ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
Ақпарттық қауіпсіздік жүйелері кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі т.ғ.қ., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 2020 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Ақпаратты криптографиялық қорғау процесін жеделдетуге арналған аппараттық-программалық құрылғыны әзірлеу

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Кубеев Айдын Ақанұлы Тобы СИБк-16-1
(аты-жөні)
Ғылыми жетекші: т.ғ.д., профессор Якубова М. З.
(ғылыми дәрежесі, атағы, аты-жөні)
Кеңесшілер:
Мамандығы бойынша:
аға оқытушы Дмитриева Маргарита Валерьевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Тіршілік қауіпсіздігі бөлімі бойынша:
доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Мөлшер бақылаушы:
аға оқытушы Альмуратова Камшат Бимуратовна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Пікір беруші:
Төлеулиев Сырым Бимуратович
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ 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: Кубеев Айдын Ақанұлы
(аты-жөні)

Жобаның тақырыбы: Ақпаратты криптографиялық қорғау процесін жеделдетуге арналған аппараттық-бағдарламалық құрылғы әзірлеу

2019 ж. «11» қараша №56 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): _____
Сандарды модуль бойынша көбейтудің екі тәсілі тәжірибе жүзінде іске асырылып, алынған деректерге сүйене отырып, жылдам жұмыс жасайтын құрылғы ұсынылды. Атап айтқанда, көбейткіштің кіші және үлкен разрядтарын талдай отырып, тізбекті әрекет модулі бойынша сандарды көбейту.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. Криптографиялық қорғаудың өзектілігі.
2. Криптографиялық қорғаудың әдістері.
3. Ақпаратты криптографиялық қорғау процесін жеделдететін құрылғының сұлбаларын жасау.
4. Құрылғы жұмысын тексеріп, есептеулер жүргізу.
5. Жұмыс жағдайында жерлендіру және эвакуация уақытын есептеу.
6. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

2.1 сурет – Тізбекті әрекет модулі бойынша сандарды көбейтудің функционалдық сұлбасы

2.2 сурет – НФЧО құрылымы

2.3 сурет – НСММ құрылымы

2.4 сурет – Көбейткіштің үлкен разрядын талдай отырып, көбейтетін тізбекті әрекет модулі бойынша көбейткіштің құрылымдық сұлбасы

2.5 сурет – Аралық қалдықты қалыптастырушының функционалдық схемасы

3.1 сурет – 8 биттік сан үшін алгоритм жұмысының диаграммасы

4.1- кесте – Жұмыс орнындың қызмет көрсетілетін аймағындағы температураның, салыстырмалы ылғалдылықтың оңтайлы нормалары

4.3-кесте – Адам ағынының тығыздығы бойынша оның жылдамдығы

5.3 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

Негізгі ұсынылатын әдебиеттер:

1. Ковтун М., Ковтун В. Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений [Электронный ресурс.] – http://docplayer.ru/30671408-Obzor-i-klassaifikaciya-algoritmov-privedeniys-po-modulyu-bolshih-chisel-dlya-kriptograficheskih-prilozheniy.html

2. Тынымбаев С.Т., Бердибаев Р.Ш., Омар Т, Шайкулова А.А., Магауин Б. Быстродействующие устройства приведения числа по модулю. Материалы XIV Международной Азиатской школы – семинара «Проблемы оптимизации сложным систем». 20-31 июля 2018, часть 2, Алматы 2018.

3.Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009. - 32 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Якубова М. З.		
Өміртішілік			
қауіпсіздігі	Жандаулетова Ф.Р.		
Тәуекелдерді есептеу			
бөлімі	Дмитриева М.В.		

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	12.02.20 – 14.02.20	орындалды
1.1 Криптографиялық қорғаудың өзектілігі	18.02.20 – 10.03.20	орындалды
1.2 Криптографияның пайда болу уақыты, тарихы	18.02.20 – 10.03.20	орындалды
2 Модуль бойынша сандарды көбейту әдістері	12.03.20 – 24.03.20	орындалды
3 Тез жұмыс жасайтын құрылғы жасау	26.03.20 – 15.04.20	орындалды
4 Өміртіршілік қауіпсіздігі	19.04.20 – 15.05.20	орындалды
4.1 Кәсіпорындағы еңбек жағдайларын талдау	19.04.20 – 02.05.20	орындалды
4.2 Есептеу бөлімі	02.05.20 – 15.05.20	орындалды
5 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу	08.05.20 – 28.05.20	орындалды
5.1 Ақпараттық қауіпсіздік тәуекелдері	08.05.20 – 15.05.20	орындалды
5.2 Екі параметр бойынша есептеу	15.05.20 – 28.05.20	орындалды

Тапсырманың берілген уақыты «12 » қаңтар 2020 ж.

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

Жобаның
ғылыми жетекшісі _____ (Якубова М. З.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Қалиев Д. Ж.)
(қолы) (аты

Андатпа

Бұл дипломдық жобада шифрлеу құрылғысының тиімділігі, тұрақтылығы бағдарламалық шифрлеу құрылғысына қарағанда неғұрлым тез жұмыс істейтінділігі қаралып дәлелденген. Жобада есептеулермен блоктық сұлбалар көрсетіліп қарастырылған. Қазіргі заман талабына сай жаңа, тез істейтін құрылғы болып табылады. Өміртіршілік қауіпсіздігі бөлімінде жұмыс аймағындағы жұмыс жағдайына талдау жүргізілді. Еңбек жағдайларының деңгейі жұмысшылар үшін қолайлы деп танылды. Ғимараттағы эвакуациялау жолдарын есептеу және жерлендіру есебі орындалды.

Аннотация

В данном дипломном проекте рассматривается и доказано, что эффективность, устойчивость шифровального устройства работают более быстро, чем программные шифровальные устройства. В проекте предусмотрены блочные схемы с расчетами. Это новое, быстродействующее оборудование, отвечающее современным требованиям. В отделе безопасности жизнедеятельности проведен анализ состояния работы в рабочей зоне. Уровень условий труда признан приемлемым для рабочих. Выполнен расчет и заземление эвакуационных путей в здании.

Anatation

This thesis project examines and proves that the effectiveness and stability of the encryption device work faster than software encryption devices. The project provides block diagrams with calculations. This is a new, fast-acting equipment that meets modern requirements. The Department of life safety conducted an analysis of the state of work in the work area. The level of working conditions is considered acceptable for workers. Calculation and grounding of evacuation routes in the building was performed.

Мазмұндама

Кіріспе

Қазіргі кезде технологияның қарқынды дамуына байланысты, сандық ақпарат барлық жерде қолданылады. Сондықтан ақпаратты қажетті деңгейде қорғау өте маңызды мәселе. Осы себепті мен дипломдық жұмысымда ақпаратты криптожүйе арқылы қорғауды қарастырдым. Криптожүйелерді қарастырып, оларға салыстырмалы түрде талдау жасадым. Ашық кілтті криптожүйенің жабық кілтті криптожүйеден басты артықшылығы: ашық кілтті криптожүйе қауіпсіздік ықтималдығы ең жоғары болып табылады, себебі құпия кілтті жіберіп және түпнұсқалығын тексеру қажеті жоқ. Шифрлеу құрылғысында қолданылатын схемаларды талдап, олардың функционалдық және принципиялдық деңгейде жұмысын қарастырдым.

Шифрлеу құрылғысы:

- Жұмыс өнімділігін нығайтады.
- Шифрлеу жылдамдығын арттырады.
- Крипто беріктікті сақтайды.
- Аз ресурстарды пайдаланады.

Осы сапаларына қарап құрылғы үлкен мүмкіндікке ие екенін көрсе болады.

1.Криптографиялық алгоримдер.

Криптография - ежелгі ғылымдардың бірі, ол бірнеше мың жылдарды құрайды. Оның үстіне, басында жазудың өзі криптографиялық жүйе болған, өйткені ежелгі қоғамдарда оған тек элита ғана ие болған. Ежелгі Египеттің, Ежелгі Үндістанның қасиетті кітаптары бұған мысал бола алады.

Жазудың кең таралуымен криптография дербес ғылым ретінде қалыптаса бастады. Алғашқы криптожүйелер біздің дәуіріміздің басында табылған. Бірінші және екінші дүниежүзілік соғыстар кезінде криптографиялық жүйелер тез дамыды. Соғыстан кейінгі кезеңнен бастап бүгінгі күнге дейін есептеулердің пайда болуы криптографиялық әдістердің дамуы мен жетілдірілуін тездетті.

