ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Қуанышбек Құралай

Телекоммуникациялық жүйелердің сенімділігін арттырудың қазіргі заманғы принциптері

Дипломдық жобаға

ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
тех.ғыл.канд-ы
_____ Е.Таштай
«____» _____2019 ж.

Дипломдық жобаға

ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: Телекоммуникациялық жүйелердің сенімділігін арттырудың қазіргі заманғы принциптері

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Орындаған: Қуанышбек Құралай

Рецензия беруші
ҚазҰАУ, ЭҮжА каф.
доктор PhD.,
қауымдастырылған профессор
_____ Әлібек Н.Б.
«____» _____ 2019 ж..

Ғылыми жетекші
ЭТжҒТ каф PhD докторы,
сениор-лектор
_____ Қ.Н. Тайсариева
«___»_____2019 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
тех.ғыл.канд-ы
_____ Е.Таштай
«____» _____2019 ж.

Дипломдық жоба орындауға
ТАПСЫРМА

Білім алушы: *Қуанышбек Құралай*
Тақырыбы: *Телекоммуникациялық жүйелердің сенімділігін арттырудың қазіргі заманғы принциптері*
Университет ректорының *«16» қазан 2018 ж. №1162-б* бұйрығымен бекітілген
Аяқталған жобаны тапсыру мерзімі "____"_____ 2019 жыл.
Дипломдық жұмыста қарастырылатын мәселелер тізімі ақпараттық қауіпсіздік жүйесі, сөйлесулерді қорғау әдістері, Simulcrypt арқылы қақтығыстар туралы ақпарат
Дипломдық жұмыста қарастырылатын мәселелер тізімі:
1) Жүйенің сенімділігі, телекоммуникациялық жүйелердің сенімділігін арттырудың қазіргі заманғы принциптері
2) Simulcrypt арқылы қақтығыстар туралы ақпарат, криптографияның симметриялық шифрлау жүйесі, криптографияның асимметриялық (ашық кілт) шифрлау жүйесі
3) Беру жүйесінде регенераторлардың қорғалуын есептеу; Жабдық
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызбалық материалдар слайдпен көрсетілген
Ұсынылатын негізгі әдебиет 25 атау

дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Телекоммуникациялық жүйелердің сенімділігін арттырудың қазіргі заманғы принциптері	8.02.2019	
Сөйлесулерді қорғау әдістері	22.03.2019	
Цифрлық беріліс жүйесін кедергіден қорғаудың есебі	21.04.2019	

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа (жобаға) қойған

қолтаңбалары

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Норма бақылау	Тайсариева Қ.Н. PhD., докторы, сениор лектор		

Ғылыми жетекшісі _____ К.Н.Тайсариева

(қолы)

Тапсырманы орындауға алған білім алушы _____ Қ. Қуанышбек

Күні “___” _____ 2019 ж.

АҢДАТПА

Дипломдық жоба телекоммуникациялық жүйелерде арнайы әдістерді қолдана отырып телефонмен сөйлесу мәселелерін зерттеуге және телекоммуникациялық жүйелердің сенімділігін арттырудың қазіргі заманғы принциптеріне бағытталған.

Әртүрлі шифрлау алгоритмдерін қолданатын құрылғылар ұсынылған. Телекоммуникация желілеріндегі ақпаратты қорғауды ұйымдастыру үшін пайдаланылатын технология, тасымалдау мерзімдері мен сенімділік факторларының бағалары есептеледі.

АННОТАЦИЯ

Дипломный проект в специальных телекоммуникационных системахи фокусируется на современных принципах надежности и исследования телекоммуникационных систем.

Предлагаются устройства, использующие разные алгоритмы шифрования. Рассчитаны технология, время транспортировки и факторы надежности, используемые для организации защиты информации в телекоммуникационных сетях.

ANNOTATION

Graduation project in special telecommunication systems and focuses on modern principles of reliability and research of telecommunication systems.

Devices using different encryption algorithms are offered. The technology, time of transportation and reliability factors used to organize information security in telecommunication networks are calculated.

МАЗМҰНЫ

КІРІСПЕ

Байланыс арналарына көбінесе қолдау көрсетілмейді және осы арнаға кіру мүмкіндігі бар кез келген адам байланыса алады. Сондықтан сайттарға ақпаратты шабуылдауға болады.

Ақпаратты қорғау құралдары - мемлекеттік құпияларды құрайтын деректерді қорғаудың техникалық, криптографиялық, бағдарламалық және басқа да құралдарын, сондай-ақ ақпараттық қорғаудың тиімділігін бақылау құралдарын.

Ақпараттық қауіпсіздік жүйесі әртүрлі тәсілдермен жасалуы мүмкін және бұл екі фактор ақпараттық қауіпсіздік жүйелеріне арналған деректерді өңдеудің автоматтандырылған жүйелерінің ағымдағы жай-күйіне және ақпараттық қауіпсіздік жүйесін қорғауға жұмсалған қаражаттың көлеміне әсер етуі мүмкін.

Ақпараттық қауіпсіздік жүйелерін жобалау және дамыту мынадай тәртіппен жүргізілуі мүмкін:

- қорғаудың тізбесі мен құнын анықтау үшін деректерді өңдеу жүйесін талдау;
- ықтимал қылмыскерлердің үлгісін таңдау;
- болжамды қылмыскердің таңдалған үлгісіне сәйкес ақпаратқа қол жеткізудің заңсыз арналарының максималды санын іздеу;
- қолданылатын әр қорғаныш жабдығының күші мен ұзақ мерзімділігі;
- орталықтандырылған басқару және басқару құралдарын дамыту;
- Ақпараттық қауіпсіздік жүйелерінің сапасын бағалау [1].

1 Ақпараттық қауіпсіздік жүйесі

1.1 Қорғаныс жүйесін құру кезеңдері

Қауіпсіздік жүйесін құру тұжырымдамасы, мысалы, кез-келген басқа бағдарламаның тұжырымдамасы келесі мәселелерді шешуді талап етеді: ақпараттық қауіпсіздік саласындағы практикалық әзірлемелердің маңыздылығы, қауіпсіздік жүйесінің негізгі кезеңдері және қауіпсіздік проблемаларын шешудің әр түрлі жолдарын салыстырмалы талдау.

Қорғаныс жүйесінің негізгі кезеңдері келесідей жіктеледі (1.1-сурет):

Сурет 1.1- Қорғаныс дамыту жүйесінің сатылары

1. Потенциалды тәуекелдерді талдау келесі негізгі қауіп-қатерлерге бағытталады:

- ақпараттың құпиялылығына қауіп төндіреді;
- ақпараттың тұтастығын бұзу қаупі.

Бұл фаза қауіп-қатер жиынтығынан шынымен елеулі зиянды бағдарламалар (вирустар, ұрлықтар) таңдауымен аяқталады.

2. Қорғауды жоспарлау кезеңінде қорғалатын құрылымдардың тізімі және олар үшін ықтимал қауіптер бар. Қорғаудың келесі бағыттары қарастырылуы керек:

- заңды және этикалық;
- моральдық және этикалық;
- қорғауды қамтамасыз ету жөніндегі әкімшілік шаралар;
- аппараттық және бағдарламалық қамтамасыз етуді қорғау шаралары.

3. Қауіпсіздік жүйесі ақпаратты өңдеудің жоспарланған ережелерін іске асыру үшін қажетті құралдарды орнатуды және конфигурациялауды қамтамасыз етеді.

4. Қорғаныс жүйесінің қызмет ету мерзімі жүйенің жұмысын қадағалаумен, оқиғалар туралы жазумен, кемшіліктерден қорғауды анықтаумен және қорғау қажеттілігін түзетумен сипатталады.

Аппараттық мүмкіндіктерді пайдалану келесі мүмкіндіктерді ұсынады:

- TRD-800, ол естуден және бейнеден қорғайды

радио қабылдағыштар мен магнитофондар;

- Бейнебақылау бөлімшелері ғасыры;
- ақпараттың дұрыстығын растайтын ақпараттық схемалар;

Құпия құжаттарды жіберу үшін SAFE-400-ден шифрланған факс хабарламалары. Қорларды қорғау әдістері қарқынды. Бағдарламалау әдістері есептік алгоритмдерді және қол жеткізуді шектеуді қамтамасыз ететін бағдарламалар мен ақпаратты рұқсатсыз пайдалануды болдырмайды. Бағдарламалау әдістері келесі функцияларды орындайды:

- сәйкестендіру, түпнұсқаландыру, авторизация (PIN-код, пароль

сөздерді пайдалану);

- резервтік көшіру және қалпына келтіру процедуралары;

антивирустық бағдарламаларды белсенді пайдалану және антивирустық ресурстардың жиі жаңаруы;

- мәмілені өңдеу.

Ақпаратты криптографиялық қорғау криптографиялық кілтсіз және кері айналымсыз қол жеткізуге болмайтын ақпаратты шифрлау, кодтау немесе басқаша өзгертудің арнайы тәсілі болып табылады. Криптографиялық қорғау ең сенімді әдіс болып табылады, себебі ақпарат өзі тікелей қол жетімді емес (мысалы, шифрланған файлды оқуға болмайды).

Бұл қорғаныс әдісі стандартты операциялар немесе бағдарламалық пакеттер түрінде болады. Операциялық жүйеге қарай қорғану құралдарын басқаруды басқару жүйесімен толықтыруға болады, бұл қол жеткізуді бақылау рәсімдеріне мүмкіндік береді.

Қазіргі уақытта ақпараттық қауіпсіздіктің криптографиялық классификациясы жоқ. Дегенмен, сіз жіберген хабардың әр функциясы шартты түрде 4 негізгі топқа кодталады:

- шифр мәтінін ауыстыру белгіленген немесе ұқсас алфавит таңбасымен ауыстырылады;

- аналитикалық трансформациядағы шифр мәтіні кез-келген аналитикалық ережеге бағынады;

- Шифрланған мәтін таңбаларының орналасуы осы мәтін блогындағы кез келген ереже арқылы кодталады.

Шифрлау дәрежесі үшін көптеген бағдарламалық өнімдер бар. Ең танымал бағдарламалардың бірі - Зиммерман жасаған Pretty Good Privacy (PGP). Бұл криптографиялық қорғау үшін қуатты құрал. Оның танымалдығы мен шығарылымы бүкіл әлем бойынша PGP стандартына айналды. PGP желісінде желіге кіру мүмкіндігі бар [2].

1.2 Ақпараттық қауіпсіздік

Ақпараттық қауіпсіздік - мемлекеттік ақпараттық ресурстардың, сондай-ақ жеке және жеке тұлғалардың қоғамдық мүдделер саласындағы құқықтарын қорғау жағдайы.

Ақпараттық қауіпсіздік - ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар жиынтығы. Ақпаратты қорғау әдістері деректердің тұтастығын, енгізілуін, сақталуын, өңделуін және шығарылуын, сондай-ақ қажет болған жағдайда құпиялылықты қамтамасыз ету үшін қолданылады. Осылайша, ақпаратты қорғау - ағып кетудің, ұрланудың, жоғалудың, рұқсатсыз жоюдың, өзгертудің, өзгертудің, рұқсатсыз көшірудің, бұғаттаудың алдын алу жөніндегі шаралар жиынтығы. Ол қауіпсіздікке қатысты шектеулерді қорғауға арналған ұйымдастыру, бағдарламалық қамсыздандыру, аппараттық құралдар мен құралдарды қамтиды.

Ақпараттық қауіпсіздікті құру - қиын міндет. Оны шешу үшін заңнамалық, ұйымдастырушылық, бағдарламалық және техникалық шаралар қажет.

Ақпараттық қауіпсіздіктің үш маңызды аспектісін атап өту маңызды: қолжетімділік (оптимизм), тұтастық және құпиялылық.

Қол жетімді (оптимистік) - ақылға қонымды уақыт ішінде қажетті ақпараттық қызметтерді алу мүмкіндігі. Ақпаратқа, ақпаратқа, технологияға және өңдеу технологиясына қолжетімді ақпаратқа қол жетімділік (белгісіз).

Адалдық - бұзушылықтар мен заңсыз өзгерістерден қорғау. Ақпараттың тұтастығы - компьютерде немесе автоматтандырылған жүйеде кездейсоқ ақпарат немесе ақау (немесе ақпарат) арқылы жіберілген ақпараттың бұл ақпараттың өзгермеуін қамтамасыз ететіндігін білдіреді. Құпиялылық - заңсыз қол жеткізуден немесе оқытудан қорғау.

1983 жылы АҚШ Қорғаныс министрлігі сарғыш жабынды компьютерлік жүйелердің сенімділігін бағалау критерийін шығарды.

Қауіпсіз жүйе - белгілі бір адамдарға немесе процестерге ақпаратты оқуға, жазуға, жасауға және жоюға мүмкіндік беретін ақпаратқа қол жеткізуді басқаратын жүйе.

Сенімді жүйе - әр түрлі құпиялылық тәжірибелері туралы ақпаратқа қол жеткізу құқығын бұзбай бір уақытта пайдаланушылар топтарын өңдеу үшін жеткілікті ақпарат пен бағдарламалық қамтамасыз етуді пайдаланатын жүйе.

Жүйенің сенімділігі (немесе сенімділігі дәрежесі) екі негізгі параметрмен бағаланады: қауіпсіздік саясаты және кепілдік.

Ақпараттық қауіпсіздік саясаты Қауіпсіздік саясаты ұйымдағы ақпаратты өңдеуді, қорғауды және таратуды реттейтін заңдар, ережелер мен мінез-құлық кодекстерінің жиынтығы болып табылады. Бұл ережелер пайдаланушы нақты деректер жиынын өңдей алатындығын көрсетеді. Қауіпсіздік саясатын қорғаныстың белсенді бөлігі ретінде қарастыруға болады, ол ықтимал қатерлер мен қарсы шараларды қамтиды.

Қауіпсіздік саясаты кем дегенде мынадай элементтерді қамтуы тиіс: ерікті қол жеткізуді бақылау, сайт қауіпсіздігі, қауіпсіздік белгілері және ымыраға.

Кепілдік жүйесінің өнімділігі мен жұмыс істеуі үшін сенім деңгейі көрсетіледі. Бұл қауіпсіздік саясатын іске асыруға жауапты тетіктердің дұрыстығын көрсетеді. Бұл әрекетті адвокаттың әрекетсіздігі ретінде сипаттауға болады. Кепілдіктің екі түрі бар: операциялық және технологиялық. Біріншісі - сәулет және жүйені енгізу, екіншісі - жинау және техникалық қызмет көрсету әдістеріне қатысты.

Есеп берушілік (немесе есеп берушілік) маңызды қауіпсіздік құралы болып табылады. Сенімді жүйе барлық қауіпсіздік оқиғаларын тіркеуі керек, ал хаттамаларды тексеру (аудит журналы деректерін талдау) толықтырылады.

Сенімді база (SSE) - бұл компьютерлік қауіпсіздік саясатын іске асыруға жауапты қорғаныс рөлдерінің жиынтығы. Компьютерлік жүйенің сенімділігін бағалау үшін оның есептеу базасын ғана қарастыруға болады. ЭБЖЖ-нің негізгі мақсаты - қол жеткізуді бақылау міндетін жүзеге асыру, яғни объектілер бойынша белгілі бір операциялардың орындалуын қадағалау.

Енгізу мониторы - пайдаланушыны бағдарламалық жасақтаманың немесе деректер әрекеттерінің әрбір ықтимал тізіміне тексеретін монитор. Access Monitor үш функцияны қажет етеді:

- Біз өмір сүрдік. Монитор жұмыс кезінде зақымданудан қорғалуы тиіс;
- толықтығы. Монитор сіз оны әр кезде оған қол жеткізгенде қоңырау шалады. Қазіргі уақытта оны жылжыту мүмкін емес;
- Рационалды түрде. Мониторды бақылауға және тексеруге мүмкіндік беру үшін ол ықшам болуы керек.

Қауіпсіздік рөлі - қол жеткізуді бақылау мониторы. Қауіпсіздік ядросы барлық қорғаныс механизмдерінің негізі болып табылады. Бұл логикалық мүмкіндіктерге қосымша, қауіпсіздік механизмі оның тұтастығын қамтамасыз етуі керек.

Қауіпсіздік периметрі - сенімді шот базасының шекарасы. Ол сенімді, бірақ сенімсіз. Сыртқы және ішкі әлем арасындағы байланыс көлеңкелерден тұрады. Магнит - антивирустық немесе шабуылға қарсылас деп саналады [3].

Объектінің ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жұмыс бірнеше кезеңге бөлінеді: дайындық кезеңі, түгендеу, тәуекелдерді талдау, қорғаныс жоспарын жүзеге асыру. Осы кезеңдер аяқталғаннан кейін операция кезеңі басталады.

Дайындық кезеңі: осы кезең барлық іс-әрекеттердің ұйымдастырушылық негізін қалыптастыру, түпкілікті құжаттарды әзірлеу және бекіту, сондай-ақ процеске қатысушыларды анықтау үшін қажет. Дайындық кезеңінде ақпараттық қауіпсіздік жүйесінің ақпараттық міндеттері анықталды.

Ақпараттық ресурстардың түгендеуі. Бұл кезеңде объект сервердің автоматтандырылған ақпараттық ағындарының құрылымы туралы ақпаратты жинайды және хабарламаларды өңдеу, деректерді өңдеу және сақтау әдістерін қамтиды. Зияндылық қорды анықтағаннан кейін талданды.

Тәуекелдерді талдау. Келесі оқиғалардың нәтижелері ақпараттық ресурстардың толықтығы мен дәлдігіне байланысты болады. Тәуекелдерді талдау мыналарды қамтиды: аналитикалық объектілерді таңдау және талдау; тәуекелдерді бағалау әдіснамасын таңдау; қатерлер мен олардың салдарларын талдау; тәуекелді бағалау; қауіпсіздік талдауы; қызметтің жекелеген түрлерін жүзеге асыру және тексеру; қалдық тәуекелді бағалау.

Қауіпті болу қаупі бар. Тәуекелдерді талдау кезеңі тәуекелдерді талдаудың негізгі элементі болып табылады. Тәуекелдерді болдырмау үшін шаралар мен құралдар қажет. Тәуекелдерді талдау, ең алдымен, ықтимал тәуекелдерді (оларды анықтау), ал екіншіден, болашақ болжамдарды болжауға арналған. Іске асырудың нәтижесі сайтқа қауіп-қатерлерді жіктеу болып табылады.

Олардың барлығы ақпараттық қауіпсіздікті қамтамасыз ету жүйесіне қойылатын талаптарды анықтауға, ең тиімді шаралар мен құқықтық қорғау құралдарын анықтауға мүмкіндік береді, сондай-ақ оларды жүзеге асыру шығындарын анықтайды.

Қорғаныс жоспарын құру. Осы кезеңде талдаудан бұрын анықталған тәуекелдерді бейтараптандыру үшін тиісті институционалдық және техникалық сақтық шараларын таңдау қажет.

Қорғау жоспарын құру ақпараттық қауіпсіздік жүйесінің дамуының функционалдық схемасынан басталады. Ол қауіпсіздік жүйесінің міндеттерін анықтайды және объектінің ерекшеліктерін ескере отырып, жүйелік талаптарды талқылайды. Жоспарға келесі құжаттар кіреді: қауіпсіздік саясаты, ақпараттық қауіпсіздік құралдарының орналасуы, қорғаныс жүйесінің жұмысы үшін шығын сметасы, ақпараттық және техникалық қорғауды ұйымдастыру бойынша күнтізбелік жоспар.

Қорғаныс жоспарын іске асыру. Бұл кезеңде жабдықтарды монтаждау және іске қосу, қажетті құжаттар әзірлеу және т.б. жеткізушілермен келісімдер талап етіледі. Мұндай шаралар қабылдануы тиіс.

Қауіпсіздік саясатының негізгі элементтері. Қауіпсіздік саясаты (ұйым тұрғысынан) реттеу және қол жеткізу үшін қаражаттың, сондай-ақ қауіпсіздік бұзушылықтардың алдын алу және оларға жауап берудің тәртібін анықтайды.

Қауіпсіздік саясатының тұжырымдамасын келесі қадамдар ретінде қарастыруға болады.

Ұйымдастыру мәселелерін шешу. Бұл кезеңде ақпараттық қауіпсіздік қызметі ақпараттық қауіпсіздікті, пайдаланушылар санаттарын, жауапкершілік деңгейін, барлық пайдаланушы санаттарының құқықтары мен міндеттерін қамтамасыз етуге арналған.

Тәуекелдерді талдау King Analyze қорғауды, қорғауды және қорғауды анықтайды. Мүмкін болатын барлық қатерлер зиян келтіруі мүмкін екенін есте ұстаған жөн. Қорғалған қаржылық қорғау құны қорғалған объектінің құнынан аспауы тиіс.

Жеңілдік анықтамасы. Ресурстарды пайдалану құқықтары, ресурстарды пайдалану ережелері, әкімшілік артықшылықтар, пайдаланушылардың құқықтары мен міндеттері, жүйелік әкімшілердің құқықтары мен міндеттері, жасырын ақпаратпен жұмыс істеу және тағы басқалар.

Қауіпсіздік саясатының реакциясын анықтау Қауіпсіздік бұзушылықтарды анықтауға және анықтауға, сондай-ақ белгілі әдістерді қалпына келтіруге және бұзушылықтардың салдарын жоюға бағытталған шаралар.

Ұйымдастыру-әкімшілік құжаттарды дайындау. Қауіпсіздік саясаты бойынша нұсқаулар түрлі нұсқаулықтармен, нұсқаулармен, ережелермен және ережелермен реттеледі.

Қауіпсіздік саясаты ақпараттық қауіпсіздік жүйесіндегі қиындықтарға қарсы тұруға бағытталған құқықтық нормалар жиынтығын, ұйымдық (құқықтық) шараларды, бағдарламалық және аппараттық шешімдерді анықтайды.

