ТОШКЕНТ АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Ҳимояга
МУТ ва Т кафедра мудири
доц. У.Б. Амирсаидов
_____

2012___ й. “____”_____

«МОБИЛ АЛОҚА ТИЗИМЛАРИДА АХБОРОТ ХАВФСИЗЛИГИ ТАХЛИЛИ»

мавзуида

МАЛАКАВИЙ БИТИРУВ ИШИ

Битирувчи	**_____**	**Махкамов А.А.**
	(имзо)	**(Ф.И.Ш.)**
Раҳбар	**_____**	**Нурматова С.Б.**
	(имзо)	**(Ф.И.Ш)**
Тақризчи	**_____**	**_____**
	(имзо)	**(Ф.И.Ш)**
ХФХ	**_____**	**_____**
	(имзо)	**(Ф.И.Ш)**

Тошкент 2012

МУНДАРИЖА

КИРИШ

Замонавий ҳаммабоп телекоммуникацияларни ривожлантиришни стратегик мақсади юқори сифатли алоқани ҳар қандай истеъмолчига исталган вақтда ер шарининг исталган нуқтасига етказиб бериш хисобланади.

Бу ўринда гап хозирги жаҳон иқтисодий инқирозининг оқибатларини бартараф этиш, банк-молия тизимини мустаҳкамлаш, реал иқтисодиёт корхоналарига ёрдам кўрсатиш, янги иш ўринлари яратиш ва аҳолини ижтимоий ҳимоя қилиш каби чора-тадбирларни амалга оширишга эътибор қаратиш билан бирга, биз эртанги кунимизни, келажагимизни асло унутмаслигимиз зарурлиги ҳақида бормоқда.

Симсиз алоқа қурилмаларининг хавфсизлиги жуда мухимдир, чунки улар бутун тармоқ хавфсизлигига таъсир қилади. Симсиз алоқа қурилмаларини химоясини оширишга йўналтирилган харакатлар симсиз алоқа тармоғининг умумий хавфсизлиги даражасини оширишга катта таъсир ўтказади.

Охирги йилларда Ўзбекистонда кундан кунга харакатдаги объектлар билан радиоалоқа тизимлари назарияси ва амалиётида қўлланиши ривожланган сайин унга талаб тобора ортиб бормоқда. Ҳаракатдаги алоқа тизимини амалда

қўллаганда, яхши натижалар кўрсатади ва кейинчалик уларни такомиллаштиришни лозимлиги келиб чиқади.

Ҳозирги пайтда ҳаракатдаги радиоалоқа тизими қуйидагиларга бўлинади:

- персонал (шахсий) радиочақириқ тизими (Paging system);
- ҳаракатдаги профессионал (ҳусусий) радиоалоқа тизими (PMR, PAMR);
- ҳаракатдаги уяли радиоалоқа тизими (Callular Radio System);
- симсиз телефонлар тизими (Cardless Telephony).

Биринчи шахсий ҳаракатдаги алоқа тизими деб “мультитон” шахсий чақириш тизимини ҳисобласа бўлади. Бу тизимда диспетчер абонентни қабул қилгич ёрдами билан чақиради.

Бундай тизимни юқорироқ даражада шахсий радио телефон орқали тизим ишида ва жамоат ТФ тармоғига диспетчер орқали сухбат ташкил қилиш мумкин. Бундай тизим билан корхоналар, касалхоналар, ишлаб чиқариш комплекслари ва бошқалар жихозланади (PMR, PAMR).

Радиотелефон хабари қабулини юқори халақитга чидамли бўлишини таъминлаш мақсадига йўналтирилган тизимларни лойихалашга асосий ахамият қаратилди ва бу йўналишда аниқ ютуқларга эришилди, бу ютуқлар ахборотни қабул қилиш сифати бўйича харакатдаги алоқа симли ТФ алоқа даражасига яқинлашди. Бу радио абонентлар кўпайишига олиб келади ва харакатдаги алоқага ажратилган частота ресурсини тўла тугашига олиб келди, бу эса ишлаб чиқарувчиларни ажратилган частота спекторини эффектив ишлатиш ва юқори ўтказиш қобилиятли тизимни яратиш сохасида катта изланишлар ўтказишга олиб келади. Бундай муносабатда энг қулайи харакатдаги уяли алоқа тизими (ХУАТ) тан олинди. Бу тизим янги қурилиш тузилишига ва алоқа ташкил қилишга эга бўлиб, аниқроғи бир тармоққа уланган кўпгина базавий станциялардан (BTS) иборат. Абонент станцияси (MS) ҳаракати жараёнида бир BTS дан бошқа BTS “эстафета равишда узатилади”, биринчи BTS команда (буйруқлари) бўйича автоматик равишда керакли частотали каналга ўтказилади

ва шу тарзда алоқани узулмаслиги таъминланади. ХУАТда ажратилган каналлар бир-биридан ҳимоя масофаси узоқлигида жойлаштирилган уяларда абонентлар томонида кўп маротаба такроран ишлатилади. Бундай қурилиш принципида актив частотали каналлар сони ошади, шу тарзда юқори ўтказиш қобилият ва частота спекторини янада эффектив ишлашини таъминланади (Cellular Radio Systems).

Симсиз алоқани қўлаган ҳолда, катта афзалликларга эришиш мумкин. У фойдаланувчиларга алоқани йўқотмаган ҳолда эркин ҳаракатланиш имконини беради, уланишни ташкил этишга катта имкониятлар яратади, шунингдек тармоқ қурилишида – корхоналарни бир-бири билан боғланиши учун юқори имконият яратади, шунингдек мос ҳолда тармоқ муҳитига кириш учун кўпгина қурилмалар пайдо бўлади. Лекин бунда симсиз технология ўзи билан доимий симли тармоқга нисбатан кўпроқ ҳавф туғдиради. Симсиз ҳавфсиз илова яратиш учун ҳамма имкониятларни симсиз “ҳужум”га қаратиш керак. Афсуски, илова тўлиқ ҳавфсиз бўлмайди, ҳимояланиш даражасини кўтариш учун симсиз технологияни юқори потенциаллик билан ўрганиш лозим.

Симсиз ва симли тармоқлар ўртасидаги асосий фарқ умуман назоратсиз тармоқнинг охирги нуқталари билан боғлиқ. Етарли кенг майдонда симсиз уяли тармоқ бошқарилмайди. Симсиз қурилмаларни ишлаб чиқарувчилар ўзини қурилмаларига ҳавфсизликни таъминловчи тизимларни олиб кириш муҳим эканлигини англаб етишди. Шунга қарамасдан симсиз алоқанинг кўпгина нозик жойлари ўрта истеъмолчини унчалик безовта қилмаяпти, лекин симсиз технологиялар ишлатилишининг сектори доимо кенгаймоқда, шунинг учун бизни (смс хабарлар орқали тарқаладиган) симсиз вируслардан кутилмаган хавф-хатарларни , шунингдек “хизмат кўрсатишни рад этиш” каби хужумларни кутиш мумкин. Худда Internetни ривожланиш даврида маълумотлар ҳавфсизлиги муаммоси жуда долзарб бўлган каби, симсиз технологияларнинг

тез тарқалиши симсиз алоқани ҳавфсизлигини таъминланиш борасидаги мавзуни янада машҳур қилади

1. МОБИЛ АЛОҚА ТАРМОҒИНИНГ СТРУКТУРАСИ ВА КЛАССИФИКАЦИЯСИ

1.1. Очиқ тизимларнинг ўзаро таъсири модели

Замонавий ҳаммабоп телекоммуникацияларни ривожлантиришни стратегик мақсади юқори сифатли алоқани ҳар қандай истеъмолчига исталган вақтда ер шарининг исталган нуқтасига етказиб бериш хисобланади. Шунга мувофиқ стандартлаштириш бўйича халқаро ташкилот (ISO — *International Standards Organisation)* томонидан умумий фойдаланиш алоқасининг мобил тармоқ концепцияси ишлаб чиқилди. Тармоқ остида сақланишни амалга оширадиган турлича маълумотларни қайта ишлайдиган ва ўтказиладиган кўпгина яъни бир – бири билан ўзаро таъсир остида бўлган системалар тушунилади.

Глобал тармоқ умумий фойдаланиладиган телефон тармоқларини уяли ва йўлдошли алоқа тизимларини бирлаштиради. У барча ҳар хил фойдаланувчи терминалларини (симли ва симсиз телефон аппаратлари шахсий компьютерлар

уяли ва йўлдош телефонлар факсимал алоқа аппаратлари) алоқа линиялари (кабелли оптик симсиз ва бошқалар). Коммутация тугунлари (идоравий), районли ва шаҳарлараро бошқарув роли ва техник ҳизмат кўрсатишни амалга оширади.

ISO томонидан ишлаб чиқилган эталон модель OSI *(Open Systems Interconnection),* одатда ISO/OSI модели сифатида кўрсатилади ва шу маънода базаси хисобланадики, баъзи бир системаларни тасвирлаш учун унинг компонентларининг бир қисми етарлидир. Алтернатив ракобат ҳусусияти борлигига қарамасдан, модель OSI ҳамма жойга ёйилишини қўлга киритди ва информацион тизим техникада концептуал асос сифатида кенг фойдаланилади.

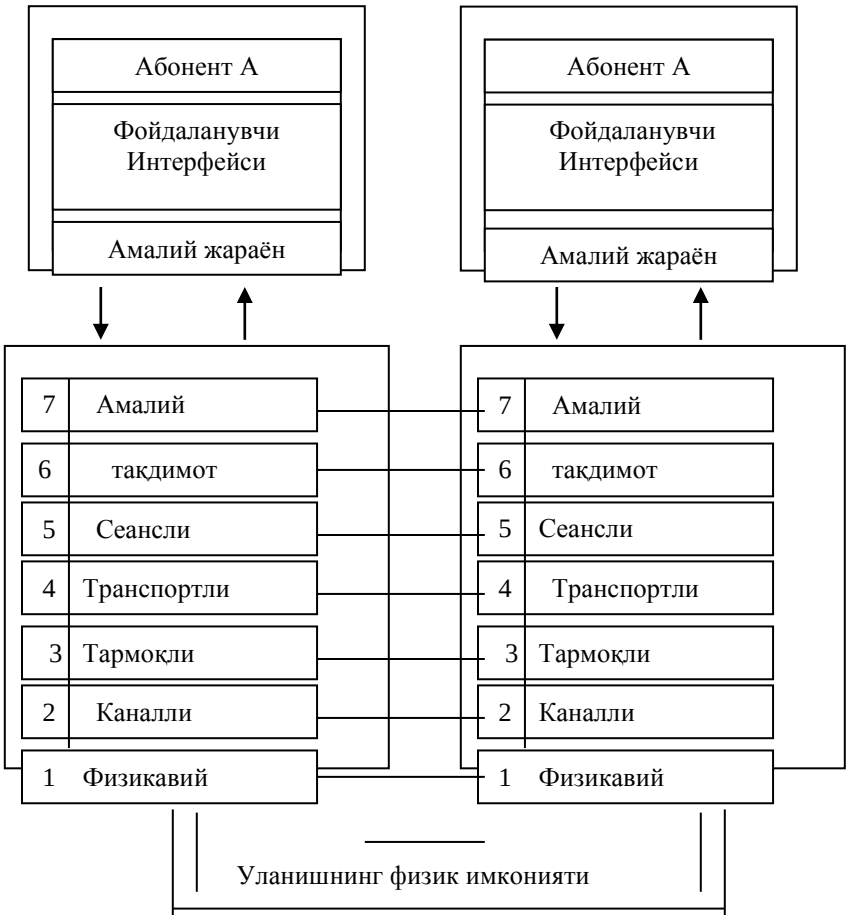
Очиқ система остида ҳалқаро ташкилот талабларини ёки ишлаб чиқарувчи талабларини қондирадиган, ўтказиш бозорни катта қисмини бошқарадиган тизим тушинилади, очиқлик тизим бирор кишини мулки эмаслигини англатади, бошқача қилиб айтганда хохлаган ишлаб чиқарувчи тизим ҳизматларига амалий киришга мўлжалланган шахсий махсулотни ишлаб чиқаришга ва сотувга қўйишга хаққи бор. Ишлаб чиқарувчилар орасида жиҳозларни нархини арзонлашишига сабаб бўладиган рақобат пайдо бўлади. Фойдаланувчилар бунда фақат битта ишлаб чиқарувчига боғлиқ бўлиб қолмайдилар ва аппаратура билан таъминловчиларини ўзгартириб туришлари мумкин. 1.1.- расмдаги диаграмма умумий кўринишда кўрсатилган элементларининг ўзаро таъсири ва базавий моделини даражасини схемасини тасвирламоқда. Бази бир тизимларни модели бу элементларнинг фақат бир қисмини ўз ичига олади. Шундай қилиб, коммутация канали тизимлари битта даражали модел билан тасвирланади. Ишлатиладиган терминалларни шарҳи қуйидагича:

Амалий жараён фойдаланувчи эхтиёжи учун маълумотларни қайта ишлашни ё баъзи бир аппарат программали асбоблари ёрдамида, ёки бевосита инсон миясида амалга оширади.

Интерфейс фойдаланувчиси ёрдамида абонент амалий жараёнга вазифа беради ва бажарилган натижани қабул қилади. Ўзаро таъсир қилиш минтақаси деб функционал блокларни тизимлараро маълумотлар алмашинуви учун мўлжалланган *иерархик* гурухи деб аталади. Бу функцияларни базали модели сатхлар, билан номланган 7 та ўзаро бўлиниб жойлаштирилган қатламлар қуйидаги 1.1. расмда берилган.

Физик уланиш воситалари — бу системалар орасидаги сигналларнинг узатилишини таъминловчи аппаратура ва тарқатиш муҳитининг бирлашмасидир.

Абонент фойдаланувчи интерфейси орқали илова процессига топшириқ беради ва уни бажариш натижасини олади



1.1 расм. Очиқ тизимларнинг ўзаро таъсири модели**.**

Юқоридаги етти у ёки бу амалий жараённи ўзаро таъсирининг турли хил кўринишларини таъминловчи амалий интерфейс хисобланади. Бу сатхда вазифавий бошқарув, электрон имзо адрес билан парол орқали фойдаланиши идентификациясини амалга оширади.

Тақдимот сатҳида керакли формага 7 – чи сатхдан келиб тушувчи хабарларни кодлаштириш амалга оширилади. Бу ерда хам зарурий жараёнда қисқа маълумотлар ва шифирлаш амалга оширилади.

Сеансли сатҳ у ёки бу амалий жараён орасидаги ўтказилган сеанслар жараёнини аниқлайди ва сақланиш ва уланишни узишни таъминлайди.

Транспорт сатҳ портлараро жойлаштирилган (500-2000 бит маълумот блоклари) виртуал канал пакетларига аниқ етказилишини таъминлайди.

Тармоқли сатҳ йўналишни виртуал каналларни маълумотлар бир портдан иккинчи портга ўтишини хосил қилади.

Каналли сатҳларда шакллантириш ва кадрларни улаш (маълумотлар блоклар) хатоларни топиш ва тузатишни амалга оширади.

Физик сатҳ физик уланиш тизим учун интерфейс ҳосил қилади. (Электрик ва оптик кабелларга, радио эфирга маълумотлар узатиш апппаратураси билан бирга). У бит эргашувчи узатувчига жавоб беради инкор ва хатоликлар пайдо бўлишидан огоҳ қилади .

Барча маълумотлар биринчи физик сатҳдан узатилади, шу билан бирга OSI моделидан мантиқий каналлар аниқланади, йўл тушунчасини берадиган, қайсики сигналлар ёки маълум номдан сатҳлар билан узатилади. Демак 4 – сатхни боғловчи *йўл транспортли канал* деб номланади, учинчи сатҳдаги йўл тармоқли, иккинчиси информацион ва ниҳоят хақиқий физик сатҳни уловчи йўл хисобланади.

Трафика (фойдаланувчи канал) мантиқий канал алоҳида ўринга эга бўлиб абонентлар орасида маълумот алмашинувини таъминлайди. Эталон модел сервиснинг *тиниқлиги* ва *кириш* хусусиятига эга.

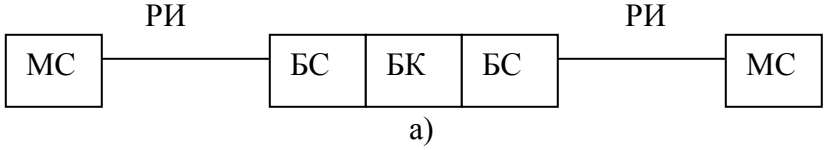
Тиниқлик шуни билдирадики маълумотлар қандайдир сатҳдан қуйи сатҳга ўтказилганда қабул қилинган томонга худди шу сатҳ ҳеч қандай ўзгаришсиз қайтади. Шундай қилиб қуйидагича кўриниш ҳосил бўладики, кўриб чиқувчи номдан сатҳлар қуйида мавжуд эмас – улар тиниқдир. Телефон тракти шаффоф объектга ёрқин мисол бўлиб ҳизмат қилади. Телефондан фойдаланувчи кўпгина инсонлар телефон каналидаги мавжуд ўзгартиришлар ҳақида хаттоки тушунчага ҳам эга эмаслар.

Сервисга кириш мумкинлиги юқоридаги ҳизматлар сатҳидан фойдаланиш имконияти тушинилади (маълумотлар) ихчамлиги тўсиқлардан сақлаш тасдиқланилмаган маълумотлардан фойдаланиш қуйи сатхларда бажарувчи (амалга оширувчи).

1.1 расмда линиялар билан, номдош сатҳлар боғловчиси қонунларнинг ўзаро таъсири объектлар қонунининг икки ёки ундан ортиқ ўзаро таъсири протоколларда белгиланади. Протоколлар номланиши мавжуд сатҳларни номланишига тўғри келади масалан, сеансли, транспортли, тармоқ протоколлари мавжуд.

1.2. Мобил алоқа тармоғи структураси

Асосий айниқса умумий алоқа тармоғи элементлари 1.2 расмда берилган. Улар мобил станцияларини (МС), базали станцияларни (БС), бошқарув маркази ва коммуникацияларни (БК), радиоинтерфейсларни (РИ) ўз ичига олади.



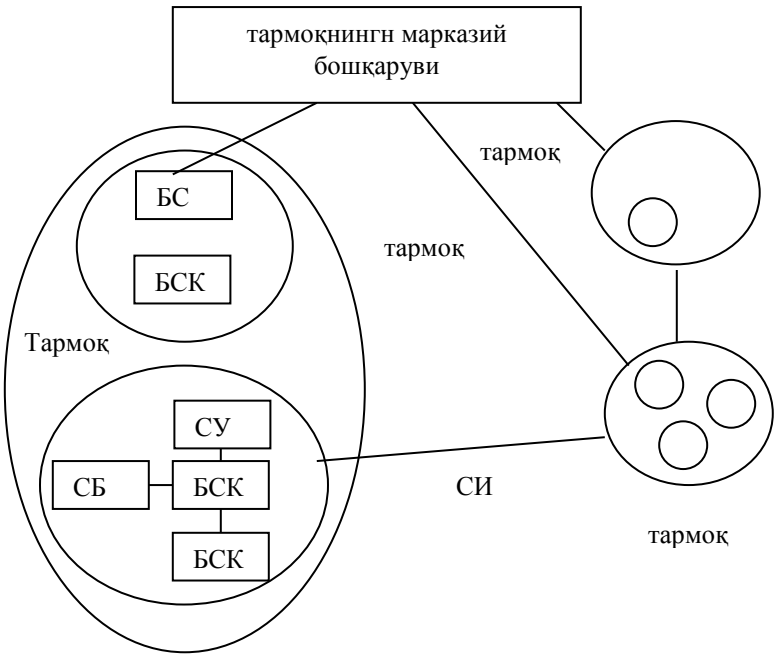
а)

РИ

1.2-расм. Алоқа тармоғи элементлари.

Мобил станциялар силжитувчи абонентлар ёрдамида қўлланилади. БС — кўчмайдиган маълумот узатувчиси стнанциялар аниқ замонда МС билан (ячейкада, сотада, секторда) радиоалоқани таъминловчилардир. БК да маълумотлар узатиш (коммуникация) йўналиши танланади.

Мобил станциялар БК орқали (1.2, а расм), ёки бевосита (1.2, б расм) маълумотлар белгиланади. Асосий элементлардан фойдаланган холатда мобил алоқа регионал ва миллий тармоқ (тармоқ ости) қуриш мумкин бу структура 1.3 расмда соддалаштирилган кўринишида берилган.



1.3-расм. Алоқа тармоғи структураси.

Алоҳида тармоқ ва тармоқ ости тармоқлараро интерфейслар ёрдами орқали ягона структурага бирлашади. (СИ) — кабелли иш радиотизими. Базали станциянинг контроллерлари (БСК) коммутатция функцияларини амалга оширади БС бошқарув, ташқи тармоқларда доктурни таъминлайди. (телефонли маълумот узатиш). Улар асосий (кенг имкониятлар билан) бўлиниши мумкин.Тармоқ ости шахсий бошқарув станцияни (СУ) сақлаши мумкин. Бу шаклда бошқарув функцияси ва коммутатция барча тармоқда тақсимланади, бу эса чақурувни зудлик билан узатилишини ва алоҳида жиҳозларнинг шикастланганлик вақтида тармоқнинг ишлаш қобилиятини сақланиши.

