ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўлёзма ҳуқуқида

ЮНУСОВА ШАХНОЗА МИРБОИСОВНА

Инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш усулларини тадқиқ этиш

5А311301- Алоқа узатиш қурилмалари тизими

Магистр
академик даражасини олиш учун ёзилган
диссертация

Илмий раҳбар:
т.ф.н. О.П.Аҳмедова

Тошкент – 2014

МУНДАРИЖА

Кириш……..... 2

I Боб **Инфокоммуникацион тармоқларни яратиш принциплари**….. 6

1 Инфокоммуникацион тармоқлар архитектурасининг асосий элементлари…….... 6

2 Инфокоммуникацион тармоқларга қўйиладиган ўзига хос талаблар……..……. 12

3 Тармоқларнинг функционал имкониятлари…….. 16

I Боб бўйича хулосалар……..……..... 25

II Боб **Инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш усуллари ва воситалари**…….. 27

1 Инфокоммуникацион тармоқларда ахборот хавфсизлиги муаммолари …… 27

2 Инфокоммуникацион тармоқларда фойдаланиладиган ахборот хавфсизлигини таъминлаш усуллари ва воситалари …..……... 35

3 Ахборот хавфсизлигини таъминлашнинг криптографик усул ва воситалари……. 47

II Боб бўйича хулосалар …….……..……..…… 56

III Боб **Инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш алгоритми ва унинг дастури** …….. 57

1 Криптографик алгоритмларни ишлаб чиқишга асос бўлган функциялар ва теоремалар …….…… 57

2 Параметрли функция асосида такомиллаштирилган алгоритм ва унинг дастури…….. 63

3 Такомиллаштирилган алгоритмдан инфокоммуникацион тармоқларда фойдаланиш бўйича тавсиялар…… 69

III. Боб бўйича хулосалар..……..…… 72

Хулоса..... 73

Адабиётлар рўйхати..... 74

Илова..... 76

Кириш

Диссертация мавзусининг асосланиши ва унинг долзарблиги

XXI асрда ахборот замонавий дунёга жуда ҳам кучли таъсир этувчи стратегик омиллардан бири ҳисобланади. Ахборот соҳаси ўзининг жуда юқори бўлган заифлиги туфайли бузғунчилар, жиноий структуралар ва бошқа деструктурали кучлар учун давлатнинг сиёсий, иқтисодий ва ижтимоий тузилмаларига таъсир этиш учун кенг тарқалган соҳа ҳисобланади. Ўзбекистон Республикаси Президентининг 2012 йил 21 мартдаги «Замонавий ахборот-коммуникация технологияларини янада жорий этиш ва ривожлантириш чора-тадбирлари тўғрисида»ги Қарори [1] шунингдек Ўзбекистон Президенти И.А.Каримовнинг «Жаҳоннинг молиявий-иқтисодий кризиси, Ўзбекистон шароитида уларни ечишнинг чоралари ва йўллари» [2] китобида алоқа ва ахборотлаштириш соҳасига тегишли масалаларнинг ечими ҳақида ҳам айтиб ўтилган. Шунинг учун ҳам давлат ҳокимияти ва бошқаруви органларининг қуйи идоралари бўлган муассаса, ташкилот ва корхоналар билан, шунингдек бевосита аҳоли билан замонавий алоқа ва ахборот воситалари орқали ўзаро фаолияти давомида ахборот хавфсизлигини таъминлаш муҳим ўринни эгаллайди. Ҳозирги вақтда ахборотни сақлаш, қидириш, таҳлил қилиш ва етказиб беришни амалга оширувчи тармоқлар инфокоммуникацион тармоқлар номини олган.

Замонавий инфокоммуникацион технологияларнинг жадал суръатлар билан ривожланиши кўп сонли ва юқори сифатли маълумотлар базасини яратиш, турли базалардан ахборотнинг осон тарқатилиши, нусха олиш ва модификация қилишнинг осонлигини таъминлаш учун кенг имкониятлар яратади. Мустақил республикамизда компьютерлаштиришни ривожлантириш, юқори технологияларни самарали ва сифатли даражада қўллашга катта эътибор қаратилмоқда. Инфокоммуникацион тармоқлар орқали узатиладиган ахборот жамият ривожининг муҳим шартларидан бири бўлиб қолди. У ишлаб чиқариш ресурси, инсонлар орасидаги алоқани

таъминловчи қудратли воситага айланди. Шу сабабли мамлакатимизда компьютер ва ахборот технологиялари, текоммуникация ва маълумот узатиш тармоқларини, Интернет хизматларини ривожлантириш ва замонавийлаштириш, уларни дунё стандартларига етказиш мақсадида кенг кўламли ислоҳотлар босқичма-босқич амалга ошириляпти.Айни вақтда ахборотни криптографик усулда ҳимоя қилиш энг самарали усул ҳисобланади. Шунинг учун ҳам инфокоммуникацион тармоқларнинг ахборот хавфсизлигини таъминлаш усулларини ўрганиш жуда долзарб ҳисобланади.

Тадқиқот объекти ва предметининг белгиланиши

Ушбу магистрлик диссертация ишида тадқиқот объекти сифатида инфокоммуникацион тармоқлар хизмат қилади.

Тадқиқотнинг предмети сифатида эса инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш усуллари ва воситалари хизмат қилади.

Тадқиқот мақсади ва вазифалари

Ушбу магистрлик ишининг асосий мақсади инфокоммуникацион тармоқларнинг ахборот хавфсизлигини таъминлаш усулларини тадқиқ этиш ва юқори даражадаги ҳимояни таъминлайдиган криптографик алгоритмни ишлаб чиқишдан иборат.

Қўйилган мақсадни амалга ошириш учун магистрлик диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

- инфокоммуникацион тармоқларни қуриш принцпларини таҳлил қилиш;

- инфокоммуникацион тармоқларга қўйиладиган талабларни тадқиқ қилиш;

- тармоқлар ахборот хавфсизлигини таъминлаш усулларини ўрганиб чиқиш;

- инфокоммуникацион тармоқларда фойдаланиладиган ахборот хавфсизлигини таъминлаш усуллари ва воситаларини таҳлил қилиш;

- ахборот хавфсизлигини таъминлашнинг криптографик усулларини тадқиқ қилиш;

- инфокоммуникацион тармоқларда ахборотни криптографик ҳимоя қилиш алгоритмини ишлаб чиқиш ва бу алгоритмдан фойдаланиш бўйича тавсиялар шакллантириш.

Тадқиқотнинг асосий масалалари ва фаразлари

Инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш усулларини тадқиқ этиш параметрли функция асосида такомиллаштирилган алгоритм ахборотларнинг ва фойдаланувчиларнинг ҳақиқийлигини белгилаш механизмини аниқлаш имкони мавжудлиги масаласини ҳал этиш имкониятини беради.

Мавзу бўйича қисқача адабиётлар таҳлили

Тадқиқот даврида ҳозирги кунда ахборот хавфсизлигини таъминлаш усуллари ва воситалари ёритилган адабиётлар ўрганиб чиқилди. Шу жумладан, Л.Блахнов, В.Игнатенковнинг “Инфокоммуникационные сети: основы построения” мақоласи, Э.Габидулин, Н.Пилипчук, О.Трушинанинг “Защита информации в телекоммуникационных сетях” мақоласи, В.Зима, А.Молдовян, Н.Молдовяннинг «Безопасность глобальных сетевых технологий» китоби, Б. Шнайернинг «Прикладная криптография», С.Ғаниев, М.Каримов ва К.Ташевнинг «Ахборот хавфсизлиги», Х.Хасановнинг «Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари» каби адабиётлар ва Б.Шнайер, П.Хасанов каби олимларнинг илмий ишлари ўрганиб чиқилди.

Тадқиқотда қўлланилган услубларнинг қисқача тавсифи

Магистрлик диссертация ишида инфокоммуникацион тармоқларни қуриш усуллари ва ахборот хавфсизлигини таъминлашнинг криптографик усулларидан фойдаланилган.

Тадқиқот натижаларининг назарий ва амалий аҳамияти

Ушбу магистрлик диссертация ишида таклиф этилган криптографик алгоритм ва ишлаб чиқилган тавсиялар миллий ахборот коммуникация тизимлари ва ресурсларининг ахборот хавфсизлигини таъминлашда муҳим аҳамиятга эга.

Ушбу магистрлик диссертацияси ишида ишлаб чиқилган алгоритмдан миллий инфокоммуникацион тизимларда, шу жумладан миллий ҳимояланган электрон почта тизимларида фойдаланиш, унинг муҳофазасини оширишга хизмат қилади.

Тадқиқотнинг илмий янгилиги

Мазкур магистрлик диссертацияси натижасида инфокоммуникацион тармоқларда фойдаланиладиган ахборот хавфсизлигини таъминлаш усуллари ва воситалари таҳлил қилинди, инфокоммуникацион тизимларнинг муҳофазасини оширишга хизмат қиладиган криптографик алгоритм ва ундан фойдаланиш бўйича тавсиялар ишлаб чиқилди.

Диссертация таркибининг қисқача тавсифи

Диссертация ишининг ҳажми ва таркиби. Магистрлик диссертация иши кириш, учта боб, ҳулоса, фойдаланилган адабиётлар рўйхати ва иловадан ташкил топган.

I Боб. Инфокоммуникацион тармоқларни яратиш принциплари

1. Инфокоммуникацион тармоқлар архитектурасининг асосий элементлари

Инсоният цивилизацияси ривожланишининг саноатлашган босқичида инсоният трансформациясининг тизимли ташкил этувчи омили тармоқ типидаги инфратузилма ёрдамида очиқ ахборот муҳитида замонавий инфокоммуникация технологияларидан фойдаланиш асосида шакллантириш ҳисобланади. Ахборот муҳити и инфратузилмасининг асосий вазифаси оммавий ахборот алмашинуви ва оммавий коммуникация эркинлигини ва кириш имконияти мавжудлигини таъминлашдан иборат.

Инсоният фоалиятининг барча соҳаларига замонавий ахборот технологияларининг кириб келиши, яъни ахборотни яратиш, тўплаш ва тарқатиш, ҳисоблаш техникаси ва телекоммуникация воситаларининг яратилиши, принципиал янги ва анъанавий инфокоммуникацион тизим ва тармоқларни рақамлаштириш шартли равишда сифатли ўзгариш ва ҳажмларнинг доимий кенгайтириб борилиши давлат ва жамиятнинг иқтисодий, ижтимоий ва сиёсий соҳаларининг ривожланишига имкон яратувчи ресурс ҳисобланади. Шу билан бирга, шуни ҳам ҳисобга олиш керакки, ахборот ресурслари бир қатор ўзига хос хусусиятларга эга.

Инфокоммуникация – бу информацион ва телекоммуникацион технологияларнинг бир бутун бўлиб ривожланишини ўзида мужассам этувчи иқтисодиётнинг янги тармоғидир [1]. Инфокоммуникацияларда алоқа технологиялари турли хилдаги ихтиёрий узоқликдаги *ахборот узатиш воситаси сифатида* фойдаланилади.

Ахборотни сақлаш, қидириш, қайта ишлаш ва узатишни амалга оширувчи тармоқлар инфокоммуникацион тармоқлар (ИТ) номини олган. Информацион жараён ахборотларнинг ўзаро боғланган ва ўзаро шартланган

жараёнларини намоён қилиш, танлаш ва шакллантиришни жамлайди ҳамда уларни техник тизимга киритади, таҳлил қилади, қайта ишлайди ва сақлайди.

Инфокоммуникацион тармоқ аввал “информацион тармоқ”, “компьютер тармоғи” ва бошқа номлар билан аталган [4]. Электр алоқа интеграцияси ва информатизация воситалари жараёнлари телекоммуникацион тармоқларнинг инфокоммуникацион тармоқларга айланишига имконият яратиб бермоқда.

Инфокоммуникацион тармоқлар фойдаланувчиларга ахборот алмашиниш, у билан таъминланиш, қайта ишлаш, сақлаш ва тўплаш билан боғлиқ хизматлар кўрсатиш учун мўлжалланган. Информацион тармоққа кириш имконияти мавжуд ахборот истеъмолчиси информацион тармоқ фойдаланувчиси (user) ҳисобланади. Жисмоний шахслар ҳам, юридик шахслар (фирмалар, ташкилотлар, корхоналар) ҳам фойдаланувчи сифатида чиқишлари мумкин.

Компьютер тармоқларида алмашинадиган электрон маълумотларни бузғунчилардан ҳимоялаш ва тармоқларда махфий маълумотлар алмашиш учун муҳофазаланган канални ташкил этиш муҳим масалалардан бири ҳисобланади. Вақт ўтиши билан бир биридан узоқ масофада жойлашган тармоқларни ҳам бир-бири билан боғлаш зарурияти туғилди. Шундай қилиб, *тармоқлар ўртасидаги тармоқ* (таржимаси: inter - *орасида* ёки *ўртасида*, net - *тармоқ*) бўлмиш Интернет пайдо бўлган, яъни Интернет локал тармоқларни битта глобал тармоққа бирлаштиради [5].

Телекоммуникация ва ахборот технологияларини ягона тармоққа интеграциялаш, яъни инфокоммуникациялаш – телекоммуникацион тармоқларни ривожлантириш ва унинг асосида глобал ахборот хизматлари сонини кенгайтиришга йўналтирилган умумжаҳон ғоясидир. Тармоқнинг хизмат кўрсатиш платформаларини ташкил қилувчи турли хил элементларнинг ўзаро ташкиллаштирилиши қоидаларини билиш тармоқ ресурслари билан ўзаро мослашиш имконини беради.

Тармоқ хўжалик фаолиятини бошқариш, унинг ривожланишини режалаштириш учун тармоқ маъмурияти тармоқнинг ташкилий тузулмасини, тармоқ хизматлари тузилмасини, бошқарув, хизмат кўрсатиш, таъминлашни ва ҳ.к. ни таҳлил қилиши лозим.

Шунингдек, тармоқ қуриш вазифаси топширилган тармоқ яратувчиси юқорида кўрсатиб ўтилган жихатларини ўзида муассам эта олиши лозим. Яъни, унга тармоқ архитектурасига оид билимлар зарур.

Тармоқ архитектураси деб тармоқнинг барча элементлари турли кўринишини, улар орасидаги алоқаларни ва ўзаро ҳаракат қоидаларини кўрсатиб берувчи тизимли тавсифи тушунилади [3]. Тизимли тавсиф деб модел кўринишидаги объектнинг кўп даражали тавсифи тушунилади, уларнинг ҳар бири объектни кўрилаётган аниқ бир жиҳатда акс эттиради (абстрактлаштириш даражаси). Юқорида айтиб ўтилган глобал ахборот инфратузилманинг бир қисми ҳисобланган ҳар қандай электралоқа тармоғини инфокоммуникацион тармоқ структураси сифатида қўриш мумкин (1.1-расм).

1.1-расм. Инфракоммуникацион тармоқнинг тузилиши

Транспорт тармоқларининг асосий вазифалари ўз ичига турли хил объектлар (тармоқ тугунлари) орасида ахборот оқимларининг қўчишини олади. Кириш имконияти мавжуд тармоқлар аниқ фойдаланувчиларнинг

терминал ускуналарига ахборот оқимини индивидуал равишда етказиб беришни таъминлайди, яъни хизмат кўрсатувчи боғлама интерфейси билан ҳар бир фойдаланувчининг тармоқ интерфейси ўртасида ахборот узатади. Кириш ва тармоққа кириш тушунчалари кенг маънога эга бўлиб, улар тармоқ ёки қурилманинг тавсифини, алоқа воситаларининг ўрнатилиши жойини аниқлаши ҳамда компьютер хотирасидан маълумотларни чиқаришни ва ҳ.к.ни аниқлаши мумкин. Транспорт тармоқлари ҳамда кириш тармоқлари биргаликда ўзида миллий, регионал ва маҳаллий инфокоммуникацион тармоқларни мужассам этади. Инфокоммуникацион тармоқларни электралоқа тармоқларига (аслида ҳам маълумотлар узатишни амалга оширади) маълумотларни сақлаш, узатиш ёки қайта ишлаш учун қўйилган ахборот тизимлари сифатида ҳам кўриш мумкин.

Модель – бу объектнинг шундай тасвирики, унда объектнинг асосий элементларини бошқа аҳамиятсиз нарсаларга чалғимасдан қўйилган мақсад сари ўрганиш имконини беради. Абстрактлаштириш даражаси одатда иерархик тартибда (катталарга бўйсунган ҳолда) амалга оширилади [3].

Тармоқнинг мураккаб тизим (унинг архитектураси тавсифи) сифатидаги моделли тавсифини фақатгина ягона йўл билан амалга ошириш мумкин –ажратиб кўрсатилган бирон бир тармоқ даражасини кўриб чиқиш аниқ бир гуруҳлар ўртасида ўзаро тасвирланган элементларнинг кўпгина тизимларини бўлиш орқали аниқланади.

Шундай қилиб, архитектура кенг қамровли тушунча бўлиб, тармоқнинг турли тизимлари ўртасидаги боғлиқликни тавсифлайди: жойларни (топологияни) бирлаштирувчи чизиқлар конфигурацияси; тармоқ қурилмасини тасвирловчи ташкилий тузилма; тармоқ иши мантиқини тушунтирувчи функционал тузилма; тармоқ таркибининг мураккаб ва кўп тармоқли дастурий таъминотини тавсифлайдиган дастурий тузилма; алоқа ўрнатиш қоидаларини тасвирловчи ва ахборот алмашинувини таъминловчи тармоқнинг протоколга оид модели; тармоқнинг физик ресурсларини ва

фойдаланилаётган қурилмалар типини баҳолашга имкон берувчи физик тузилмадир.

Замонавий ИТ – бу ўзида ахборотни қайта ишлаш ва алмашиш аппарат-дастурий воситалари ҳамда минтақавий тақсимланган информацион тугунлардан ташкил топган (ахборотни қайта ишлаш қуйи тизими) ва ИТ нинг физик тузилмасини ўзида жамловчи ахборот узатишнинг физик каналларини мужассам этган маконда мураккаб равишда тақсимланган технологик тизимдир [3].

ИТ умумлаштирилган архитектурасининг асосий элементларига қуйидагилар киради:

• кириш тармоқлари орасидаги оқимларни тақсимлаш йўли билан хабарлар оқимини уларнинг манбаларининг бир кириш тармоғидан хабарларни қабул қилувчи бошқа кириш тармоғига кўчириш (транспортировка) вазифасини бажарувчи электралоқа тармоғининг қисмини ўзида мужассам этувчи рақамли алоқа транспорт тармоғи;

• кириш тармоғи ва алоқа транспорт тармоғи орасида чегарадош бўлган хабар жўнатувчининг (қабул қилувчининг) фойдаланиш ускунасини кириш тугунига улашни таъминловчи абонент кириш тармоғи;

• чақирув (сеанс) ва хизматларни бошқаришни амалга оширувчи, шунингдек, анъанавий (мавжуд) алоқа тармоқлари ва турли алоқа операторлари тармоқлари билан ўзаро алоқа қилишда керак бўладиган интерфейс ва протоколларнинг қайта ўзгартирилишини амалга оширувчи компонентлар.

Протокол деганда электралоқа тармоғи элементларининг ўзаро ҳаракатини регламентловчи қонунлар (процедуралар) жамланмаси тушунилади [-].

Бундай кўптарафлама тармоқ тадқиқотини тизимли ёндашиш нуқтаи назардан системологиянинг (катта (мураккаб) тизимларни ўрганувчи билимлар) методология принципига асосланган ҳолда ўтказиш лозим.

Алоқа тармоғи мураккаб тизимларнинг барча белгиларига эга бўлиб, уларга хос бўлган қонунийликка бўйсунади. Улардан баъзиларини кўрсатиб ўтамиз.

Иерархиялик – бутун бир элемент қисмлари ва элементларининг юқоридан пастга тартибида жойлашувидир. Бу қонунийликка кўра биз тармоқни алоҳида қуйи тармоқлар (сегментлар)га бўлишимиз мумкин [7].

Коммуникативлик – тизимнинг кўпгина алоқалари (коммуникациялари) кўрсатилган қонунийликдир: ташқи – муҳит билан ва ички – қуйи тизим элементлари билан. Бу шуни билдирадики, ҳар бир алоқа тармоғини қуйи тармоқ (қуйи тизим) ёки янада юқори тартибдаги (масалан, Глобал Ахборот Инфратузилмаси элементи сифатида) тизим элементи сифатида кўриб чиқиш мумкин, шу билан бирга у ўзига қуйи тизимларни (сегментлар) қўшувчи алоҳида мустақил тизим сифатида кўриш мумкин.

Эмержентлик – тизим томонидан яхлит сифат – бутунликни ўз ичига олувчи қонунийликдир, унинг алоҳида элементларига бу хос эмас. Масалан, алоқа тармоғида биз функционал муҳим ва нисбатан мустақил қуйи тизимларни ажратиб кўрсатишимиз мумкин, яъни транспорт тизими, ахборотни тақсимлаш тизими, тармоқни бошқариш тизими. Ҳеч бир алоқа тармоғини тўлалигича санаб ўтилган тизимлар билан таққослаб бўлмайди, фақатгина улар орасидаги ўзаро боғлиқлик ушбу тушунчани кўрсатиб беради. Бошқа тарафдан эса, алоҳида қуйи тизимларни кўриб чиқиш ва ўрганиш натижасида биз турли жиҳатларда тизим тушунчасини кўриб чиқдик.

Архитектура тушунчаси тармоқ қурилмаси тўғрисидаги тўлиқ тушунчани ифодалайди, демак унинг эмержентлигини кўрсатади.

Юқорида келтирилган қонунийликларига кўра, ҳар бир мураккаб тизимли қуйи тизимни унинг архитектурасига хос бўлган эмержентлик хоссаларини тасвирловчи мустақил тизим сифатида кўриш мумкин. Шундай қилиб, тизимларнинг иерархик тақдим этилишини кўриб чиқиш даражасига кўра биз тармоқ архитектураси, терминал комплекс архитектураси,

коммутацион тизим архитектураси, ҳисоблаш машинаси ҳамда алоҳида интеграл схема тўғрисида тўлиқ гапиришимиз мумкин.

Тармоқ архитектурасини тавсифлаш учун модель тушунчасининг турли усуллари қўлланилиши мумкин. Масалан, тармоқ топологиясини қуйи тизим ва элементларининг ўзаро ҳаракатини тасвирлаш учун жадвалли моделлардан фойдаланилади, тармоқнинг дастурий таъминоти ишини тасвирлаш учун алгоритмли моделдан фойдаланилади.

Тармоқнинг умумий кўриниши ва деталлаштирилган кўриниши турли хил даражадаги элементларнинг ўзаро ҳаракати қоидаси одатда тармоқ тасвирининг кўп даражалилиги протоколига оид модель сифатида тасаввур қилинади.

2. Инфокоммуникацион тармоқларга қўйиладиган ўзига хос талаблар

Инфокоммуникацион хизматларда одатда ахборотни мультимедиа кўринишида узатиш режалаштирилади, у эса ўз навбатида узатишнинг юқори тезлиги ҳамда ахборот оқими кириши ва чиқишининг носимметриклиги билан тавсифланади. Кўпгина инфокоммуникацион хизматлар «иловалар» ҳисобланади, яъни уларнинг вазифалари хизмат билан таъминлаш ускуналари ҳамда фойдаланувчининг сўнгги ускуналари ўртасида тақсимланади. Хулоса қилиб шуни айтиш керакки, сўнгги ускуналар вазифаларини ҳам инфокоммуникацион хизматлар таркибига киритиш лозим, ва буни уларнинг регламентациясида ҳисобга олиш зарур.

Бизнес-модель – инфокоммуникацион хизматларни тақдим этиш жараёни қатнашчиларини ва улар ўртасидаги ўзаро муносабатни аниқлайди, шунингдек анъанавий электралоқа хизматлари моделидан фарқ қилади [1]. Анъанавий электралоқа хизматлари модели кўрсатиб ўтилганидек атиги учта иштирокчидан иборат: оператор, абонент ва фойдаланувчи. Янги ишбилармон модел ўзида хизмат билан таъминлашни мужассам этган бўлиб,

у абонент ва фойдаланувчиларга инфокоммуникацион хизматларни тақдим этади. Шу билан бирга таъминотчи алоқа тармоғи оператори томонидан тақдим этиладиган кўчириб ўтиш хизмати истеъмолчиси ҳисобланади. Бозорда хизматлар билан таъминлашнинг бошқача кўринишлари ҳам бўлиши мумкин: *ахборот таъминотчиси, брокерлар, ретейлерлар* ва бошқалар [1].

Ахборот таъминотчиси хизмат таъминотчисига ахборотни тарқатиш учун тақдим этади.

Брокер хизмат таъминотчиси ва уларнинг потенциал абонентлари тўғрисидаги ахборотни тақдим этади ҳамда фойдаланувчиларга улар талаб қилган хизматни кўрсатувчи хизмат таъминотчиларини топишга ёрдам беради.

Ретейлер фойдаланувчининг индивидуал талабларига хизматни мослаштириш мақсадида хизмат таъминотчиси ва фойдаланувчи ўртасида воситачи сифатида туради.

Инфокоммуникацион хизматларга қуйидаги талаблар қўйилади:

- *чаққонлик;*
- *янги хизматларга мослашувчанлик ва тез яратувчанлик;*
- *кафолатланган сифат.*

Инфокоммуникацион хизматларга қўйиладиган талабларга катта таъсир асосан конвергенция жараёнида содир бўлади, у эса ўз навбатида инфокоммуникацион хизматларнинг кириш усулидан қатъий назар фойдаланувчи учун ҳамёнбоп бўлишига олиб келади.

Инфокоммуникацион хизматларнинг кўриб чиқилган афзалликларини эътиборга олган ҳолда, алоқа тармоғи истиқболига қўйиладиган қуйидаги талабларни аниқлаш мумкин [1]:

- *«мультисервислик»*, ушбу атама хизмат кўрсатиш технологияларининг транспорт технологияларидан мустақил хусусиятга эга эканлигини ифодалайди;

- *«кенгполосалилик»*, ушбу атама фойдаланувчининг жорий эҳтиёжларидан келиб чиқган ҳолда ахборот узатиш тезлигини кенг диапазонда мослаштириш ва динамик ўзгартириш имкониятини ифодалайди;
- *«мультимедиялилик»*, ушбу атама тармоқнинг *реал вақтда ушбу компонентларни керакли синхронизация билан* ва уланишнинг мураккаб конфигурацияларидан фойдаланиб кўп компонентли ахборотни (нутқ, маълумотлар, видео, аудио) узатиш имкониятини ифодалайди;
- *«интеллектуллилик»,* ушбу атама фойдаланувчи ёки хизмат таъминотчиси томонидан хизматни, чақирувларни ва уланишларни бошқариш имкониятини ифодалайди;
- *«кириш инвариантлиги»,* ушбу атама фойдаланаётган технологиядан қатъи назар ташкилотнинг хизматига кириш имкониятини ифодалайди;
- *«кўп операторлилик»*, ушбу атама хизмат кўрсатилаётган жараёнда бир нечта операторнинг иштирок этиши ва уларнинг фаолияти доирасига кўра жавобгарликларини бўлиб ташлаш имкониятини ифодалайди.

Бундан ташқари, преспектив мультисервис тармоқларига қўйиладиган талабларни шакллантиришда хизмат таъминотчиси фаолиятининг ўзига хос хусусиятларини ҳам назарда тутиш лозим [1]. Жумладан, уланишда хизматлар регламентациясига замонавий ёндашишда хизмат таъминотчиларининг киришлари назарда тутилган, ҳамда ўзининг хусусий инфратузилмасига эга бўлмаган фойдаланувчиларга ҳам умумий фойдаланишдаги тармоқ ресурсларига *камситишларсиз* киришга йўл қўйиш назарда тутилган.

Шу билан бирга, хизмат таъминотчиси томонидан тармоқ муҳитига қўйиладиган асосий талабларга қуйидагилар киради:

- ускуналарни «мультиоператор» муҳитида ишлаши имкониятини таъминлаш, шу билан бирга кириш даражасида ҳам тармоққа бир онда бир нечта алоқа операторларини улаш учун интерфейс сонини кўпайтириш;

- хизматни ҳамкорликда тақдим этиш учун хизмат таъминотчилари боғламаларининг ўзаро ҳаракатини таъминлаш;
- ускунанинг мақбул бошланғич нархида «кенг кўламли» техник ечимларни қўллаш имконияти.

Ҳозирги вақтда коммутация каналлари ва коммутация пакетлари билан умумий фойдаланишдаги мавжуд алоқа тармоқлари юқорида кўрсатиб ўтилган талабларга жавоб бермайди. Анъанавий тармоқларнинг чекланган имкониятлари янги инфокоммуникацион хизматларни жорий қилиш йўлини тўхтатиб қўйган омил ҳисобланади. Бошқа тарафдан эса, тақдим этилаётган инфокоммуникацион хизматларнинг ҳажмини ошириш мавжуд алоқа тармоқларининг базали хизмат чақирувларига хизмат кўрсатиш сифати кўрсаткичларининг салбий тарафга ўзгаришига олиб келади.

Буларнинг барчаси мультисервис тармоқларини яратиш йўналишида анъанавий алоқа тармоқларини ривожлантириш усулларини режалаштираётганда инфокоммуникацион хизматларнинг мавжудлигини ҳисобга олишга ундайди.

Юқорида келтирилганларга асосланган ҳолда инфокоммуникацион тармоқларга қўйиладиган ўзига хос талабларни қуйидагича шакллантириш мумкин:

- кенг миқёсдаги хизматларни уларнинг ҳимояси, бошқарилиши ва кўпайтирилиши бўйича мослашувчан имкониятлари билан тақдим этиш;
- тармоқнинг стационар ва мобиль компонентлари учун тақсимланган коммутация билан тармоқ ечимларини унификациялаш ва алоқа транспорт тармоғининг универсаллигини таъминлаш;
- охирги тармоқ боғламаларидаги хизмат кўрсатиш функцияларини амалга ошириш;
- анъанавий тармоқлар ва алоқа хизмати билан интеграция ва конвергенция;

- мултисервислилик, тармоқ хусусияти сифатида ҳамда унинг асосида иккита ва кўпроқ электралоқа хизматларини ташкиллаштиришга имкон яратиши сифатида;
- кенг полосалилик, фойдаланувчининг жорий талабларидан келиб чиққан ҳолда кенг диапазонда маълумотларни узатиш тезлигини мослаштириш ва динамик ўзгартириш имконияти сифатида;
- мультимедиялик, тармоқнинг реал вақтда кўп компонентли ахборотни (нутқ, маълумотлар, видео, аудио) керакли синхронизация билан ҳамда уланишнинг мураккаб конфигурацияларидан фойдаланган ҳолда узатиш имконияти сифатида, шунингдек, ускунанинг минимал бошланғич нархида «кенг кўламли» техник ечимларни қўллаш имконияти сифатида;
- интеллектуаллик, фойдаланувчи ёки хизмат таъминотчиси томонидан хизматни, чақирувларни ва уланишларни бошқариш имконияти сифатида, ҳамда хизматни ҳамкорликда тақдим этиш учун хизмат таъминотчилари боғламаларининг ўзаро ҳаракатини таъминлаш;
- кириш инвариантлиги, фойдаланаётган технологиядан қатъи назар ташкилотнинг хизматига кириш имконияти сифатида;
- кўп операторлилик, хизмат кўрсатилаётган жараёнда бир нечта операторнинг иштирок этиши ва уларнинг фаолияти доирасига кўра жавобгарликларини бўлиб ташлаш имконияти сифатида;
- абонент терминаллари ва ахборот хизматлари серверларининг кенг номенклатурасини уламоқ;
- инфокоммуникацион хизмат тақдим этувчи хизмат ва хабарларни ташувчи хизмат орасидаги технологик мустақилликни таъминлаш.

3. Тармоқларнинг функционал имкониятлари

ИТ функционал имкониятлари ва мос равишда унинг функционал архитектураси асосан хизмат сифатининг берилган параметрлари бўйича турли кўринишдаги ахборотларни узатишда фойдаланувчиларнинг (амалий

жараёнларнинг) талаблари асосида аниқланади. Замонавий ИТ функционал архитектурасини қуриш асоси ўзаро боғланган протоколлар (стандартлар) рўйхати ва ИТда ўзаро алоқа функцияларини амалга оширишни таъминлашни ўзида акс эттирган протоколлар профили ҳисобланади.

Ҳозирги вақтда “де-факто” ёки “де-юре” халқаро стандартлар ҳисобланган бир қатор турли архитектуралар мавжуд, улар орасида қуйидагиларни ажратиб кўрсатиш мумкин [1]:

• Интернет тармоқлари архитектураси;

• IBM корпорациясида яратилган SNA (Systems Network Architecture) тизимли тармоқ архитектураси ва SAA (Systems Application Architecture) тизимли амалий архитектураси;

• IBM томонидан тақдим этилган BNA (Broad Network Architecture) кенг полосали тармоқ архитектураси;

• DEC фирмасининг DNA (Digital Network Architecture) рақамли тармоқ архитектураси;

• British Telecom фирмасининг ONA (Open Network Architecture) очиқ тармоқли архитектураси ва бошқалар.

ИТ учун тармоқнинг ҳудудий тақсимловчи тугунларида ахборотни мазмунли қайта ишлаш функциясини бажарувчи информацион жараёнларнинг ўзаро ҳаракатида фақат очиқ тизимлар ўзаро алоқаси (ОТЎА) функциясини амалга оширишга мўлжалланган, батафсил ишлаб чиқилган ва стандартлаштирилган архитектурасига намуна бўлиб етти даражали архитектураси очиқ тизимларининг ўзаро алоқаси эталон модели (ОТЎА ЭМ) ҳисобланади [1].

Турли даражадаги эталон моделлари томонидан амалга оширилувчи ОТЎА ЭМ ва функциялари ўзининг мазмунига кўра барча мавжуд тармоқли архитектураларни умумлаштиради.

Замонавий тармоқларни ташкиллаштиришнинг асосий функционал принципларига хизмат кўрсатишни ташкиллаштириш принципи киради. Уни амалга ошириш эса қуйидаги талабларни шакллантиришни талаб этади:

• кўчириш хизматлари ва телехизматлар;

• тармоқли ахборот ресурсларига кириш хизматлари (ахборот-маълумот берувчи хизматлар);

• сигнализация тизимлари;

• рақамлаш ва адреслаш тизимлари;

• синхронлаштириш тизимлари;

• бошқариш тизимлари.

Глобал ахборот инфратузилмаси (ГАИ) нинг асосий компонентларига қуйидагилар киради:

• ўзида қайд қилинган тармоқни ҳамда мобиль тармоқни мужассам этган B-ISDN кўринишдаги транспорт тармоғи;

• хизматлар маълумотлар базаси;

• кириш тармоғи;

• фойдаланувчиларнинг кўп функцияли юқори тезликли терминаллари.

ГАИ ўзида дунё миқёсида янги авлоднинг телекоммуникация ва ахборот хизматлари саноатини ривожлантириш бўйича комплекс ечимини акс эттирган. ГАИни бир қатор базали технологиялар композицияси кўринишида кўриб чиқиш мумкин, уларни ГАИ концепцияси доирасида интеграциялаш фаолият шароити ва инсоният ҳаётининг ижобий тарафга ўзгаришини тахмин қилади.

ГАИ базали технология пакети ўзида кейинги саноат кўринишларини мужассам этади:

• компьютер;

• телекоммуникация;

- маиший электрон асбоблар (consumer electronics);
- ахборот иловалари ёки хизматлари, шунингдек уларни сермазмун хизматлар ёки иловалар саноати деб ҳам аташ мумкин (content or application industry).

Шу билан бирга ГАИ концепцияси талабларини қондирувчи базали технологиялар комбинациясининг ўзига хослиги – бу уларнинг келишилганлиги, бутунлиги ва тугалланганлигидир, яъни технология маълумотлар комбинацияси охирги фойдаланувчига хизмат (сервис) кўрсатишнинг тугалланган сценарийсини аниқлайди.

Ҳозирги вақтда ГАИ технологияларининг яратилиши стандарти ва принципларини ишлаб чиқиш бўйича кучли халқаро кооперация шакллантирилган. ГАИни стандартлаштириш бўйича кенг кўламдаги ишлар дастури ишлаб чиқилган, у ўзида жадал суръатлар билан амалга оширилиши лозим бўлган бир неча ўнлаб устувор лойиҳаларни қамраб олган. ГАИни ҳаётга татбиқ этишнинг умумий стратегияси ривожланишнинг эволюцион йўлини талаб қилади, яъни ГАИнинг мавжуд тизим ва технологияларини янги принцип ва стандартлар базасида изчиллик билан модернизация ва интеграция қилиш асосида қуриш. Жумладан, ГАИнинг потенциал хизматлари бўлиб замонавий телефония хизматлари, маълумотлар узатиш хизматлари ва Интернет тармоғининг иловалар хизмати бўлиши мумкин.

Айни вақтда ГАИнинг бир қатор таърифлари мавжуд. ГАИ деганда телекоммуникацион ва ахборот сервисларининг (хизмат) глобал интеграциялашган муҳити тушунилади, улар қуйидагиларни ифодалайди [9]:

- ГАИ хизматларининг маконда узлуксиз ва вақт бўйича физик имкониятларининг мавжудлиги, яъни ГАИ га ҳоҳлаган вақт ва дунёнинг барча жойларидан кириш имкониятининг мавжудлиги;
- махсус информацион кириш/чиқиш янги авлод ИА (Information Appliances) ускуналаридан (қурилма, терминаллар) фойдаланиш натижасида ГАИга киришнинг техник осонлиги;

- ГАИ хизматларининг ҳамма учун қулайлиги, энг аввало хизматнинг нархи бўйича, бу эса ўз навбатида ҳар бир одамга маъқул бўлган нархда ГАИнинг ахборот ва телекоммуникация сервисларига осон уланиш имкониятини яратади;
- ГАИ хизматидан фойдаланишда хизмат кўрсатишнинг талаб қилинадиган сифатини ва ахборот ҳимоясини таъминлашни кафолатлаш;
- Барча мавжуд ахборот кўринишларини ўз ичига олувчи тақдим этилаётган амалий хизматлар ассортиментининг кенглиги: аудио, видео, график, динамик графика, маълумотлар, ҳужжатлар, гипермультимедия;
- ўзаро бир-бири билан ипсиз боғланган коммуникацион тармоқ, компьютер ускуналари, информацион маълумотлар базаси ва информацион терминалларга асосланган ГАИ ресурсларига киришни бошқаришнинг умумий принциплари бўйича халқаро келишувга етишиш асосида функциялаштириш.

ГАИ хусусиятларини тасвирлаш ва таҳлил қилиш учун бир неча моделлар тўпламидан фойдаланилади, улар ёрдамида эса тадқиқот объекти ҳар хил нуқтаи назардан кўриб чиқилади. ГАИнинг бир нечта модель кўринишларини кўриб чиқамиз.

ГАИ ўзида жуда ҳам мураккаб комплекс технологияни мужассам этган. Ушбу муаммони ўрганаётган мутахассислар шундай хулосага келдиларки, ГАИ технологиясини таснифлаш учун фақатгина ягона эталон моделдан фойдаланишни тасаввур қилиб бўлмайди [1]. Шунинг учун ҳам хусусиятлари, хизматлари, функционаллаштириш принциплари, ташкилий тузилмалари ва бошқа жихатлари мақсадларини таснифлаш учун ГАИда бир қатор турли хил моделлардан фойдаланилади.

ГАИнинг фойдаланишдаги энг кенг тарқалган моделларидан бўлиб, унга атроф муҳитни хаёт билан тўлдирувчи манба сифатида қаралади ва у қуйидаги асосий вазифаларни амалга оширади:

- информацион, коммуникацион, муаммоли-йўналтирилган хизматлар, жумладан, электрон почта, видеоконференция, телемаркетинг,

телемедицина, масофали ўқитиш ва ҳ.к. каби амалий сервисларни жамлаш ва интеграциялаш;

- ГАИ сервислари ва ресурсларига турли хил терминаллар, маълумотларни киритиш/чиқариш қурилмалари, коммуникацион қурилмалар, ахборотни қайта ишлаш қурилмаси, ҳамда уларнинг комбинацияларидан фойдаланган ҳолда истеъмолчининг вақти ва жойидан қатъий назар кафолатланган шахсий кириш билан таъминлаш;
- ГАИ функционаллаштиришни қўллаб-қувватлаш учун керакли барча ташкилий-технологик жиҳатлар.

Шу билан бирга ГАИ тармоқли инфраструктураси компонентлари ягона қамраб олинган телекоммуникацион муҳитга интеграциялаштирилган турли типдаги замонавий тармоқ технологиялари бўлиши мумкин. Масалан, ГАИнинг тармоқли компонентларига хизматлар интеграцияси билан боғлиқ рақамли тармоқнинг қисқа полосали ва кенг полосали тизимлари (N-ISDN, B-ISDN); пакетли коммутация тармоқлари (PSDN); кабелли телевидение тармоғи (CATV); замонавий локал тармоқ технологиялари (LAN) ва бошқаларни киритиш мумкин [1].

ГАИни янада батафсил тасвирлаш учун функционал декомпозиция (физик тасвирига қарама-қарши) методидан фойдаланилади, бу метод орқали ГАИнинг функционал тузилмаси (Punctional structure of the ГАИ) аниқланади, у ўз навбатида қуйидаги функционал даражалардан ташкил топган:

- тармоқли инфратузилма (Network infrastructure) – энг қуйи даража;
- дастурий таъминот – ўрта даража (Middleware);
- иловалар даражаси – юқори даража (Application) .

Тармоқли инфратузилма турли хилдаги ахборотлар, шу жумладан маълумотлар, матн, факсимиль хабарлар, аудио ва видео ахборотлар,

ҳужжатлар, гипермультимедия, график образлар, турли хил информацион контейнерлар транспортировкаси учун ишончли сервисни тақдим этади. У фойдаланувчиларнинг ГАИ ресурсларига кириш имкониятини яратувчи турли хилдаги тармоқ типларидан қурилади. ГАИ инфраструктурасига интеграцияланган тармоқлар ўзининг хусусий, янада чуқурлаштирилган тузилишига эга бўлиши мумкин. ГАИ тармоқли инфратузилмаси ўзида фойдаланувчи тармоғи деб номланувчи охирги тармоқ фойдаланувчиларини ҳам қамраб олган.

Ўрта даража ўзида кўпгина иловалар томонидан фойдаланиладиган универсал сервисларни амалга оширувчи функцияларни қамраб олган. Ўрта даража дастурий таъминотининг ўзига хос вазифаларига ахборотни ҳимоялашни таъминлаш воситалари, маълумотнома хизмати, номлар хизмати, маълумотларни бошқариш сервиси, хизмат кўрсатиш таннархини ҳисоб-китоб (биллинг) қилиш ва ҳ.к.ни киритиш мумкин.

Иловалар даражаси ўзида фойдаланувчига тақдим этиладиган ва ГАИнинг асосий вазифаси ҳисобланган тармоқли ва информацион муаммоли-йўналтирилган хизматлар (сервис)нинг кенг спектрини қамраб олган. Тармоқ ресурслари ахборот, маълумотларни қайта ишлаш ва сақлаш, дастурий ва коммуникацион қисмларга ажратилади [2].

Ахборот ресурслар – бу илмнинг барча жабҳаларида, жамиятнинг маданияти ва ҳаётида тўпланадиган ахборот ва билимдир, шунингдек кўнгил очиш индустрияси маҳсулоти ҳисобланади. Буларнинг барчаси тармоқ фойдаланувчилари ўзаро ҳаракатини амалга оширадиган тармоқлараро маълумотлар базасида системалаштирилади. Ушбу ресурслар информацион тармоқнинг истеъмол қийматини аниқлайди ва фақат доим яратилмасдан ва кенгайтирилмасдан, балки вақтида янгиланиши, бунда эски маълумотлар архивга жўнатилиши лозим. Тармоқдан фойдаланиш муҳим ахборотни керак бўлган ҳолда олиш имкониятини таъминлайди.

Маълумотларни қайта ишлаш ва сақлаш ресурслари тармоқ компьютерлари процессорларининг ишлаш тезлиги ва хотира

қурилмаларининг ҳажми билан, шунингдек улардан фойдаланиш вақти билан аниқланади. Тармоқ компьютерлари сервер деб номланади. Серверлар файлли, хизматларни бошқариш пунктлари ва бошқа турларга бўлинади.

Дастурий ресурслар ўзида фойдаланувчиларга хизмат кўрсатишда иштирок этувчи дастурий таъминотни, шунингдек, функциялари билан боғлиқ дастурларни мужассам этади. Уларга қуйидагиларни киритиш мумкин: ҳисоблар тўғрисида маълумотнома, хизматлар ҳақини рўйхатга олиш, навигация (тармоқда ахборот қидирувини таъминлаш), тармоқлараро электрон почталарга хизмат кўрсатиш, телеконференцияни ташкиллаштириш, узатилаётган информацион хабарлар форматларини қайта тиклаш, ахборотни криптоҳимоялаш (кодлаш ва шифрлаш), аутентификация (ҳужжатларнинг ҳақиқийлигини тасдиқловчи электрон дастхат)..

Интернет тармоғига фақат кабель ёки телефон линияси орқали симли уланиш, балки мобил алоқа воситалари ёрдамида симсиз уланиш ҳам мумкин. Интернет тармоғига симсиз уланиш компьютер орқали ёки мобил телефоннинг ўзида амалга оширилади (1.2-расм) [10].

1.2-расм. Мобил алоқа тармоқларида Интернетга уланиш

Интернет – ахборотга эга бўлиш, янгиликлар билан танишиш, билимга эга бўлиш, ўқиш, илғор технологиялар ва тажрибалар билан танишиш, иш муносабатларини тезда ҳал қилиш, шерик ва буюртмачиларни назорат қилиш, истеъмолчининг талаби ва муаммоларини билиш, маҳсулот баҳосини

назорат қилиш имкониятларини беради. Хулоса қилиб айтганда, Интернет тармоғидан ахборотлар алмашиниш, масофавий таълим олиш, конференциялар ўтказиш, веб-сайтларни ташкил этиш, электрон почтани жорий қилиш, мулоқот ўрнатиш ва шу каби мақсадларда фойдаланилади.

Қуйидаги 1.3-расмда ўзида асосий компонентларни мужассам этувчи интеллектуал тармоқ архитектураси келтирилган: хизматлар коммутацияси тугуни, хизматларни бошқариш тугуни ва хизматларни бошқариш тизимлари [2].

1.3-расм. Перспектив интеллектуал тармоқ архитектураси

Коммутация хизматлари тугуни электралоқа тармоғи фойдаланувчиларининг интеллектуал тармоқ хизматларига киришини таъминлайди. Ушбу элементнинг асосий функцияси интеллектуал тармоқ билан боғлиқ хизматларга буюртмаларнинг мавжудлигини аниқлаш ҳисобланади. Коммутация хизматлари тугуни буюртмани аниқлагандан сўнг қайта ишлашни тўхтатиб туради ва сигнализация тармоғи орқали уни қайта ишлашни давом эттириш учун йўриқнома кутади. Коммутация хизматлари тугуни функциялари унверсал бўлиши лозим ва буюртма қилинаётган хизмат кўринишига тобе бўлмаслиги керак.

I боб бўйича ҳулосалар

Ахборот муҳити инфратузилмасининг асосий вазифаси ахборотларнинг оммавий алмашинуви ва оммавий коммуникацияларнинг эркинлигини ва фойдаланиш мумкинлигини таъминлаш ҳисобланади. Тармоқ инфратузилмасининг транспорт асоси эса – илмий телекоммуникацион тармоқлар турли хил депозитарийлар, ахборот манбалари, ахборот манбалари ва истеъмолчининг турли хил тўпламларини ўзаро бирлаштириб, инфокоммуникация тизимларини ва турли хил функционал вазифаларни бажарувчи тармоқларни ташкил этади, улар биргаликда глобал тармоқнинг миллий сегментини ҳосил қилади.

Инсон фаолиятининг барча соҳаларига ахборот яратиш, тўплаш ва тарқатишнинг замонавий технологияларини, ҳисоблаш техникаси ва телекоммуникация воситаларини жорий қилиш, мутлоқо янги инфокоммуникация тизимлари ва тармоқларини яратиш ҳамда анънавийларини рақамлаштириш ахборотнинг бундай тизимларида ва тармоқларида айланувчи ҳажмларни сифат жиҳатидан ўзгартиришни ва доимо кенгайтириб боришни шарт қилиб қўяди, у жамиятнинг ва давлатнинг иқтисодий, ижтимоий ва сиёсий ривожланиши учун муҳим ресурс бўлиб қолади.

Ҳозирги вақтда каналлар коммутацияси ва пакетлар коммутацияси билан мавжуд умумий фойдаланиш алоқа тармоқлари замон талабларига жавоб бермайди, чунки одатдаги тармоқларнинг чекланган имкониятлари янги инфокоммуникоцион хизматларни жорий қилишга тўсқинлик қилувчи омил хисобланади.

ГАИ ўзида жуда ҳам мураккаб комплекс технологияни мужассам этган. ГАИ технологиясини таснифлаш учун фақатгина ягона эталон моделдан фойдаланиш мумкин эмас, шунинг учун ҳам хусусиятлари, хизматлари, функционаллаштириш принциплари, ташкилий структуралари ва бошқа аспектлари мақсадларини таснифлаш учун ГАИда бир қатор турли хил моделлардан фойдаланилади.

II Боб. Инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш усуллари ва воситалари

1. Инфокоммуникацион тармоқларда ахборот хавфсизлиги муаммолари

Ҳозирги пайтда компьютер тизимларининг турли соҳаларда ва кенг кўламда ишлатилиши ҳамда ахборотлаштиришнинг жадал тараққий этиши ахборот хавфсизлиги муаммосини келтириб чиқармоқда.

Ахборот хавфсизлиги деганда, табиий ёки сунъий характердаги тасодифий ёки қасддан қилинган таъсирлардан ахборот ва уни қўллаб-қувватлаб турувчи инфратузилманинг ҳимояланганлиги тушунилади [1]. Бундай таъсирлар ахборот соҳасидаги муносабатларга, жумладан, ахборот эгаларига, ахборотдан фойдаланувчиларга ва ахборотни муҳофаза қилишни қўллаб-қувватловчи инфратузлмага жиддий зарар етказиши мумкин.

Ўзбекистон Республикасининг 2002 йил 12 декабрдаги 439 II-сон «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида» қонунида [2] ахборот хавфсизлиги ахборот борасидаги хавфсизлик деб белгиланган ва у ахборот соҳасида шахс, жамият ва давлат манфаатларининг ҳимояланганлик ҳолатини англатади.

Ўзбекистон Республикасининг ахборот хавфсизлиги давлатнинг доимий диққат-эътиборида бўлиб келмоқда. Ахборот хавфсизлиги давлатнинг миллий хавфсизлигини таъминлаш билан узвий боғлиқдир (2.1-расм).

Ахборот хавфсизлиги – кўп қиррали фаолият соҳаси бўлиб, унга фақат тизимли, комплекс ёндашув муваффақият келтириши мумкин. Ушбу муаммони ҳал этишда ҳуқуқий, маъмурий, процедурали ва дастурий-техник чоралар қўлланилади.

Бугунги кунда ахборот хавфсизлигини таъминлайдиган учта асосий тамойил мавжуд [1]:

– маълумотлар бутунлиги – ахборотнинг йўқотилишига олиб келувчи бузилишлардан, шунингдек маълумотларни муаллифлик ҳуқуқи бўлмаган ҳолда ўзлаштириш ёки йўқ қилишдан ҳимоя қилиш;

– ахборотнинг махфийлиги ахборот ва унинг ташувчисининг ҳолатини белгилайди ва унда ахборот билан рухсатсиз танишишнинг ёки уни рухсатсиз ҳужжатлаштиришнинг (нусха кўчиришнинг) олдини олиш таъминланган бўлади;

– фойдаланиш ҳуқуқларига (муаллифликка) эга барча фойдаланувчилар ахборотдан фойдалана олишлари.

2.1-расм. Ахборот хавфсизлиги турлари

Таъкидлаш жоизки, айрим фаолият соҳалари (банк ва молия институтлари, ахборот тармоқлари, давлат бошқарув тизимлари, мудофаа ва махсус тузилмалар) уларда кўриладиган масалаларнинг муҳимлиги ва характерига кўра, уларнинг ахборот тизимлари фаолияти ишончлилигига нисбатан юқори талаблар ва хавфсизлик бўйича махсус чоралар кўрилишини талаб этади.

Ахборот хавфсизлигининг замонавий концепцияси ахборот хавфсизлигини таъминловчи мақсадлар, вазифалар, тамойиллар ва асосий йўналишлар бўйича расмий нуқтаи назарлар мажмуини билдиради.

Қуйида ахборот хавфсизлигининг асосий ташкил этувчилари ва жиҳатлари келтирилган [1]:

− ахборотни муҳофаза қилиш (шахсий маълумотларни, давлат ва хизмат сирларини ва бошқа турдаги тарқатилиши чегараланган маълумотларни қўриқлаш маъносида);

− компьютер хавфсизлиги ёки маълумотлар хавфсизлиги – компьютер тармоқларида маълумотларнинг сақланишини, фойдаланишга рухсат этилганлигини ва махфийлигини таъминловчи аппарат ва дастурий воситалар тўплами, ахборотдан рухсатсиз фойдаланишдан ҳимоя қилиш чоралари;

− ахборот эгаларига ёки ахборотдан фойдаланувчиларга ҳамда уни қўллаб-қувватловчи инфратузилмага зарар етказиши мумкин бўлган табиий ёки сунъий характердаги тасодифий ёки қасддан таъсир этишлардан ахборот ва уни қўллаб-қувватловчи инфратузилманинг ҳимояланганлиги;

− фуқаролар, алоҳида гуруҳлар ва ижтимоий қатламлар, умуман олганда аҳолининг яшаш фаолияти, таълим олиш ва ривожланишлари учун зарур бўлган сифатли ахборотга бўлган талабларининг ҳимояланганлиги.

Ахборотни муҳофаза қилиш – ахборот хавфсизлигининг (маълумотларнинг бутунлиги, фойдалана олиш ва зарур бўлганда, маълумотларни киритиш, сақлаш, қайта ишлаш ва узатишда фойдаланилувчи ахборот ва унинг захиралари махфийлиги) муҳим жиҳатларини таъминлашга йўналтирилган тадбирлар мажмуидир [1].

Ахборот хавфсизлиги ахборотни муҳофаза қилишнинг комплекс ташкилий-техник чора-тадбирлари ва дастурий-аппарат воситаларини ўз ичига олувчи тизим билан таъминланиши керак. Давлат ахборот ресурсларининг ахборот хавфсизлигини таъминлаш тизими давлат органининг ўз ахборот ресурсларини муҳофаза қилишга ёндашувини акс эттирувчи хавфсизлик сиёсатига мувофиқ амалга оширилиши керак.

Хавфсиз тизимда тегишли аппарат ва дастурий воситалардан фойдаланиб, ахборотни ўқиш, ёзиш, ҳосил қилиш ва ўчириш ҳуқуқига эга шахслар ёки улар номидан амалга ошириладиган жараёнлар орқали ахборотдан фойдалана олиш бошқарилади. Маълумки, мутлоқ хавфсиз тизимлар мавжуд эмас, лекин «ишониш мумкин бўлган тизим» маъносидаги ишончли тизимлардан фойдаланилади. Етарлича аппарат ва дастурий воситалардан фойдаланиб, бир вақтнинг ўзида турли махфийлик даражасидаги маълумотларни фойдаланувчилар гуруҳи томонидан фойдаланиш ҳуқуқларини бузмаган ҳолда қайта ишлаш имконини берувчи тизим ишончли ҳисобланади .

Ахборотни муҳофаза қилишнинг асосий объектларига қуйидагилар киради:

– давлат сирлари билан боғлиқ ва махфий маълумотларни ўзида сақловчи ахборот ресурслари;

– воситалар ва ахборот тизимлари (ҳисоблаш техникаси воситалари, тармоқлар ва тизимлар), дастурий воситалар (операцион тизимлар, маълумотлар базаларини бошқариш тизимлари, амалий дастурий таъминот), автоматлаштирилган бошқарув тизимлари, алоқа ва маълумотларни узатиш тизимлари, рухсати чегараланган ахборотни қабул қилиш, узатиш ва қайта ишлаш техник воситалари (овоз ёзиш, овоз кучайтириш, овоз эшитиш, сўзлашув ва телевизион қурилмалар, ҳужжатларни тайёрлаш, кўпайтириш воситалари ҳамда бошқа график, матн ва ҳарфли-рақамли маълумотларни қайта ишлаш воситалари), махфий ва давлат сирлари тоифасига оид бевосита қайта ишловчи тизим ва воситалар. Бундай тизим ва воситаларни кўпинча

ахборотларни қабул қилиш, сақлаш ва қайта ишлаш техник воситалари деб аташади.

Ахборот ҳимояси турлари икки асосий белгига кўра таснифланади: биринчидан, ахборот хусусийлиги, аниқроғи қўриқланадиган сирлар турига кўра; иккинчидан, ахборот ҳимояси учун қўлланилувчи кучлар, воситалар ва усуллар гуруҳлари бўйича .

Ахборотни муҳофаза қилишда фойдаланиладиган асосий усуллар қуйидагилар ҳисобланади: яшириш, ранжирлаш, нотўғри маълумот бериш, бўлаклаш, суғурта қилиш, ҳисобга олиш, кодлаш ва шифрлаш [2].

Яшириш – ахборотни муҳофаза қилиш усули сифатида амалиётда маълумотларни ҳимоялашнинг асосий ташкилий усулларидан бири ҳисобланади, махфий маълумотларга рухсат этилган шахслар сонини чегаралайди. Яшириш – ахборотларни ҳимоя қилишда жуда кенг қўлланилувчи усуллардан бири ҳисобланади.

Ранжирлаш ахборот ҳимоя усули сифатида, биринчидан, махфий маълумотларни махфийлик даражаси бўйича тақсимлайди, ва иккинчидан ҳимояланган ахборотга рухсатни чегаралайди.

Нотўғри маълумот бериш – ахборотни ҳимоя қилиш усулларидан бири бўлиб, бирор объект ҳақидаги ҳақиқий маълумот ўрнига атайин ёлғон маълумот тарқатишни англатади.

Ахборотни бўлаклаш усули ахборотни бўлакларга бўлиб, унинг бирор қисми орқали тўлиқ маълумот олиб бўлмасликни англатади. Бу усул ҳарбий техника ва қуролланиш воситаларини ишлаб чиқаришда, шунингдек янги маҳсулотларни ишлаб чиқаришда кенг қўлланилади.

Суғурта қилиш – ахборотни муҳофаза қилиш усули сифатида эндигина тан олинмоқда. Унинг маъноси ахборот эгаси ҳуқуқлари ва манфаатларини ёки ахборот воситаларини анъанавий таҳдидлар ва ахборот хавфсизлиги таҳдидларидан ҳимоя қилишни билдиради. Ушбу усул тижорат сирларини сақлашда кўпроқ қўлланилиши эҳтимоли мавжуд. Ахборотни суғурта

қилишда у дастлаб, аудиторлик текширувидан ўтиши ва хулосага эга бўлиши талаб этилади.