Ақпараттық қауіпсіздікті қолжетімділікті тиісті ұйымдастыру шаралары арқылы ғана жүзеге асыруға болады. Ұйымдастыру шараларының кешені ақпараттық қауіпсіздік шараларын жасау, дамыту және қолдау, ұйымдастырушылық және әкімшілік құжаттар жүйесін жасау, сондай-ақ қауіпсіздік жүйесін құру және қолдау үшін ұйымдастырушылық, ұйымдастырушылық және техникалық шаралар кешенін қамтиды.

Ұйымдастыру, ұйымдастырушылық және техникалық шаралар ақпараттың жаңа арналарын жылдам анықтауға, оларды бейтараптандыруға, қауіпсіздік жүйелерін толықтай жақсартуға және қауіпсіздік бұзушылықтарды дереу жоюға мүмкіндік береді. Тестілеу - қауіпсіздік саясатының дамуындағы маңызды қадам.

Қазіргі уақытта ақпараттық қауіпсіздіктің көптеген түрлері бар, олар қымбат және әр түрлі сапалы мақсаттарға ие. Ең қиын мәселелердің бірі - олардың арасындағы таңдау.

Қауіпсіздік саясаты келесі элементтерден тұрады: ерікті қол жеткізуді бақылау, қауіпсіздік, қалпына келтіру, қауіпсіздікті таңбалау және компромисс.

Ерікті қатынауды бақылау - қол жеткізуді шектеу негізінде адамның немесе топтың субъектісін қамтиды. Ерікті басқару - белгілі бір тұлға (әдетте

объектінің иесі) өз қалауы бойынша басқаларға тең қол жеткізу туралы шешім қабылдауы мүмкін.

Ағымдағы қолжетімділік мәртебесі ерікті бақылау кезінде матрица түрінде көрсетіледі. Объектілер мен матрицалар арасындағы қатынастарды орнату құқығы (оқу, жазу, орындау және т.б.) - бағандарда кіші бағдарламалар бар.

Көптеген операциялық жүйелер мен дерекқорды басқару жүйелері бұл ерікті бақылауды жүзеге асырады. Оның басты артықшылығы - икемділік, ал негізгі кемшіліктер - орталықтандырылған тестілеудің күрделілігін және күрделілігін, сондай-ақ деректерге қол жеткізу құқығын (құпия ақпаратты дұрыс пайдаланбау жалпы файлдарға жүктеледі) [4].

Қауіпсіздік объектілерін қалпына келтіру. Бұл тармақ құпия ақпаратқа маңызды қосымша болып табылады, жасырын түрде әдейі немесе қасақана ашылуды бақылайды. Жадты пайдалану, сыртқы сақтауды қайтару және кіріс / шығыс кәдеге жарату. Қайта пайдалану үшін үш ықтимал қауіп бар.

Қорғау әдістерінің бірі - ЖЖҚ қашықтан тазалау немесе құпия ақпаратты өңдеу. Ең жақсы тәсілі - қысу бағдарламаларын пайдалану.

Мысалы, принтердің жадында құжаттардың бірнеше бетін сақтауға болады. Олар тіпті процестің аяқталғанын есіне алады. Сондықтан оларды жеке пайдалану үшін арнайы шаралар қабылдау қажет. Әдетте үш кездейсоқ ретпен азуға жеткілікті.

Біз қайта пайдаланудан қорғауымыз керек. Пайдаланушы ұйымнан шыққанда, ол жүйеге кіруді қабылдамауы және барлық нысандарға кіруге тыйым салу керек.

Қауіпсіздік белгішесі. Объектілер мен нысандар қауіпсіздік аймағымен әрекеттескен кезде өзара әрекеттеседі. Элементтің сипаты оны дұрыс емес деп сипаттайды. Нысан жапсырмасы нысандағы ақпарат деңгейін көрсетеді.

Қауіпсіздік логотипі екі бөлікке бөлінеді: құпиялылық және санат.

Құпиялылық деңгейі басқаша болуы мүмкін және әртүрлі жүйелердің құпиялылық дәрежесінен өзгеше болуы мүмкін. Қазақстан Республикасының заңнамасына сәйкес мемлекеттік құпиялардың ашылуы үш сипаттаманы анықтап, келесі номинациялар бойынша келесі құпиялылық белгілерін анықтады: «өте маңызды», «өте құпия», «құпия» және «құпия»

Бөлімдер белгіленбеген жиын болып табылады. Олардың міндеті - облыс тақырыбын деректерге қатысты сипаттау.

Қауіпсіздік тұтастығын қамтамасыз ету - осыған байланысты негізгі проблемалардың бірі. Біріншіден, нысандар мен нысандар көрсетілмеуі керек. Әйтпесе, қауіпсіздік панелі (пайдаланған кезде) тесіктері бар, бұл жағдайда ол қорғалуы мүмкін ақпаратты бүлдіруі мүмкін. Екіншіден, қорғаныс белгілері көрінбейтін болып қалуы керек.

Қауіпсіздік функцияларының қауіпсіздігін қамтамасыз ету бойынша қауіпсіздік шараларының бірі құрылғылардың көп деңгейлі және бір деңгейлі құрылғыларға бөлінуі болып табылады. Көп жақты құрылғылар

құпиялылықтың әртүрлі деңгейлерінде сақталады және сол құрылғы деңгейінде құпиялылық туралы бір ғана ақпарат деңгейіне ие болуы мүмкін.

Міндетті ымыралы реттеу. Қол жеткізуді бақылаудың себебі міндетті болып табылады - қарым-қатынас мүмкіндігі субъектінің субъектісіне байланысты емес. Бұл басқару объектілер мен объектілердің объектілерін салыстыру негізінде құрылады.

Пәннің құпиялылығы субъектінің құпиялылығынан аз болады және барлық қауіпсіздік элементтері объектінің эмблемасы болған жағдайда (яғни, осындай екі шарт орындалды) объектінің кез келген ақпаратын оқиды. Мысалы, «өте құпия» пәні «өте құпия» және «құпия» файлдарды оқи алады. Бұл жағдайда «тақырып қауіпсіздігі белгішесі нысанның қауіпсіздік белгісінен асып түседі» [5].

1.3 Қазіргі әлемдегі ақпараттың рөлі

Қазіргі әлемдегі ақпараттың рөлі артып келеді. Бізге белгілі барлық процестер материалдық және материалдық емес қоспалардан тұрады. Ең алдымен, белгілі бір көлемдегі өндіріс үшін қажетті құралдарды, материалдарды және энергияны қажет етеді. (ол не істейді және не істейді). Екіншіден, өндіріс технологиясы (қалай жасалады). Жердің өндірістік қуатының жалпы сипатын ескере отырып, әрбір оқырман кез-келген аймақтағы ұзақ мерзімді өсуде ақпараттық компоненттің (сондай-ақ, бағалардың) рөлін көре алады.

Өткен ғасырда көптеген филиалдар пайда болды. Соның ішінде 100% тек бір ақпарат: мысалы, дизайн, бағдарламалық жасақтама әзірлеу, жарнама және тағы басқалар. XX ғасырдағы өндірістік шпиондық бағдарламалардың пайда болуы өндірістегі ақпараттың рөлін анық көрсетеді: бұл материалдық құндылық емес, ең таза ақпарат.

Өткен ғасырда адамдар өндіріс процесін еске түсіріп, құрал-саймандар мен материалды өңдеу машиналарын қолданды. XX ғасырда машинаның басымдылықтарының бірі - деректерді өңдеу машинасы.

Бұл үрдістер XXI ғасыр ақпараттың ғасыры болатынын, материалдық жағы екінші орында болатындығын дәлелдейді. Сондықтан біз осы тұжырымға келдік.

Қорғалған құн Ақпараттың бағасы мен көлемі өсіп, оның құны өседі.

Бір жағынан, ақпараттық ағын. Яғни ақпарат немесе ұрлық мүлікке зақым келтіруі мүмкін. Ақпарат, екінші жағынан, оның бақылауы болып табылады. Рұқсатсыз бақылау жүргізіледі. Мысалы, қазіргі заманғы әскери ғылымға сәйкес, байланыс құралдарының бәрін жою армияның құлдырауына әкеледі.

Ақпараттық қауіпсіздік - бұл басқа адамдарға қол жетімді ақпарат және көшіру мүмкін емес.

Екінші тапсырма бірінші тапсырмамен байланысты болмауы мүмкін, бірақ олай емес. Бірінші жағдайда ақпараттың иесі қол жеткізуге тыйым салуға тырысуы мүмкін, ал екінші жағдайда ол ақпаратты оқуға рұқсат етіледі, бірақ оны өзгерту мүмкін емес. Алдыңғы бөлімдерде біз осы мәселелер бір бағытта шешілгенін көрдік.

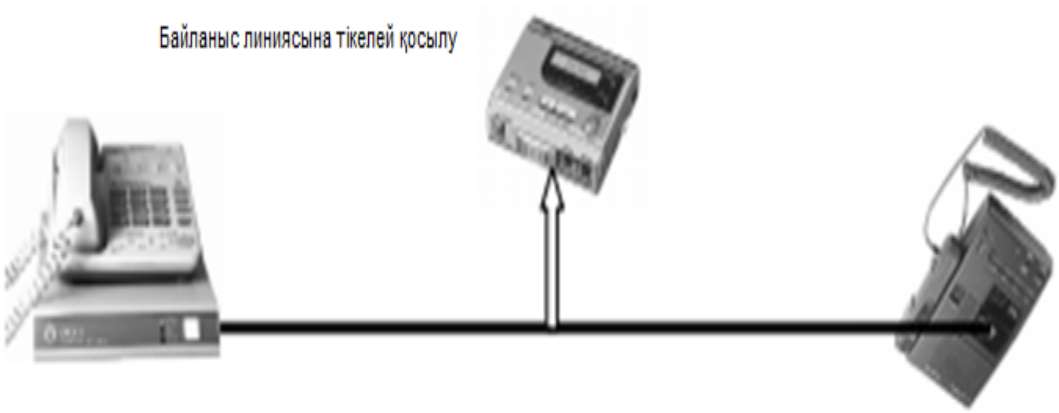
Қорғау аспектілері. Ең алдымен, ақпараттың сапасы қымбат. Нашар сапалы қорғауды қамтамасыз етудің қажеті жоқ, немесе барлық ақпарат белгілі болса, барлық ақпарат жоғалады. Сондықтан ақпараттық қауіпсіздік мәселелерімен айналысқан кезде бірінші сұрақтың маңыздылығын білу маңызды. Ақпаратты қорғау құны оның құнынан аспауы керек.

Екіншіден, ақпаратты қорғау үшін не істеп жатқанымызды анықтау маңызды, өйткені әлемді барлық салдардан қорғау мүмкін емес, мысалы, Интернетті қорғау талап етілуі мүмкін. Немесе хакерлер сіздің ақпаратыңызға риза болуы мүмкін, бұл жағдайда сіз өзіңізді жұмыс істейтін адамдардан қорғауыңыз керек немесе сіз ақпарат жоғалтуыңыз мүмкін, әйтпесе, басқа біреу қол жетімді болады, бірақ бұл ақпарат проблемалы болуы мүмкін. Үш жағдайда үш айқын айырмашылық бар.

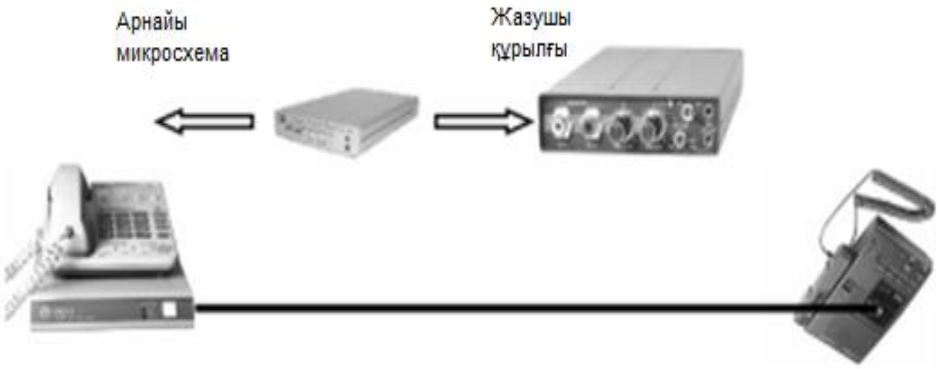
Үшіншіден, ақпараттық қауіпсіздік схемаларын жоспарлауда объективті сенімділікке ие болу ғана емес, сонымен қатар басқа адамдардың құқықтарын қорғау және кейбір жағдайларда ақпаратты қорғау үшін маңызды. Адамдар). Бұл жағдайда сертификат кейін талқыланады және талқыланады [6].

1.4 Ақпараттың негізгі түрлері

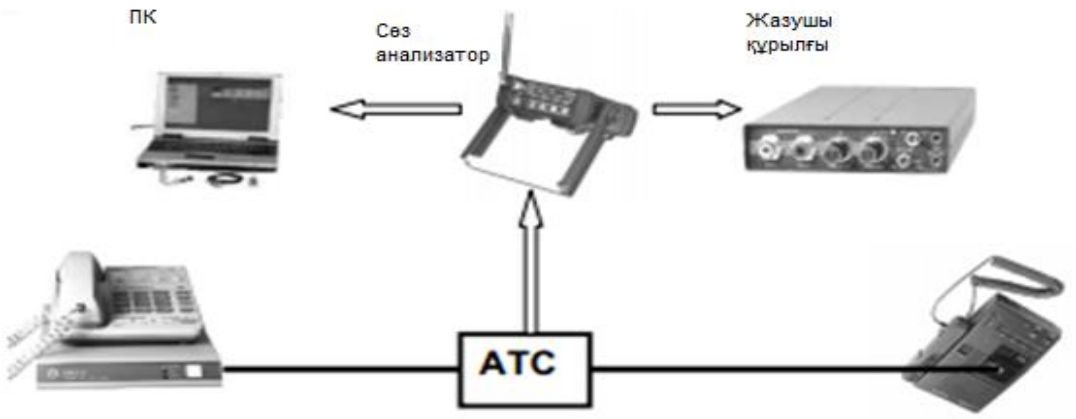
Қазіргі уақытта ақпаратты рұқсатсыз кіруден қорғау маңызды. Оны қалай қорғау керектігін білу маңызды. Байланыс желілері - магистральдық (кабельдік, микротолқынды, спутниктік және т.б.), физикалық және байланыс желілері мен магистральдық (халықаралық және қалааралық) жолдарды қоса алғанда, жол және кабельдік құрылғылар. Төмендегі суретте желінің қол жетімділігі көрсетіледі.



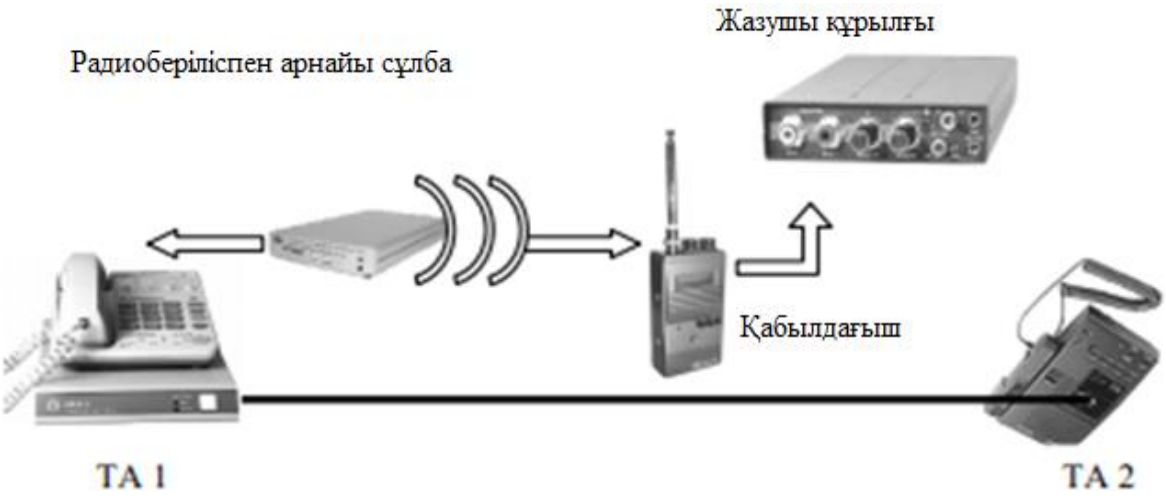
Сурет 1.2– Байланыс желісіне тікелей қосылу схемасы



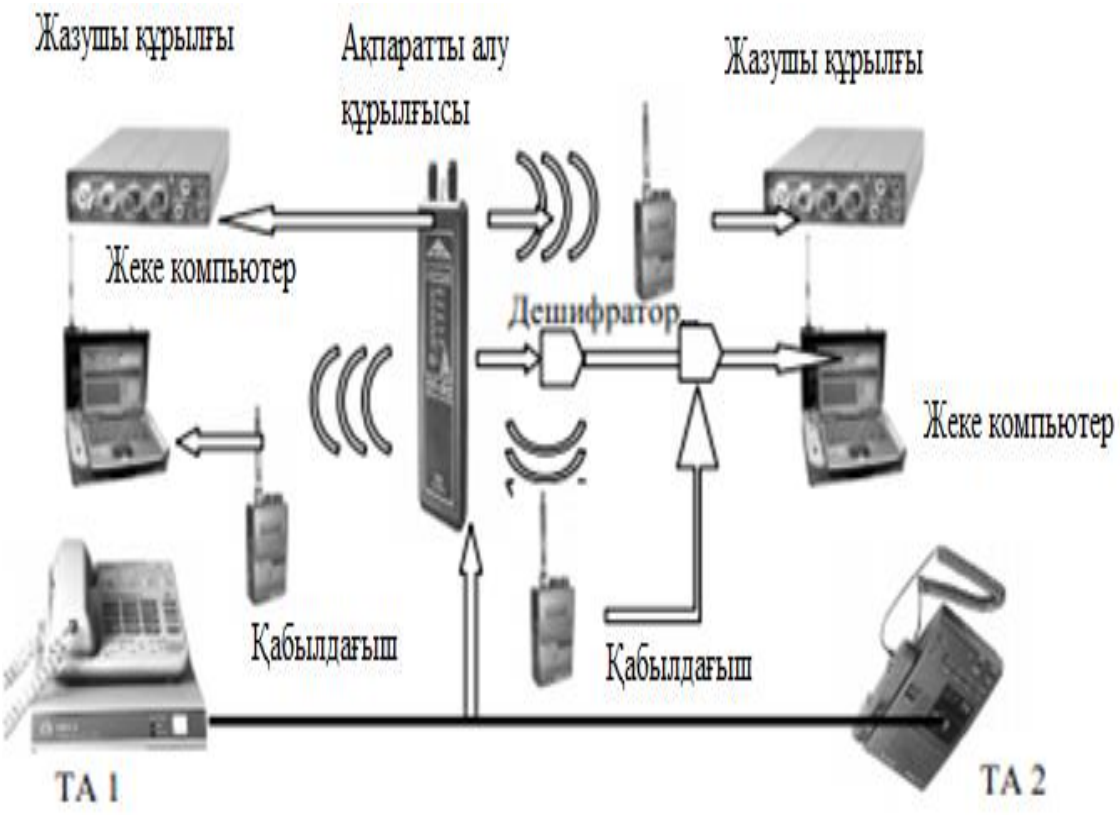
Сурет 1.3 –Арнайы микросхемалар арқылы қосылу



Сурет 1.4 - Сөз анализаторы арқылы телефондық желісіне қосылу әдісінің көрінісі



Сурет 1.5 –Радио арналарды қолдану арқылы ақпаратты алу сұлбасы



Сурет 1.6 - Радиоарналар арқылы телефондық желісіне қосылу әдістері

Ақпаратты қорғау жүйесінің негізі - қауіпті және оның деңгейін білу. Деректерді беру енді қысқа толқын, ультракүлгін толқындар, ғарыштық байланыс арналары, кабель, вулкан және оптикалық байланыс желілерін қамтиды. Байланыс арнасының түріне байланысты техникалық арналарды 3-ке бөлу қажет: электромагниттік, электрлік және жылтыр.

Электромагниттік канал туралы ақпарат алу. Электрмагниттік ереуіл таратқышы шығаратын жоғары жиілікті ақпараттық сигнал ауадан естіліп, ауруханаға жіберіледі. Бұл арна телефонды тыңдау үшін, сондай-ақ радио, ұялы немесе спутниктік байланыс үшін кеңінен қолданылады.

Электр арна туралы ақпарат алу. Кәбіл желісі арқылы қуат көзінен ақпарат алу смартфон кабель қосылымына қосылғандығын білдіреді. Ең оңай жолы - байланыс желісіне параллель байланыс. Бұл техниканың болмауы кернеудің төмендеуіне байланысты байланыс желісіндегі өзгерістер туралы ақпаратты алуға мүмкіндік береді. Бұған жол бермеу үшін құрылғыны кернеуді тұрақтандыруға жол бермеуге болады. Соңғы жағдайда, зерттеу құрылғысы мен кернеуді басқару құрылғысы, өз кезегінде, байланыс желісіне қосылған, бұл адамдарға ақпарат алуға қиындық тудырады. Кабельдік ақпарат жиі төмен жиілікті коаксиалды кабельден алынады. Жоғары қысымды ауа цилиндрлері Арнайы дабылдарды жасау үшін қысымды төмендеткіштерді пайдаланыңыз.