Неліктен қазіргі кезде ақпараттық жүйелерде криптографиялық әдістерді қолдану мәселесі өзекті болып отыр?

Бір жағынан, компьютерлік желілерді қолдану кеңейе түсті, атап айтқанда ғаламдық Интернет, ол арқылы мемлекеттік, әскери, коммерциялық және жеке сипаттағы үлкен көлемдегі ақпарат жіберіледі, бұл оған бөтен адамдарға қол жеткізуге мүмкіндік бермейді.

Екінші жағынан, қуатты жаңа компьютерлердің, желілік және нейрондық есептеуіш технологиялардың пайда болуы жақында болжанбаған болып саналған криптографиялық жүйелердің беделін түсіруге мүмкіндік берді. Ақпаратты оны түрлендіру арқылы қорғау мәселесі - криптология (грекше: криптос - құпия, логотиптер - ғылым).

Криптология екі бағытқа бөлінеді - криптография және криптоталдау. Бұл бағыттардың мақсаттары тікелей қарама-қарсы.

Криптография ақпаратты түрлендірудің математикалық әдістерін іздеумен және зерттеумен айналысады. Криптоталдаудың қызығушылық саласы - бұл кілттерді білместен ақпаратты шифрлау мүмкіндігін зерттеу.

Қазіргі ақпараттандырылған қоғамда криптографияның кейбір қолдану салаларын келтірейік:

- ашық байланыс арна арқылы берген кезде деректерді шифрлау (мысалы, Интернетте сатып алу кезіндегі мекен жайы, телефон, кредит картанын нөмірі сияқты мағлұматтар шифрланады);
- банк пластикалық карточкаларға қызмет көрсету;
- желі ішінде пайдаланушылардың парольдерін сақтау және өңдеу; алысталған байланыс арна арқылы бухгалтерлік есептерді өткізу; жергілікті және ғаламдық желі арқылы кәсіпорындарға банктік қызмет ету;
- рұқсат етілмеген қатынаудан деректерді компьютердің қатқыл дискісінде (мысалы, Windows операциялық жүйеде арнайы термин бар – файлдық шифрланған жүйе EFS) қауіпсіз сақтау.

Дәстүрлі криптография қамтамасыз ететін қауіпсіздік бірнеше факторларға байланысты.

Біріншіден, криптографиялық алгоритм жеткілікті берік болуы керек, сондықтан шифрланған хабарлама шифрланған хабарламаның әртүрлі

статистикалық үлгілерін немесе оны талдаудың басқа әдістерін қолданып кілтсіз шешілмейді.

Екіншіден, берілетін хабарламаның қауіпсіздігі алгоритмнің қауіпсіздігіне емес, кілттің қауіпсіздігіне байланысты болуы керек. Шифрланбаған және шифрланған хабарламалар арасындағы байланыс нашар жасырылған әлсіздіктердің болуын болдырмау үшін алгоритмді мамандар талдауы керек. Сонымен қатар, егер бұл шарт орындалса, өндірушілер арзан шифрлау алгоритмін жүзеге асыратын арзан аппараттық чиптер мен ақысыз бағдарламалар жасай алады.

Үшіншіден, алгоритм осындай кілттің көмегімен шифрлау кезінде алынған көптеген жұптарды (шифрланған хабарлама, шифрланбаған хабарлама) біле отырып, кілтті тану мүмкін болмайтындай болуы керек.

XX ғасырға дейін криптографиялық әдістер тек рұқсатсыз қатынаудан қорғау үшін деректерді шифрлауға ғана қолданылатын. XX ғасырда жаңа криптографиялық әдістерін жасағандықтан криптографияның міндеттерінің спектрі де кеңейді. Қазіргі уақытта криптография келесі міндеттерді шешуге арналған:

- рұқсатсыз қатынаудан қорғау үшін деректерді шифрлау;
- хабарлардың дұрысын (тап өзін) тексеру: хабарды алушы оның шығу көзін тексере алады;
- берілетін деректердің бүтіндігін тексеру: жіберу барысында хабар өзгерді ме не ауыстырылды ма алушы тексере алады;
- бас тартудан мүмкін еместігін қамтамасыз ету, яғни алушыға да берушіге де жіберуден бас тартудын мүмкін еместігі.

1.1 Шифрлау

Шифр – бастапқы құпиялы хабарды қорғау үшін оның алдын ала айтылған түрлендіру тәсілдерінің жиынтығы.

Бастапқы хабарлар әдетте ашық мәтін деп аталады.

Кез келген шифрды пайдаланып түрлендіруден кейінгі алынған хабар шифрланған хабар (*жабық мәтін, криптограмма*) деп аталады.

Ашық мәтіннің криптограммаға түрлендіруі шифрлау (шифрлану) деп аталады. Кері іс-әрекет шифрды ашу (*дешифрлау*) деп аталады

Кілт – хабарларды шифрлау мен дешифрлау үшін қажетті ақпарат.

Шифрді ашу және дешифрлау терминдері бір біріне синоним, бірақ әдетте екінші термин көбінесе қаскүнем (яғни кілтті білмейтін адам) үшін пайдаланады.

Шифрлау жүйесі немесе шифржүйесі – бұл хабар мәтінің қайтымды өзгерту үшін (жолданған адамнан басқа барлықтарға мәтін түсініксіз болсын оймен) пайдаланатын кез келген жүйе.

Кілтті білмегенде шифрды ашуға беріктікті анықтайтын шифр сипаттамасы (яғни криптоталдауға қарсы тұру қабілеті) криптоберіктік деп аталады.

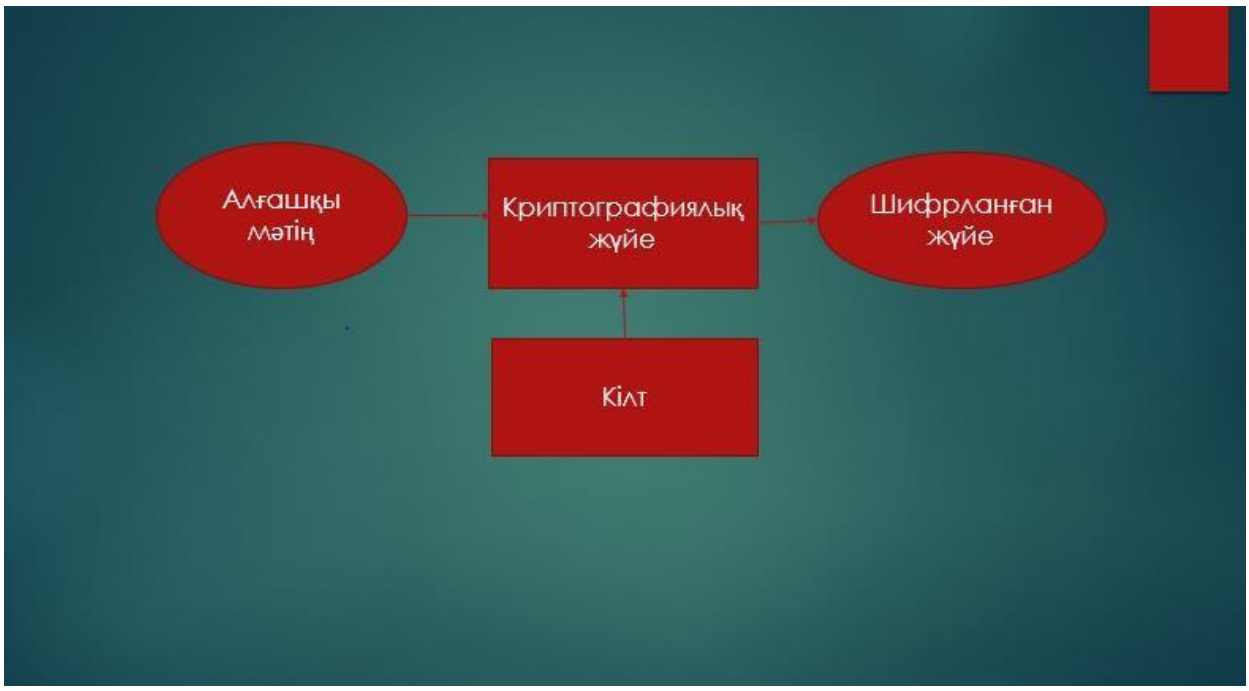
Шифрлау процесі бастапқы ақпараттың қайтымды математикалық, логикалық, комбинаторлық және басқа да түрлендірулерін жүргізу болып табылады, нәтижесінде шифрланған ақпарат әріптердің, цифрлардың, басқа символдардың және екілік кодтардың ретсіз жиынтығы болып табылады.
Стандартты шифрлау алгоритмі әр түрлі платформаларда жүзеге асырылуы керек, олар сәйкесінше әр түрлі талаптарды ұсынады.

