бўлимларда кўриб ўтилган криптографик тизимларнинг таҳлили ва бардошлилик хусусиятлари келтирилган. Ҳар бир криптографик ҳимоя воситаси бардошлилиги албатта унда ишлатилган криптографик тизимнинг бардошлилиги билан ўлчанади. Криптографик тизим қанчалик бардошли бўлса, ундаги амалларни дастурий ва аппарат шаклда амалга оширишга қулай бўлса, албатта бу тизим самаради ва бардошли саналади.

КАДҲВ ни бардошлилик хусусиятини ошириш мақсадида уларга ҳозирда криптобардошли саналган тизимлар(юқорида келтирилган)дан фойдаланиш юқори самара беради.

Шуларни ҳисобга олган ҳолда қийидаги жадвалларда биз келтириб ўтган криптотизимлар хусусиятлари бўйича таҳлили келтирилган.

12-жадвал

Хэш функциялар таҳлили жадвали

Хусусият/ хэш функциялар	**ГОСТ Р 34.11-94**	**MD 5**	**SHA-1**	**SHA-256**	**SHA-384**	**SHA-512**	**O‘z DSt 1106 : 2009**
Хэшлаладиган матн узунлиги	Ихтиёрий	Ихтиёрий	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$	Ихтиёрий
Кириш блокининг узунлиги	256	512	512	512	1024	1024	128, 256
Хэш қиймат узунлиги	256	128	160	256	384	512	128, 256
Ҳар бир блокни хэшлаш қадамлари сони	19	88	80	64	80	80	16b+74, 16b+46, Бу ерда b-блоклар сони

Ушбу натижалардан кўриниб турибдики, O‘z DSt 1106 : 2009 ва ГОСТ Р 34.11-94 стандартилари кириш матн узунлиги ва коллизияга бардошлиги билан қолган хэш функцияларидан ажралиб туради. Ушбу кўрсаткичлар эса унда фойдаланилган математик амаллар қийинчилиги ва алгоритмнинг бардошлиги хусусиятлари орқали таъминланган.

ГОСТ Р 34.11-94 стандарти эса O‘z DSt 1106 : 2009 стандартига қараганда босқичлар сонидан фарқ қилади. Бу эса ГОСТ Р 34.11-94 ни тезкорлигини таъминлайди.

13-жадвал

Симметрик шифрлаш тизимлари таҳлили

Хусусият/ номи	**ГОСТ 28147-89**	**AES-FIPS 197**	**O`z Dst 1105:2009**	**DES**
Кирувчи блок узунлиги	64	128,192,256	256	64
Раундлар сони	32	10,12,14	8	16
Блокли шифрлаш асоси	Янги Фейстел тармоғи	Векторлар устида амаллар бажаришга	Устунларни аралаштириш ва байт бўйича алмаштириш	Фейстел тармоғи
Калит узунлиги	256	128,192,256	256,512	56 бит
Математик амаллар	$\mathrm{mod}\,2^{32}$ қўшиш, S - блокли акслантириш, циклик суриш, бирлаштириш, хор	Байтлар устида амаллар, кўпҳадларни кўпайтириш, қўшиш, хор амали	Параметрли алгебра асосида кўпайтириш, даражага ошириш, тескарилаш, 256 mod бўйича қўшиш, хор	*IP* ўрин алмаштириш, *T* –блокли акслантириш, S-блокли алмаштириш, хор амали
Хавфсизлик даражаси	Калит, S-блок ҳолатига боғлиқ	Калитга боғлиқ	Сеанс калити, параметрга боғлиқ	S-блок, калитга боғлиқ
Ҳужумга бардошлилиги	Бардошли, амалий томондан тўлиқ ҳужумга учрамаган	Бардошли, амалий томондан ҳужумга учрамаган	Бардошли	Бардошсиз, амалий томондан ҳужумга учраган

13-жадвал ҳар бир шифрлаш стандартининг хусисияти кўрсаткичлари бўйича таҳлили бўлиб, ҳар бир стандарт бардошлиги ундаги математик амаллар бардошлиги билан белгиланади.

Ушбу жадвалдан кўриниб турибдики, ГОСТ 28147-89, AES-FIPS 197 ва O`z Dst 1105:2009 шифрлаш стандартлари бардошлиги ва аппарат-дастурий амалга ошириш имкониятлари мафжуд.

Ушбу имкониятлар эса ушбу стандарт алгоритмларни амалда қўллаш ва ундан юқори натижа олиш мумкинлиги кўрсатади.

Ушбу шифрлаш стандартлари ҳозирга кунда тўлиқ амалий ҳужумга учрамаган, бу эса уларнинг бардошли еканлигидан далолатдир.

14-жадвал

ЭРИ алгоритмлари таҳлили жадвали

Белгилар	**O`z Dst 1092:2005**	**DSA**	**ГОСТ Р 24.10-2001**
Алгебраик структираси	Параметрли алгебра	Чекли оддий майдон	Чекли оддий майдон, аниқланган ЭЭЧ
Модул типи ва ўлчами	Туб сон $p>2^{255}$(афзаллиги: тезкорликда)	Туб сон $2^{511}<p<2^{1024}$	Туб сон, $p>2^{255}$
Процедураларда фойдаланилган асосий амаллар	1. Параметрли кўпайтириш 2. Параметр билан даражага ошириш 3. Параметр билан тескарилаш 4. Тескарилаш	1. Кўпайтириш 2. Қўшиш 3. Даражага ошириш 4. Тескарилаш	1. Қўшиш 2. Инкор 3. Кўп марталик қўшиш (камчили: амалларнинг мураккблигида)
Даража асоси типи	Махфий – g. (афзаллиги: дискрет логарифм масаласини қўшиш мураккаблигида)	Ошкора – g. (камчилиги : дискрет логарифмлаш масаласини қўшиш осонлигида)	Ошкора – p. (камчилиги: ЭЭЧ дискрет логарифмлаш масаласини қўшиш осонлигида)
ЭРИ узунлигини қисқартиришга ёндошув	Фактор ((p-1) нинг туб кўпайтувчиси) дан фойдаланиш $2^{254}<q<2^{256}$	Фактордан фойдаланиш $2^{159}<q<2^{160}$	Циклик группанинг тартибидан фойдаланиш $2^{254}<q<2^{256}$ q-группа тартиби
Ёпиқ калит шакли	Жуфтликлар(r,s) $\mu=0$, (r,s,y_1) $\mu=1$. (камчилиги: $\mu=1$)	Жуфтлик(r,s)	Жуфтлик(r,s)
Бардошлилик	$\mu=1$ да даража	Модуллар (512-	Модул 255 битдан

	параметри муаммосининг мураккаблигига асосланган (афзаллиги:RSA га нисбатан бардошли)	1024) бит бўланда дискрет логарифмлашнинг муракка	ката бўлганда ЭЭЧ да дискрет логарифмлашнинг мураккаблигига асосланган.
Текшириш калити шакли	Жуфтлик (y,z) μ=0, (y,z,y_1) μ=1 да (афзаллиги: сохта имзони аниқлашда)	Жуфтлик (s, y)	Параметр – Q
Имзони текшириш натижаси шакли	Хэш функция қиймати ёки хэшлашдан фойдаланилмаган даги хабар блоки (афзаллиги: хэшланиши шарт бўлмаган қисқа хабарларни узутмаслик мумкинлиги)	Ижобий ёки салбий	Ижобий ёки салбий
Фойдаланиладиган мезон	1. Сеанс калитисиз (μ=0) 2. Сеанс калити билан (μ=1) (афзаллиги: янги имкониятлар туғилишида)	Сеанс калитисиз	Сеанс калитисиз
Фойдаланилган протоколлар	Стандартга μ=1 маромда (камчилиги: калитларни рўйхатга олиш марказига ортиқча юклама тушади)	Ананавий	Ананавий

Ушбу жадвалда ҳозирда кенг қўлланилайтган бардошли саналган ЭРИ стандартлари келтирилган.

Юқоридаги жадваллардан кўриниб турибдики, ҳар бир криптотизим ўзига тегишли бўлган афзалликлар ва камчиликларга ега. Ҳар бир криптографик ҳимоя воситаси яратаётган томон талабидан келиб чиққан ҳолда, ушбу тизимлардан бири танланади.

II боб бўйича хулоса

Магистрлик диссертациясининг иккинчи бўлимида замонавий криптографик аппарат-дастурий воситаларга дастурий қисм сифатида фойдаланилган бардошли криптографик тизимлар ҳақида тўхталди.

Таҳлиллар натижасида O‘z DSt 1106 : 2009 ва ГОСТ Р 34.11-94 хэшлаш стандартлари бошқа хэш алгоритмларга қараганда бардошлиги ва маълумотни яхлитлигини таъминлашда фойдаланиш мумкинлиги исботланди.

Шифрлаш стандартлари сифатида эса ГОСТ 28147-89, AES-FIPS 197 ва O`z Dst 1105:2009 олиниб уларни хусисиятлари бўйича таҳлилланди. Ушбу стандартлар аппарат-дастурий восита шаклида амалга ошириш қулайлиги ва уларни ҳозирда Россияда ишлаб чиқариладиган криптографик аппарат-дастурий воситаларда фойдаланилиши ҳақида тўхталди.

Ҳозирда маълумотларни ҳақиқийлигини ва муаллифини аниқлашда ЭРИ тизимидан кенг фойдаланиляпти. Бу жараённи ишончли амалга оширишда ундаги алгоритм бардошлиги муҳим аҳамиятга ега. Шуни ҳисобга олиб ЭРИ имзо алгоритмлари таҳлил қилиниб, фойдаланиш тартиби ҳақида маълумот берилди.

Умумий ҳолда иккинчи бўлимда криптографик аппарат-дастурий воситаларда фойдаланилган криптографик алгоритмлар таҳлил қилиниб, криптобардошлик хусусиятлари санаб ўтилди.

III боб. Бардошли дастурий криптографик модулни ишлаб чиқиш

3.1. “CRYPTO” номли криптографик дастурий воситасини ҳосил қилишга ва дастурлаш тилларига бўлган талаблар

Ушбу яратилган криптографик дастурий восита “CRYPTO” номи билан аталиб, у қуйидаги криптографик тизимларни ўз ичига олган:

- блокли шифрлаш тизимлари;
- ЭРИ алгоритмлари;
- хэшлаш тизимлари ;
- қўшимча криптографик тизимлар.

Криптографик дастурий воситанинг асосий вазифаси ҳозирда кенг тарқалган “SecretDisk” дастурларига ўхшаш бўлиб, яратилган вертуал дискда маълумотларни бардошли блокли шифрлаш тизимлари ёрдамида ҳимоялашдан иборатдир. Юқоридаги фикрларни ҳисобга олган ҳолда “CRYPTO” дастури қуйидаги талабларни ҳисобга олган ҳолда яратилди:

- бардошли криптографик тизимлардан фойдаланиш;
- тизимни ҳимоялашда ахборот хавфсизлиги усулларидан фойдаланиш;
- тизимдан фойдаланиш қулайлиги.

Ҳар бир дастурий воситани яратишда дастурлаш тилларига ҳам алоҳида эътибор берилади. Чунки дастурлаш тиллари қанчалик яратилаётган тизим функцияларига мос бўлса, бу имконият дастурловчига ҳам, яратилган дастурий воситага ҳам қулайлик туғдиради. Шунинг учун ушбу криптографик дастурий воситани яратишда дастурлаш тилига ҳам алоҳида эътибор берилди ва уларга қуйидаги талаблар қўйилди:

- дастурлаш тили обектга мўлжалланган бўлиши;
- тизим ресурслари билан осон боғланиш имконияти мавжуд бўлиши;
- дастурлаш тилида хавфсизлик усулларидан фойдаланиш имконияти;

- фойдаланилган дастурлаш тилида ҳисоблаш амаллари(катта сонлар устида) мавжудлиги ва бажариш осонлиги ва бошқалар.

Ушбу талабларни ҳисобга олган ҳолда ушбу криптографик дастурий воситани яратишда Mircosoft Visual Studio 2008 дастурий воситалари компонентаси таркибига кирувчи Visual C# дастурлаш тили танланди.

Mircosoft Visual Studio 2008 дастури Microsoft корпорацияси томонидан ишлаб чиқилган бўлиб, бу дастур дастурчилар учун мўлжаллангандир. Бу дастур ёрдамида қуйидаги дастурлаш тилларида дастурлашни амалга ошириш мумкин:

- Visual Basic .NET
- Visual C# .NET
- Visual C++ .NET
- Visual J# .NET

Microsoft Visual Studio 2008 дастури ёрдамида Windows муҳити учун, телефонлар учун, тармоқлар учун, Web дастурларни яратиш мумкин. Microsoft Visual Studio 2008 муҳитида Visual C#, Visual Basic, Visual J# тиллари ёрдамида Web дастурларни ва Visual C#, Visual Basic, Visual J#, Visual C++ тиллари ёрдамида Windows муҳити учун дастурлар яратиш мумкин.

Қуйида ушбу дастурлаш тиллари билан танишиб чиқамиз:

Visual Basic .NET - Microsoft Visual Studio 2008 таркибидаги енг самарадорлиги катта дастурлаш тиллардан бири бўлиб, бу дастурлаш тилини тўлиқ обектга йўналтирилган дастурлаш тили деб айтишимиз мумкин. Visual Basic .NET дастурлаш тили ёрдамида Windows иловаларини ва Web иловаларни яратиш мумкин.

Visual C# .NET - Microsoft корпорацияси томонидан ишлаб чиқилган бўлиб, бу дастурлаш тили айнан .NET платформаси учун ишлаб чиқилган. Visual C# .NET дастурлаш тили имкониятлари бошқа обектга йўналтирилган дастурлаш тиллари(C, C++, Java ва Delphi)дан анча кенг

бўлиб, бу дастурлаш тилида Visual Basic .NET каби Windows иловаларини ва Web иловаларни яратиш мумкин.

Visual C++.NET - дастурлаш тили паст сатҳдаги дастурчи учун иловаларни бошқаришда талаб қилинади. .NET платформасининг Visual C++ дастурлаш тили бошқа дастурлаш тилларидан шу билан фарқ қиладики, бу дастурлаш тили .NET платформасининг кодли модели (managed code model) ва Windows (unmanaged native code model) кодли моделини қўллаб қувватлайди.

Visual J# .NET - Microsoft .NET платформаси учун Web-сервис ва иловалар яратувчи Java-дастурчилари ишлатиши мумкин. Visual J# .NET дастурлаш тили.

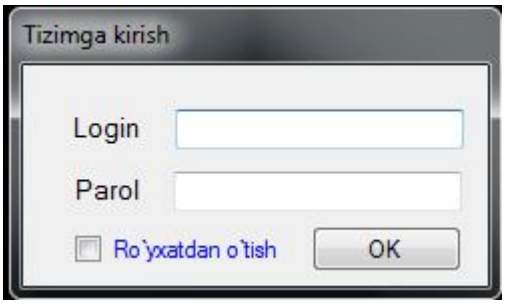
C# дастурлаш тилининг афзаллик тарафлари шундаки, бу дастурлаш тилида жуда кўплаб кутубхоналар бор. Бу кутубхоналар дастурчи учун қулайлик туғдирибгина қолмасдан, кам ҳато қилишга олиб келади. C# дастурлаш .NET Framework кутубхоналари билан ишлайди.

Яратилган криптографик дастурий модул фақат Microsoft, Macintosh операцион муҳитларида ишлайди. Бу дастур ишлаши учун бир талай қўшимча дастурлар керак бўлади. Масалан енг кераклиси .Net Framework дастурисиз ишлай олмайди. Биз бу дастурнинг ойнали (Windows Application) бўлимида туздик. C# дастурлаш тили C оиласи дастурларига киради. Шунинг учун уни C дастурлаш тилини билган дастурчига у унча қийинчилик туғдирмайди. C# дастурлаш тили C++ дастурлаш тилининг ихчамланган, фойдаланувчига қулай кўринишида чиқарилди. C++ дастурлаш тилида қўлда ёзиладиган дастур қисмлари C# дастурлаш тилида автоматик тарзда махсус буйруқлар орқали киритиладиган бўлди.

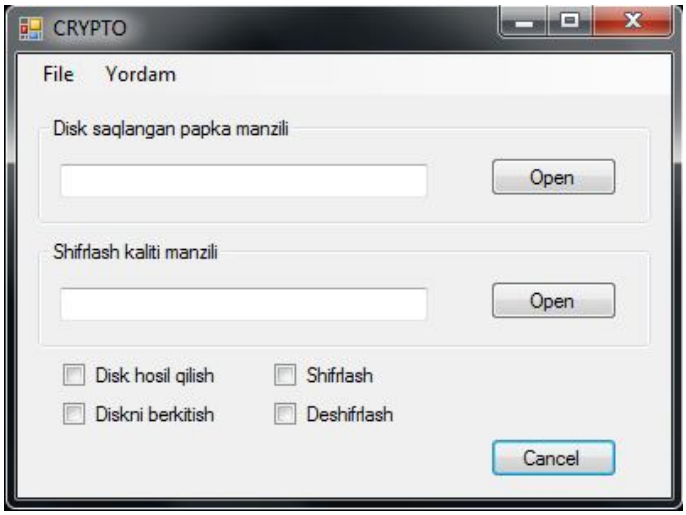
3.2. “CRYPTO” криптографик дастурий воситани умумий тавсифи ва ундан фойдаланиш тартиби

Ушбу криптографик дастурий восита Visual C# дастурлаш тилида яратилган бўлиб, ушбу дастур ишлаши учун .Net Framework 3.5

компонентасини ўрнатиш талаб этилади. Дастур ўрнатилгандан сўнг тизим фойдаланувчиси дастурдан фойдаланиш учун рўйхатдан ўтилади. Ушбу маълумот(парол, логин) орқали фойдалнувчи дастурнинг асосий саҳифасига киради ва ундан фойдаланиш имкониятига эга бўлади. Дастурнинг асосий саҳифаси кўриниши қуйидагича:



11-расм. Дастурга кириш ойнаси



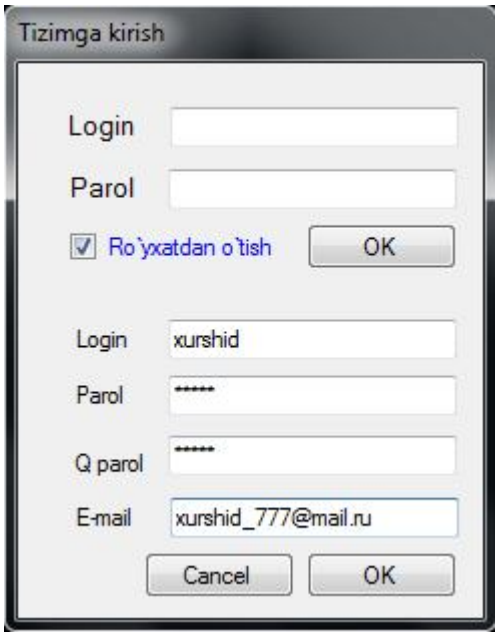
12-расм. Дастурнинг умумий кўриниши

Дастурдан фойдаланиш учун дастлаб вертуал диск яратилади. Бунинг учун диск яратиладиган диск манзили кўрсатилади. Дастур ойнасидан фойдаланиб вертуал дискни осонлик билан яратиш ва беркитиш мумкин.

Дискдаги маълумотларни хавфсизлигини таъминлаш учун уларни AES шифрлаш тизимидан фойдаланилди. Калитларни сақлаш еса калит манзили кўрсатиш билан бажарилади.

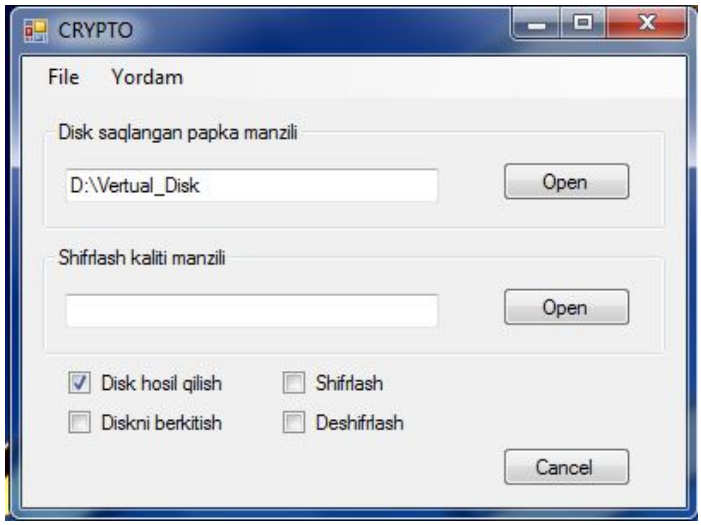
Дастурдан фойдаланиш тартиби қуйидагича:

1. Дастлаб дастур ўрнатилиб, ундан фойдаланиш учун рўйхатдан ўтилади ва дастурнинг асосий ойнасига кирилади.

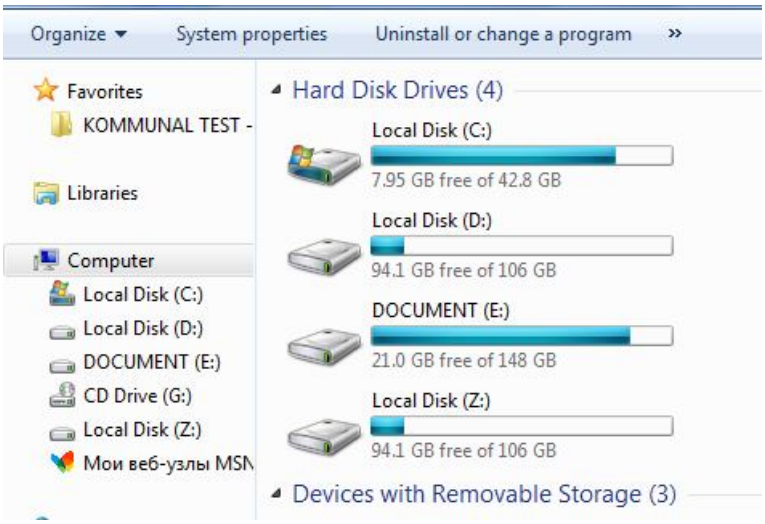


13-расм. Рўйхатдан ўтиш ойнаси

2. Дастлаб вертуал диск яратилади. Бунинг учун вертуал диск манзили кўрсатилади ва дискни ҳосил қилиш амали бажарилади. Шунда “Z” вертуал диск ҳосил бўлади.

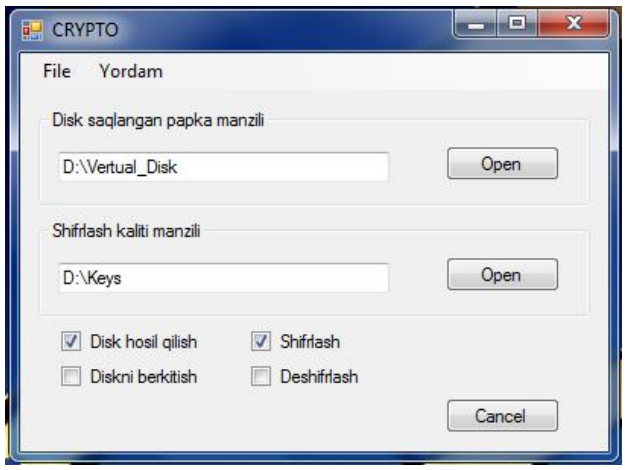


14-расм. Вертуал диск яратиш жараёни

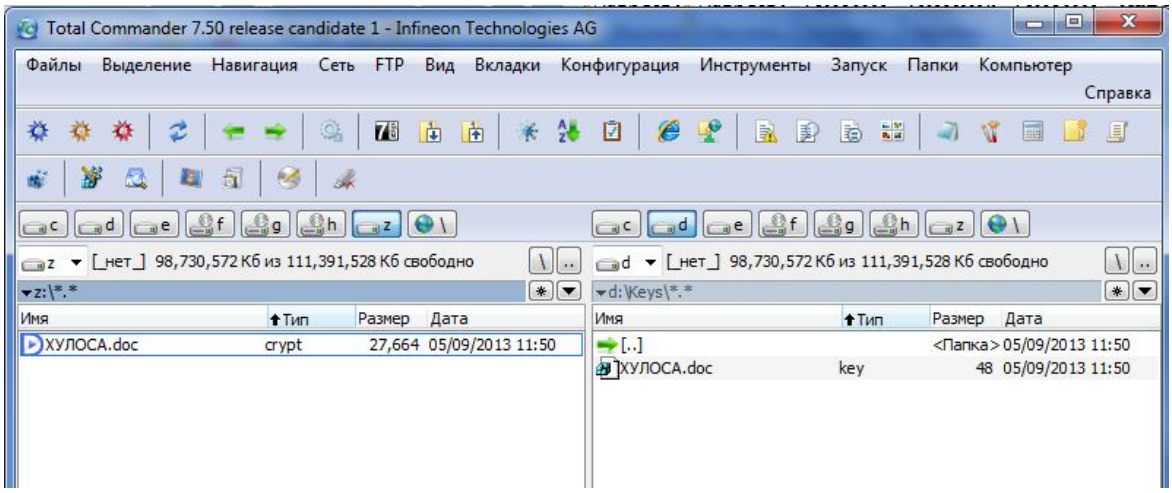


15-расм. Яратилган вертуал диск

3. Сақланаётган маълумотлар ушбу ҳосил бўлган дискда сақланади. Агар сиз маълумотларни шифрлаб сақламоқчи бўлсангиз унда маълумотларни шифрлаб сақлаш бандини белгилайсиз. Калитларни хавфсизлигини таъминлаш учун уларни ўзингиз хохлаган манзилга сақлашингиз мумкин. Буни калитни сақлаш манзилини белгилаш орқали амалга ошириш мумкин.



16-расм. Маълумотларни шифрлаб сақлаш



17-расм. Калит ва дискдаги шифрланган маълумот кўриниши

4. Барча маълумотлар дискда кўчирилади ва шифрлаб сақланганидан кейин дискни беркитиш банди белгиланиб дастурдан чиқилади. Дастурдан чиқилгандан сўнг диск манзили(папкаси) тизимнинг барча фойдаланувчилари учун фойдаланиш ҳуқиқи тақиқланади.

Ушбу вазифалар яратилган дастурнинг асосий вазифаси ҳисобланиб, бундан ташқари дастурга қўшимча криптографик тизимлар ҳам киритилган.

Бундан ташқари дастур қуйидаги имкониятларша ега:

18-расм. Дастурнинг қўшимча имконятлари

Ушбу қўшимча имкониятлар орқали фойдаланувчи маълумотларни шифрлаш стандартлари орқали шифрлаш, уларга ЭРИ қўйиш, уларни текшириш, симметрик ва ассиметрик тизимлар учун криптобардошли калитларни ишлаб чиқарувчи генераторлардан фойдаланиш мумкин.

3.3. Ишлаб чиқилган дастурий криптографик модулни бардошлилигини баҳолаш

Ушбу илмий тадқиқот ишида криптографик аппарат-дастурий воситанинг дастурий қисми саналган дастурий интерфейс яратилди. Ушбу дастурий восита C# дастурлаш тилида яратилди. Ушбу дастурлаш тили хусусиятлари ва унинг имкониятлари ҳақида юқоридаги бўлимда тўхталди.

Ишлаб чиқилган дастурнинг бардошлилиги қуйидаги параметрларга боғлиқ:

- Фойдаланилган дастурий воситанинг имконияти ва хавфсизлик даражасига боғлиқ;
- Фойдаланилган криптографик тизимнинг бардошлилигига;
- Криптоалгоритмни шакллантириш жараёни ва усулига.

Ушбу параметрлардан келиб чиқиб, ишлаб чиқилган дастурий воситани бардошлилигини қуйидагилар билан асослаш мумкин:

- Ушбу дастур C# дастурдаш тилида яратилганлиги (унинг имкониятлари юқорида келтирилган);
- Шифрлашда бардошли саналган AES ишлатилди(асосий қисмда);
- Қўшимча дастурий воситалар сифатида эса қуйидагилар ишлатилди:
    - Шифрлаш (AES, DES ва ГОСТ);
    - ЭРИ (RSA);
    - Калит генератори (туб сон генератори ва RC4 генератори).

AESнинг криптобардошлиги. Ушбу шифрлаш стандарти криптобардошлиги тўғрисида АҚШ Миллий хавфсизлик агентлиги томонидан берилган маълумотга кўра 128 бит калит ёрдамида шифрлаганда маълумотнинг махфийлик даражаси “SECRET”, 192 ёки 256 бит ҳолда “TOP SECRET” махфийлик даражасида бўлади [31].

Ушбу хусусида Брюс Шнайер қуйидагича ёзган: ”AES га биз тўлиқ ишонмаслигимиз керак. Бунинг сабаби AES содда алгебраик тузулишга эга. Ҳеч бир шифрлаш тизими ҳоттоки бундай содда тузулишга эга эмас. Лекин ушбу сабаб AESнинг бардошлигига боғлиқлиги ҳозиргача бизга маълум эмас” [12].

Николя Картуа ва Йозеф Пепшик 2002 йилда AES и Serpent шифрлаш тизимлари устида XSL-ҳужумини (инг. eXtended Sparse Linearization) олиб борди. Ҳужум натижаси эса AES шифрлаш тизимини бузиш имконини бермади [31].

AES шифрлаш тизими қуйидаги турдаги ҳужумларга бардошли [32]:

- кучсиз калитлар орқали юзага келадиган хужумлар;
- дифференциал криптоанализ;
- чизиқли (линейного) криптоанализ;
- Square ҳужумига (квадрат тузулишиги эга бўлган алгоритмларга хос);
- интерполяция (қўшимча киритиш) усулига.

2007 йилнинг май ойида криптоанализчилар томонидан AES шифрлаш тизимида қуйидаги ҳужумлар олиб борилди ва қуйидаги натижалар олинди:

- AES (192 бит, 12 раунд) варианти учун 10-раундгача назарий томондан ҳужум қилинганлиги;
- AES га side-channel-atak ҳужуми орқали бир нечта ҳужумлар олиб борилди.

Ҳозирги замон технологияси ривожи ва криптоанализнинг ривожлвнишини ҳисобга олид шуни айтиш мумкинки AES 2100 йилга

қадар ўзининг криптобардошлигини ёқотмайди. Шуни ҳам айтиб олиш керакки, AES шифрлаш тизими муаллифи ҳозирда унинг криптобардошли саналган янги AES-24 (24 раунддан иборат бўлган) вариантини тавсия этган [32].

“CRYPTO” дастурий воситасида яратилган вертуал диск сақланадиган манзилни ҳимоялаш *GrantEveryoneFullControlRight()* функцияси ёрдамида амалга оширилади. Ушбу функция тизимдаги барча фойдаланувчилар учун диск сақланган манзилдан фойдаланиш имкониятини беркитади.

Манзилдан фойдаланишга рухсат бериш учун:

```
FileSystemAccessRule rule = new FileSystemAccessRule(
userlar[i], FileSystemRights.FullControl,
AccessControlType.Allow);
```

Манзилдан фойдаланиш рухсатини чеклаш учун:

```
FileSystemAccessRule rule = new FileSystemAccessRule(
userlar[i], FileSystemRights.FullControl,
AccessControlType.Deny);
```

буйруқларидан фойдаланилади.

III боб бўйича хулосалар

Магистерлик диссертациясининг учунчи қисми амалий қисм ҳисобланиб, ушбу бўлимда криптографик дастурий восита амалга оширилиш тартиби кўриб чиқилди.

Дастурилаш тили сифатида C# дастурлаш тили танланиб, дастур Windows операцион тизими учун, Freamwork 3.5 платформаси асосида яратилди. Ушбу дастурлаш тилини танлашдан асосий мақсад қилиб, дастурнинг ишлаш тизимидан келиб чиқиб, дастурчига қулайлик туғдириши олинди.

Дастур амалга ошириш вазифасига кўра “SecretDisc” ютилиталарига ўхшаш бўлиб, фарқли равишда ҳимоялаш мақсадида AES шифрлаш тизими олиниб, ҳосил қилинган вертуал дискдаги барча файллар алоҳида калитлар ёрдамида шифрланиб сақланади. Калитларни сақлашдаги хавфларни олдини олиш мақсадида калитларни кўрсатилган манзилга сақлаш имконини кўрсатиш мумкин.

Дастурда қўшимча ЭРИ, шифрлаш алгоритмлари ва калит генератори ютилиталари мавжуд бўлиб, улар фойдаланишда қулайлик туғдиради.

Ушбу яратилган дастурий воситанинг бардошлигини унда фойдаланилган дастурлаш тили ва фойдаланилган криптографик тизим бардошлиги орқали белгилаш мумкин.

ХУЛОСА

Криптографик аппарат-дастурий воситалар асосида ахборот-коммуникация тизимларида электрон маълумот алмашинувини ҳимоя қилиш ҳозирги замонавий ахборот хавфсизлигининг асосий йўналишларидан биридир. Криптобардошли саналган аппарат-дастурий воситалардан ахборот хавфсизлигини таъминлашда фойдаланиш самарали усуллардан биридир. Ушбу илмий тадқиқот ишида қуйидаги натижалар олинди:

1. Криптографик ҳимоя воситаларга қўйилган талаблар асосида криптографик дастурий, аппарат ва аппарат-дастурий воситалар ишлаш принципи таҳлил этилди, хусусиятлари бўйича таҳлил этилди.
2. Ҳозирги кунда етакчи саналган криптографик аппарат-дастурий ҳимоя воситалари ишлаб чиқарувчи компаниялар ҳимоя воситалари кўриб чиқилди ва таҳлил этилди.
3. Криптографик аппарат-дастурий воситаларнинг қуриш усуллари таҳлил қилиниб, фойдаланиш учун фойдали кўрсатмалар берилди.
4. Криптографик аппарат-дастурий воситаларда дастурий қисм сифатида фойдаланилган криптографик тизимлар таҳлил этилди ва уларнинг бардошли параметрлари ҳақида малумотлар берилди.
5. Мавжуд криптографик тизимлардан фойдаланган ҳолда “SecretDisc” дастурий воситаси ишлаб чиқилди ва ушбу дастурни яратишда фойдаланилган дастурлаш тили таҳлил қилинди.
6. Яратилган дастурий модулнинг бардошлиги таҳлил қилиниб, ушбу параметрлар асосида тизимнинг криптобардошлигини ошириш мумкин эканлиги айтиб ўтилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. “Электрон рақамли имзодан фойдаланиш соҳасида норматив-ҳуқуқий базани такомиллаштириш” тўғрисида Ўзбекистон Республикаси Вазирлар маҳкамасининг қарори.
2. “Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш” тўғрисидаги низомни тасдиқлаш ҳақида Ўзбекистон Республикаси Вазирлар маҳкамасининг қарори.
3. Ўзбекистон Республикаси президентининг “Миллий ахборот ресурсларини муҳофаза қилишга доир қўшимча чора-тадбирлар тўғрисида” 2011 йил 8 июлдаги пқ-1572-сон қарорини амалга ошириш чора-тадбирлари ҳақида Ўзбекистон Республикаси вазирлар маҳкамасининг қарори.
4. “Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари” тўғрисида Ўзбекистон Республикаси президентининг қарори.
5. “Ахборотлаштириш соҳасида норматив-ҳуқуқий базани такомиллаштириш” тўғрисида Ўзбекистон Республикаси вазирлар маҳкамасининг қарори.
6. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.
7. Аппаратно-программные средства и методы защиты информации. С.К. Варлатая, М.В. Шаханова. Владивосток 2007.
8. Методы и средства криптографической защиты информации. О.н. Жданов в. В. Золотарев. Красноярск 2007.

9. Cisco 2951, Cisco 3925 and Cisco 3945 Integrated Services Routers (ISRs) Version 0.13. July 2011. Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA.
10. Cisco VPN 3002 Hardware Client Security Policy. Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA.
11. Стандарт криптографической защиты- AES. Конечные поля. Зензин О.С.,Иванов М.А. "КУДИЦ-ОБРАЗ" Москва 2002.
12. Практическая криптография. Нильс Фергюсон, Брюс Шнайер. 2005.
13. Средство криптографической защиты информации АККОРД-У . Руководство по эксплуатации 11443195.4012-023. Москва 2010.
14. Средство криптографической защиты информации. Жтяи.00046-01 90 03. ПАКМ "криптопро hsm". Руководство администратора безопасности. 2009 г.
15. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. – 448с.
16. O‘z DSt 1106:2009. Государственный Стандарт Узбекистана. Информационная технология. Криптографическая защита информации. Функция хэширования. – Ташкент. Узбекское агентство стандартизации, метрологии и сертификации. 2009.
17. O‘z DSt 1105:2009. Государственный Стандарт Узбекистана. Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных. Ташкент. Узбекское агентство стандартизации, метрологии и сертификации. 2009.
18. O‘z DSt 1092:2009. Государственный Стандарт Узбекистана. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Ташкент. Узбекское агентство стандартизации, метрологии и сертификации. 2009.
19. O‘z DSt 1109:2006 Ахборот технологияси. Ахборотнинг крипто-график муҳофазаси. Атамалар ва таърифлар.

20. ГОСТ Р 34.11 – 94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования. – Москва. Издательство стандартов, 1994.
21. Applied Cryptography Second Edition Protocols, Algorthms, and Source Code in C. Bruce Schneier. Publication Date: 01/01/96.
22. Криптографическая защита информации. А.В.Яковлев, А.А.Безбогов, В.В.Родин, В.Н.Шамкин. Тамбов. Издательство ТГТУ 2006.
23. Симметрик криптотизимларда калит генерациялаш алгоритмлари тадқиқи. Қурбонов Х.А., Худойқулов З.Т., Фатиллаев Б.Қ. Республиканиский семинар: «Информационная безопастность в сфере связи и информатизации. Проблемы и пути их решения». Ташкент 30 октября 2012 г.
24. http://stavkombez.ru/method/PASOIB/html/content/lect_2.html - Программно-аппаратные средства шифрования.
25. http://www.cryptopro.ru/
26. http://www.ancud.ru/crzam.html
27. http://www.aladdin-rd.ru/catalog/etoken/
28. http://www.crypto.ch/en/products-and-services
29. http://www.emc.com/domains/rsa/index.htm
30. http://www.cisco.com/en/US/products/index.html
31. http://imo.kture.kharkov.ua/rus/products.php?type=view&num=87
32. http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard
33. http://www.computerra.ru/cio/old/it-market/e-safety/320673/

Дастурнинг асосий қисми

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.IO;

namespace CRYPTO
{
    public partial class des : Form
    {
        public des()
        {
            InitializeComponent();
        }
        public string text;
        private void button1_Click(object sender, EventArgs e)
        {
            DialogResult result = openFileDialog1.ShowDialog(); // Show the
dialog.
            if (result == DialogResult.OK) // Test result.
            {
                string file = openFileDialog1.FileName;
                try
                {
                    text = File.ReadAllText(file);
                    textBox2.Text = file;
                }
                catch (IOException ex)
                {
                    MessageBox.Show(ex.ToString());
                }
            }
        }
        private void button2_Click(object sender, EventArgs e)
        {
            string folderPath = "";
            FolderBrowserDialog folderBrowserDialog1 = new
FolderBrowserDialog();
            if (folderBrowserDialog1.ShowDialog() == DialogResult.OK)
            {
                folderPath = folderBrowserDialog1.SelectedPath;
                textBox3.Text = folderPath;
            }
        }
        private void button3_Click(object sender, EventArgs e)
        {
            string key = textBox1.Text;
            string natina = DESshifrlash(text, key, false);
            StreamWriter file = new
StreamWriter(Path.Combine(textBox3.Text,
Path.GetFileNameWithoutExtension(textBox2.Text) + "_shifr.txt"));
            file.Write(natina);
            file.Close();         }
        private void button4_Click(object sender, EventArgs e)
        {
            string key = textBox1.Text;
```