Замонавий мобил алоқанинг тизими (ЗМТ) қўллаш тартибига кўра ахборот технологиялардан фойдаланишга кўра ва уюшманинг принципига кўра турлича бўлади. Шунинг учун уларнинг мавжуд кўриниши (обзор) дастлабки системалашувсиз мушкиллик туғдирарди.

МРТ нинг классификацион кўриниши:

• тизим бошқарув усули**,** ёки абонентлар бирлашув усули - марказлаштирилмаган . Маркашзлаштирилган алоқа бирлашуви абонентлараро марказий (ёки базали) станция орқали ишлаб чиқарилади. Қарама – қарши ҳолатда алоқа фойдаланувчилар ўртасида бевосита яъни базали станциянинг иштирокисиз ўрнатилади;

• ҳизмат қилиш доираси— *радиал* (радиус чегарасида радиостанциянинг ҳаракати), *чизиқли* (чизиқли кимёвий доира), *территориал* (майдоннинг маълум конфигурацияси учун);

• алоқанинг йўналишли - базали станция ўртасида ва бир йўналишли ёки икки йўналишли алоқа абоненти;

• тизимнинг ишлаш кўриниши — *симплекс* (базали станцияга абонентдан навбатма - навбат узатиш ва қайта узатиш) ёки *дуплекс* — бир вақтли узатиш ва берилган икки йўналишнинг ҳар бирини қабул қилиш;

• радиоалоқа тизимида каналлар тақсимот усули ёки кўплик кириш усули - *частотали, вақтинчалик* ёки *кодли*;

• ажратилган алоқа тизими, частотали манбадан фойдаланиш усули ҳисобланиб абонентлараро каналларни қаттиқ таркалиши умумий частотали манбага абонентларни кириш имкониятлари (транкингли тизимлар), узаткичларни фазавий тарқалиш хисоби частоталарни қайта ишлатилиши ;

• абонентлар алоқа тизимида қабул қилиш категорияси профессионал (касбга оид) (ҳизматга оид корпаратив) абонентлар, алоҳида шахслар;

• маълумот узатиш кўриниши - мавзу кодланган маълумотлар ва бошқалар.

Ушбу рўйҳат аломатларни ясовчи мавжуд тизимларни барчасини тугатмайди, частотадан фойдаланиш диапазони, сигналлар модуляциясининг кўриниши, умумий фойдаланиш жараёнида коммутацияланган телефон тармоғи ёрдамида алоқа тизимини улаш усули (АТУУ), қабул қилинган абонентлар сони ва бошқалар. Эслатиб ўтиши мумкин, бироқ мавжуд МРТ учун хилма – хиллик кўриниши етарли.

Мавжуд МРТ турини кенг тарқалганлигини ҳисобга олиб шу қаторда улар ривожланишининг переспективини МРТ классификацияси навбатдаги тизимини таклиф қилиш мумкин, юқорида ажратилган аломатларнинг учтаси, санаб ўтилган асосга эга:

• тизим вазифаси ва радиоқоплама;

• кўплик дастурининг методи;

• радиотармоқда каналларида дуплекс схемаси.

Кўплик дастури уюшмасининг усулига кўра частотали - вақтинчалик манба алоҳида алоқа каналлараро у ёки бу технологияларнинг тақсимоти:

• Транкингли алоқа тизими (ТАТ);

• махсус радиочақирув тизими (МРТ);

• махсус йўлдошли алоқа тизими (МЙАТ);

• мобил алоқанинг уяли тизими (МАУТ).

МРТ учта рақобатлашувчи технологиялар негизида ажратилади:

• каналларни частотали тақсимланиши кўплик дастури;

(КЧТКД, инглис тилидаги аббревиатура PDMA — *frequency division multiple* access);

• каналларни вақтинчалик тақсимланиши кўплик дастури *(КВТКД* ёки TDMA — *time division multiple* access);

• каналларни кодли тақсимлаш кўплик дастури *(ККТКД* ёки CDMA — соде *division multiple* access).

Каналларни дуплексли классификациясига тегишли бўлиб, шундаги икки томонлама алоқа радиоканалида маълумот алмашув усули абонентлараро ёки базали станциялар билан ва абонентлар билан амалга ошади. Энг юқори тарқалиш частотали ва вақтинчалик ажратиш асосида дуплексли узатиш организацияси билан тизим мавжуд.

Умумийлик сифатида айниқса аниқ тузилган GSM стандартига яқин, ССМС схемаси танланади.ССМС нинг функционал тузилиши 2.4 - расмдаги схемада курсатилган. Келтирилган схемада шартли равишда 4 та асосий компонентларни ажратиш мумкин. Марказий бошқарув ва ҳизмат кўрсатгичи (МБХК) (яъни *operations and maintenance center*- ОМС) ва 3 та тизим ости:

• мобил станцияда тизим ости МСТ *(Mobile station sub- system* MSS);

• базали станцияда тизим ости БСТ *(base station sub- system* BSS);

•тизим ости коммутацияси ТК *(switching subsystem* SSS),— интерфейслар қаторида ёзилувчи функционал уланиш.

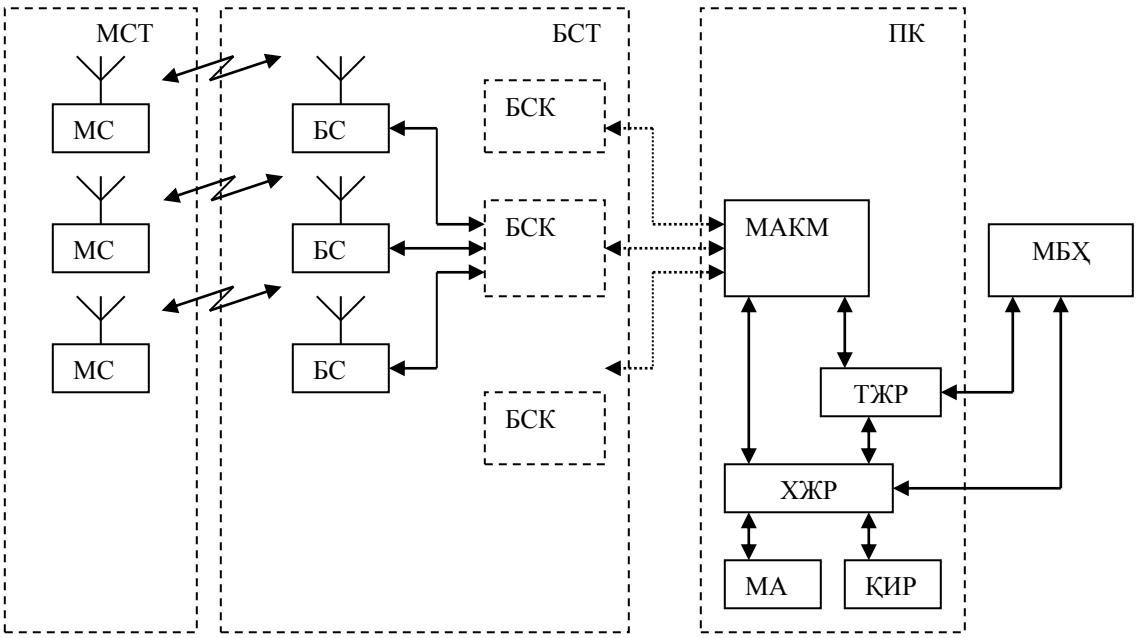
Бўлим сўнгида ССМСнинг асосий элементларини ва улар табиатининг (характер) ўзаро таъсирини кўриб чиқамиз. Гарчи турли стандартларнинг уяли

тизими деталларда сезиларли фарқ мавжуд бўлиб, баъзи умумлашган моделлар ёрдами билан улар тасвирнинг интеграллашиши эҳтимолли ва фойдали. Шу каби умумлашма сифатида ССМС схемаси танланади, GSM стандартига яқин келувчи, энг аниқ тузилган. ССМС функционал кўриниши 2.4. расмдаги схемада тасвирланган. Келтирилган схемада шартли равишда 4 та асосий компонентга ажратиш мумкин – марказий бошқарув ва ҳизмат кўрсатиш (МБХК) (яъни *operations and maintenance center*- OMC) ва 3 та тизим ости:

• мобил станцияда тизим ости МСТ *(Mobile station sub- system* MSS);

• базали станцияда тизим ости БСТ *(base station sub- system* BSS);

• тизим ости коммутацияси ТК *(switching subsystem* SSS),— интерфейслар қаторида ёзилувчи функционал уланиш.



1.4-расм. ССМС нинг умумий структурали схемаси.

МБҲ ССМС нинг марказий элементи бўлиб, бошқа тизим компанентлари бошқарувини, ва шу билан бирга функцияланиш сифат контролини таъминлайди. Мобил станция тизим ости абонентларини тизимга дастурни таъминловчи жихозларни таъминлайди. ССМС меъморчилигида асосий ҳалқа коммутация тизим ости хисобланиб, мобил алоқада коммутация марказини ичига олади. МАКМ *(mobile switching center* MSC), тарифли (мехмонхона) жойлашуви регистр ТЖР *(visited location register* VLR), хонаки жойлашув регистри ХЖР *(home location register* HLR), аутентификация маркази АМ *(authentication center AUC)* ва жиҳозлар идентификацияси регистри ЖИР *(equipment identity register* EIR). Базали қабул – узатувчи станция БС киради *(base transceiver station* BTS) ва базали станция контроллерлари БСК *(base station controller* BSC).

Мобил алоқа коммутация маркази катак гурухини қабул қилади ва мобил станцияда иш жараёнига зарур бўлган барча кўринишдаги уланишларни таъминлайди, у ёки мобил абонентлар коммутатцияси ўзаро ТРОП абоненти билан ва бошқа шу билан бирга МКМС да каналлар коммутацияси функцияси кутилади, қайсики «хизмат кўрсатиб узатиш» (ёки «навбатма – навбат (эстафета) узатиш») тааллуқлидир ва кучли тўсиқ пайдо бўлганда катакда каналлар қайта ёқилиши (ўзгариши) ва шикастланиш фақат бу БСК вазифаси бўлмаса МКМС коммутация вазифасига қарамай хонаки ва ташрифли жойлашув регистрлар ёрдамида мобил станцияларида зичланиши жараёни бошқаради чақурувчи етказишни таъминлаш учун, шу билан бир қаторда аутентификация жараёнида АМ ва ҚИР ёрдамида абонентлар идентификацияси.

ХЖР ва ТЖР блоклари моҳиятига кўра ўзи билан маълумотлар базасини ифодалайди. Биринчиси улар учун берилган МКМС абонентларда доимий кўшимча ёзилган маълумотларни ва улар кўриниши маълумотини сақлайди. Иккинчи, вақтинчалик МКМС маълумот қабул қилиши доирасида (зона) мавжуд бўлган абонентлар ҳақидаги маълумотни сақлайди. Аутентификация

маркази абонентлар аутентификацияси жараёнининг ўтиш имкониятини ва узатилган хабарлар шифрланишини таъминлайди. ҚИР улар аниқлиги ва фойдаланишига руҳсат этилган мобил станциялар ҳақида ахборотни сақлайди.

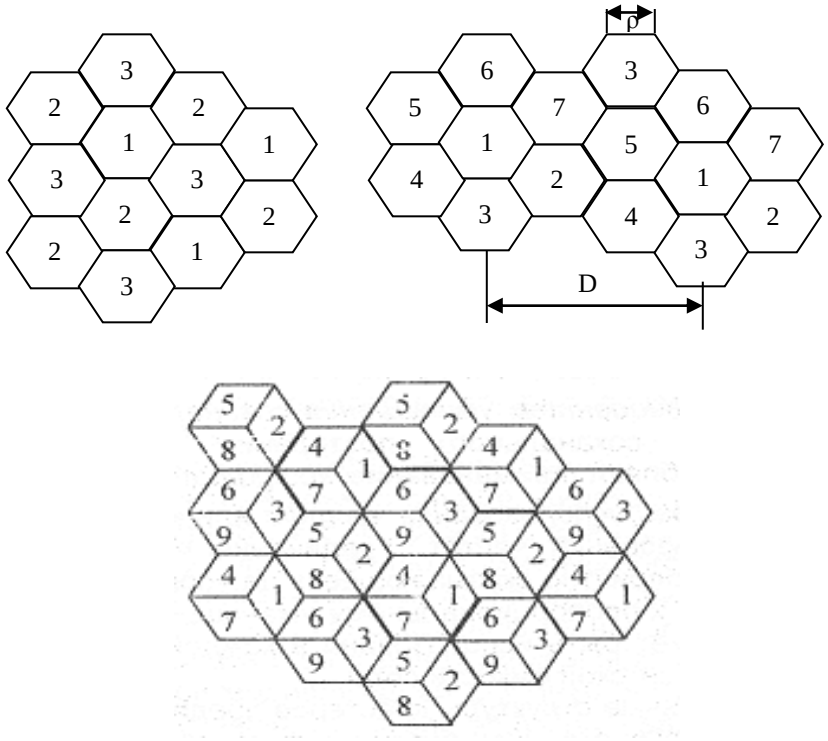
Базали станциялар котроллери бир қанча БС бошқарувини амалга оширади, қайсики МС радиоинтерфейс орқали алоқани таъминлашини, шу билан бир қаторда МКМС орқали узатилувчи маълумот жойлашувини ва унинг қайта йўналиш узатиш вақтида қайта жойлашни амалга оширади. БСК ишлаб чиқариш жараёнининг сонига катакларарo МС га ўтиш жараёнида қабул қилиш узатуви тегишлидир, худди шу БСК назорат қилувчи, МС орасида чиқарувни узатиш турли БС харакат доирасида мавжуд бўлган, лекин бир ва худди шу назоратчи (қарама – қарши ҳолатда биринчи бошқарув МКМС да қаратилади). БСК бошқаруви остида алоқа каналида радиоўлчов амалга оширилади, мобил ва базали станцияда узатиш қуввати бошқарилади.

1.3. Мобил алоқанинг уяли тизимлари

Радиоқоплама майдонининг жойи белгиланган частота йўлида алоқа амалга оширилишини тўғри олти бурчак кўринишида схематик тарзда тасвирлайди ва ари инига ўхшаш бўлгани учун катакча номини олган МРТ натижасида частотани фазовий тарқалиши мобил алоқада уяли тизим (МАУТ) номини олган. Катаклар тури, тўсиқсиз частотали йўлининг такрорий фойдаланиши мавжуд бўлмай, уни *кластер* деб номланади. Уяли топология радиал тизими билан солиштирганда тизим абонентлар сиғимини кўп маротаба оширади ва алоқа сифатини пасайтирмаган ҳолатда фойдаланишни катта майдонини қанча истаса қамраб олади ва ажратилган частотали диапазон кенгайишини ҳам эгаллайди.

Шу билан бир қаторда қуришнинг уяли принципи фойдаланувчиси мураккаб қаторини ҳам тахмин қилиб қайсики мобил абонентни ўтишни жойига тегишли таъриф ва уни бир катакдан бошқа катакка аралаштириш жараёнидаги узлуксиз алоқани таъминлайди. Мавжуд жараён эстафетали (навбатма – навбат) узатиш номини олган. Инглиз тилида (hanoff ёки handover)

СОМС юқори эффектив спектраллиги бир ва ўша частотали йўлнинг максимал частотали қайта фойдаланиш бахосига ётади, ва шу нуқтаий назарда ҳаммасидан кўра участкавий (ёки уч элементли) кластер афзал бўлар эди, 2.3 а расмда тасвирланган, бир хил рақамлар тасвирланган, бир хил рақамлар билан частотали каналлар тўпламига ўхшаш катаклар кўрсатилган.



1.5-расм. ССМС кластер тизим варианти.

Бундан ташқари маълум турнинг ҳар бир кластер хатага частотали чизиқ ажратилади, учинчи тўлиқ частотали диапазонга тенг, демакки тизимда алоқа каналининг умумий соннинг учдан бир қисми, қайсики: катакнинг сезирарли абонент яхлитлигини таъминлайди Бу билан бирга тез – тез такрорланиб турувчи майдон бир хил йўл билан юзланади. Тўсиқ сезирарли сатхларни характерлайди у ёки бу частотанинг худду шу йўлда ишловчи тизим станциядаги тўсиқ, лекин сон саноқсиз катакларда бўлади. Канални тўсиқни таъсирини камайтириш учун катта миқдордаги элемент кластерларига нисбатан қулайдир масалан 7 – элементлар, 2.3 б расмда тасвирланган. Кўрсатиш мумкин, ячейкалар *D* масофа, қайсики частотанинг бир хил чизиғи ишлатилади ва у сонни кластерда элементлар қуйидагига нисбатан боғланган.

$$D=\sqrt{3}nc\ p,$$

қаерда р — ячейка радиуси, у ёки бу айлана радиуси, тўғри олти бурчак атрофида тасвирланган. Аниқловчи нисбат параметрини каналли тўсиқни камайиш коэффициенти ёки такрорий каналли коэффициент деб айтадилар g = 1)n, ўлчаш учун частотанинг тез – тез фойдаланишнинг такрорий самарадорлик коэффициенти ва ва такрорий фойдаланиш коэффициенти каби номларни ишлатадилар кластерда элементлар сонини ёйилиши каналли тўсиқлар сатҳида ижобий бахоланиб ҳар бир катакда фойдаланилган частота йўлларини пропорционал камайишига олиб келади

Кўриб чиқилган кластерларнинг тузилиши йўқолиши айлана диаграмманинг базали станция антеналари билан фойдаланишни мақул кўрадилар, қайсики сигнал узатишни барча йўналишга бир хил қувватда амалга оширади, каналли тўсиқни самарали усули пасайишининг 120 ёки 60', йўналишли диаграмма кенглигида йўналган антеналарни тадбиқ қилиш (горизонтал текисликда) натижада олти бурчакли ячейка 3 ёки 6 секторга бўлинади у ёки бу катак секторизациясида антена билан фақат бир томонларга нур тарқалади тарқалиш сатхи қарама – қарши йўналлишига минимум

қисқартиради. Бу кўринишда катак секторизацияси кластерда частотанинг бир хил йўллари улар тузилишини хеч ўзгаришларсиз аввалги сезирарли каналли тўсиқлар сатхини пасайтиради.

Агар кластердан ташкил топган бўлса, ҳар бир мавжуд бўлган катаклар, секторлар, айтиш мумкинки, кластернинг хажмидир *(u,, u,* х *m,).* Кластернинг маълум турдаги хажми, амалиётда кенг қабул қилинувчи хисобланади. 2.3 расмда секторланган кластер хажмлилигини частотали каналлар тўпланишини тақсимлашнинг қулай варианти берилган. Таъкидлаш мумкинки, ССМС топологик қайта ишлаш ўзига хос ва етарлича мураккаб вазифа хисобланади.

СОМС юқори эффектив спектраллиги бир ва ўша частотали йўлнинг максимал частотали қайта фойдаланиш бахосига ётади, ва шу нуқтаий назарда ҳаммасидан кўра участкавий (ёки уч элементли) кластер афзал бўлар эди, 2.3 а расмда тасвирланган, бир хил рақамлар тасвирланган, бир хил рақамлар билан частотали каналлар тўпламига ўхшаш катаклар кўрсатилган.

Радиоқоплама майдонининг жойи фиксирланган частота йўлида алоқа амалга оширилишини тўғри олти бурчак кўринишида схематик тарзда тасвирлайди ва ари инига ўхшаш бўлгани учун катакча номини олган МРТ натижасида частотани фазовий тарқалиши мобил алоқада уяли тизим (МАУТ) номини олган. Катаклар тури, тўсиқсиз частотали йўлининг такрорий фойдаланиши мавжуд бўлмай, уни *кластер* деб номланади. Уяли топология радиал тизими билан солиштирганда тизим абонентлар сиғимини кўп маротаба оширади ва алоқа сифатини пасайтирмаган ҳолатда фойдаланишни катта майдонини қанча истаса қамраб олади ва ажратилган частотали диапазон кенгайишини ҳам эгаллайди.

Кўриб чиқилган кластерларнинг тузилиши йўқолиши айлана диаграмманинг базали станция антеналари билан фойдаланишни маъқул кўрадилар, қайсики сигнал узатишни барча йўналишга бир хил қувватда амалга оширади, каналли тўсиқни самарали усули пасайишининг 120 ёки 60', йўналишли диаграмма кенглигида йўналган антеналарни тадбиқ қилиш (горизонтал текисликда) натижада олти бурчакли ячейка 3 ёки 6 секторга бўлинади у ёки бу катак секторизацияда антенна билан фақат бир томонларга нур тарқалади тарқалиш сатхи қарама – қарши йўналлишига минимум қисқартиради. Бу кўринишда катак секторизацияси кластерда частотанинг бир хил йўллари улар тузилишини хеч ўзгаришларсиз аввалиги сезирарли каналли тўсиқлар сатхини пасайтиради.

2. МОБИЛ АЛОҚА ТИЗИМЛАРИДА МАЪЛУМОТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АСОСИЙ ХАРАКТЕРИСТИКАЛАРИ ВА УСУЛЛАРИ

2.1. Уяли радиоалоқада радиотўлқинларнинг тарқалиш муҳити характеристикалари.

Радиоканал хохлаган симсиз алоқа тармоқнинг ажралмас ва танқидий муҳим компоненти хисобланади. Ўз навбатида, радиоканал характеристикаси радиотўлқинни тарқалиш мухити сифатида, охиргисини узунлигига ёки частота диапазони тузилишини эгаллайди.

Частотали диапазонни танлаш тармоқни лойихалашнинг ўта маъсулиятли эталонидир ва эътиборга бир қатор техник, экономик ва уюштирма режа факторларни инобатга олиш керак:

- частота каналларининг керакли миқдорда ажралиши;
- радиотўлқиннинг трассада тарқалиши;

• бина ва иншоатларнинг ўтказувчанлиги;

• берилган участка спекторидан табиий ва сунний халақитларнинг ўтиши;

• яқин частоталарда ишлайдиган бошқа тармоқлар билан электромагнит бирлашиши;

• талаб қиладиган экономик, эргонолик ва эксплуатацион характеристикали абонент аппаратурасининг қурилиш имконияти.

2.1-жадвалда, мавжуд бўлган асосий уяли радио алоқа тармоқларида ишлатиладиган частота полосалари келтирилган. Битта частотали диапазонда ишллайдиган хар хил радио воситаларнинг электромагнит бирлашиши муамоси билан бир қаторда, хар хил уяли радиоалоқа тармоқларининг бирлашиши муамоси ҳам мавжуддир. Бу тизимларнинг ривожланиши ҳар хил мамлакатларда ўхшаш йўллар билан боради. Лекин биринчи эталонларда ўзаро келиша олмади.

2.1 - жадвал. ССМС да ишлатиладиган частота полосалари.

Стандарт (тил)	Частота полосаси, МГц
NMT-450	453…457.5; 463…467.5
NMT-900	890…915; 935…960
AMPS/D-AMPS (IS-54)	824…849; 869…894
TACS / ETACS	890…905; 935…950
PDS	810…836;940…956
	1429…1465; 1477…1513
GSM – 900	890…915; 935…960
GSM – 1800	1710…1785; 1805…1880
IS-136	1750…1810; 1830…1890

GSM – 900 (IS-661)	1850…1910; 1930…1990
IS-95 (CDMA – 800)	824…849; 869…894
CDMA – 1900	1850…1910; 1930…1990

Натижада Европа мамлакатларида "қуроқ кўрпа" деб номланувчи ташкил топади: бир вақтнинг ўзида қурилиш принциплари бўйича жуда ўхшаш, бир хил частота диапазонини ишлатадиган (масалан, 450 МГц), лекин бир бири билан бирлашмайдиган ўхшаш уяли алоқа тармоқлари вазифа бажаришади.

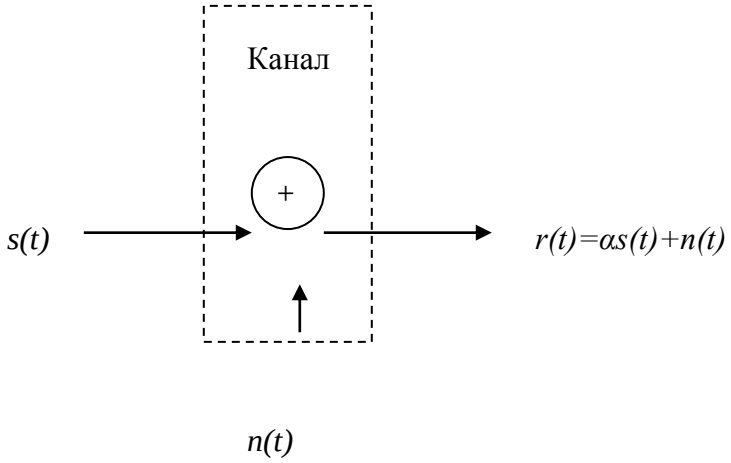
Европада рақамли системаларга ўтишда умумевропа GSM стандартини ишлаб чиқариш билан амалга оширилди. 900 МГц диапазонидаги частота чизиқлари ажратилди. Кейинчалик бу стандартнинг мукаммалашиши янги — 1800 МГц диапазонни ўзлаштиришга олиб келади.

2.1.1. Уяли алоқа каналларида ҳалақитлар

Махсус радиочакирув тизими (МРТ) ишида диапазонда дешифратор билан тўлқин узунлиги, деярли барча мавжуд тизимларда уяли алоқада фойдаланилади, турли тўсиқлар табиий ва сунъий чиқиш таъсир кўрсатади. Табиий келиб чиқишнинг асосий тўсиқлари қабул қилгич шовқини, атмосфера шовқини момақалдироқ вақтида электрик разрядларни юзага келиши хисобланади. Бундан ташқари, ҳалал берувчи таъсирлар статик электр, фазовий ва қуёш шовқуни хосил қилиши мумкин.

Одатда тахлил вақтида ва алоқа тизими синтези бу тўсиқларни аддентив оқ гауссовли шовқин (АОГШ) каби кўриб чиқади.

Каналнинг аддентив шовқини модели 2.1 расмда берилган. (*a* параметр - бу ерда каналда сигнал сўнишини характерлайди.



2.1-расм. Каналнинг аддентив шовқини модели

Ахолиси зич жойлашган регионларда сунъий табиатда тўсиқнинг сезирарли жадаллиги хизмат қилувчи маънбаларга хосдир:

• электротранспорт ва автомобил ўт олдириши;

• саноат электро қурилмаси;

• турли вазифадаги радиоэлектрон воситалари (яқин навигация радиотизимини эслатиб ўтиш мумкин, стандарт уяли тизим диапазони озгина ёпиб турадиган частота йўли GSM).

Шуни алоҳида таъкидлаш жоизки тизим ости (каналли) тўсиқлар бир қанча станцияда частота бир йўлда бир вақтда ишлаши шартлашган (масалан, қўшни кластерда бир частотада ишловчи абонентлар, ёки IS-95 тармоғида қўшни катакдаги базали станцияда) ишловчи.

Мобил радиоалоқа тизимининг қуриш вақтидаги жиддий муаммо, нафақат белгиланган тўсиқлар таьсирига боғлиқ, балки МРТ функцияланишининг ўзига хос (специфик) шароитга хам боғлиқ..

• МРТ таьсир майдони асосан шахар ва туманларда турлича қалинликда қурилиши характерига, транспорт харакатининг интенсивлиги, сиртдан қоплаш тури хисобланади;

• мобил станция таркибига кўра, базали станциянинг нотўғри радио кўринишда мавжуд;

• сигналнинг нуқтасига қабул кўп миқдордаги нур тарқалиши натижасида келиб тушади, у ёки бу кўп миқдордаги тўсиқда намойн бўлиши (бино, дарахт, сиртдан тўшамоқ)

• мобил станцияда харакат частотанинг зўрға судралиб хосил бўлишига олиб келади.

Такидланган факторлар натижасида масофага тобеь бўлган холатда сигналлар сўниши эркин фазода солиштирганга нисбатан кескин хисобланади, шу билан бирга катта босим хосил қилган қувват кўп нурли интерферцион расмлар ўзгариш хисобига сигнал сўниши – абонент терминалини аралаштириш вақтида хосил бўлади.

2.1.2. Радио сигналлар тарқалишидаги сўнишлар

Радиосигналнинг тарқалишида унинг кучи масофанинг кучайиши билан камаяди. Умумий кўринишида, бу боғлиқликни бундай ёзиб қўйиш мумкин:

$$P_r \text{ —— } a_0 P_T R^{-v}, \qquad (2.1)$$

қаерда *P*> ва *PR* — тарқаладиган ва қабул қиладиган сигналга тегишлидир; R — ўтказадиган ва қабул қиладиган станциялар орасидаги масофа; v —сўнишни кўрсатувчи ; *a* — нормалаб кўпайтирувчи.

Эркин фазода узатиш майдонида ва объектлар бўлмаган вақтда сингдирувчи ва энергияни таъсвирловчи қабул қилинган сигналнинг қуввати (v= 2) ; масофа квадратига орқага пропорционал бўлади.

МРТда радиотўлқинларнинг тарқалиши, очиқ майдонда тарқалишига мўлжалланган, тўсиқ бўлмаган жуда кичкина йўлларда мавжуддир.

Нурнинг куч тарқалишида сўниш кўрсаткичи ошади ва МРТ да ишлатиладиган диапазонлар учун тажриба натижалари кўрсатганидай жойлашиш характерига қараб v = 3 — 5 га ўзгаради.

МРТ учун жойларнинг қуйидаги классификацияси қўлланилади:

• очиқ туманлар – унча катта қийматга эга бўлмаган табиий – тўсиқлар майдони худди бино ёки дарахтга ўхшаш**;**

• шаҳар атрофдаги (четидаги) майдонлар - объектига яқин жойда жойлашган дарахтлари ва бинолари хам бўлган участкалар;

• шаҳар туманлари – зич қурилган кўп қаватли бинолар, қурилган участкалар.

Функцияланишнинг аниқ талаби радиоканал учун энергетик потенциалнинг аниқ аналитик хисоботи МРТ математик таърифга тўғри келмайдиган деярли кўплик факторининг яхлитлиги учун мумкин эмас.

Окамури – Хата модели айниқса фойдаланишга қулай бўлиб, график ва аналитик аппроксимация амалий ўлчамлари натижаси.

График аппроксимациясида барча кийматлар децибелда келтирилган тенгламадан фойдаланилади:

$$P_R = P_0 — A_m(f, R) + H_b(H, R) + H_m(h, f) + K_s(f), \quad (2.2)$$

қаерда Р, — эркин фазода узатилиши вақтида қабул қилиш сигналнинг қуввати; *A(f,* R) — мобил станцияларнинг антеналари *h = 3* м, базали станциянинг таъсир вақтидаги антена баландлиги *H* = 200 м эркин фазода аналогик муносабатга оид қувватнинг медиан аҳамиятини пасайиш фактор; *H(H,* R) — мобил станция учун " кучайтириш — баландлик " фактори; *Hm(h, f)* " кучайтириш — баландлик " фактори базали станция учун; $K_s(f)$, — жойнинг тури билан аниқловчи, тўғирловчи коэффициент.

A_m, *H*>, H_m жойлашув графиги ва К, Окамура томондан ўтказилган тажриба натижаларига асосланган.

Хаталар хона кўп миқдордаги тажрибаларнинг натижаларини умумлаштиради. Барча йўналишига оид антеналар вақтида *L* нинг тарқалиш вақтида ўртача йўқотиш хисоботи учун базали станцияда эмпирик формула қабул қилади. Бу формулалар маълумки Окамури томонидан олдиндан айтилган усулидир.

Келтирилган формулалар кўпгина холатда аниқ етказилади (максималь хато 1 дБ атрофида) навбатдаги талабни бажариш жараёнида тажриба маълумотларга тегишлидир:

$F_0 Є$ [150, 1500] МГц,

H Є [30, 400] м,

h *Є* [1, 10] м, R < 80 км.

Окамури - Хата моделининг биргина камчилик томони шундаки базали ва мобил станция жойлашган районнинг специфик талабини инобатга олмаслигидадир.

Қўшимча параметрлар қатори Ксиа-Бертони модели ҳисобланади. Бу модел тўлқинли оптика тенглигига асосланиб қурилган ва уйларнинг деворида акс этувчи, томнинг қиррасида дифракция каби сигнал тарқалишининг шундай детали диққатни жалб қилади. Қабул қилинган аналитик ифодаларга кўра кенглиги бино қаввати баландлиги бирмунча томнинг ўртача сатхи (шу билан бир қаторда БС жойлашган, антеналар томнинг ўртача сатхидан паст) ҳисоблашга рухсат этади. Бироқ бу ифода бироз бесонақай бўлиб, ифодалаш, ва такрорлаш мақсадга мувофиқ бўлмайди.

Қўпол баҳо учун тарқалиш жараёнида қувват йўқолиши параметрларига қарашли тахминан (яқинлаштирилган) лигидан фойдаланиш мумкин:

а) масофага оид: 38 дБ декадага;

б) базали станция антена баландлигига оид : 6 дБ октавадан;

в) мобил станцияда антена баландлигига оид: 3 дБ октавага $h < 3$ м, ёнидан 6 дБ октавада $И > 3$ м ёнида;

г) шаҳар четида йўқотиш тахминан 10 дБ дан кичик, шаҳарга нисбатан.

Шуни таъкидлаш жоизки, сигнал тарқалиши вақтида қувватнинг йўқолиши бошқа кўпгина факторларга боғлиқ бўлади, берилганлардан ташқари (масалан, дарахтдаги баргларнинг аниқлиги хисоблаш нихоятда мушкул). Шу сабаб билан МРТ характерлаш вақтида тахмин қилинган бурама районда сигнал қуввати сатхини эксприментал тадқиқотни ўтказиш зарурдир. Хусусан, бундай тажрибаларнинг натижасида базали станцияларнинг жойлашув жойи асосланиши шарт.

2.1.3. Сигналларнинг сўниши

Қабул қилувчи нуқтадаги сигнал, радиотўлқин интерференцияси натижасида ҳосил бўлади. Ҳар бир радиотўлқин ўзининг параметрлари билан

характерланади: ёйилиш вақти, доплер частотаси ва амплитудаси билан. Математик қуйидаги кўринишда ёзилиши мумкин:

Бу тенгликда і- радиотўлқин *a,* келиши бурчак билан (i =1...,N) M дан композицияга ташкил қилувчи сифатида киради. Радиотўлқин ушланиб қолиш вақти T билан трасса ёйилишига тегишли узунлик аниқланади. Ҳар бир радиотўлқиннинг доплер частота силжиши МС ва келиш бурчаги жойининг ўзгаришини тезлиги билан аниқланади:

Амплитуда кўпайтиргич СД-ҳар бир ташкил қилувчининг энергияси билан аниқланади.

Тарқалиш шароитлари, холати ва акс эттирувчи объектларнинг хусусиятлари ва бошқаларнинг ўзгаришида интерференцияли суръат бўлади. Бу МС ўзгармас бўлганда ҳам содир бўлиши мумкин (масалан, агар битта ёки бир нечта сигналлар ўзгармас МС га бошқа ҳаракатланувчи объектлардан акс этгандан кейин келса). Лекин қабул қилинаётган сигналларнинг кучини ўзгаришидаги асосий сабаби МС ни харакатидир.

МСни жойини ўзгаришида 2 та жараён бир вақтнинг ўзида содир бўлади:

• бу радиотўлқинларнинг тарқалиш йўлларининг тарқалишида**,** улардан натижавий сигнал тўпланадиган радиотўлқинлар орасидаги фазовий боғланишларнинг ўзгариши;

• радиотўлқинларнинг тарқалиш йўлларининг ўзгариши, ёки акс эттирувчи нуқталарнинг.

Иккала жараён ҳам эгуллувчи натижавий сигналнинг мувозанати ўзгаришига олиб келади, лекин бу ўзгаришларнинг характери муҳим фарқлидир. Агар қабул қилинган МС сигнални ажратилган натижавий эгилган *r(t)* ва тўлиқ фазо *e(t)* билан ёзилса

$$s(t) = r(t)\cos[\phi.(t)],$$

унда эгулувчини самара сифатида кўрсатиш мумкин.

$$r(t) = m(t)r_0(t),$$

бу ерда биринчи кўпайтирувчи *m(t)* радиотўлқинларнинг тарқалиш йўлдаги ўзгаришлари билан боғлиқ секин ўзгаришларни акс эттирад, иккинчиси— *г* (1) — фазовий боғланишларнинг ўзгариши билан боғлиқ тез ўзгаришларни акс эттиради.

Секин сўниш сигнали (қотиб қолиш) абонентга эгадир (»10А). МС нинг бундай кўчишидан радиотўлқинларнинг келиб чиқиш йўллари деярли тўлиқ ўзгаради. Моҳиятдан секин тўхташлар кўп нурлилик билан ҳосил қилинган, тез қотиб қолишлар устига тушадиган ўртача даражали сигналнинг МС га ўчирилишидаги силкинишни ўзида акс эттиради.

Экспериментал маълумотлар билан яхши келишадиган, секин қотиб қолишлар учун умумий қабул қилинган модель логарифмик – ўртача тақсимланиш қонуни хисобланади.

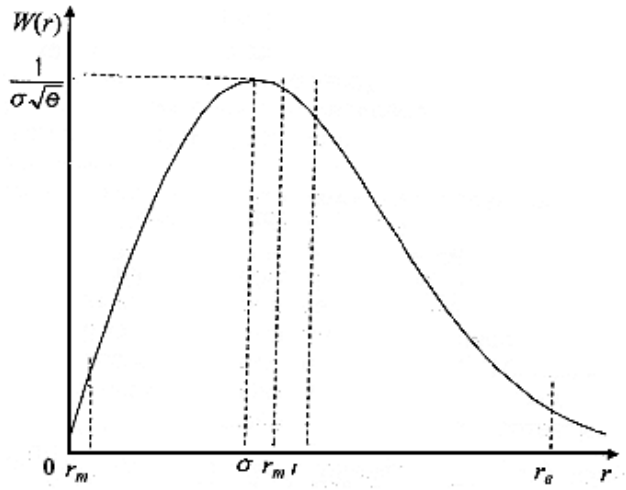
Секин қотиб қолишларни чуқурлиги одатда *о* = 10дБ ни, шаҳар шароитида о = 6дБ ни ташкил қилади.

МС 1/ = 60 км/С силжиш тезлигида секин қотиб қолишларнинг интервал 900 МГц диапозонда ишлайдиган 1...2 тартибини ташкил этади.

Тез қотиб қолишлар кўп нурли сигналларнинг тарқалиши билан боғлиқдир. Марказий чекланган теорема асосида кўп миқдорли ёйилиш трассасида электромагнит компонентлари тахминан гауссов тасодифий жараёнлар деб хисобланиши мумкин. Бундай ҳолатда эгулувчан қабул қилинадиган сигналнинг жуда тез аҳамиятининг тарқалиш зичлигининг эҳтимоллиги Рэлея — Райса қонуни билан тасвирланади:

Агар тўғридан тўғри сигнал бўлмаса (МС БСнинг тўғридан тўғри кўринишидан ташқарида бўлади), унда Q, = 0 эгулувчи аҳамиятининг тарқалиш зичлигини Рэлея қонуни билан тасвирланади (бу экспериментал маълумотлар билан яхши келишади):

2.2. расмда Рэлея эҳтимолининг тарқалиш тасвири кўрсатилган таркалиш максимум *r = o* да эгадир. Ўртача аҳамият (математик кутиш) *r* = cruz/2, мередиана эса *r* = v42ln2 .



2.2- расм. Рэлея эҳтимолининг тарқалиш тасвири.

Кўп нурли тарқалишда натижавий сигнал ўртача аҳамиятда кўпроқ ҳам бўлиши мумкин, камроқ ҳам. Тарқалиш асимметрияси шунга олиб келади Ўртачанинг камроғи ўртачанинг кўпроғига қараганда аҳамиятлироқдир.

Имкониятли диапазондаги сигнал даражасини ўзгаришини баҳолаш учун *[r, r,]*, эгулувчининг кўрсатилган чегарадан ташқарига чиқмаслигига *P* эҳтимолининг чегаравий аҳамиятини топшириш керак:

Бу ердан диапазон берадиган чегаравий нуқталарни олиш мумкин, бунда эгулувчан аҳамияти *2P* дан кўп бўлмаган эҳтимол билан чегарага чиқади;

Агар *Pp* = 10, эҳтимол даражаси билан чегараланса, бунда: *r,* = 3,717а; rД = 0,045ст. Эгулувчан даражасининг диапазон ўзгариши *г, /г,,* = 83,1 тезда (38 дБ)ни ташкил қилади. Бунда эгулувчан даражасининг ўртача аҳамиятдан кўпайиши *r, /r = 3* тезда (9,4 дБ)ни ташкил қилади. Бузилишлар эса ўртача аҳамиятдан пастроқ — *r/rД = 27,7* марта (28,6 дБ).

Тез қотиб қолишлар жараёни сигналлар амплитудаси фарқини ҳар хил частоталарда ҳар хил вақтларда характерлантирадиган эгилувчининг корреляция коэфициенти асосида баҳоланиши мумкин:

Корреляция коэффициентининг аниқлаш учун тарқалишда сигнал тарқалишининг ушланиб қолиш қонунини ва алоҳида радиотўлқинларнинг келиш бурчагига тарқалиш қонунини билиш керак.

Экспериментал маълумотларнинг анализи, тарқалиш эҳтимолида сигнал ушланиб қолишнинг аппроксимация зичлигининг экспоненциал тарқалишини кўрсатади:

Умумий истеъмолли алоҳида радиотўлқинларнинг келиш бурчаги учун бир хил тарқалиш ҳисобланади:

2.2.-расмда корреляция коэффициентининг тобелиги нол холатдаги вақтидан кўрсатилган (M = 0).

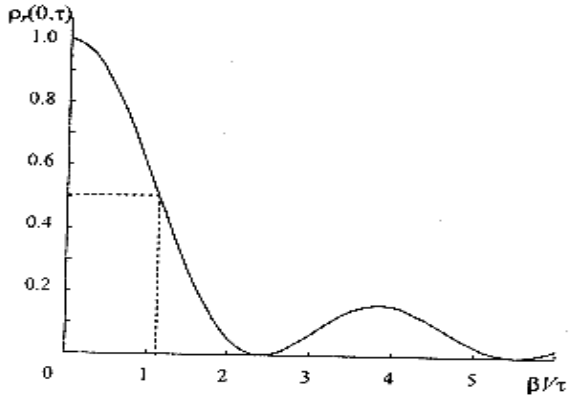
Корреляция коэффициентининг биринчи ноли ДУг=2,4, ўрнига эга ёки d= *Уг* = 0,38А да. Ўлчанишлар кўрсатадики, қишлоқ жойларда биринчи ноли 0,8А d тартибида бўлади. Бу шу билан боғлиқ алоҳида радиотўлқинларнинг келиш бурчагининг тарқалиши бир меъёрдагидан фарқ қилади. Шаҳар шароитларида корреляция коэффициентининг биринчи нулига тегишли ўлчанган d, нинг аҳамияти ҳисобланганда анчагина камроқ чиқади.