- Алгоритмді шифрлау / шифрды шешуге арналған арнайы жабдықта тиімді жүзеге асыру керек.
- Ірі процессорлар. Ең жылдам қосымшалар үшін әрқашан арнайы аппараттық құралдар пайдаланылады, бірақ бағдарламалық жасақтаманы ендіру жиі қолданылады. Алгоритм 32 биттік процессорларда бағдарламалық қамтамасыз етуді тиімді енгізуге мүмкіндік беруі керек.
- Орташа өлшемді процессорлар. Алгоритм микроконтроллерлерде және басқа орташа процессорларда жұмыс істеуі керек.
- Шағын процессорлар. Пайдаланылған жадқа қатаң шектеулерді ескере отырып, алгоритмді смарт-карталарда қолдану мүмкіндігі болуы керек.

Шифрлау алгоритмі мүмкіндігінше кейбір қосымша талаптарды қанағаттандыруы керек.

- Бағдарламалық жасақтама қателіктерінің ықтималдығын азайту үшін код жазу алгоритмі қарапайым болуы керек.
- Алгоритмде кілттердің жалпақ кеңістігі болуы керек және мүмкін болатын кілт ретінде кез-келген кездейсоқ жолдың кез-келген жолына жол берілуі керек. Әлсіз кілттердің болуы қажет емес.
- Алгоритм қауіпсіздіктің әртүрлі деңгейлері үшін оңай өзгертілуі керек және минималды және максималды талаптарды қанағаттандыруы керек.
- Деректердің барлық әрекеттері байтқа немесе 32 биттік сөзге еселенген блоктарда орындалуы керек.

Ақпаратты шифрлау үшін түрлендіру алгоритмі және кілт қолданылады. Әдетте, белгілі бір шифрлау әдісі үшін алгоритм өзгеріссіз. Шифрлау алгоритмі үшін бастапқы деректер шифрлауға жататын Ақпарат және шифрлау кілті болып табылады. Кілтте шифрлеу алгоритмін іске асыру кезінде қолданылатын операндтардың шамасы мен алгоритмнің белгілі бір қадамдарында түрлендіруді таңдауды анықтайтын басқарушы ақпарат бар. Операнд-бұл константа, айнымалы, функция, өрнек және операция жасалатын бағдарламалау тілінің басқа объектісі.



Сурет 1.1 – шифрлау процесі

Шифрдің криптоберіктілігі оның тиімділігінің негізгі көрсеткіші болып табылады. Ол кілтті білмейтін жағдайда, шифрмәтін туралы бастапқы ақпаратты алу үшін криптографикке қажет қаражаттың уақыты немесе құнымен өлшенеді.

Кеңінен қолданылатын шифрлау алгоритмін құпия түрде сақтау мүмкін емес. Сондықтан, алгоритмде криптаналитиктер пайдаланатын жасырын әлсіздіктер болмауы керек. Егер бұл шарт орындалса, шифрдің криптографиялық беріктігі кілттің ұзындығымен анықталады, өйткені Шифрланған ақпаратты ашудың жалғыз тәсілі - кілттің тіркесімдерін іздеу және шифрды шешу алгоритмін орындау. Осылайша, криптовалютаға кететін уақыт пен ақша кілт ұзындығына және шифрлау алгоритмінің күрделілігіне байланысты болады.

Криптографияда Киркхоф ережесі қабылданады, яғни шифрдың беріктігі тек кілттің қауіпсіздігімен анықталуы керек. Сонымен, барлық стандартты шифрлау алгоритмдері (мысалы, AES, DES, PGP) кеңінен танымал, олардың егжей-тегжейлі сипаттамасы оңай қол жетімді құжаттарда бар, бірақ олардың тиімділігі төмендемейді. Егер шабуылдаушы шифрлау алгоритмі туралы бәрін білсе, бірақ құпия кілтті білмесе, жүйе қорғалады.

Криптожүйелердің екі класы бар - симметриялы және асимметриялық. Симметриялық шифрлау схемаларында (классикалық криптография) құпия шифрлау кілті құпия шифрлау кілтіне сәйкес келеді. Ассиметриялық шифрлау схемаларында (ашық кілттердің криптографиясы) ашық шифрлау кілті жеке шифрлау кілтіне сәйкес келмейді

1.2 Симметриялық криптожүйелер.

Симметриялық криптожүйе. Кодтау және декодтау үшін бірдей кілт пен бірдей кодтау алгоритмі қолданылатын кодтау әдісі симметриялы деп аталады. Симметриялық кодтау әдісінде К кілті құпия, жеке болып табылады. Сіз абоненттерге құпия кілтті жеткізе аласыз:

• физикалық түрде электронды ақпарат тасымалдаушыларда (дискілер, флэш-карталар және т.б.), пластикалық карталардағы, әкімшінің өзі есеп беретін парольдер түрінде;

• байланыс каналы арқылы шифрланған түрде. Бұл жағдайда абоненттердің құпия ақпаратты жіберуге мүмкіндігі болуы керек.

Тәжірибеде әдетте құпия кілттермен жұмыс жасаудың аралас моделі қолданылады, ұзақ мерзімді кілттер абоненттерге физикалық түрде жеткізіледі;

• ұзақ мерзімді кілттердің көмегімен тек бір байланыс сеансында қолданылатын сеанстық кілттер шифрланады және жіберіледі;

• құпия ақпарат сессияның кілттері негізінде шифрланады.

Бұл криптожүйелер шифрлаудың ең жоғары жылдамдығымен сипатталады және олардың көмегімен құпиялылық пен түпнұсқалық, сонымен қатар берілетін ақпараттың тұтастығы қамтамасыз етіледі. Симметриялық криптожүйені қолдана отырып ақпарат берудің құпиялылығы шифрдың беріктігіне және шифрлау кілтінің құпиялылығына байланысты болады.

Әдетте, шифрлау кілті - бұл файл немесе мәліметтер жиынтығы және дискета немесе смарт-карта сияқты жеке кілт ортасында сақталады; Жеке кілт тасымалдаушысының иесінен басқа ешкімге қол жетімді болмауын қамтамасыз ету үшін шаралар қабылдау өте маңызды.

Түпнұсқалылық алдын-ала шешілместен, семантикалық түрлендіруді және криптографиялық жабық хабарламаны қолдан жасау мүмкін емес екендігінің арқасында қамтамасыз етіледі. Жасанды хабарлама құпия кілтті білместен дұрыс шифрлана алмайды.

Деректердің тұтастығы берілетін деректерге құпия кілтпен жасалынатын арнайы кодты (модельделген кірістіру) тіркеу арқылы қамтамасыз етіледі. Имитациялық кірістіру - бұл тексерудің бір түрі, яғни хабарламаның кейбір анықтамалық сипаты, соңғысының тұтастығы тексеріледі. Имитациялық кірістіруді құру алгоритмі оның хабарламаның әр битіндегі кейбір күрделі криптографиялық заңдарға тәуелділігін қамтамасыз етуі керек. Хабардың тұтастығын тексеруді хабарлама алушы алынған хабарға сәйкес құпия кілтті құру және оны хабарламаның алынған мәнімен салыстыру арқылы жүзеге асырады. Егер ол сәйкес келсе, ақпарат жіберушіден алушыға дейінгі жолда өзгертілмеген деген қорытынды жасалады.

Симметриялық шифрлау «өзіңіз үшін» ақпаратты шифрлау үшін өте ыңғайлы, мысалы, иесі болмаған кезде оған рұқсатсыз кіруді болдырмау үшін. Бұл таңдалған файлдардың мұрағаттық шифрлануы немесе логикалық немесе физикалық дискілердің мөлдір (автоматты) шифрлануы болуы мүмкін.

Шифрлаудың жоғары жылдамдығына ие, бір кілтті криптожүйелер ақпаратты қорғаудың көптеген маңызды міндеттерін шешуге мүмкіндік береді. Алайда, компьютерлік желілерде симметриялы криптожүйелерді автономды қолдану пайдаланушылар арасында шифрлау кілттерін тарату проблемасын туғызады.

Шифрланған деректерді алмасуды бастамас бұрын, барлық алушылармен құпия кілттерді алмасу керек. Симметриялық криптожүйенің құпия кілтін беру жалпыға қол жетімді байланыс арналары арқылы жүзеге асырылмайды, құпия кілт жіберушіге және алушыға қауіпсіз арна арқылы берілуі керек. Желіде таратылатын хабарламалардың тиімді қорғалуын қамтамасыз ету үшін жиі өзгеретін кілттердің көп саны қажет (әр қолданушыға бір кілт). Пайдаланушыларға кілттерді беру кезінде үлкен қосымша шығындарды талап ететін шифрлау кілттерінің құпиялылығын, шынайылығын және тұтастығын қамтамасыз ету қажет. Бұл шығындар жеке байланыс арналары арқылы құпия кілттерді беру қажеттілігімен немесе арнайы жеткізу қызметін, мысалы, курьерлер арқылы осындай кілттерді таратумен байланысты.

Сурет 1.2 – Симметриялық криптожүйелердің түрлері

Алмастыру шифрлары.

Алмастыру шифрымен шифрлау кезінде мәтіннің әрбір символы осы мәтін аумағында белгілі бір ереже бойынша ауыстырылады. Алмастыру шифрлары ең қарапайым және ең көне шифрлар болып табылады.

Жай алмастыру шифрлары.

Шифрлау кезінде шифрланатын мәтіннің таңбалары осы алфавиттің немесе басқа алфавиттің таңбаларымен алдын ала дайындалған ереже бойынша алмастырылады. Жай алмастыру шифрында бастапқы мәтіннің әрбір таңбасы осы алфавиттің таңбаларымен барлық мәтін ұзындығында бірдей

алмастырылады. Жай алмастыру шифрлары біралфавитті қойылым шифрлары деп аталады.

Күрделі алмастыру шифрлары.

Берілген хабардың әрбір символын шифрлау үшін қарапайым алмастырудың өз шифры қолданылатын болғандықтан, күрделі алмастыру шифрлары көп алфавитті деп аталады. Көп алфавитті қойылым қолданылатын алфавиттерді тізбектеп және цикіл бойынша өзгертеді.

Гамма әдісімен шифрлау.

Гамма процесі деп ашық мәліметтерге гамма шифрдың қандай да бір анықталған заңы бойынша бірігуін айтамыз. Гамма шифр ашық мәліметтерді берілген алгоритм бойынша шифрлау және шифрланған мәліметтерді шешуге арналған – кездейсоқ жүйелілік. Шифрлау процесі гамма шифрдың негізінде (генерация) және алынған гамманы негізгі ашық мәтінге қайтарымды бейнемен салу болып табылады.

Симметриялы криптожүйеден қарағанда ашық кілтті криптожүйеде екі кілт: ашық және жабық (жабық сақталады құпия) пайдаланылады. Ашық кілт ЭЦҚ-ны тексеру үшін және хабар шифрлауы үшін пайдаланылады. Жабық кілт

– ЭЦҚ-ті генерациялау үшін және шифрді ашу үшін қолданылады.

1.3 Data Encryption Standard

Жеке кілті бар ең танымал криптографиялық жүйелердің бірі - DES - Data Encryption Standard. Бұл жүйе деректерді шифрлау саласындағы бірінші болып мемлекеттік стандарт мәртебесін алды. Оны IBM мамандары әзірледі және 1977 жылы АҚШ-та күшіне енді. DES алгоритмі әр түрлі есептеу жүйелері арасында мәліметтерді сақтау және беру кезінде кеңінен қолданылды; пошта жүйелерінде, электронды сызу жүйелерінде және коммерциялық ақпараттың электрондық алмасуында. DES стандарты бағдарламалық және аппараттық құралдармен бірге қолданылды. Әр түрлі елдердің кәсіпорындары деректерді шифрлау үшін DES көмегімен сандық құрылғылардың жаппай өндірісін бастады. Барлық құрылғылар стандартқа сәйкестігіне міндетті сертификаттаудан өтті.

Біраз уақыттан бері бұл жүйе мемлекеттік стандарт мәртебесіне ие болмаса да, ол әлі күнге дейін кеңінен қолданылады және жеке кілтпен блоктық шифрларды зерттеу кезінде назар аударуға лайық.

DES алгоритміндегі кілт ұзындығы - 56 бит. DES-тің түрлі шабуылдарға төтеп беру қабілетіне қатысты негізгі қарама-қайшылық осыған байланысты. Өзіңіз білетіндей, жеке кілтпен кез келген блок шифрды барлық мүмкін кілт комбинациялары бойынша сұрыптау арқылы бұзуға болады. Кілттің ұзындығы 56 бит, 2^{56} түрлі кілт болуы мүмкін. Егер компьютер бір секундта 1,000,000 кілттер арқылы өтетін болса (бұл шамамен 2^{20}), онда барлық 2^{56} кілттерді сұрыптау үшін 2^{36} секунд немесе екі мың жылдан астам уақыт кетеді, бұл, әрине, шабуылдаушылар үшін қолайсыз.

Дегенмен, жеке компьютерге қарағанда қымбат және жылдам есептеу жүйелері мүмкін. Мысалы, егер сізде параллельді есептеу үшін миллион

процессорды біріктіруге мүмкіндігіңіз болса, онда пернелерді таңдаудың максималды уақыты шамамен 18 сағатқа дейін қысқарады. Бұл уақыт өте ұзақ емес, сондықтан қымбат техникамен жабдықталған криптографик қолайлы уақыт ішінде DES шифрланған деректердің автоматты түрде жасалуын жүзеге асыра алады.

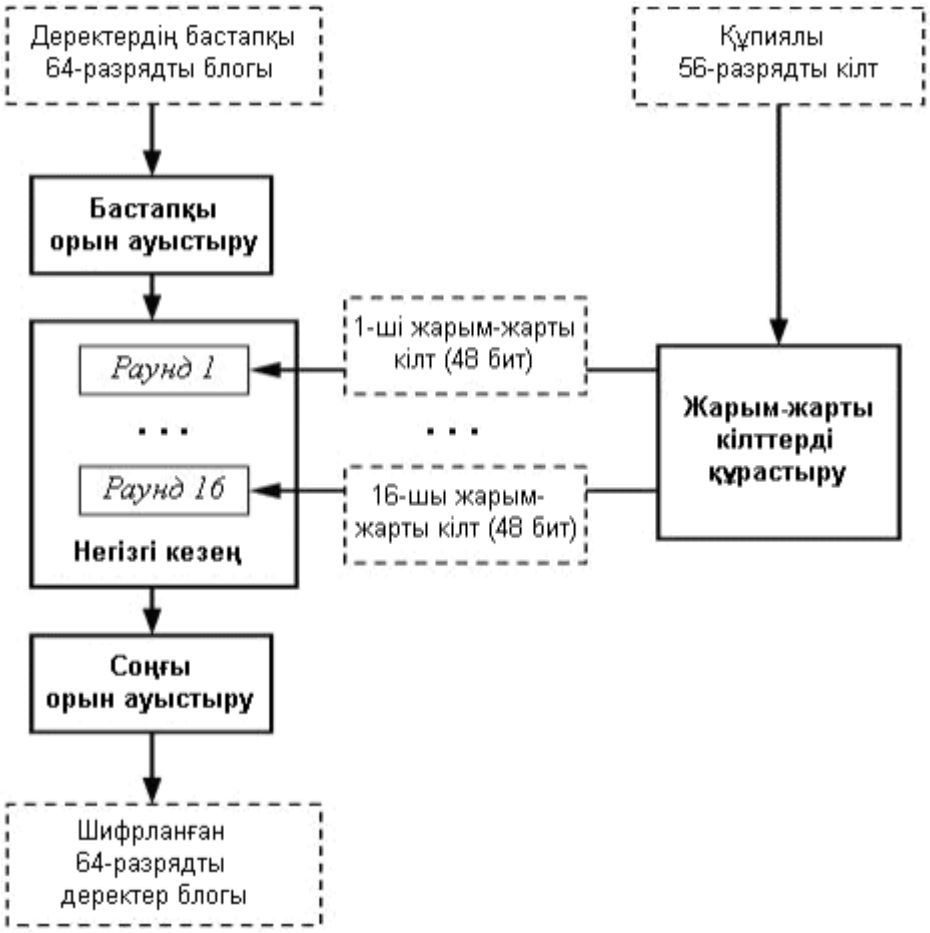
Сонымен қатар, DES жүйесін кіші және орта қосымшаларда шамалы мәліметтерді шифрлау үшін қолдануға болатындығын атап өтуге болады. Мемлекеттік маңызы бар немесе коммерциялық маңызы бар деректерді шифрлау үшін, DES жүйесі, әрине, қазіргі уақытта пайдаланылмауы керек. 2001 жылы Америка Құрама Штаттарында арнайы жарияланған бәсекелестіктен кейін Бельгия сарапшылары әзірлеген Рижндаэл шифріне негізделген AES (Advanced Encryption Standard) деп аталатын блок шифрлаудың жаңа стандарты қабылданды. Бұл код дәріс соңында қарастырылады.

DES негізгі параметрлері: блоктың өлшемі 64 бит, кілтінің ұзындығы 56 бит, айналым саны - 16 DES - бұл екі филиалы бар классикалық Feistel желісі. Алгоритм 64 биттік кіріс деректер блогын бірнеше айналымда 64 биттік шығыс блогына айналдырады. DES стандарты қайта жоспарлау, ауыстыру және ойын жабдықтарын бірлесіп пайдалануға негізделген. Шифрланған мәліметтер екілік түрінде ұсынылуы керек.

Шифрлау. DES-ң жалпы құрылымы 2.1 суретте көрсетілген. Бастапқы мәліметтердің әрбір 64- битты блоктын шифрлау процесін үш кезеңге бөлуге болады:

1) деректер блогын дайындау;
2) негізгі циклдың 16 раунды;
3) деректер блогының соңғы өңдеуі.

Бірінші кезеңде бастапқы мәтіннің 64-битты блогының бастапқы орын ауыстыруы орындалады, сол кезде биттер белгілі түрде қайталанып реттеледі.



Сурет 1.3 – DES-ң жалпы схемасы

Келесі (негізгі) кезеңде блок әрқайсысы 32 биттен тұратын екі бөлікке (бұтақтарға) бөлінеді. Оң жақ тармақ F функциясының және негізгі шифрлау кілтінен алынған арнайы перне түрлендірудің арнайы алгоритмін қолдана отырып, өзгертілген. Содан кейін мәліметтер блоктың сол және оң тармақтары арасында алмасады. Бұл циклде 16 рет қайталанады. Соңында, үшінші кезеңде негізгі циклдің он алты сатысынан кейін алынған нәтиже өзгереді. Бұл ауыстыру бастапқы орын ауыстырудың кері әдісі болып табылады.

DES стандартына сәйкес криптографиялық түрлендірудің барлық кезеңдерін толығырақ қарастырайық.

Алғашқы қадамда 64 биттік бастапқы деректер блогы бастапқы ауыстырудан өтеді. Әдебиетте бұл операция кейде «ағарту» - ағарту деп аталады. Бастапқы пермутация кезінде мәліметтер блогының биттері белгілі бір жолмен ретке келтіріледі. Бұл операция бастапқы хабарға «кездейсоқтықты» береді, статистикалық әдістермен криптанализді қолдану мүмкіндігін азайтады.

Деректер блогын бастапқы орын ауыстырумен қатар, кілттің 56 битінің бастапқы пермутациясы жасалады. 1.3 суретте көрсетілгендей әр раундта 48-биттік Кі-нің сәйкес келетін жартылай кілті қолданылатыны байқалады. Кі

кілті белгілі бір дәрежеде алынады.

Кі кілттері бастапқы алгоритм бойынша алынады, бастапқы батырманың әр битін бірнеше рет қолданады. Әр айналымда 56 биттік кілт 28 биттік екі жартыға бөлінеді. Содан кейін жартысы айналым санына байланысты бір немесе екі битке солға жылжиды. Ауыстырудан кейін 56 биттің 48-і белгілі бір жолмен таңдалады. Бұл биттердің жиынтығын таңдап қана қоймай, олардың тәртібін өзгертетіндіктен, бұл операция «сығымдау арқылы пермутрация» деп аталады. Оның нәтижесі 48 бит жиынтығы. Орташа алғанда, бастапқы 56 биттік кілттің әр биті 16 ішкі кілттің 14-інде қолданылады, дегенмен барлық биттер бірдей пайдаланылмайды.

Әрбір аралық мәннің сол және оң тармақтары L және R әріптерімен белгіленген 32 биттік жеке мәндер ретінде қарастырылады.

Бастапқыда Ri блогының оң жағы 48 битке дейін орын ауыстыруды және 16 битті кеңейтуді анықтайтын кестені қолдана отырып кеңейтілді. Бұл операция XOR операциясын орындау үшін оң жартысының өлшемін кілт өлшеміне бейімдейді. Сонымен қатар, осы операцияның арқасында нәтиженің барлық биттерінің бастапқы деректер мен кілтке байланысты болуы тез өседі (бұл «көшкіннің әсері» деп аталады). Белгілі бір шифрлау алгоритмін қолданған кезде көшкіннің әсері неғұрлым күшті болса, соғұрлым жақсы болады.

Алынған 48 биттік мәнді кеңейтумен орын ауыстыруды жасағаннан кейін, XOR операциясы 48-биттік кіші кілтпен орындалады. Содан кейін алынған 48-разрядты S ауыстыру блогының кірісіне жібереді (ағылшынша алмастыру - алмастырудан), нәтижесінде 32-биттік мәні болады. Ауыстыру сегіз алмастырғыш блокта немесе сегіз S-қорапта жүзеге асырылады. Осы операцияны орындау кезінде 48 бит бит сегіз 6 биттік қосалқы бөліктерге бөлінеді, олардың әрқайсысы ауыстыру кестесінде төрт битпен ауыстырылады. S-блокты ауыстыру DES-тің маңызды қадамдарының бірі болып табылады. Бұл операцияға арналған алмастырғыш үстелдер қауіпсіздікті қамтамасыз ету үшін арнайы жасалынған. Осы қадамның нәтижесінде тағы 32 биттік мәнге қайтадан біріктірілген сегіз биттік 4 блок алынды.

Әрі қарай, алынған 32-разрядтық мәні орын ауыструмен P көмегімен өңделеді (ағылш. Permution – орын ауыстыру), ол қолданылған кілтке тәуелді емес. Орын ауыстырудың мақсаты биттердің ретін өзгертуді барынша арттыру, осылайша шифрлеудің келесі айналымында әр бит басқа S-блокпен өңделуі мүмкін.

Соңында, енгізудің нәтижесі XOR операциясын пайдаланып, 64 биттік бастапқы деректер блогының сол жағымен біріктіріледі. Содан кейін сол және оң жартысы ауыстырылып, келесі айналым басталады.

Он алты раундтан кейін шифрлау нәтижесі бойынша түпкілікті өзгеріс жасалады. Бұл ауыстыру бастапқы термияға кері (кері).

Осы қадамдардың барлығын орындағаннан кейін, деректер блогы толық шифрланған болып саналады және сіз бастапқы хабарламаның келесі блогын

шифрлауға кірісе аласыз.

Қағаздағы DES-тің қарапайым сипаттамасы да өте күрделі болып көрінеді, тіпті оны бағдарламалық жасақтамамен іске асырудан басқа! Толығымен DES сәйкес дұрыс және оңтайлы жұмыс істейтін бағдарламаны жасау үшін оны тек тәжірибелі бағдарламашылар жасай алады. Бағдарламалық жасақтаманы іске асыруда кейбір қиындықтар туындайды, мысалы, алғашқы пермутация немесе кеңейту арқылы пермутрация Бұл қиындықтар бастапқыда DES-ті тек аппараттық қамтамасыз етуде енгізу жоспарланғандығымен байланысты. Стандартта қолданылған барлық операцияларды аппараттық құралдар оңай орындайды және оны орындауда қиындықтар болмайды. Алайда, стандарт жарияланғаннан кейін біраз уақыт өткен соң, бағдарламалық жасақтама жасаушылар шетте қалмауға шешім қабылдады және шифрлау жүйесін құруды бастады. Болашақта DES аппараттық және бағдарламалық қамтамасыздандырумен қатар енгізілді.

Өздеріңіз білетіндей, криптографиялық жүйе тек шифрлауға ғана емес, сонымен бірге хабарламалардың шифрын шешуге де мүмкіндік беруі керек. DES-ті дешифрлау процесі өте күрделі болады деп күтуге болады. Алайда, әзірлеушілер стандарттың әр түрлі компоненттерін таңдады, сондықтан шифрлау мен шифрын шешуде бірдей алгоритм қолданылады. Шифрлау кезінде шифрланған мәтін алгоритмнің енгізілуіне беріледі. Жалғыз айырмашылық - ішінара Кі пернелерін қолданудың кері тәртібі. K_{16} бірінші айналымда, K_1 соңғы айналымда қолданылады.

Шифрлау процесінің соңғы айналымынан кейін шығудың екі жартысы ауыстырылады, осылайша қорытынды пермутация кірісі R_{16} және L_{16}-дан тұрады. Бұл кезеңнің нәтижесі - шифрланбаған мәтін.

DES Файстель шифрінің он алты айналым шифрін қолданады. Әр мәтін сегіз раундқа шифрланғаннан кейін, шифр мәтінінің әр биті бастапқы мәтіннің әр битінің және әр биттің функциясы болатындығы дәлелденді. Шифермәтін - бұл мәтін мен шифр мәтінінің кездейсоқ функциясы. Міне, жақсы шифрлау үшін сегіз раунд жеткілікті болуы керек. Алайда, эксперименттер көрсеткендей, DES-тің он алты раундтан аз нұсқалары, күшті шабуылдардан гөрі, білім көздерінің шабуылдарына он алты раундты қажет етеді.

Қорытындылай келе, қазіргі уақытта DES-тің басты кемшілігі - бұл кішкене кілт ұзындығы. Криптанализ процесін күрделендірудің қарапайым тәсілі - әр түрлі кілттермен бірдей алгоритмді қолданып екі реттік шифрлау.

1.4 Асимметриялық криптожүйелер (Ашық кілтті)

Асимметриялық шифрлау немесе ашық кілттердің криптографиялық жүйесі - деректерді шифрлау және шифрын ашу үшін ашық кілттер мен жеке кілттерді пайдаланатын криптографиялық жүйе. Бұл кілттер деп аталатын кілттер жұбын құрайды және үлкен сандар болып табылады, олар белгілі бір тәуелділікпен байланысты, бірақ бір-бірінен ерекшеленеді.

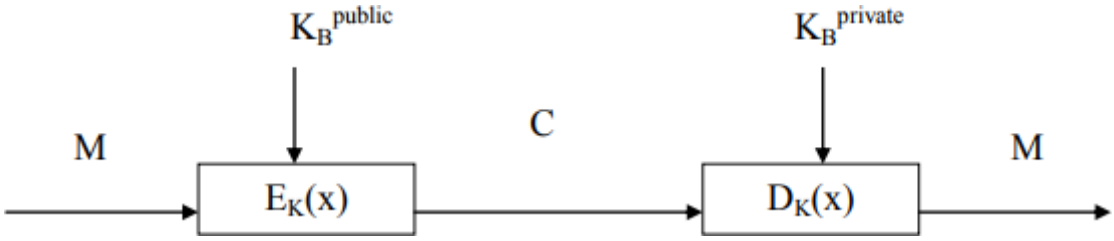
Ашық кілт қауіпсіз байланыс арналары арқылы беріледі және бәріне

белгілі. Ашық кілттің көмегімен мәліметтер шифрланады және құжаттардың электрондық қолтаңбасы (ЭЦҚ) тексеріледі.

Деректердің шифрын ашу үшін құпия кілт қолданылады. Осылайша, симметриялық шифрлаудың асимметриялық шифрлаудың басты артықшылығы - тараптардың құпия байланыс арналарын пайдаланбай бір-бірімен байланысып, деректер алмасу мүмкіндігі.

Шифрлау күші (криптографиялық беріктілік) кілт ұзындығына тәуелді және кілт ұзындығымен экспоненциалды түрде артады.

Алгоритмнің сүлбесі 3-суретте көрсетілген. Кейбір криптографиялық алгоритмдерде, мысалы, электрондық қол таңбаны алу үшін, хабарды жабық кілтпен шифрлайды. Шифр мәтінді дешифрлау үшін ашық кілтті қолданады.



Сурет 1.4 – Ашық кілтті криптожүйенің сүлбесі.

Криптографиялық алгоритм жалпыға мәлім болуы тиіс. Қазіргі криптографиялық жүйелер келесі Керкхофф ережесі бойынша қарастырылады:

– алгоритмде қолданылатын түрлендірулер механизмі жалпыға белгілі деп саналады;

– алгоритмнің сенімділігі тек қана құпия кілтке байланысты деп саналады.

Асимметриялық шифрлау алгоритмдерінің дамуы криптография тарихындағы ең үлкен және мүмкін жалғыз шынайы революциялық жетістік болып табылады.

Ашық кілт алгоритмдері деп аталатын ассиметриялық шифрлау алгоритмдері симметриялық шифрлау алгоритмдерінен түбегейлі ерекшеленеді. Ашық кілттерді шифрлау ассиметриялық болып табылады, өйткені ол симметриялық шифрлауға қарағанда, шифрлау мен дешифрлау үшін екі түрлі кілт қолданады, сол шифрлау және шифрлау үшін сол кілт қолданылады. Ашық кілт алгоритмдері негізінен ауыстыру және қозғалыс операцияларын қолданатын симметриялық шифрлау алгоритмдеріне қарағанда математикалық функциялардың қасиеттеріне негізделеді. Екі кілттің болуы аутентификация, кілттерді тарату және құпиялылық сияқты салаларда маңызды қолданылады.

Ашық кілт алгоритмдері симметриялы шифрлауды қолдану кезінде туындайтын екі қиын міндеттерді шешу үшін жасалды.

Бірінші міндет - кілтті тарату. Симметриялық шифрлау кезінде екі тараптың да ортақ кілті болуы керек, оны қандай да бір түрде алдын-ала беру

керек. Ашық кілт шифрлауды құрушылардың бірі Диффи бұл талап криптографияның мәнін жоққа шығаратынын, оның басты мақсаты байланыс құпиясын сақтау болып табылатындығын атап өтті.

Екінші міндет - кез-келген қатысушыны алмастыру мүмкін болмайтын осындай тетіктерді құру қажеттілігі. нақты әлемде қолданылатын қолтаңбаның аналогы қажет. Мұндай аналогты әдетте цифрлы немесе электрондық қолтаңба деп атайды (ағылшынша нұсқасы Digital Signature). Байланыстарды көптеген мәселелерді шешу үшін пайдаланған кезде, мысалы, коммерциялық және жеке мақсаттар үшін электрондық хабарламалар мен құжаттарда қағаз құжаттарындағы қолтаңба баламасы болуы керек. Электрондық хабарламаның белгілі бір қатысушы жібергеніне барлық қатысушылар сенімді болатын әдісті жасау керек. Бұл парольді немесе ортақ құпияны пайдалану арқылы аутентификацияға қарағанда анағұрлым күшті талап.

1.5 RSA криптожүйесі

Соңғы бірнеше онжылдықтар ішінде, адамзат үлкен көлемді ақпараттарды жіберу қиындықтарымен кездесті. Жіберу кезінде бұл ақпараттарды рұқсатынсыз көру немесе оқу мәселесін шешу қазіргі таңда ең өзекті мәселелердің біріне айналды. Алгоритмнің қауіпсіздігі оның кілттеріне негізделген. Кілттерді генерациялау барысында криптографиялық әлсіз процессті қолдансаңыз, онда сіздің жүйеңіз жалпы әлсіз болады. Ең сенімді алгоритмдер бәріне мәлім болғанымен, шифрленген хабарламаның кілттерін, мүмкін мәндері бойынша іріктеу арқылы есептеп алуға болады. Ақпараттану заманында ассиметриялық криптожүйелерді жиі қолданады. Себебі, ассиметриялық криптожүйелердің ерекшелігі екі кілттің қолдануында. Біреуі бәріне мәлім болса, екіншісі құпия болып табылады және олар математикалық қандай да бір заңдылықпен байланысқан. Яғни, ашық кілтпен шифрленген хабарды білгенімен құпия хабарды аша алмайсыз, ал құпия кілттің көмегімен дешифрлей алсаңызда ашық хабарды шифрлей алмайсыз. Ең қиыны кілттерді құпия түрінде сақтау болып табылады. Оларды тарату кезіндегі жіберілген қателіктердің, сонымен қатар немқұрай сақтаудың салдарынан бұзушы жабық ақпаратқа қол жеткізе алады. Осыдан кілттерді басқару есебі туындайды.

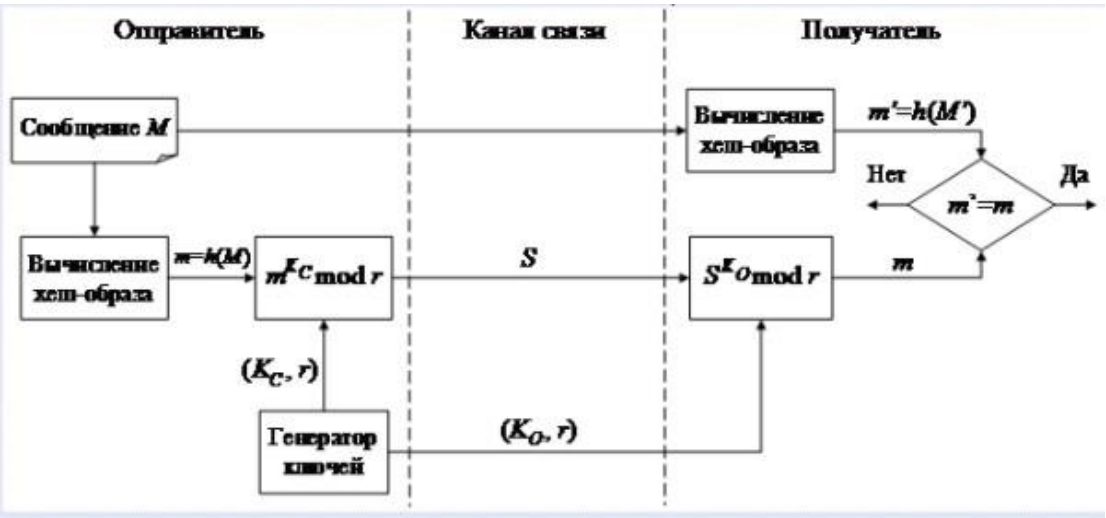
Кілттерді басқару жүйесінің негізгі этаптары:

- кілттерді генерациялау,
- кілттерді тарату,
- кілттерді қолдану,
- кілттерді тексеру,
- кілттерді жаңарту,
- кілттерді сақтау,
- кілттерді жою.

Ақпараттарды қорғау үшін криптографиялық жүйеде ең тиімді және жиі қолданылатын жүйелердің бірі RSA криптожүйесі болып табылады. Бұл

криптожүйені 1978 жылы Р.Л Райвест, А.Шамир және Л.Адлеман деген үш математик ғалымдар ойлап тапқан. Өте қарапайым және «ашық кілтті криптожүйенің» тамаша үлгісі болғандықтан қазір бүкіл әлемде кеңінен таралған. Бұл криптожүйенің негізгі қиындығы –модулінің жай сандарға жіктелуі болып табылады. RSA криптожүйесі үлкен сандарды факторизациялау күрделілігіне негізделген жақсы криптоберіктілікпен ерекшеленеді. Бұл алгоритм мәліметтерді шифрлеу режимінде және электронды сандық қолтаңба режимінде жұмыс істей алатын ең бірінші толыққанды алгоритм болып саналады. Ол ашық жүйелер үшін дүниежүзілік стандартқа айналды. Сонымен қатар RSA SWIFT, ANSI X9.31 rDSA және американдық банктер үшін қолданылатын жобасының X9.44 стандартының бөлігі болып табылады. Бұл алгоритм жеке криптографиялық өнімі ретінде, сонымен қатар қосымшаларға ендірілген құрал ретінде қолданылады.Заманауи криптографияның математикалық негізі ретінде сандар теориясы қолданылады. Жоғарыда криптожүйенің негізгі қиындығы үлкен санның екі үлкен жай сандарға жіктелуі туралы атап айтқандай, бұл саладағы көптеген зерттеулердің ішінде ең өзектілерінің бірі санды жай не жай еместігіне тексеру болып табылады. RSA криптожүйесінің n=p*q модулін есептеу үшін p,q екі үлкен жай сандары қолданылады. Осыған байланысты RSA криптожүйенің кілттерін генерациялау жылдамдығы n модулін есептеу барысындағы, таңдалған сандардың жай не жай емес мәселесін шешу жолдарымен анықталған. RSA ассиметриялық шифрлау алгоритмдеріне сілтеме жасайды: егер ашық кілт шифрлау үшін пайдаланылса, онда шифрды ашу үшін жеке кілт қолданылады және керісінше. Бірінші сипат кез-келген адамға ашық кілтпен хабарламаны жеке кілт иесінің мекен-жайына шифрлауға және сол арқылы оның құпиялылығын қамтамасыз етуге мүмкіндік береді. Екінші сипат кілт иесіне хабар хэшін жеке кілтпен шифрлауға мүмкіндік береді, осылайша кез-келген адам шифрланған хэшті шешіп, оны хэшпен салыстырып, хабарлама өзгертілгенін анықтай алады.

Негізінде RSA негізгі міндеті екі қарапайым үлкен сандар факторлау. Шифрлау үшін қарапайым операция N модуль бойынша дәрежеге шығару пайдаланылады. Шифрды ашу үшін қажет Эйлер функциясын N санының есептеу қажет, бұл үшін n санының жай сандарға ыдырауының білу қажет, (бұл факторлау міндет).



Сурет 1.5 – Электронды кілт сұлбасы.

Қазіргі таңда санның жай, не жай емес екендігін тексеретін алгоритмдер мен тесттар бар. Санның жай не жай еместігін ерте заманнан бастап зерттегенмен, ең басты бағыты XX ғасырдың II-ші жартысында бастау алды. Оның себебі кілттерді генерациялауда үлкен жай сандардың қолданылуы болып табылады. Жай сандарды тексеру алгоритмдері екіге бөлінеді: детерминирленген және ықтималды. Олардың ішінде кең таралған және жиі қолданылатын ықтималды алгоритмдер болып табылады.

XVII ғасырда француз математигі Пьер Ферма сандарды жай санға тексеруге арналған мүмкін тесттердің бәрінің негізі болатын тұжырымдаманы енгізіп кеткен.Ферманың кіші теоремасы:
егер p – жай сан болса, a – кез келген бүтін сан болса, онда $a^p = a(mod\ p)$, ал егер p a-ны бөлмесе, онда $a^{p-1} = 1(mod\ p)$.

Бұл теоремаға сүйеніп, санды жай санға тексеру үшін қолданылатын мықты тесттердің бірін құруға болады.

Ферма тесті: n >1 үшін a >1 теңдігін қанағаттандыратын a — ны таңдаса және $a^{n-1} = 1(mod\ n)$ есептейміз. Егер нәтижесінде 1 шықса, онда ол сан жай сан болып табылады. Ал егер, 1-ге тең емес болса, онда ол сан құрама сан болып шығады.

Ықтималды алгоримдердің ең жиі қолданылатын тесттері Соловей-Штрассен мен Миллер-Рабин.

Соловей-Штрассен тесті Эйлер критерияларына және квадраттық шегеру ұғымына негізделген. Квадраттық шегеру дегеніміз — кез келген санның квадратын p модулі бойынша бөлгендегі қалдығы болып табылатын a бүтін санын айтамыз: $x^2 = a(mod\ p)$.

Эйлер критериясы: p — жай сан болсын, $a \in z_p$ a квадраттық шегеру болып табылады, егер $a^{p-1/2} = 1(modp)$ салыстыруы орындалса.
Соловей-Штрассен тесті еңбекті көп қажет етпейді және k рет орындалғаннан кейін санды жай екенін анықтау қатесінің ықтималдылығы 0.5-ден аспайды. Бірақ практика жүзінде бұл тестің сенімділік дәрежесі

жеткіліксіз.

Соловей-Штрассен тестіне қарағанда, жоғарырақ сенімділікті Миллер-Рябин тесті береді. Бұл тест Ферма тестімен $a^{N-1} = 1(modN)$ бірігу жолында алынған. Келесі салыстырулардың көмегімен$a^{2st} = 1(modN)$, $2^st = N - 1$ (N,t— тақ сандар) құрама сандарды шығарып тастайды.

Осыған байланысты, санның жай екендігін анықтайтын алгоритмдер (мысалы Миллер-Рабин алгоритмі), RSA криптожүйесіндегі кілттерді генерациялауда атқаратын рөлі өте маңызды. RSA зертханасы қарапайым есептер үшін кілттің ұзындығы 1024 битке тең, ал маңыздырақ есептер үшін кілттердің ұзындығы 2048 битке және одан да ұзынырақ болуына нұсқау береді. Мысалы, Қазақстан Республикасының қауіпсіздігін қамтамасыз ету стандартында СТ РК 1073–2007, 3-ші қауіпсіздік деңгейін қамтамасыз ету үшін кілттің ұзындығы 4000 бит, ал 4-ші қауіпсіздік деңгейін қамтамасыз ету үшін кілттің ұзындығы 8000 бит болуы керек екендігі көрсетілген.

Іс жүзінде ашық кілттерді арнайы мәліметтер базасына орналастыруға болады. Егер серіктеске шифрланған хабарлама жіберу керек болса, алдымен оның ашық кілтін сұрауға болады. Оны алғаннан кейін сіз шифрлау бағдарламасын іске қосып, оның нәтижесін адресатқа жібере аласыз. Ашық кілттерді пайдалану жіберушінің бірегейлігін анықтауға мүмкіндік беретін электрондық қолтаңба деп аталады. Ұқсас құралдарды жіберушіден алушыға хабарламада түзетулердің алдын алу үшін пайдалануға болады. 512 биттік жоғары жылдамдықты аппараттық модуль 64 кбит / с жылдамдықты шифрлауға мүмкіндік береді. Мұндай операцияларды 1 МБ / с жылдамдықта орындауға қабілетті ХҚ дайындау. Е параметрін орынды таңдау алгоритмнің орындалуын едәуір жеделдетуі мүмкін. Сандық қолтаңбаның маңызды қасиеті - оны автордың ашық кілтіне қол жеткізе алатын кез келген адам тексере алады. Электрондық цифрлық қолтаңба расталғаннан кейін, хабар алмасуға қатысушылардың бірі қол қойылған хабарламаны осы қолтаңбаны тексере алатын басқа біреуге бере алады. Мысалы, А жағы электронды чекті В жағына жібере алады. В партиясы чекте А қолтаңбасын тексергеннен кейін, ол оны өз банкіне тапсыра алады, оның қызметкерлері қолтаңбаны тексеріп, сәйкес ақша операцияларын жүргізе алады.

Қол қойылған m шифрланбағанын ескеріңіз. Ол түпнұсқа түрінде жіберіледі және оның мазмұны құпиялылықтан қорғалмаған. Жоғарыда аталған шифрлау схемалары мен цифрлық қолтаңбаларды RSA жүйесінде бірлесіп қолдану арқылы сіз шифрланатын және сандық қолтаңбасы бар хабарламаларды жасай аласыз. Ол үшін автор алдымен электрондық цифрлық қолтаңбаны хабарламаға қосып, содан кейін алынған жұпты (хабарламаның өзі мен қолтаңбасынан тұратын) алушыға тиесілі ашық кілтпен шифрлауы керек. Алушы қабылданған хабарламаны өзінің құпия кілтін пайдаланып шифрлайды . Егер біз кәдімгі қағаз құжаттарын жіберумен ұқсастық алсақ, онда бұл процесс құжат авторының мөрін оның астына салып, содан кейін оны қағаз конвертке салып, мөр басылған кезде конвертті хабарлама жіберілген адам ғана басып шығаратындығына ұқсайды.

RSA-да ашық және жабық кілт жұп және бүтін сандардаң тұрады. Жабық кілт құпияда сақталады, ал ашық кілт басқа қатысушыға хабарланады немесе басқа жерде жарияланады.

SSH, OpenPGP, S / MIME және SSL / TLS сияқты көптеген протоколдар деректерді шифрлау үшін RSA қолданады. Сондай-ақ, RSA браузерлерде қолданылады, өйткені үнемі қауіпті желі арқылы қауіпсіз байланыс орнатуға немесе сандық қолтаңбаны тексеруге тура келеді. Бұл RSA цифрлық қолтаңбасын тексеру қазіргі кезде АТ-да ең кең таралған жұмыс болып табылады.

RSA алгоритмі AES және симметриялы блок шифрларын қолданатын басқа алгоритмдерге қарағанда әлдеқайда баяу. RSA ашық кілтінің криптографиялық жүйесі екі үлкен жай сандардың көбейтіндісін факторизациялау мәселесінің күрделілігіне негізделген. Шифрлау үшін қуатты модульге дейін көбейту операциясы қолданылады. Саналы уақыт аралығында шифрды шешу (кері операция) үшін берілген үлкен санның Эйлер функциясын есептей білу керек, ол үшін санның негізгі факторларға бөлінуін білу қажет.

Ашық кілттің криптографиялық жүйесінде әрбір қатысушыда ашық кілт (ашық кілт) және жеке кілт (жеке кілт) болады. RSA криптографиялық жүйесінде әр кілт жұп бүтін сандардан тұрады. Әр қатысушы өзінің жеке және жеке кілттерін жасайды. Олардың әрқайсысы жеке кілттің құпиясын сақтайды және ашық кілттерді кез-келген адаммен бөлісуге немесе тіпті жариялауға болады.

Алгоритм дұрыс емес немесе оптималды емес қолданылған немесе қолданылған жағдайда арнайы криптографиялық шабуылдар мүмкін, мысалы, кішігірім экспоненттті схемаларға немесе жалпы таңдалған модуль мәні бар схемаларға шабуылдар.

Қорытындылай келе RSA жүйесі бағдарламалық жасақтаманы және цифрлық қолтаңба схемаларын қорғау үшін қолданылады. Ол сонымен қатар PGP ашық шифрлау жүйесінде және басқа шифрлау жүйелерінде қолданылады (мысалы, DarkCryptTC және xdc форматы) симметриялық алгоритмдермен үйлесімде.

Қазіргі уақытта ең көп қолданылатыны - аралас шифрлау алгоритмі, онда сеанс кілті алдымен шифрланады, содан кейін қатысушылар өздерінің хабарламаларын симметриялы жүйелермен шифрлайды. Сеанс аяқталғаннан кейін сессияның кілті әдетте жойылады.

1.6 RSA-да кілттерді генерациялау

Барлығы ашық және жабық кілтті генерациялаудан басталады. Табылған жай сандардың өнімі ашық және жеке кілттердің алғашқы элементі болып табылады. Жоғарыда аталған алгоритм ақылға қонымды уақытта тек алғашқы миллион жай сандарды табуға мүмкіндік береді. Ақпаратты қорғау үшін қолданылатын RSA енгізулерінде сандардың көптігі бар жай сандарды табу

үшін қарапайым іздеу алгоритмдері қолданылады; Санды жай факторларға бөлудің алгоритмінің ең танымал алгоритмі цифрлар санының көрсеткішіне пропорционалды уақыт аралығында жұмыс істейтіндігіне байланысты, қарастырылып отырған ашық кілттен екі санды қысқарту мүмкін емес деп саналады. RSA-да кілттерді генерациялау былайша жүзеге асырылады:

1) Екі жай санын p және q таңдалады (мұндай p мен q тең болмау қажет).
2) N=p∗q модуль есептеледі.
3) Эйлер функциясының модулі есептеледі *N: $\phi(N)=(p-1)(q-1)$.*
4) e саны таңдалады, ашық экспоненті деп аталатын, e саны аралығында жатуға тиіс. 1<e<ϕ(N), сондай-ақ болуы мүмкін өзара жай мәндегі функциялар ϕ(N).
5) Мұнда d саны деп аталатын құпия экспонент, мұндай, бұл $d*e=1(mod\phi(N))$, яғни болып табылады мультипликативно кері санына e модуль бойынша ϕ(N).

Сонымен, біз екі кілт алдық:
Жұп (e,N) ашық кілт. Жұп (d,N) - жабық кілт.

1.7 RSA-да шифрлау және шифрды шешу

Келесі сценарий бар: Болат және Алия интернетте хат алмасап жатыр, бірақ шифрлауды пайдаланғысы келеді хат құпияда болу үшін. Алия алдын ала жабық және ашық кілтті есептеп алды, содан кейін Болатқа ашық кілтті жіберді. Болат шифрланған хатты Алияға жібергісі келеді:

Шифрлау: Болат m хатты шифрлайды, Алияның ашық кілтің қолданып (e,N) : C=E(M)=Memod(N), содан кейін Алияға жібереді.

Шифрді ашу: Алия кодталған c хабарды қабылдайды. Жабық кілт (d,N), пайдалана отырып, хабардың шифырың ашады M=D(C)=Cdmod(N).

Негізінде RSA негізгі міндеті екі қарапайым үлкен сандар факторлау. Шифрлау үшін қарапайым операция *N* модуль бойынша дәрежеге шығару пайдаланылады. Бұл схема іс жүзінде сенімді емес (семантикалық қамтамасыз етілген) болғандықтан қолданылмайды. