ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Алынатын модульді алдын-ала анықтау арқылы сандарды модульге келтіруші құралды жобалау»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған:Қалқаман Әлімжан Тобы: СИБк-15-1
Ғылыми жетекші: т.ғ.к., профессор Тынымбаев С.Т.

Кеңесшілер:
Экономикалық бөлім бойынша:
т.ғ.к, профессор Аренбаева Ж.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Тәжібаев Д.Д
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
т.ғ.к., профессор Тынымбаев С.Т.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «07» 05 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Аскарова Н.Б
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «7» мамыр 2019 ж.
(қолы)

Пікір беруші:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 201__ ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент: Қалқаман Әлімжан
(аты-жөні)

Жобаның тақырыбы: Алынатын модульді алдын-ала анықтау арқылы сандарды модульге келтіруші құралды жобалау

2018 ж. «26» 10 №124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Сандарды есептелетін модуль бойынша келтірудің қолданыстағы тәсілдерін талдау негізінде сандарды алынатын модульге алдын ала келтіретін құрылғы ұсыну, оның ішінде жекеленген қайдықтарды қалыптастырушы негізінде тізбектелген, матрицалық және конвейерлік әрекет құрылғысын әзірлеу.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: R модулі бойынша Я санын есептеу процесімен және осыған кезінде қолданылатын құрылғылармен қысқаша таныстыру. Алынатын модуль бойынша саннан қалдықтарды қалыптастырудың қолданыстағы тәсілдерімен танысып, оларды талдау. Сандарды алынатын модуль бойынша келтіру үшін жекеленген қалдықтарды қалыптастырушы негізінде тізбекті, матрицалық және конвейерлік әрекет құрылғысын жобалап,

әзірлеу. Ұсынылатын жекеленген қалдықты қайнтастыруышының Artix-7 платасында Verilog жобалау тілінде іске асу.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі: 1 Бір сумматор және үш санауштыру схемаларынан тұратын жекеленген қалдықтарды қайнтастыруыш құрылғысының сұлбасы.
2. Тізбектей әрекет ету модулі бойынша сандарды келтірудің жоғарғы әрекет етуші құрылғысының құрылымдық сұлбасы.
3. Сандарды алынатын модуль бойынша келтірудің матрицалық әрекет ету құрылғысының құрылымдық сұлбасы
4. Алынатын модуль бойынша сандарды келтіру құрылғысының конвейерленген сұлбасы.

Негізгі ұсынылатын әдебиеттер: 1. Рябко Б.Я., Фионов А.И. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004
2. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. - Спб.: Питер, 2011
3. Айтхожаева Е.Ж., Тыныбаев С.Т. Аспекты аппаратного приведения по модулю в ассиметричной криптографии. - Алматы: Журнал вестник НАН РК №5
4. Тыныбаев С.Т., Шайкулова А.Н., Имангбаева А.Ж., Зуро А.А. Матричные схемы для приведения чисел по модулю. - Алматы: Вестник КазНИТУ, 2017

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Экономика бөлімі	Арепбаева Ж.Г.	04.03-27.05.19	
Негізгі бөлім	Тыныбаев С.Т.	02.02-07.05.19	
Өмір тіршілік қауіпсіздігі бөлімі	Торгаев Э.Э.	11.03-27.05	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	02.02.2019	
Рмодулі бойынша Ғ санын есептеу үдерісімен танысып, талдау	18.02.2019	
Модуль бойынша саннан қайта қалпына келтірудің қолданыстағы тәсілдерімен танысып, талдау	25.02.2019	
Сандарды алынатын модуль бойынша келтіру үшін тізбекті, матрицалық және конвейерлі әрекет ететін құрылғыларға талдау жасап, жобалау	20.03.2019	
Шекеленген қалдықты қалпына келтіру құрылғысын алгоритмдеп, ПЛИС платасына тізіп, іске қосу	25.04.2019	
Техникалық-экономикалық негіздеме	12.05.2019	
Өмір тіршілік қауіпсіздігі	27.04.2019	
Қорытынды	28.05.2019	

Тапсырманың берілген уақыты «28» қазан 2018 ж.

Кафедра меңгерушісі _____ (с.ғ.к. Бердібаев Р.Ш.)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (т.ғ.к. Тоныкбаев С.Т)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Қайқаман Ә.М.)
(қолы) (аты-жөні)

АҢДАТПА

Үш екілік сумматор негізінде құрылатын алынатын модульді алдын-ала анықтау арқылы сандарды модульге келтіруші құралдар белгілі. Мұндай құрылғылар, әсіресе матрицалық және конвейерлік схемаларды құру кезінде үлкен аппараттық шығындармен сипатталады. Бір екілік сумматор және үш салыстыру схемасының негізінде жекеленген қалдықтарды қалыптастырушыны жылдам әрекет еттіретін құрылым ұсынылып отыр. Бұл алынатын модульді алдын-ала келтіру арқылы әр түрлі разрядтылық сандарды модуль бойынша келтіру үшін аппараттық шығындарды айтарлықтай жеңілдетуге мүмкіндік береді. Ұсынылған жекеленген калдықтарды қалыптастырушы Xilinx компаниясының Artix-7 платасында Verilog жобалау тілінде іске қосу арқылы тексерілді.

АННОТАЦИЯ

Известны быстродействующие устройства для приведения чисел по модулю с предварительыс определением вычитаемого модуля, которые строятся на базе трех двоичных сумматоров. Такие устройства характеризуются большими аппаратными расходами, особенно при построении матричных и конвейерных схем. На основе одного двоичного сумматора и трех схем сравнения предлагается быстродействующий формирователь частичных остатков. Это позволяет значительно упростить аппаратные затраты для приведения различных разрядных чисел по модулю для предварительного определения вычитаемого модуля. Предложенный формирователь частичных остатков проверен с помощью запуска на платформе Artix-7 от компании Xilinx языком проктирования Verilog.

ABSTRACT

There are known high-speed devices for bringing the numbers modulo with a pre-determinant of the deductible module, which are built on the basis of three binary summators. Such devices are characterized by high hardware costs, especially in the construction of matrix and conveyor schemes. On the basis of one binary adder and three comparison schemes, a high-speed partial residue generator is proposed. This allows to simplify the hardware cost to bring the different bit numbers on the module for pre-determining the deductible of the module. The proposed shaper partial balances checked by running on the platform Artix-7 from the company Xilinx with Verilog language prektirovaniya.

Мазмұны

Кіріспе

Цифрлық экономика ғасырында елдің аса маңызды инфрақұрылымдарының ақпараттық қауіпсіздігін (АҚ) қамтамасыз ету проблемасы алдыңғы жоспарға ұсынылуда. Кибершабуылға үкіметтік инфрақұрылым объектілері, банктер, Атом және су электр станциялары және басқа да аса маңызды объектілер ұшырауы мүмкін. Бүгінгі таңда, сарапшылардың пікірінше, киберкеңістілік белсенді милитарияланып, мемлекеттер арасындағы қақтығыс аренасына айналуда. Соңғы уақытта өзінің функционалдық сипаттамалары бойынша киберқұрылыс класына жататын бағдарламалардың ерекше түрі пайда болды. Осындай қауіп-қатерлерді құруда елеулі қаржы ресурстарына ие мемлекеттік құрылымдар жиі тұр. Сондықтан киберкеңістікті қорғау кез келген мемлекеттің басты міндеті болып табылады.

Ақпаратты қорғаудың ең тиімді және кең таралған тәсілдерінің бірі қорғалатын ақпаратты (бастапқы мәтінді) криптографиялық алгоритмнің көмегімен шифрланған хабарламаға (Шифр мәтінге, криптограммаға) түрлендіруге негізделген шифрлеу болып табылады. Қазіргі таңда ақ саласында симметриялы және асимметриялы шифрлау жүйелері кеңінен ұсынылған.

Жалпы құпия (жабық кілт) жүйелер деп аталатын шифрлау симметриялық алгоритмдері деректерді шифрлау және шифрлеу үшін жалғыз кілтті пайдаланады. Жалпы Құпия ең кең қолданылатын алгоритм RC4, RC5, DES, үш есе DES, IDEA стандарты болып табылады. Симметриялық Алгоритмдер асимметриялық емес, есептеу ресурстарын едәуір аз пайдаланады. Әдетте, олар көлемді деректер ағындарын шифрлаудың жалғыз қолайлы тәсілі болып табылады. Жабық кілтті алгоритмдердің анық кемшілігі біреуге қорғалған хабарламаны жіберу үшін осы тұлғаға Жабық кілтті берудің қауіпсіз тәсілі болу қажет.

Ашық кілтті жүйе деп аталатын шифрлеудің асимметриялық алгоритмдері бірнеше кілттерді пайдаланады-ашық және жабық. Мұндай жүйелерде бір кілтпен шифрланған деректер тек оған жұптық кілтпен шифрленуі мүмкін. Бір кілтке ие бола отырып, оның бу кілтін алу мүмкін емес. Асимметриялық криптографияның жұмыс істеу принципі ашық кілтті кең қол жеткізуге ұсыну болып табылады, ал жабық кілт құпия сақталады. RSA, Эль-Гамал, Диффи-Хеллман, Фиата-Шамир, Саранчи және т. б. алгоритмдері кеңінен танымал.

Симметриялы алгоритмдермен салыстырғанда, асимметриялы есептеу ресурстарының едәуір санын тұтынады және сондықтан әдетте көлемді ағынды деректерді шифрлау үшін қолданылмайды. Ассиметриялық шифрлау SSH, OpenPGP, S/MIME және SSL/TLS сияқты әртүрлі хаттамаларда, сондай-ақ қорғалмаған желіге қауіпсіз қосылуды талап ететін әртүрлі жүйелерде қолданылады. Бұдан басқа, ол электрондық цифрлық қолтаңбада (ЭЦҚ)

деректер көзін куәландыруға және осы электрондық құжатты қолдан жасаудан қорғауға арналған электрондық құжаттың деректемесі пайдаланылады.

Шифрлау алгоритмін бағдарламалық, аппараттық немесе бағдарламалық-аппараттық тәсілмен жүзеге асыруға болады. Бірінші әдіс кезінде криптоалгоритм негізінде қандай да бір тілде бағдарлама жасалады, ол компьютердің орталық процессорында (ЦП) орындалады шифрлеу – бұл тікелей есептеу құрылғыларымен іске асырылатын шифрлау процесі, ал бағдарламалық-аппараттық құрамдастырылған тәсіл болып табылады.

Бағдарламалық іске асырудың артықшылықтары анық: шифрлаудың бағдарламалық құралдары оңай көшіріледі, олар пайдалану оңай, оларды нақты қажеттіліктерге сәйкес түрлендіру қиын емес, сондай-ақ шифрлаудың ең қол жетімді, бірақ бағасы болып табылады.

Бағдарламалық шифрлаудың кемшіліктері:

– егер шифрлау кілті компьютерде сақталса, шабуыл оның мәнін ашуға әкелуі мүмкін;

– бағдарламалық шифрлау орындалатын Операциялық жүйе вирустарға, іркілістерге және басқа да қауіптерге ұшырайды;

– өз кезегінде, сенімді бағдарламалық орындаудың криптографиялық алгоритмін аппараттық және бағдарламалық-аппараттық іске асыру.

Осы шифрлаушылардың негізгі артықшылықтары санына мыналар кіреді:

– үлкен жылдамдықпен ие-кез келген алгоритмді аппараттық іске асыру, соның ішінде криптографиялық, бағдарламалық іске асыруға қарағанда жоғары жылдам әрекетті қамтамасыз етеді;

– шифрлаудың сенімді кілттерін және ЭЦҚ қалыптастырады-кездейсоқ сандардың аппараттық сенсоры шын мәнінде кездейсоқ сандарды жасайды;

– алгоритмнің тұтастығын сақтайды-ол аппараттық іске асыруға кепілдік береді;

– шифрлеуші төлеміндегі кілттерді шифрлайды және сақтайды — бұл қолжетімділікті қиындатады;

– жүктейді кілттерді шифрующее құрылғы, электронды кілт Touch Memory (i-Button) және смарт-карталарды тікелей арқылы емес, жүйелі шину компьютердің ОЗУ – бұл мүмкіндігін жоққа шығарады ұстайтын кілттер;

– компьютерге қолжетімділікті шектеу жүйесін іске асыруға мүмкіндік береді;

– барлық есептеулерді орындау үшін арнайы процессорды қолданады-бұл компьютердің орталық процессорын жүктейді. Сондай-ақ, бір компьютерде бірнеше аппараттық шифрларды орнатуға болады, бұл ақпаратты өңдеу жылдамдығын арттырады;

– парафазалы шиналарды пайдалану мүмкіндігін қарастырады-бұл шифрпроцессорды жасау кезінде электромагниттік сәуленің тербелістері бойынша негізгі ақпаратты оқу қаупін болдырмайды;

– оқылмаған адам пайдалана алады-шифрлау құрылғысы қарапайым компьютерге немесе модемге қосылады, ал ОЖ-да шифрлау функцияларын байқаусыз енгізу-кәсіпқойлар жүзеге асыратын жеткілікті еңбекті қажетсінетін процесс.

Сондықтан мәліметтерді шифрлау құралдарының көпшілігі арнайы физикалық құрылғылар түрінде құрылады, онда деректерді шифрлауға дайындаудың барлық рәсімдері бағдарламалық түрде орындалады, ал деректерді шифрлау бойынша рутиндік есептеулер аппараттық түрде орындалады.

Шифрлау алгоритмінің криптотөзімділігі кілттердің ұзындығымен анықталады. Сондықтан ақпаратты сенімді қорғауды қамтамасыз ету үшін кілттердің ұзындығын арттыру керек, бұл өте үлкен сандарға күрделі және үлкен математикалық есептеулерге әкеледі. Бұл әсіресе ашық кілтті криптожүйеге тән (мысалы, RSA, Эль-Гамаль және Рабин сандар Ю309 өлшеміне жетеді). Осыған байланысты ашық кілтпен шифрлау алгоритмін аппараттық іске асырудың жылдам әрекет ететін схемаларын әзірлеу міндеті өзекті болып табылады.

Ашық кілтті криптожүйелер үшін базалық операция-бүтін сандарды р (AmodP) модулі бойынша дәрежеге тұрғызу. Бұл рәсім "көбейту", "квадратқа тұрғызу" және "модуль бойынша келтіру" операцияларын қолданумен іске асырылады. Сондықтан ашық кілтті криптожүйелердің өнімділігін арттыру үшін осы операцияларды орындауды жылдамдататын алгоритмдерді әзірлеу қажет.

Көбейту және квадратқа тұрғызу операцияларын жылдамдату үшін екілік сумматорлардың массивтерін, Браун матрицасын, Уоллес ағашын, Дадда есептегіштерін, систолалық және ведможительдерді және басқа да әдістерді пайдалануға болады. Алайда, бұл көбейтгіштер мен квадраторлар әртүрлі кластағы компьютерлерге арналған көбейткіш блоктарды құруда кеңінен қолданылған "аз разрядты" операндтарды есептеу кезінде тиімді.

Жоғарыда аталған жұмыстарды талдау әр түрлі класқа есептер үшін жылдам әрекет ететін бүтін көбейтгіштер мен квадраторлардың теориялық және практикалық сұрақтары жақсы пысықталғанын көрсетеді, оны модуль бойынша келтіру операциясы туралы айтуға болмайды.

Белгілі болғандай, бөлу операциясы барлық арифметикалық операциялардың ең көп еңбек сыйымдылығы болып табылады. Модуль бойынша келтіру операциясы р модулі бойынша санды бөлуден қалдықты алу болып табылатындықтан, ол сондай-ақ іске асыру кезінде үлкен есептеу ресурстарын талап етеді. Бұдан басқа, модуль бойынша дәрежеге көтеруді жеделдету үшін, кейіннен өте үлкен санды р модуліне бөле отырып, бірнеше рет көбейтудің орнына, жаңа туындының әрбір қадамында модуль бойынша келтірумен көп қадамдық тізбекті көбейту пайдаланылады, бұл осы операцияны бірнеше рет қайталауға әкеп соғады.

Жоғарыда айтылғандарды ескере отырып, модуль бойынша келтіру операциясын орындаудың аппараттық тәсілінің жылдам әрекет ететін

сұлбаларын әзірлеу ассиметриялық криптоалгоритмдерді іске асыратын шифропроцессорларды құруда негізгі проблема болып табылады.

Есепте жобаның күнтізбелік жоспарына сәйкес келесі мәселелер қаралады:

– модуль бойынша сан қалдықтарын қалыптастырудың әртүрлі тәсілдерін талдау және олардың негізгі параметрлері бойынша салыстырмалы бағасын жасау, ішінара қалдықтарды қалыптастыру уақыты бойынша және қалдықты қалыптастыру үшін аппараттық шығындар бойынша;

– теріс қалдықтарды бұғаттаумен сандарды бөлу алгоритмі негізінде сандарды модуль бойынша келтірудің матрицалық және конвейерлік құрылғылары;

– Алынатын модульді алдын-ала анықтау арқылы сандарды модульге келтіруші құралды әзірлеу;

– Ұсынылатын сандарды модульге келтіруші құрылғысын ПЛИС арқылы алгоритмдеу;

– Жасау барысындағы өмір тіршілік қауіпсіздігін және құрылғының техникалық-экономикалық тұрғыдан шығыны мен бағасын есептеу.

1 Тақырыптық салаға шолу

1.1 P модулі бойынша A санын есептеу процесі

Компьютерлік жүйелер мен желілердегі деректер қауіпсіздігі проблемасын шешудің ең сенімді тәсілдерінің бірі криптографиялық алгоритмдердің көмегімен бастапқы мәтінді шифрлеу жолымен ашық мәтінді шифртекстке айналдыруды қамтамасыз ететін криптографиялық қорғау болып табылады: симметриялық асимметриялық шифрлау алгоритмдері. Криптографиялық Алгоритмдер арнайы криптографиялық құрылғыларда (криптопроцессорларда) бағдарламалық, аппараттық пли бағдарламалық-аппараттық түрде іске асырылады.

Криптографияны дамытудың қазіргі кезеңінде асимметриялық криптоалгоритмге ерекше көңіл бөлінеді. Ассиметриялық шифрлауда кілттердің жұптарын пайдалану құпия кілттерді беру проблемасын алып тастайды. Екі негізгі қорғау құралдарын кеңінен пайдалану осы электрондық құжатты қолдан жасаудан қорғауға арналған электрондық құжаттың деректемесі болып табылатын электрондық цифрлық қолтаңбамен де байланысты. 1997-да ANSI X9 стандарты әзірленді. 30 Digital Signature Standard қолдайтын (сандық қолтаңба стандарты). Кейінірек ANSI X9 стандарты енгізілді.31, онда RSA сандық қол қоюларына екпін жасалған. Бұл нақты қалыптасқан жағдайға, атап айтқанда, қаржы мекемелері үшін көп пайдасы тиетіні көпшілікке мәлім.

Ашық кілтті криптожүйелер жиі шифрлеу, кейіннен симметриялық криптожүйенің құпия кілтін шифрлеу үшін қолданылады. Асимметриялық криптожүйе хабарламаларды шифрлау және жіберу үшін қолданылады. Ашық кілтті криптожүйелер жылдамдықтың төмендігінен қолданылмайды, өйткені шифрлеу кезінде дешифрлеу кезінде өте үлкен сандарды модуль бойынша дәрежеге тұрғызудың күрделі және үлкен процедуралары қолданылады. Бұл р модулі бойынша дәрежеге сандарды тұрғызу жылдамдығының проблемасына криптографияның теоретиктері мен практиктерінің жоғары назары түсіндіріледі.

Шифрлаудың аппараттық құралдары мамандандырылған жабдық болып табылады. Олар бағдарламалық шифраторлардан қымбат және іске асыру қиын, бірақ бағдарламалық құралдардың алдында бірқатар маңызды артықшылықтарға ие: жоғары өнімділік, қарапайымдылық, қорғалу және т.б..

Ақпаратты шифрлаудың аппараттық құралдарының үш түрі бар:

– шифрлау модульдері (олар кілттермен барлық жұмысты өз бетінше орындайды);

– байланыс арналарында шифрлау блоктары;

– дербес компьютерлерге орнату үшін кеңейтудің шифрлау платалары.

Негізгі кемшілігі ассиметриялы криптоалгоритмов болып табылады төмен жылдамдығы, өйткені рәсімдер шифрлау және дешифрлау пайдаланылады ауқымдылығы арифметикалық есептеулер үстінен сандармен жоғары дәрежелі (тұрғызу дәрежесі бойынша модуль). Сондықтан асимметриялы криптоалгоритмдердің басты проблемасы – бұл сандарды модуль бойынша дәрежеге салуды жеделдету мәселесі. Бұл проблеманы шешудің бір жолы - сандық көбейту, квадратқа тұрғызу, модуль бойынша келтіру-сандарды модуль бойынша дәрежеге жылдам тұрғызудың базалық операцияларын орындау үшін аппараттық құралдарды пайдалану болып табылады.

Қазіргі уақытта көбейтуді жеделдетудің әртүрлі әдістерін қолданатын жылдам әрекет ететін бүтін көбейтгіштер мен квадраторларды әзірлеуде үлкен тәжірибе жинақталған. Көбейтуді жеделдету әдістері аппараттық және логикалық болып бөлінеді.

Жылдам әрекет етуші - көбейту жылдамдығының аппараттық әдістері.

Бұл жағдайда көбейту операциясын жеделдету:

– ішінара туындыны параллель қалыптастыру (IT);

– қосу санын азайту;

– IT қалыптастыру кезінде тасымалдардың таралу уақытын азайту.

IT параллельді есептеу барлық көбейтгіштерде бар, онда көбейту аппараттық іске асырылған. Жиынтықтау операциясын іске асыруға байланысты олар матрицалық және ағаш тәрізді болып бөлінеді. Екі жағдайда да қосу өзара байланысты бір реттік сумматорлар массивінің көмегімен жүзеге асырылады.

Матрицалық құрылымдарда сумматорлар матрица түрінде, ал ағаш тәрізді құрылымдарда - сол немесе басқа түрдегі ағаш түрінде ұйымдастырылған.

Матрицалық көбейту кезінде екі n-биттік екілік сандардың айырмасынан нәтижені A және B таңбасыз өрнектермен сипаттауға болады:

$$C = A * B = \left(\sum_{i=0}^{n-1} a_i * 2^i\right) * \left(\sum_{j=0}^{n-1} b_j * 2^j\right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j * 2^{i+j};$$

(1.1)

Көбейту сумматорлар матрицаларының көмегімен N-разрядты ішінара туындылардан биттердің параллельді қалыптасуына әкеледі. Мұндай схема Браун көбейткіш ретінде белгілі.

Матрицалық көбейтгіштерде кідірісті қысқарту ағаш тәрізді құрылым бойынша құрылған схемаларда мүмкін. Егер матрицалық көбейтгіштерде ішінара туындыларды N қосу үшін сумматорлардың N-жолдары талап етілсе, онда ағаш тәрізді схемаларда сумматорлар сатыларының саны log2n пропорционалды. Бұл IT сомасын есептеу уақытын қысқартуға әкеледі. Алайда, мұндай көбейтінділерді жүзеге асыру кезінде бірдей салмағы бар разрядтарды біріктіру үшін қосымша байланыстар қажет, себебі кристалдағы схемамен алып отырған алаң ұлғаюы мүмкін [1].

Қазіргі уақытта IT сомасын алудың үш ағаш тәріздес схемасы ең көп таралған: Уоллес ағашы, Дадда ағашы және төңкерілген сатылы ағаш.

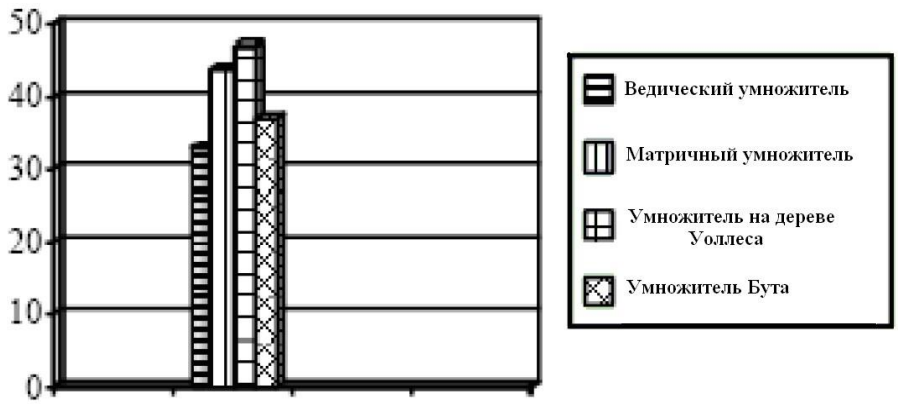
Уоллес схемасы ең жылдам болып табылады, бірақ оның құрылымы ең аз тұрақты, себебі басқа ағаш тәрізді құрылымдарға артықшылық беріледі. Схема негізінен үлкен разрядтық сандарды жылдам көбейту үшін қолданылады. Шағын разрядтық сандарды көбейту кезінде Д'адда схемасы жиі қолданылады. Осы көбейтгіштің негізінде аз сумматор санымен Уоллес ағашы жатыр. Уоллес пен Д'адд сызбасының жалпы кемшілігі – құрылымның жүйеленбеуі. Төңкерілген баспалдақтың схемасы (overturnedstairs) ағаш тәріздес құрылымды тұрақты жасауға талпыныстардың бірі болып табылады, бұл интегралды орындаудағы оның іске асырылуын жеңілдетуге мүмкіндік береді. 1.1-кестеде қолданылатын логикалық элементтердің саны бойынша ең үнемді матрицалық көбейтгіш болып табылады, содан кейін Уоллес ағашындағы көбейтгіш.