Шундай қилиб, айтиш мумкинки, МС га А/2 тартиб масофада кўчишда қабул қилинаётган сигналлар кучсиз коррелияцияланган бўлади.

Бунда алоҳида нурларни сигналларнинг тарқалиш йўллари деярли доимий бўлиб қолади, фазовий боғланишларнинг ўзгариши эса катта масофаларда эгилувчи натижавий синалнинг ўзгаришига ёки тез қотиб қолишларга олиб келади.

Тез қотиб қолишларнинг жараёни тахминан МС нинг А/2 масофага кўчиш вақтига тўғри келади. Масалан, 900 МГц, диапазонда ишлайдиган

системалар учун V = 60 км/ч да д флюктуация жараёни тахминан 10 мс ни ташкил қилади.



2.3-расм. Корреляция коэффициентининг вақтга боғлиқлиги.

Тез қотиб қолишларнинг ёқимсиз оқибатларидан бири эгилувчан сигналнинг белгиси остонадан пастга тушиб кетганида содир бўладиган хатолар пакетларнинг пайдо бўлиши ҳисобланади. Хатолар пакетининг узунлиги ва пайдо бўлиш эҳтимоли частота танланишлари (даражани кесиб ўтиш) ва қотиб қолишларни давомийлиги билан аниқланади.

Рэлеев қолдиқлари учун частота *NR,* Я сатхини кесиб ўтиш даражаси қуйидагича айтилиши мумкин:

Экспериментал маълумотлар билан яхши мувофиқлаш хисоб китоблар кўрсатадики, 30...10дБ чуқурликда 60 км/ч тезликда ўртача частота қотишлари 5...50 Гц ни ташкил килади, қотишларнинг ўртача давомийлиги эса 30...10дБ дан паст даражада худди шу тезликда - 0,2...2 мс (900 МГц диапазонда ишлайдиган системалар учун).

Чиқадиган сигналлар маълум бир давомийлигига ва частотасига эга. Агар ҳамма спектрал ташкил қиладиган сигналлар бир хил қотса ва радиоканал характеристикаси вақтида ўзгармаса, қотишлар силлиқ деб номланади.

Практикада бу иккала шароит тез тез бажарилмайди. Бундай ҳолатда *частота – селективли* (ЧСС) ва *вақтинчалик селектив сўнишлар* (ВСС) содир бўлади.

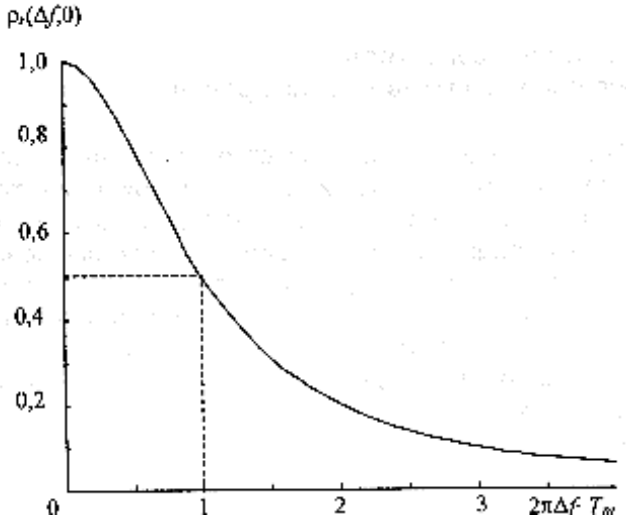
ЧСС нинг асосий сабаби кўп нурли тарқалиш оқибатида вақтинчалик тарқалишлик ҳисобланади. Ҳар хил йўллар билан тарқаладиган бир хил частота компонентлари орасидаги фазоларнинг ҳар хиллиги, ҳар хил частота спектрлари учун деярли мустақил бўлиши мумкин, шундайда баъзи гармоникалар кўп нурли интерференция оқибатида кучайиши мумкин, баъзилари эса сусайиши мумкин.

Частота – селектив сўнишлар шунда пайдо бўладики, қачонки спектр сигналининг кенглиги алоқа каналининг *когерент чизиғини* - Вс, частота интервали ошганда, чегараларида спектрал компонент сўниб қолишлари аниқ бир корреляция коэффициентинингт тўхташ аҳамияти билан ҳарактерланганда. Йўл қўйиладиган бузилишларнинг даражаси кодек ва модемда сигналларнинг қайта ишлаш усулларига боғлиқдир.

Ушбу боғлиқлик 2.4. расмда кўрсатилган. Корреляциянинг 0,5 даражасида когерентлик кенглиги ВС =1. Т катталигининг қиймати деярли кенг миқдорда ўзгариши мумкин.(0,1...10 мкс) шаҳар шароити учун хос бўлган T = 2 мкс қийматида когерентлик кенглиги Вс = 80 кГц бўлади.

Частота - селектив қотиши кўпчилик холларда МРТ фаолиятини кўпинча қуйидаги холларда қийинлаштиради:

• 403 эквиваленти нотекис амплитуда – частота характеристикаси ва қабул қилинаётган сигнал спектори ва унинг формаларини бузилишига олиб келади;



2.4-расм. Сигналларнинг қайта ишлаш усулларига боғлиқлиги.

• агар МТРнинг тўғри ва қайтувчи каналлари частота бўйича фарқи когерентлик кенглиги ошади (ушбу холат уяли алоқанинг деярли барча тизимлари учун характерли), ЧСС алоқа канали ассиметрлигига олиб келади, ва бу МС ва БС узаткичлари қувватини бошқариш холатини қийинлаштиради.;

• ЧСС вақт бўйича қабул қилунувчи сигналлар чўзилиши билан кузатилади, бу эса символлараро интерференцияга олиб келиши мумкин;

• ЧСС тизим кўринишида мураккаб техник ечилмаларини қўллашни талаб этади (масалан, эквалайзерлар).

Шу билан бир қаторда ЧСС маълум ижобий шароитларга эга:

• тор полосали тизимларда қачонки сигнал спектри тўлиқ каналнинг когерент чизиғида жойлашган бўлса, аммо узатилувчи когерентлик чизиғидаги қийматдан юқори қийматга ўзгарувчан бўлиши мумкин, бу билан кам сўнишли частота каналини аниқлаш имкони туғилади;

• кенг полосали тизимларда канал когерентлик чизиғидан сигнал спектори жуда кенг бўлганда (масалан IS-95 стандарт тизимида), катта сўнишлар кичик спекторнинг кичик қисмини йўқотади, бу дегани ташқи сўнишлар таъсиридан сўнишлар пропорционал кичик бўлади.

Вақт ўтиши билан радиоканал характеристикаларининг ўзгаришида ВСК рўй беради. ВСК нинг асосий сабаби доплер ёйилиши (рассеяние) – кўп нурли тарқалиши алоҳида радиотўлқинларнинг частотаси доплер қадами фарқи. ВСК МС харакати ва кўпнурли тарқалиши бўлганда доим қатнашади. Бу маънода тез қотишнинг сигнали хисобланади.

ВСК – ахборот жўнатмалари (узунлиги) давомийлиги Т алоқа каналининг когерентлик ва теорема катталигидан (катта бўлса) ошса (кўринади) пайдо бўлади. *Т«* — чегарасидаги қотиш коррецияси коэффицентининг аниқ қиймати биланхарактерланадиган вақт орасида (3.18) ифода: Корреляция бўсағавий даражаси 0,5 (2.3. расмга қаранг) *Тсс* 9/(16) бўлганда.:

Масалан харакатнинг 60 км/ч соат тезлигига корреляция вақти 900 МГц диапазонда 4 мсни ташкил этади.

Селектив қотиш кенг чизиғли тизимларда содир бўлади. (масалан, CDMA тармоғида). Бунда кескин содир бўлмайди, бироқ қабул қилинувчи сигналларни вақт бўйича тузилиши жойига ва символлараро интерфференцияга эга.

2.2. Шифрлаш усуллари

Симсиз алоқа тизими радиоэфирга доступ эркинлиги кучи турли хил ёмон ниятли кишиларга бегона ахборотдан саноқсиз фойдаланиш билан хабарни эгалаш каби, абонент ва тармоқлар алдови режасида потенциал сигнали узвийдир. Шунинг учун алоқа тизими стандартлари қонуний фойдаланувчиларни ва тармоқни шундай харакатлардан ҳимоя қилишнинг турли механизимларини эътиборга оладилар. Маълумотларни шифрлаш ва аутентификацияси жараёнлари шундай механизимларга киради. Шифрлаш хабарнинг маъносини беркитиш мақсадида баъзи қойидаларга (ишоралаш алгоритми) асосан чиқувчи очиқ матнни криптограмма айлантиришидан иборат. Шифрлаш холати деб номланувчи ушбу алгоритмининг баъзи параметрлари

фақатгина қонуний абонентларга маълум ва кишилар учун конуний фойдаланувчи шифрни чиқувчи матнга қайта ўзгартиришни осонгина бажара олади. Саноқсиз очиқ матнга эга бўлмоқчи бўлган субъектив, яъни криптоаналитик эса калитни аҳамияти (маъносини) ўйлаб топишга тўғри келади. Хабар таркибидаги маълумотларнинг махфийлик даражасига боғлиқ ҳолда (Давлат аҳамиятига мойиллик, харбий ва х.к.). Шифрлашнинг турли тизимлари ишлаб чиқилмоқда ва қўлланилмоқда. Уларни тизимда интеллектуал ва техник аналитика имкониятлари ҳам ҳисобга олинади. Ёмон ниятли якка кишидан маълумотни беркитиш, калитни очиш учун катта мутахассислар ва янги техникани талаб қила олиш имкониятига эга бўлган давлатга нисбатан осонроқ..

Одатда очиқ матн фрагментига нисбатан чидамли бўлган шифрлаш тизимини ишлаб чиқилади. Бунда тахмин килинадики, аналитикга криптограмма билан солиштириш учун, унга криптограмма, шифрлаш алгоритми ва очиқ матн фрагменти маълум бўлса. Шу сабабли шифрлаш чидамлилиги, аналитикнинг харакатларига, яъни асл матнни очиш харакатига қарши тура олиш ҳусусияти, калитни очиш қийинлиги билан белгиланади.

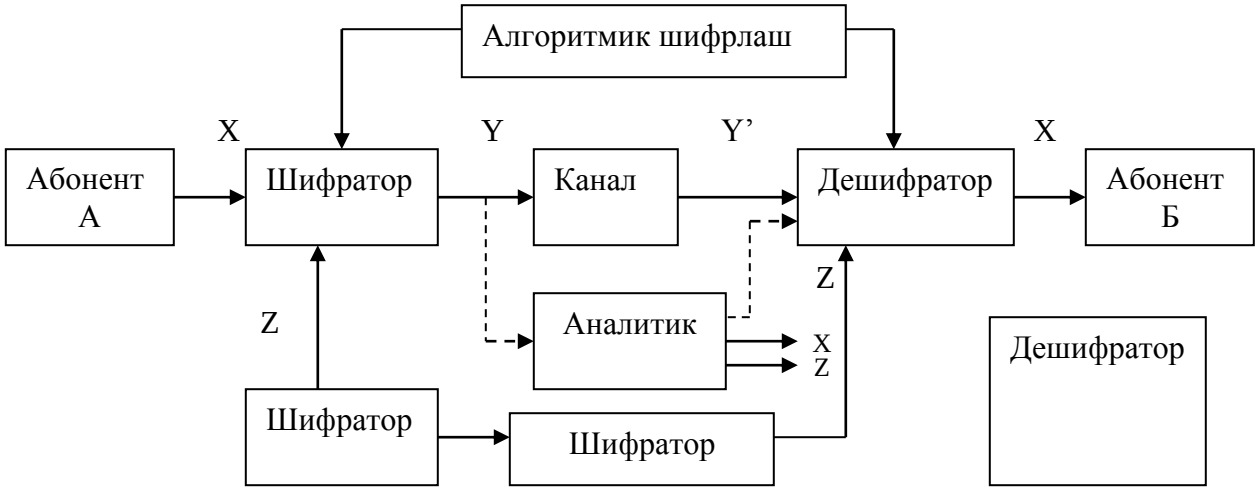
Чидамлилик баҳоси учун турли киритишлар сингари сурилади. Нисбатан объектив бу калитни очиш учун мавжуд алгоритмини қийинлигидир (кўпайтиришлар сони) агар операциялар сони пропорционал мураккабликни очиш алгоритмигина маълум бўлса, унда шифрлаш тизими муккамал чидамлиликка эга ҳисобланади. Масалан бундай ечиш алгоритми, вариантларни тўғри очишни такидлайди. Аналитик турли шароитда параметрлар танлови (кучли кутиш)дан фойдаланган ҳолда, мукаммал чидамлиликга эга бўлган тизимни ишлаб чиқиши мумкин эмас. Кичик мураккабликка эга калитни очиқ алгоритмини маълум бўлган бошқа шифрлаш тизимлари – масалан, полиномиал (линияли) u', га пропорционал операциялар сони билан, кичик чидамлиликга эга тизим хисобланади.

Шифрлаш тизимининг яна бир муҳим характеристикаси, калитини билган ҳолда шифрлаш ва дешифрлаш алгоритимларининг тез таъсири ҳисобланади. Кўплаб шифрлаш тизимлари симметрик бир калитли ва ассиметрик икки калитли ёки очиқ калитли тизимларга ажратилади. Шифрлаш ва шифрни очиш учун классик симметрик тизимларида фақат битта калит ишлатилади. Ассиметрик тизимларида шифрлашни очиш учун ҳаммага маълум (ёмон ниятли кишиларни ҳам) очиқ калит ишлатилади, асл матнни шифровкаси бўйича олиш учун эса – махфий, хабарни қонуний олиш учун кишигагина маълум калит ишлатилади. Ушбу калитлар орасида шифрни тўғри очишни таъминловчи, очиқ калит бўйича мавхум калитни аниқлаш имкониятини бермайдиган алоқа мавжуд.

2.2.1. Шифрлашнинг симметрик тизими

Узатувчи тарафда асл матнни $\mathbf{X} = (\mathbf{X_1}, X_2, ..., X_n)$ маълум алгоритм ва махфий калит **Z** = (Z,, Z,, ..., ZД) ёрдамида шифтограммага ўзгаради **У** = (У,, У, ..., У„). Ушбу кетма – кетликлар компоненти турли хажмдаги бир ёки бир нечта алфавитлардан олинган бит, символлар бўлиши мумкин. Одатда улар битлардир. Қабул қилвчи тарафда маълум бўлган Z калит асл матн X га тикланади.

Аналитик шифтограммани олиб, асл матнни тушунишга ёки шифрларни калитини аниқлашга харакат қилади. Бундан ташқари у Б абонентнинг олдинги қисмига нисбатан шахсий системасидаги қалбаки криптограммасини тадбиқ этиши мумкин.



2.5-расм. Хабар аутентификацияси.

Шу йўл билан шифрлаш тизими фақатгина алоқа махфийлигини сақлаб қолмасдан, балки сақланмаган ўзгариш, **X** хабарни алмаштиришдан химоя қилишни ҳам таъминлаши керак. Хабар аутентификацияси *бутунлик* текшируви деб номланувчи сўнги масала 2.5-расмда мухокама қилинмоқда.

Ушбу схемадан кўринадики, қабул қилувчи тарафга шифрлаш калитини оператив етказиб бериш учун махсус, ҳимояланган канал бўлиши керак. Фойдаланувчилар орасида шифрлаш калитини тақсимлаш масаласи ёки калитларни бошқариш масаласи пайдо бўлади. Симметрик тизимдан фойдаланганда алоқа ўрнатишни хохловчи абонентлар кўп бўлса калитларни тақсимлашда жиддий муаммо касб этади.

Назария ва амалиёт юқори тезликли шифрлаш тизимлари калитларига бир қатор талабларни шаклланишига имкон берди. Маълумотлар назарияси томонидан криптограммани калитсиз очиш бўйича энг кўп қийинчиликлар, агар унда X ва Y тасодифий жараёнларни статистик мустақиллигини таъминловчи ўзгартиришларни ифодаловчи X тўғрисида маълумот йўқ бўлганда вужудга келади.

Бу талабни тахлили қуйидаги тавсияларни вужудга келтиради. Калитнинг аниқ қиймати фақат битта хабарни шифрлаш учун бир марта ишлатилиши мумкин. Калит қийматлари бир хил эхтимоллик 1/L билан танланиши лозим, бу ерда L – калитнинг символларининг алфавит хажми. Калит узунлиги k хабар узунлиги *и* дан кам бўлмаслиги зарур.

Амалиётда амалга оширилиши мураккаблиги ва нархининг баландлиги туфайли юқорида санаб ўтилган талабларнинг хаммаси хам қондирилмаслиги мумкин. Амалий шифрлаш тизиларини қуриш учун ёйилиш ва аралаштириш принциплари қўлланилади. Биринчиси матнни битта белгиси криптограмманинг кўпроқ символларини ўзгаришини талаб этади. Иккинчиси **Y** ва **X** лар ўртасидаги статистик алоқани узувчи ўзгартиришларни қидиришга қаратилган.

Амалий пухта (чидамли) шифрларни тузишда умумий ёндашиш, матн символларини, оддий шифрлаш усулларини қайта қўйиш (алмаштириш) йўли билан такрорий қўллашдан, хамда скремблашдан иборат.

Ўриналмаштириш методи, матн символларини шифрлаш калити томонидан бериладиган қоидага асосан шу ёки бошқа алфавит бўйича алмаштиришга асосланади. Бунда матндаги символнинг жойлашиш ўрни ўзгармайди.

Қайта қўйишда очиқ матндаги символлар кетма-кетлиги калит билан мос равишда ўзгаради. Символнинг қиймати бунда сақланиб қолади. Қайта қўйишнинг символлари блокли бўлиб, матн аввало блокларга бўлинади ва уларда берилган калит бўйича қайта қўйиш амалга оширилади.

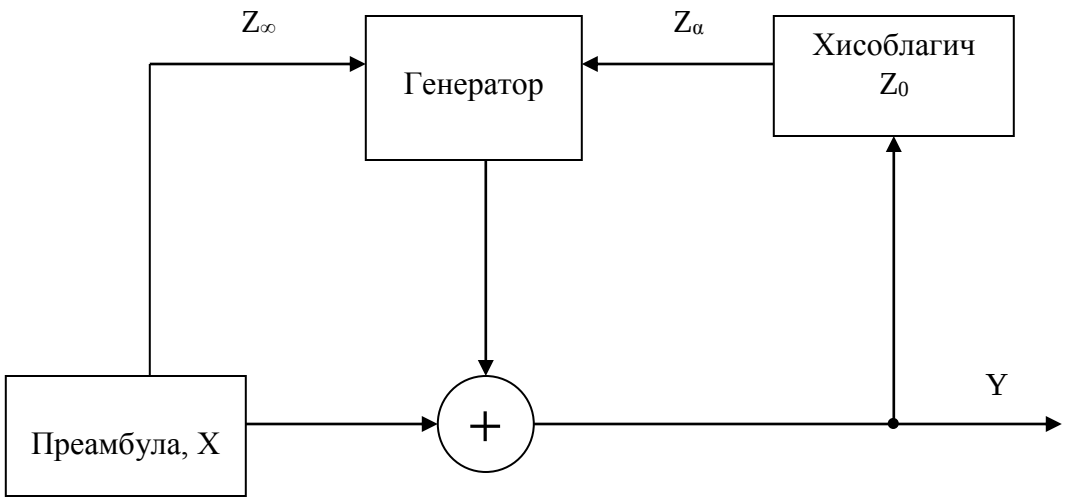
Скремблаш деганда очиқ матннинг символлари кодлари ўрнига гамма деб аталувчи (грекча гамма харфи бўлиб, математикада тасодифий жараёнларни ифодалайди) тасодифий кетма-кет сонлар кодларини қўйиш тушунилади. Гаммалаш (Гаммирование) оқимли шифрлаш усулларига таълуқлидир, очиқ

текстнинг кетма-кет жойлашган символлари мос равишда шифрограмма символларига айлантирилади ва шу хисобига ўзгартириш тезлиги тезлашади.

Гамма сифатида *сохта тасодифий кетма-кетликлар* (СТК) қўлланилади. Y криптограмма символларининг X ва Z кодларини модул 2 бўйича разрядлараро суммаси мавжуд. **X** = Y'+Z = X+Z+Z = X қоида бўйича расшифровка қилинади ва қабул қилиш қисмида худди шундай фазага эга бўлган СТК хосил қилиниши зарур. Скремблаш барқарорлиги СТК параметрлари билан аниқланади. Улардан энг мухими кетма-кетлик даври хисобланади. Амалиётда даври бир неча хафтага тенг бўлган СТК генераторлари қўлланилади. СТК нинг оддий хосил қилиниши ва юқори шифрлаш тезлиги мавжудлиги туфайли – скрембли дешифрлаш мобил алоқанинг кўпчилик стандартларида қўлланилади (GSM, TETRA, IS-95).