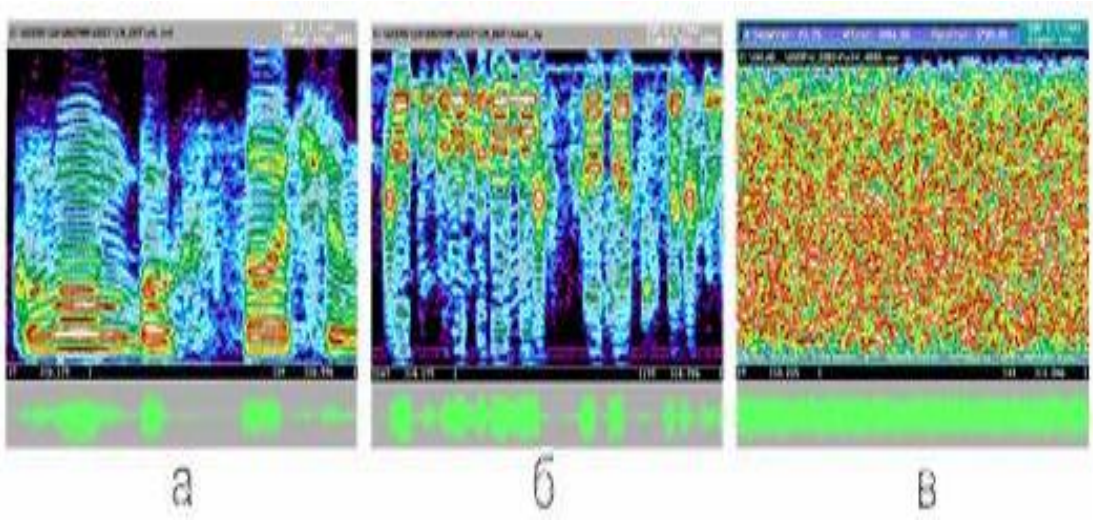
Индукциялық арна арқылы ақпарат алу. Сигналдық құрылғының тұтастығын бақылағанда, оның қарсылығын және реактивтілігін құрылғы қосулы кезде анықталады. Сондықтан арнайы қызметтер осы әдісті жиі

пайдаланады және байланыс арнасына қосылудың қажеті жоқ. Бұл арнадағы байланыс кабелінің айналасындағы электромагниттік ағынның индукциялық сенсор арқылы ақпараттық электр сигналдарын беру үшін пайдаланылады. Индуктивті сенсорлар негізінен теңдестірілген жоғары жиілікті кабельдерден ақпарат алу үшін қолданылады. Заманауи индукторлар оқшаулаудан оқшауланбайды, соның ішінде пакеттегі екі болат кабельден ақпаратты алу мүмкіндігі. Арнайы магниттік антенналары бар төменжиілікті күшейткіштер ақпарат алу үшін жасалған телефон желілеріне қол жеткізу үшін қолданылады [7].

Телефоныңызды қорғаңыз. Кез келген қорғау әдісін таңдамас бұрын, біз кімнің бірінші кезекте екенін және қандай қару мен қарудың қарулы екенін білуіміз керек.

Таспалы құрылғыда немесе радио станцияға ауыса отырып, ақпаратты арнаның арнасына тікелей қосуға болады. Мұның бәрі белгілі бір шығындарды талап етеді, сондықтан қорғау әдісін таңдаудан бұрын хакердің әлеуетін қарастырыңыз. Абоненттерді санкцияланбаған ұрлау бақыланбайды және оларды елемеуге болмайды, сондықтан белгілі бір құрылғыларды пайдаланбастан телефон қоңырауларын толығымен алып тастау мүмкін емес. Бұл құрылғылар акустикалық сигналдарды қосу принципі бойынша жұмыс істейді және олар телефонның пішінін біледі немесе оны қалай қолдайтынын біледі. Барлық желілер қауіпсіз түрде өзгертіліп, абонентке жеткен кезде танылған түрге ауыстырылады. Бұл жағдайда қоңыраулардың түрлері тиімсіз, себебі келіссөз жүргізуді қалайтын әрбір абонент осы құрылғыны сатып алу керек. Бұл құрылғылар ережелерге сәйкес жұмыс істейді. Келіссөздерде арнадан немесе сандық модем қосылымы арқылы сигнал сигналын қорғаудың екі жолы бар. Ережеге сай, бірінші әдіс сөздіктегі өзгерістердің динамикасын анықтау үшін кодтауды қолданады, ал екіншісі арнадан сандық ағындарды қорғау үшін кодтауды пайдаланады. Қорғаныс әдістерімен анықталған кезде аналогтық сигнал беру құрылғысы уақытша тұрақтылық класына жатады және сандық сигнал таратқышы кепілдік тұрақтылық класы деп аталады.

Уақытты тұрақтандырудан қорғау үшін сигналдық сөздің жиілігін өзгертетін барлық сигналдар мен маска сөздері іске қосылады. Оның декодтауы шифрланған түрдегі сигналдың автоматты және жартылай автоматты түрде қалпына келуіне негізделген криптографиялық сигналдың ұзақ мерзімді түзетілуіне негізделген. 1.7 - 1.8-сурет шығу және кодталған аудио сигналдарды (уақытша жиіліктер) көрсетеді. 1.8-суретте кілт сөздерді шифрлау кішкентай ұяшыққа ұқсайды және ешкім бұл ақаулыққа кепілдік бере алмайды.



а – шығыс сөздік сигнал;б – скремблерден кейінгі сөздік сигнал;в – цифрлық түрде бергендегі сөздік сигнал (протокол V.34)

Сурет 1.7 - Сонограммалау түрлері

Сандық таратқыш ретінде пайдаланылатын лексика да вокодер деп аталады. Дауыстық кодектер үшін ағылшын тілі. Қажетті ақпарат саны 64 Кбит / с, сондықтан қажетті аудио линзаның мазмұны 2400-9600 Кбит / с дейін азаяды және стандартты телефон желісі арқылы арнаның жылдамдығына сәйкес келеді. Арнада шу бар, ал декодер тұрақты үйлестірушіні пайдаланғанда тұрақтылықты қамтамасыз етеді.

Қорғау тобының негізгі сипаттамаларының бірі ауысымнан кейін сөйлеу сапасы. Шифрланған сөздердің сапасы байланыс арнасындағы өзгерістердің күрделілігіне және сипаттамаларына байланысты. Егер кодек жақсы канал болса, ақпараттың сапасы 90% құрайды. Егер бес балдық шкала бағаланса, жылжу 3-тен 4,5-ке дейін болады. Егер арна жаман болса, шифрланғаннан кейін дереу жіберілетін ақпараттың сапасы дереу болады.

Криптографияның тарихы 4 400 жылға жуық. Криптографияға арналған негізгі критерий ретінде пайдаланылатын шифрлау әдістерінің технологиялық сипаттамасын пайдалануға болады.

Бірінші кезең (б.э.д. үшінші ғасыр) қазірдің өзінде бір жақты каллиграфистермен сипатталады (бас әріптер басқа әріптермен немесе басқа алфавитен алынған символдармен алмастырылады, түпнұсқа алфавитін ауыстырады). Екінші кезең - 20 ғасырдың басында Леонард Альберт Батистистің 19-шы ғасырдан бастап 10-шы ғасырдың басына дейінгі полипропилен және кейбір біліктер деп аталатын электромеханикалық құрылғылардың хронологиялық тәртібі.

Төртінші кезең - 1920-ші жылдардың ортасынан бастап 1970-жылдарға дейін - математикалық криптографияға көшу. Shannon қатаң ақпараттың, ақпараттық көлемнің, энтропияның және шифрлаудың қатаң математикалық анықтамаларына ие. Міндетті шифрлау қадамы әр түрлі шабуылдарды

тексереді.) Сызықтық және дифференциалды криптоталдандыруға олардың осалдығы. Алайда 1975 жылға дейін криптография «классикалық» немесе криптографиялық криптография болды.

Криптографияны дамытудың қазіргі кезеңі (1970-ші жылдардың аяғынан бастап) криптографиялық криптографияның пайда болуымен және дамуымен сипатталады. Ол жаңа техникалық мүмкіндіктері ғана емес, криптографияны салыстырмалы түрде пайдалану үшін де қолданылады. Түрлі елдерде құқықтық криптографияның барлық мүмкіндіктері бар. Финалдық криптография математика және информатика бойынша ғылыми көзқарас қалыптастырады - осы саладағы жұмыстар ғылыми журналдарда жарияланады, жүйелі конференциялар ұйымдастырылады. Криптографияны іс жүзінде қолдану заманауи қоғам өмірінің ажырамас бөлігі болып табылады - электрондық коммерция, электронды құжат айналымы (сандық жазуды қоса алғанда), телекоммуникация және басқа салаларда [8].

Сөздің сапасы трансляция арнасының жылдамдығын қысу үшін қолданылатын сөзге және алгоритмге байланысты. 4800 және 9600 бит / с-ға негізделген аналитикалық алгоритмдер негізінде алгоритмдерді қолданғанда, сапа сөздің сапасына сәйкес келеді.2400 бит / с-ге жуық жалпы болжамдарға негізделген алгоритмдерді қолданғанда, қосымша LPC-10 қозғау сигналы 86% құрайды. 3,5 ұпай. Сандық хабар тарату негізі - байланыс арнасы арқылы берілетін сигналдың сапасы, модемдік кедергіге байланысты. Сонымен қатар, жоғары абоненттік желіде жоғары сапалы дауыстық жүйені пайдалану кезінде сөйлеу сапасы жоғары, оның ішінде әдеттегі телефон жүйесі.

Қолданбалы қауіпсіздік құралдарының көптеген ерекшеліктеріне қарамастан, таңдау қандай ақпаратты таңдауға және қандай ақпарат ақпараттарды қорғауға тиімді екеніне негізделуі керек. Бірақ келесі ереже бар: қорғаныс құны қорғалатын ақпарат көлемінен аспауы керек.

Құрылғыларды және телефон қоңырауларын қорғаудың қазіргі заманғы тәсілдері хакерлік немесе ұрлықтың көптеген түрлерін жасай алады. Жалпы алғанда, мұндай жағдайларға қарсы тұрудың екі жолы бар:

- Бейтараптандырғышты, сүзгіні және физикалық арна ақауларын іздейтін физикалық ақпаратты қорғау;

- Құпия ақпаратты қорғау (криптографиялық жағдайда).

Көптеген жариялаушылардың сымды телефондарына қарсылығы. Сөздік сигналында кедергі жоқ және оның номиналды деңгейі бірнеше есе жоғары. Елеулі кедергі телефон желісіне және жалғанған құрылғыларға зақым келтіруі мүмкін. (дыбыс ауқымында шуыл бар, сөзді өшіру қиын). Телекоммуникация желісінде абоненттің телефонындағы кіріс сигналының жоғары пассивті сүзілуіне байланысты шу жоқ.

Шуылмен салыстырғанда, бейтараптандырушы телефон желісіндегі рұқсат етілмеген құрылғыларға қайтарымсыз және қайтарымсыз өзгерістер жасайды. Бұл құрылғылардың жұмысы қарапайым: телефон желісінде рұқсат етілмеген кернеуге кедергі келтіретін жоғары жиілікті кернеудің қысқа тұйықталуы (шамамен 1500 вольт). Басқа құрылғылар сөзді өзгерту қағидаты

бойынша жұмыс істейді және негізінен телефон немесе сүйікті ретінде пайдаланылады.

Телефонмен сөйлесуді тыңдау үшін көптеген электронды құрылғылар ақпарат алу үшін, телефон желісіне рұқсатсыз қосылу: тұрақты (бір сым бұзылған) және параллельді (екі сымдар) немесе индукциялық сенсорларды пайдаланады.

Алынған ақпарат магнит жолағы, ЖЖҚ жазылады немесе радио арқылы қабылдағышқа жіберіледі. Ол телефонда ғана белсенді.

Телефон желісі ұсынатын ақпарат семантикалық және жігерлі. Энергия деңгейіндегі ақпараттық қауіпсіздікті болсақ, мұнда шу бар, сондықтан ақпарат толық түсінілмейді.

2 Сөйлесулерді қорғау әдістері

2.1 Скремблерлер

Шифрлаушы кодталған сөздерді кодтауға арналған құрылғы болып табылады. Бұл мобильді телефондарда қолданылатын криптография туралы емес, нақты қорғау туралы. Scrambler телефоны қосылған немесе өшірілген кезде жұмыс істейді. Бірақ ол шифрланған кезде микрофоннан сигналдарды шифрлап, шифрлайды, содан кейін оны шығысқа жібереді. Word түрлендіру Антенна сигналдары кодтаушыға жіберіліп, динамикке жіберіледі.

Жұмыс принципі. Кездейсоқ биттерді жасайды (шифрлау және дескремблер үшін). Айналдырылған екілік модульде кездейсоқ битке кодера қосылады. Содан кейін бит шығысқа шығады, кодтаушы келесі кірісті алады, кіріс ретімен алады және операцияны қайталайды. Сол сияқты, бөлу кезінде ол екі жақты кері кері байланыс тізілімінен және екі «оқшауланған» немесе «енгізу» элементтерінен тұрады. Кері түрлендіру кері тәртіпте орын алады. Кездейсоқ тізбек циклдік түрде қолданылады. Шифрлау көптеген сандық байланыс жүйелерінде қолданылады.

Scramble - шифрлаудың жеке түрі. Бұғатталған шифрлау алгоритмі пайда болғаннан кейін, шифрлау мәні екінші орында тұр. Скремблердің негізгі міндеттерінің бірі кинетикалық сипаттамамен қатар дәйектілікті дәйектілікпен беру [10].

Шифрлаушының артықшылығы: телефон қоңырауын қорғау байланыс желісінің барлық бөліктерінде жүзеге асырылады, яғни. Ақпарат тек келісімшарттардан телефон арқылы беріледі. Бұл қашықтық қашықтықты шектейді, яғни көп емес.

Жаудың кемшіліктері - екі құрылғыға бірдей болу қажеттілігі. Бұл құрылғы көбіне визиткалары бар адамдармен қолданылады.

Скремблердің басты ерекшелігі - жоғары сапалы қорғау. Қазіргі заманғы құрылғылар барлық талаптарды қанағаттандыру үшін криптографиялық алгоритмдерді пайдаланады. Бұдан басқа, браузерлер ұялы телефондардың барлық түрлерін тыңдаудан қорғалуы мүмкін, оның ішінде операторға орнатылған арнайы құрылғылардан қорғау мүмкіндігі. Өкінішке орай, бұл технологияның кейбір кемшіліктері бар. Негізгі жетіспеушілігі - бұл құрылғыны қауіпсіз үйлестіруді қажет ететін құрылғы. Егер біз осы салада жұмыс істейтін компаниялардың санын қарастырсақ, онда оларда құрылғы болады деп келіседі. Себебі екі жағынан бірдей алгоритмді қолданатын құрылғы қажет. Әрине, бұл талап шифрлау құрылғысын дамытуға кедергі келтіретін бір немесе екі түрлендіруге байланысты құрылғыны қажет етпейді. Міне, сондықтан Scrambler негізінен адамдарға қарап немесе үнемі қарап отырған адамдарға арналған.

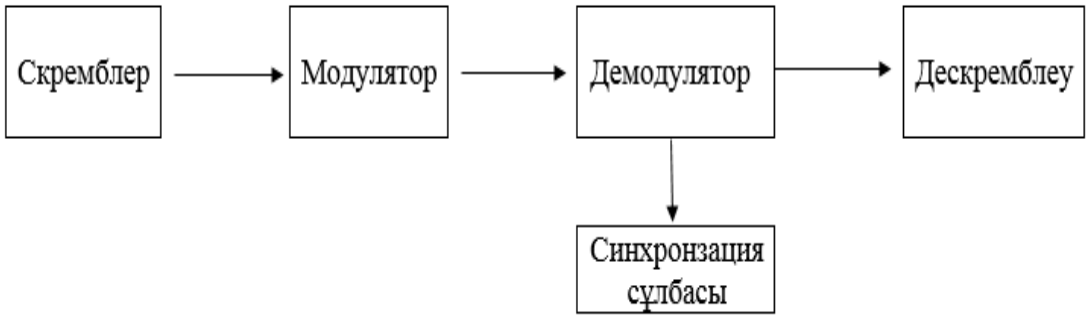
Қазіргі уақытта ұялы телефондарда қанша шприц сатылады? Егер біз оны дұрыс қарастыратын болсақ, онда бағаны анықтауға болады. Оның бағасы

ақпараттық қауіпсіздік құрылғысының сенімділігіне байланысты. Ең арзан құрылғыларда арнайы құрылғылардың көмегімен жарылуы мүмкін оңтайлы кодтау алгоритмі қолданылады. Бұған қоса, оны жасаған адамдар алгоритмді және олардың сипаттамаларын пайдаланбайды. Басқаша айтқанда, сөйлесулеріңіз маңызды емес болса, белгілі бір қызметтерді тыңдамасаңыз, келесі шифрлау пайдалы болуы мүмкін.

Құрылғының сенімділігі неғұрлым жоғары болса, екіншісі алгоритмді пайдаланады. Алайда, егер біреу ақпарат немесе сұхбат маңызды деп есептесе, сіз ағымдағы шифрлау алгоритміне назар аударуыңыз керек.

Scrambler - арна шифрлау утилитасы. Скремблер - бұл цифрлық ағынның жылдамдығын өзгертпей, қайта құрулардың кездейсоқ реті. Шифрланғаннан кейін «1» және «0» сандары сәйкес келеді. Шаблинг - бұл шығыс хабар алгоритмін пайдаланып қалпына келтіруге болатын қалпына келтіру процесі. Акустикалық сигнал келесі параметрлерге сәйкес амплитудасы, жиілігі және уақыты бойынша шифрлау процесінде өзгеруі мүмкін. Ұялы радио жүйесінде жиілік пен уақыт өзгерді. Радиоқабылдағыштың кедергісі акустикалық сигналдың амплитудасын қалпына келтіруді қиындатады, сондықтан амплитудадағы өзгерістер өзгермейді.

Сигналды беру сигналдың статистикалық қасиеттерін жақсарту үшін байланыс жүйесінде қолданылады. Шифрлау модуляция алдында цифрлық өңдеудің соңғы сатысында орындалады (2.1 суретті қараңыз) [11].

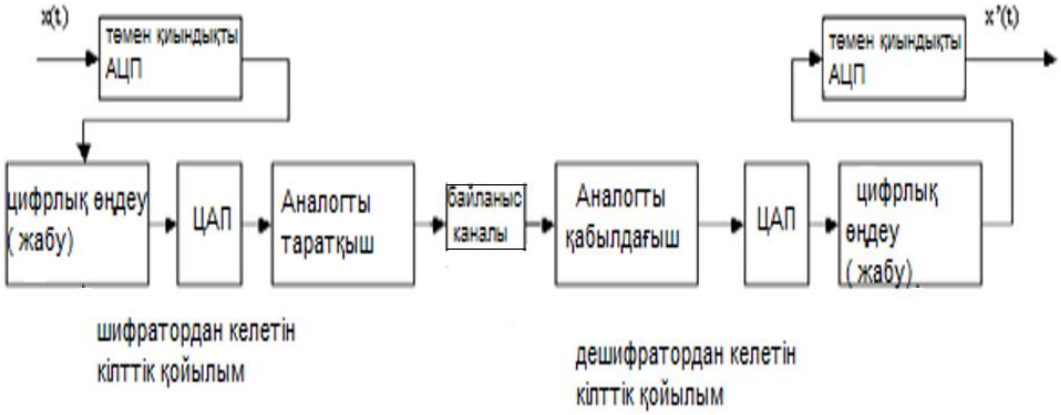


Сурет 2.1 - Сызғышты және дескремберді байланыс арнасына қосу схемасы

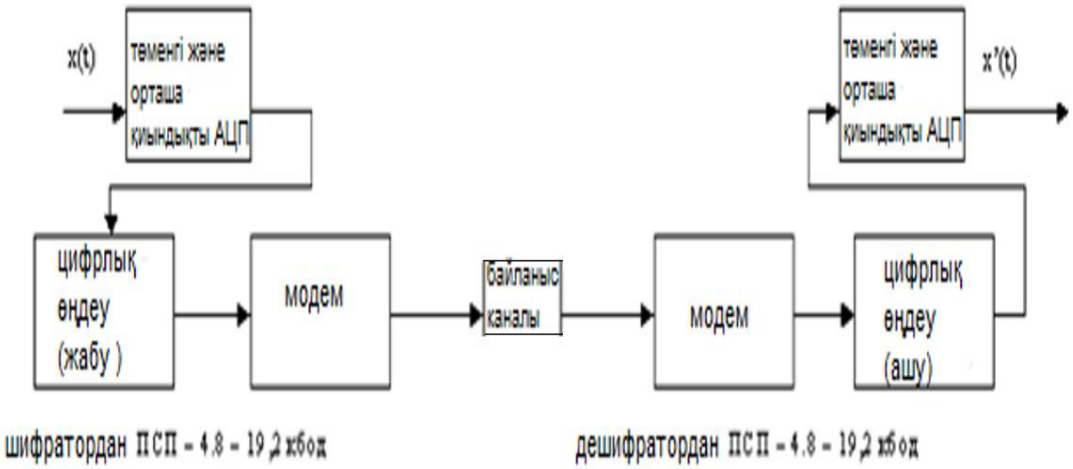
Аналогтық шифрлау. Аналогтық кодердің көмегімен қазіргі кездегі сөздік сигналдары жабылған деген қорытындыға келді. Екіншіден, бұл құрылғы 3 кГц стандартты телефон желісін, үшіншіден, декодталған сөздің коммерциялық сапасын және төртіншіден, жоғары сапалы қамтуды қамтамасыз етеді. Аналогты кодтаушы:

- сөйлемдерді жиі немесе уақытша ауыстыруға негізделген қарапайым сценарийлер;

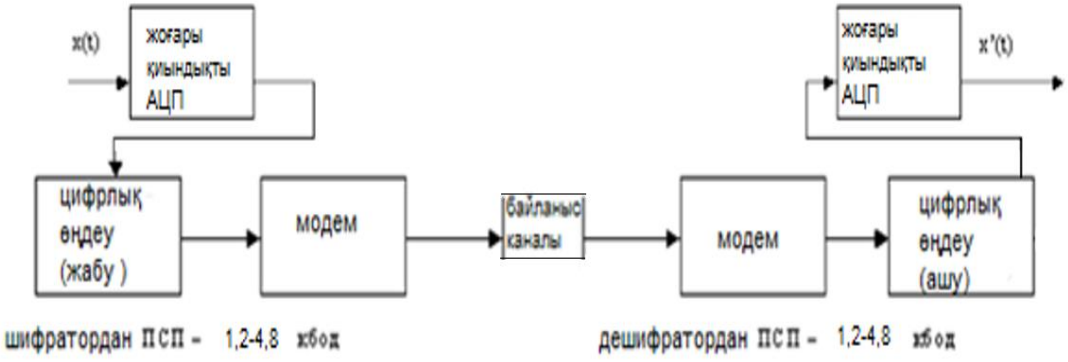
Аралас сөздік кодегі (2.2 сурет) жартылай немесе уақытты ауыстыру негізінде цифрлық сигналдарды өңдеу арқылы нақты уақыт есептерінде ішінара жинақталады.



Сурет 2.2- Жиілік немесе уақытты өзгертуге негізделген қарапайым шифрлаушы сценарийлері



Сурет 2.3 - Сөзді жасырудағы цифрлық жүйе



Сурет 2.4 - Сөздік хаттамаларды жасыру жүйесінің түрлері

ADC / CAS - аналогты - сандық / сандық - ұқсас өзгерістер.

Жүйе C немесе D шығу сигналының бөлігі болуы мүмкін (2.4 сур.). Компоненттер сандық ағындармен кодталады, бұл бір криптографиялық алгоритмі бар бір ядролы қалыптастыруға әкеледі, бұл хаттама протоколына кері байланыс арна арқылы модем арқылы жүргізіледі. Алушы ашық хаттаманы алу үшін қайтарады. Біріктірілген Wide-Roll Socket технологиясы delta модуляциясын тануға қабілетті. Жалғыз дискретті тіл кең жолақты, әдетте 4,8-19,2 кГц және секундына 2400 бит болады. Мұндай жағдайларда D-жүйесі ең күрделі жұмыс үшін пайдаланылады, ал көптеген жағдайларда күрделі сөздік қорын қолдану арқылы алгоритм құру қиын. Кодтау - жоғары сапалы фильм, бірақ бұл әдіс тар арналарды алдын алады. Жаңа, аса күрделі дискретті кодектер сенімділік сапасына қосылды [12].

Аналогты кодтаушының амплитудасы сағат пен уақытты 12 түрлі комбинацияда ауыстырады. Шифрланған сигнал сигнал немесе шығу арқылы байланыс арнасы арқылы беріледі. Автокөлік аумағында бір немесе бірнеше аналогтар қолданылады.

а) қателер саласында қатаң шифрлау:

- инверсия жиілігі (жергілікті осциллятор немесе сүзгіні өзгерту спектрі);

- кері және кері тәртіп (фракцияның басымдығына теріс әсері), көлденең қиманың ені мен ені;

с) уақыт белдеуі бойымен сырғытыңыз (уақытша сегменттер немесе сегменттелген сегменттер);

с) кодтау кезінде уақытша және жиілік кедергісі.

Барлық таңдалған уақыт немесе жиілік аймақтарында олар сөздердің, сегменттердің немесе сөз бөлімдерінің ережелеріне, яғни бір хаттамаға шифрлау кілтін өзгерту ережесіне сәйкес кездейсоқ тәртіпте сұрыпталады. Ресивердегі байланыс арнасындағы сандық сигнал декодталған және аналогқа айналды. Бұл әдіске негізделген әдіс өте күрделі, өйткені сапалы сөйлеу сигналы жоғары жылдамдықты аналогтық кіріс сигналын қажет етеді, сондықтан жоғары жылдамдықтағы ақпарат байланыс арнасы арқылы беріледі. 2400 дейін кең жолақты өткізу қабілеті кең жолақты деп аталады, егер таратылатын хабарлардың жалпы саны 2400 болса, бұл принцип дискреттік құрылғыларды шифрлау арқылы бұзылуы мүмкін. Оның күрделілігіне қарамастан, құрылғы коммерциялық нарықта ұсынылады, олардың көпшілігі 2.4 - 19.2 кбит / с модуляция жылдамдығын және тұрақты телефондармен салыстырғанда бірнеше сәтсіз сөздерді бере алады. Шифрлаудың және цифрлаудың негізгі артықшылықтарының бірі байланыс ақпаратының қорғалуын қамтамасыз ететін жоғары деңгейдегі сөздерді және әдістерді басу үшін криптографиялық әдістерді пайдалану болып табылады.

Бірінші дүниежүзілік соғыс кезінде әзірленген технологияның сөздігі. Бұл аймақтағы жетістіктердің бірі - цифрлық сигналдарды өңдеу үшін интегралды схемаларды және процессорларды және микропроцессорларды пайдалану. Осының бәрі құрылғыны жабудың көлемін және құнының төмендеуіне әкелді. Сандық аналогты сигналды сандық сигналды сөз сигналына немесе оның қондырғыларына беру үшін көптеген әрекеттерден аулақ болды және сөз

қорғауының жоғары деңгейіне жетті. Аналогтық сигналдардың шифрланған нұсқалары арнайы құрылғыларды (мысалы, модемдерді) пайдаланбай, қарапайым коммерциялық арнада шығарылатын шығыс сигналымен бірдей жиілікте болады. Сондықтан, шифрлау құрылғысы салыстырмалы түрде қымбат емес және төмендегі цифрлық шифрлауды қолданатын іріктеу құрылғысын пайдалануда ерекше қиындықтар жоқ. Аналогтық код жұмыс режиміне байланысты екі класқа бөлінеді:

1. Кодтау схемасы ауызша презентация кезінде өзгермейтін статикалық жүйе;

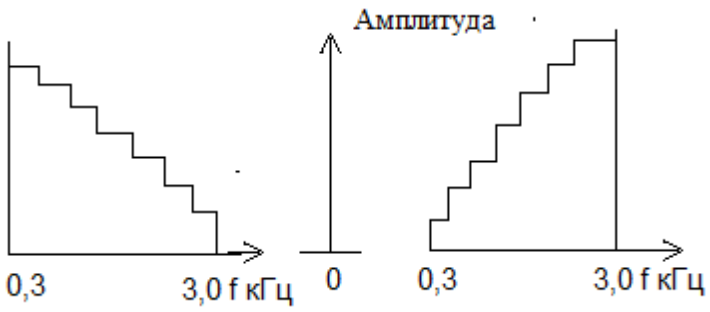
2. Трансмиссия кезінде кодты үздіксіз шығаратын динамикалық жүйе (тасымалдау кезінде бір секундта бірнеше рет өзгеруі мүмкін).

Барлық таңдалған уақыт немесе жиілік аймақтарында сөздердің, сегменттердің немесе сөз бөлімдерінің ережелеріне сәйкес, яғни хаттама үшін кодтау кілттерімен алмасу ережелері бойынша кездейсоқ сұрыпталады. Ресивердің байланыс арнасындағы сандық сигнал декодталған және аналогқа айналды. Бұл әдіске негізделген әдіс өте күрделі, өйткені сапалы сөйлеу сигналы жоғары жылдамдықты аналогтық кіріс сигналын қажет етеді, сондықтан жоғары жылдамдықтағы ақпарат байланыс арнасы арқылы беріледі. 2400 дейін кең жолақты өткізу қабілеті кең жолақты деп аталады, егер таратылатын хабарлардың жалпы саны 2400 болса, бұл принцип дискреттік құрылғыларды шифрлау арқылы бұзылуы мүмкін. Оның күрделілігіне қарамастан, құрылғы коммерциялық нарықта ұсынылады, олардың басым бөлігі 2,4 - 19,2 кбит / с модуляция жылдамдығын және тұрақты телефондармен салыстырғанда бірнеше сәтсіз сөздерді бере алады. Шифрлау мен цифрландырудың басты артықшылықтарының бірі - байланыс ақпаратының қорғалуын қамтамасыз ететін жоғары деңгейдегі сөздерді және әдістерді басу үшін криптографиялық әдістерді пайдалану.

Бірінші дүниежүзілік соғыс кезінде дамытылған технологиялық сөздік. Бұл аймақтағы жетістіктердің бірі - цифрлық сигналдарды өңдеу үшін интегралды схемаларды және процессорларды және микропроцессорларды пайдалану. Осының бәрі құрылғыны жабудың көлемін және құнының төмендеуіне әкелді. Сандық аналогты сигналды ауызша сигналға немесе оның параметріне жіберу әрекеттерінен аулақ болды және сөз қорғауының жоғары деңгейіне жетті. Аналогтық сигналдардың шифрланған нұсқалары арнайы құрылғыларды (мысалы, модемдер) пайдаланбай қарапайым коммерциялық арнада шығатын сигнал ретінде бірдей жиілікте болады. Сондықтан, шифрлау құрылғысы салыстырмалы түрде қымбат емес және төмендегі цифрлық шифрлауды қолданатын іріктеу құрылғысын пайдалануда ерекше қиындықтар жоқ. Аналогты код жұмыс режиміне байланысты екі класқа бөлінеді:

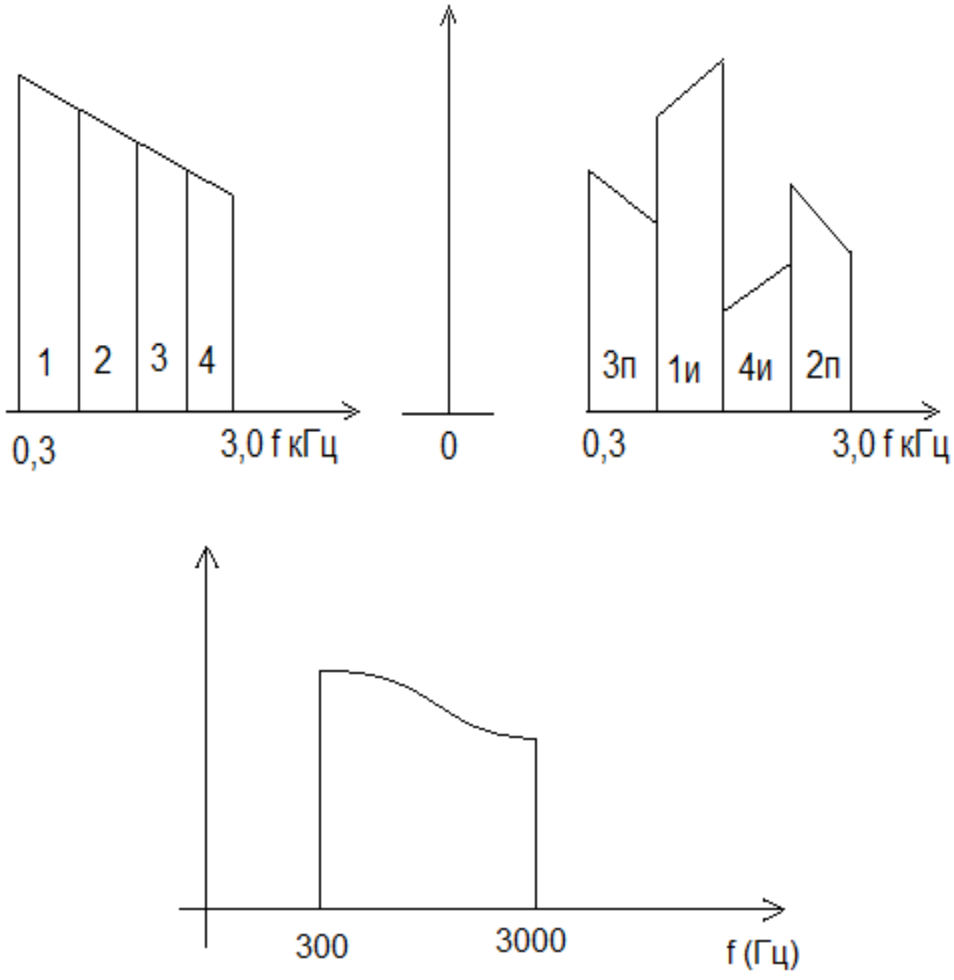
1. Кодтау схемасы ауызша презентация кезінде өзгермейтін статикалық жүйе;

2. Трансмиссия кезінде кодты үздіксіз шығаратын динамикалық жүйе (тасымалдау кезінде бір секундта бірнеше рет өзгеруі мүмкін).



Сурет 2.5 - Инверсті скремблерлеу

Сөздік спектрді бірдей ені бар бірнеше жиілік жолдарына бөлінеді, аралас және кері болуы мүмкін. (2.6-сурет).

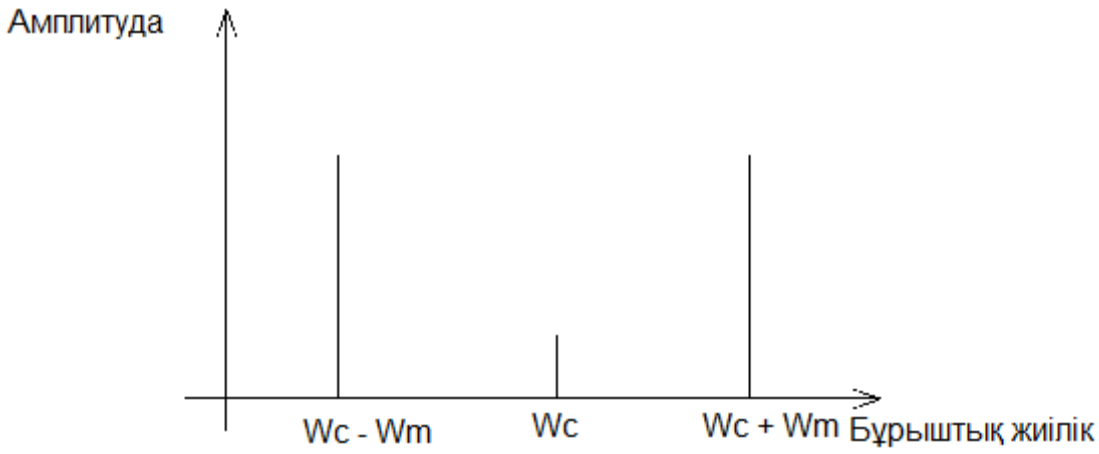


Сурет 2.6 - Сызықтық шрамминг

Жиілік жауабын мұқият қарастырайық.
Осылайша, жиі қолданылатын жиілік диапазонында қайта қаралады:
Инверсия
- Циклдық инверсия және жиіліктің өзгеруі.

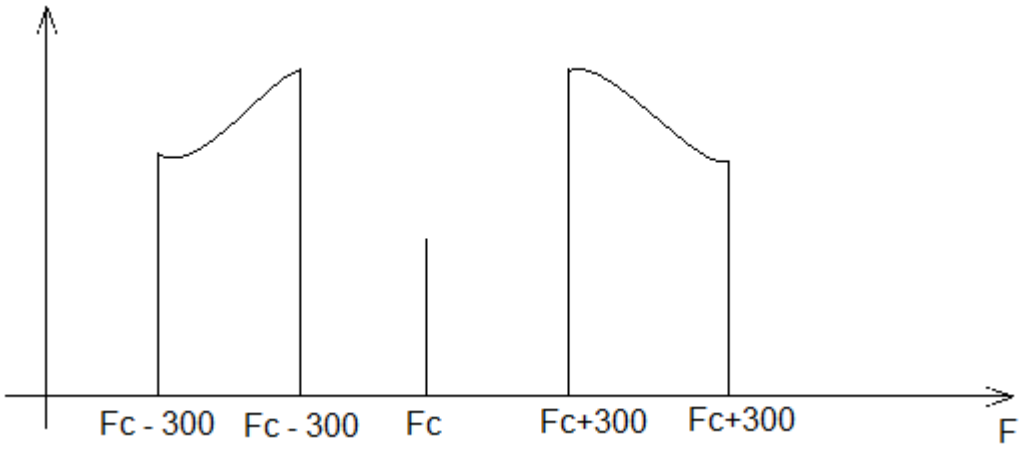
Кодтаудың ең көп тараған түрі - жоғарыда сипатталғандай кері спектральды түрлендіру.

Мысалы, 300-3000 Гц диапазонында сигнал қарастырыңыз (2.7-сурет).



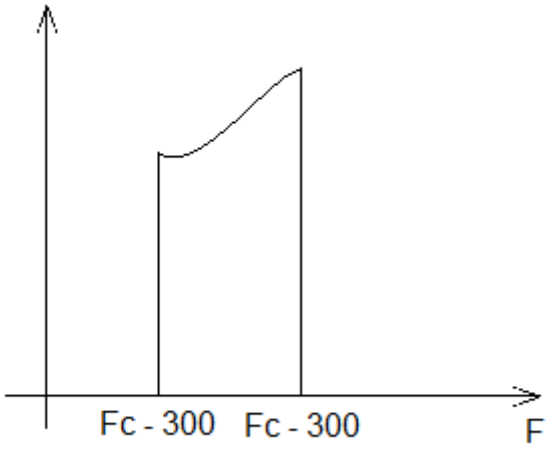
Сурет 2.8 - Инверсиялық сигнал спектрі

Сигналдың әр гармоникасын және оған сәйкес келетін қоспалауышты қарастырған кезде келесі графикті аламыз (2.9 -сурет).



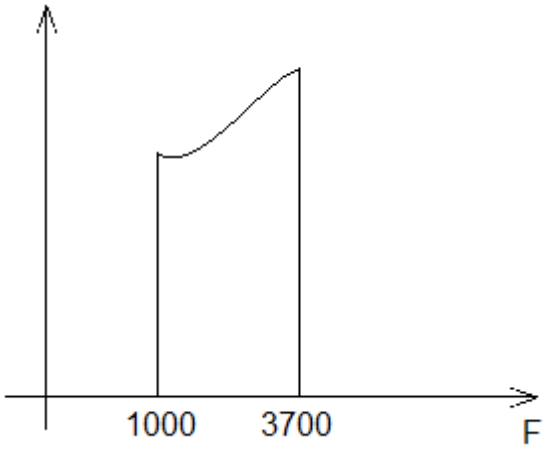
Сурет 2.9 - Сигнал қоспалауыштары мен спектрі

Жүргізушінің ортасында екі диапазон бар: жоғарғы және төменгі диапазондар. Жоғарғы диапазон шығыс сигналына ұқсас, тек жоғары (әр жиілік компонентіне көбейтілген). Төмен ауқым - шығыс сигналының айна бейнесі. Енді өткізу жолағының енін таңдап, өткізу қабілеттілігін кодтау үшін бүтін сандарды қолдануға болады. (2.10 сурет).



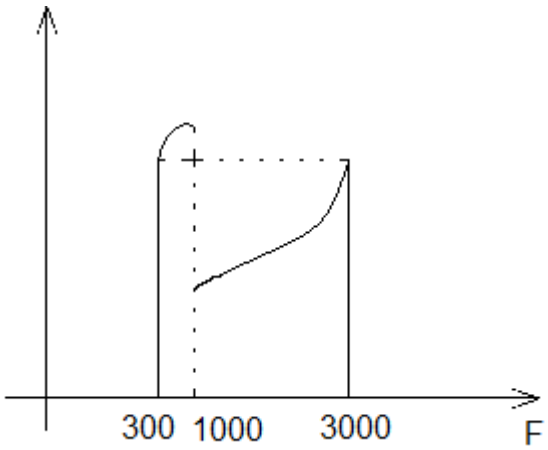
Сурет 2.10 - Іріктеу сигналы

Басқа сигнал таңдалғанда, тасымалдаушы жиілігі басқа жиілік диапазонына ауыстырылуы мүмкін. Бұл бір арнада бірнеше телефон хабарландыруларын жіберуге мүмкіндік береді. Инверсияны өзгерту құпия кілтке байланысты емес. Бұл жаудың шабуылдарына қауіп төндіре алмайтын кодтау. Циклдік инверсия кезінде инверттелген код үшін құпия кілт жасау идеясы пайдаланылады. Циклдық инверсияның мағынасы осында. Егер магистраль шығыс диапазонында болса (300 - 3000 Гц), тасымалдаушы жиілігі 3300 Гц. Басқа тасымалдаушы жиілігі 4000 Гц үшін спектр үшін кері сигнал беріледі.



Сурет 2.11 – Инверттелген сигнал

Бұл сигнал шығыс сызыққа тимейді. 3000 Гц – тен асатын спектрдің бөлігін шығыс спектрдің төменгі жағына алмасытруға болады. (2.12 -сурет).

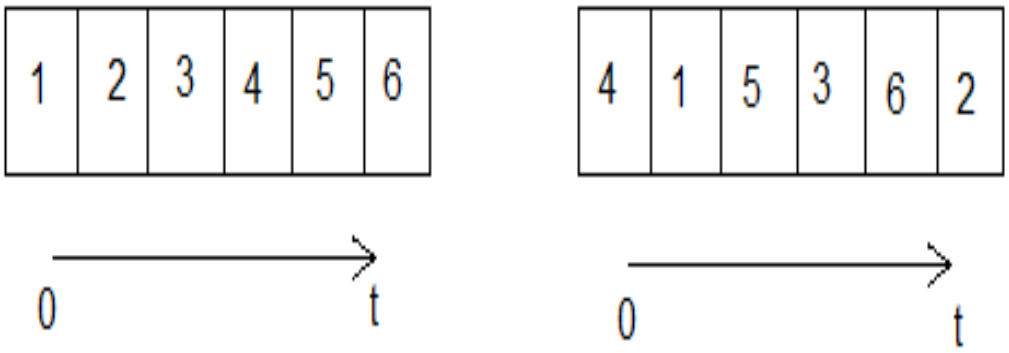


Сурет 2.12 – Шығыс спектрдің төменгі жағы

Спектрді ауыстыру - циклдік инверсия идеясы. Әдеттегі таратқышта 4-тен 16-ға дейінгі тасымалдағыш жиілігі болады. Бұл сан циклдік ығысуды ескереді. Шифрлар үшін кілтпен тасымалдағыш жиілігін таңдауға болады, ол жай ғана ауысады. Жүргізушінің жиілігін өзгерту үшін кездейсоқ сандардың генераторы пайдаланылуы мүмкін. Әдетте бұл 10 немесе 20 мс аралықты пайдаланады. Бұл әрекетті циклдық инвертор деп атайды. Бірақ екі әлсіз нүкте бар. Біріншіден, қалпына келтірілген өткізу қабілеттілігінің аздығын шығу сигналы арқылы қалпына келтіруге болады. Екіншіден, өндірістің қалған бөлігі осы әдіс үшін тым жоғары, себебі ол тыңдай алады. Жиілік доменінде сигналды түрлендірудің үшінші тәсілі - кеңірек ауқымды таңдау. Сигнал спектрі бір-бірімен алмастырылуы мүмкін бірнеше ұқсас жолақтарға бөлінеді. Бұны негатив шкаласымен түсіндіруге болады [13].Уақыт сенсоры корпустың екі түріне негізделген: уақыт сегменті түрлендіргіштері және олардың уақыттық жинақтылығы. Скремблердің кідірісі кодшының жиілігінен әлдеқайда жоғары,

бірақ оны азайтудың бірнеше жолы бар. Тікелей кодерде сөз сигналы уақытша сегменттердің дәйектілігіне бөлінеді, және әрқайсысы уақыттың соңынан уақытша өзгереді. Мұндай скремблерлер сегменттің ұзындығына байланысты сегменттердің шектеулі санын қамтамасыз етеді, ал сегменттер ұзартылған сөздерден аулақ болу үшін ұзындығы 250 мс болуы керек. Бұл жүйе кідірісі шамамен 500 мс және кейбір бағдарламалармен үйлесімді емес.

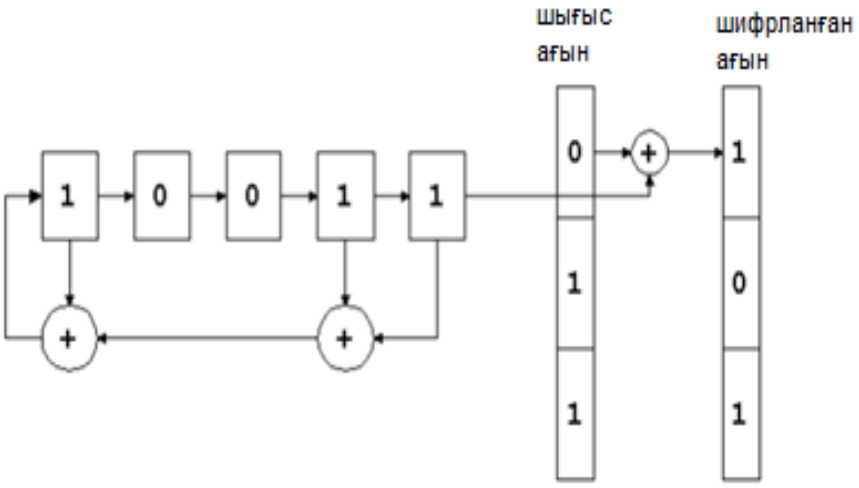
Уақыт интервалы әдісі жабу деңгейін жоғарылату үшін сөздік тақтасының бекітілген сөздікпен шектеледі. (2.13-сурет). Ауыстыру ережелері жүйенің кілті болып табылады және оны өзгерту арқылы сөздің жабылу деңгейін арттыруға болады.



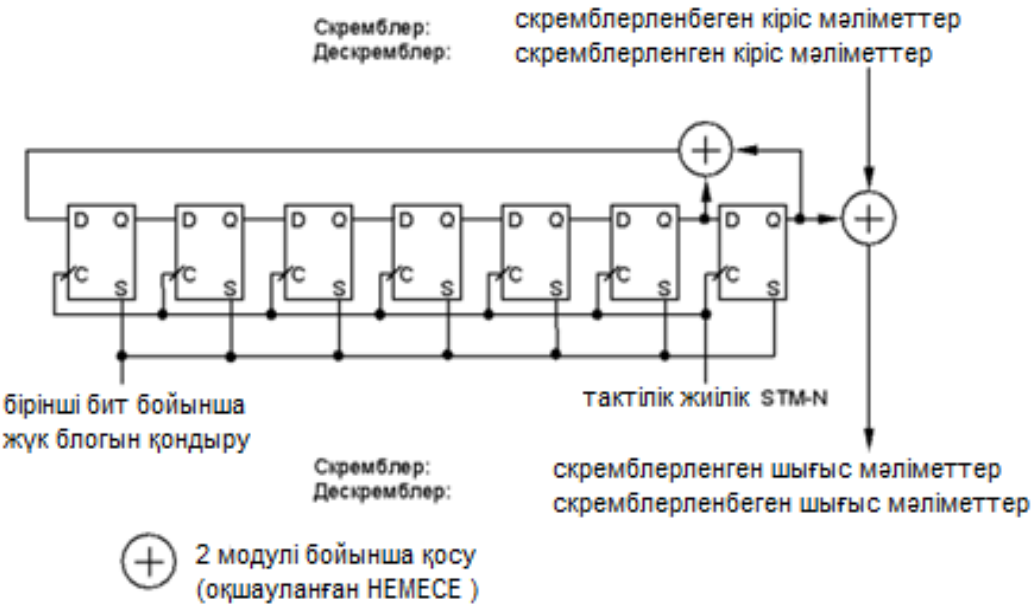
Сурет 2.13 – Сигналдың фиксирленген кадры

Смартфонның монтаждық жақтауымен негізгі кемшілігі - бұл жүйенің кешігуінің үлкен саны, яғни кадрдың ұзындығы екі есе көп. Сценарийлердің болмауы - сөздікке уақытша фрагмент. Ықтимал комбинациялардың кез-келген саны шектеуден аспайтын етіп шектелуі мүмкін. Шығарылатын сөздің әрбір сегменті уақыт терезесіне ие, сондықтан шифрлау үшін қажетті бос орынды бағалайды. Әрбір сигнал сегменті үшін бұл терезе кейде жылжиды. Кешігу терезенің ұзындығына тиеді.

Жүйелік жіп пен бөлімдерде орын алатын өзгерістерді қарастырайық. Сценарийлерде қолданылатын жалғыз әрекет XOR немесе BUT болып табылады. Әдепкі бойынша, кодтаудан ақпараттық ағымның параллель ағымы бит ағымына беріледі және кодтау ағыны деп аталады. Шифрлауды тікелей XOR кодтау арқылы кодтауға болады. Құрылған битмаптың ретін келесі алгоритмден басталатын ең кішкентай ақпарат басталады: Бит орнатылғаннан кейін XOR таңдалады және орналастырылады. Барлық сандар 1 битпен жылжытылады және жаңа алынған мәндер («0» немесе «1») ең төменгі битке орналастырылады. Ауыстырмас бұрын, үйдің жоғарғы жағындағы мән келесі бит ретінде кодталған тізімге қосылады (Суреттер 2.14 және 2.15).



Сурет 2.14 –Уақыттық скремблердегі мәліметтер ағынының бит бойынша өзгеруі



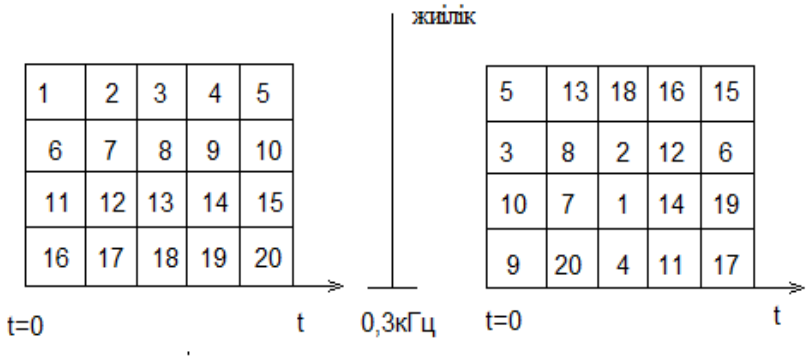
Сурет 2.15 – Уақыттық скремблердегі мәліметтер ағынының бит бойынша өзгеруі

Деректерді беру теориясынан криптографияның екілік жазбалар секілді ұқсас сұлбалары бар. 2.15 суретте көрсетілгендей, шифрлау комбинациясы құрылғының кері байланыс жүйесіне сәйкес келеді. Скремблерді енгізу электронды немесе электронды түрде жүзеге асырылады, ол өрісте кеңінен қолданылады. Шығу жолының әрбір биті бір кіріс битіне байланысты, бұл шифрлаушы деректерінің ағындарының қауіпсіздігін жақсартады. Бұл кодтау экрандағы кіру биттерінде кездесетін кедергілерге байланысты, олар экранда қорғалмаған, бірақ байланысты блокта емес. Шифрланған схема декодтау кодтау схемасымен сүйемелденеді, сондықтан ол алгоритм жоғалтпай қалпына келтіруге болатын «оқшауланған НЕМЕСЕ» пайдаланады. Алынған сығындыға рұқсат беріңіз. Спатула негізіндегі шифрлаудың басты мәселесі таратқыштың (кодтауыштың) және қабылдағыштың (декодер) синхронизациясы болып табылады.

Бір бит жіберілгенде немесе дәл емес болса, ақпаратыңыз толығымен жоғалады. Шифрланған шифрлау жүйесінде үндестіруге көп көңіл бөлінеді. Іс жүзінде бұл екі әдіс біріктіріледі:

а) синхрондалған тарап табылмаған кезде алдын ала анықталған бит синхрондау туралы ақпаратты жіберушіге қосу;

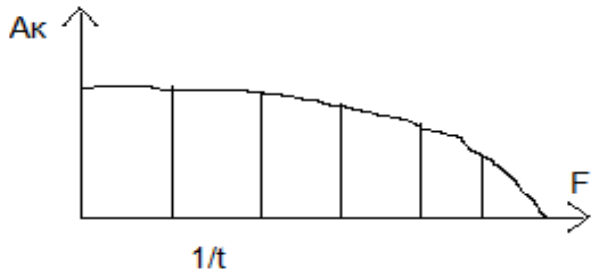
б) синхрондау кезінде алынған синхрондау барысында алынған алынған бит ақпаратын декодтау үшін жоғары жиілікті импульстардың генераторын пайдалану. Контакт арқылы алынған биттердің саны шифрлау деңгейі деп аталады. Scrambler 5 саннан көп [14].



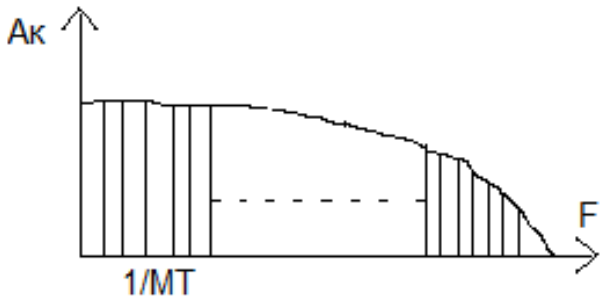
Сурет 2.16 – Аралас скремблердің жұмыс істеуі

2.16-суретте сөзді жабу жүйесі 4 сандық сигнал процессорын қолданады. Қайталанатын кері спектрлердің саны - төрт. Жиілік - Элементтің максималды уақыт кешігуі бес. Цифрлық-аналогтік түрлендіргіштен жабық сигнал аналогқа айналады және байланыс арнасына беріледі. Алгоритм сөздік сигналды қалпына келтіру үшін өзара әрекеттеседі, бұл сөзді жабу жүйесімен сәйкес келеді. Керісінше, тербелістердің барлық түрлері (жиіліктік инверсиясымен) кері сөздікке әкелуі мүмкін. Уақыт белгінің шекаралары сигналдың тұтастығын бұзады, себебі ол сызықты емес байланыс жасайды. Теріс әсерлері байланыс арнасының өткізу қабілеттілігін тудырады, бұл сенімді байланыс үшін шу мен шудың болмауына әкеледі. Алайда, жоғарыда аталған мәселелерге қарамастан, коммерциялық арналардағы ақпаратты қорғау үшін, жиілікте және уақытта шифрлау әдістері, сондай-ақ комбинациялық әдістер қолданылады.

Шифрлау энергетикалық спектрдің екілік сигналына әсер етеді.



Сурет 2.17 – Скремблерлеуге дейінгі сигнал спектрі



Сурет 2.18 – Скремблерлеуден кейінгі сигнал спектрі

Жоғарыдағы суретте Т0 ұзақтығы бар 6 бинарлық элементтерден тұратын

мерзімді сигналдың энергетикалық спектрі көрсетілген. Шифрлаудан кейін M = 2n-1 элементтерімен кездейсоқ өзгеру спектрі байытылған. Осыдан кейін спектрдің компоненттері көбейтілген, сондықтан әрбір компоненттің деңгейі де [15] сияқты азаяды.

2.2 Simulcrypt арқылы қақтығыстар туралы ақпарат

Шифрланған бағдарламалық жасақтама. Бұл әдісті пайдаланып, ақпаратты шифрладым: ол да қызмет арқылы шифрланады. Ол үшін серверге шартты кіру жүйесін қосыңыз. Хамелеон және мұндай байланыс бақылау порты арқылы ұйымдастырылады.

Жабық бағдарламаны жасау үшін Хамелеонға қадамдар:

- қажетті пакеттік бағдарламаларды орнату.

- Шартты кіру серверін ЕММ (Қол жетімділік туралы ескерту) және ECM (Access Control Notification) талаптарына сәйкес конфигурациялау.

- симулятордың интерфейсінде ЭММ генераторына қосылу үшін хамелеон жасау.

- Шығатын пакетке ЕММ қосылымын орнатыңыз.

- Simulsrypt интерфейсінде EMS генераторына қосылу үшін хамелеон жасау.

- ECM генераторына «ECM» қосыңыз.

- Жеке топ жасаңыз және оны ECM ағынына қосыңыз.

- Егер сізге шифрлау қажет болса, сіз қызметті жабық топта (SCG) қосуыңыз қажет.

Шифрлау кілттерінің ең көп саны - 64. Әрбір жабық топ тек бір шығыс сигналына қосылуы керек. Әрбір шығыс сигналы үшін жеке топты құру қажет.

ЕММ генераторына қосылуды ұйымдастыру.

Біз Хамелеонға шартты қатынау жүйесіне IP мекенжайын беруіміз керек.

ЕММ генераторына қосылыңыз.

Simulcrypt мәзірінің SETTINGS бөліміне өтіңіз және осы батырманы басыңыз.

ЕММ генераторының терезесінде ҚОСУ түймесін басыңыз. Сонда:

1. ЕММ генераторына қосылу үшін ат беру керек.

2. Клиенттің идентификаторын және портын енгізіңіз.

3. Қажет болса, он алтылық сандардағы жеке деректеріңіздің мәнін енгізіңіз.

4. Ең үлкен жылдамдықты енгізіңіз. (BW) ЕММ үшін (kbps)

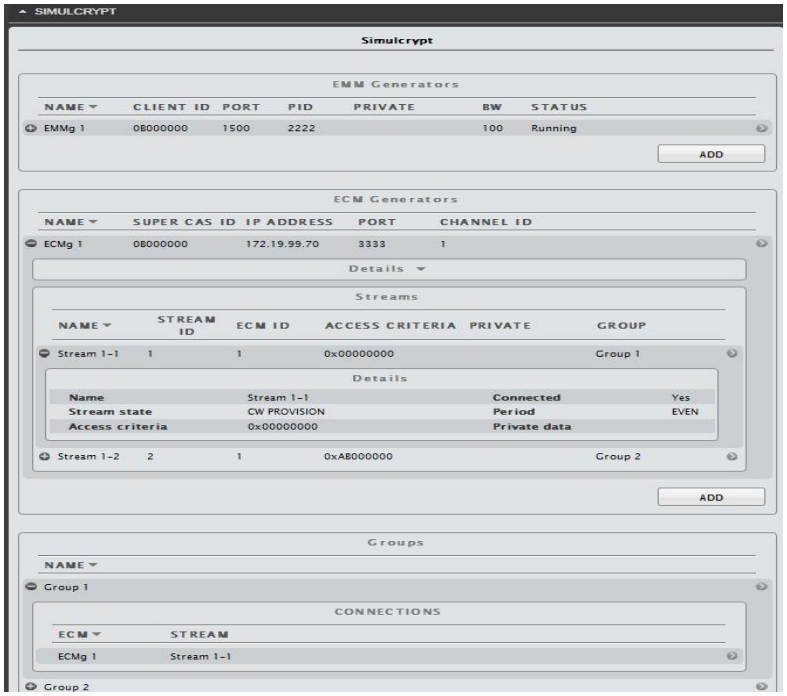
5. түймесін басыңыз.

ЕМА генераторының жанында. Жоғарыдағы қадамдарды қайталаңыз.

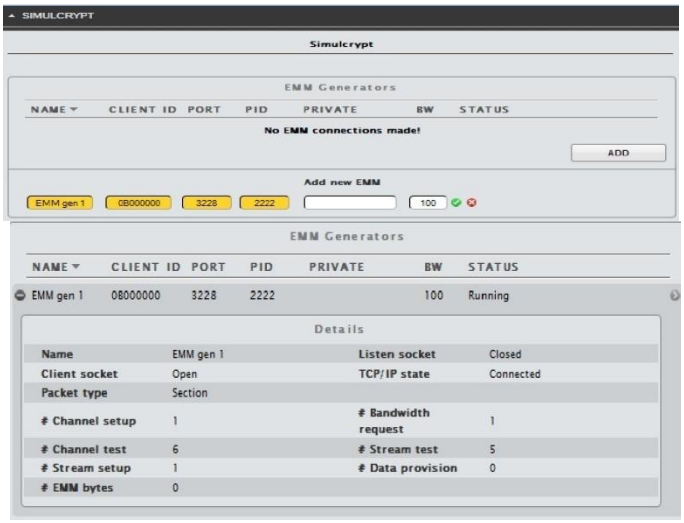
ЭММ-ге қосылу пакеттерін ұйымдастыру.

SERVICE (ҚЫЗМЕТ) мәзірінде бағыт бағдарын тінтуірдің оң жақ түймешігімен басып, ашылмалы мәзірден «Add EMM Connection» тармағын

таңдаңыз. Бұл шығуды пайдалану үшін EMM генераторын таңдаңыз.



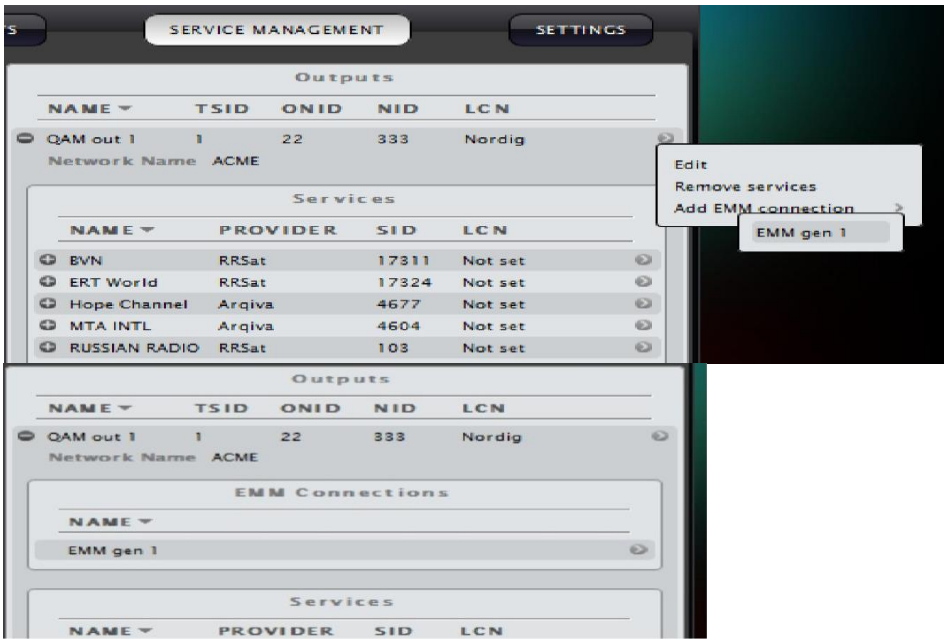
Сурет 2.20 – Simulcrypt бағдарламасының негізгі терезесі



Сурет 2.21 – Simulcrypt бағдарламасында CAS серверін EMM генераторымен қосу

2. ECM генераторына қосылуды ұйымдастыру.
3. Simulcrypt мәзірінің SETTINGS бөліміне кіріп, осы батырманы басыңыз.
4. ESC генератор терезесіндегі ҚОСУ батырмасын басыңыз. Сонда:
5. 1. Қосылу үшін ECM генераторына атаңыз.
6. 2. Супер CAS идентификаторын енгізіңіз.

7. 3. CAS серверінің IP-мекен-жайын енгізіңіз.
8. 4. ECM порт нөмірін енгізіңіз.
9. 5. Арна идентификаторын (арна ID) енгізіңіз.
10. немесе enter пернесін басыңыз.



Сурет 2.22 – Simulcrypt бағдарламасында EMM – ді шығыс ағынмен қосу

Сурет 2.23 – Simulcrypt бағдарламасында ECM генераторын құру

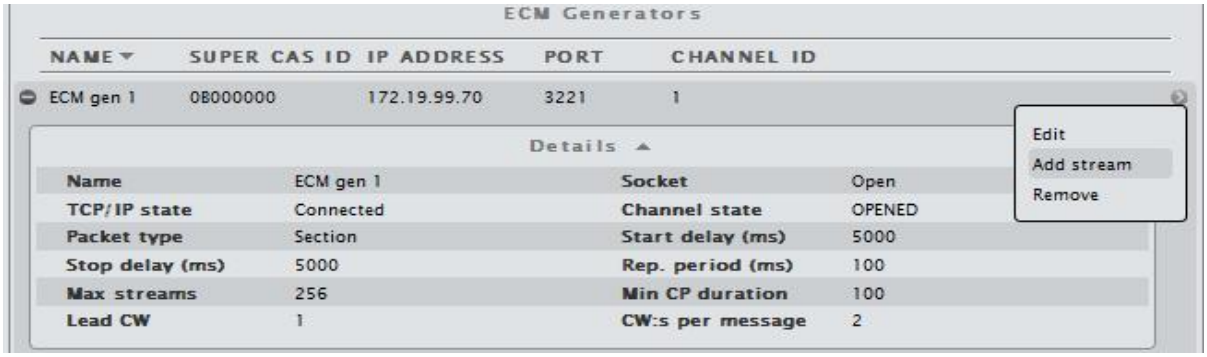
ECM генераторына басқа қосылуларды қосу үшін алдындағы қадамдарды қайталау керек.

ECM генераторына «ECMағынын» қосу.

Концепция «ECM ағыны»ECM генераторларына жабық топтарға рұқсат алу үшін керек. Қатынау критерийін енгізген кезде, бұл смарт картаға ақпаратты дескремблерлеуге мүмкіндік береді.

ECM генераторына «ECM ағынын» қосу.

Simulcrypt менюінің SETTINGS бөлімінде ECM генераторының оң жағындағы ● белгісіне басу керек, «ағынды қосу» пунктін таңдау.



2.24- Сұраным - ECM ECM Simulcrypt сәтсіз болғанда әмбебап генератор шығарады

1. ECMagyna atra қабылдайды.

2. STREAMIDgeNECMID (жергілікті идентификатор).

Катинау критериясы.

4. Егер Керек Болса менің баспана алу форматында жеке мәліметтерімді беруі керек болса.

5. Жариялауды бастаңыз.

Кірпіктер ECM жүйесінде ECM жүйесінде тығыздалған.

JMF - жоғары анықтамалық аудио / бейне бейімдеуге арналған нұсқаулық, сондай-ақ WWW-кодтар мен ЭЦМ диалог критерийлері критерийлері.

Тосттар, шыңдар (SCG).

Мәзір опциялары Simulcrypt болып табылады және Kerek филиалына арналған тюйммеге басы болады.

Add (Қосу) түймешігін басыңыз (Карабск қ. Бақылау топтары):

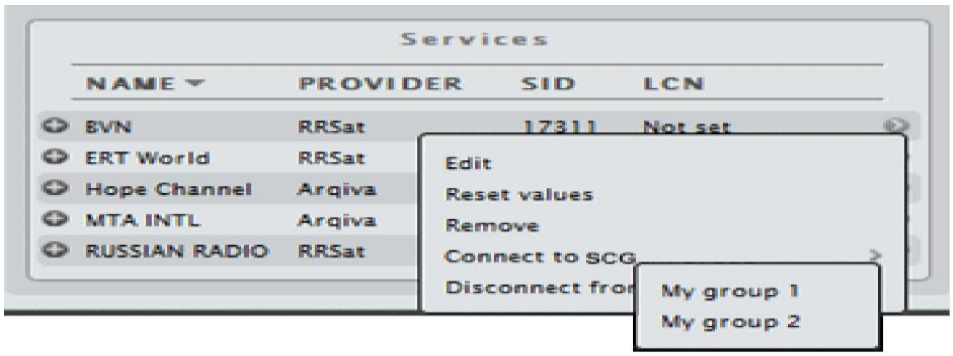
1. Топқа ат беріңіз.

2. Қымбатты басым

Сурет 2.25–- Simulcrypt бағдарламасында группа құру терезесі

Жабық топқа ECM ағындарын қосу.

Simulcrypt менюінің SETTINGS бөлімінде ECM ағынының оң жағындағы түймесін басу. Түсірмелі менюінде «Группаға қосуды»(“Connect to group”) басу және қосылуға қажетті жабық топты таңдау.



Сурет 2.26– Simulcrypt бағдарламасында ECM ағынын жабық группаға қосу

Скремблерлеу қажет ақпараттарды жабық топқа енгізу.

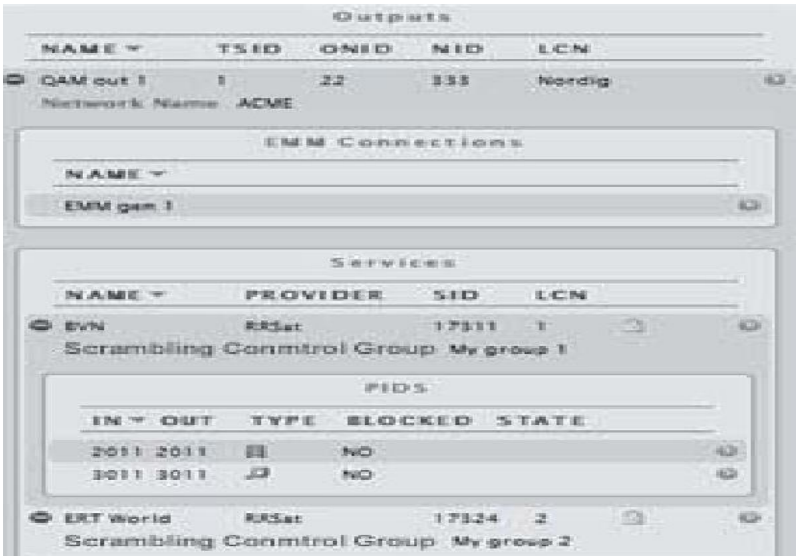
SERVICE MANAGEMENT менюінің «Outputs» бөлімінде сервистің оң жағындағы түймесін басу.

Түсірмелі менюде «группаға қосылу» (“Connect to SCG ”) пунктін таңдау және қосылатын топтың атын таңдау.

Егер сіз белгісіне басып, жабық топқа қосылған сервисті ашатын болсыңыз, онды сервистің атында сіз осы сервистің қосылып тұрған тобының атын көре аласыз.

Скремблерленген ақпарат құлп ретіндегі белгімен көрсетіледі.

Жабық топқа қосылған сервистегі барлық аудио және видеолар, сөздер скремблерленген болады.



Сурет 2.27–- Simulcrypt бағдарламасында қорғалған ақпарат терезесі

Бұл бағдарламаның маңызы зор. Simulcrypt бағдарламасы маңызды ақпаратты қорғауға мүмкіндік береді. 2.27– суретте көрсетілгендей әр қорғалған топтың немесе ақпараттың жанында құлп белгісі тұрады. Бұл бағдарлама арқылы өзінде көрсетілген қадамдар арқылы өзіңізге қажетті ақпаратты қорғай аласыз. Және де қорғалған ақпаратты қайтадан баршаға ортақ ақпаратқа айналдыру функциясы да бар.

2.3 Криптография

Криптография - бұл деректерді және хабарламаларды қауіпсіз түрде сақтауға және таратуға мүмкіндік беретін код беру үшін стандарттар мен хаттамалардың жиынтығы. Медиа орта (мысалы, Интернет) сенімсіз болса, құпиялылық файлдарды шифрлау үшін криптографияны қолдануға болады - басқа адамдардың бұл түсіну қабілеті төмендейді және деректерді топтастыру құпия болып қала береді.

Сіз цифрлық қолтаңбалар мен сертификаттарды пайдаланып, шифрланған деректер мен хабарларды тексере аласыз. Криптографиялық әдісті пайдаланған кезде криптографиялық кілттер құпия болып табылады. Дегенмен, алгоритмдер, негізгі файл өлшемдері мен пішімдері қауіпсіздікті бұзбайды.

Криптографияның екі негізгі әрекеті - шифрлау және шифрлеуді анықтау. Шифрлау деректерді кодтау болып табылады, сондықтан ол бастапқы мәліметтерді шығара алмайды. Декодтау кезінде шифрланған деректер криптографиялық кілттермен түпнұсқаға қайтарылады.

Сізге криптографиялық алгоритм және шифрлау мен шифрды анықтаудың кілті қажет. Шифрлаудың көптеген алгоритмдері, соның ішінде, деректер шифрлау стандарты (DES) шифрлары, Rivest / Sharmir / Adleman (RSA), RC2 және RC5 шифрлары бар. Бұл опциялардың әрқайсысы үшін кілт

қарапайым мәтінді (оқылатын) қою мәтінге (кодталған және оқылмайтын) айналдыру алгоритміне сәйкес пайдаланылады.

DES, RC2 және RC5 симметриялық кілт немесе криптографиялық кілт технологиялары ретінде белгілі, себебі деректерді шифрлау үшін пайдаланылатын кілт сонымен қатар оның шифрын анықтау үшін қолданылады. Сондықтан, деректерді шифрлау тобы мен оны анықтайтын топ арасында кілт құпия түрде берілуі керек.

RSA әдетте криптография немесе асимметриялық криптография деп аталады, себебі ол екі түр кілтті пайдаланады: ашық кілт және жеке кілт. Кілттер математикалық түрде өзара байланысты, бірақ сіз олардың біреуін білмесеңіз басқа біреуді басып шығара алмайсыз. Жеке кілт құпия болып табылады - тек криптографиялық жұпты құрғандар оған қол жеткізе алады. Ашық кілт Интернет сияқты қорғалмаған орталарда пайдаланылады. Ашық кілт жүйелерін пайдаланған кезде, екі тарап арасында ортақ құпия жоқ. Егер ашық кілт деректерді шифрлау үшін пайдаланылса, оның жеке кілті оны тек қана шифрлай алады. Сол сияқты, жеке кілт деректерді шифрлау үшін пайдаланылса, жалпыға қолжетімді кілт оны шифрлай алады.

Шетелдіктерге үйренуге мүмкіндік бермейтін ақпаратты трансформациялау әдістерімен қорғау мәселесі бұрыннан бері адамзатқа жағымды әсер етті. Криптографияның тарихы адамзат тарихына оралады. Бұдан басқа, ежелгі хаттар тек ежелгі қауымдастықтармен таңдалған және алғашқы тіркелген криптографиялық жүйе болатын. Бұл мысал ежелгі Үндістанның көне мысырлық, қасиетті кітабы. Жазуды кеңінен қолданғандықтан, криптография жеке ғылым ретінде қалыптасты. Бірінші криптожүйелер біздің дәуіріміздің басында табылды. Осылайша, Цезарь өз атымен жазылған жүйелік шифрларды қолданды. Бірінші және екінші дүниежүзілік соғыс кезінде криптографиялық жүйе тез дами бастады. Соғыс жылдарынан бастап қазіргі уақытқа дейін есептегіш құралдардың пайда болуы криптографиялық әдістерді дамытуды және жетілдіруді жеделдетті. Деректерді қорғаудың криптографиялық әдістері компьютерде сақталатын немесе әртүрлі типтегі компьютерлерде сақталатын ақпаратты қорғаудың автоматтандырылған жүйелерінде қолданылады. Криптографиялық трансформацияның алдын-ала рұқсат етілмеген алдын алу әдісі ретінде ұзақ тарихы бар. Қазіргі уақытта көптеген шифрлау әдістері жетілдірілді, және пайдалану үшін теориялық және практикалық негіз әзірленді. Бұл әдістердің көбісі ақпаратты жабу кезінде пайдаланылуы мүмкін. Ақпараттық жүйеде криптографиялық әдістерді пайдалану мәселесі қандай да бір себептермен өте маңызды. Бір жағынан, үкіметтік ақпараттың үлкен көлемін қамтитын компьютерлік жүйе ғаламдық Интернет жүйесі арқылы пайдаланылады, ол әскери, коммерциялық және жеке тұлғаларға рұқсатсыз қол жеткізуді жібереді. Екінші жағынан, жаңа, қуатты және нейрондық компьютерлік техниканың пайда болуы криптографиялық жүйеге деген сенімді арттырды, ол шешілмеген болып қала береді. Криптология трансформация арқылы ақпаратты қорғаумен айналысады (криптос - рдемдесер, логос-ғылым). Криптология криптография және

криптетанализ. Бұл бағыттардың мақсаты бір-біріне қайшы келу. Криптография ақпараттың трансформациясы үшін математикалық әдістерді іздеу және зерттеу жұмыстарымен айналысады. Cryptanalysis Environment - ақпараттың құпия сөзсіз ашылу мүмкіндігін зерттейді. Қазіргі криптография 4 негізгі бөлімнен тұрады:

1. Симметриялық криптожүйелер.

2.Ашық кілті бар криптожүйелер.

3. Электрондық қол қою жүйесі.

4. Негізгі басқару.

Криптографиялық әдістерді пайдаланудың негізгі бағыттары - ақпарат беру (мысалы, электрондық пошта), хабарламаларды жіберу құнын растау және шифрланған деректерді (құжаттар, деректер базаларын) сақтау болып табылады. Осылайша, криптография ақпарат кілтінің тек оқуға рұқсат ету үшін ғана өзгереді. Электрондық қолтаңба - бұл басқа пайдаланушыларға қосымша криптографиялық түрлендіру, сондай-ақ мәтіннің авторы және мәтінді тексеру.

Қазіргі заманғы ақпараттық жүйелерде пайдаланылатын әліпбидің мысалы:

- бос алфавиттің және кеңістіктің 32 адресі (мәселе);

- ASCII және KUU-8 стандартты классификациясына енгізілген белгілер;

Екілік алфавит;

- талап етілетін немесе он алтыншы алфавит;

Шифрлауды декомпрессионизациялау процесі: түпнұсқа мәтін шифр мәтінімен ауыстырылады. Кері шифрлау кері үрдіс. Шифрланған мәтін бастапқы кодпен өзгертіледі.

Критографиялық жүйе ашық мәтінді T отбасын ұсынады. Бұл отбасы мүшелері индекстеледі және k таңбаланған, параметр k - кілт. Бос орын мүмкін кілттер жиынтығы. Әдетте алфавит әріптерінің дәйектілігі тұрады. Криптожүйелер симметриялық және ашық кілттерге бөлінеді. Симметриялық криптожүйеде шифрлау немесе қайта шифрлау үшін тек бір кілт қолданылады. Ашық кілттер жүйесінде 2 кілтті математикалық ашық және жеке кілтпен бір-бірімен байланысу үшін пайдаланады. Бұл ақпарат оны қалайтындардың барлығына мүмкіндік беретін ашық кілтпен шифрланады және қайта шифрлау тек алушыға белгілі жеке кілт көмегімен жүзеге асырылады. «Кілттер» және «кілттерді басқару» терминдері пайдаланушылар арасында ақпарат өңдеу жүйесіндегі үрдістерге жатады.

Криптографиялық тұрақтылық - бұл сәтсіздік жағдайында тұрақтылықты анықтайтын шифрлардың сипаты. Криптографиялық тұрақтылықтың бірнеше көрсеткіштері бар:

- Потенциалды кілттер саны - сценарий үшін қажетті орташа уақыт. Деректерді криптографиялық түрде жабу процесі бағдарламада да, ақпаратта да жүзеге асырылады. Көп ақша жұмсаңыз, бірақ ол жоғары өнімділік, қарапайымдылық, қорғаныс және тағы басқа артықшылықтарға ие. Бағдарламалау өте ыңғайлы, сондықтан пайдалану өте икемді.

Ақпаратты қорғаудың заманауи криптографиялық жүйесі келесі талаптарға жауап береді:

- шифр мәтіні кілтпен ғана оқылуы тиіс;

- Шифрлау үшін пайдаланылатын жұмыс кілттерінің саны, кем дегенде, шифрланған хабарламаны көрсету үшін қажетті пернелердің жалпы саны болуы керек;

- барлық кілттерді таңдағанда және қазіргі заманғы компьютерлердің мүмкіндіктерін асыра отырып, қайта шифрлау үшін қажетті операциялардың саны қатаң болуы керек;

- шифрлау алгоритмін білу қорғаудың тиімділігіне әсер етпеуі тиіс;

Кілт сөздің кішкене өзгерісі шифрланған хабарламаның түріне елеулі өзгеріс әкелуі керек, тіпті сол кілтді пайдаланғанда да керек;

- шифрлау алгоритмінің элементтерін өзгертуге болмайды;

- шифрлау кезінде үнемі пайдаланылатын кілт сөздерге байланысты қарапайым және қарапайым қолдануға болмайды;

- шифр мәтінінің ұзындығы мәтіннің ұзындығынан аспауы тиіс;

- алгоритм бағдарламалық қамтамасыз ету мен ақпаратқа рұқсат беріп, кілт ұзындығын өзгерту шифрлау алгоритмінің сапасына әсер етпеуі керек;

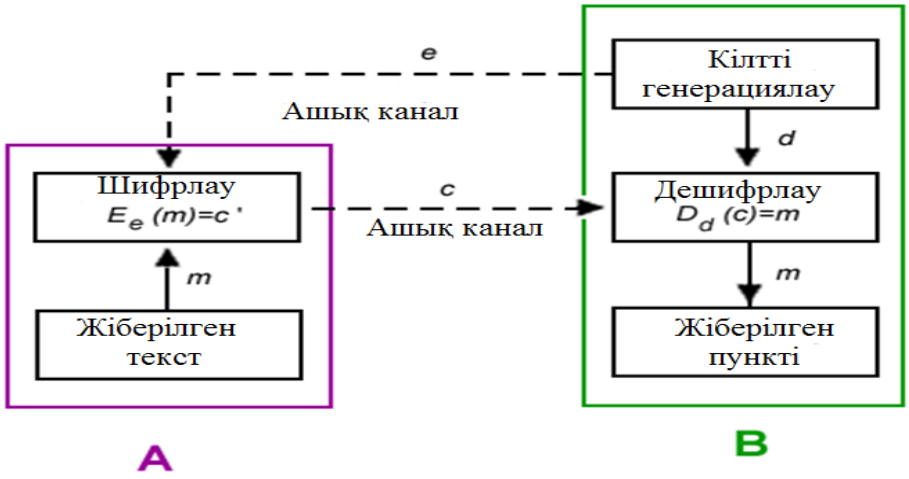
Диск қауіпсіздігі - бұл әлсіз бөлік: ол тұрақты болғанда сенімдірек болады. Жақсартылған криптожүйеде алгоритм, протокол, кілт және басқа да өте күрделі сынақтан өту керек. Егер криптографиялық алгоритм тұрақсыз болса, онда кез-келген криптоаналит бұл қатені анықтайды. Егер генератор көтерілсе, жад слоттары қорғалмаса, қауіпсіздік талап етілмейді.

Оның үстіне, іс жүзінде ақпараттық қауіпсіздік тек криптондық аналитиктерге ғана тәуелді емес [16].

Алайда ашық кілтті дамытудан бастап криптожүйелердің артықшылықтары мен кемшіліктері туралы пікірталастар жалғасуда. Симметриялық криптографиялық алгоритм кілт ұзындығына ие және асимметриялық емес. Алайда, ашық кілттердің криптожүйелерін ойлап тапқандардың бірі американдық криптолог. Деффидің айтуынша, олар әмбебап криптожүйенің жаңа түрі ретінде қарастырылуы керек.

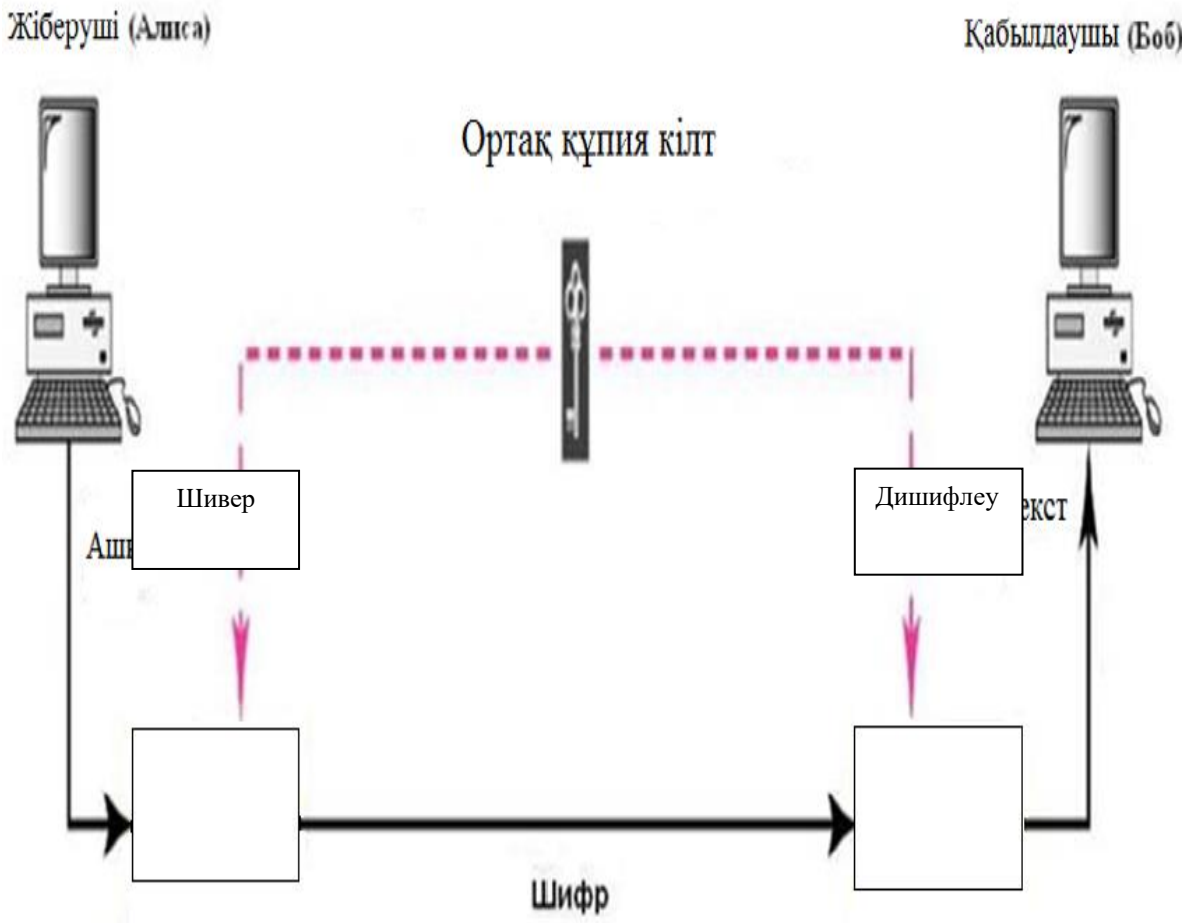
Ашық кілттер жүйесі. Алайда, криптографиялық жүйелердің күрделілігі мен сенімділігі, олардың ең осал тұстары негізгі коммутация проблемалары болып табылады. Егер сіз екі ақпараттық жүйенің субъектілері арасында құпия ақпарат алмасатын болсаңыз, бір нысан кілт жасайды және оны қайтадан конфигурациялауы керек. Яғни, жалпы айтқанда, кілтті таратуға арналған криптографиялық жүйені пайдалану қажет. Нәтижелерге сүйене отырып, классикалық және заманауи алгебрада осы мәселелерді шешуге арналған ашық кілттер жүйесі бар. Қысқаша айтқанда, ақпараттық жүйелердің 2 алушыларының әрқайсысы бір-бірімен байланысқан 2 кілтті құруы керек. Бір кілт мөлдір, екіншісі жабық деп жарияланды. Хабарламаны адресатқа жібергіңіз келетіндерге ашық кілт беріледі. Бұл құпия кілт болып қалады. Бастапқы код алушының ашық кілтімен шифрланады және оған жіберіледі.

Шифрланған мәтін бұл кілтпен шифрланбайды. Хабарды қайта шифрлау адресатқа белгілі құпия кілт арқылы ғана мүмкін болады.



Сурет 2.28 – Криптографияның асимметриялық (ашық кілт) шифрлау жүйесі

Симметриялық криптожүйелер. Шифрлау және оны қайтадан ашуға бір криптографиялық кілт қолданылатыншифрлау түрі. Асимметриялық шифрлау түрі шыққанға дейін симметриялық шифрлау негізгі шифрлау түрі болды. Кілт екі жақта да құпия түрінде сақталуы керек.



Сурет 2.29 – Криптографияның симметриялық шифрлау жүйесі

Неміс криптографиялық қорғанысының басты ерекшелігі - Advanced Encryption Standard (AES) және 256-бит Twofish шифрлау алгоритмін пайдалану. Бұл құрылғының сенімділігін көрсетеді. Оның үстіне, автордың пікірі бойынша, компания мемлекеттің ешқандай байланысы жоқ - коммерциялық ұйым. Германияда осындай құрылғылардың сатылуы туралы мәселе пайда болды.

Сондықтан, келіссөз жүргізу маңызды деп санайтын адамдар осы құрылғыны пайдаланған кезде қате жасамайды.

Кемсітушілік кемшіліктері:

- бүйірлік құрылғыларға деген қажеттілік;
- сөз кідірісі (бірнеше секундқа созылуы мүмкін);
- әңгімеде эхо пайда болды.

Криптофонның артықшылығы: танымал криптоформаторлар танымал алгоритмдерді пайдаланады. Бұл алгоритмдер бірнеше рет хакерлерден қорғалған. Мұндай криптофондар ұялы телефонның сенімділігін қамтамасыз етеді [17].

Мұндай құрылғының сипаттамаларын қарастырайық.

Кесте 2.1 - Жұмыс режимі

Параметр	Комментарий
Дауысты шифрлау	Толықдуплексті режим (4800, 9600 бит/сек)
Coder-ISDN – мен бірігуі	

Кесте 2.2 - Трансляция принципі

Параметр	Комментарий
Радио модем стандарт GSM 900/1800 мГц	
Модем	V.110
Модем жылдамдығы	9600 бит/сек

Кесте 2.3 –Криптографиялық сипаттамалары

Параметр	Комментарий
Алгоритм	Жарияланбайды, 256 бит
Кілтті тарату түрлері	Симметриялы
	Сеансты кілттер әрбір байланыс сеансына автоматты түрде айналады
Кілт генераторы	Кілт генератор шуы арқылы айналады
Кілттік қуат	10 77
Қосымша кілттерді тарату	Сыртқы тасушыда ұзақ уақыттық, группалық кілтті жазу
Рұқсатты басқару	Ұзақ уақыттық жеке кілттің болуы
Тазарту функциясы	Байланыс сеансының соңында сеанстық кілттер автоматты түрде жойылады
	Байланыс сеансының кілтін қалпына келтіру қарсыластың телефонына рұқсат болғанның өзінде мүмкін емес

3 Цифрлық беріліс жүйесін кедергіден қорғаудың есебі

Қазіргі таңда бағыттылған ортада цифрлық сигналды беруде симметриялық электрикалық кабельдер және коаксиалды кабельдер көбірек қолданыс тапты.

Цифрлық линиялық трактегі цифрлық ағынға басқа жақтан электрикалық кедергі болып табылатын электрикалық сигналдар келіп түседі. Осындай кедергілердің сипаттамалары әр кабельге әр түрлі әсерін тигізеді.

Біздің жағдайда ИКМ – 120У цифрлық беру жүйесі симметриялық кабельде жұмыс жасайды. Бұл кабельге ең негізгі кедергі өтпелі кедергі болып табылады. Олар өткінші өшудің соңғы аумағында төрттік жұп кабельдің арасында және төрттікте пайда болады.

ИКМ – 120У цифрлық беру жүйесі екі кабельді жүйе болып табылады. Ол үшін кабельдің соңғы жағындағы кедергі үлкен рөл атқарады. ИКМ – 120У цифрлық беру жүйесіндегі цифрлық линиялық тракт үшін шағылған сигналдардан түскен кедергі маңызды кедергілердің бірі болып табылады. Олар кабельдің толқындық кедергісінің қабаттасуынан болады, регенератордың кіріс және шығыс тізбегінен, толқындық кедергінің құрылыстық ұзындығының түйіскен жерінің бірыңғай болмауынан болады. Қабаттасқан және бірыңғай болиаған жерлерде цифрлық ағындар цифрлық линиялық сигналдан озады немес қалады, соның әсерінен кедергі келтіретін электрикалық сигнал пайда болады[18].

3.1Линиялық трактта қатенің рұқсат етілген ықтималдығын есептеу

Өткінші кедергілер және регенератордың күшейткішін дұрыстайтын меншікті шулар қабылдағыш станцияның кірісінде цифрлық қатенің пайда болуына әкеліп соғады.

Цифрлық қатенің телефондық беріліске әсері аналогты беріліс жүйесіндегі каналдың кедергісімен салыстырғанда тамаша. Декодерленгеннен кейінгі трактағы әрбір қате телефонда жағымсыз тықыл тудырып, аналогты сигналдың көлемінің бірден өзгеруіне алып келеді. Екілік ақпаратты цифрлық линиялық тракт арқылы берудің негізгі бағасы қате ықтималдығы болып табылады (немесе қате коэффициенті).

Қате ықтималдығы қате қабылданған белгінің санының $N_к$ жалпы берілген белгінің санына $N_ж$ қатынасы болып табылады.

$$P_k = \frac{N_k}{N_{ж}}; \qquad (3.1)$$

Цифрлық линиялық тракт арқылы берілетін цифрлық ағынға үнемі ауытқу кедергілер әсер етеді және олар цифрлық қатеге әкеліп соғады.Бұл қандай да бір бинарды белгінің бөлігі қате қабылданды дегенді білдіреді: «1» белгісінің орнына «0» белгісі және керісінше болуы мүмкін. Сондықтан қате ықтималдығы үнемі нөлден өзгеше: $P_к \neq 0$.

Каналды цифрлық сигналдың ИКМ – мен кез – келген кодтық комбинациясы екі жоғары разрядтағы қатесі айқын тыңдау тықылын тудырады. Егер цифрлық берілу жүйесіндегі каналда минутына бір тықылдан кем тыңдалатын болса, анықталған норма бойынша телефондық ақпаратты беру сапасы қанағаттанарлықтай.

Қазіргі барлық цифрлық беру жүйесінде 8 кГц дискретизация жиілігінде әр канал бойынмен 1 минут ішінде 8000·60=480000 кодтық комбинация беріледі.Тықылдың кезінде екі жоғары разрядты кодтық комбинация немесе 2·480000=960000 белгі қауіпті. Кез – келген белгіні қате қабылдағандағы бірдей ықтималдықта цифрлық беру жүйесінің каналындағы цифрлық линиялық тракттың максималды созылымдылығының қате ықтималдығы мына шартты қанағаттындыруы керек:

$$P_k \leq \frac{1}{960000} \approx 10^{-6};$$

Қайталып қабылдағыш участогының тональді жиілікпен ұзындығы 2500 км болғандағы 1км трактіге рұқсат етілетін қате:

$$P_k \leq \frac{10^{-6}}{2500} = 4 \cdot 10^{-10} \frac{1}{км};$$

Жоғары сапалы ақпарат беру үшін телефония және телеграфия бойынша халықаралық консультациялық комитет (МККТТ) жүйені өңдей кезінде қате ықтималдығы ЦЛТ 1 км-ге $10^{-10}\frac{1}{км}$ нормасы қолданылады. Бұл жағдайда линиялық тракт L үшін рұқсат етілетін қате ықтималдығы келесі формуламен анықталады:

$$P_{K_{доп L}} = 10^{-10} \cdot L; \qquad (3.2)$$

$$P_{K_{доп L}} = 10^{-10} \cdot 80 = 8 \cdot 10^{-9} \frac{1}{км};$$

Спецификалық кедергінің цифрлық беру жүйесіне әсерінің кедергіден қорғалуы тоналды жиіліктің каналының шығысындағы кедергі келтіретін тықылдардың жиілігімен сипатталатын линиялық тракттің қатесінің ықтималдылығымен бағаланады.

3.2 Беру жүйесінде регенераторлардың қорғалуын есептеу

Цифрлық сигналды беру кезінде қатенің пайда болуының себебі лездік мәндері шектелген мәнінен асып кететін кедергілер және ол артық импульсті тудырады немесе бар импульсті жоғалтып жібереді.

Симметриялық кабельмен жұмыс жасайтын ИКМ-120У екі кабельді цифрлық жүйеде басым кедергілер ретінде линиялық ауысулардан туындайтын кедергі және алыс шеттегі ауысым кедергілер болып табылады.

Қорғау есебі келесі формуламен анықталады:

$$A_{з_l} = A_{l_{ср}} - a_{ру_{t\max}} - 10\lg(n-1) - \delta_l - q; \qquad (3.3)$$

мұндағы,

$A_{з_l}$ - алыс шеттегі орташа ауысым өшуі, *дБ*

δ_l - стандартты ауытқу $A_{l_{ср}}$, *дБ*

$$\delta_l = 5{,}65 \text{ дБ};$$

n – кабельдегі екіжақты цифрлық тракттің саны n = 2;

$a_{р.у.\max}$ –максималды проектті температурада регенерациялық участоктың өшуі, *дБ*;

q=3 –регенераторды дайындау кезінде қорғау рұқсаты;

Ауыспалы өшудің орташа мәні келесі формуламен анықталады:

$$A_{l_{ср}} = -10\lg\left(\frac{1}{m}\sum_{i=1}^{m} 10^{-0.1\cdot A_{l_i}}\right); \qquad (3.4)$$

мұндағы,

m–симметриялық кабельдегі жұптар саны, m = 2;

A_{l_i} - алыс шеттегі жұптар арасындағы қорғалу мәні,*дБ*

$$A_{l_i} = 90 \text{ дБ} \quad /2/$$

$$A_{l_{ср}} = -10\lg\left(\frac{1}{2}\sum_{i=1}^{2} 10^{-0.1\cdot 90}\right) = -10\lg\left(\frac{1}{2}\cdot 2\cdot 10^{-9}\right) = 90 \text{ дБ}$$

Максималды температура кезіндегі регенерациялық участоктың өшуі:

$$a_{р.у_{\cdot t\max}} = \alpha_{t\max,\,f_р} \cdot l_{р.у.расч} + 2a_{тр} + a_{ил},; \qquad (3.5)$$

мұндағы,

$a_{ил}$ – жасанды сызықтың өшуі,*дБ*;

$a_{тр}$ – сызықтық трансформатордың өшуі ($a_{тр}$ = 1*дБ*);

$l_{р.у.расч.}$ = 5 км –регенерациялық участоктың ұзындығы;

$\alpha_{t_{\max,\,f_р}}$ –грунт температурасының максималды мәніне сәйкес келетін есептік жиіліктегі кабельдің километрлік өшуі,*дБ*/км;

$$\alpha_{t_{\max,\,f_р}} = 11{,}159\,дБ,$$

$$\alpha_{t_{\max,}} = 11{,}159 \cdot 5 + 2 \cdot 1 + 0 = 57{,}79\,дБ$$

Алынған мәндерді (3.5) формуласына қойып, алыс шеттегі қорғалуын табамыз:

$$A_{з_l} = 90 - 57{,}79 - 10\lg(2-1) - 5{,}65 - 3 = 23{,}56\ \ дБ$$

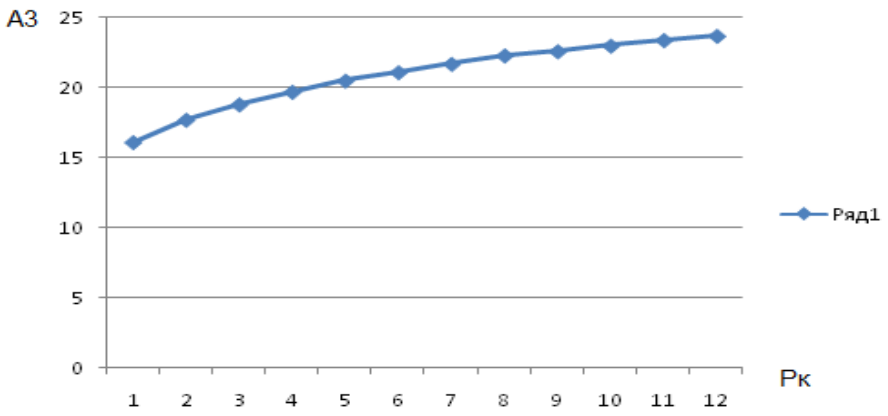
Регенератордың қатесінің ықтималдығын есептеу. Регенратордың қатесі мен қорғалуының ықтималдығында байланыс бар –қорғауды жоғарылату қате ықтималдылығының төмендеуіне әкеліп соғады. Линиялық код ретінде АМ-I импульстерінің полярлылығын кезектестіру коды немесе КВП-3 модофицирленген квазиүштік код қолданылатын ИКМ-120У беру жүйесі үшін қате ықтималдылығының мәнін 3.1 - кестесі арқылы анықтаймыз.

Ол үшін таблицадан есептелген мәнге жақын, одан аз $А_з$мәнін таңдаймыз (шарт бойынша $А_з$таблицада болмайды).

Кесте 3.1 –Квазиүштік код үшін $А_з$және $Р_к$ – ның арасындағы байланыс

з	6,1	7,7	8,8	9,7	0,5	1,1	1,7	2,3	2,6	3,0	3,4	3,7
$Р_к$	0^{-3}	0^{-4}	0^{-5}	0^{-6}	0^{-7}	0^{-8}	0^{-9}	0^{-10}	0^{-11}	0^{-12}	0^{-13}	0^{-14}

Осы кестені қолданып, $А_з$ = 23,56 *дБ*болғандағы қатенің ықтималдығы $Р_к=10^{-13}$.



Сурет 3.1 – А3 – тің Рk – ға тәуелділік сұлбасы

3.3 Цифрлық беріліс жүйесіндегі күтілетін кедергіге тұрақтысының есебі

Цифрлық беріліс линиясының кедергіге тұрақтысы цифрлық сигналдың цифрлық линиялық трактың барлық элементтері арқылы өткенде пайда болытн қате ықтималдылығымен бағаланады. Әр түрлі регенераторларда қателер бір – біріне байланыссыз түрде пайда болады, сондықтан цифрлық линиялық трактағы қате ықтималдылығын анықталған участоктардың қате ықтималдылықтарының қосындысы түрінде анықтауға болады.

Күтілетін кедергі тұрақтысы линиялық трактың барлық ұзындығының қате ықтималыдылығы бойынша анықталады, оны келесі формуламен көрсетеміз:

$$P_{K_{L_{ож}}} = \sum P_{K_i} ,$$

мұндағы,

P_{K_i} - *i*-ші регенератордың қате ықтималдылығы;

i – регенератордың нөмірі.

Егер барлық трактың регенераторы үшін қате ықтималыдылығы бірдей болса, онда біздің жағдайдағыдай, линиялық трактағы күтілетін қате ықтималыдылығын келесі формуламен анықтаймыз:

$$P_{K_{L_{ож}}} = (N+1) \cdot P_K , \qquad (3.6)$$

мұндағы,

N - регенерациялық пункттердің саны.

$$P_{K_{L_{ож}}} = (15+1) \cdot 10^{-13} = 16 \cdot 10^{-13}$$

$P_{K_{ож}}$ теңдігін орындағаннан кейін, оны 3.1 пунктінде табылған, рұқсат етілген қате ықтималдылығымен $P_{K_{L_{доп}}}$ салыстыру керек.

$$P_{K_{L_{ож}}} \le P_{K_{L_{доп}}}$$
$$16 \cdot 10^{-13} \le 8 \cdot 10^{-9}$$

Теңсіздік орндалып тұр, сондықтан ҚРП дұрыс қойылды.

ИКМ-120У – дың қорек көзі. ИКМ-120У құрылғысының біріншілік электр көзін тұрақты тоқтың станциялық қорегі қамтамасыз етеді және кернеулері 60В±10% немесе 24±10%. Сол уақытта құралғыны қоректендіру үшін біріншілік желіден ерекшелеп тұратын кернеу керек. Осы кернеуді алу үшін электр көзінің жүйесінде біріншілік желідегі кернеуді трансформатордың көмегімен керек деңгейге дейін көтеретін немесе түсіретін кернеуді түрлендіргіш қолданылады және ол түзеткішке жіберіледі.

ИКМ-120У құрылғысының электр көзінің барлық құрылғысында дұрыстаудың импульсті әдісі қолданылған. Электр көзінің аппаратурасында дұрыстаудың импульсті әдісі ПӘК-ін 70-75 %-ға дейін жеткізді. ИКМ-120У аппаратурасының екіншілік электр көзін маңыздылығы бойынша екіге бөліп қарастыруға болады: қызмет етілмеген регенерациондық пункктерде орналасқан соңғы құрылғының электр көзі және аралық құрылғының электр көзі.

К-60П-4 құрылғысының ИКМ-120У құрылғысына тікелей ауыстырылуы магистральдарда қызмет етілмеген күшейткіш пункттардың орнына қашықтықтық қорек көзін ұйымдастыратын қызмет етілмеген регенерациондық пункттар қойылады.

Қызмет етілмеген пункттардағы қашықтықтық қорек көзін ұйымдастыру.Қорек көзі – қызмет етілмеген регенерациондық пункттарда орналасқан линиялық тракттың құрылғысы және ол кернеудің тізбектей қосылуынан кейінгі қашықтықтық тұрақты токпен жүзеге асады. Қашықтық қорек көзі жасанды қатар арқылы «сым-сым» сұлбасы бойынша ұйымдастырылған және ол ақпаратты беру желісі арқылы жүзеге асады.

Қызмет етілмеген аппаратураның ИКМ-120У цифрлық беру жүйесінің «АКТОБЕ–ОКТЯБРЬСК» магистралі үшін қашықтықтық қорек көзінің сұлбасы А қосымшасында көрсетілген. Қашықтық қорек көзі ҚҚК-24М блогы арқылы жүзеге асады. ҚҚК-24М блогы сызықтық құрылғы кернеуі 24В болған кезде қондырылады. ҚҚК блогы қызмет етілмеген пункттың регенератордың қорек көзі бір беріліс жүйесін қамтамасыз етеді.ҚҚК блогының беріліс жүйесіне байланысты санын 3.2 - кесте арқылы анықтаймыз.

Кесте 3.2 - ҚҚК блогының санының ИКМ-120У блогының санына тәуелділігі

Беріліс сызығы	Жүйе санына байланысты ҚҚК блок саны							
	1	2	3	4	5	6	7	8
ҚКП	1	2	3	4	5	6	7	8
ҚКРП	2	4	6	8	10	12	14	16

Біздің магистраль екі ИКМ-120У беру жүйесіне есептелген, 240 КТЧ. Екі соңғы пункттар және ҚҚК–нің блок саны да екіге тең.

Соңғы станцияларда жоғары вольтті токты тұрақтандыратын ҚҚК –нің құрылғысы орналасады.Әрбір ҚРП –да ҚҚК – нің тогын кернеуге түрлендіретін ҚҚК қабылдағышының құрылғысы қондырылған және ол біржақты регенератордың және телебақылау құрылғысының қоректендіруге керек.

«Актобе-Октябрьск» магистралінің ұзындығы 80 км және ол бір жарты секциядан аспайды. ИКМ-120У цифрлық беру жүйесіндегі бір жарты секцияның ұзындығы 120 км –ге дейін жетуі мүмкін.

ИКМ-120У аппаратурасының ҚҚК құрылғысының негізгі техникалық сипаттамалары:

- кіріс кернеу, В - 60±6.0; 24±2,4;
- ҚҚК номиналды тоғы, мА –65;
- шығыс кернеу, В – 35….480;
- ҚҚК тоғының тұрақсыздығы ДП, % не более +-5;
- шығыстағы пульсация кернеуі, В әсер. – 2;
- ҚҚК – нің сөнуі және сигнализацияның пайда болуы;
- ҚҚК қатарының үзілуі - ИӘ;
- ҚҚК тоғының өсуі, мА - 72±3.

ҚҚК – нің кернеуінің есебі. Әрбір жарты секциялы ҚҚК үшін ҚҚК кернеуінің есебі:

$$U_{ККК} = I_{ККК} \cdot r_{t\max} \cdot \sum_{i=1}^{n} l_{рег.i} + n_{КРП} \cdot U_{КРП}, \qquad (3.7)$$

мұндағы,

$I_{ҚҚК}$ =65 мА – ҚҚК – нің тоғының номиналды мәні;

r_{tmax} – грунттың максималды температурасы кезіндегі кабельдің электрикалық кедергісі, ом/км.

$l_{регі}$- *i*–нші регенерациялық участоктың ұзындығы, км;

Бізде барлық ұзындықтар бірдей болғандықтан, $l_{рег.}$ = 5 км;

$N_{КРП}$ =15 – ҚҚК блогымен қоректенетін ҚРП саны;

$U_{КРП}$- бір ҚРП – дағы кернеудің түсуі, В

$U_{КРП}$=10D

Грунттың максималды проектті температурасы кезіндегі кабельдің электрикалық кедергісін табамыз, формула бойынша 20°С:

$$r_{t\max} = r_{20} \cdot [1 + \alpha_r (t_{\max} - 20^o)], \quad (3.8)$$

мұндағы,

r_{20} - 20°С кезіндегі сымның кедергісі, ом/км.

r_{20} = 15,95 ом/км

t_{max} = 18°С – кабель сымының кедергісі анықталатын температура, °С

$\alpha_r = 4 \cdot 10^{-3} \frac{1}{C^o}$ – кедергінің температуралық коэффициенті

$$r_{t\max} = 15{,}95 \cdot [1 + 4 \cdot 10^{-3}(18^o - 20^o)] = 15{,}82 \frac{OM}{км}$$

“Актобе –Октябрьск” магистралінің ұзындығы бір ҚҚК жарты секциясынан аспағандықтан, ҚҚК кернеуінің есебі бір ғана жарты секция үшін есептелген (3.7 формуласы бойынша).

$$U_{ККК} = 0{,}065 \cdot 15{,}82 \cdot \sum_{i=1}^{15} 5 + 15 \cdot 10 = 0{,}065 \cdot 15{,}82 \cdot 15 \cdot 5 + 150 = 227{,}12B$$

ҚҚК – нің есептелген кернеуі нормадан аспайды, бұл ҚРП – ның орналасуы дұрыс дегенді білдіреді.

3.4 Цифрлық беру жүйесінің сенімділігі

Жүйенің сенімділігі ретінде белгілі бір шартта берілген тапсырманы белгілі бір сапамен, бірілген уақытта орындау саналады. Көрсетілген параметрлерін өзгертетін жүйенің жағдайының өзгеруі бас тарту деп аталады.Копканалды беру жүйесі қайта қалпына келетін жүйеге жатады, яғни бас тартуды қалпына келтіруге болады.

Сенімділік теориясының жағдайларының бірі ол бас тартуды кездейсоқ оқиға ретінде қарастырады. Жүйені қосқаннан бастап бірінші бас тартуға дейінгі уақыт аралығы кездейсоқ мән болады және бас тартусыз жұмыс уақыты деп аталады.Бас тартусыз жұмыс істеудің уақыты t – дан кем болатын бұл кездейсоқ мәннің интегралды таралу функциясы *q(t)*және *0÷t* аралығында бас тарту ықтималдығы бар. Осы интервалдағы қарсы жатқан мәннің ықтималдылығы мынаған тең:

$$P(t) = 1 - q(t). \quad (3.9)$$

Элементтердің сенімділігі (t) деп белгіленетін бас тарту ықтималдылығы болып табылады және t моментінде шартты тығыздық ықтималдылығын көрсетеді, бірақ осы моментке дейін бас тарту болмауы керек.λ(t) и p(t) функцияларының арасында өзара байланыс бар:

$$P(t) = l^{-\int_0^t \lambda(t)dt} \quad (3.10)$$

Нормалды эксплуатация периодында бас тарту интенсивтілігі жуықша алғанда тұрақты: $\lambda(t) \approx \lambda$. Бұл жағдайда $P(t) = l^{-\lambda t}$.

Нормалды эксплуатация периодын сипаттайтын тұрақты бас тарту интенсивтілігі уақыттың өтуімен бас тартусыз жұмыстың ықтималдылығының экспоненциалды төмендеуіне сәйкес келеді.

Бас тартусыз жұмыстың орташа уақытын кездейсоқ мәннің математикалық күтімімен анықтайды:

$$t_{ср} = \lambda \cdot \int_0^{\infty} t \cdot l^{-\lambda t} \cdot dt = \frac{1}{\lambda} \quad (3.11)$$

Сенімділік параметрінің есебі. Цифрлық линияның бас тарту интенсивтілігін мына формула бойынша табамыз:

$$\lambda_{жүйе} = \lambda_{ҚРП} \cdot n_{ҚРП} + \lambda_{СП} \cdot n_{СП} + \lambda_{каб} \cdot \alpha \quad (3.12)$$

мұндағы,

$\lambda_{ҚРП}$ – ҚРП бас тартуының интенсивтілігі;

$\lambda_{СП}$ – СП, ҚРП бас тартуының интенсивтілігі;

- $\lambda_{каб}$ – кабельдің бір километрінің бас тартуының интенсивтілігі;
- α –магистраль ұзындығы, км;
- α= 80 км;
- n –ҚРП саны;
- $n_{ҚРП}$ = 15;
- $n_{СП}$ – СП, ҚРП саны;
- $n_{ОП}$ = 2.

Кесте 3.3 – ЦЛТ элементтерінің сенімділік параметрі

Элементтің аты	ҚРП (+)	СП,ҚРП (-)	Кабель

λ, 1/с	$3\cdot10^{-8}$	10^{-7}	1 км– ге $5\cdot10^{-8}$
tВ,с	4,0	0,5	5,0

Берілген 3.3 – кестеніқолданып:

$$\lambda_{жүйе.}= 3\cdot10^{-8}\cdot15+\cdot10^{-7}\cdot2+5\cdot10^{-8}\cdot80=4{,}65\cdot10^{-6}\cdot\ 1/сағ;$$

Бас тартусыз жұмыстың орташа уақытын (3.11) формуласы бойынша табамыз:

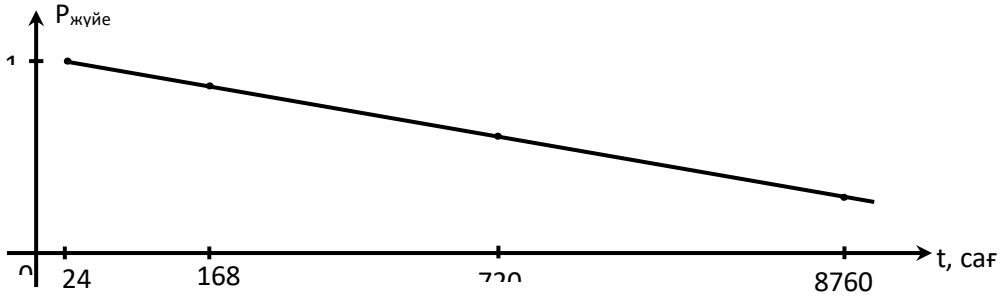
$$t_{op_{жүйе.}} = \frac{1}{\lambda_{жүйе}} = \frac{1}{4{,}65\cdot10^{-6}} = 2150853{,}76\,саг = 24{,}55\ жыл$$

Берілген уақыт аралығындағы бас тартусыз жұмыс ықтималдылығы: t_1=24 сағ (күніне), t_2 = 168 сағ (аптасына), t_3 = 720 сағ (айына), t_4=8760 сағ (жылына) келесі формуламен анықтаймыз:

$$P_{eqt.} = l^{-\lambda_{;eqt}\cdot t}$$

t_1 = 24 сағ $P_{жүйе}$ = 0.9998
t_2 = 168 сағ $P_{жүйе}$ = 0.9992
t_3=720 сағ $P_{жүйе}$ = 0.9966
t_4 =8760 сағ $P_{жүйе}$ = 0.9600

Осы есептердің қорытындысы бойынша $P_{жүйе}$ (t) графигін құрамыз.



Сурет 3.2 – Уақыт бойынша бас тартусыз жұмыстың ықтималдылығының өзгеруі

Жүйені қалпына келтірудің орташы уақытын табамыз:

$$t_к=(\lambda_{КРП}\cdot n_{КРП}\cdot\ t_{В\cdot КРП}+\lambda_{СП}\cdot n_{СП}\cdot t_{В\cdot СП}+\lambda каб\cdot\alpha\cdot t_{Вкаб.})\cdot\frac{1}{\lambda жүйе};$$

бұл жерде $t_{кҚРП}$, $t_{кСП}$, $t_{ккаб}$– ҚРП, СП және кабельдің қалпына келтіру уақыты, мәндері кестеде көрсетілген.

$$t_к=(3\cdot10^{-8}\cdot15\cdot4{,}0+10^{-7}\cdot2\cdot2\cdot0{,}5+5\cdot10^{-8}\cdot80\cdot5{,}0)\cdot\frac{1}{4{,}65-10^{-6}}=(1{,}92\cdot10^{-6}+10^{-7}+$$

$$+2\cdot10\text{-}5)\cdot\frac{1}{4{,}65-10^{-6}})=4{,}735 \text{ сағ};$$

Енді цифрлық линиялық тракттың дайындық коэффициентін анықтаймыз.

$$K_д=\frac{t_{ор}}{t_{ор}+t_к} \qquad (3.13)$$

мұндағы $t_В$ – жүйені қалпына келтірудің орташа уақыты;
$t_{ср.}$ – бас тартусыз жұмыстың орташа уақыты.

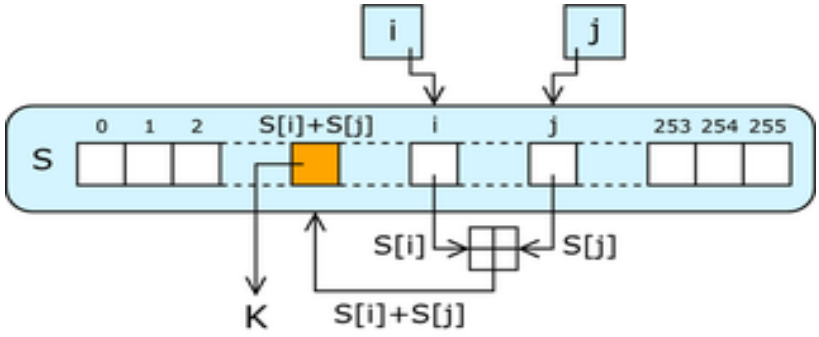
$$K_д=\frac{215053{,}76}{215053{,}76+4{,}735}=0{,}99997$$

Дайындық коэффициенті 0.998– ден төмен емес және ол станцияның линияға дұрыс орналасқандығын дәлелдейді, цифрлық тракт сенімділігінің параметрлері шартты қанағаттындырады.

Сенімділік параметрін ЭЕМ –мен де есептеуге болады[19].

3.5 Шифрлау алгоритмі

RC4 шифрлау алгоритмі. RC4 — бұл компьютерлік желінің ақпараттарын қорғауға қолданатын ағынды шифр. Шифр RSA Security Inc. компаниясымен ойлап табылды және оны қолдану үшін лицензия керек. RC4 авторы Рональд Ривест (Ronald Rivest). Ол Ron’s Code және Rivest’s Cipher болып шығады.



Сурет 3.3 - RC4 кілттік ағынының генераторы

Алгоритм ядросы кілттік ағынның генерация функциясынан тұрады.Бұл функция биттердің тізбегін генерациялайды және екілік модуль бойынша ашық текстке бірігеді. Оны қайтадан қалпына келтіру кілттік ағынды регенерациялап, шифрограммамен екілік модуль бойынша қосу керек. Алгоритмнің басқа негізгі бөлігі — айнымалы ұзындықты кілтті кілттік ағынның бастапқы қалпына келтіретін инициализациялау функциясы.

RC4 — блоктың көлемін анықтайтын алгоритм класы. Бұл n алгоритмі сөз көлемі болып табылады. Жалпы n = 8, бірақ талдау мақсатында оны кішірейтуге болады. Бірақ оның қауіпсіздігін үлкейту үшін оның мәнін де үлкейту керек. RC4 ішкі жағдайы 2^nкөлемді сөз және екі есептегіштен, яғни әр көлемге бір сөзден келеді. Массив S-бокс атымен белгілі және содан кейін S әрпімен белгіленеді. Екі есептегіш іжәнеj әріптерімен белгіленеді.

RC4 инициализациялау алгоритмі төменде көрсетілген. Бұл алгоритм l байт ұзындыққа ие және Key – де сақталған кілтті қолданады.ИнициализацияS массивін толтырудан басталады, әрі қарай осы массив арнайы анықталған кілт бойынша орналастырылады. S – ке бір әрекет қолданылған кезде, құптау орындалуы керек.

Құпия кілт тек қана бастапқы ауытыруды қамтамасыз етеді.

Бастапқы құру:

$$j \leftarrow 0 \quad S \leftarrow (0, 1, \dots, 2^n-1)$$
$$\text{for i = 0 to } 2^n - 1 \text{ do}$$
$$j \leftarrow (j + S_i + K_{i \bmod l}) \bmod 2^n$$
$$S_i \leftrightarrow S_j$$

Инициализация:

$$i \leftarrow 0 \qquad j \leftarrow 0$$

Алгоритма денесі:

$$i \leftarrow (i + 1) \bmod 2^n$$
$$j \leftarrow (j + S_i) \bmod 2^n$$
$$S_i \leftrightarrow S_j$$
$$t \leftarrow (S_i + S_j) \bmod 2^n$$
$$Z_i \leftarrow S_t$$

1. Генератордың бастапқы құрамын жүзеге асырамыз.

$$j = 0, \qquad S = \begin{pmatrix} S_0 & S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix},$$

$$i = 0, \ j = (0+0+8) \bmod 8 = 0, \ S_0 \leftrightarrow S_0, \ S = \begin{pmatrix} S_0 & S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix},$$

$$i=1,\ j=(0+1+3)=4,\qquad S_1\leftrightarrow S_4,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,4,2,3,1,5,6,7\end{pmatrix},$$

$$i=2,\ j=(4+2+8)\bmod 8=6,\ S_2\leftrightarrow S_6,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,4,6,3,1,5,2,7\end{pmatrix},$$

$$i=3,\ j=(6+3+3)\bmod 8=4,\ S_3\leftrightarrow S_4,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,4,6,1,3,5,2,7\end{pmatrix},$$

$$i=4,\ j=(4+3+8)\bmod 8=7,\ S_4\leftrightarrow S_7,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,4,6,1,7,5,2,3\end{pmatrix},$$

$$i=5,\ j=(7+5+3)\bmod 8=7,\ S_5\leftrightarrow S_7,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,4,6,1,7,3,2,5\end{pmatrix},$$

$$i=6,\ j=(7+2+8)\bmod 8=1,\ S_6\leftrightarrow S_1,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,2,6,1,7,3,4,5\end{pmatrix},$$

$$i=7,\ j=(1+5+3)\bmod 8=1,\ S_7\leftrightarrow S_1,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,5,6,1,7,3,4,2\end{pmatrix}.$$

2. Кездейсоқ тізбек үшін сандарды жазамыз.

$$i=1,\ j=(0+5)=5,\ S_1\leftrightarrow S_5,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,3,6,1,7,5,4,2\end{pmatrix},$$

$$t=(3+5)\bmod 8=0,\ Z_1=S_0=0,$$

$$i=2,\ j=(5+6)\bmod 8=3,\ S_2\leftrightarrow S_3,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,3,1,6,7,5,4,2\end{pmatrix},$$

$$t=(1+6)=7,\ Z_2=S_7=2,$$

$$i=3,\ j=(3+6)\bmod 8=1,\ S_3\leftrightarrow S_1,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 0,6,1,3,7,5,4,2\end{pmatrix},$$

$$t=(6+3)\bmod 8=1,\ Z_3=S_1=6,$$

$$i=4,\ j=(1+7)\bmod 8=0,\ S_4\leftrightarrow S_0,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 7,6,1,3,0,5,4,2\end{pmatrix},$$

$$t=(7+0)=7,\ Z_4=S_7=2,$$

$$i=5,\ j=(0+5)=5,\ S_5\leftrightarrow S_5,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 7,6,1,3,0,5,4,2\end{pmatrix},$$

$$t=(5+5)\bmod 8=2,\ Z_5=S_2=1,$$

$$i=6,\ j=(5+4)\bmod 8=1,\ S_6\leftrightarrow S_1,\ S=\begin{pmatrix}S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\\ 7,4,1,3,0,5,6,2\end{pmatrix},$$

$$t=(4+6)\bmod 8=2,\ Z_6=S_2=1.$$

Сонымен генерацияланған тізбек мынаған тең болады:

$$Z=(0,2,6,2,1,1).$$

Алынған тізбекті екілік түрде көрсетейік:

$$Z = (000\ 010\ 110\ 010\ 001\ 001).$$

3.11.2 Алгоритм RSA. Асимметриялық шифрлаудың көп тараған түрінің бірі –RSA алгоритмін қолданатын ашық кітпен шифрлау болыр табылады. Алгоритм тізбек ретінде көрсетілген модульдік арифметиканы қолдануға негізделген.

Жазылған ақпаратты қатеге тексеру:

Ашық кілтті қолдану арқылы ақпаратты шифрлаймын (e,n),:

$$s = m^e \bmod(n), \tag{3.14}$$
$$Y_1 = (41^7) \bmod(77) = 13,$$
$$Y_2 = (28^7) \bmod(77) = 63,$$
$$Y_3 = (26^7) \bmod(77) = 5.$$

Жабық кілтті қолдану арқылы ақпаратты қалпына келтіру(d,n),:

$$s = y^d \bmod(n), \tag{3.15}$$

мұндағы d - жабық деңгей,

$$S_1 = (13^{43}) \bmod(77) = 41,$$
$$S_2 = (63^{43}) \bmod(77) = 28,$$
$$S_3 = (5^{43}) \bmod(77) = 26.$$

S саны цифрлық жазу болып табылады.Ол жай ғана ақпаратқа қосылады және жазылған ақпарат <m,s> шығады.

Енді жазылған ақпараттың параметрін (яғни e және n) білетін әр адам жазудың қатесін тексере алады. Ол үшін теңсіздіктің орындалатынын тексеріп алған жөн:

$$h(m) = s^e \bmod(n), \tag{3.16}$$

$$h_1(m) = (41^7) \bmod(77) = 13,\ h_2(m) = (28^7) \bmod(77) = 63,\ h_3(m) = (26^7) \bmod(77) = 5;$$

ҚОРЫТЫНДЫ

Қазіргі кезде ақпаратты қорғау жалпы ұлттық мәселеге айналып отыр. Информациялық технологияның қарқынды дамуы және Интернеттің тез таралуы конфиденциалды ақпаратты қорғаудың әдістерін дамытуға, әсіресе криптографияның дамуына көп әсер етті. Мемлекеттің барлық салаларына қатысты ақпарат нақты саяси, материалдық және бағалылығы жағынан да құнды болып саналады. Ақпаратты қорғау мемлекеттің көзқарасымен алғанда қазіргі кезде өзекті мәселеге айналды және мемлекет алдындағы бірден-бір шешілуі қажет, ұлттық қауіпсіздіктің негізгі элементі ретінде қарастырылып отыр.

Бағалы ақпаратты құқықсыз немесе байқаусыз жағдайда бұзу, өзгерту немесе жою амалдарынан сақтап қалу үшін криптографиялық әдістер немесе скремблерлеу әдістері пайдаланылады. Криптографиялық әдістердің негізінде математика бөлімінде шешілген есептер қолданылады.

Ақпараттың қорғалуын қамтамасыз ету үшін біріншіден, туындаған проблеманың қаншалықты маңызды екенін білу керек, екіншіден, оны шешудің негізгі жолдары мен әдістерін бөліп алу қажет. Ақпаратты қорғау негізінде тек компьютерлік ақпарат емес, және басқа да көптеген аспектілер: фирманың бухгалтерлік есебі, шоттағы ақшаның саны, іспеттес серіктестер, келіссөздер мен жасалған келісімдер және тағы да басқалар жататынын есте сақтаған жөн.

Конфиденциалдық, басқарылмалы, ғылыми-техникалық, саудалық және басқа да бәсекелестерден басым түсуге жол ашатын ақпаратты қорғау қажет. Мұндай ақпараттың таралуы иесіне үлкен көлемде зиян әкелуі мүмкін.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Железняк В.К. Защита информации от утечки по техническим каналам: Учебное пособие.–Санкт - Петербург, - 2006.-45 с.

2 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001.-С.168-172.

3 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. - СПб.: Питер, 2001.-128с.

4 Петраков А.В., Лагутин В.С., Косариков А.В. Утечка и защита информации в телефонных каналах. –М.: РадиоСофт, 2011. -254 с.

5 Ершов В. А., Кузнецов Н.А. Мультисервисные телекоммуникационные сети. –изд-во МГТУ им. Н.Э. Баумана, 2003.– 155с.

6 Зайцев А.П., Шелупанова А.А. Технические средства и методы защиты информации.–М.: Машиностроение, 2009. - С.170 -192.

7 www.microsoft.com/rus/ /library/security/w2k_IPSecurity.html.

8 Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: 2001. - С.98 -112.

9 www.wikipedia.ru/gost34.310.2004/html.

10 Методы и средства сокрытия данных путем скремблирования: Методическое пособие для выполнения домашнего задания по выбору студента, 2012. -196с.

11 www.zortsorft.kz.

12 Исследование скремблеров и дескремблеров: Лабораторная работа. – Москва, 2010.- С.212 - 229.

13 www.ietf.org/html.charters/ipsec-charter.html.

14 Пожарная безопасность: Взрывоопасность. Справочник/Под ред. А.Н. Баратова – М.Химия, 1988. – С.142-138.

15 Анисимова И.Н., Стельмашонок Е.В. Защита информации. Учебное пособие. - 2002.-185 с.

16 Анисимова И.Н. Защита информации. Методические указания по выполнению лаб. работ для студентов всех специальностей. - 2001. -176 с.

17 Нечаев В.И. Элементы криптографии. Основы теории защиты информации.: Учеб.пособие для ун-тов и пед.вузов. - М.: Высшая школа, 1999. - 109 с.

18 Криптографические методы защиты информации: учебное пособие для студентов вузов, обучающихся по направлению "Прикладная математика и информатика" и "Информационные технологии";рец. В.С. Анашин, А.Б. Фролов, УМО по классическому.-М.: Академия, 2010. – С.256 - 259.

19 Как построить защищенную информационную систему./ Под науч. ред. Зегжды Д.П. и Платонова В.В. - СПб: Мир и семья, 1997. -145 с.

21 Маринченко А.В. Безопасность жизнедеятельности: Учебное пособие. – 2-е изд., доп. и перераб. – М.: Издательско-торговая корпорация «Дашков и К», 2007. -С.152-168.

24 Ермакова Т.В. Методика расчета экономической эффективности и привлекательности инвестиций (оценка инвестиционных проектов). Практическое пособие, - Алматы – 2005. -97 с.

25 Н.П. Резникова Маркетинг в телекоммуникациях. – М.: Эко–Трендз, 1998. -117 с.