Кесте 1.1 – Логикалық элементтер саны бойынша салыстыру нәтижелері

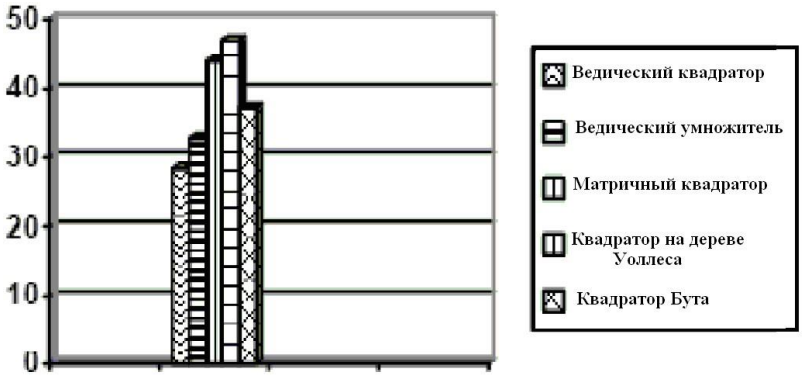
Ведикалық көбейткіш	Матрицалық көбейткіш	Уоллес ағашындағы көбейткіш	Бут көбейткіші
799	559	762	905

1.1 және 1.2-суреттерде салыстырмалы талдау үшін, сәйкесінше, шартты бірліктерде әр түрлі көбейтгіштер мен квадраторлардың кідіріс уақыты келтірілген. 1.1 және 1.2-суреттер бойынша ең жылдам әсер ететін ведикалық көбейтгіштер мен квадраторлар екенін айту қиын емес.

Аппараттық көбейтгіштер енгізілетін сандардың санына шектеледі. Жоғары разрядты көбейтуші кіші разрядты модульдерден, көбейту операциясының рекурсивті декомпозициясын құру арқылы алуға болады. Мысалы, 8*8 бит көбейтгішін құру үшін 4*4 төрт модульді қолдануға болады және соңғы нәтижені қалыптастыру үшін қосымша сумматорлар қажет. Модульдерді ROM бойынша жүзеге асыруға болады. Содан кейін мұндай көбейту кестелік-алгоритмдік көбейту деп аталады. Егер қосымша сумматорлар модуль ішінде кіріктірілген болса, онда оларды көбейткіш-жиынтықтаушы блоктар (КЖБ) деп атайды [2].



Сурет 1.1 – Әр түрлі көбейтгіш түрлерін салыстыру диаграммалары



Сурет 1.2 – Әр түрлі квадрат түрлерін салыстыру диаграммалары

Матрицалық және ағаш тәрізді көбейтушілерде өнімділіктің тағы бір әлеуеті бар – конвейеризация мүмкіндігі. Конвейерлік ұйым кезінде көбейту процесі аяқталған кезеңдердің дәйектілігіне бөлінеді. Көбейту кезеңдерінің әрқайсысы конвейердің өз сатысында орындалады, және де барлық сатылар параллель жұмыс істейді. I сатыда алынған нәтижелер конвейердің (i+1) сатысына одан әрі өңдеуге беріледі. Сатыдан сатыға ақпарат беру олардың арасында орналастырылатын буферлік жады арқылы жүзеге асырылады. Конвейер схемасы матрицалық және ағаш тәрізді көбейтушілерге оңай қолданылуы мүмкін.

Жоғары разрядтық көбейтгіштер мен квадраторларды іске асырудың жоғарыда қарастырылған әртүрлі тәсілдері ассиметриялық криптоалгоритмдердің базалық операциялары болып табылатын көбейту және квадратқа тұрғызу операцияларын орындауды жеделдетуге мүмкіндік береді [3].

Асимметриялық криптоалгоритмдердің келесі базалық операциясы P модулі бойынша келтіру болып табылады.

Жұмыста анықталған сипатты белгілердің негізінде модуль бойынша келтіру құрылғыларының жіктелуінің мынадай түрлері ұсынылды:

– параллель және тізбекті;

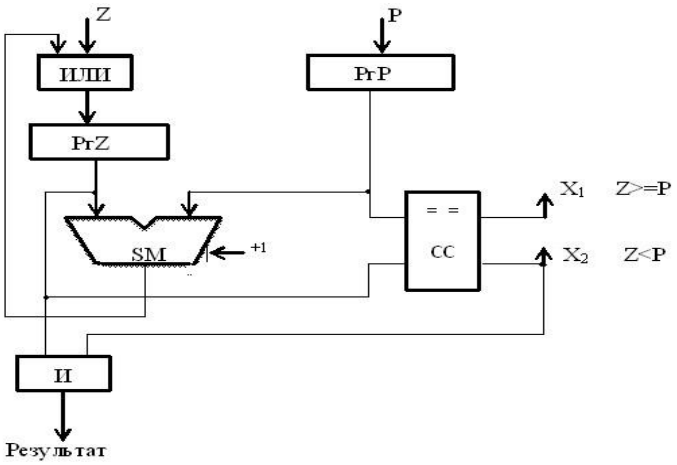
– бір актілі және көп актілі;

– басқарушы блоктың болуы немесе болмауы бойынша;

– қолданылатын есептеу жүйесі бойынша.

1.3-суретте модуль бойынша келтіру құрылғысының сұлбасы келтірілген, мұнда қалдық екі санның туындысын қалыптастырғаннан кейін Z бастапқы келтірілген саннан модулді бірнеше рет азайту жолымен анықталады. Құрылғы тізбекті (*), көп активті (**) циклдік, микро бағдарламалы, екілік есептеу жүйесі қолданылады. Операция микробағдарламаның басқаруымен сандар үстінде жүргізіледі. Z ретінде $z=X*У$ немесе $Z=X^2$ сандарының туындысы болуы мүмкін. РгZ және РгР регистрлеріне қабылдағаннан кейін Z операндасы және P модулі сәйкес, олар салыстыру схемасында (СС) салыстырылады. Егер бұл ретте $Z < P$ ($X^2=1$)

болса, онда схеманың шығуының нәтижесі ретінде РгZ мазмұны беріледі. Z>=P кезінде Z сумматорда P шегеріледі SM: инверсиялық шығулардан РгР түседі –P және сумматордың кіші разрядының үшінші кіруіне +1 беріледі. Бұл ретте, РгZ микрооперациясы орындалады: $РгZ = РгZ +(- РгР)_{д.к.}$, яғни азайту қосымша кодта қосумен ауыстырылады және қалдық ЕСЖ жазылады(1.3-сурет).



Сурет 1.3 – Модульді тізбекті шегерумен модуль бойынша келтіру сызбасы

Содан кейін РгZ жаңа мәні РгР мазмұнымен салыстырылады. Және барлық циклдік мәндер РгZ мәнінен (X^2=1) аз болғанша қайталанады. Мысалы, P=33 және Z=1080 кезінде, азайту саны 32 құрайды. Кесте аппараттық шығындар бойынша оңтайлы болып табылады, бірақ баяу әсер етеді.

Модуль бойынша келтірудің жылдам әрекет ететін біртактілі құрылғысын алу үшін Z–P, Z-2P, Z-3P, Z-4P және т. б. бір мезгілде есептеуге болады. Сонда Z бөлігінен P div = 4-ке бөлінген бүтін бөлік және келесі шегерімдерді орындау қажет:

C_1=Z-P=33_{10}-7_{10}=0.100001_2-0.000111_2 = 0.100001_2 + 1.111001 = 10.011010_2 = + 26_{10} ;

C_2=Z-2P=33_{10}-14_{10}=0.$100001_2$0.001110_2=0.100001_2+1.110010_2= 10.010011_2 = +19_{10};

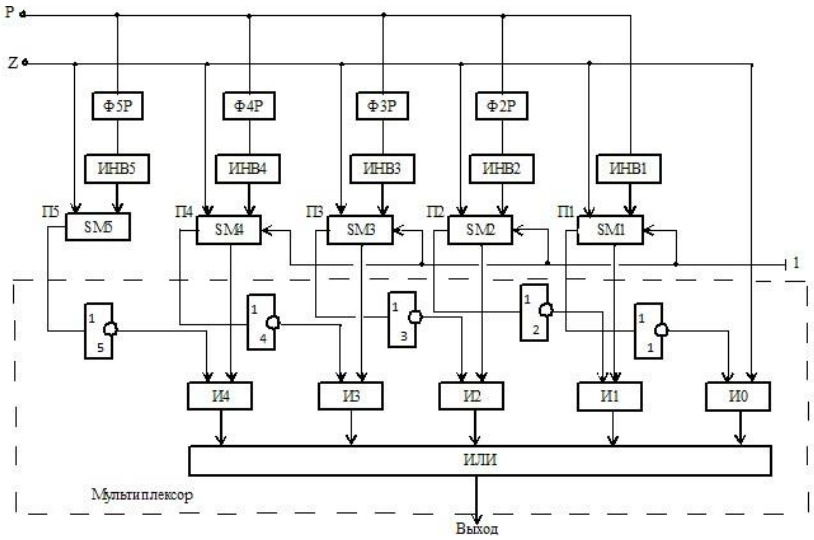
C_3=Z-3P=33_{10}-21_{10}=0.100001_2-0.010101_2=0.100001_2+1.101011_2=10.001100_2 = +12_{10};

C_4=Z-4P=33_{10}-28_{10}=0.100001_2-0.011100_2=0.100001_2+1.100100_2=10.000101_2 = +5_{10};

C_5=Z-5P=33_{10}-35_{10}=0.100001_2-0.100011_2=0.100001_2+1.011101_2=01.111110_2 = --2_{10}.

Алынған С1÷С4 мәндерін р модулімен салыстыру қажет және Сі<Р кезінде І-ден сұлба шығысына модуль бойынша келтіру нәтижесі ретінде беру қажет. Бұл құрылғы құрамына бір уақытта жұмыс істейтін төрт салыстыру сұлбасын қосуды талап етеді. Төрт салыстыру сұлбасын жою үшін қосымша 5-тен есептеледі. Мысалы, С1, С2, С3, С4 есептеу кезінде оң нәтиже алынған. Бұл ретте белгі разрядтарынан П1=П2=П3=П4=1 ауысулар пайда болады. С5 есептеу кезінде теріс сан (-210) және П5=0 таңбалық разрядынан ауысу алынады. П5 сигналының көмегімен С4 мәні бар, ол нәтиже болып табылады, модуль бойынша келтіру блогының шығысына жіберу мүмкіндігі бар.

Осы тәсіл қолданылатын модуль бойынша келтірудің бір актілі блогының схемасы суретте көрсетілген. Р еселік мәні (2Р, 3Р, 4Р, 5Р) формулярларда қалыптасады (Ф2Р, Ф3Р, Ф4Р, Ф5Р). Инверсиялық р, 2Р, 3Р, 4Р, 5Р мәндерін алу үшін инверторлар ИНВ1, ИНВ2, ИНВ3, ИНВ4, ИНВ5 талап етіледі. ZiP азайту екілік сумматорларда SM1=SM5 жүргізіледі, олардың алғашқы кіруіне Z мәні беріледі, ал екінші кіріске Р, 2Р, 3Р, 4Р, 5Р инверсиялық мәндері беріледі(1.4-сурет).



Сурет 1.4 – Модуль бойынша келтірудің бір актілі блогының сызбасы

Қосылу сәтінде адъюнкттардың төменгі реттік саны +1 (қосымша код үшін -Р) беріледі. Топтаманың соңында Р1, Р2 ... Р5 және қалдықтары әр қосқыштың шығуында қалыптасады. Егер қалған Сі = Z-iP > P болса, Рі = 1, әйтпесе Рі = 0. Әр SMi тартқыштың шығуында Сі, Рі және Рі + 1 кірістері бар тізбек бар. Пи + 1 инверттелген оң сигнал Рі = 1 болса, Сі нәтижесін шығуына мүмкіндік береді. Осы мақсатта тізбектерді шығарып аламын және ОР схемасымен біріктіріледі және оның шығуында қалған қалдықтың мәні - модульдің азаюының нәтижесі пайда болады. Инверторлар, схемалар Ал, шығу схемасы немесе мультиплексорға арналған схема. SM1 шығысындағы Р> Z кезінде П1 = 0 сигналы және сәйкесінше И0 схемасы арқылы Z мәні мультиплексордың шығуына беріледі.

Бұл схема мен және P арақатынасының аз мәндерінде жылдам әсер ететін және өте тиімді болып табылады. Мысалы, Z=3020 және P=55, div=54 кезінде. Іске асыру үшін блок келтіру модуль бойынша талап етіледі 54 схемасын алу мәні i*P, 55 двоичных сумматоров орындау үшін операциялар Ci= Z-iP [3].

Бірінші қарастырылған сұлба бойынша келтірілген сұлба өте қарапайым және үлкен аппараттық шығындарды талап етпейді, бірақ тез әрекет ету өте төмен.

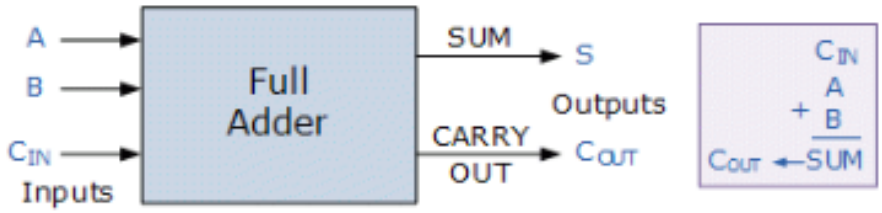
Екінші кесте тез әрекет ететін, бірақ аппараттық шығындар өте жоғары. Осыдан модуль бойынша келтіру блоктарын одан әрі жетілдіру бойынша зерттеу бағытын ескеру қиын емес.

Бірінші схемада аппараттық артықшылық блогының құрамына ақылға қонымды шектерде енгізу жолымен жылдам әрекетті арттыру қажет, ал екінші схемада аппараттық шығындарды азайту қажет. Бұл үшін модуль бойынша келтірудің жаңа алгоритмдерін және осы алгоритмдерді іске асыратын жаңа схемотехникалық шешімдерді әзірлеу қажет [4].

1.2 Жұмыс кезінде қолданылатын құрылғылар

1.2.1 Екілік сумматорлар

Екілік сумматорлар-екі екілік санды қосу үшін қолданылатын жартылай сумматорлар және толық сумматорлар түріндегі арифметикалық схемалар(1.5-сурет).

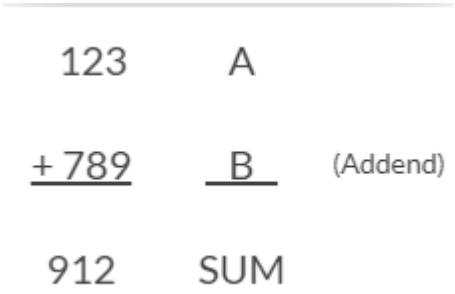


Сурет 1.5 – Екілік сумматордың сызбасы

Екі немесе одан да көп екілік сандарды бірге қоюға мүмкіндік беретін бірнеше негізгі Логикалық элементтерді пайдалана отырып салынуы мүмкін тағы бір кең таралған және өте пайдалы комбинациялық логикалық схема екілік сумматор болып табылады.

Екілік қосқыштың негізгі схемасы стандартты И және Исключающий ИЛИ элементтерінен жасалуы мүмкін, бұл А және В екілік бинарлық екі сандарын қосуға мүмкіндік береді.

Осы екі санды қосу қосылым сомасы деп аталатын шығуды және екінші шығыс, деп аталатын CARRY немесе Carry-out, (C_{OUT}) бит екілік қосу ережелеріне сәйкес. Арифметикалық және есептеу сұлбаларында екілік сумматор үшін негізгі қолданулардың бірі. Төменде екі екілік сандардың қарапайым қосындысын қарастырайық(1.6-сурет).



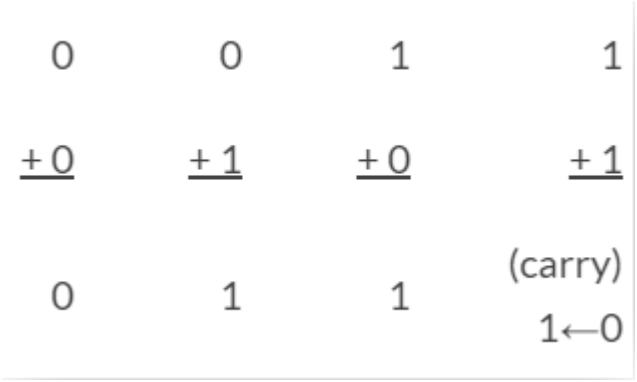
Сурет 1.6 – Екілік сандардың қарапайым қосындысы

Мектептегі математика сабақтарынан біз сандардың әрбір бағанасы оң жағынан бастап бірге қалыптасатынын және әрбір санның бағандардағы жағдайына байланысты өлшенген мәні бар екенін білдік.

Әрбір бағанды қосқанда, Егер нәтиже 10-нан артық немесе тең болса, базалық Сан жасалады. Бұл тасымал содан кейін келесі бағанды қосу нәтижесіне қосылады және т.б., мектеп математикасын қарапайым қосу, сандарды қосу және тасымалдау.

Екілік сандарды қосу-бұл ондық сандарды қосу үшін бірдей идея, бірақ бұл жолы carry нәтижесі кез келген бағанада "2" - ден артық немесе тең болғанда ғана жасалады. Басқаша айтқанда, 1 + 1 тасымал жасайды.

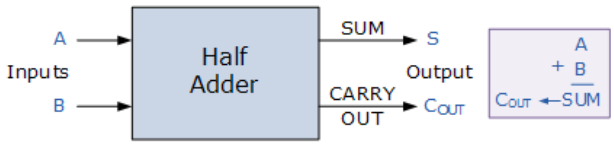
Екілік қосылым жоғары денарлық қосылым үшін, екілік санда "1" ең үлкен саны бар екі сан ғана бар екенін қоспағанда, осы негізгі ережелер қажет. Осылайша, a Carry екілік сандарды қосқан кезде, "сумма" екіге тең немесе одан көп (1+1) кезде жасалады және бұл қосу үшін келесі бағанға берілетін кез келген кейінгі қосу үшін "CARRY" биті болады. Төменде бірбеттік қосуды қарастырайық(1.7-сурет).



Сурет 1.7 – Екі битті екілік қосу

2 жалғыз бит бірге қосылған кезде, қосу "0+0", "0+1" және "1+0" сіз "1+1" Соңғы бағанына жеткенше не "0" немесе "1" әкеледі, онда сомасы "2" тең. Бірақ екі саны екілік емес, бірақ 2 екілік 10, басқа сөзбен айтқанда, сома үшін нөл плюс қосымша бит тасымалдау.

Сонда қарапайым сумматордың жұмыс істеуі үшін екі шығыс, теңдеу және бит тасымалдау (C) сомасын (S) беретін екі кіріс деректер қажет(1.8-сурет).



Сурет 1.8 – Екілік сумматордың блок-схемасы

Қарапайым 1 биттік қосу мәселесі үшін жоғары нәтижелі тасымалдау биті елеусіз болуы мүмкін, бірақ сіз осы екі битті қосуға қатысты тағы бір нәрсе байқаған шығарсыз элементтің сомасына ұқсас олардың екілік қосу сомасы немесе. Егер біз А және В сияқты екі битті белгілесек, онда қорытынды ақиқат кестесі екі биттің жиынтығы болады, бірақ соңғы тасымалсыз [4].

1.2.2 Сандық компаратор

Сандық компаратор – екі екілік санның мәнін салыстыру үшін қолданылатын тағы бір өте пайдалы комбинациялық логикалық схема.

Цифрлық немесе екілік компараторлар стандартты және, не стробтардан жасалған, олар өзекшелерінде бар кіріс сигналдарын салыстырады және сол кіріс сигналдарының жағдайына байланысты шығуды жүргізеді.

Мысалы, екілік сандарды қосу және азайту мүмкіндігімен қатар, біз оларды салыстыра аламыз және А енгізуінің шамасы В, В және т.б. кірісіндегі мәннен аз немесе тең бола ма екенін анықтауымыз керек. Сандық компаратор бұл бульдық алгебра принциптерінде жұмыс істейтін бірнеше логикалық элементтерді қолданады. Цифрлық компараторлардың екі негізгі түрі бар:

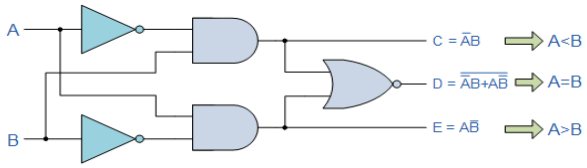
– ұқсастықтың компараторы – А=Б, немесе А=Б=1 (жоғары) немесе А=Б=0 (төмен) кезде тек бір шығу терминалы бар сандық компаратор);

– шаманың компараторы – 3 шығу терминалы бар сандық компаратор шама компараторы, А = Б қарағанда, А > Б > және А қарағанда көп.

Цифрлық компаратордың мақсаты - айнымалылар немесе белгісіз сандарды салыстыруға, мысалы, В (В1, В2, В3, ... Вn, В1, В2, В3, Вn, т.б.) және салыстыру нәтижесіне байланысты шартты немесе шығу туы жасайды. Мысалы, екі 1-биттік кірістері (А және В) тұратын мәндер компараторы бір-бірімен салыстыра отырып, келесі үш шығу шарттарын шығарады: A > B, A = B, A < B.

Нені білдіреді: А көп В-дан, А мен В тең, немесе А В-дан аз.

Біз екі айнымалыны салыстырғымыз келсе және кез келген үш шартты орындау кезінде нәтиже алғыңыз келсе, бұл пайдалы. Мысалы, колваның белгілі бір санына жеткенде есептеуіштен шығарыңыз. Төменде қарапайым 1 биттік компаратор қарастырайық(1.9-сурет).



Сурет 1.9 – Сандық компаратордың 1-биттік схемасы

Сонда 1 биттік сандық компаратордың жұмысы келесі ақиқат кестесінде келтірілген(1.10-сурет).

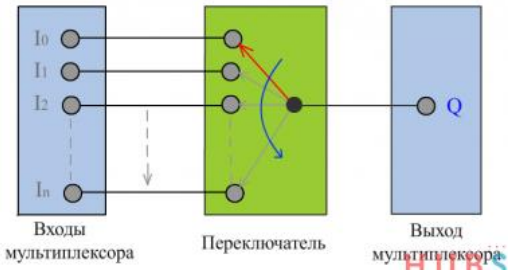
Inputs		Outputs		
B	A	A > B	A = B	A < B
0	0	0	1	0
0	1	1	0	0
1	0	0	0	1
1	1	0	1	0

Сурет 1.10 – Сандық компаратордың шындық кестесі

Сіз жоғарыда берілген ақиқат кестесінен компаратордың екі ерекше ерекшеліктерін байқай аласыз. Біріншіден, схема екі "0" немесе екі "1" арасында ажыратылмайды, себебі шығу A = B екеуі де тең болғанда немесе A = B = "0" немесе A = B = "1" болып шығады . Екіншіден, A = B үшін Шығыс шарты жалпы қабылданған логикалық элементтің шарттарына, Exclusive-NOR немесе Ex-NOR (эквиваленттілік) функциясына ұқсас, әрбір n-разрядтағы: Q = A*B [4].

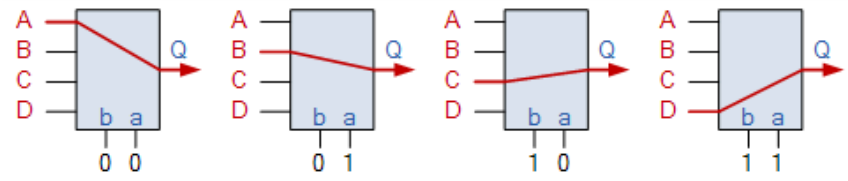
1.2.3 Мультиплексор

Мультиплексор – берілген цифрлық кодқа сәйкес бірнеше кірісті жалғыз шығу үшін қосатын қосқыш. Шын мәнінде, мультиплексорлардың екі түрі бар: аналогтық және цифрлық, аналогты далалық әсерлі транзисторларға орнатылады және екі бағытта да сигналды жібереді, ал таңдалған кіріс сигналы сигнал шығу сигналын қайталайды(1.11-сурет).



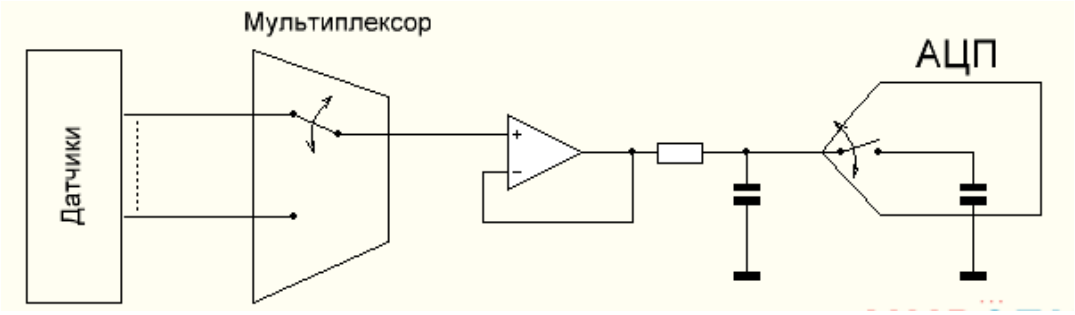
Сурет 1.11 – Аналогтық мультиплексордың сызбасы

Жоғарыда жазылғандай арнаны таңдау төменде суретте көрсетілгендей берілген сандық кодқа сәйкес жүзеге асырылады(1.12-сурет).



Сурет 1.12 – Аналогтық мультиплексордың сандық коды

Келесі жағдайды елестетейік, бізде АЦП және бірнеше аналогтық датчиктер бар, ол ақпаратты өңдеуге тиіс. АЦП тек бір ғана, ал датчиктер көп болғандықтан, оларға тек кезек бойынша қызмет көрсете алады, ал оған бұл мультиплексор көмектеседі(1.13-сурет).

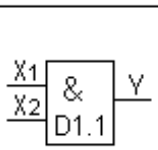


Сурет 1.13 – Мультиплексордың АЦП-мен жұмысы

Қалыпты кернеу бөлгішін және мультиплексорды пайдалана отырып, сигналды дұрыс санға қайта әлсіретуге болады. Ал қосып мультиплексор бірнеше резисторларды кері байланыс күшейткіштің салынған ОУ болады күшейту сигнал керекті саны [4].

1.2.4 Логикалық функция

"И" (AND) – қосу функциясы (егер барлық кірістерде бірлік болса, онда шығуда бірлік болады, әйтпесе, егер ең болмағанда бір кірісте нөл болса, онда шығуда нөл болады). Алгебра-логикада элемент "және" немесе “конъюнктор” деп аталады(1.14-сурет).



X1	X2	Y
0	0	0
1	0	0
0	1	0
1	1	1

Сурет 1.14 – 2И логикалық функциясының шындық кестесі

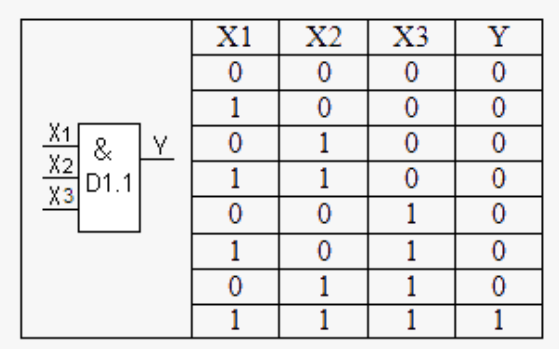
"2И" элементінің атауы оның екі кірісін білдіреді және ол "И"функциясын орындайды. Схемада тікбұрыштың ішінде микросхема " & " белгісі сызылады, бұл ағылшын тілінде "AND" (орыс тіліне аударылғанда И) дегенді білдіреді.

Шындылық кестесі бойынша "И" элементінің шығуында тек бір жағдайда ғана логикалық бірлік болады — екі кіріс кезінде логикалық бірлік болады. Егер ең болмағанда бір кіру нөл болса, онда шығу нөл болады.

Сізге "2И", "3И", "4И" және т.б. деген түсінікті болу үшін "3И" элементінің ақиқаттық кестесі мен графикалық белгілеуді келтіремін.

Шындылық кестесі бойынша "3И" элементінің шығуында тек барлық үш кіріс кезінде логикалық бірлік болған жағдайда ғана логикалық бірлік

болады. Егер бір кіруде логикалық нөл болса, онда элементтің шығуында да логикалық нөл болады. "3И" функциясын орындайтын ең көп таралған ТЛ микросхемасы ішінде "3И" үш элементі бар К555ЛИ3 микросхемасы болып табылады(1.15-сурет).

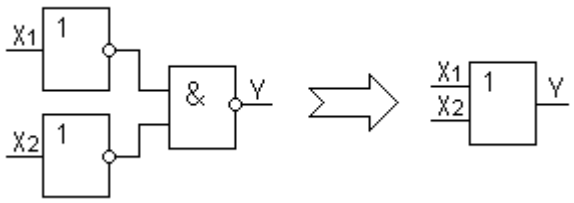


X1	X2	X3	Y
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	0
0	0	1	0
1	0	1	0
0	1	1	0
1	1	1	1

Сурет 1.15 – 3И логикалық функциясының шындық кестесі

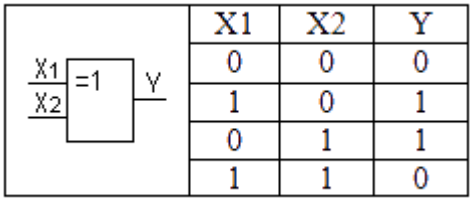
"ИЛИ" (OR) – таңдау функциясы (егер ең болмағанда бір кіріске – бірлік, онда шығуда – бірлік, әйтпесе шығуда әрдайым нөл болады). Алгебра-логикада элемент "или" немесе "дизъюнктор" деп аталады.

Бізге сызбада(1.16-сурет) "2ИЛИ" функциясын орындайтын элемент қажет деп болжаймыз, бірақ бізде тек "емес" және "2И-емес" элементтері бар, онда "2ИЛИ" функциясын орындайтын схеманы жинауға болады.



Сурет 1.16 – 2ИЛИ логикалық функциясының сызбасы

"Исключающее ИЛИ" (XOR) – екі кіріс теңсіздігінің функциясы (егер элементтің екі кірісінде бірдей сигналдар болса, онда шығу кезінде – нөл, әйтпесе шығу кезінде әрқашан бірлік болады). Ол орындайтын Операция жиі "2 Модуль бойынша қосу" деп аталады(1.17-сурет).



X1	X2	Y
0	0	0
1	0	1
0	1	1
1	1	0

Сурет 1.17 – 2XOR логикалық функциясының шындық кестесі

Біз схемада "болдырмау немесе" функциясын орындайтын элемент қажет деп болжаймыз, бірақ бізде тек "2И-емес" элементтері бар, онда келесі схеманы жинауға болады [4].

1.3 ПЛИС туралы жалпы мағұмат

Қазіргі уақытта микроэлектроникада қарқынды дамып келе жатқан бағыттардың бірі PLD (programmable logic device - бағдарламаланатын логикалық құрылғылар) болып табылады. PLD – бос чип. Қарапайым сандық микросхемаларға қарағанда, ПЛИС жұмысының логикасы дайындау кезінде фабрикада емес, қосымша бағдарламалау (жобалау), (далалық жағдайда field-programmable, FPGA – (Field Programmable Gate Array) арқылы арнайы құралдар: программаторлар және бағдарламалық қамтамасыз ету арқылы беріледі. Бұл технология өз архитектурасы бар өзінің микросхемасын жасауға мүмкіндік береді.

ПЛИС – жүйеішілік қайта бағдарламаланған жоғары интеграцияланған икемді әмбебап логикалық құрылғылар. Олардың ішкі құрылымын нақты уақытта өзгерту мүмкіндігімен құрылғыға сұраныстың артуы, орындалатын функцияларды тез қайта құрумен плиталарды қолдану аясын кеңейтті. Оны қолданудың мақсатқа лайықтылығы түпнұсқалық аппаратураны әзірлеу немесе қарапайым АЖ ауыстыру қажеттілігімен негізделеді, бұл құрылғының өлшемін азайтуға, тұтынылатын қуаттылықты азайтуға және сенімділігін арттыруға мүмкіндік береді [9].

Стандартты емес схемотехникалық шешімдерді талап ететін бұйымдарда ПЛИС-ті тиімді пайдалану. Бұл жағдайда ПЛИС тіпті интеграцияның орташа дәрежесіндегі (24 қорытынды) әдетте 10-15 кәдімгі АЖ-ға дейін алмастырады.

ПЛИС микропроцессорлық техникада кеңінен қолданылады. Оның негізінде сандық сүзгілерді, дешифраторларды, микропроцессорларды жиектеу логикасын, басқару сигналдарын қалыптастырғыштарды әзірлеуге болады.

ПЛИС қолданудың артықшылықтары мен салалары:

– сандық (соңғы) автоматтарды (state machine) құру. ПЛИС табиғи түрде еркін синхронды автоматқа сай келеді. Триггер матрицасы және дискретті комбинациялық логика жобалау және жөндеу бағасына және соңғы өнім мөлшеріне жол береді;

– икемділік. Сонымен қатар, егер де, егер де қате жіберілсе немесе бірдеңе өзгерту қажет болса, онда, ПЛИС – бағдарламаланатын схема маңызды артықшылығы бар: қорытынды схеманы жобалау кезеңінде уақыт пен құралдарды жоғалтпай, өз өнімін қайта бағдарламалауға мүмкіндік бар. Бұл өте пайдалы, әзірлеуші әлі соңына дейін оның схемасы қалай жұмыс істейді деп ойлаған кезде, әр түрлі идеяларды қолдануға мүмкіндік береді.

Электрониканың әлемдік нарығында ПЛИС-ті кеңінен пайдалануға байланысты зияткерлік меншікті қорғау маңызды орын алады.

Зияткерлік қызмет өнімдерінің құндық бағалары бар, өйткені олар коммерциялық шарттарда тауар айналымына енгізілуі мүмкін. Зияткерлік меншікті ұрлауға қауіп төндіреді, оның салдары экономикалық шығындар

болып табылады. Сандық электрондық құрылғыларды қорғау арқылы оны болдырмауға болады.

Бағдарламалық өнімді заңсыз көшірудің таралуы, БҚ әзірлеудің жоғары құны(қазіргі заманғы күрделі бағдарламалар бағдарламашылар командасымен жазылады), ПЛИС-ті тұрақты есте сақтау құрылғыларынан ақпаратты кедергісіз алу мүмкіндігі, электроника нарығында жосықсыз бәсекелестіктің болуы зияткерлік меншікті қорғау туралы ойлануға мәжбүр етеді.

Бұл жұмыс криптографиялық әдістерге негізделген ПЛИС-ті бағдарламалық қамтамасыз етілуін қорғауға арналған [10].

1.3.1 FPGA туралы жалпы ақпарат

FPGA (Field Programmable Gate Array) – кеңістік бойынша бағдарламаланатын вентильді матрицалар, логикалық блоктар арасында орналасқан қосындылардың тізбектері арқылы талап етілетін электр схемасына қосылады. Мұндай архитектурасы бар микросхеманы бағдарламалау қағидаттық схема жұмысының логикасына өзгерістер енгізуге әкеледі, бұл өзгерістер кез келген уақытта қолданылуы мүмкін. Микротәсімдер көптеген кіретін және бір шығатын (логикалық вентильдер) конфигурацияланатын логикалық блоктардан тұрады. Бұл сұлбада негізгі екілік операциялар AND, NAND, OR, NOR және XOR жүзеге асырылады [11].

FPGA архитектурасы бар ПЛИС бағдарламаланатын элементтердің үш түрін қамтиды: логикалық блоктар (le логикалық элементтері), енгізу/шығару блоктары және блоктар арасындағы ішкі байланыс функцияларын орындайтын бағдарламаланатын кілттер.

Қазіргі заманғы FPGA – энергияға тәуелді. FPGA конфигурациясы қуатқа байланысты жадта сақталады, нәтижесінде қуат өшірілгенде олардың конфигурациясы жоғалады, сондықтан тікелей FPGA тақтасында орналасқан арнайы флэш жадына қажеттілік бар және ол қуат қосылған кезде қақпақ матрицасына жүктелген конфигурациялық файлды қамтиды.

Сандық электроника нарығында ASIC (Application-Specific Integrated Circuit) танымал. ASIC – тапсырыс микросхемалар, оларды ПЛИС аналогтары деп атауға болады, бірақ кейбір ескертпелер де бар.

ПЛИС пен ASIC салыстырмалы сипаттамасы:

– құны. Сонымен қатар, жобаланатын құрылғының сипаттамасында қате жіберу бүкіл партияның өндіріс құнымен салыстырылатын шығындарға алып келеді. ASIC-ті пайдалану арзанырақ болуына қарамастан, ірі сериялы өндіріс жоспарланған жағдайда, микросхемаларды жобалауға және баптауға үлкен шығындар мүмкіндігін болдырмауға болмайды (өндірістегі ASIC – тің кез келген модификациясы шаблон беретін жұмыстарға үлкен шығындарға әкеп соғады);

– қайта тігу. Плиталардың үлкен артықшылығы құрылғыны жобалау, өндіру, сондай-ақ одан әрі қызмет көрсету кезеңінде түрлендіру мүмкіндігі болып табылады, мысалы, тігісті жаңарту. ASIC, өз кезегінде, өндіріске іске

қосылғаннан кейін "ауыртпалықсыз" модификациялау мүмкіндігі жоқ, сондай-ақ, микросхеманың өзін ауыстырудан басқа, клиенттің құрылғыны жаңарту мүмкіндігі жоқ, бұл сирек орындала алады.

ПЛИС – микросхемалар жасау саласындағы көшбасшылар екі компания: Xilinx және Altera. Бұл компаниялар осы бағытта жұмыс істейтін негізгі бәсекелестер болып табылады. Олардың әрқайсысы FPGA – чиптердің түрлі серияларын ұсынады. Xilinx – бұл Virtex(өнімділігі жоғары, ресурсты қажетсінетін міндеттерді шешуге арналған), Spartan (өнімділігі төмен және арзан, қымбат емес жиынтықтаушы ірі сериялы өндіріс құрылғыларында пайдалануға арналған), Altera - Stratix (өнімділігі жоғары микросхема), Cyclone (ресурсын аз қажетсінетін есептер үшін) және Arria (өндіріс пен құн арасындағы компромисс ретінде).

Макеттік нұсқаны жасау үшін қажетті бағдарламалық және аппараттық қамтамасыз ету ретінде Xilinx FPGA, САПР және программист негізінде төлем макетін шығарады. Әрбір FPGA өндіруші компания бағдарламаланатын логиканың әрбір түрі үшін жобалаудың барлық кезеңдерін жүзеге асыруды қамтамасыз ететін жеке САПР әзірлейді және шығарады. САПР HDL синтездеу және модельдеу, жобаларды орналастыру және қадағалау, сондай-ақ jtag-интерфейсінде кристалдарды бағдарламалау кіреді. ISE WebPACK қарапайым игеру және толық функционалды жобалау ортасын ұсынады және тегін қол жетімді [12].

Бұл жобалау ортасында VHDL және Verilog сияқты аппаратураны сипаттау тілдері кеңінен қолданылады.

1.3.2 Интегралды схемаларды сипаттау тілі

Аппаратураны сипаттау үшін көптеген тілдер бар, бірақ пайдалануда айқын көшбасшылар-VHDL және Verilog. Verilog тілінің синтаксисі C тілінің синтаксисімен ұқсас, бұл оны оңай игереді. Қазіргі заманғы есептеу жүйелерінде VHDL жобалау тілі Базалық тіл болып табылады, ол базалық деректер түрлерінің кең жиынтығы бар, сондай-ақ өз күрделі түрлерін жасауға мүмкіндік береді.

Verilog-интегралды схемалар аппаратурасын сипаттау тілі, электрондық жүйелерді әзірлеудің барлық кезеңдері үшін логикалық схемаларды формальды сипаттау мақсатында 1983 жылы Пентагонның тапсырысы бойынша жасалған. Тіл көбінесе вентильді деңгейде, регистрлік берілістер деңгейінде және микросхемалар корпустарын модельдеу үшін арналған, сондай-ақ құрылғыларды синтездеу кезінде де табысты қолданылады [12].

Verilog аппараттық архитектураны сипаттау үшін үш түрлі стильді қолдайды:

– құрылымдық сипаттама (structural description) – сәулет байланысты компоненттердің иерархиясы ретінде сипатталатын стиль;

– ағын сипаттамасы (data-flow description) – архитектура параллель регистрлік операциялардың жиыны ретінде сипатталатын стиль, ол өз кезегінде вентильді сигналдармен басқарылатын;

– мінез-құлық сипаттамасы (behavioral description) - алгоритмдік стиль, онда түрлендіру кез келген қазіргі заманғы жоғары деңгейлі тілдерде қолданылатын дәйекті бағдарламалық нұсқаулықтармен сипатталады.

Verilog тілі көптеген жүйелерде сандық сұлбаларды модельдеу, бағдарламаланатын логикалық интегралды микросхемаларды, базалық матрицалық кристалдарды, тапсырыстық интегралды микросхемаларды жобалау үшін қолданылады [13]. Мысал ретінде Xilinx компаниясының платасының техникалық сипаттамаларын карастырып көрейік: Xilinx XC3S500E-4FTG256C:

– жүйелік вентильдер саны: 500 мың;

– логикалық ұяшықтар саны: 10476;

– логика отбасы: КМОП;

– орнатылған ЭСППЗУ көлемі: 4 Мбит;

– шина негізіндегі плиталарды жөндеу/тиеу үшін кіріктірілген интерфейс USB;

– жалпы мақсаттағы енгізу/шығару желілері: 32 сандық енгізу/шығару желілері, максималды кернеу 3.3 В, максималды ток 8 мА;

– тұрақты ток көзі: 15 в Тұрақты ток, 650 мА;

– жалпы тұтыну қуаты: 6 Вт макс.

2 Модуль бойынша саннан қалдықтарды қалыптастырудың қолданыстағы тәсілдерін талдау

Модульге бөлу кезінде қалдықтарды қалыптастырудың әртүрлі әдістерінің көп саны бар.

Бүтін оң сандардың екілік (әдеттегі) көрінісін пайдалану кезінде еркін модуль бойынша қалдықтарды қалыптастырудың үш тәсілін бөлуге болады.

Бірінші әдіс қалдықтарды тізбекті қалыптастыруға негізделген.

Екінші тәсілде келтірілген а санынан қалдықты қалыптастыру үшін P,l (i=l, 3, 5) еселік модельдері есептеледі ... К).

Үшінші тәсілде а санын екілік бөлудің машиналық алгоритм принципі пайдаланылған.

Төртінші және бесінші тәсілдерде модуль бойынша келтірудің матрицалық және конвейерлік принципі қолданылған.

2.1 Жекеленген қалдықтарды кейіннен модуль бойынша қосу арқылы қалыптастыру

Қалдықты қалыптастыру тәсілі р модулі бойынша бөлуден екілік санның (2^i) разрядтық таразылардың қалдықтарын (r_i) тізбектей қалыптастыруға негізделген, Р модулі бойынша одан әрі р модулі бойынша А коэффициенттері бар қалдықтарды қосу; тиісті таразылар бірлікке тең.

Сонда р модулі бойынша А санынан R а қалдығын есептеуге арналған формула келесі түрге ие:

$$r_A = AmodP[\int_{i=0}^{k-1}(2^i modP)a_i]modP \qquad (2.1)$$

Мұндағы, 2^i – А (i = 0÷k-1) санының і-ші санының салмағы, a^i – А санының і-ші санының коэффициенті.

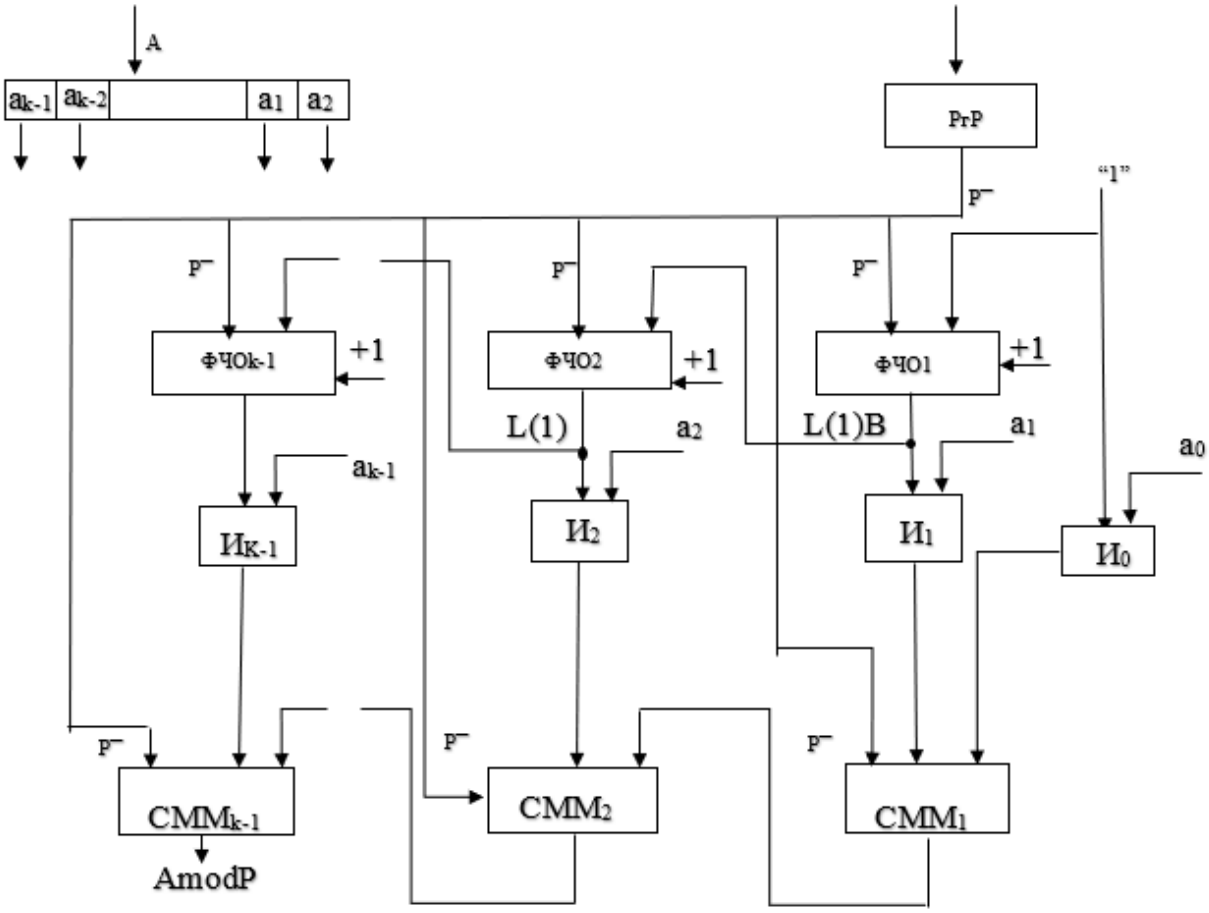
Екілік сандар жүйесіндегі болсақ, a_i (i = 0, ... K-1) коэффициенттері тек екі мәнді қабылдайды (0 немесе 1), алдын ала есептелінген қалдықтардың R модулін 2^i (i = 0, ... K-1), ал үшін a_i = 1 коэффициенті бар және қалған модулін Р санынан аламыз. Кез келген модуль үшін (Р ≥ 2) 2^0 ішінара қалдық бір уақытта бірдей болады. 2^1 ішінара қалдықтары 2^0 қалғанын және т.б. 2^i ішінара қалдықтары $2^{(i\ -1)}$ ішінара қалдық болып табылады. Осылайша, 2^i ішінара қалдықтың есебі $2^{(i-1)}$ екі қалдық қалдықтарымен көбейтіледі және нәтиже модулін азайтады. Екі көбейту операциясы көбейтілген санның барлық цифрларын солға қарай ауыстыру арқылы жүзеге асырылады.

2Р-1 шамасынан аспайтын сандар үшін Р модулі бойынша келтіру операциясы былайша іске асырылады. Егер Сан Р шамасынан аспайтын болса, онда ол өзгеріссіз қалады, егер Сан Р-ден 2Р-1-ге дейінгі аралықта болса, онда одан р модулі шегеріледі, ал нәтиже қалдық болып табылады [5].

2.1-суретте қалдықтарды қалыптастыруға арналған құрылғының функционалдық сұлбасы берілген, 2.2-суретте ішінара қалдықтарды

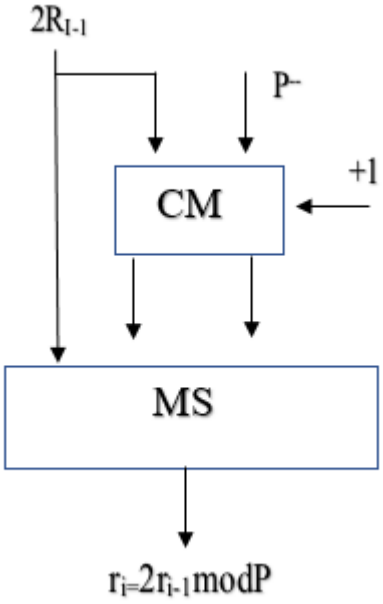
қалыптастырғыштың функционалдық сұлбасы, 2.3-суретте модуль бойынша сумматордың функционалдық сұлбасы (СММ) көрсетілген.

Модуль бойынша қалдықтарды қалыптастыру құрылғысы (2.1-сурет) тізбектелген ФЧО, схемалар мен $И_0$=$И_{к-1}$ және К-1 модуль бойынша сумматордан тұрады. А тіркелімінің $a_0 \div a_{n-1}$ санының разрядтары тиісті схемаларға және $И_0 \div И_{k-1}$беріледі, мұнда $r_0 \div r_{k-1}$ ішінара қалдық мәндерімен қисынды көбейтіледі.

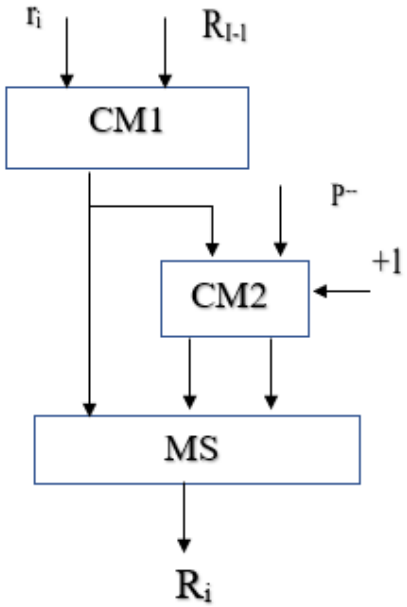


Сурет 2.1 – Модуль бойынша қалдықты қалыптастыратын құрылғының функционалдық сұлбасы.

Модульдің кері шамасы $ФЧО_1 \div ФЧО_{k-1}$ $СММ_1 \div СММ_{k-1}$ кірісіне берілуде. Қалқынды есептеудің алғашқы қадамында 2^0 = (ішінара қалдық r_0) $И_0$ тізбегінің бірінші кірісіне және екінші кіру a_0 мәніне беріледі. Егер $a_0 = 1$ болса, $И_0$ шығуында аралық қалдық R_0 қалыптасады, ол қалған есептеудің екінші сатысында СММ1 кірісіне беріледі. Сонымен қатар, екінші кезеңде, R_1 ішінара қалдықтары $ФЧО_2$(2.2-сурет) шығуынан есептеп, бір цифрмен солға қарай жылжиды, $ФЧО_1$-дің кірісі де беріледі және $И_2$ тізбегінің бірінші кірісі екінші шығыс қосылады, оның a_2 разряд коэффициентінің мәні беріледі. $A_2 = 1$ болса, $И_2$ шығуынан r_1 қосқыштың және СММ2(2.3-сурет) модулінің кірісіне беріледі және оның шығуында R_1 аралық қалдық құралады.



Сурет 2.2 – Ішінара қалдықты қалыптастырушының функционалдық схемасы (ФЧО)



Сурет 2.3 – Модуль бойынша сумматордың функционалдық схемасы (СММ)

$ФЧО_{К-1}$ шығуындағы К қадамдарынан кейін, r_{k-1} ішінара қалдық $a_{n-1}=1$ кезінде қалыптасады, бұл қалдық $СММ_{k-1}$ кірісіне беріліп, шығу коэффициентін R = AmodP құрайды.

$Т_{ф.0i}$ r_i қалдығын қалыптастыру уақыты мынадай формула бойынша айқындалады:

$$Т_{ф.0i} = ЗТ_{см} \quad (2.2)$$

Бұл ретте екілік сумматорлар саны:

$$Q=3(K-1)N_{см} \quad (2.3)$$

Мұндағы, Тсм - қосу уақыты, К - сумматорлар және Р модулінің разрядтары.

Енді қалдықты қалыптастыру процесін жеделдетуге мүмкіндік беретін схеманы қарастырайық. Бұл үшін (2.1) формуланы келесі түрде ұсынамыз:

$$A=2^{2к}(2a_{к+1}+a_{2к})+...+2^4(2a_2+a_2)+2^2(2a_1+a_1)+(2a_0+a_0) \quad (2.4)$$

Р модулі бойынша А санынан қалдықты есептеу үшін (4) формулада $2^{2i}(2a_{2i}+ 2_{2i})$ сандарынан Р модулі бойынша ішінара қалдықтарды ойлануға жеткілікті.

Р модулі бойынша 2^{2i}-ден ішінара қалдықтарды есептеу әдісі мыналардан тұрады: 2^{2i} -ден ішінара қалдықты есептеу төрт ішінара қалдықты $2^{2(i-1)}$ көбейту және нәтижені модуль бойынша келтіру.

Бұл ретте модуль бойынша келтіру операциясы мынадай түрде іске асырылады. Егер Сан Р шамасынан аспаса, онда ол өзгеріссіз қалады. Егер ол Р-ден 2р-1-ге дейінгі аралықта жатқан болса, онда одан 2р модулі есептеледі. Егер Сан 3р-ден 4р-1-ге дейінгі аралықта болса, онда неюден жойылған модуль-3Р есептеледі.

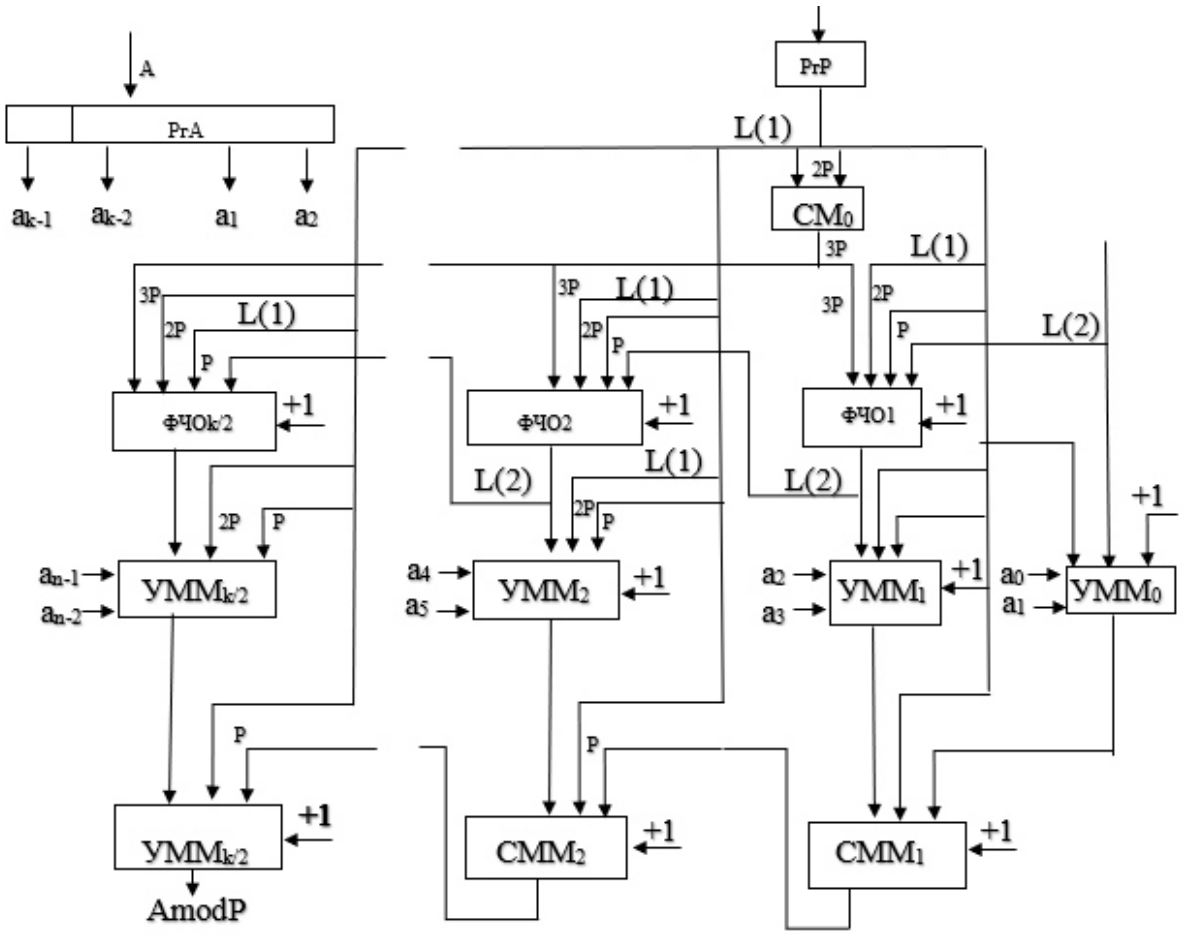
Р модулі бойынша 2^{2i}-ден ішінара қалдықты $(2_{2i}+a_{2i})$ санға көбейту тәсілі келесіден тұрады. $2a_{2i}$-ге көбейтілген Р модулі бойынша 2^{2i}-ден ішінара қалдық A_{2i}-ге көбейтілген Р модулі бойынша 2^{2i}-ден ішінара қалдықпен жинақталады. Егер алынған нәтиже Р шамасынан аспаса, онда ол өзгеріссіз қалады. Егер сан 2Р-ден 3Р-1-ге дейінгі аралықта жатса, онда одан екі еселік модуль – 2Р алынады. 2.4 – суретте модуль бойынша қалдықты қалыптастыру құрылғысының схемасы көрсетілген. 2.5 суретінде ішінара қалдықтарды (ФЧО) Қалыптастырғыш бар. 2.6-суретте модуль бойынша көбейтуші (УММ). Екі (СММ) модуль бойынша көбейту құрылғысының схемасы 2.3-суретте келтірілген [6].

Қалдықты қалыптастыруға арналған құрылғы схемаға(2.4-сурет) И, К/2, ФЧО, УММ. ФЧО бір-бірімен тізбектеліп қосылған, $ФЧО_0$ кіруіне разрядты екі разрядқа солға жылжытатын бірлік коды берілген. Алдыңғы жж разрядтарының шығуы кейінгі (L2) ФЧО кіруіне үлкен жағына (L2) екі жылжытумен беріледі. Әрбір ФЧО кірісінде екі еселенген Р модулінің мәні беріледі, екі еселенген 2Р және еселенген Р 3Р мәні сумматорда СМ0 қалыптасады.

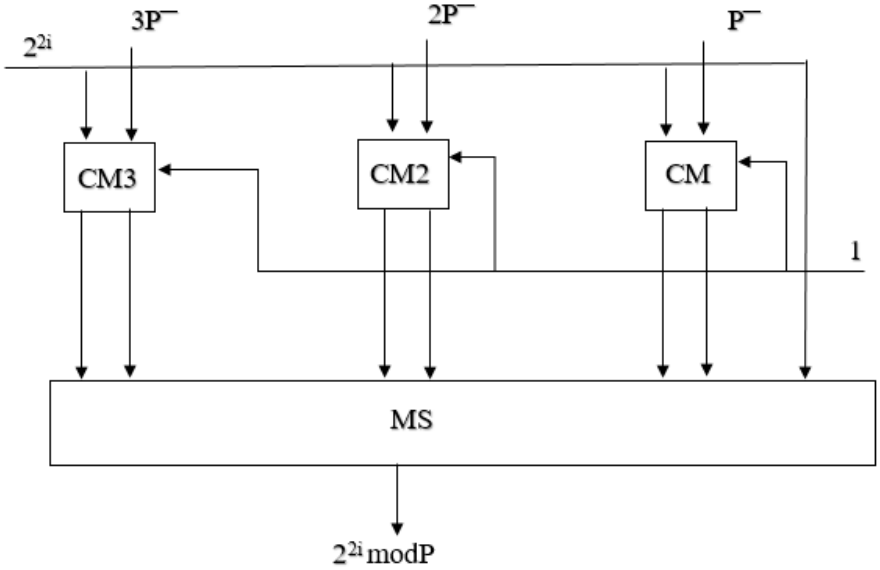
УММ-нң ақпараттық кірісі ФЧО-ның шығуынан және $2a_0a_0$, $2a_1a_1$, $2a_2a_2$, ... $2a_{n-1}a_{n-1}$ жұбының жұптарының мәндерінен және УММ шығуларынан СМmodР кіріс сигналдарының кодтары мен алдыңғы СМmodР-ның шығуынан кодталады, ал нөлдік модуль Р - екі төменгі реттік сандар аі және а0.

Әрбір ФЧО (2.5-сурет) үш қосқышты (СМ1 ÷ СМ3) және мультиплексорды (MS) қамтиды. Үш қосқыштың бірінші ақпараттық шығарылымы ФЧО-ның шығу кодынан беріледі. СМ3 кірісі – үш еселенген 3Р

модулінің кері коды. 2Р модулінің қос коды СМ2 кірісіне беріледі және модульдің кері коды СМ1 ендірушісінің кірісіне беріледі.

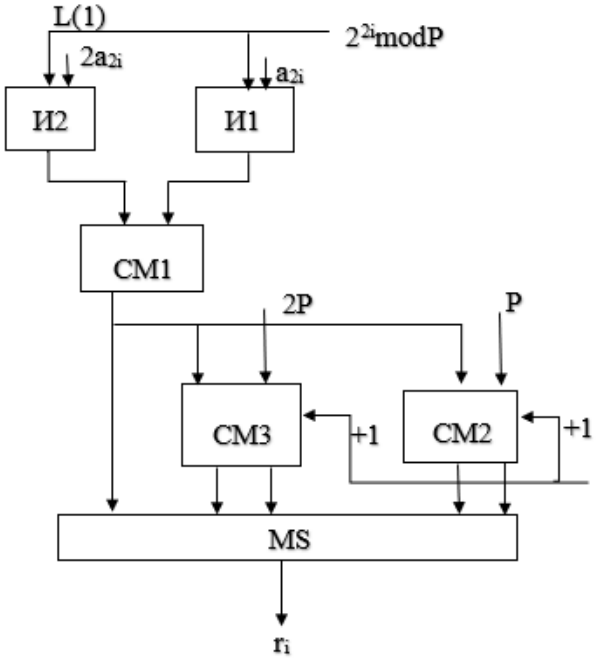


Сурет 2.4 – Модуль бойынша қалдықты қалыптастыруға арналған құрылғы



Сурет 2.5 – ФЧО құрылымы

MS мультиплексоры өзінің кірісін белгілі бір сумматордың шығуымен немесе ақпараттық шығысымен коммутациялайды, онда 2^{2i} разрядты таразылардың мәні 2^{2i} 3P, 2P, P шамаларымен арақатынасына байланысты беріледі. Әрбір УММ (2.6-сурет) екі И1 және И2 сұлбасын қамтиды, ол А Сан кодының разрядтарымен басқарылатын, үш сумматор СМ1, СМ2, СМ3 1 MS мультиплексоры. СМ1 шығу коды, MS және СМ3, және СМ2 кіруіне беріледі.



Сурет 2.6 – Модуль бойынша көбейтудің құрылымы (УММ)

Қалған бөлігін есептеудің бірінші кезеңінде $УММ_0$ кірісі $УММ_0$ шығу кезінде $r_0 = 2^0 = 1$ беріледі, аралық қалдық $R_0 = 2^0(2a_0 + a_0)$ қалыптасады. Бұдан басқа, r_0 мәні жоғары екі санға қарай жылжиды, яғни. $4r_0$ = ФЧО1 кірісіне беріледі.

Екінші кезеңде $ФЧО_1$ шығуда r_1 ішінара қалдығы қалыптасады, ол $УММ_1$ кіруіне беріледі, мұнда r_1 2a $_3a_2$ көбейтіледі. Одан кейін ол P модулі бойынша жинақталады және r_i қалыптасады, ол $СММ_1$ кіруіне беріледі, мұнда $R_i=(R_0+r_i)$modP аралық қалдығы есептеледі, бұдан басқа екінші қадамда 2P солға (L2) ығыстырумен гі мәні $ФЧО_2$ ақпараттық кіруіне беріледі, ал $СММ_2$ кірісінде R_1 және СММ2 мәні беріледі.

Үшінші кезеңде $ФЧО_2$ шығуында мәні $УММ_2$ кіруіне берілетін ішінара қалдық қалыптасады, мұнда r_2' a_4 және $2a_5$ разрядтарының мәндеріне көбейтіледі. Содан кейін олар P модулі бойынша жинақталады, ішінара r_2 қалдығы, одан әрі r_2 ішінара қалдығы $СММ_2$ кіруіне жіберіледі. $СММ_2$ r_2-ден R_1-ге модуль бойынша жинақталады және $R_2=(R_1+r_2)$mod P аралық қалдығы түзіледі [6].

2.4-суретте келтірілген санды солға екі разрядқа жылжытумен P модулі бойынша қалдықты қалыптастыру құрылғысы қалдық К/2 қадамға

қалыптасады және әрбір қадамда R ішінара қалдығы $ФЧО_i$, $УММ_i$, $СММ_i$ арқылы өтеді, онда қалдықты қалыптастыру уақыты анықталады:

$$T_{фо} = 1/2(T_{ФЧО} + T_{УММ} + T_{СММ}) = 1/2 = (T_{см} + 2T_{СМ} + 2Tсм) = 2{,}5T_{СМ}$$

Сумматорлар саны:

$$N_{СМ} = 1/2\ (N_{ФЧО} + N_{УММ} + N_{СММ}) = 1/2\ (5N_{СМ} + 3\ N_{СМ} + 2\ N_{СМ}3) = ½*8\ N_{СМ} = 4$$
$$N_{СМ}$$

2.2 А санынан модульге еселік сандарды параллель шегеру жолымен қалдықтарды қалыптастыру тәсілі

Модуль бойынша А санынан қалған қалдықтарды қалыптастырудың бір актілі құрылғысы үлкен аппараттық шығындармен сипатталады. Мұндай құрылғыларда әртүрлі блоктарда қатар P*i еселік модульдері қалыптастырылады (мұнда і= 2, 3 ..., к). Содан кейін Р модулі және 2р, 3р, құрастырылған еселік модульдер 2р, 3р, ... ең аз оң қалдық $R=A+P_i+1$ нәтиже болып табылады [18]. 2р, 3р еселік қалыптастыру үшін 2р, 3р, ... к; К-1 сумматор қажет.

Div = [A / P] санының артуымен қалдықтың мәнін және і * Р көбейткіштерін есептеуге арналған қоспа саны күрт артады. Мысалы, егер div = 7 болса, онда р, 2р, ... 6р және 7р көбейткіштері үшін 3р, 5р, 6р және 7р көбейткіштері 7 сумматор мен 4 құрастырушы қажет болады. 2р және 4р мәндері Р-ны 2 және 4-разрядқа ауыстыру арқылы алуға болады [6].

Қалдықты қалыптастыру уақыты 2р, 3Р, ... kp еселік қалдықты қалыптастыру уақытымен және Тфо қалдықты қалыптастыру уақытымен қалыптасады:

$$T_{фо} = T_{кр} + T_{фо}=1{,}5T_{СМ}$$

Сумматорлар саны:

$$N_{СМ} =1{,}5(N_{kp}+N_{ФО}) = 1{,}5KN_{СМ}$$

2.3 А санын Р модуліне бөлу арқылы қалдықты қалыптастыру тәсілі

Бөлінетін А мен бөлгіш Р жеке Q деректері үшін және қалдық R қатынасы орындалатындай етіп есептеледі

$$A= Q * P+R \qquad (2.5)$$

Мұнда, A= 2n – биттік сан, P - n – биттік сан, R<P .

Бөлуді екі негізгі жолмен жүзеге асыруға болады:

– қозғалмайтын бөлгішпен және оңға жылжитын бөлгішпен;

– қозғалмайтын бөлгішпен және солға жылжитын бөлгішпен.

Бірінші тәсілдің кемшілігі-сумматор бөлу құрылғысында және қос ұзындықты бөлгіш регистр болу қажеттілігі. Екінші тәсіл-фактураға тораптары дара ұзындығы. Сондықтан біз бөлудің бірінші әдісін қарастырмаймыз.

Егер А және Р саны оң болса, онда жеке Q және R қалдығы оң болады. Бөлудің дәйекті алгоритмі а санын жылжытады және Р А-дан $0 < R < n$ шартын қанағаттандыратын R қалдығы табылғанға дейін шегереді. Алайда, шегергеннен кейін теріс қалдық болуы мүмкін. Дәл осы, яғни, теріс қалдықты алған кезде, қалпына келтіру және қалпына келтірусіз бөлу алгоритмдері бір-бірінен ерекшеленеді.

R_i арқылы бөлу алгоритмінің і-ші қадамында алынатын қалдықты белгілейміз. 2n – бит саны, ал Р - n – бит саны болып табылады, онда Р бит n-ге сол жақ шеті бойынша теңестіруге қол жеткіземіз, яғни 2^nр-ден бастаймыз.

Бұл ретте R бастапқы мәні $A_{ст}$ санының үлкен разрядына тең алынады, осыдан кейін $A_{ст}$-тан Р шегереміз және ЧО-ның ішінара қалдығын аламыз.

Егер ЧО≥0 болса, онда басқа қадамға өтіңіз. Әйтпесе, алдыңғы қалдық мәнін қалпына келтіреміз [6].

Қалдықты қалпына келтіру арқылы бөлу алгоритмін қарастырайық. А санын Р модулі бойынша келтіру ерекшеліктерін ескере отырып, осы алгоритм былайша сипатталуы мүмкін:

– ішінара қалдықтың (ЧО) бастапқы мәні бөлінетін үлкен разрядтарға тең болады;

– ЧО-дан бөлгіш шегеріледі және қалдық белгісі талданады;

– егер қалдық оң болса, онда бөлу мүмкін емес, асыра толтыру белгісі қалыптасады және процесс аяқталады, әйтпесе, ЧО бөлгішті қосу арқылы қалпына келтіріледі және бөлу жалғастырылады;

– ішінара қалдық солға бір разрядқа жылжытылады, ал босаған жылжытуда ЖБО кіші разряды бөлінетін А-ның кезекті саны енгізіледі;

– жылжымалы ЧО-дан бөлгіш шегеріледі және азайту нәтижесінде талданады;

– егер нәтиже белгісі теріс болса, онда ЧО бөлгішке қосу арқылы қалпына келтіріледі;

– 4-6 тармақтары R>A алу үшін дәйекті түрде орындалады.

Жоғарыда сипатталған алгоритмнің жетіспеушілігі – ішінара қалдықты қалпына келтіру үшін қосымша қосу операцияларын жекелеген қадамдарда орындау қажеттілігі. Бұл Операндтар кодтарының нақты үйлесіміне байланысты өзгеруі мүмкін бөлу уақытын арттырады. Көрсетілген себептерге байланысты нақты бөлгіштер қалдықты қалпына келтірмей жылжымайтын бөлгіші бар бөлу алгоритмі негізінде құрылады. Бұл алгоритмде 1-4 және 7-тармақтар қалдықты қалпына келтіре отырып, бөлу алгоритмінің тиісті тармақтарымен толық сәйкес келеді, ал 5 және 6-тармақтарда мынадай тұжырым болады: "егер қалдық қойылса, жылжытылған ЧО-дан бөлгіш

шегеріледі және егер қалдық теріс болса, жылжытылған ішінара қалдыққа бөлгіш қосылады".

2.7-суретте қалдықты қалпына келтірмей алгоритм бойынша жұмыс істейтін а бүтін оң санның р модулі бойынша келтіру құрылғысының функционалдық сұлбасы келтірілген [7].

Модуль бойынша келтіру құрылғысы регистрлер блогынан (блоктан), ішінара қалдықты (ФЧО) қалыптастырушыдан, синхрондау блогынан (БлС) тұрады.

БлРг А (РгА) регистрінен тұрады, ол солға қарай бір сандық ауысу сұлбасы бар. РгА сыйымдылығы – 2n. РгА сақтауға қызмет етеді, бөлгіш А, модуль R беріледі. РгР бөлгішті сақтауға қызмет ететін - модуль R. Сыйымдылығы n.

Жартылай қалдық блогы (БЧО) сумматордан (СМ) және басқарылатын инвертор режимінде жұмыс істейтін п разрядтық блоктан тұрады.

Синхрондау блогы (БлС) л.3.1 кідіріс сызықтарынан, И2 және И1 схемаларының т триггерінен тұрады, мұнда А - дан Р кезекті шегергеннен кейін қалдық белгісі есте сақталады.

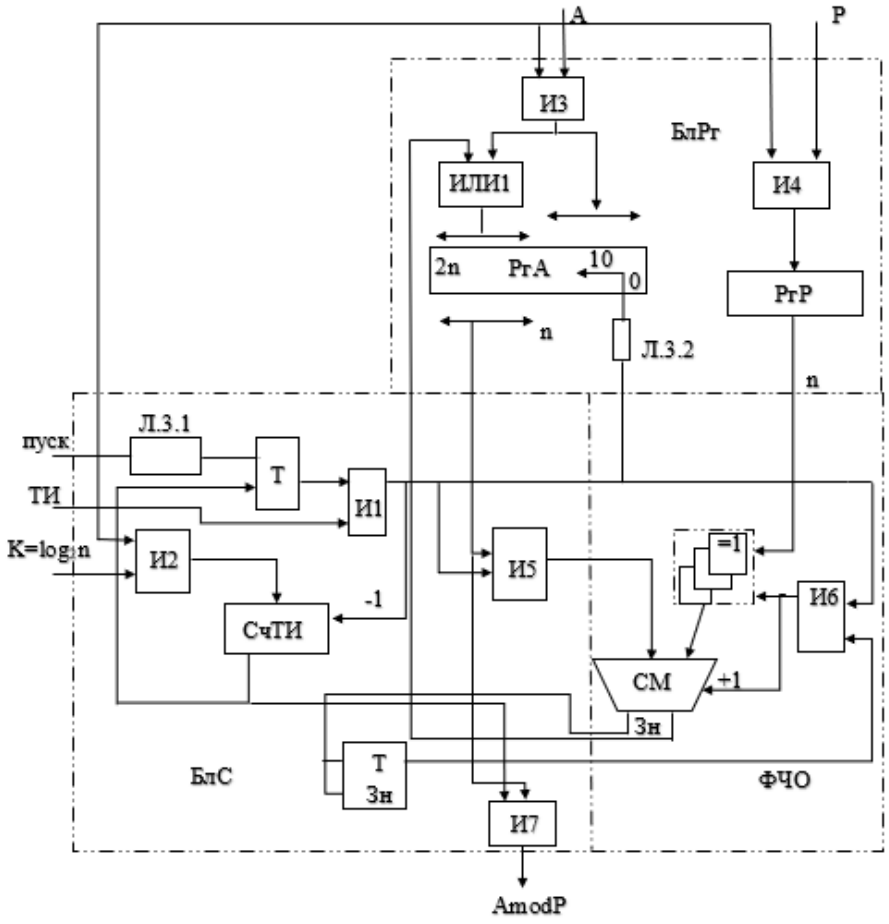
Схема арқылы РгА үлкен разрядының (2n÷n) және 5 сумматордың сол жақ кіруімен байланысты, ал сол жақ кіріске СМ келесі қалдық белгісіне байланысты тікелей немесе кері кодпен РГА разрядтары беріледі. Қалдық белгісінің мәні сумматордың кіші разрядының кірісі беріледі.

Сумматор шығулары схема арқылы немесе РгА-ның үлкен разрядтарымен байланысты, онда үлкен разрядқа жылжытуға жататын ішінара қалдықтар есте қалады. Операциялар аяқталғаннан кейін РгА регистрінен [2n-1-n] қалдық мәні "операцияның аяқталуы" сигналы бойынша И7 сызбасы беріледі.

Бөлгіш құрылғысының негізінде модуль бойынша келтіру құрылғылары қалдық қалпына келтірусіз алгоритм бойынша жұмыс істейтін адам былайша жұмыс істейді.

Сигнал бойынша бөлінетін А саны И3 схемамен РгА-да [2n-1÷0] қабылданады, ал Р модулі (бөлгіш) РгР алынады. И1-схема арқылы іске қосу сигналы СчТИ к санына байланысты жылжу санының екілік коды жазылады.

А және Р, сондай-ақ К санын жазу кезінде "іске қосу" сигналы кідіріс сызығымен кідіртіледі 3.1. Операндтарды қабылдағаннан кейін 3.1 шығудан бастап "іске қосу" сигналы т триггерінің жеке кіруіне келіп түседі және оны И2 схемасының шығысына сигналдың бірінші тактикасынан өтуіне рұқсат беретін жалғыз күйге ауыстырады. 1-ге келіп түскен және оның көрсеткішін бір бірлікке азайтады. Сонымен қатар, Т1 Л 3.2 кідіріс сызығының кіруіне, РГА регистрі [2n-1=n] мазмұнының берілуіне рұқсат ете отырып, и5 сұлбасының кіруіне, сумматордың сол жақ кіруіне түседі(2.7-сурет).



Сурет 2.7 – Қалпына келтірусіз алгоритм бойынша құрылған р модулі бойынша А санын келтіру құрылғысы

ТИ1 сондай-ақ И6-схемаға келіп түседі, оның екінші кіруіне белгі триггерінің (Тзн) жеке шығуынан "0" беріледі. Бастапқы белгінің триггерінен "0" деңгейі келіп түсетіндіктен, онда "болдырмау немесе" схемасының шығуында Р модулінің кері коды қалыптасады.

R1 схема арқылы немесе Рг-ға [2n-1÷n], ал нәтиже белгісі белгі триггеріне жазылады. Осыдан кейін ТИ1 арқылы Л3.2 РгА жылжитын кіріске түседі және оны солға бір разрядқа жылжытады. Бұл ТИ1 тактикалық импульсінің әрекеті аяқталады.

Импульстің ТИ2-ге келуімен, СчТИ-ді оқу тағы бір разрядқа қысқартылады. Ілінген ішінара қалдық $2r_i$ И5 схемасы арқылы тартқыштың екінші кірісіне жіберіледі және екінші шығыс модулы Тзн = 1 (теріс қалдық) немесе кері кодты Тзн = 0 (оң қалдық) жағдайда модульді алады. Бұл жағдайда $r_2= 2r_1+P+1$ оң баланспен толтырғышта немесе теріс баланспен $r_2= 2r_1+P$ кезінде қалыптасады. Сонда СМ шығарылымдарынан r_1 РгА-да жазылады және бір санды солға жылжытады.

N-ші тактілік импульс келіп түскеннен кейін СчТИ алдыңғы қалдық белгісіне байланысты 43 екі еселеніп п-1-ші бөлгіш (модуль) шегеріледі немесе жинақталады және нәтиже РгА жазылады [2n-1÷0]. Соңғы қалдықты

қалыптастыру кезінде "операцияның аяқталуы" сигналы оны нөлдеу кезінде СчТИ қалыптастыратын қалдық И7 схемасының шығысына беріледі [7].

2.4 Негізгі көрсеткіштер бойынша қалдықтарды қалыптастыру тәсілдерін салыстырмалы бағалау

2.1-кестеде r_i қалдықты қалыптастыру уақыты бойынша және $N_{СМ}$ екілік сумматордың К-разрядтық саны бойынша r_i қалдықты қалыптастыру тәсілдерін келтіру. Бұл ретте, T_{MS} « $T_{см}$ және N_{MS}«$N_{СМ}$ себебі кестеде олар ескерілмеген.

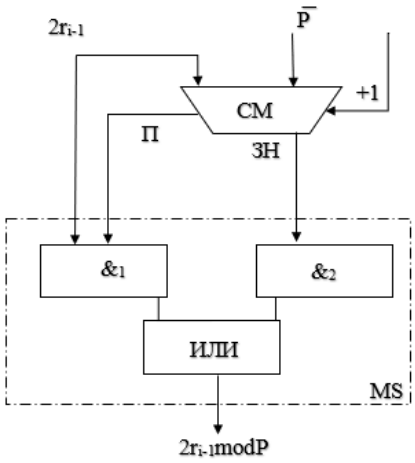
Кесте 2.1 – Қалдықты қалыптастырудың әртүрлі тәсілдері үшін $T_{фо}$ және $N_{СМ}$ параметрлері

Қалыптастыру тәсілдері	$T_{Ф.О.}$	$0_{Ф.О.}$
Қалдықты тізбектей қалыптастыру	3 $T_{см}$	3 $N_{см}$
Қалдықты тізбектей қалыптаструдың екінші жолы	2,5$T_{см}$	4 $N_{см}$
Параллель шегерумен қалдықты қалыптастыру	1,5 $T_{см}$	1,5$N_{см}$
Бөлу арқылы қалыптастыру	$T_{см}$+T=1	$N_{см}$+N=1

Бұл кестеден Тфо-ның ішінара қалдығын қалыптастыру уақыты бойынша және Ncm-ның аппараттық шығындары бойынша артықшылық төртінші тәсілге бөлу құрылғысы негізінде ішінара қалдықты қалыптастыруға беріледі.

2.5 Модуль бойынша қалдықты матрицалық және конвейерлік тәсілмен келтіру

Модульдік модуляцияланған сандар үшін матрицалық схемаларды құрастырған кезде, келесі $ФЧО_i$ шығуынан ішінара қалдықтар бір сандық элементтің солға қарай келесі $ФЧО_{i+1}$ кірістеріне ауысуымен беріледі. Қалдық қалдығының (ФЧО) функционалдық диаграммасы 2.8-суретте көрсетілген.



Сурет 2.8 – Жекеленген қалдық қалыптастырушының функционалдық диаграммасы

ФЧО келесі түрде жұмыс істейді

Егер алдыңғы еселенген $2r_{i-1} \geq P$ балансы болса, $2r_{i-1}$-P аяқталғаннан кейін сумматор П = 1 ауыстыруды жасайды және айырмашылықтың белгісі ЗН = 0 болса, онда $2r_{i-1}$-P айырмашылығы И2 схемасы арқылы қабылдағыштың СМ шығысы ИЛИ схемасының шығуына беріледі. Егер $2r_{i-1} < P$ болса, $2r_{i-1}$-P айырымын айтарлықтай бөлу кезінде, ЗН=1 қалыптасады және П = 0 болса, онда ЗН=1 сигналы И1 тізбегі арқылы $2r_{i-1}$ және ИЛИ шығысқа беріледі . Сонымен қатар, $r_i = 2r_{i-1}$ [8].

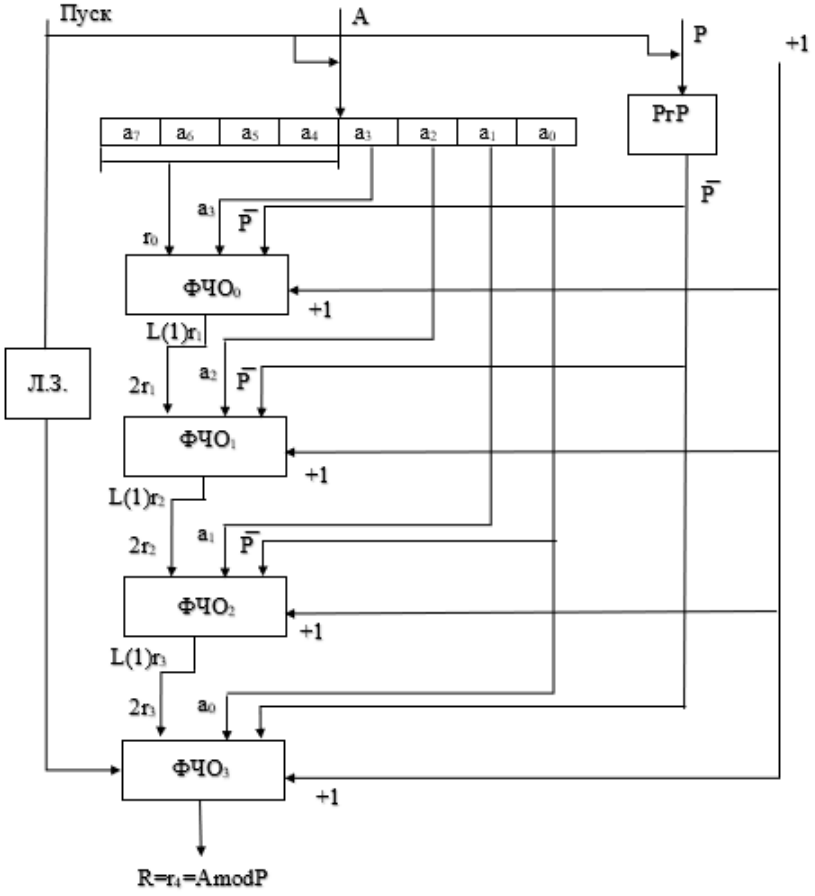
Енді жоғарыда қарастырылған ФЧО негізінде А модулін өзгертуге арналған құрылғының матрицалық схемасын құруға болады. 3.3-інші суретте А = а7 а6 а5 а4 а3 а2 а1 а0 және Р = Р3 Р2 Р1 Р0 нөмірлерімен модуль үшін азайту схемасының блок-схемасын көрсетеді. Матрицалық сұлба келесідей жұмыс істейді. «Старт» сигналында «А» санатындағы нөмір РгА регистраторына алынады, ал Р модулінің биттері РгР тіркелімінде қабылданады. Р және 1-деңгей модулінің кері коды $ФЧО_0$ - $ФЧО_3$ қалдық қалдықтарының r = а7, а6, а5, а4 кірістері $ФЧО_0$ кірісіне беріліп, сонымен бірге $ФЧО_0$ шамасы $2r_0$ мәніне келтірілген, оның мәні Р коды қосымша кодта $2r_0$ модулімен қосу арқылы алынып тасталады, жартылай қалдық $r_1 = 2r_0+P+1$ есептеледі. Ішінара қалдық қалдырылғаннан кейін, қалған қалдық екі саннан солға қарай жылжиды және ағыны a_0-ге $ФЧО_3$ кірісіне қосып, онда $r_2 = 2r_1+P+1$ қалыптасады. $ФЧО_2$-дегі $ФЧО_3$ ішінара қалдықтары r_3 және r_4 құрады. r_4 мәні - $R = r_4 = AmodP$ мәні.

Кешіктіру уақыты Л.З. $ФЧО_0$-$ФЧО_3$ арқылы А санының кодтарын қабылдау арқылы анықталады. Бір ФЧО-$Т_{ФЧО}$-дағы кешігу уақыты - тартқыштың ($\tau_{СМ}$) және мультиплексордың (τ_{MS}) кешігу уақытының сомасы. $\tau_{СМ}$ $Т_{ФЧО} = \tau_{СМ} + \tau_{MS}$ содан кейін $Т_{Л.З.} = n * Т_{ФЧО}$. Уақытша $Т_{Л.З.}$ модуль санын азайтудың матрицалық схемасының орындалуы анықталады.

Сандарды модуль бойынша келтірудің матрицалық схемасында өнімділікті арттырудың өте маңызды әлеуеті – конвейеризация мүмкіндігі бар. Конвейеризация кезінде модуль бойынша барлық келтіру процесі аяқталған қадамдардың дәйектілігіне бөлінеді. Модуль бойынша келтіру процедурасының әрбір кезеңі конвейердің өз сатысында орындалады, және де барлық сатылар параллель жұмыс істейді. сатының алынған нәтижелері конвейердің (i+1)-ші сатысына одан әрі өңдеуге жіберіледі. I-нші сатыдан сатыға ақпаратты көшіру олардың арасында орналастырылатын буферлік жады арқылы жүзеге асырылады. Конвейер жұмысының синхрондылығы тактілік импульстермен қамтамасыз етіледі, олардың уақыты τі конвейерінің ең баяу сатысымен және буферлік жад элементінде кідіріспен анықталады.

2.9-сурет конвейердің функционалды схемасын N-бит модуліне Р модулін 2-нші санға дейін жеткізеді. Конвейер N-кезеңдерден тұрады және әр кезең ФЧО бірліктерін құрастырушылардан тұрады және ішінара қалдықтар

үшін $Ргг_i$ буферлік регистрлерден тұрады, буфер әрбір А санының әртүрлі модулі болса, әрекетке кірмеген А санының төменгі сандары үшін тіркеледі және Р - РгР модулінің аралық тізілімі.



Сурет 2.9 – Сандарды модуль бойынша келтірудің матрицалық схемасы

N сатыдан тұратын модуль бойынша сандарды келтіру тактілі конвейерлік құрылғыда. Келтірілген А сандары және оның Р модулі – модуль бойынша келтірілгенге қарағанда N интервалмен кіріске берілуі мүмкін. Сонымен қатар, конвейер шығуында нәтижелер де пайда болады.

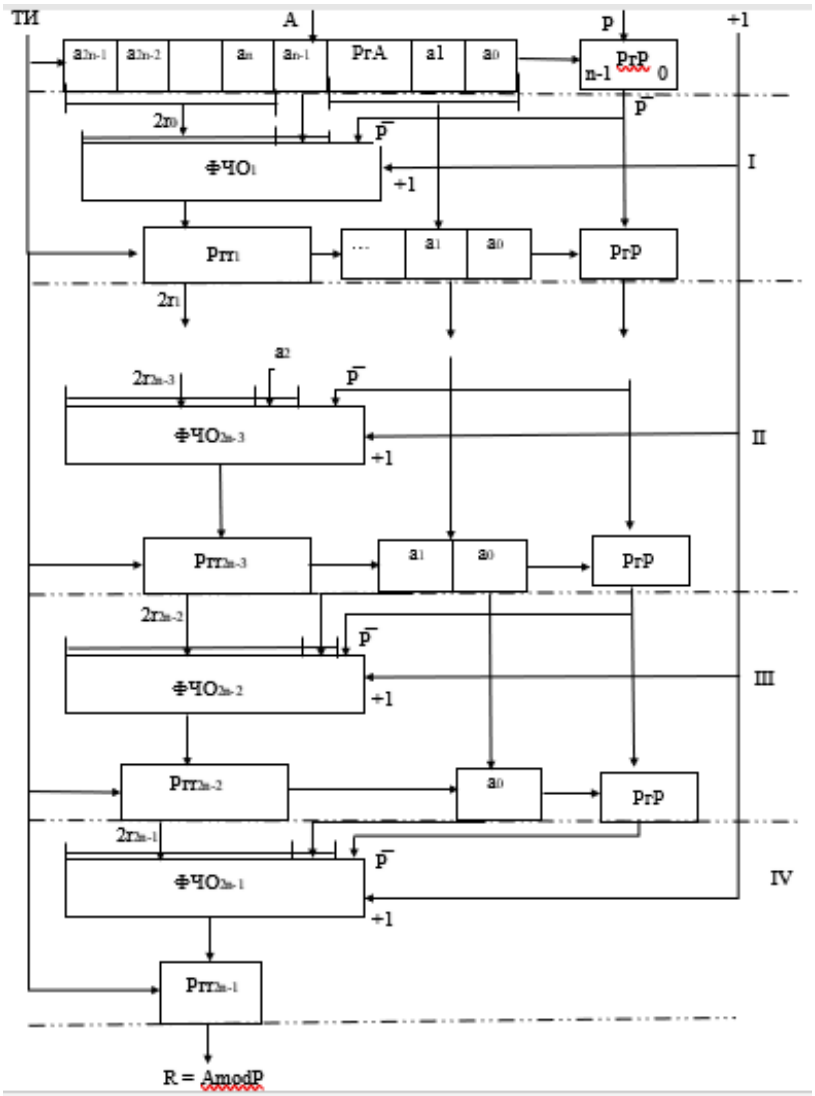
Конвейер келесідей жұмыс істейді. ТИ1 тактикалық импульсін РгА және РгР регистрлеріне бергеннен кейін сандардың А1 және Р1 бірінші жұбы қабылданады. Бұл ретте РгА регистрінің $a_{2n-1} \div a_n$ үлкен бөлігі - r_0 құрайды, ал $2r_0$ екі еселенген мәні $A_{2N-1} \div a_{n-1}$ разрядтарын құрайды, олар $ФЧО_1$ кірісіне ТИ2 екінші тактикалық сигналымен беріледі және $R_i=2r_0 modp$ операциясын орындай отырып, $R_i=2r_0+p+1$ деп есептеледі, ол РгА буферлік тіркеліміне жазылады.

Бұл ретте РгА регистрінің $a_{n-1} \div a_0$ разрядтары бірінші сатының буферлік регистріне жазылады, ал РгР мазмұны бірінші сатының РгР регистіріне жазылады. РгА және Ргг регистрлеріне ТИ2 тактикалық импульсімен, сондай-ақ сандардың келесі жұбы А2 және Р2 қабылданады. ТИ3 үшінші тактілік импульсін РгА және РгР регистрлеріне бергеннен кейін А3 және Р3 бір мезгілде А2 және Р2 сандарының жұбы ФЧО-да өңделеді және осы жұп үшін

r_0 есептеледі және нәтиже $Ргr_i$ регистріне қабылданады. А2 өңделмеген разрядтары бірінші сатының буферлік тіркеліміне жазылады, ал Р2 РгР тіркеліміне қабылданады және $ФЧО_2$ кіруіне беріледі, мұнда $r_2=2r_1 mod p$ мәндері есептеледі және екінші сатының $Ргr_2$ буферлік тіркеліміне жазылады және екінші сатының тіркелімдерінде операцияға енбеген А1 және Р1 сандары жазылады.

$ТИ_N$ тактілік импульсі бергеннен кейін $Ргr_{2n-1}$ соңғы сатысының регистірінде $R=r_{n-1}$ нәтижесі қалыптасады.

$ТИ_N+1$ типі, $ТИ_N+2$ типі, $ТИ_N+3$ типі берілгеннен кейін $Ргr_{2n-1}$ тіркелімінде А2Р2 және А3Р3 сандардың жұбынан қалдықты қалыптастырушы болады(2.10-сурет) [8].



Сурет 2.10 – Модуль бойынша санды келтірудің конвейерленген матрицалық схемасы

Конвейердің әртүрлі сатыларында R=AmodP есептеу мысалын қарастырайық.

$$A=a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0 = 01001110 = 78_{10};$$

$$P = 1011_2 = 11_{10};$$

$$[p]_{доп} = \overline{p}+1 = 1.10101;$$

$$r_0 = 0100;$$

$$R=78 \bmod 11=1;$$

Конвейер сатыларындағы ішінара қалдықтарды есептеу тәртібі 2.2-кестеде келтірілген.

Кесте 2.2 – Конвейер сатыларындағы ішінара қалдықтарды есептеу реті.

	ТИ1	ТИ2	ТИ3	ТИ4
РгА РгР	$A=0.01001110_2$ $P=0.1011_2$			
$ФЧО_1$ I-ст.		$r_1=(2r_0 + a_3) \bmod P$ $2r_0 + a_3$ 0.01001 $\overline{p}+1$ $\frac{1.10101}{1.11110}$ ЗН=1 поэтому $r_1=0.01001$		
$ФЧО_2$ II-ст.			$r_1=(2r_1 + a_2) \bmod P$ $2r_1 + a_4$ 0.10011 $\overline{p}+1$ $\frac{1.10101}{1.01000}$ ЗН=0 и П=0 $r_2=0.01000$	
$ФЧО_3$ III-ст.			$r_1=(2r_2 + a_1) \bmod P$ $2r_2 + a_1$ 0.10001 $\overline{p}+1$ $\frac{1.10101}{1.00110}$ ЗН=1 и П=0 $r_3=0.00110$	
$ФЧО_4$ IV-ст.				$r_4=R=(2r_3 + a_0) \bmod P$ $2r_4 + a_0$ 0.01100 $\overline{p}+1$ 1.10101 ЗН=0 и П=0 $R=r_4=0.01000$

3 Сандарды модульге келтіруші құралды жобалау

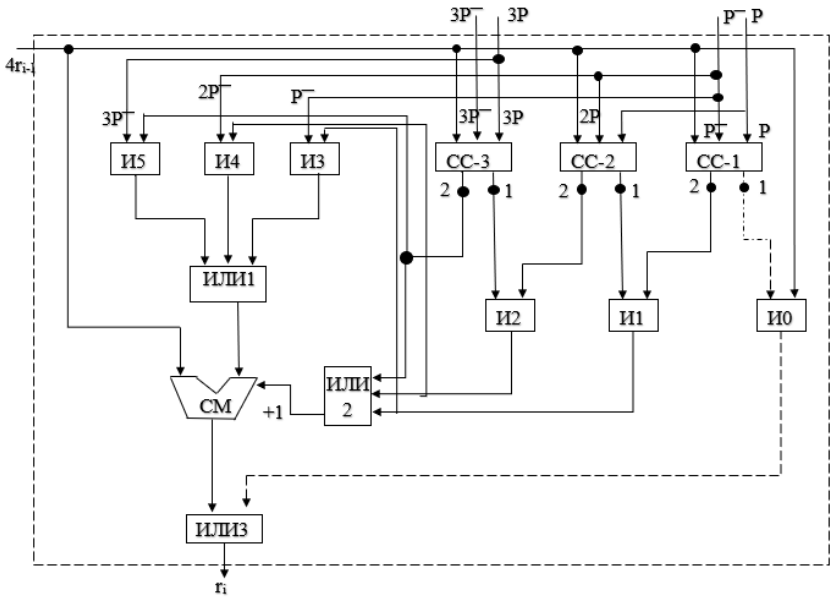
3.1 Алынатын модульді алдын-ала анықтау арқылы сандарды модульге келтіруші құралды құру

Аппараттық шифрлау бағдарламалық шифрлау алдында бірқатар маңызды артықшылықтарға ие, олардың бірі жоғары жылдамдық. Криптоалгоритмді аппараттық іске асыру оның бүтіндігіне кепілдік береді, ал кілттерді шифрлеу және сақтау компьютердің жедел жадында емес, шифратордың өзінде жүзеге асырылады. Осылайша, алгоритмнің өзін жүзеге асырудың қорғалуы қамтамасыз етіледі, бұл да маңызды артықшылығы болып табылады. Сондықтан ашық кілтті аппараттық және бағдарламалық-аппараттық криптожүйелерді жобалау кезінде базалық операциялардың бірін іске асырудың схемалық шешімдерін әзірлеу міндеті - санды модуль бойынша келтіру өзекті болып табылады.

Бүтін сандарды модуль бойынша келтірудің жылдамдық бірліктері талқыланады, мұнда ішінара қалдықтардың формасы үш екілік сумматорларға негізделген. N-разрядты сумматордың аппараттық құны N-разрядты сумматордың Екі N-разрядты Қос сумматорын үш n-разрядты схемамен ауыстыра отырып, n-разрядты салыстырудың N-разрядты схемасынан үш есе артық болғандықтан, салыстыру ішінара қалдықтардың генераторларын құруға аппараттық шығындарды айтарлықтай төмендетуге мүмкіндік береді. Бұл әсіресе матрицалық немесе құбыр сызбаларында құйылған құрылғыны құру кезінде қатты сезіледі [7].

ФЧО құрылымы

3.1-суретте бір екілік сумматордан және үш СС-1, СС-2 және СС-3 салыстыру сұлбасынан тұратын ФЧО блок-схемасы көрсетілген.



Сурет 3.1 – Бір сумматор және үш салыстыру схемаларынан тұратын жекеленген қалдықтарды қалыптастырушы құралығысының сұлбасы

Тиісті тіркелімнің 3Р және 3Р модулдерінің үш еселенген мәндері және Р және Р кодының алдыңғы және кері кодтарындағы мәндері ФЧО кірістерінде қабылданады. 2Р және 2Р мәндері Р мәндерін тиісінше бір солға солға қарай жылжыту арқылы қалыптастырылады. Бұдан басқа, алдыңғы қалдықтың мәні екі цифрдың солға, яғни $4r_i$-1-ке ауысуы. $4r_i$-1+3Р+1 толықтыруларының біреуінің нәтижесі бойынша, $4r_i$-1+2Р+1, $4r_i$-1+Р+1 жартылай қалдықты құрайды.

$4r_i$-1 бұрынғы тепе-теңдікте көбейтіледі де СС-1, СС-2, СС-3 салыстыру сұлбаларының бірінші кірісіне және бірінші қосқышына беріледі. СС-1-нің екінші кірістері Р-ның мәндерімен және Р-ның кері мәнімен беріледі, ол СС-1 құрылымын жеңілдетеді. Сол сияқты, 2Р және 2Р екінші СС-2 кірістеріне беріледі. 3Р және 3Р мәндері СС-3 кірістеріне беріледі.

СС-1 $4r_i$-1 және Р-кодтарды салыстырады. Егер сол уақытта $4r_i$-1<p болса, оның шығуында 1 сигнал жасалады және оның шығуында «0» сигналы пайда болады. Керісінше, егер $4r_i$ -1 ≥ р болса, онда шығу Осы схеманың 2-інде «1» сигналы шығарылады, ал шығу кезінде 1 «0» сигналы шығарылады.

СС-2 схемасы 4р-1 мәнін 2р модулінің мәнімен салыстырады. Бұл тізбектің 1-ші позициясында «1» сигналы $4r_i$-1 < 2р болса, ал «2» 2-ші мәнде орнатылады. Егер $4r_i$-1 ≥ 2р болса, онда шығу 1 «0» деп орнатылады және шығыс 2 «1» деп орнатылады.

СС-3 схемасы $4r_i$-1 және 3р кодтарын салыстырады. Осы схеманың шығуында 1 «1» сигналы қалыптасады, егер $4r_i$-1 < 3р болса, онда шығу 2 «0» деп орнатылады. Егер сол уақытта $4r_i$-1 ≥ 3р болса, онда «1» сигналы шығу 1-де жасалады және сигнал «1» 2-де орнатылған [8].

3.1 кестеде Р, 2Р, 3Р модульдерінің әртүрлі мәндеріне сәйкес $4r_i$-1 мәндерінің коэффициенттеріне байланысты орындалатын операциялар түрлері көрсетілген.

Кесте 3.1 – Әр түрлі $4r_i$-1 коэффициенттері бойынша Р, 2Р, 3Р - мен жасалған операциялар.

№	Өзара байланыс	Орындалатын операциялар
1	4ri-1 < p	ri = 4ri-1
2	p ≤ 4ri-1 < 2p	ri = 4ri-1 + p +1
3	2p ≤ 4ri-1 < 3p	ri = 4ri-1 + 2p +1
4	3p ≤ 4ri-1	ri = 4ri-1 + 3p +1

Р < $4r_i$-1 <2Р коэффициенттері кезінде, бір мезгілде ИЛИ2 және И3 контурлық блогына берілетін ИЛИ1 тізбегінің шығуында бірыңғай сигнал пайда болады, екінші модуль кіретін модуль кері бағытта шығарылатын Р коды беріледі, олар СМ қабылдағышының дұрыс кірістеріне беріледі. $4r_i$-1

коды жинағыштың сол кірісіне жіберіледі және қосқыштың төменгі регистріне +1 сигналы жіберіледі, ал жұмыс кезінде $r_i = 4r_i\text{-}1 + P + 1$ жұмыс жасайды.

$4r_i\text{-}1 > 2P$ және $4r_i\text{-}1 < 3P$ көрсеткіштері кезде, И2 тізбегінің шығысы ИЛИ2 тізбегінің кіруіне және И4 тізбектерінің кірісіне берілетін бірыңғай сигнал шығарады, екінші ақпарат кірісі жеткізіледі кері 2Р кодында екі есе үлкейтілген модуль биті бар. ИЛИ1 схемалары СМ ендіргішінің дұрыс кірістеріне беріліп, +1 коды жинақтағыштың төменгі дәрежелі битіне беріліп, алушы $r_i = 4r_i\text{-}1 + 2P + 1$ операцияларын орындайды.

СС-3 салыстыру сұлбасының екінші шығысындағы $4r_i\text{-}1 \geq 3P$ коэффициенті кезде, И5 тізбектерінің блок кіруіне бірыңғай сигнал беріледі. Бұл тізбектің ақпараты 3Р модулінің биттерімен орындалады. ИЛИ1 кодтарының схемасы арқылы алынған кодтар 3Р жалдаушының дұрыс кірісіне беріледі. Бұл жағдайда қосалқы құрал $r_i = 4r_i\text{-}1 + 3P + 1$ операциясын орындайды.

Редукционды модуляция құрылғыларында $4r_i\text{-}1 < P$ жағдайында дәйекті жұмыс, алдыңғы қалдық қалдық тізілімде сақталады.

$4r_i\text{-}1 < P$ бар матрицалық тізбектерде $4r_i\text{-}1$ мәні И0 тізбегі және ИЛИ3 логикалық схемасының блогы арқылы келесі ФЧО-ға жіберіледі.

Кездейсоқ құрылғының құрылымы

3.2 сурет модульдер арқылы сандарды жылдам түрлендіруге арналған құрылғының блоктық схемасын көрсетеді, оған мыналар кіреді:

– РгА нөмірінің 2n + 2 биті солға қарай екі санға ауысады;

– РгЗР және РгР тіркеледі, онда операция басталғанға дейін, тиісінше, модульдің үш еселенген мәні - 3Р және Р модулінің мәні;

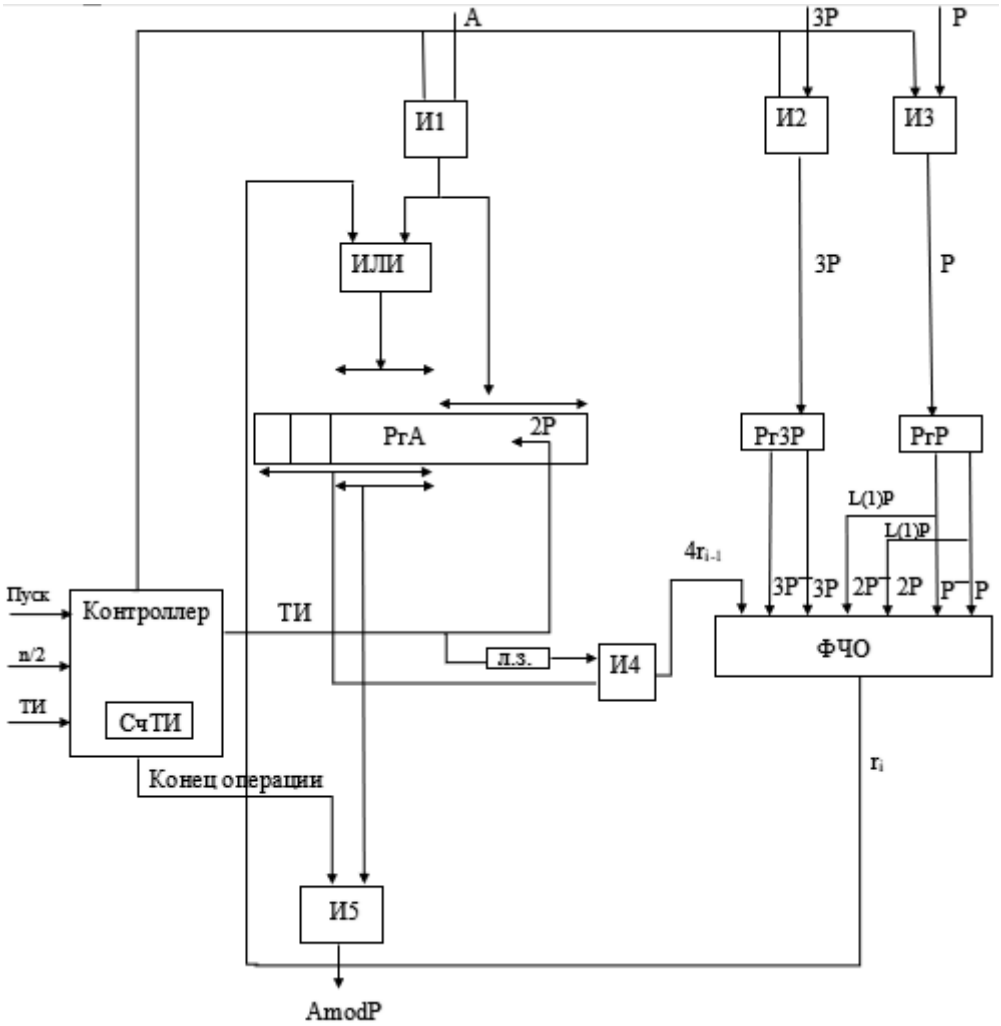
– ФЧО ішінара қалдықтары;

– контроллер, оқуға арналған есептегіш бар.

РгА тізбегінің аға тізбегі И4 блок диаграммасы арқылы ФЧО-мен байланысты. И арқылы $4r_i\text{-}1$ мәнін РгА тізілімінен жіберетін контроллерден келетін ТИ бақылауында. 3Р, 3Р, 2Р, 2Р, Р, Р мәндері ФЧО кірістеріне беріледі. ФЧО-ның блоктық схема арқылы немесе одан кейінгі ішінара теңгерімін шығару РгА-ның кірісіне беріледі. И5 диаграммасының блогы бойынша «Операциялар соңы» сигналы арқылы есептеу нәтижесі шығарылады. R = AmodP есептеу үшін қажетті «старт» сигналы, ТИ сағат сигналдары және ауысымдардың саны n / 2 контроллердің енгізулеріне жіберіледі.

Құрылғы келесідей жұмыс істейді. «Бастау» сигналы бойынша А және Р операндалары тиісінше РгА, Рг3Р және РгР тіркеушілерінде тіркеледі. Сонымен қатар, «СТАРТ» сигналы ауысымдардың n / 2 санын контрсағалық сағаттық импульстерде жазады. Мультифункционалды қабылдаудан кейін әр модульде контроллер ТИ сағат импульсін шығысқа шығарады, ол РгА мазмұнын солға екі санмен ауыстырады. Кешіктіріп кеткен ТИ кешігу кейін Л.3, РгА биттерінің мәні қалыптасады, онда 4R0 мәні И4 тізбегі арқылы

қалыптасады, ФЧО жиынтықтың кірістеріне беріледі. қалған қалдықтардың мәні қалыптасады. Бұл теңгерім ИЛИ схемасы арқылы РгА-да жазылады. Сағаттық импульс ТИ есептегіш көрсеткішін біреу азайтады. Осы сәтте келесі ТИ схемаға түседі, оның көмегімен келесі қалдық ФЧО-да қалыптасады, ол РгА-ға жіберіледі және т.б. Төмендегі 3.2-суретте көрсетілгендей.



Сурет 3.2 – Тізбектей әрекет ету модулі бойынша сандарды келтірудің жылдам әрекет етуші құрылғысының құрылымдық сұлбасы

N / 2 сағаттық импульс ұсынылғаннан кейін, РгА-да сақталатын ФЧО шығу кезінде n / 2 қалдық құралады. Бұл импульстың көмегімен СчТИ нөлдік күйге көшеді және «Операция соңы» сигналын шығарады. Бұл әрекет нәтижесінде РгА жоғары биттерінің нәтижесі И5 тізбегі арқылы алынады [8].

3.2 Сандарды модульге келтіруші құралды ПЛИС-те алгоритмдеу

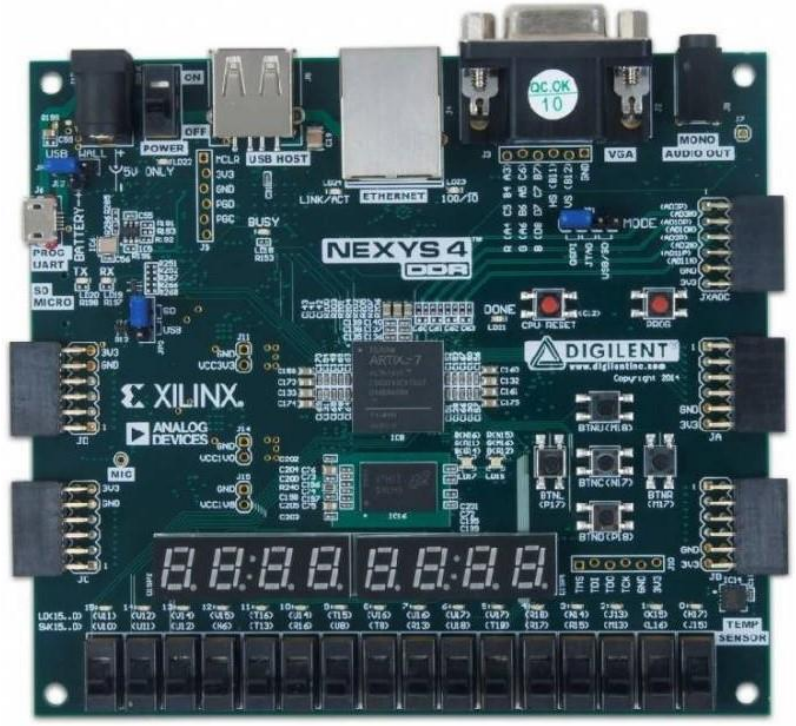
Сандарды модуль бойынша келтіру үшін жылдам әрекет ететін құрылғының алгоритмін тексеру тізбектей әсер ететін ең аз аппараттық шығындармен бағдарламаланатын логикалық интегралды схемаларда (ПЛИС) жүзеге асырылды. Жұмыс орны Xilinx фирмасынан Nexys4 Board бағдарламаланатын логикалық интегралды сұлба платасын таңдап алды (3.3-

сурет). Ал модуль бойынша санды есептеу схемасын сипаттау үшін Verilog тілі таңдалған. 3.2-кестеде ПЛИС Artix-7 платасының ресурстары көрсетілген

Кесте 3.2 – ПЛИС Artix-7 ресурстары

Ресурс	Саны
LUT	63400
FF	126800
IO	210
BUFG	32

Кіріс деректерін енгізу және аралық нәтижелерді көзбен көрсету үшін FPGA Board барлық қажетті порттар мен перифериялық құрылғылармен жабдықталған, олардың негізгілері 16 ауыстырып-қосқыш, 16 жарықдиодты, сондай-ақ USB-UART көпірі, DDR2 128MB және т. б. болып табылады [14].



Сурет 3.3 – Nexys 4 платасы

3.4-суретте санын келтіру кезінде ішінара қалдықтардың мәнін қалыптастырудың уақытша диаграммасы келтірілген және $A_{a7} \div a_0$ жоғарғы биттері $r_0 = 11_{10} = 1011_2$ болып табылады.

$$A_{a7} \div a_0 = 187_{10} = 10111011_2,$$

$$P = 14_{10} = 1110_2,$$

$$2P = 28_{10} = 11100_2,$$

$$3P = 42_{10} = 101010_2$$

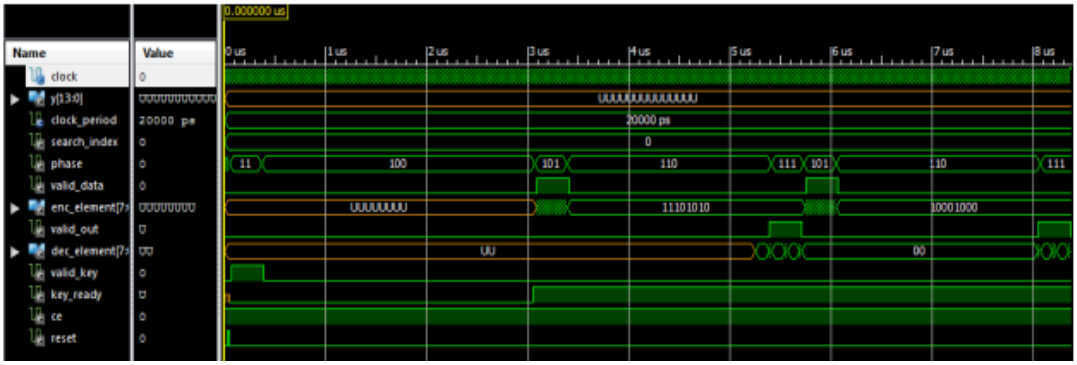
3.4-суретте ТИ1 тактілік импульстің алдыңғы фронты бойынша А регистрінің мазмұны солға екі разрядқа жылжиды және регистрде үлкен алты разрядта $4r_0 + a_3a_2$ қалыптасады, бұл 101110_2=46 екілік кодына сәйкес келеді, яғни И4 схемасының шығуында (Сурет 3.4) 46 саны $P = 14_{10}$, $2p = 28_{10}$ және $3P = 42_{10}$ және СС-3-тің 2 шығуында 1 сигналы қалыптасады, ол сумматорда операцияны орындауға әкеледі 46-3P = 46-42 = 4 = r_1 және $4_{10} = 100_2$ екілік сандар РгА регистрінің жоғарғы дәрежелеріне беріледі.

РГА регистрінің ТИ2 тактілік импульсінің алдыңғы фронты бойынша солға екі разрядқа жылжытады және онда $4R_1 + a_1a_0 = 16 + 3 = 19_{10}$ тоқтайды. 1-ші және 2-ші сигналдар саны Р, 2р және 3Р салыстырылады және 2-ші СС-1 шығыста 1 сигналы шығарылады, ол 19-P=19-14=5 операцияларды орындауға әкеледі, бұл 3.4 суретте көруге болады, яғни R=5-ші операция нәтижесі 187mod14=5 болып табылады.

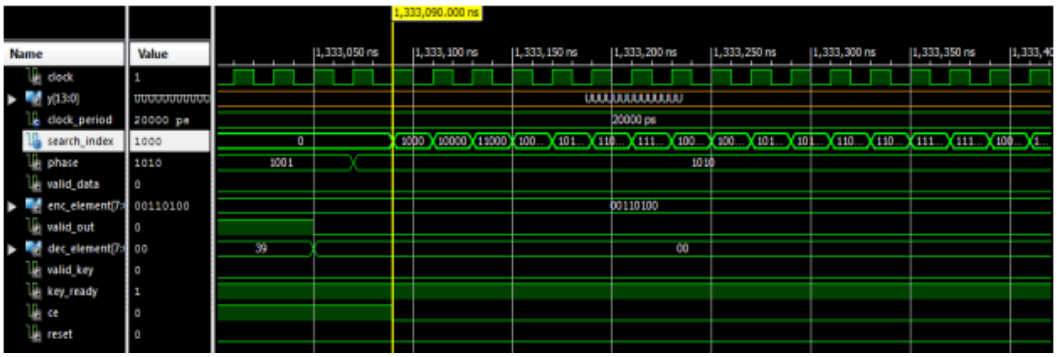
3.5-суретте $A_{a15} \div a_0 = 27317_{10}$ және $P = 209_{10}$; $2P = 418_{10}$ және $3P = 627_{10}$ сандар үшін жартылай қалдықтарды қалыптастырудың уақыт диаграммасы келтірілген.

$A_{a15} \div a_0 = 01101010110001_2$ және $P = 11010001_2$ осы жерден $R_0 = 01101010_2 = 106_{10}$ диаграммадан R_1=8, r_2=0 және r_3=0, r_4=147 көруге болады.

СМ2 тартқыштың шығуындағы $r_2 = r_3$ мәндерін есептеу кезінде біз PrA-ның «ескі» ішінара қалдықтарын сақтап қалатын теріс айырмашылықтар пайда болады.



Сурет 3.4 – 8-биттік сан үшін алгоритм диаграммасы



Сурет 3.5 – 16-биттік сан үшін алгоритм диаграммасы

Сандарды ішінара қалдықтарды формалау құрылғыларында екі екілік сумматорды үш салыстыру схемасына ауыстыра отырып, сандарды модуль бойынша келтірудің жылдам әрекет ететін құрылғысының құрылымын азайтуға болады.

4 Өмір тіршілік қауіпсіздігі

4.1 Компьютердің адам денсаулығына әсері

Жастар арасында салауатты өмір салтын қалыптастыру-қазіргі қоғамның өмір салтының көптеген компоненттерін қамтитын және жастардың тіршілік әрекетінің негізгі салалары мен бағыттарын қамтитын күрделі жүйелі процесс.

XX ғасырдың соңында бас айналу жылдамдығын алған ғылыми-техникалық прогресс компьютер және компьютерлік технологиялар сияқты қазіргі заман ғажабының пайда болуына себеп болды.

Компьютерлер біздің санамыздағы өз орнын ала отырып, адам өміріне тез енгізілуде, ал біз көбінесе осы қымбат бағалы түсті металл кесектерінің жұмыс қабілеттілігіне байланысты бастайтынымызды түсінбейміз [15].

4.1.1 Компьютер алдында дұрыс отыру ережесі

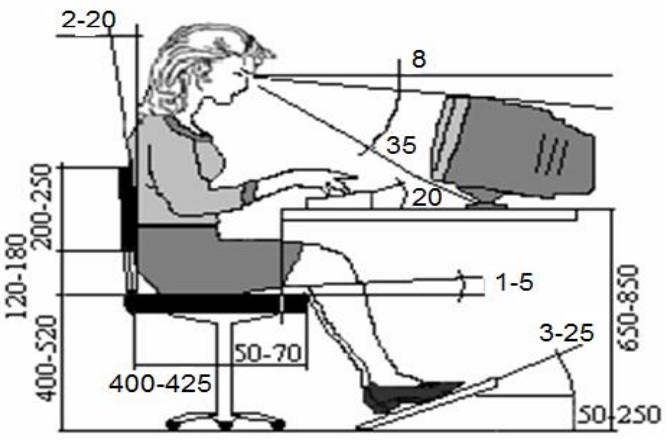
Монитор мен пернетақтаны биіктігі бойынша дұрыс орналастырудың маңызы зор. Монитор ыңғайсыз тұрған жағдайда арқа және мойын бұлшық еттеріне салмақ түсуі салдарынан бас ауруы мүмкін. Қарапайым бір қағида бар: монитордың жоғарғы шеті көзбен бір деңгейде болуы, ал осы деңгей мен бейне беттің орталығы арасындағы бұрыш 15 градусты құрауы тиіс:

– арқаңызды тік ұстаңыз;

– ықтарыңызды бос ұстаңыз, шынтақтарыңыз тік бұрыш жасап бүгілген болсын. Басыңызды сәл алдыға еңкейтіп тік ұстаңыз;

– орындығыңыздын отырғышы жұмсақ болуы, тізелеріңіз тік бұрыш жасап бүгіліп, табандарыңыз жерге толықтай тіреліп тұруы тиіс;

– арақашықтықты сақтаңыз. Көз бен монитор экраны арасындағы қашықтық 70 см – ден аз болмауы тиіс. Басқаша айтсақ, сіз қолыңызды алдыға созып, бейне бетке әрең жетуіңіз тиіс (4.1-суретте корсетілген) [15].



Сурет 4.1 – Компьютер алдында дұрыс отыру ережесі

Компьютерде жұмыс істеген кезде біз одан Білім түрінде ғана емес, сонымен қатар біздің денсаулығымыз үшін зиян да пайда табатынын ұмытамыз.

Компьютердің адам денсаулығына әсері:

– тұрақты отыруға жағдай;

– үлкен көру кернеуі;

– қолмен қайталанатын жүктемелермен;

– сондай-ақ компьютер адамның психикасына әсер ететін жүйке-эмоциялық кернеу.

Компьютердің денсаулыққа қауіптілігі аталған проблемалардың адам денсаулығына әсері бірден емес, тек бір уақыттан кейін ғана пайда болады.

Компьютермен жұмыс істеу кезінде адам денсаулығына әсер ететін негізгі факторлар:

– монитордың жыпылықтауы (көзге әсер етеді);

– электромагниттік сәулелену;

– шу (тітіркендіреді);

– психикаға әсер ету;

– қысылған поза (омыртқаға әсер етеді);

– үй-жайдың микроклиматы (ылғалдылығы, шаңдылығы);

– жұмыс режимі (демалуға қажетті үзілістер).

Компьютер бүкіл ағзаға зиянды әсер етеді:

– көру мүшелері;

– есту;

– тірек-қимыл аппараты;

– арқа.

Клавиатурамен қарқынды жұмыс шынтақ буындарында, білектерде, білектерде, қол саусақтарында және қол саусақтарында ауырсыну сезімін тудырады. Қазір пернетақталар пайда бола бастады, олардың эргономикасы қолға түсетін жүктемені азайтуға арналған. Клавиатурадағы негізгі клавиш блогы екі бөлікке бөлінген, осылайша пайдаланушыға қолды жылжытуға және шынтақтарды қоюға тура келеді.

Компьютерде ойнайтындарға тән бел мен мойынның ауырсынуы веналар мен аяқ-қол буындарының ауруларына әкелуі мүмкін. "Программист синдромы" (жауырынның арасындағы ауырсыну) жүрек пен өкпеге қауіп төндіреді. Ол әдетте трапеция тәрізді бұлшықеттердің спазмымен жүреді, олар омыртқаны құтқару әрекеттерінде миға баратын артерияларды қысады.

Бірақ болашақта өзін түзетілмейтін салдарлардан қорғау үшін компьютерде жұмыс істеу ережелерін сақтау қажет:

– адам бетінен мониторға дейінгі қашықтық кемінде 60-70 см болуы тиіс;

– компьютермен жұмыс істеу кезінде үй-жай жақсы жарықтандырылуы тиіс. Сонымен қатар дербес компьютері бар үй-жайлардағы жарықтандыру аралас болуы тиіс: табиғи, күн сәулесінің есебінен, жасанды;

– экранның жарықтығы мен қоршаған кеңістіктің арасында үлкен контрасты болдырмау керек;

– компьютермен қараңғы немесе жартылай қараңғы үй-жайда жұмыс істеуге тыйым салынады;

– жұмыс уақытында көзге арналған гимнастика жүргізу қажет;

– компьютермен жұмыс істеу кезінде, сондай-ақ дұрыс осанканы сақтау керек.

Компьютерді артық пайдалану – демалыс уақытының көп бөлігін, соның ішінде түнгі уақытты өткізу, қала бойынша, метрода жүру жолында ойын-сауық үшін қалта компьютерлерін пайдалану. Уақыт компьютерді пайдалануға, оқу, өндірістік қызметке және денсаулық жағдайына нұқсан келтіретін DVD-дискілер мен телебағдарламаларды көруге жұмсалады.

Егер дәстүрлі тәуелділіктің түрлерін қалыптастыру үшін жылдар қажет болса, онда Интернетке тәуелділік үшін бұл мерзім күрт қысқарады.

Компьютерлік техниканы пайдаланушының қауіпсіздік дәрежесі әр түрлі халықаралық стандарттармен реттеледі, олар жылдан жылға барлық стрижокқа айналады. Ғалымдардың соңғы зерттеулері компьютерлік техниканың өзі ғана емес, адам ағзасына теріс әсер етудің тікелей факторы, оның дұрыс орналаспауы, еңбек пен демалуға қатысты қарапайым гигиеналық нормалардың сақталмауы екенін көрсетті.

Компьютердің адам денсаулығына әсер ету проблемасын зерттей отырып, қазіргі заманғы ақпараттық технологиялар құралдары пайдаланушының ағзасына қатты әсер ететіні және компьютермен "қарым-қатынас" жұмыс уақытын қатаң регламенттеуді және мұндай әсер етуді азайту және алдын алу бойынша санитарлық-гигиеналық іс-шараларды әзірлеуді талап ететіні айқын болады.

Адамдар бұл туралы бүгін ойлануы керек. Әр түрлі ғылыми пәндер осы саланы зерттеуде бірігуі тиіс, ал психология осы жұмыстардың — адамның компьютермен өзара іс-қимылының психологиялық аспектілерін зерттеу жұмыстарының басында болуы тиіс [15].

4.2 Электр магниттік өрістердің адам ағзасына тигізетін қаупін қайтару

Электр магниттік өріс-зарядталған бөлшектер арасындағы өзара іс-қимыл жасайтын материяның ерекше түрі. Өзара байланысты айнымалы электр өрісі және магнит өрісі. Электр және магнит өрістерінің өзара байланысы олардың біреуінің кез келген өзгеруі екіншісінің пайда болуына әкеп соқтырады: жылдам қозғалатын зарядтармен (көзімен) туындайтын айнымалы электр өрісі кеңістіктің аралас салаларында айнымалы магнит өрісін қозғайды, ол өз кезегінде кеңістіктің оған іргелес аймақтарында айнымалы электр өрісін қозғайды және т.б. осылайша электромагнитті өріс нүктеден көзден жүгіретін электромагнитті толқындар түрінде кеңістіктің нүктесіне дейін таралады. Тарату жылдамдығының аяқ-қолының арқасында электр магниттік өріс оны тудырған көзден дербес болуы мүмкін және көзін

жою арқылы жоғалмайды (мысалы, радиотолқындар сәулелендіру антеннасында токтың тоқтауымен жойылмайды).

Электр магниттік өрістерді адам көрмейді және сезінбейді, сондықтан бұл өрістердің қауіпті әсерінен әрдайым сақталмайды. Электр магниттік сәулелер адам ағзасына зиянды әсер етеді. Электролит болып табылатын қанда электромагниттік сәулелердің әсерінен тіндердің қызуын тудыратын иондық токтар пайда болады. Жылу шегі деп аталатын сәуленің белгілі бір қарқындылығы кезінде организм пайда болған жылуды жеңе алмайды [16].

Қызуы әсіресе интенсивті емес қан айналымы (көз, ми, асқазан және т.б.) әлсіз дамыған тамыр жүйесі бар органдар үшін қауіпті. Көзді бірнеше күн бойы сәулелендіру кезінде хрусталик майлануы мүмкін, бұл катаракту тудыруы мүмкін.

Жылу әсерінен басқа электр магнитті сәулелер жүйке жүйесіне қолайсыз әсер етеді, жүрек-қантамыр жүйесі, зат алмасу функцияларының бұзылуын тудырады.

Электр магнитті өрістің адамға ұзақ әсер етуі шаршау тудырады, жұмыс операцияларын орындау сапасының төмендеуіне, жүрек аймағындағы күшті ауырсынуға, қан қысымы мен пульстің өзгеруіне әкеледі.

Электр магнитті өрістің адамға әсер ету қаупін бағалау адамның денесімен сіңірілген электр магнитті энергияның шамасы бойынша жүргізіледі.

Электр магниттік өрістердің сипаттамалары

Ток өтетін өткізгіштің жанында электр және магнит өрістері бір мезгілде пайда болатыны белгілі. Егер ток уақыт өзгермесе, бұл өрістер бір-біріне байланысты емес. Айнымалы ток кезінде магнит және электр өрісі бір-бірімен байланысты.

Электр магниттік сәулеленудің негізгі сипаттамалары жиілік, толқын ұзындығы және поляризация деп саналады.

Жиілігі электр магниттік өріс — бұл саны тербеліс өріс секундына. Жиілікті өлшеу бірлігі – герц (Гц), секундына бір тербеліс жасалатын жиілік.

Толқын ұзындығы-бір-біріне жақын екі нүктелер арасындағы қашықтық.

Поляризация-бұл электр өрісінің кернеулігі векторларының бағытталған тербеліс құбылысы немесе магнит өрісінің кернеулігі.

Электр магниттік өріс белгілі бір энергияға ие және электр және магнит кернеулігімен сипатталады, бұл еңбек жағдайларын бағалау кезінде ескеру қажет.

Электр магниттік өріс көздері

Жалпы электр магнитті фон табиғи (Жердің электрлік және магниттік өрістері, күн мен галактикалардың радиосәулеленуі) және жасанды (антропогендік) шығу тегі (телевизиялық және радиостанциялар, электр беру желілері, электр тұрмыстық техника) көздерінен тұрады. Электр магниттік сәуле шығару көздері радиотехникалық және электрондық құрылғылар, индукторлар, термиялық қондырғылардың конденсаторлары,

трансформаторлар, антенналар, толқынды трактілердің фланецті қосылыстары, аса жоғары жиіліктегі генераторлар және т. б. қызмет етеді.

Қазіргі заманғы геодезиялық, астрономиялық, гравиметриялық, аэрофототүсірілім, теңіздегі геодезиялық, инженерлік-геодезиялық, геофизикалық жұмыстар электр магниттік толқындар диапазонында жұмыс істейтін аспаптарды, ультражоғары және аса жоғары жиіліктерді пайдалана отырып, сәулелену қарқындылығы 10 мкВт/см2 дейін жұмыс істейтіндерді қолдана отырып орындалады [16].

4.2.1 Сәулеленуді бақылау

Жылына кемінде 1 рет Е, Н, σ өлшей отырып жүргізеді.

Өлшеуге арналған датчиктер: диполь (Е үшін); рамка (Н үшін); рупор антеннасы (σ үшін) болып табылады.

Электр магниттік сәулеленуден қорғау тәсілдері мен құралдары:

– көзді немесе жұмыс орнын экрандау;

– қашықтықты қорғау (жұмыс орнын көзден жою);

– ЖҚҚ (жеке қорғау құралдары);

– жұмыс орнына тікелей және шағылысқан энергияның ең аз бағытталуын қамтамасыз етуге мүмкіндік беретін сәуле шығаратын жабдықты үй-жайға ұтымды орналастыру;

– сәулеленудің шеткі рұқсат етілген деңгейінен асып кетуі туралы сигнал беру (П2-2 типті сигнализатор);

– персонал мен жабдықтардың жұмыс ұзақтығын шектеу [17].

4.2.2 Экрандау

Шағылыстыратын экрандар үшін жоғары өткізгіштігі бар металдар (мыс, жез, алюминий, болат) пайдаланылады. Қалыңдығы 0,5 мм табақтар түріндегі экрандар (немесе есептеу бойынша); сымнан жасалған торлар 0,1 1,0 мм ұяшықтары бар торлар 11, 10, 10 мм (құрылғыға байланысты қажет). Экрандардың пішіні: жабық (камералар); тұйықталмаған (қалқан, П-тәрізді, жартылай сфера және т.б.).

Электр магнит экрандарын пайдаланған кезде энергия металлдың үстіңгі қабатына сіңеді, көз жағына ішінара әсер етеді. Экранның негізгі сипаттамасы - экрандау тиімділігі, яғни электр магниттік өрістің әлсіреу дәрежесі Э = σ /σс экр.

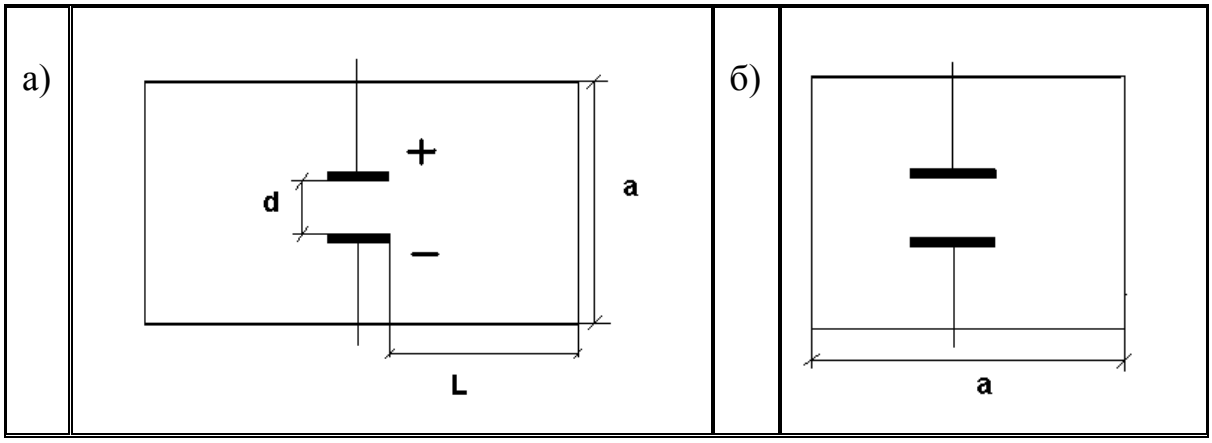
Жоғары жиілікті термиялық қондырғыларды экрандау

Жұмыс элементі-конденсатор

Есептеу экранның өлшемін анықтаудан тұрады. Электр өрісінің кернеулігі Е экранмен әлсірейді және (Х) көзден операторға дейінгі қашықтықтың квадратына кері пропорционал түсіреді.

$$E_{р.м.} = E_{ист.} * e^{-\frac{\pi(1/a)}{a}} * \frac{1}{x^2} \leq E_{доп.} \quad (4.1)$$

Экран ретінде, мысалы, тұйық шаршы түтік қолданылуы мүмкін(4.2-сурет) [17].

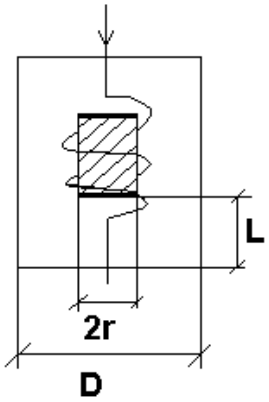


Сурет 4.2 – экранның бойлық және көлденең қимасы.

Экранның геометриялық өлшемдерінің қатынасы:

$$\frac{l}{a} = \frac{1}{\pi} ln \frac{\text{Е}_{\text{ист}}}{\text{Е}_{\text{доп}} * x^2} \quad (4.2)$$

Мұнда, $\text{Е}_{\text{р.м.}} = \text{Е}_{\text{доп.}}$ – жұмыс орнындағы кернеу
Жұмыс элементі – индуктор(4.3-сурет)
Экран – d диаметрі бар тұйық цилиндр.



Сурет 4.3 – индуктордың сұлбасы

Жұмыс орнындағы магнит өрісінің кернеулігі:

$$\text{Н}_{\text{р.м.}} = \left(\frac{I * r * n}{4}\right) * e^{-3.6\left(\frac{l}{D}\right)} * \frac{1}{x^2} \quad (4.3)$$

Экранның геометриялық өлшемдерінің қатынасы:

$$\frac{l}{D} = \frac{1}{3.6} ln \frac{\text{Н}_{\text{ист.}}}{\text{Н}_{\text{доп.}} * x^2} = \frac{1}{3.6} ln \frac{I * r * n}{4x^2 * \text{Н}_{\text{доп.}}} \quad (4.4)$$

мұнда I, r, n – ток, индуктор радиусы, оның орамдарының саны;

х – жұмыс орнына дейінгі қашықтық [17].

4.2.3 Аса жоғарғы жиілік энергиясынан қорғау

Толқын жолға сәулеленуді әлсірету үшін радио локациялық станция сипаттамаларын алу кезінде жұтатын жүктемені – ұнтақ темір, граффит - цементті толтырғыш және т. б. қосады.

Энергияның кемуінен тұйық және тұйықталмаған түрдегі металл экрандармен қорғалады.

Экран қабырғасына түсетін Энергия $\sigma_{\text{раб.место}} = \sigma_{\text{х}} \text{e}^{-2kz}$ заңы бойынша жойылады

$$K = \sqrt{\frac{\varphi * \gamma * \mu}{2}} \tag{4.5}$$

мұндағы К-экран материалындағы электромагниттік энергияның әлсіреу коэффициенті

ω – айналмалы жиілік

γ – меншікті электр өткізгіштігі

μ – ... экранның магниттік өткізгіштігі

Z – электрмагниттік энергияның экран материалына ену тереңдігі немесе қажетті қалыңдығы

$$Z = \frac{1}{2k} ln \frac{\sigma_k}{\sigma_{\text{доп.}}} \tag{4.6}$$

Металдар оларға түсетін барлық энергияны көрсетеді.

Экрандардан, жабдықтардан ішінара шағылысқан энергияны энергия жылу шығындары түрінде шашырайтын өткізбейтін материалдардан (каучук, поролон және т. б., өткізуші қоспалары бар) жабындардың көмегімен жұтады.

Кез келген материалды көрсету коэффициенті мынадай формула бойынша анықталады:

$$\text{К}_{\text{отр.}} = \sqrt{\frac{\varepsilon_{\text{а}} - \mu_{\text{а}}}{\varepsilon_{\text{а}} + \mu_{\text{а}}}, \varepsilon_{\text{а}} \approx \mu_{\text{а}}, \text{К}_{\text{отр.}} \to 0} \tag{4.7}$$

Жұтатын жабындардың басқа түрі тура және кешіктіретін шағылысқан толқындардың амплитудаларын азайту принципі бойынша әрекет етеді. Бұл интерференциялық сіңіру жабындары [18].

Аса жоғарғы жиілік қондырғыларын баптау және сынау кезінде сәулеленуден қорғау.

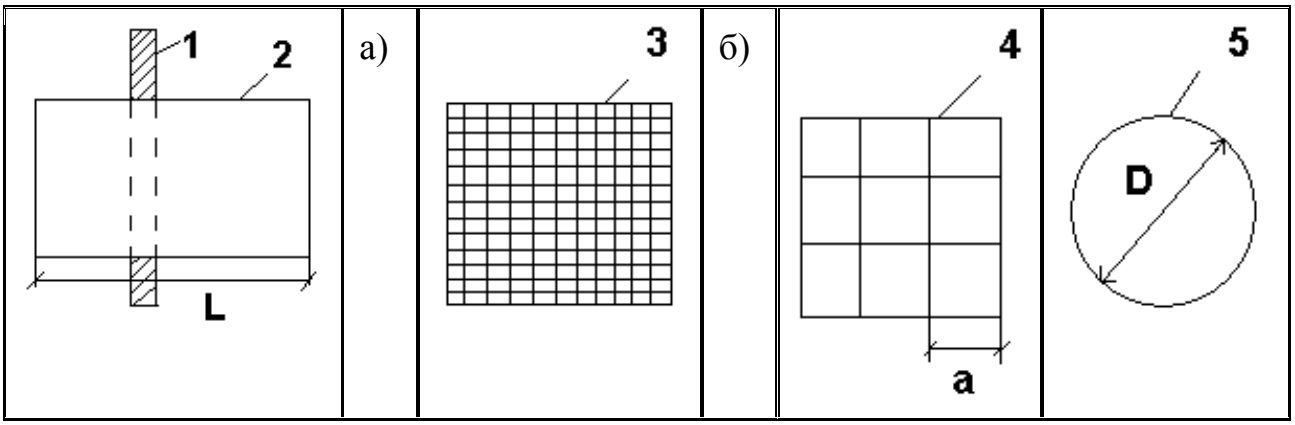
Орнату жабық камералар-экрандарда орындалады, оған қойылатын талаптар(4.4-сурет):

1) Толық қуатпен жұмыс істеу кезінде энергияның ағуы $\sigma_{\text{доп.}}$ – тан аспауы қажет;

2) Орнатуды қашықтан басқару;

3) Есіктерді құлыптау (есіктерді ашу кезінде кернеуді автоматты түрде жояды);

4) Желдеткіш, қарау тесіктері, басқару тұтқалары қоршаған ортаға энергияның ағып кетуінен қорғалуы тиіс.



Сурет 4.4 – Тесік арқылы ағып кетуден қорғау тәсілдері

1 – орнату қабырғасы немесе экран;

2 – L – ұзын құбыр;

3 – құбырға кіруде және шығуда ұсақ ұяшықтары бар тор;

4, 5 – сот түріндегі немесе дөңгелек құбыр қимасы.

а) кіру және шығу торлары түріндегі Қорғаныс. Тор ұяшығының өлшемі. Тор толқынның қуаты мен ұзындығына байланысты кестелерден таңдалады;

б) құбырдың ішінде барлық ұзындығы бойынша l – тен жасалған металл тор орналасады [18];

Тор өлшемдерінің қатынасы:

$$\frac{l}{a} = 0.37lg\frac{\sigma_{\text{ист}}}{\sigma_{\text{доп.}}} \quad (4.8)$$

в) ашық құбыр - өлшемі бар цилиндр:

$$\frac{l}{D} = 0.31\frac{\sigma_{\text{ист.}}}{\sigma_{\text{доп.}}} \quad (4.9)$$

4.3 Программист–оператордың жұмыс зонасына қойылатын талаптар

4.3.1 Программист–оператордың жұмыс зонасындағы микроклимат

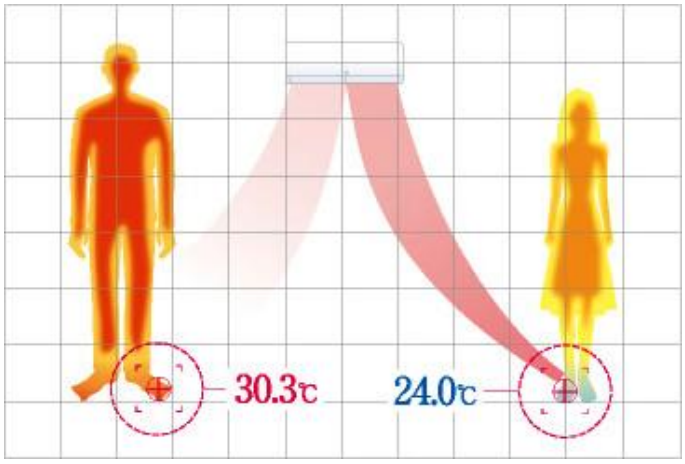
Өндірістік бөлмелердің микроклиматы – бұл бөлменің ішкі климат ортасы. Микроклимат адам организміне әсер ететін температура, ылғалдылық және ауаның қозғалыс жылдамдығымен анықталынады.

Программист - оператордың орналасу бөлмесінде оператор оңай физикалық жұмыстар атқарады, сондықтан келесі шаралар орындалады, ауа температурасы оптималдылығы – 22С (рұқсат етіледі – 20 - 24С), ауаның

оптималды ылғалдылығы – 40 - 60% (рұқсат етіледі - 75% аспау керек), ауаның қозғалыс жылдамдығы 0.1 м/с -тан аспау керек.

Ауаның табиғи өзгеруіне байланысты автоматтандырылған кондиционерлер пайдаланады, ол температураны, ылғалдылықты, ауаның қозғалыс жылдамдығын және жиілікті суық уақытта оптималды водяной кезге, ал жылы уақытта кондиционердің ауасын пайдаланады.

Автоматтандырылған кондиционерлерді пайдалану өте ыңғайлы, ауа бөлмесін кондиционердің регуляторы арқылы кез келген бөлме параметрін беріп қоюға болады(4.5-сурет) [19].



Сурет 4.5 – микроклимат

4.3.2 Дербес компьютерлердің орналасуына және жабдықталуына қойылатын талаптар

Есептеуіш техникасы кабинетінде оқушылардың жұмыс орнын олардың кіріп – шығуына ыңғайлы етіп орналастыру қажет. Бүгінгі күнге дейін компьютерлік сыныптарда жабдықтарды орналастырудың бірнеше тәсілдері сынақтан өткізіліп, оларды тиімді орналастырудың кейбір талаптары тұжырымдалды. Сонымен бірге, мұндай сыныптарда ауаның ылғалдылығы, бөлме температурасы, шудың естілуі, электрдің және радиацияның әсері, т.б. ескеріледі [20].

Жалпы жағдайда:

– оқушылар мен мұғалімнің жұмыс орнының қауіпсіздігі;

– кабинеттегі жабдықтардың орналасу ретінің оқушыларға ыңғайлы болуы;

– оқушылар мен мұғалімнің әртүрлі оқыту тәсілдерін үйлестіруге қолайлылығы;

– бақылауды ұйымдастыру тұрғысынан мұғалімге ыңғайлы болуы;

– қызмет көрсетуге және жөндеуге қолайлы болуы, кабинет ауданын тиімді пайдалану т.б. ескерілуі тиіс.

Мектепте және мектепке дейінгі мекемелерде есептеуіш техника кабинетіндегі бір жұмыс орнының ауданы 6 м , ал көлемі 24 м , биіктігі 4 м-ден кем болмауы тиіс және информатика кабинеті жанынан егер

компьютерлер саны 10-нан кем болмаса, онда ауданы 18 м кем емес қосалқы бөлменің болуы стандартқа сай болып табылады.

Компьютерді орналастырудың екі жағдайы 4.3 – суретте көрсетілген. 1 – жағдайда дербес компьютерлер II (периметр) түрінде орналастырылады. Бұл оқушылармен кабинеттегі жабдықтар үшін қауіпсіз деп есептеледі. Лабораториялық жұмыстар үшін мұндай орналастыру тиімді болғанымен, теориялық сабақтар үшін қолайсыздығы байқалады. 2-жағдайда, компьютерлер қабырғаны бойлай немесе қабырғаға жанай орналастырылады. Сынып бөлмесіндегі бос орындарға үстелдер мен орындықтар қойылады. Бұл сабақ формаларын алмастырып, үйлестіріп жүргізуге мүмкіндік береді. Оқушылардың бір бөлігі ортада отырып, қалғандары дербес компьютерлер алдында отырып жұмыс жасай алады. Екі орынды үстелдерді біріктіріп қоюға тиым салынады. Егер үстелдер қатар бойымен орналастырылса, онда олардың арақашықтығы 1 м немесе 1,1 м болуы [20].

4.3.3 Компьютер кабинетінде өрт қауіпі

Өрт – бұл адамның өмірі мен денсаулығына, қоғам мен мемлекетке зиянын тигізетін, қоршаған ортаға үлкен материалдық зақым келтіретін, қоршаған ортадағы заттардың бақылаусыз жануы. Ең күрделі, зиян тигізетін өрттер өртке қауіпті объектілерде және басқа да зақымдау факторлары (жарылыс, улы заттардың жиналуы т.б.) бар объектілерде болады. Сонымен бірге, адамдар көп шоғырланған жерлерде өрт шығу қаупі бар.

Өрт қауіпсіздігі – бұл өрт болу мүмкіндігін болдырмау және оның пайда болған кезінде адамдарға, құрылыс және материалдық құндылықтарға өрттің қауіпті факторларының жағымсыз әсерлерін жою үшін қажетті шараларды қолдану болып саналады.

Өрт қауіпсіздігі өрттің алдын алу шаралары мен және белсенді өрт қорғанысымен қамтамасыз етіледі. Өрттің алдын алу болып өртті болдырмау немесе оның салдарын азайтуға бағытталған іс-шаралардың кешені саналады. Белсенді өрт қорғанысы – бұл өрт немесе жарылысқа қауіпті жағдайларымен белсенді күресуді қамтамасыз ету шаралары.

Компьютер кабинетінде өрт болған жағдайда ең бірінші адамның іс-қимылы:

– біріншіден өрт сөндіретіндерге хабарлау;

– ыстық жанғыш затты толықтырғыштай бөлектеу;

– ауадағы оттегі концентрациясын азайту;

– ыстық жанғыш заттың температурасын оталдыру температерасынан төмендету.

Компьютер кабинетінде өрт болған жағдайда өртті су мен сөндіруге болмайды, себебі компьютер желіге жалғанған болса, үлкен мөлшерде ток ұру кауіпі бар. Өртті арнайы өрт сөндіргіш құралымен сөндіру қажет.

Өрт сөндірудің кең тараған құралдары болып: көмірқышқылы, сулағыштар, химиялық және ауалық – химиялық көбік, галойдталған көмірсутектер түйіршікті қоспалар, бромэтилды қосылыстар, CO_2, инертті

газдар және т.б. табылады. Осы аталған өрт сөндіру құралдары келесі түрлерге жіктеледі: суытатын және оқшаулайтын, яғни жану аймағына оттегінің түсуін көбік қабатын жабу немесе құрғақ түйіршіктерді себу арқылы оқшаулау жүргізіледі. Электр өткізгіштігіне қарай: электр өткізетіндер (көбік, су, бу) және электр өткізбейтіндер (түйіршіктер мен кейбір газ түрлері) болып бөлінеді. Уыттылығы жағынан: уытты еместер (су, көбік, түйіршіктер), орташа уыттылар (көмірқышқылы және азот) және уыттылар (бромэтилды қоспалар, фреондар) болып бөлінеді.

Өртті сөндіру тәжірибесінде әртүрлі сулағыштар, көбіктер, инетті газдар мен механикалық құралды кең ауқымды қолданысқа ие.

Адамдарға қауіпті өрт факторларының әсерінен өту үшін жобаланған тапсырмада адамды ғимараттан тез арада шығару мүмкіндігі қарастырылған. Шығару уақыты ($t_{ш.есебі}$) жұмыс орынынан бастап сыртқа шығуға дейін арақашықтығы анықталады. Максималды қашықтығы алыс жұмыс орнынан бастап шығару есігінен қалыптасады. Ол өнеркәсіп категориясына ғимараттағы өрт тұрақтылық сатысы 100 мм-ден жоғарламау керек. Шығару есігінің саны ережедегідей болу керек, яғни екеуден аз емес. Есік шығарылуы деп аталады (ҚНжЕ 2.02.02-85) егер олар манадай жолға апарса: ғимараттын 1 – ші қабатынан сыртқа және вестибюль арқылы , осы қабаттан басқа ормандық торға апармайтындай коридорда сыртқы есігі болу керек немесе сол қабаттығы бөлмеде және көрші бөлмеде жоғарыда айтылған ескертулермен қамтамасыз етілу керек. Лифтер және басқа механикалық құрылғылар адамдарға жүктелген, шығаруға жатпайды [20].

Адамдық ағымның жылжу есебінде және коммуникациялық бөлменің өлшемін анықтау жоланда шығару келесі парамертлермен саналады:

1) D коммуникациондық бөлмемінің ауданына адамдардың сыйу тығыздығы, адам/м^2

$$D=F/N \tag{4.10}$$

Мұндағы, N – адам саны ,яғни берілген бөлім аудандағы бар адамдар (50 адам). F – коммуникациялық бөлімнің ауданының жолы.

$$F=21*25=525м^2$$

Онда,

$$D=50/525=0.1адам/м^2$$

2) Q жол мүмкіндігін жіберу (адам/мин):

$$Q=D\nu\delta, \tag{4.11}$$

Мұндағы, ν – адамдық ағынының қозғалыс жылдамдығы(100м/мин);
δ – жолдың ені ,м.

Жолдың ені формула бойынша табу:

$$\delta=NF/L_{шек}D \quad (4.12)$$

Мұндағы, L – шек-шығару жолындағы бөлім үшін шекті болатын ұзындық (100). Онда,

$$\delta=50*525/100*0,1=2625м$$

(4.9) формуласы бойынша өтуге болатын жолды табамыз:

$$Q= 0.1*100*2642 = 26420 адам/мин$$

3) q адамдық ағымның интенсивтік қозғалысы,м/мин

$$q=D\nu, \quad (4.13)$$

Онда,

$$q=0,1*100=10м/мин$$

Адам ағымының қозғалыстағы тәртіпсіздікпен қамтамасыз ету барлық қозғалыс жолына қажеттілігі бойынша алдынғы бөлімді (n+1) жіберуге мүмкіндік беру үшін шартты ұстану керек

$$Q_n \leq Q_{(n-1)max} \quad (4.14)$$

Шығарудың есеп уақытын анықтап (жолдың әр бөлісіндері уақыт құны):

$$t_{есеп}=L/\nu \quad (4.15)$$

Онда:

$$t_{есеп}=150/100=1,5с$$

Оны $t_{эн}$ шығару уақытының нормативімен салықтырады (ҚНжЕ 2.01.02-85). Міндетті түрде шарт орындалу қажет:

$$t_{есебі} \leq t_{эн} \quad (4.16)$$

Шарт орындалады [20]:

$$t_{есебі} = t_{ен} =1,5с$$

5 Техникалық-экономикалық тарау

5.1 Жобаның сипаттамасы

Менің дипломдық жобамның мақсаты алынып тасталатын модульді алдын ала анықтайтын құрылғыларды әзірлеу болып табылады.

Инновациялық шешімді әзірлеуге жоба жетекшісі, әзірлеуші-бағдарламашы және аппараттық криптограф сияқты мамандар қатысады. Жоба жетекшісі міндеттеріне жұмыс кестесін тексеру және оларды сақтау кіреді. Программист-әзірлеуші өз кезегінде техникалық негіздемені, бағдарламалық қамтамасыз етуді, оны тестілеу мен сүйемелдеуді әзірлеуі тиіс. Ал аппараттық криптографтың міндеттеріне ақпаратты шифрлеу және шифрлеу кіреді.

Техникалық-экономикалық негіздеме мынадай тармақтардан тұрады:

– бағдарламалық өнімді әзірлеудің еңбек сыйымдылығын анықтау;

– бағдарламалық өнімді (БӨ) әзірлеуге арналған шығындарды есептеу;

– дайын өнімнің құндылығын анықтау.

5.2 БӨ әзірлеудің еңбек сыйымдылығы

Бағдарламалық қамтамасыз етуді әзірлеудің күрделілігін дәл анықтау үшін тапсырмаларды кезеңдерге бөлу керек. Бағдарламалық қамтамасыз етуді әзірлеудің және дамудың күрделілігінің үлестіру үлгісі 5.1-кестеде келтірілген.

Кесте 5.1 – БӨ әзірлеу кезеңдері

БӨ әзірлеу кезеңдері	Жұмыс түрі	БӨ әзірлеудің еңбек сыйымдылығы, адам саны х сағ.
1 кезең	Тапсырманы қою	10
2 кезең	Модуль бойынша санды есептеу процесін іздеу және танысу	15
3 кезең	Модуль бойынша саннан қалдықты қалыптастыру тәсілдерін іздеу және зерттеу	15
4 кезең	Сандарды модуль бойынша келтіру үшін құрылғыларды әзірлеудің қолданыстағы	15

	әдістерін іздеу және зерттеу	
5 кезең	Сандарды тізбектей әрекет модулі бойынша келтіру үшін құрылғыны әзірлеу	20
6 кезең	Матрицалық әрекет модулі бойынша сандарды келтіруге арналған құрылғыны әзірлеу	20

5.1 кестенің жалғасы

7 кезең	Сандарды конвейеризацияланған әрекет құралы бойынша келтіру үшін құрылғыны әзірлеу	20
8 кезең	ПЛИС бойынша сандарды Алгоритмдеу процесін визуализациялау	20
9 кезең	Бағдарламалау тілін таңдау	10
10 кезең	Бағдарламаланатын логикалық схеманы таңдау	16
11 кезең	Бағдарламалық қамтамасыз етуді жазу	30
12 кезең	Жобаны іске асыру	35
13 кезең	Баптау	25
14 кезең	Атқарылған жұмыс туралы есеп жасау	15
15 кезең	Өнімді тестілеу	10
Қорытынды	жобалық жұмысты орындаудың еңбек сыйымдылығы	276

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық қамтамасыз етуді іске асыру үшін 35 жұмыс күні қажет.(276/8≈35)

5.3 БӨ әзірлеуге арналған шығындарды есептеу

Бағдарламалық өнімді әзірлеу үшін қажетті шығындарды анықтау қолда бар ақпарат негізінде жүргізіледі, ол мынадай элементтерді қамтиды:

– материалдық шығындар;
– еңбекақы төлеу шығындары;
– әлеуметтік салық;
– негізгі қорлардың амортизациясы.

Материалдық шығындар негізгі және қосалқы шығындарға, энергияға және БӨ әзірлеуге қажетті басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 5.2 кестеде берілген нысан бойынша жүргізіледі.

Кесте 5.2 – материалдық ресурстарға шығындар

Материалдың атауы	Маркасы	Өлшем бірлігі	Саны	Бірлік үшін баға, теңгемен	Соммасы, теңгемен
Кеңсе қағазы	Copyright	Қаптама	1	1 300	1 300

5.2 кестенің жалғасы

Дәптер (48 бет)	ArtSpace Gradient	Дана	2	150	300
Қалам	Hauser	Дана	2	90	180
Компьютер тінтуірі	AsusUT200	Дана	1	3500	3500
Қорытынды					5280

Материалдық құралдарға ($З_м$) қажетті жалпы соманы мынадай формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (5.1)$$

Мұндағы, P_i – материалдық ресурстың і түрінің шығысы, заттай бірліктер;

$Ц_i$ – материалдық ресурстың і түрінің бірлігінің бағасы, тг;

I – материалдық Ресурстың түрі;

N – материалдық ресурстар түрлерінің саны.

Бағдарламалық қамтамасыз етуді әзірлеу үшін Lenovo Z710 ноутбугі пайдаланылатын болады.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 5.3-кестеде келтірілген нысан бойынша жүргізіледі.

Кесте 5.3 – жоба үшін қажетті жабдыққа арналған шығындарды есептеу

Материал атауы	Маркасы	Өлшем бірлігі	Саны	Бірлік үшін баға, тг	Қорытынды, тг
Принтер	HPLaserJet 1020	шт	1	30 000	30 000
Ноутбук	Lenovo Z710	шт	1	332 000	332 000

Модем	Toshiba 77RQ	шт	1	14 000	14 000
Аппараттық құрылғы	Nexys4 Board	шт	1	24 600	24 600
Қорытынды					400600

$$Зм = 400\ 600 + 5\ 280 = 405\ 880(тг)$$

Бағдарламалық өнімді әзірлеу үшін 405 880 теңге сомаға материалдар қажет.

5.4 Электр энергиясына арналған шығындарды есептеу

Электр энергиясын тұтынбай-ақ, бағдарламалық қамтамасыз етуді әзірлеу кезінде электр энергиясына жұмсалатын шығындарды есептеу мәні бар.

5.1 – кестеге сәйкес бағдарламалық өнімді әзірлеу үшін 276 сағат қажет. Енді 276 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет. Принтер үшін есептеу 24 сағат кезеңі үшін жүргізіледі, себебі принтерді үнемі пайдалану қажет емес.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (5.2)$$

Мұндағы, $З_{эл.эн.обор.}$ – жабдықтың электр энергиясына арналған шығындар;

$З_{доп.нужды.}$ – қосымша мұқтаждықтарға электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (5.3)$$

Мұндағы, W – тұтынылатын қуат, Вт;

$К_{исц}$ – пайдалану коэффициенті ($К_{ис}$ = 0,7..0,9);

T – жұмыс уақыты;

S – тариф (1кВт / сағ = 23,81 тг).

Электр энергиясының құнын есептеу бойынша қорытынды 5.4-кестеде көрсетілген.

Кесте 5.4 – электр энергиясына шығындар

Құрылғы атауы	Төлқұжат бойынша қуат, кВт	Қуат коэффиценті	Құрылғының жұмыс уақыты, ч	ЭЭ бағасы тг/кВтч	Сомма, тг.

Ноутбук	0,8	0,7	276	23,81	2 760,05
Аппараттық құрылғы	0,08	0,7	276	23,81	368,007
Принтер	0,6	0,9	24	23,81	308,6
Жарықтандыру	0,3	0,7	276	23,81	1 380,03
Қорытынды:					4816

$$З_{эл.эн.обор.} = 4816(тенге)$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (5.4)$$

(5.4) формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз:

$$З_{доп.нужды} = 0.05 * 4816 = 240,8\ (тенге)$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 240,8 + 4816 = 5056,8\ (тенге)$$

5.5 Еңбекақы төлеу шығындарын есептеу

Бағдарламалық қамтамасыз етуді әзірлеу үшін бұрын көрсетілгендей, үш қызметкер қажет:

– жоба жетекшісі-жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;

– әзірлеуші-БӨ әзірлеу, тестілеу және сүйемелдеу.

– аппараттық криптография- хабарламаны шифрлеу және дешифрлеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша есептеуге болады:

$$З_{тр} = \sum ЧС_i * T_i \quad (5.5)$$

Мұндағы, $ЧС_i$-і қызметкердің сағаттық мөлшерлемесі, тг;

T_i-модельді әзірлеудің еңбек сыйымдылығы, адам×сағ; і-қызметкердің санаты;

n - БӨ әзірлеумен айналысатын қызметкерлердің саны.

Жұмыс уақыты әр түрлі, сондықтан әрбір қызметкердің сағаттық мөлшерлемесін және жалпы жалақы көлемін белгілеу мағынасы бар.

Қызметкердің сағаттық мөлшерлемесін мынадай формула бойынша есептеуге болады:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (5.6)$$

Мұндағы, $ЗП_i$ – і-ші қызметкердің айлығы, тг;

$ФРВ_i$ – і жұмыс уақытының айлық қоры, сағат.

Басшының айлық жалақысы 210 000 теңгеге тең және әзірлеушінің айлық жалақысы 190 000 теңгеге тең. Аппараттық криптографтың айлық жалақысы 190 000 теңгеге тең. Әр қызметкердің сағаттық мөлшерлемесін (5.6) формулаға сәйкес есептейміз:

$$ЧС_{руководитель} = \frac{210\,000}{21 * 8} = 1\,250 \text{ тг/ч}$$

$$ЧС_{разработчик} = \frac{190\,000}{21 * 8} = 1\,130{,}9 \text{ тг/ч}$$

$$ЧС_{апп.криптограф} = \frac{190\,000}{21 * 8} = 1\,130{,}9 \text{ тг/ч}$$

Басшының сағаттық мөлшерлемесі 1 250 (тг/сағ) құрайды, әзірлеудің еңбек сыйымдылығы 90 сағатқа тең. Әзірлеушінің сағаттық мөлшерлемесі 1 130,9 (тг/сағ) құрайды, әзірлеудің еңбек сыйымдылығы 276 сағатқа тең. Аппараттық криптографтың сағаттық мөлшерлемесі 1 130,9 (тг/сағ) құрайды, игерудің еңбек сыйымдылығы 106 сағатқа тең. (6.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{тр} = 1\,250 * 90 + 1\,130{,}9 * 276 + 1\,130{,}9 * 106$$
$$= 112\,500 + 312\,128{,}4 + 119\,875{,}4 = 544\,503{,}8$$

Еңбек ақы төлеу бойынша шығындарды есептеу (5.5) кестеде көрсетілген.

Кесте 5.5 – Жалақыны есептеу

Жұмысшы санаты	Біліктілігі	БӨ әзірлеу еңбек сыйымдылығы, сағ.	Сағаттық мөлшерлеме, тг/сағ	Сомма, тг.
Басшы	Жобалаушы-инженер	90	1 250	112 500
Әзірлеуші	Программист	276	1130,9	312 128,4

Аппараттық криптограф	АҚЖ маманы	106	1130,9	119 875,4
Қорытынды				544 503,8

5.6 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады:

$$С_н = (ФОТ - ПО) * 0,095 \quad (5.7)$$

Бұл жерде ПО зейнетақы қорына аударымдар ФОТ-тың 10% құрайды.

$$ПО = 544\,503,8 * 0,1 = 54\,450,38 \text{ тенге}$$

$$С_н = (544\,503,8 - 54\,450,38) * 0,095 = 46\,555,07 \text{ тенге}$$

Есептеу нәтижелері 5.6 - кестеде берілген :

Кесте 5.6 – әлеуметтік салықты есептеу

Жұмысшы санаты	Адам саны	Еңбек ақысы, тг	Зейнетақы аударымдары, тг	Әлеуметтік салық, тг
Басшы	1	112 500	11 250	9 618,75
Әзірлеуші	1	312 128,4	31 212,84	26 686,9
Аппараттық криптограф	1	119 875,4	11 987,54	10 249,3
Қорытынды				46 555,07

5.7 Негізгі қорлардың амортизациясы

НҚ амортизация нормаларын салық кодексіне сәйкес анықтау қажет. НҚ амортизациясын келесі формула бойынша анықтауға болады:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (5.8)$$

Мұндағы, $С_{об}$ – жабдықтың құны;

$Н_а$-амортизация нормасы (амортизация нормасы = 25);

(5.8) формула ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_г = \frac{332\,000 * 25}{100} = 83\,000 \text{ тенге}$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$A_{\text{г}} = \frac{83\,000 * 35}{365} = 7\,958{,}9 \text{ тенге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері кестеде келтірілген (5.7).

Кесте 5.7- НҚ амортизациясы

Құрылғы атауы	Құрылғының құны, тг	Жылдық амортизация нормасы,%	Жылдық амортизация суммасы, тг	Әзірлеудегі амортизация нормасы, тг
Ноутбук	332 000	25	83 000	7 958,9
Принтер	30 000	25	7 500	719,18

5.7 кестенің жалғасы

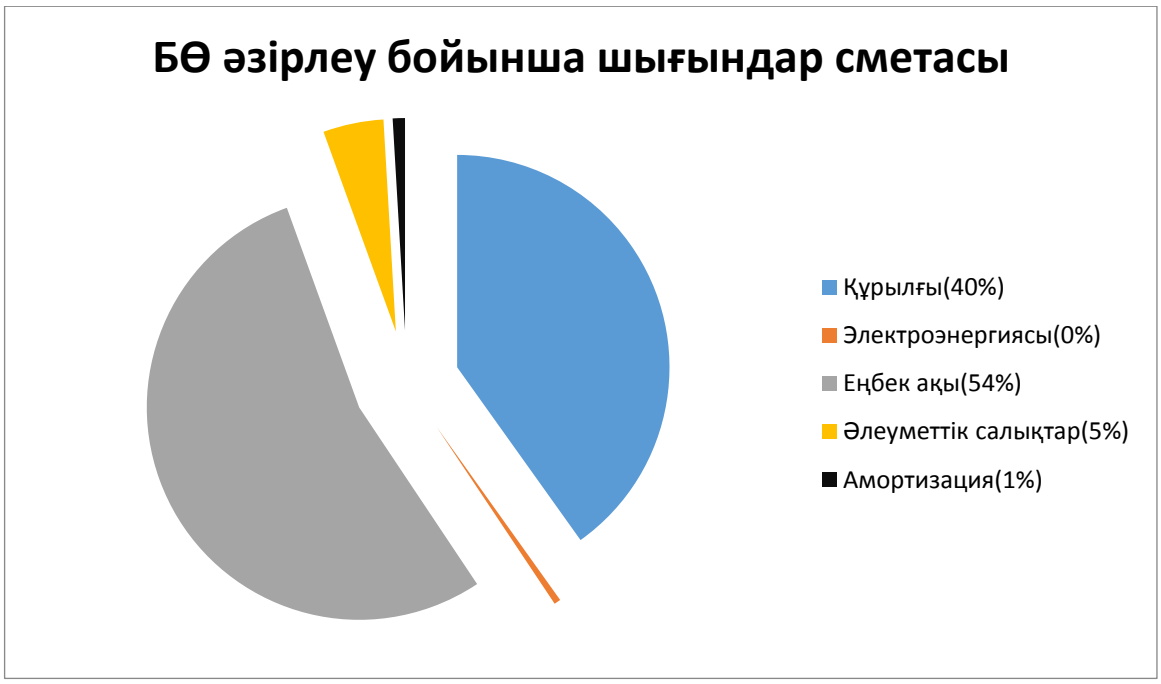
Модем	14 000	20	2 800	268,5
Аппараттық құрылғы	24 600	20	4 920	471,8
Қорытынды:			98 220	9 418,38

БӨ әзірлеуге арналған шығыстар сметасы.

Барлық берілген есеп-қисаптардың негізінде (5.8) кестеде келтірілген нысан бойынша әзірлеуге арналған шығыстар сметасын ресімдеу қажет(5.1-сурет).

Кесте 5.8 – БӨ әзірлеу бойынша шығындар сметасы

Шығындар баптары	Сомма, тг
Жабдыққа арналған шығындар	405 880
Электр энергиясына арналған шығындар	5 056,8
Еңбекақы төлеу шығындары	544 503,8
Әлеуметтік салықтар	46 555,07
Негізгі қорлардың амортизациясы	9 418,38
Смета бойынша қорытынды:	1 011 414,36



Сурет 5.1 – шығындар диаграммасы

5.8 БӨ ықтимал (шарттық) бағасын анықтау

БӨ – нің ықтимал (шарттық) бағасының құны тапсырыс берушінің (тұтынушының) және орындаушының экономикалық мүдделерін қанағаттандыратын деңгейде тиімділікті, сапаны және оны орындау мерзімін ескере отырып белгіленуі керек.

Қолданылатын БӨ үшін келісім-шарттық бағасы ($Ц_д$) келесі формула бойынша есептеледі:

$$Цд = Знир(1 + Р/100), \quad (5.9)$$

Мұндағы, $З_{нир}$ – БӨ әзірлеуге кеткен шығын (8.8 кестеден белгілі), тг;

Р – БӨ рентабельділігінің орташа деңгейі,% (20-30% мөлшерінде қабылданады). Бұл параметр 25% деп есептеледі.

Цд = 1 011 414,36 + 1 011 414,36*0,25 = 1 011 414,36 + 252 853,59 = 1 264 267,95 тенге.

Бұдан әрі қосылған құн салығын (ҚҚС) есепке ала отырып, өткізу құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамалық Салық кодексімен белгіленеді. 2019 жылға ҚҚС ставкасы 12% мөлшерінде белгіленген.

Іске асыру құны ҚҚС-ты ескере отырып есептеуге болады мынадай формула бойынша:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (5.10)$$

$$Ц_р = 1\,264\,267{,}95 + 1\,264\,267{,}95 * 0{,}12 = 1\,264\,267{,}95 + 151712{,}154 = 1\,415\,980{,}104 \text{ тенге}$$

5.9 БӨ жұмысының әлеуметтік-экономикалық нәтижелерін бағалау

Әзірлеушілердің экономикалық тиімділігі жобаны іске асырумен айналысатын жеке әзірлеушілердің де, компанияның да қаржылық жағдайын жақсарту болып табылады.

Бұл өнімді іске асыру барысында осы өнімнің техникалық-экономикалық негіздемесі мен тиімділігі туралы сұраққа жауап беруі тиіс плата нарығы, маркетинг және жарнама сияқты сұрақтарға жауап қарастырылып және алдағы уақытта шешілуі қажет.. Егер бұл өнім табысты іске асырылса, девелопер 312128,4 теңге көлемінде жалақы алады. Егер бұл жоба үлкен инвестицияларға әкелетін болса, онда жоба ұзақ уақыт бойы өтеу мерзіміне жетеді.

Бұл жобаның құны 1 011 414,36 теңге, пайда 252 853,59 теңгені құрады. Қорытындылай келе, бұл жобаның мүмкін бағасы 1 415 980 теңгені құрайды.

Қорытынды

Бұл дипломдық жобада алынып тасталатын модульді алдын ала анықтаумен сандарды келтіру құрылғысы ұсынылды және келесі міндеттер шешілді:

– Р модулі бойынша А санын есептеу процесімен қысқаша таныстырулар жүргізілді;

– модуль бойынша саннан қалдықты қалыптастырудың қолданыстағы тәсілдеріне талдау жасалып, негізгі көрсеткіштері бойынша салыстырмалы бағалау жасалды;

– сандарды келтіру құрылғысының тізбекті, матрицалық, конвейерлік сызбалары келтірілді;

– ПЛИС бойынша сандарды алгоритмдеу құралына талдау жасалып, жұмыс орны ретінде керек плата таңдалып, Verilog тілінде ПЛИСке программалық код тігілген болатын;

– өмір тіршілік қауіпсіздігіне есептеулер жүргізілді;

– техникалық-экономикалық негіздемелер келтірілген.

Қазақстан Республикасының экономикалық жағдайы қазіргі уақытта мұнай мен мұнай өнімдерінің бағасына қатты байланысты, басқа да өндіруші салаларды біртіндеп оңтайландыру азаматтардың әл-ауқатын арттырады, бұл одан әрі экономиканың басқа да бағыттары бойынша да түрткі болады.

Біз ұсынған жүйені енгізу құны 1 011 414,36 теңге, пайдасы 252 853,59 теңгені құрайтыны және қорытындылай келе, бұл жобаның мүмкін бағасы 1 415 980 теңгені құрайтыны есептеліп, жұмысшылардың техникалық және технологиялық еңбекті қорғауды қамтамасыз етілетіндігі туралы негіздемелер келтірілді.

Қысқартулар тізімі

АЦП – аналогты-цифрлық түрлендіргіш

БлРг – блоктық регистр

БлС – синхронизатор блогы

ИНВ – инвентор

КМОП (комплементарная структура металл-оксид-полупроводник) — интегралды микросхемалар құрудың жартылай өткізгіштік технологиялар жиынтығы және оған сәйкес микросхемалар схемотехникасы

Л.З. – кешігу линиясы

ПЛИС – бағдарламаланатын логикалық интегралдық сызбалар

РгА – А санының регистрі

РгР – Р модулінің регистрі

САПР – автоматтандырылған жобалау жүйесі

СМ – сумматор

СММ – модуль бойынша қосқыш

СС – салыстыру схемасы

СчТИ – тактикалық импульсті есептегіш

ТИ – тактілік импульс

УММ – модуль бойынша көбейткіш

ФЧО – ішінара қалдықты қалыптастырушы

ЭСППЗУ — электрондық өшірілетін бағдарламаланатын тұрақты есте сақтау құрылғысы

ASIC (application-specific integrated circuit) – арнайы интегралдық схеманы тағайындау

BUFG (global clock buffer) – жаһандық тактілік импульстер буфері

DDR SDRAM (Double Data Rate Synchronous Dynamic Random Access Memory – синхронды динамикалық жады) – компьютерлік жады түрі

FF (flip - flops) – триггерлер

FPGA (Field Programmable Gate Array) – бағдарламаланатын вентильдік матрицалар

I/O (input/ output) – кіріс/ шығыс

Language) – аппаратураны сипаттау тілі

LUT (lookup tables) – іздеу кестесі

MS – мультиплексор

PLD (Programmable logic device) – бағдарламаланатын логикалық құрылғылар

Verilog (Verilog Hardware Description Language) – аппаратураны сипаттау тілі

VHDL (VHSIC (Very high speed integrated circuits) Hardware Description – аппаратураны сипаттау тілі

Әдебиеттер тізімі

1 Лехин С.М. Схемотехника ЭВМ. - СПб.: БХВ-Петербург, 2010.

2 Айтхожаева Е.Ж., Тынымбаев С.Т. Аппаратные методы реализации базовых операции ассиметричных криптоалгоритмов. -Алматы: Журнал Вестник НАН РК. №6.

3 Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012.

4 Рябко Б.Я., Фионов А.И. Основы современной криптографии для специалистов в информационных технологиях. – М.: Науный мир, 2004.

5 Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. 2-е изд. -Спб.: Питер, 2011.

6 Айтхожаева Е.Ж., Тынымбаев С.Т. Аспекты аппаратного приведения по модулю в ассиметричной криптографии. -Алматы: Журнал Вестник НАН РК. №5.

7 Петренко В.Н., Сидорчук А.В., Кузьминов Н.В. Устройство для формирования остатков по произвольному модулю. Патент RU №2368942.

8 Тынымбаев С.Т., Шайкулова А.А., Иманбаева А.Ж., Зиро А.А. Матричные схемы для приведения чисел по модулю. -Алматы: Вестник КазНИТУ, 2017.

9 Хоровиц П., Хилл .У. Искусство схемотехники. -М.: Мир, 2013.

10 Турыгин И.Г. Метод выбора программируемых логических интегральных схем на основе целевого функционала при проектировании устройств цифровой обработки информации. -Пенза, 2014.

11 Programmable Devices [Электрондық ресурс] URL:http://www.xilinx.com/ (кіру уақыты: 18.03.2019).

12 Программируемые логические интегральные схемы [Электрондық ресурс] URL:http://mehatronics.ru/2011/01/программируемые-логические интеграл / (кіру уақыты: 18.03.2019).

13 Максфилд К. Проектирование на ПЛИС. -М.: Издательский дом «Додэка – XXI», 2007.

14 СтецкоИ.П., Кулик В.Д. Компьютерное проектирование цифровых систем. -М.: Издательский дом «Додэка – XXI», 2010.

15 Сулеев Д.К., Исаханова А.Б., Суйесинова Г.И., Болатбаева Т., Утепова А.Б. Электромагнитные поля в учебных аудиториях. -Алматы: Вестник КазНТУ, 2007. -№ 1/1.

16 Суйесинова Г.И. Электрмагниттік саулелерге ұшырайтын жұмысшылардың еңбек жағдайын жақсарту. // «Тіршілік қауіпсіздігі саласындағы жаңалықтар» атты он бірінші ғылыми – техникалық конференция. 3 т. -Алматы: КазНТУ, 2009.

17 Суйесинова Г.И. Электрмагниттік саулелердің жұмысшы ағзасына әсерін бәсеңдету бойынша іс-шараларды жасау. // «Тіршілік қауіпсіздігі саласындағы жаңалықтар» атты он бірінші ғылыми – техникалық конференция. 3 т. -Алматы: КазНТУ, 2009.

18 Кустов В.Н. Мусин К.А., ББД Охрана в дипломных проектах. -Алматы: КазНТУ, 2015.

19 ГОСТ 12104-91. Еңбекті қорғаудың стандартты жүйесі. Қауіпсіздіктің жалпы талаптары.

20 ГОСТ 12105-8. Еңбекті қорғаудың стандартты жүйесі. Жұмыс зонасының ауасына жалпы санитарлы – гигиеналық талаптары.