Очиқ текстнинг фрагменларини таққослаш ва шифрлашнинг СТК элементларини аниқланиши қийинлаштириш учун чиқишдан тескари алоқа ва шифротекст қўлланилади. 2.6-расмда шифротекст бўйича тескари алоқани қўллаш тушунтирилади.

Олдин хосил қилинаётган СТКнинг параметрлари тўғрисида маълумотларни хамда фазанинг бошланғич қиймати Z~ ни ўз ичига олган преамбула узатилади. Шифрограмманинг хар бир шаклланган символлари *и* га генераторда Z фазанинг янги қиймати ўрнатилади. Тескари алоқа гаммалаш усулини криптограмма бузилишларига таъсирчан қилиб қўяди. Алоқа каналларидаги шовқинлар туфайли қабул қилинган символлар бузилиши мумкин, оқибатда СТК нинг фазасини хато хисобланишига олиб келади ва кейинги расшифровкани қийинлаштиради. Бундай хол учун ёвуз ниятли одамни сохта маълумотларни киритиш харакати туфайли бузилишлар содир бўлишини мисол қилиб келтиришимиз мумкин.



2.6-расм. Тескари алоқали оқимли шифрлаш.

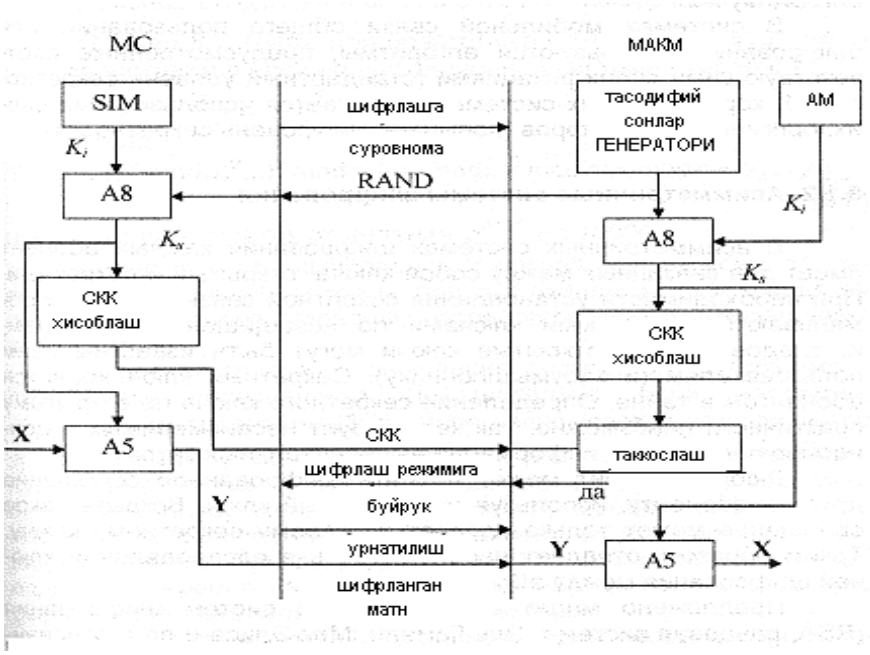
Шуни таъкидлаш лозимки, миллий стандарт шифрлашларда алмаштириш, жойини ўзгартириш ва гаммалаш усулларидан фойдаланиш белгиланган.

Калитларни тақсимлаш симметрик шифрлаш тизимларида, агар қонуний фойдаланувчилар сони катта бўлса, жиддий масала хисобланади. Калитларни тақсимлаш протоколи калитни оператив тарзда ўзгартириш ва радиоканал орқали сеанс калитини юборишни тақиқлаш имкониятига эга бўлиши зарур.

Одатда тақсимлаш протоколи икки этапни ўз ичига олади. МС ни тармоқда регистрация қилишда аутентификация маркази (АМ) унга, стандарт идентификация модули (СИМ) да сақланувчи К махфий сон ажратади.

Махфий алоқани хосил қилиш зарурияти туғилганда МС шифрлашга сўров юборади 2.7- расм. МАМК, А8 алгоритми бўйича ягона К калитни аниқлаш учун RAND *(random number)* тасодифий сонни генерациялайди хамда МС га юборилади, бу холат иккала томонда хам қўлланилади. Радиоканалларга таъсир этувчи шовқинлар туфайли RAND ни бузилиши кузатилиши мумкин ва МС даги калит МАКМ даги калитдан фарқ қилиши мумкин. Калитни асллигини текшириш мақсадида унинг хеш функцияси коди бўлмиш калитнинг сонли

кетма-кетлиги (СКК) қўлланилади. К калитнинг хар қандай ўзгариши катта эхтимоллик билан СКК нинг ўзгаришига олиб келади, лекин СКК орқали калитнинг қийматини аниқлаш жуда қийин. Шунинг учун радиоканал орқали ушлаб олинган СКК шифрни барқарорлигини пасайтирмайди. Калитларни ўрнатилиши аниқлиги текширилгандан сўнг А5 алгоритми бўйича маълумотларни оқимли шифрлаш амалга оширилади.



2.7 – расм Шифрлаш протоколи

Умумфойдаланувчи мобил алоқа тизимларида шифрлаш учун махсус спецификациялар (махфийликни стандарт даражаси)га мос келувчи алгоритмлар қўлланилади. Корпоратив тизимларда ўзларининг оригинал шифрларини (махфийликни юқори даражаси) қўлланилишига рухсат берилади.

2.2.2. Асимметрик шифрлаш тизимлари

Асимметрик шифрлаш тизимларида хар бир абонент ўзаро боғланган иккита калитларга эга бўлади: очиқ ва махфий. Махфий алоқани хосил қилиш зарурияти туғилганда абонентлар химояланмаган канал бўйлаб очиқ калитлар билан алмашадилар, шундай экан, очиқ калитлар барча фойдаланувчиларга маълум бўлиши мумкин (жумладан ёвуз ниятли одамга хам). Махфий калит эса абонентларда сир сақланади. Очиқ каналлар бўйлаб махфий калитларни аниқлаш деярли мумкин эмас, чунки бунга жуда катта маълумотлар ва вақт талаб қилинади.

Хохлаган абонент ўзининг очиқ калитини ишлатган холда бошқа абонентга шифрланган хабар юбориши мумкин. Бундай шифрланган хабарни фақатгина иккинчи абонент ўзининг махфий калити ёрдамида оча олиши мумкин. Бу холда, абонентлараро шифрлаш калитларини тақсимлаш зарурриятн йўқолади.

Жуда кўп асимметрик шифрлаш тизимлари таклиф этилган (RSA, Эль-Гамал тизими, Мак-Элис ва х.к.), аксарияти бир томонлама ёки бир йўналишли функцияларга асосланган.

$$Y = f(X) \qquad (2.1)$$

функцияси бир томонлама дейилади агар X бўйича Y ни хисоблаш полиномиал алгоритм даражасида бўлса ва Y бўйича X ни аниқлаш учун фақатгина экспоненциал даражадаги алгоритм мавжуд бўлса. Акс холда, X бўйича Y ни аниқлаш осон, Y бўйича X ни аниқлаш қийин бўлади. Берилган функция бир томонлама эканлигига аниқ далил исбот йўқ. Вахоланки математикада олдин ечилиши мумкин бўлган масалалар кейинчалик сермехнат бўлиб ечилиши қийинлашиши мумкин. Бундай тўпламларнинг энг ёрқин мисоли сифатида баъзи модуллар бўйича халқали ушлаб қолишлардаги кўрсатиш функцияси хисобланади.

Унинг бир йўналишлигини қуйидаги мисолдан кўриш мумкин.

Кўриниб турибдики Y ни хисоблаш учун фақат 16 та кўпайтириш ва бўлиш амаллари зарур бўлди, қайсики белгиланган модулда 4 қуйи разрядларни квадратга оширилишидан ушлаб қолишга харакат қилинади.

Тескари масала – дискрет логарифмни аниқлаш – деярли имкони йўқ. Хақиқатдан хам, агар, масалан Y=5678 бўлса у холда тенглик ах = * *...* 5678, тенглама кўринишида ёзилади, бу ерда * белгиси номаълум ўнли сонни билдиради. Ушбу ноъмалум сонларни фақатгина X қийматлари билан охирги вариантларни саралаб, баравар қайта тиклаш мумкин. 100 – 300 разрядлик ўнли сонларни бундай саралаш энг кучли компютер орқали хам ақл бовар қилмас катта даврни талаб қилади.

Аммо, функция “якка холда” шифрлаш мақсадлари учун яроқсиздир, чунки қонуний қабул қилувчи X текстни **т** шифрограмма бўйича аниқлаш жараёнида криптоаналитик каби қийинчиликларга дуч келдаи. Шунинг учун қонуний абонентга туйнук (яширин кириш – лазейка) киритилади, уни қўллаш оқибатида қонуний абонент тескари функцияни аниқлашда сарф харажатларни кескин тушишига олиб келади.

Лазейкали бир томонлама фунция деб У = fz(X), функцияга айтилади ва у қуйидаги хусусиятларга эга:

• **X** бўйича Y ни аниқлаш полиномиал мураккабликка эга бўлган алгоритм мавжуд;

• **X** бўйича Y ни Z маълум бўлган холда аниқлаш фақат экспоненциал мураккабликка эга бўлган алгоритм мавжуд;

• Y бўйича X ни Z маълум бўлган холда аниқлаш полиномиал мураккабликка эга бўлган алгоритм;

Таърифдан кўриниб турбдики, Z шифрограммани қонуний қабул қилувчисида бўлган махфий калит вазифасини бажармоқда. Бу ердан очиқ калитли шифрларни яратиш механизми ойдинлашади. Қийин ечиладиган

масалаларда шарт бериладики, бунда масалани полиномиал мураккаблигини ечиш алгоритмини яратиш билимига эга бўлиш зарурдир. Бу шарт қонуний фойдаланувчининг сири хисобланади.

Мисол тариқасида асимметрик шифрлаш тизими RSA (Ривест, Шамир, Адлеман) ни кўриб чиқамиз. Унинг асосига катта сонларни кўпайтувчиларга ажратиш (факторизация) каби мураккаб масала ётади. Сонларни факторизация мураккаблиги қуйидаги фактни тасвирлайди. 130 хонали сонни ажратиш учун 1600 та ЭХМ нинг 8 ой мобайнида ишлаши талаб қилинади.

Келинг $u = p\ q$ бунда p ва q — оддий сонлар бўлсин, яъни ўзига ва 1 га бўлинадиган сонлар. Хар бир фойдаланувчи p ва q ни хамда тасодифий d ни танлаган холда тенгламани ечими сифатида e ни аниқлайди, яъни ўзининг (e,n) очиқ хамда махфий (d,n) калитларини олади. Криптоаналитиклар учун d ни маълум (очиқ) калит бўйича аниқлаш юқорида қайд этилган факторизация ва мураккабликни англатади.

Х очиқ матнни шифрлаш, аниқ бир қоида билан Х бутун сонга ўзгартиришни тоқазо этади (оддий шаклда мисолда келтирилган). Криптогрпаммани берилган фойдаланувчи адресига хисоблаш қуйидаги формула бўйича амалга оширилади:

У = *Х , юқорида қайд этилганидек аналитикка Х ни маълум бўлган Y бўйича аниқлашига йўл қўймайди.* Адресат ўзининг махфий калити билан Х бутун сонни осон аниқлайди

Х=У" *modn, кейин эса у ёрдамида дастлабки (бошланғич) матн Х ни тиклайди, яъни d, қонуний абонентY расшифровкалашда фойдаланадиган лазейка хисобланади.*

RSA авторлари юқори барқарорликни таъминлаш мақсадида 200 та ўнли рақамли (хонали) сонларни ишлатишни тавсия этадилар. Гарчи сонларни юқори даражаларга оширувчи махсус хисоблагичлар яратилганлигига қарамасдан RSA нинг тезлиги паст хисобланади.

Асимметрик шифрлаш тизимлари назарий жихатдан юқори барқарорлик билан характерланади. Лекин унинг тадбиқ этилиши амалиётчилар томонидан ишончсизликка учраган. Юқорида таъкидлаб ўтилганидек, математиклар муваффақиятлари анчагина мураккаб масалаларни ечишга олиб келиш хафи доимо мавжуддир. Шифрлаш тарихи шундай мисолларни билади. У=Х, бу ерда Х – бутун сонлар устуни, бир томонлама ўзгартиришга асосланган ранцли шифрлаш тизимлари учун Х ни Ү бўйича аниқлаш алгоритми топилган бўлиб, Х ни тўғридан тўғри танлаб олишга нисбатан операциялар сонини камлиги билан фарқланади.

Шу билан бирга асимметрик шифрлаш тизимларида шифрлаш калитларини тақсимлаш талаб этилмайди. Шунинг учун гибрид тизимлар перспектив (стиқболли) бўлиб, уларда сеанс калитларини тақсимлаш вазифасини асимметрик тизим бажарса, симметрик тизим эса маълумотларни шифрлаш вазифасини бажаради. Бир томонлама функция асосланган калитларни тақсимлашнинг классик протоколи 2.2- жадвалда келтирилган.

Абонетлар мустақил ва тасодифий тарзда сонларни танлайдилар ва уларни сир тутадилар. (2.1) бўйича хар бири ўзининг очиқ калитини (е ёки ее) аниқлайди ва уни бошқа абонентга юборади.

2.2 - жадвал.

Шифрлаш калитининг тақсимлаш протоколи.

Параметр	Абонент А	Абонент Б
	$0 < d_A < p$	$0 < d_Б < p$
Очиқ калит	$e_A = a^{d_A} \bmod p$	$e_A = a^{d_Б} \bmod p$
Сеанс калити	$Z_{АБ} =$ $e_Б^{\,d_A} \bmod p = a^{d_A d_Б} \bmod p$	$Z_{АБ} =$ $e_A^{\,d_Б} \bmod p = a^{d_A d_Б} \bmod p$

(2.2) нинг бир томонламалиги туфайли очиқ калитлар бўйича махфий калитларни очиш қийиндир. Шифрлаш режими ўрнатилиши билан хар бир абонент ўз сеанс калитини хисоблайди. Бунинг учун бошқа абонентнинг очиқ калити ўзининг махфий калитига тенг бўлган миқдор даражасига оширилади. 2.2- жадвалдан кўриниб турибдики, бундай хисоблашлар бир хил Z e = ZeA қиймат беради ва уни симметрик шифрлаш тизимларида сеанс калит сифатида қўллаш мумкин. Шуни таъкидлаш жоизки, калитларни тақсимлаш алоқа канали орқали махфий параметрларни узатишларсиз амалга оширилди.

2.3. Мобил алоқа тизимларида идентификация ва аутентификация

Идентификация ва аутентификация жараёнлари қонуний абонентларни ёвуз ниятли одамларнинг алдовларидан химоя қилиш мақсадида қўлланилади.

Қурилма *идентификацияси* деганда, тармоқ хизматларига даъвогарлик қилаётган ва МАКМда рўйхатга олинган бирор МСнинг ажратилиши тушунилади. МС идентификатори одатда тайёрловчи коди, йиғиш жойи ва электрон серия рақамидан ташкил топади. Идентификация процедураси тармоқга шу МСнинг статусини аниқлашга имкон беради, яъни хизматлар рўйхати, доступ олишда приоритет даражаси, алоқа каналини ўрнатиш ва х.к. GSM стандартидаги алоқа тармоғининг коммутация маркази (КМ) қурилмаси идентификация регистрида учта рўйхат мавжуд: оқ, кулранг ва қора. Оқ рўйхатга киритилган МСга тармоқдан фойдаланишга рухсат берилади. Кулранг рўйхатда шундай МС идентификаторлари сақланадики, тармоқни ечилмаган (хал этилмаган) масалалари ёзилади (ремонт талаб, хизматларга хақ тўлашда қарзга эга). Қора рўйхатда эса йўқолган ёки ўғирланган МСлар киритилади, шунингдек, ноқонуний кўпайтирилганлари хам. Таъкидлаш жоизки,

стандартлар қурилма идентификациясидан ташқари бошқа турдаги (абонент, бошқарув, тармоқ) идентификацияларни хам кўзда тутади.

Аутентификация деганда маълум бир объектни хақиқийлиги (асллиги) ни текшириш процедураси тушинилади. Аутентификациянинг хабар, абонент, қурилма, маълумотлар массиви каби турлари мавжуд. Бу процедураларни тузилиш принципларини кўриб чиқамиз.

2.3.1. Хабар аутентификацияси

Хабар аутентификациясининг мақсади қуйидаги таклифларни тасдиқлаш ёки инкор этишдан иборат:

• хабар қонуний абонентдан келяпти;

• хабар юборилиш вақтида ўзгармаган;

• хабар керакли манзил (адрес)га етказилди;

• қабул қилинган хабар кетма-кетлиги юборилган хабар кетма-кетлиги билан мос тушади.

Аслликни текшириш шифрограмма учун жуда мухим, зеро қабул қилувчи кўпроқ ишонч хосил қилади. Аутентификация усуллари хеч қандай ташқи воситаларни жалб этмаган холда хабарнинг ўзи бўйича асллик ўрнатилади деган фараз билан яратилади. Бунинг учун узатувчи томонда X хабарига қўшимча хеш-функция коди киритилади. Шунингдек у сигнатура, комбинация назорати, имитовставка, хабар дайджести деб хам аталади. Таъкидлаб ўтилганидек, X хабари олдиндан сонга ёки сонлар тўплами X га ўзгартирилади. И(X) хеш-функция фиксирланган символлар кетма-кетлиги узунлигида X ихтиёрий узунликни тасвирлайди.

Бундай тўлдиришда узатиш тезлигини тушиши ахамиятли бўлмаслиги учун, албатта талаб: *m « /* бўлади.

(X,И(X)) хабарини асллигини текшириш, И(X) қиймати билан қабул қилинган X ни тўғридан тўғри хисобланган h '(X) ни таққослашни ўз ичига олади. Агар улар тенг бўлса, у холда (X,И(X)) ни узатишда ўзгармаган деган қарор қабул қилинади. Акс холда хабарни бузилгани қайд қилинади.

m «/, экан бир нечта коллизия деб аталувчи хабарларга битта хеш-функция қиймати мос келади. Узатилган хабарни хар қандай коллизияга алмаштириш аслликни текширишда аниқланмаслиги рашван. Хабарни мувафаққиятли сохталаштириш эхтимоллиги h(X) қийматни разряди билан аниқланади. Амалиётда 64-150 бит узунликкача ишлатилади. Хеш-функцияга қуйидаги талаблар қўйилади: матндаги мумкин бўлган ўзгаришлар (қўйилмалар, чиқаришлар, қайта қўйишлар ва х.к.) га таъсирчанлик, коллизиялар қидирувини эффектив алгоритмларини йўқлиги, h(X) қийматни хисоблашнинг оддийлиги.

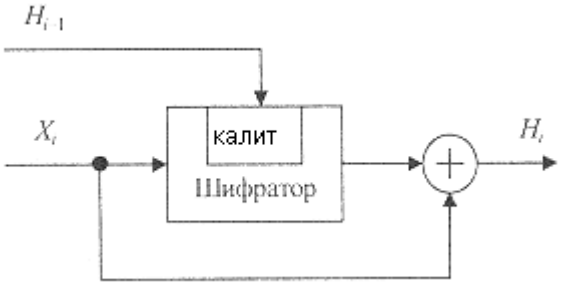
Бир йўналишлик зарурияти калитларни тақсимлаш протоколи (2.2 жадвал) тавсифидан келиб чиқади.

Хешлашни жуда кўп усуллари таклиф этилган. Имитовставка учун давлат стандарти хам ишлаб чиқилган. Мисол тариқасида хеш-функциясини кўриб чиқамиз.

Аммо ёвуз ниятли одам хам хешлаш алгоритмини билган холда сохта хабар яратиши ёки асл хабарни ўзгартириши мумкин, хеш-функцияни тўғри қийматини хисоблаб топиши мумкин. Шуниг учун рекурент жараёни турдаги махфий параметрлардан фойдаланган холда амалга оширилади. Калит сифатида махсус махфий сонлар, қиймати *H,,* хабарлар блоки X ва уларнинг комбинациялари қўлланилиши мумкин. 2.8-расмда хеш-функцияни шифрлаш схемаси келтирилган бўлиб, унда калит сифатида унинг олдинги қиймати олинади.

Кўриб чиқилган аутентификация жараёни маълумотлар алмашаётган икки абонент ўртасида ишонч бўлишини талаб этади, яъни ташқи аралашишлардан химоя қилади. Хаётда абонентлар ўртасида ишонч бўлмаган жуда кўп вазиятлар

мавжуд (молиявий ташкилотлар ўртасида электрон хужжатлар билан алмашиш, мижоз ва банк ўртасида ва х.к.).



2.8 – расм. Хеш функциянинг шифрлаш схемаси.

Бундай холларда қонуний абонентлар томнидан алдовлар бўлиши мумкин. Масалан, А узатувчи абонент ўзининг хабаридан воз кечиши мумкин, қабул қилувчи эса юборилган хабарни ўзгартириб уни абонент А шундай тарзда юборганлигини таъкидлаши мумкин.

Мобил алоқа тизимларининг ривожланиш тараққиёти шуни кўрсатадики, электрон тижоратдан катта муваффақиятлар кутилмоқда. Мобил телефон орқали хар қандай банк операциялари бажарилиши таклиф этилмоқда. Бундай шароитларда қонуний абонент алдовидан химоя қилиш мухим вазифага айланмоқда.

Хабарларни аутентификациялашда ишонч бўлмаган холларда *электрон имзо* қўлланилади. Унинг вазифаси қоғозли хужжатлардаги қўйиладиган имзолар билан бир хил. Бироқ берилган матнга электрон имзонинг тегишлилиги ушбу хужжатни бутунлигини хам таъминлайди.

Ушбу технологияни RSA мисолида тушунтириб ўтамиз. Масалан (d, *n)* ва (e, *n)* — мос равишда А абонентнинг очиқ ва махфий калитлари бўлсин.

Х хужжатга электрон имзо (ЭИ) ни қўйиш, унинг хешлаш ва (d, *n)* махфий калит ёрдамида хеш-функция қийматини *Н Д с* шифрлашни ўз ичига олади. К $H_{,,}$ абонент идентификаторини қўшиши мумкин. Хабар рақами, узатиш вақти ва бошқа маълумотлар эса бўлиши мумкин бўлган алдовдан химояланиш учун

мўлжалланган. Оқибатда имзоланган хужжат **Y** = (X, ЭП), где ЭП = *H,,″* modn кўринишга эга бўлади.

А имзони Б абонент томонидан текшириш қуйидагиларни ўз ичига олади:

• абонентни очиқ калити орқали ЭИ ни расшифровкалаш;

• X қиймати бўйича хеш-функцияни аниқлаш;

• таққослаш.

Агар бу қийматлар тенг бўлса, у холда X хабар А абонентдан келган хақиқий хабар деб қарор қабул қилинади. Тенг эмаслиги эса ё X хабар ўзгарган (алоқа каналларида бузилишга учраган бўлиши мумкин), ёки бошқа абонент томонидан юборилган.

Абонент А, Y дан воз кечолмайди, чунки у махфий калитга эга бўлар экан, ЭИ ни яратиши мумкин, унинг очиқ калити ёрдамида расшифровка тенгламаси ечилади. Абонент Б, Хни ўзгартира олмайди ва уни хақиқийлигини тасдиқлай олмайди, чунки у (d, *n)* калитни билмаган холда ўзгартирилган X га ЭИ ярата олмайди. **Y** дан электрон имзони ажратиб олиш ва уни янги хужжатга боғлаш қуйидагича топилади: сохта хужжатга *H* га тенг бўлмаган *H,* қиймат мос келади. Агар хақиқий X унинг коллизияси билан алмаштирилса алдов муваффақиятли бўлиши мумкин.

Шуни таъкидлаш жоизки, хабарларни халақитлардан химоя қилиш ва ёвуз ниятли одамлардан химоя қилиш усуллари ғоявий умумийликка эгадир. Иккала холда хам хабар билан функционал боғлиқ бўлган қўшимча символлар киритилади. Халақитбардош кодларда ушбу боғлиқликлар шундай танланадики, бунда алоқа каналларида энг кўп содир бўладиган халақитларни аниқлаш ва тўғрилаш имкони мавжуд бўлади. Ёвуз ниятли одамлардан химоя қилиш учун функционал боғланишлар махфий қилинади, бунда душманни интелектуал ва техник имкониятлари хисобга олинади. Халақитбардош кодларни тузулиш принциплари шифрлаш учун хам қўлланилиши мумкин. Бу борада Мак-Элис

асимметрик шифрлаш тизими анча машхур бўлиб, линиявий кодларни декодерлаш мураккаблигига асосланган.

2.3.2. Абонент аутентификацияси

*Абонент аутентификацияси*нинг вазифаси – алоқа тармоғи хизматларидан фойдаланаётган абонентнинг хақиқийлигини аниқлашдан иборат. Бунинг учун криптографик протоколлар ишлаб чиқилган бўлиб, улар ёрдамида қонуний абонентлар ўз мақсадига эришадилар, ноқонуний абонентлар харакатлари эса инкор этилади.

Аутентификациянинг кенг тарқалган турларидан бири бу махфий символлар (харф ва/ёки рақамлар) кетма-кетлиги – пароллар хисобланади. Абонент бирор қурилмага доступ олиш учун ўзининг паролини киритади. Бу киритилган парол қурилма хотирасида сақланаётган ва шу абонент номига бириктирилган парол билан солиштирилади. Фақатгина улар мос тушсагина абонентга рухсат берилади. Б уборада GSM стандартида парол, яъни PIN *(personal identification number)* код, МСни активациялаш учун хизмат қилади. Уч маротаба нотўғри PIN код териш натижасида симкарта блокировкаланади ва ушбу МС билан ишлаш тақиқланади.

Паролли аутентификация, тасодифий ва узун пароллар ишлатилганда , шунингдек, паролни тутиб олишлардан ва хотира қурилмасидан уни ноқонуний ўқилишидан химояланган бўлса, яхши барқарорликга эга. МС PIN код териш вақтида абонент қўлида эканлигини инобатга олсак, бу талаблар қондирилади деб хисоблашимиз мумкин.

Узоқлашган қурилмалар учун узатилаётган сигнални тутиб олинишидан сақлайдиган мураккаброқ протоколлар ишлатилади. Улар *ноль даражадаги исбот* ёки *ноль даражали ошкор этиш* принципини хосил қилади. Абонент (МС), (МАМК) га ўзининг шахсий сирини ошкор этмайди, фақатгина унга

эгалиқ қилишини кўрсатади. Одатда абонентлар учун баъзи фунцияларни хисоблаш ва бу хақда шундай хисоблашлар олиб борувчи текширувчига хабар бериш талаб этилади. Ушбу қийматларни таққослаш абонентни хақиқийлигини текширишни таъминлайди.

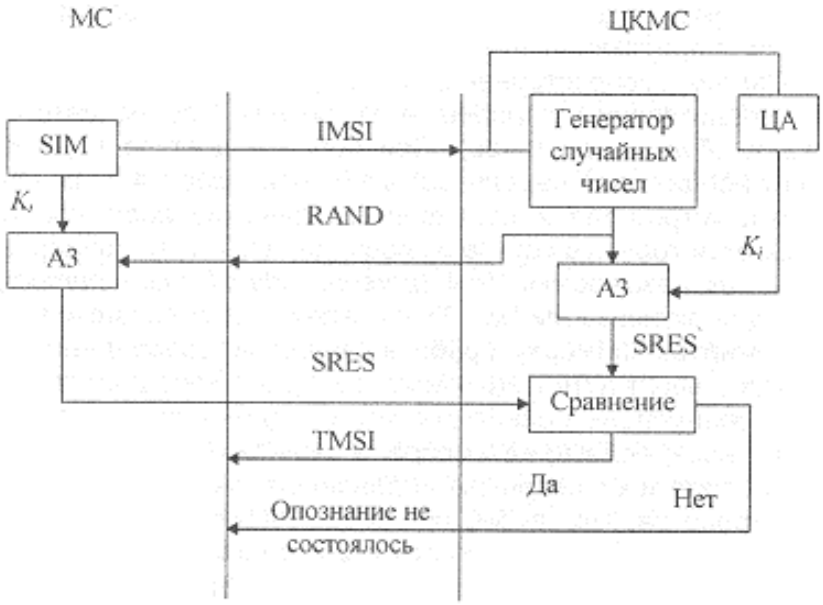
2.9-расмда GSM стандартидаги тизимларда МС аутентификациясининг соддалаштирилган схемаси келтирилган. МС дан ЦКМСга сўров тушиши билан МАКМ унга жавобан тасодифий сон RAND ни узатади. А3 алгоритми бўйича SIM да сақланувчи МС регистрация жараёнида олинган махфий калит К; ёрдамида абонент SRES *(signed response)* жавобни хисоблайди ва МАМК га хабар беради. Коммутация маркази мустақил равишда SRES' ни хисоблайди ва уни радиоканал орқали қабул қилингани билан солиштиради. Уларнинг мос келиши билан МСга аутентификацияни ўрнатилишини тасдиқлаш тўғрисида хабар юборилади. Мос келмаган холда эса – аутентификация (таниш) жараёни ўрнатилмаганлиги хақида сигнал юборилади.

Бу ерда алдов мобайнида ошкор этилмайдиган сир сифатида К; сони хисобланади. Тутиб олинган RAND ва SRES сигналлар орқали К, махфий сонини аниқлай олмасликлари учун SRES бир томонлама функция бўйича хисобланади.

Корпоратив тизимларда алоқа марказидан қилинадиган имитация (ясамалик)га қарши химоя ўрнатилади. Абонент душман томонидан яратилган тизимга эмас балки қонуний тизимга уланганлигига ишонч хосил қилиши зарур. TETRA каби транкли алоқа тизимларида МС аутентификацияси билан биргаликда тармоқ аутентификацияси хам амалга оширилади. У кўрсатилгандагидан фарқ қилмайди, фақат хақиқийликни текширувчи тармоқ эмас балки абонент хисобланади.

МАКМ ва МСларнинг ўзаро алоқаси жараёнида оператив ўзгарувчи, IMSI идентификаторлари билан боғлиқ бўлган *тахаллус* (псевдоним) ларни қўллаган холда МС ни жойлашган жойини махфийлаштириш мумкин. Шундай

экан, GSM тизимида МСнинг хар бир регистрациясидан сўнг янги TMSI идентификатори ўзлаштирилади. Абонентлар ўртасида хабарлар алмашинувининг йўналишларини махфийлиги МАКМ да бошқарув сигналларини беркитиш орқали амалга оширилади.



2.8 – расм. МС аутентификацияси

Битта частотали диапазонда ишлайдиган хар хил радиовоситаларнинг электромагнит бирлашиши муамоси билан бир қаторда, хар хил уяли радиоалоқа тармоқларининг бирлашиши муамоси ҳам мавжуддир. Бу системаларнинг ривожланиши ҳар хил мамлакатларда ўхшаш йўллар билан боради. МРТ ишида диапазонда дешифратор билан тўлқин узунлиги қайсики, деярли барча мавжуд тизимларда уяли алоқада фойдаланилганда, турли тўсиқлар табиий ва сунъий чиқиш таъсир кўрсатади. Табиий келиб чиқишининг асосий тўсиқлари кабул қилгичнинг шовқини, атмосфера шовқини момақалдироқ вақтида электрик разрядларни юзага келиши хисобланади. Бундан ташқари, ҳалал берувчи таъсирлар статик электр, фазовий ва куёш шовқуни хосил қилиши мумкин. Шуни таъкидлаш жоизки, сигнал тарқалиши

вақтида қувватнинг йўқолиши бошқа кўпгина факторларга боғлиқ бўлади, берилганлардан ташқари (масалан, дарахтдаги баргларнинг аниқлиги хисоблаш нихоятда мушкул). Шу сабаб билан МРТ характерлаш вақтида тахмин қилинган бурама районда сигнал қуввати сатхини эксприментал тадқиқотни ўтказиш зарурдир. Хусусан, бундай тажрибаларнинг натижасида базали станцияларнинг жойлашув жойи асосланиши шарт.

Селектив қотиш кенг чизиғли тизимларда содир бўлади. (масалан, CDMA тармоғида). Бунда кескин содир бўлмайди, бироқ қабул қилинувчи сигналларни вақт бўйича тузилиши жойига ва символлараро интерфференцияга эга.

Симсиз алоқа тизими радиоэфирга доступ эркинлиги кучи турли хил ёмон ниятли кишиларга бегона ахборотдан саноқсиз фойдаланиш билан хабарни эгаллаш каби, абонент ва тармоқлар алдови режасида потенциал сигнали узвийдир. Шунинг учун алоқа тизими стандартлари қонуний фойдаланувчиларни ва тармоқни шундай харакатлардан ҳимоя қилишнинг турли механизимларини эътиборга оладилар. Маълумотларни шифирлаш ва аутентификацияси жараёнлари шундай механизимларга киради.

Асимметрик шифрлаш тизимларида хар бир абонент ўзаро боғланган иккита калитларга эга бўлади: очиқ ва махфий. Махфий алоқани хосил қилиш зарурияти туғилганда абонентлар химояланмаган канал бўйлаб очиқ калитлар билан алмашадилар, шундай экан, очиқ калитлар барча фойдаланувчиларга маълум бўлиши мумкин (жумладан ёвуз ниятли одамга хам). Махфий калит эса абонентларда сир сақланади. Очиқ каналлар бўйлаб махфий калитларни аниқлаш деярли мумкин эмас, чунки бунинг жуда катта маълумотлар ва вақт талаб қилинади.

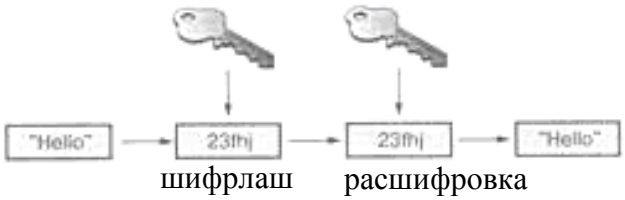
3. GSM СТАНДАРТЛИ МОБИЛ АЛОҚА ТИЗИМЛАРИДА ХАВФСИЗЛИКНИ ТАХЛИЛ ҚИЛИШ

3.1. Уяли алоқа тармоқларида хавфсизликнинг умумий принциплари

Фирибгарликдан химояланиш учун симсиз алоқа тармоқлари операторлари ва қурилма ишлаб чиқарувчилар биргаликда жуда кўп хавфсизлик чораларини амалга оширишлари зарур. Биринчи навбатда матн, овоз ёки бошқа турдаги маълумотларни бошқа форматга ўтказиш – шифрлаш принципи бўлиб, бундай маълумот тутиб олинганда хам у тушунарсиз холатда қолади.

Шифрлаш принципи жуда оддий: шифрлаш калитини текстга қўллаб, текст кодланади. Ушбу шифрланган текстни қабул қилувчи ўша калит ёрдамида уни оригинал кўринишини қайта тиклайди. 3.1-расмда шифрлашнинг асосий принциплари кўрсатилган.

Хар қандай шифрлаш тизимининг ишончлилиги унинг калитини узунлигига боғлиқ. Калит қанча узун бўлса, тизим шунчалик ишончли бўлади, зеро катта узунликдаги калитларни аниқлаш жараёнида жуда кўп вариантлар кўриб чиқилиши лозим ва бунинг учун кўп вақт талаб этилади.



3.1-расм. Шифрлашнинг асосий принципи.

Масалан, агар шифрлаш калити 0 дан 99 гача сонлар орасида бирор сондан иборат бўлса, хакер хар бир сонни калит сифатида ишлатиб кўриб, натижаларни текшириш йўли билан 100 та қиймат кўриб чиқиши мумкин. Компьютерларни ишлаш тезлиги ортиши билан шифрлаш калитларини мавжуд бўлган кобинациялардан танлаб олиш йўли билан топиш имконияти хам ўсиб бормоқда, бу усул қўпол куч ишлатиш усули дейилади.

80-йилларда 56 битли стандарт калитлар бўлиб, уларда 2та комбинация мавжуд эди. 90 йиллар охирларига келиб, бир неча ўн минглаб оддий компьютерлар тинимсиз комбинацияларни танлаши йўли билан бунда калитларни осонгина синдириш (фош этиш) мумкин эканлиги хавфсизлик экспертлар томонидан исботлаб берилди. 56-битли DES (Data Encryption Standard — маълумотларни шифрлаш стандарти) калити бундай ишлаш оқибатида тахминан бир кунда топилиши мумкин. 3.1-жадвалда берилган узунликдаги калитларни бузиш (очиш) учун тахминан қанча вақт керак бўлиши келтирилган.

Симсиз алоқа тармоқларида узун калитларни ишлатиш терминалларнинг хисоб-китоб имкониятлари камлиги туфайли муаммодир. Шунинг учун илгари GSM рақамли тизимларида қўпол куч ишлатиш усули билан топиш мумкин бўлишига қарамасдан 64 битли калитлар қўлланилган.

3.1-жадвал.

Калитни узунлигига боғлтқ равишда аниқланиш (фош этиш) вақти.

Калит узунлиги	32 бит	40 бит	56 бит	64 бит	128 бит
Калитни аниқлашга керак бўлган вақт	9 соат	12 кун	2,3 йил	58,3 йил	$10,8*10^{34}$ йил

Шифрлаш тизимларини икки категорияга ажратиш мумкин: симметрик калитли ва асимметрик калитли. Симметрик тизимлар (яна махфий калитли, ягона калитли, бир калитли тизимлар сифатида хам ммашхур) оддий ссилка асосида ишлайди: шифрлаш ва расшифровка калити битта ёки симметрик миқдор ишлатилади. Шифрланган коммуникацияларни хавфсизлаштириш учун узатувчи хам, қабул қилувчи хам битта калитга эга бўлиши керак. DES-алгоритми — симметрик калитли алгоритмга яққол мисолдир.

Симметрик тизимларда шифрлаш алгоритмлари сифатида алгоритмлар блоки ёки алгоритмлар оқими хисобланади. Биринчиси, номидан маълумки, маълумотлар блокларини шифрланган кўринишга келтиради. Бундай алгоритмлар камида 64 битли блоклар хосил қилади. Оқимли алгоритмлар маълумотнинг хар бир битини индивидуал равишда шифрланган кўринишга келтиради.

Асимметрик тизимларда шифрлаш ва расшифровка учун асимметрик калитлар ишлатилади. Асимметрик тизимлар умумий кириш имкониятли ёки шахсий калитли тизимлар сифатида хам машхур. Бу ерда шифрлаш калитларига умумий доступ берилган бўлиб, симметрик тизимларга нисбатан сезиларли афзаллик хисобланади, зеро калитларни тақсимланиш жараёнини соддалаштиради. Асимметрик алгоритмга RSA алгоритми яққол мисол бўла олади.

Умумий кириш имкониятли атамаси албатта шартли равишда ишлатилади. Хар қандай хавфсизлик тизимининг кучлилиги ихтиёрий шахсга

тизимнинг нозик томонларини билиш хуқуқини бера олишидадир. Агар жамоатчиликдан криптографик алгоритмларни сир сақланса, бу тизимга шубха уйғотиб, унинг оммабоплигини пасайишига олиб келиши мумкин. Бу фараз айниқса симсиз технологияларига мос келади, кўпдан-кўп хавфсизлик алгоритмлари глобал текширувлар оқибатида хеч қандай бузилишга учрамади, вахоланки у ерда хам оммага умуман маълум бўлмаган нозик жойлар мавжуд бўлсада.

3.1.1. Уяли алоқа тармоқларида фирибгарлик турлари

Уяли алоқада фирибгарликнинг бир неча турлари мавжуд. Энг оддийси бу телефон ўғирлашдир. Вахоланки, фойдаланувчилар телефон ўғирланганлиги хақида зудлик билан операторга маълум қилса хам хозирги кунда бу муаммо очиқлигича қолмоқда. Бу энг оддий хужумлардан бири хисобланади..

Фирибгарликнинг яна бир тури бу тармоқ хизматларига сохта хужжатлар билан уланишидир. Бундай фирибгарликни амалга ошириш осон эмас, чунки тармоқ операторларининг идентификация тизимлари жуда мураккаб тузилган. Масалан, АҚШда янги уланувчилардан шахсий гувохнома ва социал суғуртанинг рақами талаб қилинади. Бу маълумот шахснинг кредит имкониятларини текширади ва шартнома тузишдан олдин хаммаси синчклаб текширилади.

Фирибгарликнинг энг хавфли кўринишладан бири – мобил телефонни клонлаштиришдир. Бундай холатларда хакер терминалнинг электрон рақами ESN (Electronic Serial Number – электрон тартиб рақам) ни нусхалайди ва бу рақамни бошқа терминалга программалаштиради. Хар қандай сўзлашув олдидан ESN узатилади, шунинг учун агар маълумот узатилиши шифрланмаган

бўлса, хакер замонавий электрон қурилмалар орқали уни (ESNни) аниқлаб олиши мумкин.

Замонавий биллинг тизимлар йилдан йилга янгиланиб бормоқда, шу туфайли бу тизимлар битта рақамни бир нечта телефонлар ёрдамида бир вақтда ишлатилаётганини аниқлаб бера олади. Лекин, хакерлар нусха телефонларни бошқа шахар ва хатто бошқа давлатларга хам сотиб юборишлари мумкин. Роуминг хизматлари ёрдамида клонланган телефонларни аниқлаш бир қанча қийинчиликлар туғдиради.

Клонлаштириш одатда хақиқий телефон эгаси хисоб рақамидаги пул миқдори ортиқча сарфланаётганини билгандан сўнг аниқланади. Аввалига GSM тармоқларида клонлаштириш, SIM-картани клонлаштириш мураккаблиги туфайли мумкин эмас деб хисобланар эди, аммо криптографлар 90 йиллар охирига келиб GSM тармоғини бузишни ўргандилар.

Сўнги йилларда симсиз алоқа стандартлари (TIA/EIA IS-95, TIA/EIA IS-136) умумдоступли бўлганлиги туфайли клонлаштириш оддий холга айланди. Хохлаган одам уларни синчклаб ўрганиб чиқиб, тармоқни нозик жойларини топиши мумкин.

3.1.2. Фирибгарликга қарши кураш

Уяли алоқа тармоқларида рўй берадиган фирибгарликларга қарши тармоқ операторлари томонидан жиддий чоралар кўрилади. Қуйида бир нечта кенг тарқалган чоралар келтирилган:

• *шифрлаш,* ESNни нусхалашни қийинлашиши туфайли тахликни камайтиради. GSM тармоқларида ESN фақат бир марта – биринчи сўзлашув мобайнида узатилади, қолган вақтларда эса хакерлардан химоя қилиш мақсадида вақтинчалик ESN лардан фойдаланилади;

• *қора рўйхатлар*. Ўғирланган телефонларни аниқлаш мақсадида тузилади. Ягона маълумотлар базаси ўғирланган уяли телефонларни бутунжахон бўйлаб доступни чегаралаб қўйган холда ишлатиш имкониятини йўқотади.

• *трафик тахлили*. Бугунги кунда операторлар “сунъий интелект” га эга бўлган энг мураккаб дастурий таъминотлардан (ДТ) фойдаланмоқдалар ва бу ДТлар телефондан фойдаланиш жараёнида шубхали ўзгаришларни рўйхатга олади, масалан, сўзлашувларни давомийлиги кутилмаганда ортиб кетиши, халқаро сўзлашувларнинг кўпайиши. Бундай ДТлар ёмон ниятли одамни аниқлаб уни, керак бўлса, рақамини ўчириб қўяди.

Мобил алоқа бозорининг доимий равишда ўсиб бориши фирибгарлик турларини мураккаблашишига олиб келмоқда. Операторларнинг халқаро роуминг шартномаларининг ортиши ва роуминг тизими реал вақт биллинг тизимига эга эмаслиги операторларга қилинаётган қўнғироқ хақиқий эгаси томониданми ёки йўқлигини аниқлаш қийинлашиб бормоқда.

GSM тармоғи ўрнатилган мамлакатлар фирибгарликка қарши курашиш мақсадида CEIR (Central Equipment Identity Register — қурилма идентификациясининг марказий регистри) ни ташкил этдилар. Бу жуда катта маълумотлар базаси Дублин (Ирландия)да жойлашган бўлиб, дунёдаги барча GSM – телефонларни кузатади хамда ўғирланган ва клонланган телефонлар рўйхатига эга. CEIR да учта рўйхат мавжуд: “оқ”, “кулранг” ва “қора.

“Оқ рўйхат”да дунёдаги барча мобил телефонларнинг IMEI (International Mobile Equipment Identity— халқаро мобил қурилма идентификатори)лари сақланади.

“Кулранг рўйхат”, ўғирланган ёки йўқолган мобил телефонлар рўйхатини ўз ичига олади. Абонентларга қўнғироқ қилиш ман этилмаган, аммо тармоқ операторлари телефон ишлатилганлигидан бохабар бўладилар.

“Қора рўйхат”га шундай телефонларнинг IMEI лари киради, улар ё ўғирланган ёки йўқолган бўлади. Уларни ишлаши барча GSM тармоқларида блокировка қилинади.

2000 йилнинг охирида GSM-клонлаштиришнинг яна бир оддий тури пайдо бўлди. У ривожланган давлатлардан Афғонистон, Ироқ ва шиомлий Корея каби давлатларга шифрлашни чеклашга асосланган. GSM тармоқларида шифрлаш жараёни ўз-ўзидан (по умолчанию) амалга оширилмайди, шунинг учун хакер сохта базавий станция яратиши ва хақиқийсининг сигналларини ўчириб, сохта станция орқали телефонларга шифрлашни тўхтатиш сигналини юбориши мумкин.

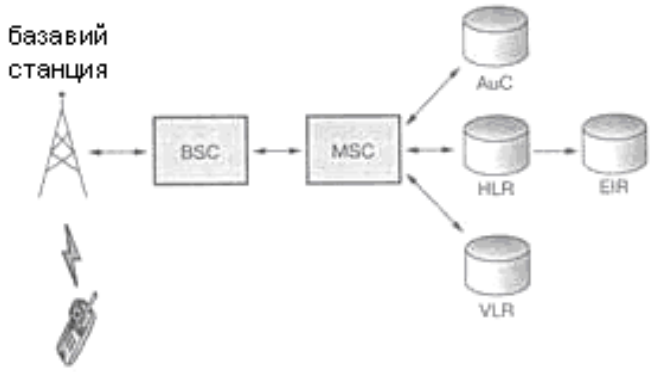
3.2. GSM да аутентификация.

3.2-расмдаги келтирилган GSM тармоғининг архитектураси саккизта асосий компонентларни ўз ичига олади:

• *SIM-картали терминаллар.* SIM-карталар — бу микропроцессорли смарткарталар бўлиб, фақат ўқиш учун 32 дан 64 Кб гача бўлган электрик дастурловчи хотирага – EEPROM (Electrically Erasable Programmable Read-Only Memory) эга. Улар GSM тармоқлари учун зарурдир. SIM-карталар икки турда бўлади: тўла ўлчамли (кредит карталар каби) ва анча кичик ўлчамли (тирноқдай). Улар хар хил муҳим маълумотларни сақланишини ва хавфсизлигини таъминлайди, масалан, эгаси хақида маълумотлар, аутентификация ва шифрлаш алгоритмлари, GSM тармоғи доступига алоқадор нарсалар;

• *базавий узатиш станциялари* **(**Base Transceiver Stations, BTS) симсиз тармоқ билан терминал ўртасидаги симсиз алоқани ташкил этади. Хар бир уяда битта базавий станция жойлашади;

• *базавий станция контроллери* (Base Station Controller, BSC) кўплаб BTS ларни бошқаради. Унинг асосий вазифаси спектрни тақсимлаш ва уни бошқаришдан иборат, шу билан бирга, фойдаланувчи бир уядан бошқасига ўтганда базавий станциялар ўртасида роумингни ташкиллаштиришдан иборат. BTS ва BSC биргаликда тизимости базавий станцияни ташкил этади (Base Station Subsystem, BSS);



3.2-расм. GSM архитектураси.

• *Мобил коммутация маркази* (Mobile Switching Center, MSC) кўплаб BSCларни бошқаради ва симли телефония билан физик боғланишни таъминлайди. MSC симли тармоқ билан симсиз тармоқ ўртасидаги қўнғироқларни ўтишини бошқаради, хамда турли BSC лар ўртасидаги уланишларни бошқаради. Фойдаланувчилар тўғрисида маълумотларни қўллаб қувватлаш ва кузатиб бориш мақсадида тўртта хар хил маълумотлар базаси ўртасидаги интерфейс сифатида хизмат қилади. Ушбу тўртта маълумотлар базаси қуйидагиларни ташкил этади: HLR (Home Location Register — ўз тармоғи доирасидаги регистрация), VLR (Visitor Location Register — мехмонлар (янги келганлар) регистри), EIR (Equipment Identity Register — қурилма идентификацияси регистри) ва AuC (Authentification Center — аутентификация маркази);

• *аутентификация маркази* (AuC) — SIM-карталар бериш маркази;

• *уй абонентлари реестри* (HLR) — маълумотлар базаси бўлиб, уланганлар хақида уланиш жойига қараб барча маълумотларни сақлайди ва кузатиб боради (масалан British Telecom абонентлари хақидаги маълумотлар British Telecom HLR сида йиғилади. Уланувчилар сонига қараб битта GSM -оператор бир нечта HLR га эга бўлиши мумкин. HLR базаси абонентлар хақидаги маълумотлардан ташқари мобил телефонларнинг IMSI (International Mobile Subscriber Identity — мобил абонентларнинг халқаро идентификацияси) ва MSISDN (Mobile Subscriber ISDN — мобил абонентлар ISDN) каби маълумотларни ўзида сақлайди. Бинобарин, HLR абонент қачон ва қаерда роумингда бўлганини кузатиб боради;

• *кўчиш реестри* (VLR) тармоқда бошқа тармоқ фойдаланувчилари хақида маълумотлар йиғади ва кузатади (масалан VLR British Telecom Англияга келган французлар хақида маълумотларга эга бўлади). VLR роуминг фойдаланувчиларга таълуқли бўлган IMSI ва MSISDN ларни ўзида сақлайди. Яна бир мухим жихат: VLR фойдаланувчиларни шундай кузатадики, агар қўнғироқ роуминг абонентига йўналтирилган бўлса тармоқ уни қаерда эканлигини “билиб туради”;

• *техник ёрдам (мадад) маркази* (Operating and Maintenance Center — OMC) бутун GSM-тармоғининг ишлашига ва уни бошқарилишига жавоб беради. OMC одатда BSC и MSC лар билан X25 тармоғи орқали боғланади.

Мобил телефондан қўнғироқ амалга оширилганда GSM-тармоғида VLR қўнғироқ қилувчининг телефонини аниқлайди ва шу ондаёқ АИС дан уланувчилар хақида маълумот олувчи HLR билан боғланади. Бу маълумот VLR га юборилади ва сўнг қуйидаги жараёнлар содир бўлади:

1. Базавий станция RAND (хажми 128 бит) номли тасодифий миқдорни генерациялайди ва уни телефонга узатади.

2. Телефон RAND ни A3 ва K_i ёрдамида расшифровкалайди. Хисоблашлар натижасида SRES (хажми 32 бит) номли имзоланган жавоб юборилади.

3. Шу билан бир вақда VLR хам SRES ни хисоблаб чиқади. Бу жуда осон, чунки VLT да K_i, RAND ва A3 ни нусхаси сақланади.

4. Телефон SRES ни базавий станцияга узатади, станция эса уни VLR га юборади.

5. VLR телефондан олинган SRES ни ўзида хисобланган SRES билан солиштиради.

6. Агар SRES лар бир хил бўлса аутентификация мувафаққиятли бўлиб, абонент тармоқдан фойдаланиш хуқуқига эга бўлади (3.3-расм).

7. Агар SRES лар қийматлари мос тушмаса, уланиш тўхтатилади ва бу хақда телефонга хабар юборилади.

3.3-расм. GSM да аутентификация.

Бу оддий жараён иккита сезиларли афзалликларга эга:

• *K_i махаллий тарзда қолади.* Зеро аутентификация калити – аутентификацияни энг муҳим компоненти экан, уни хавфсизлиги жуда хам муҳимдир. Ушбу моделда K_i хеч қачон “хаво орқали” узатилмайди, шунинг

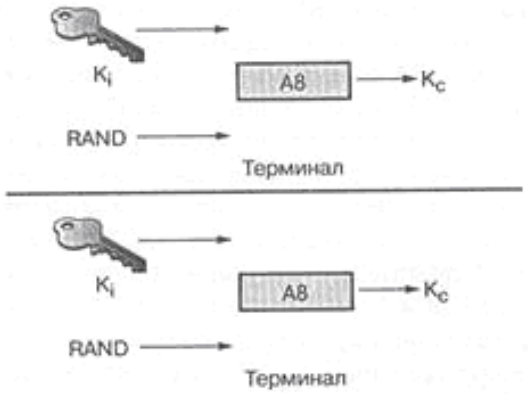
учун ушлаб олиниш хавфлардан йироқдир. K_i фақат SIM-картада ва AuC, HLR ва VLR маълумотлар базаларида сақланади.

• *тахдидларга қарши куч ишлатиш методи орқали химоя таъминланади.* 128-битли RAND 2^{128} та ёки тахминан $3{,}4x10^{38}$ та мумкин бўлган комбинацияларни ўз ичига олади. Агар хакер А3-алгоритмни билган холатда хам, хар бир берилган RAND лар учун SRES қийматларини хисоблаб чиқиш – жуда қийин масала. RAND/SRES жуфтлигини аниқлаш эхтимоллиги жуда кичикдир.

Муваффаққиятли аутентификациядан сўнг GSM-тармоғи ва телефон ўртада шифрланган рақамли канални ўрнатиш жараёнини якунлайдилар. Иккита оддий жараёнлар қилиниши керак. Биринчидан, шифрлаш калитини генерациялаш лозим. Иккинчидан, бу калит коммуникация шифровкасига қўлланилиши керак (3.4-расм):

1. SIM-карта олдиндан олинган 128 битли RAND ни олади, уни K_i билан комбинациялайди ва А8 алгоритмини қўллаган холда сессия учун 64 битли калитни хосил қилади (K_C).

2. GSM-тармоқ RANDни билгани учун ва K_i нусхасига эга бўлганлиги учун абонентни ўзлигини тасдиқлаш мақсадида худда ўша хисоблашларни такрорлайди.



3.4-расм. GSM махфийлик жараёни.

3. GSM-тармоқ ва терминал ўртасида шифрланган овозли алоқани ва маълумотлар узатишни таъминлаш мақсадида $К_С$ А5 алгоритми билан комбинацияланади.

Сессия калитлари такрорий равишда ишлатилиши мумкин – бу ўз навбатида тармоқни ишлашини яхшилайди ва потенциал кечикишларни (ушланиб қолишларни) камайтиради.

Охирги қадамда фойдаланувчи идентификацияси амалга оширилади. Оператор учун мижозлар билан реал вақтда хисоб-китобларни амалга ошириш имкониятига эга бўлиш жуда мухим. Абонент идентификацияси иккита катталик бўйича амалга оширилади: $К_i$ ва IMSI.

IMSI — уникал катталик бўлиб уни ноқонуний клонлаштиришга қўллаш мумкин, шунинг учун радиотўлқинлар орқали IMSIларни узатишни камайтиришга харакат қилиниши лозим. Шу сабабли IMSI фақатгина бир бор – янги телефон биринчи марта ишга туширилганда узатилади. Кейинги хар бир уланишлар учун TMSI (Temporary Mobile Subscriber Identity — мобил фойдаланувчининг вақтинчалик идентификацияси) қўлланилади.

TMSI аутентификация ва шифрлаш жараёнлари тугаллангандан сўнгина станцияга юборилади. Станция TMSI ни олганлиги хақида тасдиқ хабарини юборади. TMSI қайси жойда яратилган бўлса ўша ерда хақиқийдир. Региондан ташқаридаги коммуникациялар учун TMSI га қўшимча равишда LAI (Location Area Identification — жойлашиш идентификацияси) хам керак бўлади.

3.3. GSM-алгоритмлар тахлили.

Криптографик алгоритмлар GSM Хамжихатлиги меморандумига аъзо бўлган давлатлар учун махсус ишлаб чиқилган. Бу протоколларни ёки уларнинг тузилишини хеч қандай глобал криптографик обзори қилинмаган эди.

Вахоланки юқорида таъкидлаб ўтилганидек, оммавий криптографик обзорлар хар қандай хавфсизлик архитектураси учун жуда муҳим ахамиятга эга.

Афсуски, GSM уюшмаси аъзолари умумбашарий обзорларни олиб боришга харакат қилмаяптилар. Бунинг ўрнига улар махфий хавфсизлик алгоритмларини яратиш мақсадида SAGE (Security Algorithm Group of Experts — хавфсизлик алгоритми экспертлари гурухи) каби ёпиқ коммитетлар тузмоқдалар. SAGE таркибига илғор мутахасисслар киради ва бу гурух A3, A5 ва A8 каби алгоритмларни яратган. Бу жараёнларни ёпиқ холда амалга оширилиши GSM-уюшмасини барча архитектураларнинг глобал тахлилидан фойда кўришга интилмаятганлигидан далолат беради. Боз устига, GSM-алгоритмларни сир сақланиши муваффаққиятсизликка учради. Интернетга бўлган қизиқишнинг ортиши ва A-серия алгоритмлари хақидаги тортишувлар 90-йилларнинг ўрталарида маълумотларни доимий чиқиб кетишини вужудга келтирди. Тасодифан A-алгоритмларни ва GSM-архитектурасини халққа маълум қилиниши бу алгоритмларни хаваскор ва профессионал криптографлар учун нишон қилиб қўйди.

Биринчи хужум 1998 йилнинг апрелида содир бўлган бўлиб, Калифорния университетининг Берклидаги илмий ходимлари A3/A8 алгоритмини GSM-телефонларни клонлаш мумкин эканлиги каби нозик жойини аниқладилар.

Берклидаги ходимларнинг тахлиллари баъзи бир сирларнинг пардаларини очиб ташлади. A3 алгоритми 64 битли калитларни ишлатиши таъкидланишига қарамасдан, охирги 10 бит ишлатилмай, 54 битли калит сифатида қўлланилиши маълум бўлди. Модомики, бу вақтгача 56 битли калитлар куч ишлатиш методи билан паралелл равишда бир нечта хисоблашлар оқибатида аниқлаб олиниши исботланган эди. A3 нинг 54 битли калитлари эса онгли равишда бемалол аниқланиши мумкин.

Беркли тадқиқотчиларининг ёндошуви оддий эди. Аниқ бир SIM-картага аниқланган сигналлар юборилган, жавоб сигналлар эса тахлил қилинган – шу

тарзда K_i махфий калит хисоблаб чиқилган. Хужум сим карта ўқувчи GSM-телефон ва компьютер ёрдамида оддий йўл билан амалга оширилган. K_i ни аниқлаш жараёни деярли саккиз соат вақтни олган. Муваффаққиятли амалга оширилган хужум худда ўша K_i га эга бўлган SIM-картани яратишга имкон беради, бу эса ўз навбатида тармоқда бепул хар қандай хизматга эга бўлишга имкон беради.

Саноат бундай хужумларга зудлик билан чора кўрди. Шимолий Американинг саккиста катта GSM-операторларидан ташкил топган GSM-иттифоқи LLC, бир хафта ичида ушбу A3/A8-хужумига қуйидагиларни таъкидлаган холда жавоб қайтарди:

• GSM-тармоғи абонентлари учун хеч қандай хавф йўқ: бу тизимнинг ишлаши ва яратилиш жараёни аввалгидек энг юқори даражадаги симсиз алоқа хавфсизлигини таъминлайди. Ўғрилар шунчаки телефонни ўғрилаб GSM-хизматларига эга бўлишлари мумкин, алтернатив SIM-карталарни хосил қилишмайди;

• A3 алгоритмидаги бўш жойлар тасодифан эмас операторларнинг хохишлари билан қолдирилган. Бошқача қилиб айтганда, Берклида аниқлаб олинган 54 битли калит реал калит эмас (аслида у 64 битга яқин);

• олиб борилган овозни шифрлаш алгоритми A5 га қаратилмаган, бу яна бир бор шуни исботлайдики: GSM-тармоғидаги сўзлашувлар хуфёна эшитишга дучор бўлмайди (North American GSM Carriers Respond to Recent Publicizes Attacks // Business Wire, April 20, 1998 маърузага кўра).

Афсуски A5 алгоритмининг нозик жойи бир йилдан сўнг аниқланди ва бутун GSM хавфсизлигининг архитектурасини заифлигини исботлади. A3/A8 алгоритмлари авторлари Алекс Бирюков (Alex Biryukov), Ади Шамир (Adi Shamir) ва Дэвид Вагнер (David Wagner) каби криптографлар A5/1 алгоритмини қандай қилиб бузиш (очиш) мумкинлиги хақида мақолани нашр этдилар.

Бузиш учун баъзи бир тайёргарликлар зарур, аммо кейин бутун жараён оддий ШК ёрдамида амалга оширилади. Бир йил олдин сўзлашувни эшитиш мумкин эмаслигини тасдиқлаётган экспертлар, энди аксини тан олишга мажбур эдилар.

А5 нинг нозик томонини топилиши сиёсатчиларнинг криптографик методларга ўз таъсирини ўтказиши борасидаги бахс-мунозараларни вужудга келишига туртки бўлди. Брюс Шнайер таъкидлаб ўтдики, GSM структурасини мухокама қилишнинг биринчи этапида баъзи бир ғарбий европа давлатлари хавфсизлик органлари GSM-шифрлашни атайлаб соддалаштириш кераклиги масаласини ўртага ташладилар. Германия давлати ўша даврда СССР га яқин бўлганлиги туфайли янада кучлироқ криптографик химояни таклиф этди, аммо немисларнинг таклифи этиборсиз қолдирилди ва А5 алгоритмининг химояси онгли равишда сусайтирилди.

Бир қанча муваффақиятли хужумлар уюштирилгандан сўнг GSM аъзолари симсиз алоқа химояси кучсизлигидан норози фойдаланувчилар сонининг ортишига дуч келдилар. Лекин вазиятни яхшилаш албатта жуда катта молиявий харажатга тақаларди: хар қандай хавфсизлик алгоритмининг алмаштирилиши хар бир абонентнинг SIM-картасини алмаштиришга хамда тармоқни бошқа терминаллари буни қўллаб қуватлаши учун умумий қайта тузилишига олиб келарди. Операторлар учун тарозининг бир палласида – эски тизимни ишлатишни давом эттириш турса, иккинчисида - янги тизимни яратиш харажатлари турарди. Одатда операторлар архитектурани модернизациялашни кейинроққа қолдирдилар, янада сифатли алгоритмларни эса 3G тармоқларига тадбиқ этишни мақсад қилиб қўйдилар.

Аммо GSM хавфсизлигидаги нуқсонлар хам жамиятни мулкига айланиб бормоқда ва бу ўз навбатида бозорларда телефонлар учун янги шифрлаш махсулотлари пайдо бўлишига олиб келмоқда. Вахоланки, хавфсиз терминаллар харбийлар ва давлат ташкилотлари томонидан узоқ вақт мобайнида ишлатилган

бўлишига қарамай, оддий шахслар учун улар фақатгина янги асрнинг бошида маълум бўлди. 2001 йилнинг май ойида немис компанияларидан бири Siemens телефонлари асосида Top Sec GSM-терминални таклиф этди. Унга криптографик чип жойлаштирилган бўлиб, у овоз ва маълумотлар узатишда хавфсизликни ошириш учун ассиметрик ва симметрик шифрлашни амалга оширади.

Телефон ва бошқа қурилмалар иккита асосий камчиликларга эга:

• бир нуқтадан иккинчисига хавфсиз алоқани таъминлаш учун, химояланган телефон нафақат узатувчида балки қабул қилувчида хам бўлиши зарур (ёки мос равишда шифрловчи ISDN-линия ажратилади);

• баъзи бир давлатларда тижорат йўлида шифрловчи телефонларни ишлатиш қаттиқ назорат қилинади, баъзиларида эса хатто тақиқланади.

Санаб ўтилган GSM нинг криптографик протоколлари бизни кўп нарсаларга ўргатади. Биринчидан, криптографик яратмаларни махфийлаштириш – сирпанчиқ йўл эканлиги аниқ экан. У фойдаланувчиларда шубха уйғотади ва хаккерларни ўзига тортади, хамда вазиятни бошқариш янада мураккаблашади. Иккинчидан, овозли криптография максимал кенг миқёсда фойдаланувчилардан сўровни талаб қилади. Жамиятни фикрини аниқлаб, химояни ишончлилигини ошириш мумкин. Яхши томони шуки телекоммуникация саноати бўлиб ўтган хатолардан сабоқ олади.

Тармоқ операторларининг хавфсизликни таъминлашда асосий мақсадлари қандай?

• *аутентификация.* Хақиқий фойдаланувчиларгина тармоқ хизматларидан фойдаланиш хуқуқига эга эканлигига амин бўлиш зарур;

• *махфийликни сақланиши*. Сўзлашувлар (яширин тарзда) эшитиб олинмаятганлигига ишонч хосил қилиш;

• *овозли ва бошқа маълумотларни узатилишида бутунликни сақлаш*. Овозли ёки бошқа маълумотлар алоқа вақтида ушлаб олиниши мумкин

эмаслигини билиш, узатилган маълумот бутунлигига амин бўлиш зарурдир. Булар симсиз алоқа тараққиётини таъминловчи критик талаблар бўлиб, фойдаланувчилар ўзларининг электрон имзолари билан ишонч билдирадилар;

• *ишлаш қобилияти*. Бу функция хавфсизликка бевосита таълуқли эмас, аммо бутун архитектура шундай қурилиши керакки, фойдаланувчига билдирмаган холда хавфсиз транзакцияларни амалга ошириш имконияти мавжуд бўлиши зарур.

Уяли алоқа тармоқлари хавфсизлик борасида қандай тахликларга учраши мумкин?

• *птармоқнинг ва тизимларнинг ишлаш қобилияти.* Хар қандай мамлакатда уяли алоқа тармоқлари аллақачон миллий инфраструктуранинг мухим компонентларига айланган. Тармоқлар DoS (Denial of Service — хизмат кўрсатишда рад этиш) каби хужумларга қарши тура олиши ва тармоқни алохида уяларини ёки умуман ишдан чиқариш каби харакатларга қарши тура оладиган холатда бўлиши зарур;

• *физик химоя.* Тармоқ қурилмалари тармоқдан узоқда ва хавфли жойларда жойлаштирилар экан, операторлар уларни ишлашларига халақит бермасликдан ва вандализм (вайрон қилиш)дан химояланган эканига ишонч хосил қилишлари керак. Одатда битта бино ичида жойлашадиган ва тармоқлараро экран (firewall) билан химояланадиган корпоратив станциялардан фарқли ўлароқ уяли алоқа тармоғи базавий станциялари турли иқлимда ва турли об-хаво шароитида ишлашига тўғри келади. Улар хар қандай хавфни ўғриликдан тортиб – бўрондан бузилишларга таййёр туришлари зарурдир;

• *фирибгарлик.* СТармоқ операторлари телефонларни клонлаштириш ва тармоқда ўғирланган телефонлар ишлатилишига қарши чора кўришлари зарур. 90-йиллар охирларида Америкалик экспертлар бу турдаги хужумлар телекоммуникация сохасига миллиардлаб доллар зарар келтирар экан.

Телефон ва бошқа қурилмалар иккита асосий камчиликларга эга:

• бир нуқтадан иккинчисига хавфсиз алоқани таъминлаш учун, химояланган телефон нафақат узатувчида балки қабул қилувчида хам бўлиши зарур (ёки мос равишда шифрловчи ISDN-линия ажратилади);

• баъзи бир давлатларда тижорат йўлида шифрловчи телефонларни ишлатиш қаттиқ назорат қилинади, баъзиларида эса хатто тақиқланади.

Санаб ўтилган GSM нинг криптографик протоколлари бизни кўп нарсаларга ўргатади. Биринчидан, криптографик яратмаларни махфийлаштириш – нотўғри йўл эканлиги аниқ экан. У фойдаланувчиларда шубха уйғотади ва хаккерларни ўзига тортади, хамда вазиятни бошқариш янада мураккаблашади. Иккинчидан, овозли криптография максимал кенг миқёсда фойдаланувчилардан сўровнома ўтказишни талаб қилади. Жамиятни фикрини аниқлаб, химояни ишончлилигини ошириш мумкин. Яхши томони шуки телекоммуникация саноати бўлиб ўтган хатолардан сабоқ олади.

4. ХАЁТИЙ ФАОЛИЯТ ХАВФСИЗЛИГИ

Мехнатни мухофаза қилиш - бу ижтимоий, иқтисодий техника, санитар-гигиена, мехнат қонунлари ва ташкилий чора тадбирлар тизимидан иборат бўлиб, узлуксиз фаолият жараёнида инсон соғлиғига ва мехнат қобилиятини сақлашни таъминлашга қаратилган фандир.

Инсоннинг жамиятни тараққий эттириш хамда ишлаб чиқариш бошқаришда асосий куч эканлигини хисобга олиб, унинг хавфсизлигивасоғлигини сақлаш ижтимоий тараққиёт йўлидаги мухимомил хисобланади. Шунинг ишлаб чиқариш шароитини яхшилаш, ишлаб чиқаришда жарохатланиш ва касб касаллигини келиб чиқиш манбаларини йўқотиш, шунингдек иш фаолити инсон учун чарчаш толиқиш ва касалланиш манбаи бўлмасдан, қувонч ва бахт келтирувчи фаолият бўлишини таъминлашга харакат қилиш зарур.

Ўзбекистон Республикасида мехнатни мухофаза қилишнинг хуқуқий, техник ва санитария-гигиена қоидалари билан белгилаб қўйилган қонунлари

қабул қилинган ва янгидан тахрир қилинган қоидалар умумжахон талаблари даражасида ишлаб чиқилган.

4.1. Иш жойини тўғри ташкил этилиши

Иш жойи тўғри ташкил этилиши иш унумдорлигини ошириш, чарчашни олдини олиш, иш жойидаги жихозларни ва ускуналарни тўғри жойлаштиришни омиллар, рангларни тўғри танлай билишдир. Ускуналар шундай жойлашиши керакки ишчилар ортиқча харакатсиз, ўзини зўриқтирмасдан осонгина фойдаланиш.

Иш жойида мехнат шароитини яхшилаш ишларига бир қанча омиллар хисобга олган холда ташкил қилинади. Буларга ташкилий, техникавий, санитария –гигина,табиий-иқлим омиллари киради.

Ташкилий омиллар – ишнинг ташкилий этиш шакли интизом,мехнат жараёни устидан қилинадиган назоратнинг холати,мехнат мухофазаси, ишчи ходимларнинг профессионал тайёргарлик даражаси.Техник омиллар жараёнларини механизациялаш ва автоматлаштириш даражаси,бошқарувда электрон – хисоблаш техникаларини компютерларни қўллаш, химоялаш воситаларининг созлиги ва етарлиги.

Санитария-гигина омили иш жойининг санитария холатига жавоб бериш-бермаслиги эрганомик омил машина ва ускуналарни инсон билан ўзаро харакатда бўлганда машина элементларининг мос келиши. Бунда техникани тезлик параметрларига тегишли, ишчи органларидан келаётган маълумотлар хажми, иш жойининг ташкил этилиш даражаси, бошқариш органларининг қулай жойлашганлиги, оператор ўриндиғининг конструкцияси.

Психофизиологик омиллар-мехнатнинг оғирлиги ва қизғинлиги, жамоадаги психологик вазият, ишчиларнинг бир-бири билан ўзаро муносабати,

жисмоний зўриқиш, асабий-психик зўриқишлаш мехнат шароитининг инсон организмига таъсири ўрганган холда қуйидагиларни амалга ошириш керак:

-ишда бажарилаётган операциялар тез ва тез доира чегарасида ва харакатлантирувчи майдоннинг энг қулай доирасида амалга ошириш

-ишлаб чиқариш биноларида хаво мухитини текшириш;

-ишлаб чиқаришдаги метрологик омилларини аниқлаш;

-махаллий ва умумий титрашни аниқлаш;

-ишлаб чиқаришдаги шовқин даражасини аниқлаш;

-иш жойининиг ёритилганлигини аниқлаш;

-нурланганликни текшириш;

-хаво алмашувини текшириш.

Иш жойида одамни ўзоқ вақт давомида соғлигини ва иш қобилиятни сақлаб қолиш учун биринчи навбатда зарарли омилларнинг таъсирини йўқотиш ёки меъёрий даражагача камайтириш керак.

Буларга қуйидаги зарарли омиллар гурухини киритамиз.

-ишлаб чиқаришнинг холати, яъни метерологик шароитларнинг ноқулайлиги;

Технологик жараёнларга боғлиқлиги асосида хавода чанг, буғ, газларнинг кўп миқдорда тўпланиб қолиши,шовқин,титраш,радиоактив моддалар ва электромагнит спектрларнинг мавжудлиги;

-иш жараёнида баъзи мускулларнинг юқори даражада зўриқиши.

Ишлаб чиқаришдаги зарарли омилларни одамнинг иш қобилиятига хар хил таъсир этади ва уларни рухсат этилган меъёрдан ошиб кетиши, иш қобилиятига ёмон таъсир этиб касалликни келтириб чиқариши мумкин.

4.2. Электр хавфсизлик

Электр энергиядан кенг фойдаланганлиги сабабли электр ток таъсирига рўй бериши мумкин бўлган бахтсиз ходисалар ва улардан сақланиш муҳим

масалалар қаторига кириб бормоқда. Электр токи таъсирининг энг хавфли томони шундаки, бу хавфни олдини олиш имконияти йўқлигида.

Шунинг учун хам электр токи хавфига қарши ташкилий ва техник чора-тадбирлар белгилаш.Тўсиқ воситалари билан таъминлаш, ахсий ва жамоа мухофазаси тизимларини ўрганиш нихоятда мухим.

Умуман электр токи таъсири фақат биргина биологик таъсир билан чегараланиб қолмасдан, балки электр ёйи таъсири, магнит майдони таъсири ва статик электр таъсирларига бўлинади. Буларни билиш хар бир киши учун керакли ва зарурий маълумотлар жумласига киради.

Электр токидан инсон организмида термик, электролитик ва биологик таъсир кузатилади. Электр токининг термик таъсири инсон танасининг баъзи жойида куйиш, қон томирлари, нерв хужайраларининг қизиши сифатида кузатилинади. Электролитик таъсир эса, қон таркибидаги ёки хужайралар таркибидаги тузларнинг парчаланиши натижасида қоннинг физик ва кимёвий хусусиятларининг ўзгаришига олиб келадиган холат тушунилади. Бунда электр токи марказий асаб тизими ва юрак –қон тизимини кесиб ўтмасдан, тананинг баъзи бир қисмларигагина таъсир кўрсатиши мумкин.Электр токининг биологик таъсири-бу тирик организм учун хос бўлган хусусият хисобланади,бу таъсир натижасида мускулларнинг кескин қисқариши туфайли инсон организимидаги тирик хужайралар тўлқинланади, бунда асосан организмдаги биоэлектрик жараёнлар бузилади. Яъни инсон организми асосан биоэлектрик токлар орқали бошқарилади.Ташқи мухитдан юқори кучланишдаги электр токининг таъсири натижасида биотоклар режими бузилади ва оқибатда инсон организмида ток уриш холати вужудга келади. Яъни бошқарилмай қолган организмда хаёт фаолиятининг баъзи бир функциялари бажарилмай қолади: нафас олишнинг ёмонлашуви, қон айланиш тизимининг ишламай қолиши ва х.к.

Электр токидан жарохатланиш сабаблари ва асосий мухофаза воситаларини кўриб чиқадиган бўлсак.Одам асосан электр токи таъсирида электр қурилмалари ишлаётган вақтда бирор-бир сабаб натижасида электр қурилмаларни электр билан таъминлаётган электр симларнинг изоляциясининг емирилиши ёки электр қурилмаларнинг харакатга келтирилаётган ички электр ўрамларини ташкил қилган электр қурилмаси корпусига ток ўтказиб юборилиши натижасида ток уради.

Электр токи таъсирида жарохатланишнинг асосий сабаблари қуйидагилар:

1) кучланиш остида бўлган электр тоқлари ёки электр ўтказгичлари тегиб кетиш масофасига яқинлашиш;

2) электр токини ўчириб ремонт ишларини бажариш вақтида тасодифан токни ушлаб юбориш;

3) электр қурилмалари устки метал корпуслари ва қопқоқларида электр ўтказгичнинг мухофаза қобиқларининг шикастланиши натижасида электр кучланиш хосил бўлиши;

4) ер юзасига узилиб тушган электр ўтказгичи ер юзаси бўйлаб ток тарқатаётган ток потенциаллар айримасининг хосил бўлган зонага тушиб қолиши натижасида қадам кучланиши таъсирига тушиб қолиши;

5) жарохатланишнинг хавфсиз мехнат усулларини билмаслик;

6) электр қурилмаларини ўрнатиш ва улардан фойдаланишда хавфсизлик техникаси қоидаларини бузилиши;

Электр токидан жарохатланиш олдини олишга қаратилган асосий тадбирлар:

1) электр тармоқларини айрим жойлаштириш;

2) кучланиш остида бўлган ўтказгичларни қўл етмайдиган қилиб бажариш;

3) электр қурилмаларининг корпрусида электр токини хосил бўлишига қарши чоралар кўриш:

а) кам кучланишга эга бўлган электр манбаларидан фойдаланиш

б) икки қаватли мухофаза қобиқлар билан қоплашни таъминлаш

в) потенциалларини тенглаштириш

г) ерга улаб мухофазалаш

д) нол симга улаб мухофазалаш

е) мухофаза учириш қурилмалари.

4) махсус электр мухофазалаш тизимларидан (блакировка)фойдаланиш;

5) электр қурилмаларини хавфсиз ишлатиш ташкилий чора тадбирларини қўллаш;

6) ишлаб турган бутун электр жихозларни истеъмолчиларнтнг электр қурилмаларини ишлатишда риоя қилинадиган ТИҚ (техник ишлатиш қоидалари) талабларига жавоб берадиган холатда келтириш;

7) махаллий шароитдан келиб чиқиб,электр қурилмалар билан ишлаш хавфсизлигини оширадиган қўшимча тадбирлар кўриш;

8) электр асбобларни тезда алмашлаб уланишларни. Таъминлаш ишларни пасайтирилган кучланишга ўтказиш;

9) ишлатиладиган шахсий химоя воситаларини такомиллаштириш;

10) хавфсиз мехнат усулларини кўрсатиш орқали одамларнинг ўқиш сифатини яхшилаш.

Электр қурилмаларни уловчи ўтказгичларнинг мухофаза қобиқлари, ток ўчириш қурилмалари ва сақловчи қурилмалар хамда уларни ўрнатиш ва фойдаланишга маълум талаблар қўйилади.

Электр қурилмаларни ўрнатиш қоидаларига асосан икки сақловчи қурилма ўртасидаги электр тизимларидаги ёки охирги сақловчи қурилма билан хар қандай ўтказгич орасидаги мухофаза қобиғи қаршилиги 0.5 М.Ом дан кам бўлмаслиги талаб қилинади. Хавфли хоналарда бу қаршилик миқдори 20-50% ортиқ бўлиши керак. Электр қурилмасининг мухофаза қобиғи қаршилиги уни ўрнатгандан кейин ўлчаб кўрилади ва ишлатиш даврида йилига камида бир марта, хавфли хоналарда камида икки марта ўлчаб, текшириб турилади.

Электр қурилмалар билан ишлашда хонанинг нисбий намлиги 40-60% ва хаво харорати 18-20% градус ва электр токи ўтказмайдиган полга эга бўлиши керак.

4.3. Электромагнит нурланиш

Одамга ва биологик объектга ёмон таъсир бериши мумкин бўлган ташқи муҳитнинг ҳар хил факторлар орасида радио частотали нурланишшига тегишли бўлган ионсиз табиатли электромагнит майдонлар катта мураккаблигини ташкил этади. Бу ерда ташқи муҳитга ифлос факторни ташламасдан ишлаб чиқаришнинг ёпиқ цикли фойдаланилмайди, чунки радиотўлқинларнинг узоқ масофаларга тарқатиш уникал қобилияти ишлатилади. Шу сабабли нурланишни экранлаш ва таксик факторни бошқага алмаштириш мумкин эмас. Халқ ва табиатга электромагнит нурланишнинг таъсири замонавий техник ривожланиши ва телевидения ва радиоэшиттиришни кенг фойдаланилишига, радиоалоқа ва радиолокация СВЧ қурилмаларни ва технологияларни фойдаланишга жуда каттта ҳизмат кўрсатади. Лекин халққа хохламаган нурланишни камайтирувчи аниқ нурланиш канализацияларни аниқлаш ва ишлаш пайтида нур чиқарадиган қурилмаларни регламентация одамлар ЭМИ поғонанинг гигиеник масалалари катта эътиборга олинади. Америка ташқи муҳитни сақлаш агентлиги маълумотларига қараганда 1 фоиз одамлар популяциянинг 1мкВт/смдан ортиқ ЭМН таъсирига тушадилар. Буни энг катта таъсири баланд биноларда, антена тизимлари ўрнатилган жойларда аниқланган.

Энг ҳавфли майдонлар – СВЧ диапазонлардир. Сантиметр ва дециметр тўлқинлар терига таъсир қилади. Дециметр тўлқинлар 10 – 15 см чуқурликга кириб ички органларга таъсир қилади.

Афсуски, ЭМИнинг ёмон таъсири кенг масштабли нурланиш манбалар билан боғланмаган. Биз биламизки, магнит майдон электр майдонда ишлайдиган ҳар яандай қурилма орасида пайдо бўлиши мумкин. Ҳаётимизда ишлатиладиган ҳар қандай қурилма, яъни электр соатлар бўлиши мумкин.

Ҳисобга олиш кераккки, ҳамма мобил алоқалардан уяли алоқа ҳавфсиз ҳисобланади. Бу база станциялар сони етарлилиги ва абонент аппаратининг қувватини регулировка қиладиган тизимлари борлиги бўйича таъминланади. Бу ҳолатда абонент аппаратининг "экологик" асосий кўрсаткичи қувватни регулировка қиладиган тизимнинг эффектив иши бўлади, ЭМНнинг таъсирланиш даражаси эса абонентдан базали станциягача бўлган масофа бўйича аниқланади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. И.А.Каримов «Мировой финансовый экономический кризис, пути и меры по его преодолению в условиях Узбекистана».

2. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы. С-Пб.: БХВ- Санкт-Петербург, 2005.

3. Cisco Systems и др. Руководство по технологиям объединения сетей. 3-е издание. М.: Издательский дом «Вильямс», 2002.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 3-е изд. Санкт-Петербург, 2006.

5. Пескова С.А. «Сети и телекоммуникации». 3-изд. М., 2008.

6. Крухмалев В.В., Гордиенко В.Н. «Цифровые системы передачи».

7. Бабич Н.П., Жуков И.А. «Основы цифровой схемотехники». 2008.

8. Берлин А.Н. «Коммутация в системах и сетях связи». М., 2008.

9. Дианов В.Н. «Диагностика и надежность автоматических систем». 3-е изд., стер. М., 2008.

10. Бакланов И.Г. «Технологии ADSL / ADSL2 +: теория и практика применения». М., 2008.

11. Берлин А.Н. «Цифровые сотовые системы связи». М., 2008.

12. Кааранен Х. «Сети UMTS. Архитектура, мобильность, сервисы»

13. Травин Г.А. «Основы схемотехники устройств радиосвязи, радиовещания и телевидения». М., 2008.

14. Барский А. Б. «Логические нейронные сети. Учебное пособие»

15. Лапонина О.Р. «Межсетевое экранирование». М., 2008.

16. Гольдштейн А.Б. «Softswich». М., 2008.

17. Ложников П.С. «Обеспечение безопасности сетевой инфраструктуры на основе операционной системы Microsoft». Практикум

18. Семенов Ю.А. «Алгоритмы телекоммуникационных сетей. В 3 частях. Ч.1: Алгоритмы и протоколы каналов и сетей передачи данных».

19. Богданов А.В. «Архитектуры и топологии многопроцессорных вычислительных систем». Курс лекций. 2008.

20. Мелентьев О.Г. «Теоретические аспекты передачи I данных по каналам с группирующими ошибками». М., 2008.

21. Браун М., Раутани Дж. «Диагностика и поиск неисправностей электрооборудования и цепей управления». М., 2008.

22. Вегешна Шринивас. Качество обслуживания в сетях IP. : Пер. с англ. — М. : Издательский дом "Вильямс", 2003.

23. Ю.А. Семенов. «Телекоммуникационные технологии» , 2004.

24. www.cisco.com

25. www.athena.vvsu.ru/docs/tcpip/mpls/

26. www.ccc.ru/magazine/depot/01_03/0303.htm

27. www.citforum.ru/nets/semenov/

28. www.ietf.org

иловалар