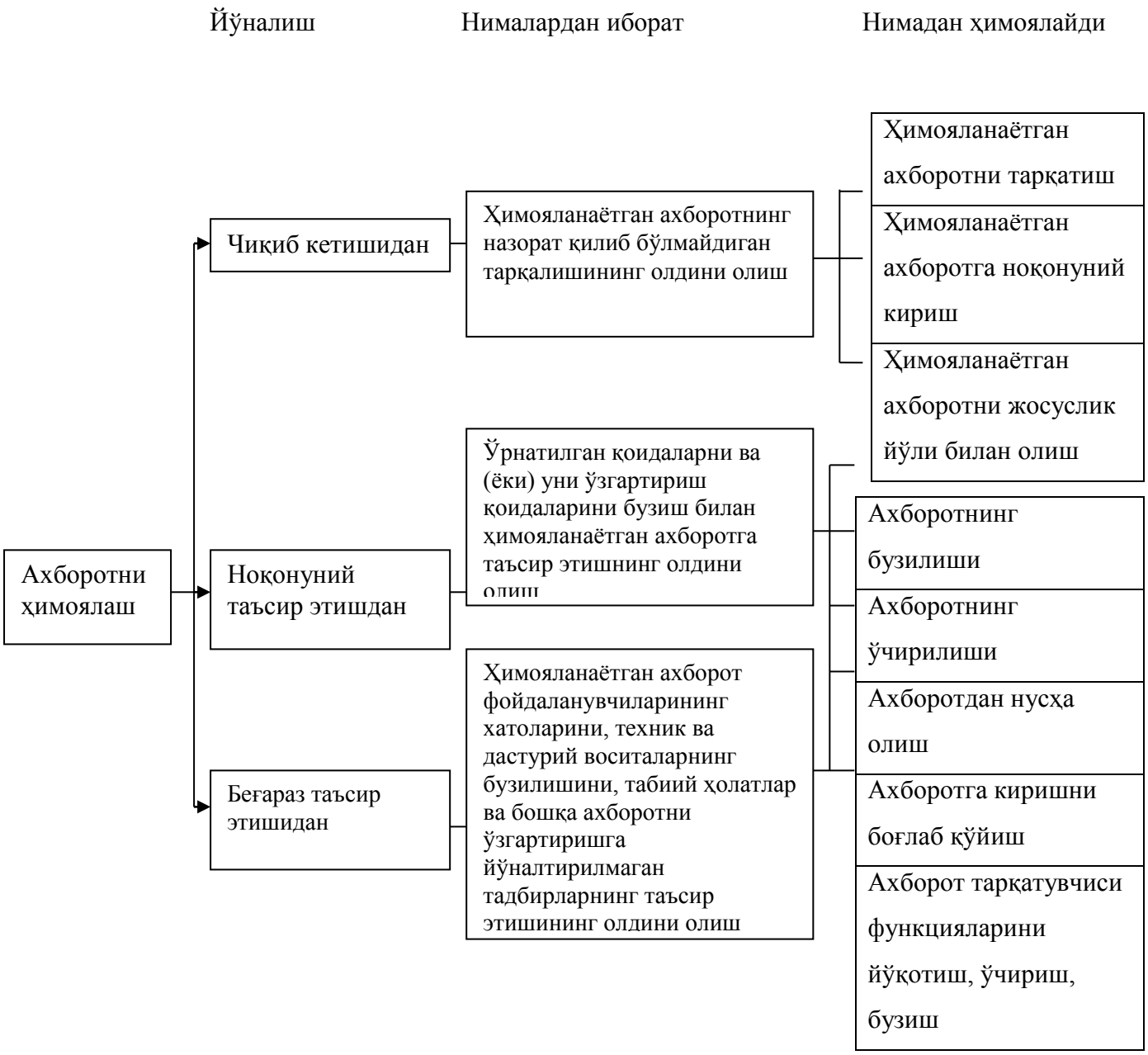
Ахборотларни маънавий-маърифий ҳимоялаш усули ахборотни муҳофаза қилишда жуда муҳим рол ўйнайди. Айнан инсон, у корхона ёки ташкилот ходими, махфий маълумотлардан воқиф бўлиб, ўз хотирасида кўплаб маълумотларни жамлайди ва баъзи ҳолларда ахборот чиқиб кетиши манбаига айланиши мумкин ҳамда унинг айби билан ўзгалар ушбу ахборотга ноқонуний эга бўладилар.

Кодлаш – ҳимояланувчи ахборотни рақибдан яшириш мақсадида, ахборотни канал орқали узатиш жараёнида ўзгалар томонидан тутиб олиниши хавфи мавжуд бўлганда, уни кодлаш усули ёрдамида очиқ матнни шартли ахборотга айлантириш усулидир. Кодлаш учун одатда белгилар тўплами (белгилар, рақамлар ва бошқалар), шунингдек ахборотни тушунарсиз белгилар тўплами кўринишига айлантириш имконини берувчи маълум қоидалар тизими фойдаланилади. Бу ахборотни ўқиш учун эса уни яна ўз ҳолига келтириш, яъни кодни очиш (калит) керак бўлади. Ахборотни кодлаш техник воситалар ёрдамида ёки қўлда амалга оширилиши мумкин.

Шифрлаш – ахборотни муҳофаза қилиш усули бўлиб, кўпинча ахборотларни радиоқурилмалар воситасида узатишда, рақиб томонидан тутиб олиш хавфи бўлганда қўлланилади. Ахборотни шифрлаш, уни ўзгалар томонидан тутиб олинганда ҳам калитсиз маъносини тушуниб бўлмайдиган ҳолатга ўтказишни англатади.

Ахборот хавфсизлиги бўйича стандартлар ахборот чиқиб кетишининг олдини олиш, ахборотга ноқонуний ва бехосдан таъсир кўрсатишга йўналтирилган фаолиятни ахборот ҳимояси сифатида аниқлайди. Агар биринчи йўналиш (чиқиб кетишининг олдини олиш) конфиденциал маълумотларнинг тарқалиб кетишини олдини олиши, уларга рухсатсиз кириши ва\ёки уларни разведка (масалан, рақобатчи фирмаларнинг тижорат разведкаси) орқали олиш керак бўлса, қолган иккита йўналиш бир хил таҳдидлардан ҳимоя килади (конфиденциал ахборотнинг бузилиши, унинг

йўқ қилиниши, киришни блокка тушириш ва ахборот тарқатувчиси билан учрайдиган ўхшаш ҳаракатлар). Уларнинг фарқи фақатгина ахборот билан ўзаро ҳаракатда ғоянинг борлиги ёки йўқлигидадир (2.2-расм) [13].



2.2-расм. Корхонада ахборот ҳимояси

Таҳдидларнинг кўп миқдорини хали ҳам компьютер вируслари (уларга анъанавий бўлган файлли, юкланадиган, макровируслар ва ҳ.к. зарарли дастурлардан ташқари “троянлар”, “вандаллар”, паролларни ушлаб

олувчилар ва бошқалар киради) ва спам тарқатувчилари ҳужумлари ташкил қилади.

Кўпгина тармоқлар йиллар давомида Интернет фойдаланувчилари учун очиқ туради, бундай ҳолатларда таҳдид солувчининг корпоратив тармоқдан махфий ахборотни олиш учун билиб туриб ҳужум қилгани ёки “хизмат кўрсатишни рад қилиш” тарзидаги ҳужумлар ёрдамида тармоқ ишини бузиш хавфли. Модомики, кичик ва ўрта тижорат тузилмалари учун маҳсус ҳимояланган алоқа линияларини яратишнинг имконияти йўқ экан, махфий ахборот ва бошқа ахборотларнинг алмашинуви учун очиқ каналлардан фойдаланишга тўғри келади, бу эса ушбу ахборотни ўзига қамраб олгани каби, унинг бутунлигининг бузилиши ёки алмашиб қолишига олиб келади.

Локал тармоқ ичида фойдаланувчиларнинг ишончли аутентификацияси муҳим ҳисобланади: мониторга логин ва парол ёзилган қоғознинг ёпиштирилиб қўйилиши бунга оддий мисол.

Кўпгина ҳолларда кириш қонуний фойдаланувчилар орасида киришга рухсат беришга аҳамият берилмайди. Бу ерда шундай ўхшашликни келтириш мумкин: хоналарга нисбатан иерархияга барча ходимлар ҳурмат билан амал қиладилар ва хеч кимнинг бошига раҳбариятнинг столини ёки хонасини эгаллаб олиш фикри келмайди, махфий ахборотга нисбатан эса бошқача, яъни “ҳар кимга – қизиқишига кўра” принципига кўра амал қилинади ва иккита – учта топ–менежер билиши керак бўлган маълумот корхона ходимларининг ярмига маълум бўлади.

Маълумотнинг чиқиб кетиши эҳтимоли бўлган яна бир канал сифатида сервис–марказларни кўриш мумкин, уларга керакли равишда йўқотилмаган ахборотли дисклар келиб тушади. Ниҳоят, шуни ҳам унутмаслик керакки, кўпгина ҳолларда фойдаланувчилар фақатгина электрон кўринишидаги ахборотни эмас, балки қоғоз кўринишидаги ахборотни ҳам ахлат челакларни доимий текшириб чиқиш орқали, қоралама ва хомаки ахборотларни олишлари мумкин, бу эса сизнинг рақобатчиларингизга ҳийлали ҳужумлар ва бузишга уринишлардан кўра кўпроқ фойда бериши мумкин.

Шундай қилиб, хулоса қилиб айтиш мумкинки, ахборотни ҳимоялш – ҳар бир муваффақиятли корхона фаолиятининг муҳим йўналишларидан биридир. Бунинг учун махсус танланган ходим (ёки бўлим) олдида қуйидаги вазифалар туради [3]:

- махфий ахборотга таҳдидни таҳлил қилиш, шунингдек, автоматлашган тизимнинг заиф томонларини таҳлил қилиш ва уларни бартараф этиш;
- ахборот ҳимоялаш тизимини шакллантириш – керакли воситаларни олиш ва ўрнатиш, уларни профилактика қилиш ва хизмат кўрсатиш;
- фойдаланувчиларни ҳимоя воситалари билан ишлашга ўқитиш, уларнинг қўлланилиши регламентига риоя қилинишини назорат қилиш;
- экстремал вазиятларда ҳаракат қилиш алгоритмини ишлаб чиқиш ва доимий “ўқишларни” ўтказиб туриш;
- автоматлаштирилган тизимлар ва қайта тиклаш тадбирлари (вирусли ҳужум ҳолатида, техник воситаларнинг ишдан чиқиши\хатолар чиқиши\рад этиши ва ҳ.к.) режасининг доимий ҳаракати режаси дастурини ишлаб чиқиш ва амалга ошириш.

Шундай қилиб, таъкидлаш мумкинки, ахборотни ҳимоялаш бўйича фаолият “компания раҳбарияти – ахборотни ҳимоялаш хизмати - фойдаланувчилар” дан иборат учбурчакдан ўтади, ҳамда ҳамкорликнинг самарали бўлиши ушбу тарафларнинг барчасига боғлиқ.

2. Инфокоммуникацион тармоқларда фойдаланиладиган ахборот хавфсизлигини таъминлаш усуллари ва воситалари

Инфокоммуникацион тармоқларда алмашинадиган электрон маълумотларни бузғунчилардан ҳимоялаш ва тармоқларда махфий

маълумотлар билан алмашиниш учун муҳофазаланган канални ташкил этиш муҳим масалалардан бири ҳисобланади.

Интернетдан кенг фойдаланишнинг асосий шартларидан бири у орқали ўтказиладиган барча транзакциялар учун хавфсизликнинг бир хил даражасини таъминлаш бўлган ва бўлиб қолади. Бу фойдаланувчилар ўртасида узатиладиган ахборотга, савдо тизимларининг маълумотлар базаларида сақланадиган ахборотга, молиявий транзакцияларга илова қилинадиган ахборотга тааллуқлидир.

Ахборот хавфсизлиги тушунчасини ахборот эгаларининг ёки ахборотдан фойдаланувчиларнинг моддий зарар кўришига олиб келадиган ахборотнинг йўқ қилиниши, бузилиши ва фош этилиши учун йўл қўйиб бўлмайдиган хавфларни бартараф этувчи тасодифий ёки атайлаб қилинган таъсирларга бардош бериш ҳолати каби таърифланади. Тармоққа ташқаридан кириш тўлиқ очиқ бўлганлиги сабабли ушбу усулларнинг аҳамияти жуда катта. Хавфсизлик омилларининг катта аҳамиятга эгалиги Интернетда ўтказиладиган кўп сонли тадқиқотлар билан белгиланади.

Қуйида Инфокоммуникация тармоғининг ахборот хавфсизлигини таъминлашнинг маъмурий усулларининг тадқиқи келтирилди.Уни ҳал этиш учун талабларни ишлаб чиқиш, хавфсизлик сиёсатини белгилаш ва амалда ишлаб чиқилган хавфсизлик сиёсатининг маъмурий ва дастурий-аппарат чораларини ишлаб чиқиш шарт. Тармоқларда узатиладиган ахборотларни бузувчи таъсирлардан ҳимоя қилишнинг маъмурий усуллари айнан содда ва арзон бўлиши мумкин.

Интернет тармоғининг ахборот хавфсизлигини таъминлашнинг маъмурий усулларига қуйидагиларни киритиш мумкин [3]:

- тармоқ трафигини таҳлил қилиш;

- сохта ARP-сервердан ҳимояланиш;

- сохта DNS-сервердан ҳимояланиш;

- ICMP протоколидан фойдаланишда сохта маршрутни мажбуран ўтказишдан ҳимояланиш;

- хизмат кўрсатилишидан бош тортишдан ҳимояланиш;

-TCP/IP протоколларидан фойдаланган ҳолда ҳимояланиш.

Тармоқ трафигини қуйидагича ҳимоялаш мумкин: агар канал бўйлаб фақат очиқ ахборот узатилаётган бўлса, кракерга тармоқда узоқлашган фойдаланувчилар алмашинаётган исталган ахборотни узатиш каналини эшитиш дастури ёрдамида тутиб олиш имконини берадиган ҳужум мавжуд. Шунингдек, узоқдан туриб фойдаланишнинг TELNET ва FTP базавий амалий протоколлари тармоқ бўйича узатиладиган фойдаланувчилар идентификаторлари (номлари) ва аутентификаторлари (пароллари)нинг элементар криптоҳимоясини кўзда тутмаслигини кўрсатиш мумкин. Шунинг учун тармоқ маъмурларига ушбу базавий пртоколлардан ўз тизимларининг ресурсларидан узоқдан туриб авторизация қилинган фойдаланишни тақдим этиш учун фойдаланишга йўл қўймасликни ва тармоқ трафигининг таҳлилини бартараф этиб бўлмайдиган, лекин уни IP-оқимнинг бардошли криптоалгоритмларини қўллаган ҳолда аҳамиятсиз қилиб қўйиш мумкин бўладиган таҳдид деб ҳисоблашни таклиф этиш мумкин.

Сохта ARP-сервердан ҳимояланишда ҳужумни йўқ қилиш учун уни амалга ошириш мумкин бўлган сабаб бартараф этилиши керак. Масофадан туриб ҳужум қилиш муваффақиятининг асосий сабаби - ҳар бир хост операцион тизимда тармоқ ушбу сегментининг ичида бошқа қолган хостларнинг мос келадиган IP- ва Ethernet – адреслари тўғрисидаги ахборотнинг йўқлигидир. Шундай қилиб энг содда ечим бу тармоқ маъмури томонидан файл кўринишидаги статистик ARP-жадвални яратишдир. Ушбу жадвалга адреслар тўғрисидаги тегишли ахборотни киритиш мумкин. Ушбу файл сегмент ичида ҳар бир хостга ўрнатилади ва операцион тизим тармоқларида масофадан туриб ARP-қидирувдан фойдаланишга ҳожат қолмайди [3].

Сохта DNS-сервердан ҳимояланиш қуйидагича амалга оширилиши мумкин: Интернет тармоғида DNS хизматидан унинг ҳозирги кўринишида

фойдаланиш кракерга уланишларни кракер хости - сохта DNS-сервер орқали сохта маршрутни мажбуран ўтказиш йўли билан глобал назорат қилиниши имконини беради мумкин. DNS хизматининг потенциал заифликларига асосланган масофадан туриб ҳужум қилишни амалга ошириш Интернет фойдаланувчиларининг кўплаб сони учун фожиали оқибатларга олиб келиши ва ушбу глобал тармоқ ахборот хавфсизлиги бузилишининг оммавий сабаби бўлиши мумкин.

Тармоқ маъмурлари ва фойдаланувчилари хамда DNS-серверлар маъмурлари учун ушбу масофадан туриб ҳужум қилишнинг олдини олиш ёки қийинлаштириш бўйича мумкин бўлган қуйидаги 2 та маъмурий усуллардан фойдаланиши мумкин:

а) тармоқ маъмурининг сохта DNS-сервердан ҳимояланиши;

б) DNS-сервери маъмурининг сохта DNS-сервердан ҳимояланиши.

Шуни белгилаш керакки, Microsoft компаниясининг маҳсулотлари мумкин бўлган масофадан туриб ҳужумлардан IP-тармоқларга хос бўлган махсус ҳимояланганлиги билан ажралиб турмайди. Шунинг учун операцион тизим маълумотларини ҳимояланган IP-тармоқнинг ҳимояланган сегментида фойдаланиш маъқул эмас. Бу ушбу масофадан туриб ҳужум қилишдан сегментни ҳимоя қилиш бўйича маъмурий ечим бўлади. Шунинг учун Интернет тармоғидаги ҳар қандай серверни масофадан туриб ҳужум қилиш ёрдамида тўлиқ ишдан чиқариш мумкин. Фақат ушбу ҳужумга дучор бўладиган тизимнинг ишлаш қобилиятини оширишнинг ягона усули – бу имкони борича қувватлироқ компьютерлардан фойдаланишдир. Процессорларнинг сони ва ишлаш тезлиги қанча кўп бўлса, оператив хотираси қанча кўп бўлса, тармоқ операцион тизим унга уланишни яратиш учун сохта сўровлар ёғилганда ишлаши ҳам кўпроқ ишончли бўлади. Бундан ташқари ҳисобланган қувватларига мос келадиган ички навбатга эга, уланиш учун сўровларнинг кўп сонини жойлаштириш қобилиятига эга операцион тизимлардан фойдаланиш зарур.

TCP/IP оиласига мансуб базавий протоколлардан фойдаланган ҳолда биргаликда ишлашда томонларнинг бирини алмаштириб қўйишдан қуйидагича ҳимояланиш мумкин. Аввал белгилаб ўтилганидек TCP/IP оиласидаги уланиш ва унинг абонентларининг хавфсизлигини таъминлаш функцияси кўзда тутилган ягона базавий протокол б транспорт даражасидаги протокол ҳисобланади. Амалий даражадаги FTP, TELNET, r-хизмат, NFS, HTTP, DNS, SMTP, базавий протоколларга келсак, улардан ҳеч бири ўз даражасида уланишнинг қўшимча ҳимоясини кўзда тутмайди ва хавфсизликни таъминлаш бўйича барча муаммолар ечимини пастроқ даражадаги TCP протоколига қолдиради. Базавий TCP/IP протоколлар оиласидан фойдаланганда уланиш хавфсизлигини таъминлаш амалда мумкин эмаслигини хулоса қилиш қийин эмас. Бу Интернет тармоғининг барча базавий протоколлари ахборот хавфсизлигини таъминлаш нуқтаи назаридан эскирди. Уланишларга сегментлараро ҳужумлардан ҳимояланиш учун тармоқ маъмурларига базавий «ҳимояланган» протокол сифатида TCP-уланиш идентификаторининг дастлабки қийматлари тасодифий тарзда ҳақиқатда генерацияланадиган TCP протолидан ва тармоқ операцион тизимидан фойдаланишни тавсия этиш мумкин.

Қуйида Интернет тармоғида масофадан туриб ҳужум қилишдан ҳимояланишнинг дастурий-аппарат усулларининг баёни келтирилади.

Ҳисоблаш тармоқларида алоқа воситаларининг ахборот хавфсизлигини таъминлашнинг дастурий-аппарат воситаларига ҳисоблаш тармоғида қуйидагилар киради:

- тармоқ трафигининг аппарат шифраторлари;
- дастурий-аппарат воситаларининг базасида амалга ошириладиган Firewall усули;
- ҳимояланган тармоқ криптопротоколлари;
- тармоқ трафигининг дастурий-аппарат анализаторлари;
- ҳимояланган тармоқ операцион тизими.

2.3-расм . Ахборот хавфсизлигини таъминлаш воситалари

Юқоридаги 2.3-расмда ахборот хавфсизлигини таъминлаш воситаларининг таснифи келтирилган.

Умуман олганда, компьютер тизимлари ва тармоқларида ахборот хавфсизлигини таъминлаш компьютер безорилари томонидан уюштирилган ҳужум ва хавфларни бошқариш ҳолатларини таҳлил қилиш ва уларнинг олдини олиш воситаларини ишлаб чиқишни тақозо этади.

Интернет тармоғида фойдаланилиши мўлжалланган ҳимоя қилишнинг ушбу воситаларига бағишланган адабиётнинг кўплаб сони мавжуд. Энди Интернет тармоғида қўлланадиган дастурий-аппарат ҳимоя воситалари қисқача таърифлаб ўтилади.

Тармоқ технологиясининг кенг кўламда қўлланиши натижасида умумий ресурслардан фойдаланиш имконини берувчи локал тармоққа компьютерлар бирлаштирилди. Мижоз-сервер технологиясининг татбиқ этилиши эса бу тармоқни тақсимланган ҳисоблаш муҳитига айлантирди. Тармоқнинг хавфсизлиги ундаги барча компьютерларнинг ва тармоқ қурилмаларининг хавфсизлиги билан аниқланади. Бузғунчи тармоқнинг бирор-бир ташкил этувчисининг ишини бузиш орқали бутун тармоқни обрўсизлантириш мумкин.

Замонавий телекоммуникация технологиялари локал тармоқларни глобал тармоққа - Интернетга улаш имконини берди. Интернетнинг ривожланиши хавфсизликни таъминлашни долзарб масалага айлантирди ва Интернетга уланган тармоқ ва тизимларда, қандай маълумотларга ишлов берилишидан қатъи назар, хавфсизлик воситалари бўлишини тақозо этади. Чунки Интернетнинг имкониятларидан фойдаланиб, бузғунчи хавфсизликни бузишни глобал масштабда олиб бориши мумкин. Интернетга уланган компьютер тажовуз объекти бўлса, ҳужумни амалга ошираётган шахсга унинг қаерда (қўшни хонада ёки бошқа қитъада) жойлашгани катта аҳамиятга эга эмас.

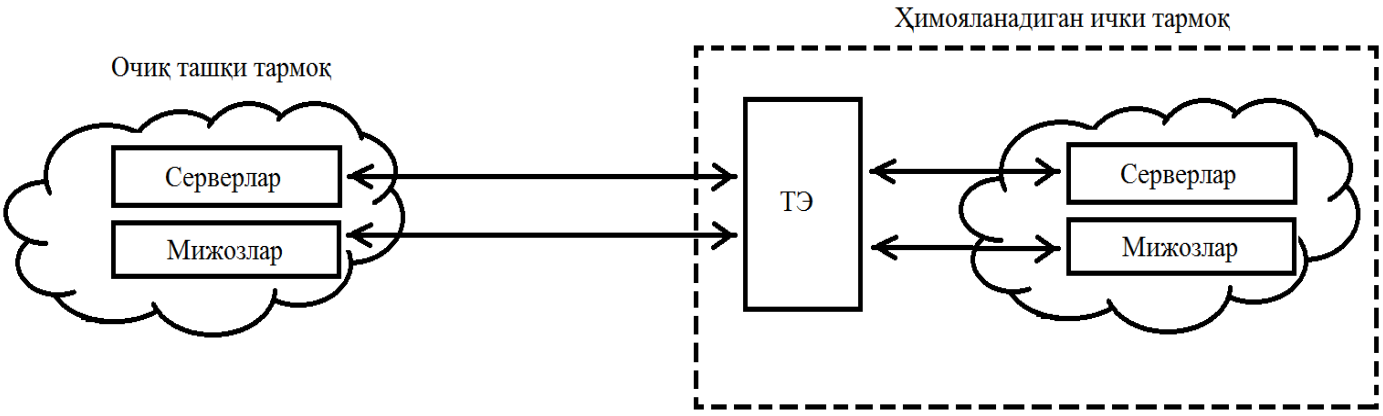
Инфокоммуникация тармоғида масофавий ҳужумлардан дастурий-аппарат ҳимоялаш усуллари ҳақида қисқача тўхталиб ўтамиз. Интернет тармоқларининг алоқа воситаларида ахборот хавфсизлигини таъминлашнинг дастурий-аппарат воситаларига қуйидагилар киради:

- тармоқ трафиги аппарат шифраторлари;
- дастурий-аппарат воситалар базасида ташкил қилинувчи Firewall (тармоқлараро экран) методикаси;
- ҳимояланган тармоқ крипто протоколлари;
- Тармоқ трафиги дастурий-аппарат анализаторлари;
- ҳимояланган тармоқ операцион тизимлари.

Ҳамма фойдаланаётган тармоқдан келиб чиқаётган таҳдидларни блокировкалаш учун юқорида келтирилган Firewall деб номланувчи дастурий ва дастурий-аппарат воситалардан фойдаланилади. Одатда, алоҳида ажратилган ва ҳимояланган инфокоммуникацион тармоқ «тармоқлараро экран» орқали ҳамма фойдаланадиган тармоққа уланади [15].

Тармоқлараро экранлар гарчи корхона локал тармоғи уланган корпоратив интратармоғидан қилинувчи ҳужумлардан ҳимоялашда ишлатилиши мумкин бўлсада, одатда улар корхона ички тармоғини Интернет глобал тармоқдан суқилиб киришдан ҳимоялайди. Аксарият тижорат ташкилотлари учун тармоқлараро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурий шарти ҳисобланади.

Рухсат этилмаган тармоқлараро фойдаланишга қарши таъсир кўрсатиш учун тармоқлараро экран ички тармоқ ҳисобланувчи ташкилотнинг ҳимояланувчи тармоғи ва ташқи ғаним тармоқ орасида жойланиши лозим ва бу тармоқлар орасидаги барча алоқа фақат тармоқлараро экран орқали амалга оширилиши лозим. Ташкилий нуқтаи назардан тармоқлараро экран ҳимояланувчи тармоқ таркибига киради [4]. Тармоқлараро экран ҳимояланган КТга келиб тушаётган ва ундан чиқиб кетаётган ахборотларни назорат қилиш учун қўлланилади (2.4-расм).



2.4 -расм. Тармоқлараро экранни улаш схемаси

Тармоқлараро экран қуйидаги тўртта функцияни бажаради:

- маълумотларни фильтрлаш;
- экранловчи агентлардан фойдаланиш;
- манзилларни трансляциялаш;
- ҳодисаларни қайд қилиш.

Тармоқлараро экраннинг асосий вазифаси (кираётган ёки чиқаётган) трафикни фильтрлашдан иборат. Корпоратив тармоқнинг ҳимояланганлик даражасига қараб фильтрлашнинг турли қоидалари ўрнатилиши мумкин. Фильтрлаш қоидалари фильтрлар кетма-кетлигини танлаш орқали амалга оширилади. Ушбу фильтрлар ўзидан кейинги фильтрга ёки протокол сатҳига маълумотларнинг узатилишига рухсат беради ёки тақиқлайди.

Тармоқлараро экран фильтрлашни каналлар, тармоқлар, транспорт ва амалий сатҳларда амалга оширади. Экран қанча кўп сатҳни ўз ичига олса, шунча такомиллашган ҳисобланади.

Тармоқлараро экранда, дастурий воситачи вазифасини бажарувчи ва субъект ва объект орасида уланишни таъминловчи, сўнгра ахборотни қайд қилиш ва назоратини амалга ошириб жўнатувчи *экранловчи агентлардан* (proxy-серверлар) фойдаланилади. Экранловчи агентларнинг қўшимча вазифаси фойдаланишга рухсат берилган субъектдан ҳақиқий объектни

яширишдан иборат. Экранловчи агентларнинг ўзаро алоқа иштирокчиларига таъсири йўқ.

Тармоқлараро экраннинг манзилларини *трансляциялаш* функцияси ҳақиқий ички манзилларни ташқи абонентлардан яшириш учун мўлжалланган. Бу тармоқ топологиясини яшириш ва агар ҳимояланган тармоқ учун етарли миқдорда манзиллар ажратилмаган бўлса, янада кўпроқ сондаги манзиллардан фойдаланишга имкон яратади.

Тармоқлараро экран махсус журналларда *ҳодисаларни қайд* қилиб боради. Бирор аниқ талаб бўйича экранни созлаш орқали журналларни юритиш имконияти назарда тутилган. Ёзувлар таҳлили ўрнатилган қоидаларни бузишга бўлган бузғунчиларнинг уринишларини қайд қилиш ва уларни аниқлаш имконини беради.

Экран симметрик эмас. У «ташқи» ва «ички» тушунчаларини фарқлай олади. Экран ички соҳани назоратсиз ва адоватли бўлган ташқи муҳитдан ҳимоясини таъминлаб беради. Шу билан бирга экран ҳимояланган тармоқ субъектлари томонидан оммавий тармоқ объектларидан фойдаланишни чеклашни ҳам таъминлайди. Фойдаланишга рухсат берилган субъектнинг ваколатлари бузилган ҳолатда унинг иш фаолияти блокировка қилинади ва барча керакли маълумотлар журналга ёзиб қўйилади.

Тармоқлараро экранларга қуйидаги замонавий талаблар қўйилади:

1. Асосий талаблар - бу ички тармоқнинг хавфсизлигини таъминлаш ва ташқаридан уланишлар ва алоқа сеансларини тўлиқ назорат қилиш;

2. Экранловчи тизим ташкилотнинг хавфсизлик сиёсатини оддий ва тўлиқ юритиш учун қувватли ва мосланувчан бошқариш воситаларига эга бўлмоғи даркор;

3. Тармоқлараро экран локал тармоқ фойдаланувчиларига сездирмасдан ишлаши ва улар томонидан рухсат этилган амалларни бажаришларига халақит бермаслиги лозим;

4. Тармоқлараро экран кўп миқдордаги мурожаатлар билан блокировка қилиб қўйишни ва ишдан чиқишининг олдини олиш учун унинг процессори

тез ишлай олиш, пик режимларида кирувчи ва чиқувчи оқимларни етарли даражада самарали қайта ишлай олишга улгуриши лозим;

5. Хавфсизликни таъминлаш тизими ҳар қандай ташқи ноқонуний таъсирлардан ҳимояланган бўлиши лозим, чунки бу таъсирлар ташкилотнинг махфий маълумотларини очиш калити бўлиши мумкин;

6. Экранни бошқарув тизими олисдаги филиаллар учун ҳам ягона хавфсизлик сиёсатини юритишни марказлашган ҳолда таъминлаш имкониятига эга бўлмоғи лозим;

7. Тармоқлараро экран фойдаланувчиларнинг ташқи уланишлари орқали фойдаланишга рухсат беришнинг муаллифлаштириш воситаларига эга бўлмоғи керак. Бу ташкилот ходимларини хизмат сафарида ҳам тармоқдан фойдаланишларига имкон яратади.

Тақсимланган тармоқлараро экранлар, анъанавий тармоқлараро экранлардан фарқли равишда, қўшимча дастурий таъминот бўлиб, хусусан корпоратив серверларни, масалан Интернет-серверларни ишончли ҳимоялаши мумкин. Корпоратив тармоқни ҳимоялашнинг оқилона ечими - ҳимоялаш воситасини у ҳимоя қилувчи сервери билан бир платформада жойлаштиришдир.

Юқорида келтирилган ахборотни ҳимоялаш воситалари ва усуллари билан бир қаторда ахборот хавфсизлигини таъминловчи амалий воситаларни қўллаш ҳам яхши самара беради. Бундай амалий воситалар қаторига брандмауерларни ўрнатиш, заиф жойларни сканерлаб туриш, парол очувчи махсус дастурларни ишлатиб туриш каби воситалар киради.

Брандмауерлар (тармоқлараро экран) ташкилотнинг энг асосий ҳимоя воситаси бўлиб, улар тармоқда кирувчи, ундан чиқувчи ахборот оқимини назорат қилади [4]. У ахборот оқимининг бирор турини тўсиб қўйиши ёки текшириб туриши ва хакерларнинг тажовузидан сақлаши мумкин.

Корхона инфокоммуникация тармоғида ахборотни ҳимоялаш учун зарурий воситалар ва методлар тўплами қуйидаги 2.1-жадвалда келтирилган.

2.1-жадвал

Корхона тармоғида ахборотни ҳимоялаш воситалари ва методлари

Минимал пакет	**Оптимал пакет (минимал пакетга қўшимча)**
Ишчи станция, файлли ва почта серверларининг антивирусли ҳимоя воситалари	Дастурий-аппаратли фойдаланиш-даги антивирусли воситалар, таркибни назорат қилиш воситалари (Content Inspector) ва спамплар билан кураш
Дастурий тармоқлараро экран (ТЭ)	Дастурли-аппаратли ТЭ, ҳужумларни аниқлаш тизими (Intrusion Detection System)
Ҳимояланган корпоратив тармоқларни шакллантириш дастурий воситалари (VPN - Virtual Private Network)	Дастурли-аппаратли фойдаланиш-да ва тармоқлараро экран билан интеграцияда ҳам худди шундай
Фойдаланувчилар аутентификацияси-нинг аппаратли воситалари (токенлар, смарт-карталар, биометрия ва ҳ. к.)	Ноқонуний киришдан ҳимоялаш (НКҲ) воситалари билан интеграцияда ва криптографик воситаларда ҳам ҳудди шундай
Ахборотни ҳимоялашнинг штатли механизмлари билан махфий ахборотга фойдаланувчиларнинг киришини чеклаш ва операцион тизим, амалий дастурлар, маршрутизаторлар ва ҳ.к.нинг киришини чеклаш	НКҲ дан ҳимоялашнинг дастурли-аппаратли воситалари ва киришни чеклаш
Очиқ алоқа каналлари орқали махфий ахборотни алмашиниш учун шифрлашнинг дастурий воситалари ва электрон рақамли имзо (ЭРИ)	Шифрлаш калитлари ва ЭРИ ларни сифатли ишлаб чиқиш учун аппаратли шифраторлар, НКҲ ва аутентификациядан ҳимоялаш воситалари билан интеграциялаш
Махфий ахборотни сақлаш учун фойдаланиладиган фойдаланувчиларнинг мантиқий дискларини “шаффоф” шифрлаш воситалари	Серверлардаги махфий ахборотни, сақланаётган ва қайта ишланаётган ахборотни “шаффоф” шифрлаш воситалари
Фойдаланилмайдиган махфий ахборотни ўчириш воситаси (масалан, шифраторларнинг мос келадиган функциялари ёрдамида)	Ахборот тарқатувчиларни аппаратли ўчириш воситалари
Заҳиравий нусха олиш воситалари, тўхтовсиз энергия манбаи, қоғозли ҳужжатлар йўқ қилувчилар	

Шундай қилиб, корхона тармоғида ахборотни ҳимоялаш учун юқоридаги жадвалда келтирилган воситалар ва усуллар тўплами бўлиши талаб этилади.

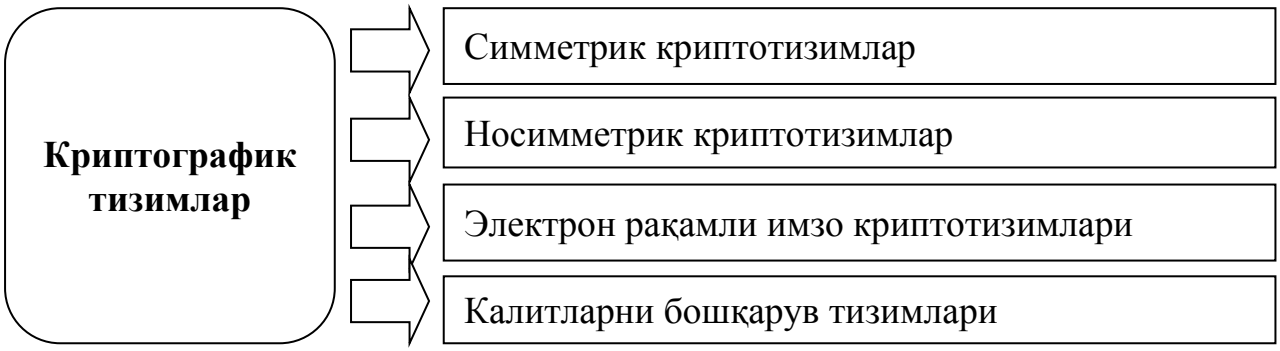
3. Ахборот хавфсизлигини таъминлашнинг криптографик усул ва воситалари

Криптография ахборотни муҳофаза қилиш усулларидан бири ҳисобланади. Криптография ахборот (маълумотларни ўзгартириш) тамойиллари, воситалари ва усулларини тадқиқ этади. Бундан мақсад ахборот мазмунидан рухсат этилмаган фойдаланишдан муҳофазалаш ва уни бузишни бартараф қилиш. Криптография маълумотларни алоқа каналлари орқали узатишда ёки сақлашда махфийликни ёки ҳақиқийликни таъминлаш усуллари билан шуғулланади. Шу билан бирга, криптография маълумотларни хабардор бўлмаган шахслар учун тушуна олмайдиган қилиш мақсадида ўзгартириш усули ҳамдир. У маълумотлар хавфсизлиги тизимининг муҳим таркибий бўлаги. Унинг моҳияти маълумотларни узатишдан олдин маъносиз белгилар ёки сигналлар жамланмасига айлантириш ва маълумотларни олувчи қабул қилиб олгандан сўнг, уларни дастлабки шаклига қайта тиклашдир [3].

Ахборот тизимларида криптографик усуллар кенг қўлланилмоқда. Чунки компьютер тармоқлари, жумладан Интернет жадал ривожланмоқда. Тармоқ орқали давлат, ҳарбий, тижорат ва хусусий таснифга эга катта ҳажмдаги маълумотлар узатилмоқда. Бу маълумотларга бегона шахсларнинг кириши мумкин эмас. Шу билан бирга, юқори қувватли компьютерларнинг, тармоқ ва нейрон ҳисоблаш технологияларининг пайдо бўлиши аввал ўта мустаҳкам, амалда ечими йўқ деб ҳисобланган криптографик тизимларни обрўсизлантирди. Бу эса замонавий криптографик усуллардан фойдаланиш ўта долзарб эканлигини англатади.

Замонавий криптография ахборот хавфсизлигининг махфийлик, бутунлик, аутентификация ва томонларнинг муаллифликни инкор эта олмасликлари муаммоларини ҳал этувчи билим соҳаси ҳисобланади. Махфийликни таъминлаш деганда ахборот билан танишиш ҳуқуқи бўлмаган шахслардан бу ахборотни ҳимоялаш тушунилади.

Криптографик усуллар турли хил кўринишдаги криптотизимлар асосида амалга оширилади (2.5-расм).



2.5-расм. Криптографик тизим турлари

Рақиб томонидан назоратда бўлган алоқа канали орқали узатиладиган хабарнинг махфийлигини таъминлаш муаммоси криптографиянинг анъанавий масалаларидан ҳисобланади. Шундай қилиб компьютер тармоқларида ахборот хавфсизлигини таъминлашнинг асосий криптографик усулларига шифрлаш, электрон рақамли имзо киради. Компьютер тармоқларида ахборот хавфсизлиги муаммосини ечиш учун криптографик усуллар ичида энг муҳимларидан бири аутентификация масаласидир. Аутентификация электрон рақамли имзо ва сертификат билан таъминланади [3].

Бутунликни таъминлаш деганда ахборотни рухсатсиз ўзгартириб бўлмаслигининг кафолати тушунилади. Бутунликни кафолатлаш учун маълумотлар бўйича бирон-бир ўзгартиришларни амалга оширишни аниқлайдиган содда ва ишончли мезон бўлиши керак. Бу ўзгартиришлар матнни ўчириш, алмаштириш, янгисини қўйиш орқали амалга оширилиши

мумкин. Ахборот бутунлигини назорат қилишнинг кўпроқ мақбул бўлган методларидан бири хэш-функциядан фойдаланиш ҳисобланади. Хэш-функциянинг қийматини унинг калитини билмасдан туриб қалбакилаштириб бўлмайди, шу сабабли хешлаш калитини шифрланган кўринишда ёки жиноятчининг «қўли етмайдиган» жойдаги хотирада сақлаш керак.

Аутентификациялашни таъминлаш ахборотли ўзаро муносабат жараёнида ахборотнинг ўзини ва томонларнинг ҳақиқийлигини тасдиқлаш усулларини ишлаб чиқишни англатади. Алоқа канали орқали узатилаётган ахборот манбаи, яратилган санаси, ташкил этувчи маълумотлари, узатиш санаси ва шу кабилар билан аутентификация қилиниши керак.

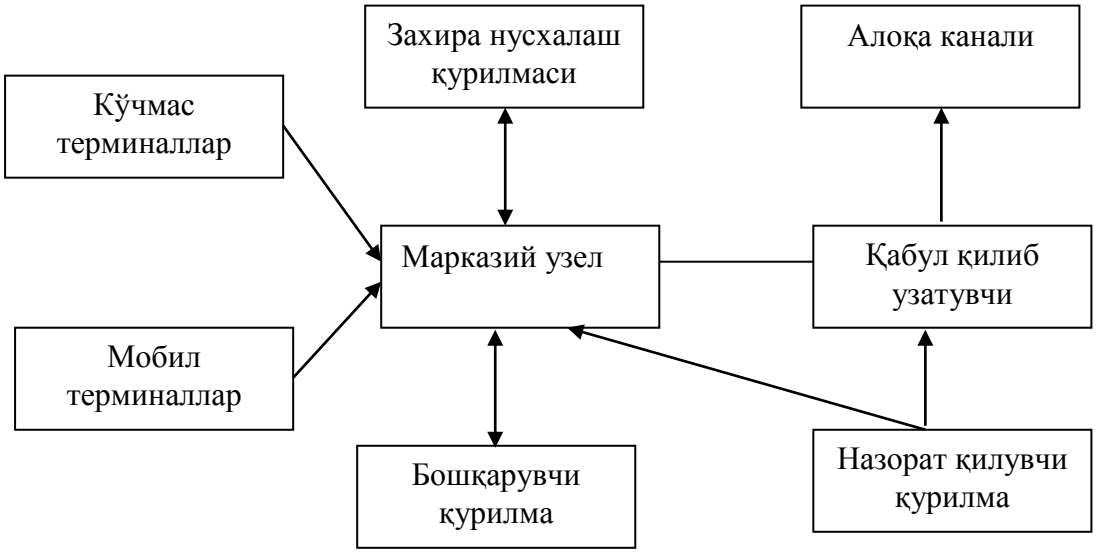
Муаллифликни инкор этолмасликни таъминлаш бу субъектлар томонидан амалга оширилган ҳаракатларни тан олмаслик ҳолати мумкинлигининг олдини олади.

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

АКҲВ қуйидаги асосий воситалардан ташкил топган:

- криптографик дастурий воситалар - бир ёки бир нечта криптографик усулларни ўзида мужассам этган, юқори ёки қуйи дастурлаш тилларида ёзилган алоҳида кутибхоналар 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 дастурий-аппарат воситалар – криптографик ҳимоя усулларини комплекс, яъни ҳам дастурий ҳам аппарат воситалар орқали амалга оширилади.

Криптографик ҳимоя воситалари принципиал фарқ қилсада, ахборот-коммуникацион тизимларида ахборот хавфсизлиги сиёсатига кўра қўлланилади. Умумий ҳолда криптографик ҳимоя воситалари ахборот-текоммуникация тизимларида қуйидаги тарзда фойдаланилади (2.6-расм):



2.6-расм. АКҲВнинг ахборот-телеккомуникация технологияларида қўллашдаги ўрни

Криптографик аппарат ҳимоя воситалар – махсус блок бўлиб, бу блок маълумотларни шифрлаш учун фойдаланиладиган қурилмалардан ташкил топган. Криптографик аппарат ҳимоя воситалари, шунингдек қўшимча ҳимоя функцияларидан иборат. Масалан, рухсатсиз фойдаланишлардан ҳимояловчи функция. Бундан ташқари, криптографик аппарат воситалар дастурий воситаларга талаб этилмайдиган қуйидаги қўшимча блоклардан иборат:

- 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 компьютер ҳам бўлиши мумкин. Бунда у марказий процессор билан махсус шина (тизим шинаси) орқали боғланади.

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 фойдаланиш;
- шахсий идентификаторлардаги калитлар билан шифрлаш тўғридан-тўғри аппаратнинг махсус процессорида амалга оширилиши;
- калитларни компьютернинг хотирасида эмас, балки шифрловчи процессор хотирасида сақланиши;
- тизим юклангунга қадар фойдаланувчиларни идентификация ва аутентификациядан ўтказиш имконияти;
- маълумотларни шифрлаш юқори тезликда амалга оширилиши.

Дастурий-аппарат ҳимоя воситалари дастурий ва аппарат ташкил этувчилар йиғиндисидан ташкил топган бўлиб, улар қуйидаги таянч модуллардан иборат:

- шифрлаш блоки (носимметрик шифрлаш тизимлари дастурий модуллар, симметрик шифрлаш 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.

Шунингдек Интернет тармоғида дастурий ҳимояланиш усулларига энг аввало ҳимояланган криптопротоколларни киритиш мумкин. Ушбу протоколлардан фойдаланилганда уланишни ишончли ҳимоя қилиш имконияти пайдо бўлади. Навбатдаги банда бугунги кунда мавжуд Интернет муносабатлари ва асосий ишлаб чиқилган протоколлар тўғрисида баён этилади. Масофадан туриб ҳужум қилишдан дастурий ҳимояланиш усулларининг бошқа синфига бугунги кундаги мавжуд дастурлар киради. Уларнинг асосий мақсади тармоқ трафигини масофадан туриб муайян актив таъсир қилишлар мавжудлиги предметини таҳлил қилишдир.

Ахборотни криптографик ҳимоялашнинг дастурий-аппарат воситаларидан бири аутентификация воситалари ҳисобланади. Уларга қуйидагиларни киритиш мумкин:

- **eToken;**
- **USB – калит / eToken PRO** смарт-картаси;
- **USB** – калит/ **eToken PRO** смарт-картаси (Java);
- Комбинациялашган **eToken NG – OTP USB** – калити;
- Комбинациялашган **eToken** NG - FLASH **USB** – калити;
- **eToken** PASS брелоки ва бошқалар.

eToken электрон калити - авторизация, аутентификация ва маълумотларни ҳимояланган сақлаш шахсий воситаси, рақамли сертификатлар ва электрон рақамли имзони қўлловчи дастурий-аппарат воситаси.(2.7-расм).

2.7-расм *eToken* электрон калитлари кўриниши

eToken USB-калит смарт-карталари ёки брелок шаклида чиқарилади. eToken NG-OTP модели ички ўрнатилувчи бир марталик пароллар генераторига эга. eToken NG-FLASH модели 4 гБайт ҳажмдаги flash-хотирали ички ўрнатилган модулга эга. eToken PASS модели фақат бир марталик пароллар генераторига эга. eToken PRO (Java) модели ЭРИ калитлари генерациясини ва ГОСТ Р 34.10-2001 стандарти бўйича ЭРИ шакллантиришни аппаратли амалга оширади.

eToken моделлари Россияда сертификатланган бўлиб, ундан фойдаланувчилар аутентификацияси ва ҳимояланганлик синфи G1 гача бўлган махфий ахборотни қайта ишловчи автоматлаштирилган тизимларда калитли ахборотларни сақлаш учун қўллаган маъқул. Улар сертификатланган ахборотни ҳимоялашнинг комплекс ситемаси (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW ва б.) учун калит маълумотларни ташишга тавсия қилинади.

eToken PRO (2.8- расм) смарт-карталар ва USB-калитлар смарт-карта микросхемалари базасида қурилган, аутентификация ва рақамли сертификатлар ва электрон рақамли имзо билан ишлашни аппарат жиҳатдан қўллаб-қувватловчи маълумотларни ҳимояланган сақлаш учун мўлжалланган.

2.8- расм. *eToken* PRO электрон калити кўриниши

USB-калит/eToken PRO (Java) смарт-картаси USB-калитлар ва eToken смарт-карталарининг янги авлоди – eTokenнинг функционал имкониятларини сезиларли даражада кенгайтирувчи ва унинг фойдаланиш кўламини кенгайтирувчи Java-карта базасида қурилган, аутентификация ва ахборот хавфсизлигини таъминловчи ечимдир.

Ушбу воситаларнинг қўлланилиши виртуал хусусий тармоқ қуришни ва улар ўртасида махфий алмашувни таъминлашни, Интернетга ҳимояланган ҳолда чиқиш ва масофавий (мобиль) фойдаланувчиларнинг хусусий тармоғидан ҳимояланган *on-line* фойдаланиш имкониятларини беради.

Нутқ ва ҳужжатли ахборотни кафолатланган криптографик ҳимоялашнинг Е-20 аппарати (2.9-расм) қуйидагиларни таъминлайди [4]:

- умумий фойдаланиш телефон аппарати режими;
- нутқни криптографик ҳимоялаш режими;
- узатиш ва ички ўрнатилувчи имитоҳимоя қурилмаси билан маълумотларни криптографик ҳимоялаш режими.

2.9-расм. Е-20 аппаратининг ташқи кўриниши

“Е14” аппарати (2.10-расм) рақамли ахборот потокларини шифрлаш аппарати ҳисобланади. Е14 ва Е14А маҳсулотлари дуплекс кабеллари, оптик толали, радиорелели каналлари рақамли тизимларида узатилувчи, юқори тезликдаги махфий ахборот оқимларини криптографик ҳимоялаш учун мўлжалланган. Калит узунлиги 256 бит [4].

2.10-расм. Е 14 рақамли ахборот потокларини шифрлаш аппарати ташқи кўриниши

Хавфсизликни таъминлашнинг юқорида таърифланган усуллари кўпгина инфокоммуникацион тизимларни қуришнинг асоси ҳисобланади. Бу ахборот алмашинув тизими ёки тўловлар ўтказиш тизими бўлиши мумкин. Уларни ташкил этиш учун хавфсизлик масалаларининг муҳимлиги аҳамиятлидир.

Юқорида келтирилган ахборот хавфсизлигини таъминлаш усуллари билан бирга бугунги кунда инфокоммуникацион тармоқлар хавфсизлигини таъминлашнинг кенг тарқалган механизмлари қуйидагилар ҳисобланади:

- Интернет орқали узатиладиган маълумотлар шифрланишини таъминловчи SSI (Secure Socret Layer) протоколи;

- Visa ва MasterCard компаниялари томонидан ишлаб чиқилган ва пластик карталар ёрдамида амалга ошириладиган келишувлар хавфсизлиги ва махфийлигини таъминловчи SET (Secure Elektronic Transactions) стандарти.

II боб бўйича хулоса

Инфокоммуникацион тармоқларда ахборот хавфсизлиги муаммоларининг ечими бугунги кунда ҳуқуқий, маъмурий, процедурали ва дастурий-техник чоралари орқали топиб борилмоқда. Виртуал хусусий

тармоқ VPNни ахборот узатилиши жараёнида ҳимоялашни амалга оширишдаги имкониятлари ёритилди.

Тармоқ маъмурларига базавий пртоколлардан ўз тизимларининг ресурсларидан узоқдан туриб авторизация қилинган фойдаланишни тақдим этиш учун фойдаланишга йўл қўймасликни ва тармоқ трафигининг таҳлилини бартараф этиб бўлмайдиган, лекин уни IP-оқимнинг бардошли криптоалгоритмларини қўллаган ҳолда аҳамиятсиз қилиб қўйиш мумкин бўладиган таҳдид деб ҳисоблашни таклиф этиш мумкин.

Тармоқ орқали давлат, ҳарбий, тижорат ва хусусий таснифга эга катта ҳажмдаги маълумотлар узатилмоқда. Замонавий криптография ахборот хавфсизлигининг махфийлик, бутунлик, аутентификация ва томонларнинг муаллифликни инкор эта олмасликлари муаммоларини ҳал этувчи билим соҳаси ҳисобланади. Бу эса замонавий криптографик усуллардан фойдаланиш ўта долзарб эканлигини англатади.

Умуман олганда, компьютер тизимлари ва тармоқларида ахборот хавфсизлигини таъминлаш компьютер безорилари томонидан уюштирилган ҳужум ва хавфларни бошқариш ҳолатларини таҳлил қилиш ва уларнинг олдини олиш воситаларини ишлаб чиқишни тақозо этади.

III Боб. Инфокоммуникацион тармоқларда ахборот хавфсизлигини таъминлаш алгоритми ва унинг дастури

1. Криптографик алгоритмларни ишлаб чиқишга асос бўлган функциялар ва теоремалар

Ҳозирги кунда инфокоммуникацион тармоқлар хавфсизлигини таъминлаш криптографик алгоритмларга асосланган ҳолда амалга оширилмоқда. Криптографик алгоритмларнинг математик асосида бир томонлама осон ҳисобланадиган даражага ошириш, эллиптик функция, рекурсия, параметрли функция ва бошқалар ётади. Улар ахборот хавфсизлигининг барча муаммоларини ечиб беришга қодир деб тан олинган.

Бир томонлама функция – бу таъриф бўйича шундай $y = f(x)$ функцияки, унинг аниқланиш соҳасидан бўлган ихтиёрий x учун $f(x) = y$ қиймат осон ҳисобланиб, қийматлар соҳасининг барча y қийматларига мос келувчи x қийматларни ҳисоблаб топишнинг амалий жиҳатдан имконияти йўқ [1]. Яширин ёки махфий услубли бир томонлама функция, таъриф бўйича бирор $z \in Z$ параметрларга боғлиқ бўлиб, тескарисига эга бўлган шундай f_z функциялар синфики, берилган z параметрда аниқланиш соҳасидаги барча $x \in X$ аргументлар учун $f_z(x) = y$ қийматларни осон ҳисоблаш алгоритми E_z мавжуд бўлиб, қийматлар соҳасидаги барча $y \in Y$ қийматлар учун $f_z^{-1}(y) = x$ қийматлар маълум бўлган E_z алгоритм билан ҳисоблашнинг имконияти йўқ (ёки бошқача айтганда $f_z^{-1}(y) = x$ қийматларни ҳисоблаш сарф-ҳаражатлари ва вақти мақсадга мувофиқ эмас). Бундай таъриф математика нуқтаи назаридан аниқ бўлмасада, амалий криптология масалаларида самарали қўлланилиши мумкинлигига шак-шубҳа йўқ.

Криптографик назарияларда турли хил усуллар билан ахборотларни муҳофаза қилиш жараёнлари кўйилгандир. Ҳар бир усул ўз имкониятлари билан бир-биридан ажралиб, ютуқ ва камчиликларга эга. Ушбу усуллар

қаторига Ферманинг кичик теоремаси ва Эйлер функциялари киради, улардан криптографик алгоритмларни ишлаб чиқишда фойдаланилади.

Теорема. Шундай бутун *u* ва*v* сонлари топилсаки, улар учун *au+bv=1* тенглик ўринли бўлса, бутун *a* ва *b* сонлари ўзаро туб бўлади.

Бу теоремани қуйидагича ҳам ифодалаш мумкин: *бутун a ва в сонлари ўзаро туб бўлиши учун, бутун бўлган и ва*v *сонлари топилиб, улар учун au+bv=1 тенгликнинг бажарилиши зарур ва етарли.*

Агар бутун *a* ва *b* сонлари ўзаро туб бўлса, яъни $(a,n)=1$ бўлса, у ҳолда ушбу $a\ a' \equiv 1 (\mathrm{mod}\ n)$ муносабатни қаноатлантирувчи бутун a' сони мавжуд бўлиб, бу a' сон *a* сонига модул *n* бўйича тескари дейилади, ҳамда, $a' \equiv a^{-1} (\mathrm{mod}\ n)$ деб белгиланади. Тескари a' элементни *a* ва *n* сонларининг чизиқли комбинациясидан иборат бўлган уларнинг ЭКУБ ифодаси $au+bn=1$дан фойдаланган ҳолда, бу тенгликнинг ҳар иккала томонини модул *n* бўйича ҳисоблаш билан $a' \equiv u\ (\mathrm{mod}\ n)$ эканлиги топилади.

Қуйида тескари элементни ҳисоблашнинг яна бир усули келтирилади.

Берилган *n* сони билан ўзаро туб бўлган $(1;n)$ ораликдаги барча элементларнинг сони билан аниқланувчи $\varphi(n)$ функцияга *Эйлер функцияси* дейлади [1:

$\varphi(n)=|M|$, бу ерда $|M|$ M – тўпламнинг қуввати, $M=\{m_i \in N : 1 \le m_i \le n;\ \ (m_i,n)=1\}$.

Агар $n = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$ бўлиб, $p_1,\ldots,p_t$ - ҳар хил туб сонлар бўлса, у ҳолда Эйлер функциясининг қиймати $\varphi(n)=\prod_{j=1}^{t}\left(p_j-1\right)\cdot p_j^{k_j-1}$ ифода билан ҳисобланади.

Ферманинг кичик теоремаси деб аталувчи ушбу тасдиқ ўринли: агар *n* – туб сон бўлса, $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$ ўринли.

Эйлер томонидан олинган, *Ферманинг кичик теоремасининг умумлашгани* деб аталувчи ушбу тасдиқ ўринли, агар *n* –туб сон бўлса, у ҳолда $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$ муносабат бажарилади.

Юқоридагилардан келиб чиққан ҳолда $a^{-1} \equiv a\ \varphi(n)-1 \pmod{n}$ муносабатнинг ўринлигига ишонч ҳосил қилинади.

Агар n – туб сон бўлса, у ҳолда $\varphi(n)=n-1$. Агар $n=pq$ бўлиб, p ва q –туб сонлар бўлса, у ҳолда $\varphi(n)=(p-1)(q-1)$. Бу каби хоссалардан очиқ калитли криптоалгоритмлар яратишда фойдаланилади. Масалан, қандай сон модуль 7 бўйича 5 сонига тескари эканлигини топайлик. Бу ерда, 7 сони туб бўлгани учун, унинг Эйлер функцияси $\varphi(7)=7-1=6$, модул 7 бўйича 5 сонига тескари сон эса $a^{-1} \equiv a\varphi(n)-1 \pmod{n}$ формулага кўра $5^{-1}=5^{6-1} \bmod 7 = 5^5 \bmod 7 = 3125 \bmod 7 = 3$. Ҳақиқатан ҳам, $5 \cdot 3 \bmod 7 = 15 \bmod 7 = 1 \bmod 7 = 1$. Бирор модул бўйича берилган сонга тескари бўлган сон ҳар доим ҳам мавжуд бўлавермайди. Мисол учун, 5 сонига модул 14 бўйича тескари сон 3 $5 \cdot 3 \bmod 14 = 15 \bmod 14 = 1 \bmod 14 = 1$. Аммо, 2 сонининг модул 14 бўйича тескариси мавжуд эмас, яъни $2x \equiv 1 \pmod{14}$ёки $2x=14k+1$ тенглама x ва k номаълумларнинг бутун қийматларида ечимга эга эмас, чунки, x ва k номаълумларнинг бутун қийматларида, ҳар доим, тенгликнинг чап томонида жуфт сон, ўнг томонида эса тоқ сон ҳосил бўлади.

Умумий ҳолда, агар, a ва n сонлари ўзаро туб бўлса, тенглама $a^{-1} \equiv x \bmod n$ ягона ечимга эга бўлади; агар, a ва n сонлари ўзаро туб бўлмаса, у ҳолда $a^{-1} \equiv x \pmod{n}$ тенглама ечимга эга эмас. Бевосита ҳисоблашлар асосида, ушбу $(a * x) \bmod n = b$ тенглама a,n,b – сонларининг қандай қийматлар қабул қилишига қараб, ёки бир нечта ечимларга эга бўлиши мумкинлигига, ёки битта ҳам ечимга эга бўлмаслигига ишонч ҳосил қилиш мумкин.

Қуйидагиларни таъкидлаш жоиз: агар M сонини a сонига бўлинса, ва b сони ҳам M сонига бўлинса, у ҳолда $M \in N$ сони $a,b \in Z$ сонларнинг *умумий бўлинувчиси* (*карралиси*) дейилади.Умумий бўлинувчилар ичида энг кичиги *энг кичик умумий бўлинувчи* дейилади ҳамда, $[a,b]$ деб белгиланади.

Криптотизимларнинг математик асоси бўлиб чекли майдон, гуруҳ, қисмгуруҳ кўринишидаги алгебраик тизимлар ва уларда криптографик

алгоритмга асос қилиб олинган модуль арифметикасининг махфийлик (секрет, лазейка)ка эга бир томонлама функция хизмат қилади [18]. Бир томонлама функцияларнинг биринчи тури $y \equiv a^x (mod\ p)$ туб майдон $F(p)$ ҳосил қилувчи элемент a ни махфий x даражага ошириш функцияси кўринишида У. Диффи ва М. Хеллман томонидан таклиф этилган, бу ерда (a, y, p) ошкора параметрдир. Улар субъектлар жуфти А ва В орасида умумий калит ўрнатиш масаласини ҳар бир субъект томонидан мос тарзда, $y_A \equiv a^{xA} (mod\ p)$ ва $y_B \equiv a^{xB} (mod\ p)$ функцияларни ҳисоблашга, сўнгра уларни ошкора канал орқали айирбошлашга ва субъектлар жуфтлигининг ҳар бири томонидан умумий махфий калитни, мос тарзда, $K_A \equiv y_B^{xA} (mod\ p)$, $K_B \equiv y_A^{xB} (mod\ p)$ ифодалар бўйича ҳисоблашга келтиришган, бу ерда $K_A = K_B$.

У. Диффи ва М. Хеллман ўзлари номида таърифланган дискрет логарифм муаммосига тенг кучли муаммони ҳам илгари сурдилар [19]:

агар туб модуль p, $GF(p)$ чекли майдоннинг ҳосил қилувчи (генератор) элементи a ва дискрет даражага ошириш функциялари қийматлари $y_A \equiv a^{xA} (mod\ p)$ ва $y_B \equiv a^{xB} (mod\ p)$ берилган бўлса, унда $y_A \equiv a^{xA} (mod\ p)$ ва $y_B \equiv a^{xB} (mod\ p)$ топилсин.

1973 йилда Британия давлат GCHQ агентлигининг криптологи Клиффорд Кокс аслида ошкора криптотизимни баён этувчи ёпиқ ҳужжатни тайёрлади [3]. Бу криптотизим бардошлилиги К. Кокс томонидан таклиф этилган бир томонлама функциянинг иккинчи турига, яъни факторлаш муаммосининг мураккаблигига асосланган.

1977 йилда америкалик Р. Райвест, А. Шамир, Л. Адлеман томонидан бир томонлама функцияларнинг иккинчи тури $y = f(d) (mod\ n)$ кўринишда таклиф этилган ва улар томонидан шифрлаш ва ЭРИ алгоритми RSA ишлаб чиқилган. RSA алгоритмида модуль $n = pq$ бўлиб, бу ерда p, q ҳар хил туб сонлардир. Лекин, К. Кокс томонидан аввалроқ RSA алгоритмига ўхшаш алгоритм яратилганлиги RSA муаллифларининг шуҳратига соя сола олмайди, чунки улар махфий ишланмани билмаган ҳолда ўз алгоритмларини мустақил яратганлар. Алгоритмда ошкора калит сифатида (n, e) жуфтликдан, шахсий

калит сифатида (*d, φ(n))* жуфтлигидан фойдаланилади, бу ерда *(d, e)* – бир-бирига модуль *φ(n)* бўйича мультипликатив тескари бутун сонлар жуфти, *φ(n) = (p-1)*(q-1)* – Эйлер пи-функцияси.

Алгоритмнинг асосий процедуралари хэшлаш ва модуль арифметикасида бутун сонли ҳалқада даражага оширишдан иборат.

Ўзбекистон Республикасида ҳам криптография соҳасида ишлар бошланганига 15 йил бўлди ва O'z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари» давлат стандарти ишлаб чиқилди [3]. O'z DSt 1092:2009 ни яратиш учун математик асос сифатида параметрли алгебра қабул қилинган. Унда модул арифметикасининг яширин йўлли янги бир томонлама функцияси қўлланилади. Янги параметрли функция асосида нафақат мавжуд носимметрик криптотизимларни улар билан тенг бардошлиликка эга бўлган уларга ўхшаш криптотизимлар яратиш, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд носимметрик криптотизимларга нисбатан юқори бардошлиликка эга бўлган криптотизимлар яратиш имкониятлари мавжуд.

Магистрлик диссертация ишида таклиф этилаётган янги алгоритмларни ишлаб чиқишда даража параметри муаммосидан фойдаланиш кўзда тутилган. Даража параметри муаммоси қуйидагича таърифланади: Агар параметрли гуруҳ *(F_p; ®)* да гуруҳ ташувчиси F_p нинг *g* ва *y* элементлари берилган бўлса, *R* параметр ва даража кўрсаткичи *x* ни топинг; бу ерда $y = g^{\backslash x}$ (mod *p)p* модули бўйича *R* параметр билан *g* нинг *x*-даражасини ифодалайди, бунда *p*– туб сон, *R*< *p*.

Қуйида анъанавий алгебрада яратилган носимметрик криптотизимлардан параметрли алгебра амалларидан фойдаланган ҳолда носимметрик криптотизим яратиш усули келтирилган [3].

Таъриф. Носимметрик криптотизимларни параметрли алгебра асосида яратиш усули криптотизим яратиш усулига асосий прототип танлашдан, прототипда фойдаланилган чекли бутун сонлар майдони устида берилган

қўшиш +, кўпайтириш *, тескарилаш $^{-1}$, даража *e* га ошириш $\uparrow^{e}$ амалларини ҳамда бирлик элементи *1*, ноллик элементи *0* ни мос тарзда параметрли алгебрада, ўзаро мос тарзда,қўшиш +, кўпайтириш ® (*R>0)*, тескарилаш *($^{-1}$)*, бирлик элементи *0*, параметрли қўшиш $®_0$(*R=0)*, кўпайтириш ® (*R>0)*, тескарилаш $\backslash^{-1}$ (*R>0)*, даража *e* га ошириш $\backslash^{e}$ (*R>0)* амаллари билан ҳамда бирлик элементи *0* (*R>0),* ноллик элементи *0* (*R=0)* билан алмаштиришдан ҳамда усулни синовдан ўтказишдан иборат.

Мазкур усул носимметрик криптотизимлар алгоритмларида анъанавий алгебраларда ўрнатилган амаллар ва элементлар рамзлари сатрини

	*	1	1	0	+	*	1	e		

параметрли алгебрада ўзаро мос тарздақўшиш +, кўпайтириш ®(*R>0)*, устунни тескарилаш $^{-1}$, устун бирлик элементи *0*, қўшиш $®_0$ (*R=0)*, кўпайтириш ® (*R>0)*, тескарилаш $\backslash^{-1}$, даража *e* га ошириш $\backslash^{e}$ (*R>0)* амаллари билан ҳамда бирлик элементи *0* (*R>0),* ноллик элементи *0* (*R=0)* рамзлари сатри

	$®_3$	d1	0	0	$®_0$		-1	$\backslash^{e}$	0	0

билан алмаштириб, криптотизим параметрлари тўпламига қўшимча тарзда камида битта бутун сонли параметр *R>0* белгилашдан иборат.

Бу ерда иккала сатрда ҳам $\uparrow^{e}$ ни $\backslash^{e}$ га алмаштиришда бутун сонли даража кўрсатгичлари бир хил эканлигини унутмаслик лозим. Бинобарин, усул прототипда фойдаланилган даража кўрсаткичларига оид тақкосламаларга тегишли бўлмай, ушбу тақкосламалар ўзгаришсиз қолади.

Таклиф этилаётган алгоритмда параметрли группадаги бир томонлама функция қўлланилади, бунда ҳисоблашлар қийинлик даражаси бўйича даражага кўтариш амаллари каби енгил амалга оширилади, функция

тескарилаш эса дискрет логарифм муаммосини ечиш жараёнидагидан кам бўлмаган ҳисоблаш сарфлари ва вақтни талаб қилади. Асосий амаллар бўлган кўпайтириш, даражага кўтариш ва тескарилаш параметрли группада параметр биланкўпайтириш, даражага кўтариш ва тескарилаш деб аталган. Бир томонлама даражага кўтариш функцияси ушбу бир томонлама функциянинг хусусий ҳолидир.

Асос X ни p модуль бўйича R параметр билан e даражага кўтариш амали қуйидагича белгиланади: $X^{\backslash e}(\mathrm{mod}\ p)$. Масалан, $e = 37$ учун параметр R бўлганда:

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

ифодага эга бўламиз,

бунда: $X^{\backslash 2}(\mathrm{mod}\ p) \equiv X(2 + XR)(\mathrm{mod}\ p)$;

R параметр билан p модули бўйичакўпайтириш амали

$X \circledR Y(\mathrm{mod}\ p) \equiv X + (1 + X R)Y(\mathrm{mod}\ p)$каби ифодаланади.

X ўзгарувчининг p модуль бўйича R параметр билан тескарилаш амали $X^{\backslash -1}$ кўринишда белгиланади ва қуйидагича ифодаланади:

$$X^{\backslash -1} \equiv - X(1 + XR)^{-1}(\mathrm{mod} p).$$

2. Параметрли функция асосида такомиллаштирилган алгоритм ва унинг дастури

Инфокоммуникацион тармоқлар ахборот хавфсизлигини таъминлаш учун аутентификация масаласини ҳал этиш муҳим роль ўйнайди. Инфокоммуникацион тармоқларда аутентификация масаласи электрон рақамли имзо алгоритмлари ёрдамида амалга оширилади. Қуйида ҳозирги кунда кўп қўлланиладиган RSA электрон рақамли имзо алгоритми баён этилади [1].

RSA электрон рақамли имзо алгоритми

RSA алгоритми шифрлаш ва электрон рақамли имзолар учун яратилган биринчи мукаммал ошкора калитли алгоритм ҳисобланади. RSA алгоритмининг хавфсизлиги катта сонларни кўпайтувчиларга ажратиш (факторлаштириш муаммоси)нинг мураккаблигига асосланади.

RSA алгоритмида ошкора модул n икки туб соннинг кўпайтмаси бўлиб, кўпайтувчилар сир тутилади. Бу туб фактор (кўпайтувчи)ларни n бўйича топиш, яъни факторлаштириш муаммоси ечиш ўта мураккаб муаммолар сирасига кириши криптотизимнинг юқори бардошлилигини таъминлайди. Кўпайтувчилардан битта кам сонлар кўпайтмаси иккинчи модул (Эйлернинг пи-функцияси $\varphi(n)$) бўлиб, у ҳам сир тутилади. Иккинчи модул бўйича ўзаро тескари икки сондан бири e шахсий ошкора калит, иккинчиси d шахсий махфий калит деб қабул қилинади.

RSA алгоритми бўйича ЭРИни шакллантириш ва узатиш қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1) M ахборот учун хэш-функция ҳисобланади:

$m = H(M);$

2) модул n ва махфий калитдан фойдаланиб m учун ЭРИ S шакллантирилади:

$S = m^d \pmod n;$

3) ахборот M ва ЭРИ S алоқа каналидан узатилади.

Қабул қилувчи томон олинган ахборот M ва ЭРИ S дан фойдаланиб қуйидаги қадамлар кетма-кетлигини амалга оширади:

1) ошкора калит (n, e) дан фойдаланиб S учун хэш-функция қиймати m шакллантирилади:

$m = S^e \pmod n;$

2) M ахборот учун хэш-функция ҳисобланади:

$m' = H(M);$

3) m билан m' таққосланади:

$m = = m'.$

Агар таққосланган қийматлар тенг чиқса, у ҳолда ахборот олувчи *(M, S)* жуфтлигининг ҳақиқийлигини тан олади. *M* ахборотдаги ЭРИ *S* ни фақат *d* махфий калит эгасигина шакллантириши мумкинлиги ўз тасдиғини топади, акс ҳолда ЭРИ ҳақиқий эмас деб топилади.

RSA рақамли имзо алгоритми камчиликлардан ҳам ҳоли эмас. *n* модулни ҳисоблашда RSA рақамли имзо тизими учун калитларни катта миқдордаги қўшимча шартлар бўйича албатта текшириш зарур. Муҳим ҳужжатларни имзолашда ҳатто назарий жиҳатдан ҳам хавфга йўл қўйиш мумкин эмас.

Шуни айтиб ўтиш керакки, криптографик алгоритмларнинг крипто таҳлилларга бардошлилиги криптотизимни амалиётга татбиқ қилишда томонларнинг келишиб олинган тартиб-қоидалари мажмуи - криптотизим протоколига ҳам жуда боғлиқ бўлади. RSA криптотизими ҳозирда ҳам ошкора калитли тизим сифатида энг бардошли тизимлар қаторида туради. RSA алгоритми ҳозирги кунда ҳам мукаммал ошкора калитли алгоритмлигини инобатга олган ҳолда диссертация ишида уни параметрли алгебра амалларидан фойдаланиб такомиллаштириш мақсадга мувофиқ деб топилди.

Қуйида параметрли алгебра амаллари ёрдамида такомиллаштирилган RSA алгоритми келтирилган.

RSA алгоритмида ошкора модул *n* икки туб соннинг кўпайтмаси бўлиб, кўпайтувчилар сир тутилади. Кўпайтувчилардан битта кам сонлар кўпайтмаси иккинчи модул, яъни Эйлернинг пи-функцияси $\varphi(n)$ бўлиб, у ҳам сир тутилади. Иккинчи модул бўйича ўзаро тескари икки сондан бири *e* шахсий ошкора калит, иккинчиси *d* шахсий махфий калит деб қабул қилинади.

RSA алгоритми бўйича ЭРИни шакллантириш узатиш қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1) *M* ахборот учун хэш-функция ҳисобланади: Хэш-функция сифатида Ўзбекистон давлат стандарти 1106:2009 дан фойдаланилади:

$m = H(M);$

2) модул n ва махфий калитдан фойдаланиб m учун ЭРИ S шакллантирилади:

$S = m^{\backslash d}(modn);$

3) ахборот M ва ЭРИ S алоқа каналидан узатилади.

Қабул қилувчи томон олинган ахборот M ва ЭРИ S дан фойдаланиб қуйидаги қадамлар кетма-кетлигини амалга оширади:

1) ошкора калит (n, e) дан фойдаланиб S учун хэш-функция қиймати m шакллантирилади:

$m = S^{\backslash e}\ (mod\ n);$

2) M ахборот учун хэш-функция ҳисобланади:

$m' = H(M);$

3) m билан m' таққосланади:

$m = = m'.$

Агар таққосланган қийматлар тенг чиқса, у ҳолда ахборот олувчи (M, S) жуфтлигининг ҳақиқийлигини тан олади. M ахборотдаги ЭРИ S ни фақат d махфий калит эгасигина шакллантириши мумкинлиги ўз тасдиғини топади, акс ҳолда ЭРИ ҳақиқий эмас деб топилади.

Бу ерда $^{\backslash d}$ - параметрли даражага ошириш амали.

Мазкур магистрлик диссертация ишида такомиллаштирилган RSA алгоритмининг дастури ишлаб чиқилди. Қуйидаги 3.1 ва 3.2-жадвалларда *RSA* алгоритмининг параметрли алгебрага асосланиб ишлаб чиқилган алгоритм билан қиёсий натижаларига доир мисоллар келтирилган.

3.1-жадвал

Мавжуд RSA алгоритми

n	p	q	$\Phi(n)$	E	d	m	S	m
77	**11**	**7**	**60**	**13**	**37**	**29**	**50**	**29**
143	**13**	**11**	**120**	**13**	**37**	**45**	**45**	**45**
323	**17**	**19**	**288**	**13**	**133**	**69**	**69**	**69**

3.2-жадвал

Такомиллаштирилган RSA алгоритми

n	*p*	*q*	*Ф(n)*	*e*	*D*	*R*	*m*	*S*	*m*
77	**11**	**7**	**60**	**13**	**37**	**3**	**29**	**29**	**29**
143	**13**	**11**	**120**	**13**	**37**	**4**	**45**	**6**	**45**
323	**17**	**19**	**288**	**13**	**133**	**5**	**69**	**229**	**69**

Юқоридаги жадвалда келтирилган натижалар шуни кўрсатадики, такомиллаштирилган RSA алгоритмида фақатгина махфий параметр киритилган.

Мазкур диссертация ишида ишлаб чиқилган такомиллаштирилган RSA алгоритмининг дастури C++ тилида ишлаб чиқилди. Ҳозирги вақтда C++, Object Pascal, Java, C# ва бошқа дастурлаш тиллари мавжуд бўлиб, улар орасида C++ тили ўзининг имкониятлари ва қўлланилиши кўламига кўра юқори ўринларда туради. Мутахассисларнинг фикрига кўра, C++ тили Ассемблер тилига энг яқин бўлиб, тезлик жиҳатидан Ассемблердан 10% орқада қолар экан. C++ дастурлаш тили C тилига асосланган. Ҳозирги кунда операцион системаларнинг асосий қисми C/C++ да ёзилмоқда. C дастурлаш тили машина архитектурасига боғланган тилдир. Аммо яхши режалаштириш орқали дастурларни турли компьютер платформаларида ишлайдиган қилса бўлади.

Юқорида келтирилганларни инобатга олган ҳолда таклиф этилаётган алгоритмнинг дастури Microsoft Visual Studio 2008 муҳитида C++ дастурлаш тилида тузилди. C++ дастурлаш тилининг бошқа дастурлаш тилига нисбатан тезкор ва мобил бўлганлиги сабабли алгоритм учун шу дастурлаш тили танлаб олинди. Магистрлик диссертация ишида таклиф этилган алгоритмнинг C++ дастурлаш тилидаги кодлари иловада келтирилди.

Ҳар қандай ЭРИ алгоритми иккита қисмдан иборат:

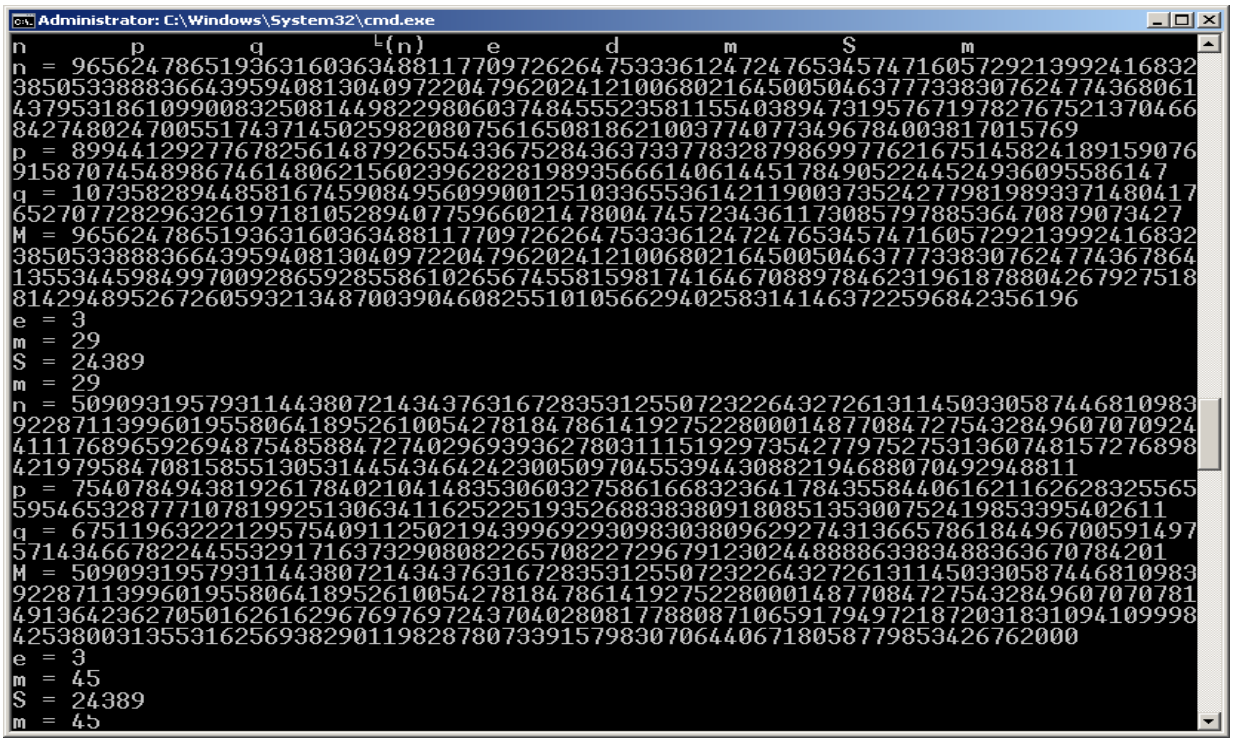
- имзо қўйиш;

- имзони текшириш.

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.

Электрон рақамли имзо қўйилган *M* маълумот хэш-функция хоссасига кўра $M=M_1$ бўлса, уларнинг хэш қийматлари ҳам тенг бўлади. Электрон рақамли имзони ҳисоблаш қисми имзо қўювчининг махфий калити ва имзоланиши керак бўлган имзонинг хэш қийматига боғлиқ бўлади.

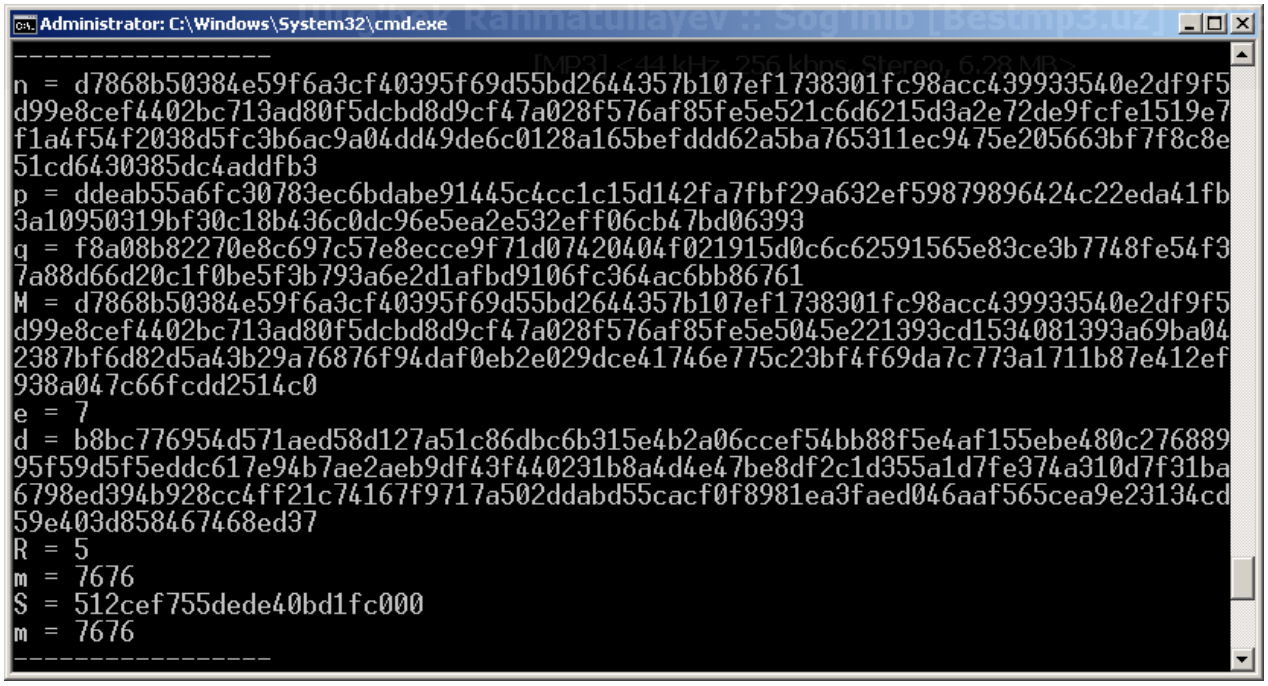
Мазкур ойнада (3.1-расм) мавжуд RSA электрон рақамли имзо алгоритмининг ташкилий босқичи жараёнида модул учун 1024 битли қиймат қабул қилинган. Бу ерда *M* – маълумотнинг хэш-функция қиймати бўйича ҳисобланган.



3.1-расм. Электрон рақамли имзони шакллантириш жараёни.

Имзони текшириш қисми имзо эгасининг очиқ калитига ва қабул қилиб олинган ҳужжатнинг хэш қийматига боғлиқ ҳолда амалга оширилади. Юқорида келтирилган натижалар буни исботини кўрсатиб турибди.

Мазкур ойнада (3.2-расм) такомиллаштирилган RSA электрон рақамли имзо алгоритмининг электрон рақамли имзони тасдиқлаш жараёнида модул учун 1024 битли қиймат қабул қилинган. Қийматлар 16 лик саноқ системасида келтирилди.



3.2-расм. Электрон рақамли имзони тасдиқлаш жараёни

Мазкур ойнада келтирилган қийматларда электрон рақамли имзо қўйилган *M* маълумотнинг хэш қийматлари тенг. Электрон рақамли имзо учун талаб қилинган исбот кўрсатилди.

3. Такомиллаштирилган алгоритмдан инфокоммуникацион тармоқларда фойдаланиш бўйича тавсиялар

Ҳар қандай тизимга алоҳида умумий талаблар бўлгани каби ахборотларни криптографик ҳимоя қилувчи алгоритмларга ҳам умумий

бўлган талаблар мавжуд. Ахборотларни криптографик ҳимоя қилувчи яратилаётган дастурий-аппарат воситаси ҳам шу талабларга мос ҳолда ишлаб чиқилиши зарур. Бу талаблар қуйидагича:

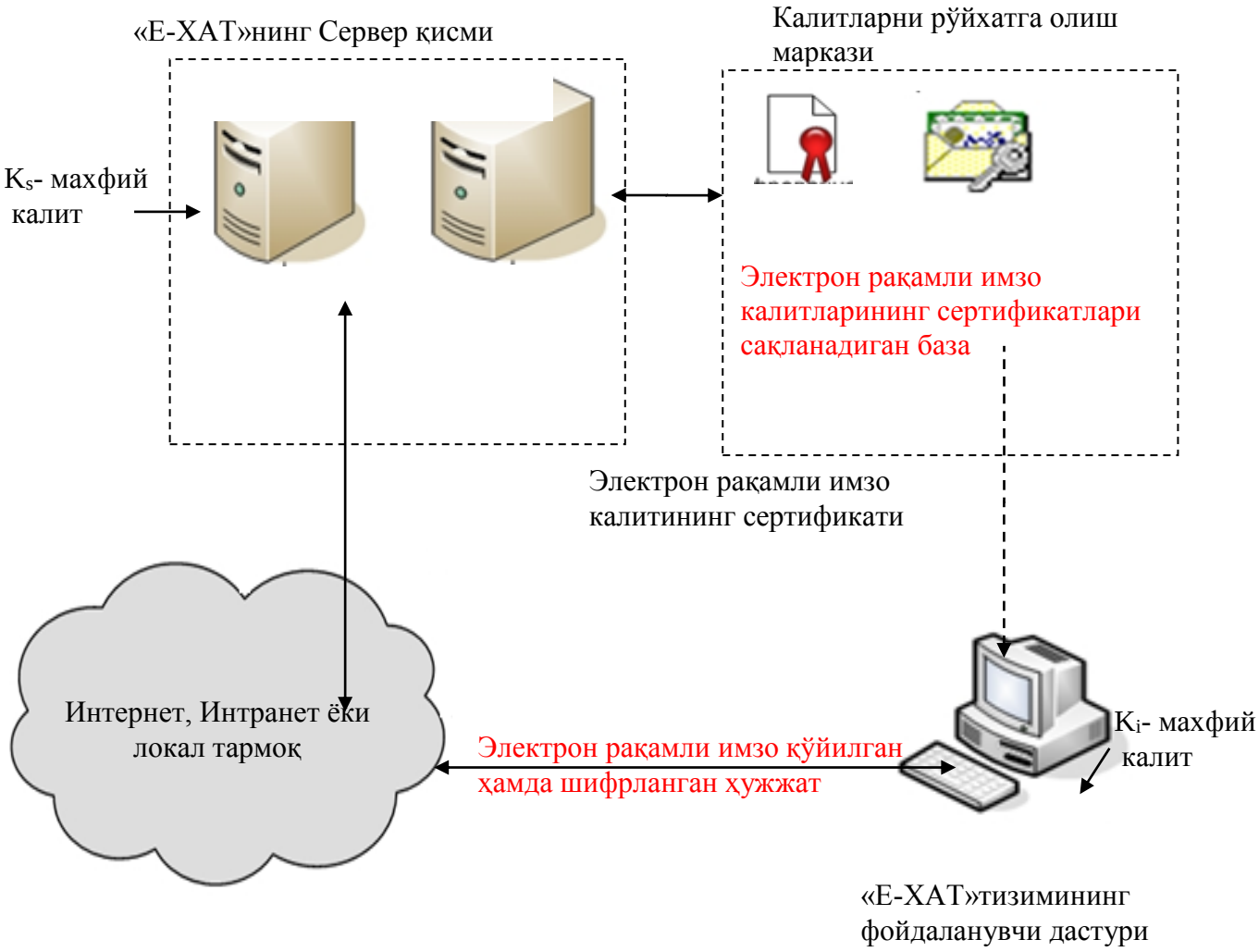
1. Алгоритм бутунлай аниқ ва лўнда бўлиши лозим;
2. Алгоритмнинг бардошлилиги фақатгина сир тутилишига эмас, балки унинг калитига боғлиқ бўлиши керак;
3. Шифрматн ва очиқ матнлар маълум бўлганда уларда ишлатилган калитни топиш вариантлари умумий калитлар вариантидан кам бўлмаслиги керак;
4. Алгоритм қўллаш жараёни самарали бўлиши лозим;
5. Алгоритмни тўғри ишлашини текшириш мураккаб бўлмаслиги керак;
6. Алгоритм аппарат-техник ва дастурий–аппарат таъминотини ишлаб чиқиш имкони бўлиши керак;
7. Алгоритм смарт-карталарга бемалол жойлаштириладиган бўлиши лозим, яъни алгоритмнинг дастурий таъминоти процессорнинг хотирасида катта жойни эгалламаслиги керак;
8. Калит узунлигининг ошиши алгоритм ишлашига салбий таъсир кўрсатмаслиги керак;
9. Шифрлаш жараёнида ишлатиладиган акслантиришлар мураккаб бўлмаслиги керак.

Инфокоммуникацион тизимларда катта ҳажмдаги маълумотлар алмашинуви олиб борилади, бу эса алгоритмнинг бутунлай аниқ ва лўнда бўлган ҳолатда криптотаҳлилчи учун етарлича катта ҳажмдаги маълумотларни криптотаҳлили учун баъзи бир қулайликларни олиб келади.

Инфокоммуникацион технологияларнинг жадал ривожланиб бораётганлиги бу юқорида санаб ўтилган талабларга қўшимча талайгина талабларни узлуксиз келтириб чиқармоқда ва бундай ҳолатларни

ахборотларни криптографик ҳимоя қилувчи дастурий-аппарат воситаларини яратишда ҳисобга олиниши доимо назарда тутилиши керак.

Муҳофазаланган электрон почта тизими ушбу тизим фойдаланувчилари ўртасида муҳофазаланган ўзаро хабарлар алмашишни ташкиллаштиришга қаратилган (3.3-расм).



3.3-расм. «E-XAT» электрон почта тизимининг инфратузилмаси

Мазкур диссертация ишида олинган натижалар шуни кўрсатадики, такомиллаштирилган RSA алгоритмида фақатгина махфий параметр киритилган. Мазкур *R* параметр электрон рақамли имзо алгоритмларининг бардошлилигини оширишга хизмат қилади. Шуларни инобатга олган ҳолда мазкур алгоритмдан муҳофазаланган электрон почта тизимларининг янги

версияларини ишлаб чиқишда ва хорижий тизимларда фойдаланиш мақсадга мувофиқдир. Таклиф этилган алгоритмдан муҳофазаланган электрон почта тизимида фойдаланиш аутентификация масаласини ҳал этишга имкон беради. Қатъий аутентификацияга асосланган криптографик алгоритмлар ёрдамида ахборот хавфсизлигини таъминлаш бугунги кунда энг самарали усул ҳисобланади.

III боб бўйича хулоса

Криптографик алгоритмларни ишлаб чиқишга асос бўлган функциялар ва теоремаларни тадқиқи натижасида Ўзбекистон Республикаси олимлари томонидан таклиф этилган параметрли янги бир томонлама функция асосида нафақат мавжуд носимметрик криптотизимларни улар билан тенг бардошлиликка эга бўлган уларга ўхшаш криптотизимлар яратиш, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд носимметрик криптотизимларга нисбатан юқори бардошлиликка эга бўлган криптотизимлар яратиш имкониятлари мавжудлиги кўрсатилди.

Инфокоммуникацион тармоқлар ахборот хавфсизлигини таъминлаш учун аутентификация масаласини ҳал этиш муҳим роль ўйнайди. Инфокоммуникацион тармоқларда аутентификация масаласи электрон рақамли имзо алгоритмлари ёрдамида амалга оширилишини инобатга олган ҳолда RSA электрон рақамли имзо алгоритмини параметрли функция асосида такомиллаштирилди ва унинг дастури ишлаб чиқилди.

Тадқиқотлар шуни кўрсатдики, такомиллаштирилган RSA алгоритмида фақатгина махфий параметр киритилганлиги электрон рақамли имзо алгоритмларининг бардошлилигини оширишга хизмат қилади.

Таклиф этилган алгоритмдан муҳофазаланган электрон почта тизимида фойдаланиш аутентификация масаласини ҳал этишга имкон беради. Шунингдек таклиф этилаётган мазкур алгоритмдан миллий электрон ҳужжат айланиш тизимларини ишлаб чиқишда фойдаланиш мақсадга мувофиқ.

Хулоса

Диссертация ишини бажариш натижасида қуйидаги натижалар олинди:

1. Инфокоммуникацион тармоқларни яратиш принциплари, инфокоммуникацион тармоқлар архитектурасининг асосий элементлари кўриб чиқилди. Инфокоммуникацион тармоқларга қўйиладиган ўзига хос талаблар таҳлил этилди.

2. Инфокоммуникацион тармоқларнинг функционал имкониятлари ёритилиб, хизматлар коммутацияси тугуни, хизматларни бошқариш тугуни ва хизматларни бошқариш тизимлари каби асосий компонентларни мужассам этувчи интеллектуал тармоқ архитектураси келтирилган.

3. Инфокоммуникацион тармоқларнинг ахборот хавфсизлигининг таъминлаш усуллари, тармоқларда ахборот хавфсизлигини таъминлаш усуллари, тармоқ протоколларининг ахборот хавфсизлигини таъминлашдаги аҳамияти, тармоқда қўлланадиган дастурий ҳимояланиш усуллари, тармоқ хизматларининг хавфсизлик протоколлари ва стандартлари каби масалалар кўриб чиқилди.

4. Тадқиқот натижалари шуни кўрсатдики, бугунги кунда инфокоммуникацион тармоқлар орқали амалга ошириладиган хизматларнинг хавфсизлигини таъминлашда энг ишончли усул сифатида ахборот хавфсизлигини таъминлашнинг криптографик усуллари тан олинган.

5. Илмий ишда инфокоммуникацион тармоқларнинг хавфсизлигини таъминлаш учун криптографик алгоритм ва унинг дастури ишлаб чиқилди. Такомиллаштирилган RSA алгоритми батафсил ёритилди. Натижалар шуни кўрсатадики, такомиллаштирилган RSA алгоритмида фақатгина махфий параметр киритилган. Параметр электрон рақамли имзо алгоритмларининг бардошлилигини оширишга хизмат қилади. Шуларни инобатга олган ҳолда мазкур алгоритмдан муҳофазаланган электрон почта тизимларининг янги версияларини ишлаб чиқишда фойдаланиш мақсадга мувофиқ.

Фойдаланилган адабиётлар рўйхати

Норматив-хуқуқий хужжатлар

1. «Замонавий ахборот-коммуникация технологияларини янада жорий этиш ва ривожлантириш чора-тадбирлари тўғрисида»ги» Ўзбекистон Республикаси Президентининг 2012 йил 21 мартдаги Қарори.

Ўзбекистон Республикаси Президенти асарлари

2. Каримов И.А. Жаҳон молиявий иқтисодий инқирози. Ўзбекистон шароитида уни бартараф этишнинг йўллари ва чоралари. – Т.: Ўзбекистон, 2009. – 56 б.

Дарслик ва қўлланмалар:

С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., “Aloqachi”. 2008, 382бет.

Илмий журналдаги қўлланмалар:

1. Зима В., Молдовян А., Молдовян Н. «Безопасность глобальных сетевых технологий». - 2-е изд.; «БХВ-Петербург», 2003. – 362 с.

2. Овчинников А.М., Лазин А.С. «Устройства защиты информации для средств УКВ-радиосвязи». Журнал «Специальная Техника", М. - №3 1998.

3. Венбо М. «Современная криптография: теория и практика». Издательский дом «Вильямс», 2005. – 764 с.

4. Э.Габидулин, Н.Пилипчук, О.Трушина “Защита информации в телекоммуникационных сетях” 2013.- том 5, №3, 97-98 с.

Асосий адабиётлар:

1. Л.Блахнов, В.Игнатенков “Инфокоммуникационные сети: основы построения”

2. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ – Москва: ТРИУМФ, 2002.

3. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. Тошкент, ФТМТМ, 2008.

4. Ю.В. Ветров, С.Б. Макаров «Криптографические методы защиты информации телекоммуникационных системах», 2011-глава 4-122с.

Қўшимча адабиётлар:

Ахмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.

Интернет сайтлари:

1. ЗАО «Голлард». «Аппаратный IP шифратор ЗАСЛОН». http://www.ip-zaslon.ru/index.htm.

2. Информационный портал Sec.ru. Оборудование. Рубрика «Защита информации». http://description.sec.ru.

3. Конфидент. Безопасность информационных систем. Собственная разработка. http://www.confident.ru/isc.

4. Российское средство аутентификации РУТОКЕН. http://www.rutoken.ru.

5. http://kikot.ru/ История связи Кубани

ИЛОВА

Такомиллаштирилган RSA алгоритмининг дастури

```
import java.math.BigInteger;
import java.security.SecureRandom;

public class RSA {
  private BigInteger n, d, e, m, p, q;

  private int bitlen = 1024;

  public RSA(int bits) {
                bitlen = bits;
                SecureRandom r = new SecureRandom();
                p = new BigInteger(bitlen / 2, 100, r);
                q = new BigInteger(bitlen / 2, 100, r);
                n = p.multiply(q);
                m =
(p.subtract(BigInteger.ONE)).multiply(q.subtract(BigInteger.ONE));
                e = new BigInteger("3");
                while (m.gcd(e).intValue() > 1) {
                        e = e.add(new BigInteger("2"));
                }
                d = e.modInverse(m);
  }

  public RSA(String pN, String qN, String eN) {
                p = new BigInteger(pN);
                q = new BigInteger(qN);
```

```
                n = p.multiply(q);
                m =
(p.subtract(BigInteger.ONE)).multiply(q.subtract(BigInteger.ONE));
                e = new BigInteger(eN);
                //System.out.print(m.gcd(e).intValue()+" - " + m +" - ");
                while (m.gcd(e).intValue() > 1) {
                  e = e.add(new BigInteger("2"));
                }
                d = e.modInverse(m);
  }
  public synchronized String encrypt(String message) {
    return (new BigInteger(message.getBytes())).modPow(e, n).toString();
  }

  public synchronized BigInteger encrypt(BigInteger message) {
    return message.modPow(e, n);
  }

  public synchronized String decrypt(String message) {
                return new String((new BigInteger(message)).modPow(d,
n).toByteArray());
  }

  public synchronized BigInteger decrypt(BigInteger message) {
                return message.modPow(d, n);
  }


  public synchronized BigInteger getN() {
                return n;
```

```
  }

  public synchronized BigInteger getE() {
                return e;
  }

  public synchronized BigInteger getD() {
            return d;
  }

  public synchronized BigInteger getM() {
            return m;
  }
  public synchronized BigInteger getP() {
            return p;
  }
  public synchronized BigInteger getQ() {
            return q;
  }

  public synchronized BigInteger diadaraja(BigInteger R, BigInteger N, BigInteger
m, BigInteger ed) {
            BigInteger d;
            BigInteger qadam;

            if(ed.equals(BigInteger.ZERO)) {
                    return new BigInteger("1");
            }
            else if(ed.equals(BigInteger.ONE)) {
                        return m;
```

```
        }
        else {
                qadam = new BigInteger("0");
                d = m;
            do {
                d = m.add(d.multiply(new
BigInteger("1").add(R.multiply(m)))).mod(N);
                    qadam = qadam.add(BigInteger.ONE);

            }while(!qadam.equals(ed.subtract(BigInteger.ONE)));
                return d;
        }
 }


 public static void main(String[] args) {
        String d[][] = {
                    {"11", "7",  "13", "29", "3"},
                    {"13", "11", "13", "45", "4"},
                    {"17", "19", "13", "69", "5"},
                    {"11", "17", "13", "13", "6"}};
        System.out.println("n\tp\tq\tΦ(n)\te\td\tm\tS\tm");
        for(int i=0; i < d.length; i++) {
                RSA rsa = new RSA(d[i][0], d[i][1], d[i][2]);
            String text1 = d[i][3];
            BigInteger plaintext = new BigInteger(text1);
            BigInteger ciphertext = rsa.encrypt(plaintext);
            plaintext = rsa.decrypt(ciphertext);
```

```
System.out.print(rsa.getN()+"\t"+rsa.getP()+"\t"+rsa.getQ()+"\t"+rsa.getM()+"\t"+r
sa.getE()+"\t"+rsa.getD()+"\t");
                    System.out.print(text1+"\t"+ciphertext+"\t"+plaintext);
                    System.out.println();

          }


        System.out.println("\n\nn\tp\tq\tΦ(n)\te\td\tR\tm\tS\tm");
        for(int i=0; i < d.length; i++) {
                RSA rsa = new RSA(d[i][0], d[i][1], d[i][2]);
                String text1 = d[i][3];
                BigInteger plaintext = new BigInteger(text1);
                BigInteger ciphertext = rsa.diadaraja(new BigInteger(d[i][4]),
rsa.getN(), plaintext, rsa.getE());
                plaintext = rsa.diadaraja(new BigInteger(d[i][4]), rsa.getN(),
ciphertext, rsa.getD());


        System.out.print(rsa.getN()+"\t"+rsa.getP()+"\t"+rsa.getQ()+"\t"+rsa.getM()
+"\t"+rsa.getE()+"\t"+rsa.getD()+"\t"+d[i][4]+"\t");
                System.out.print(text1+"\t"+ciphertext+"\t"+plaintext);
                System.out.println();
        }
  }
}
```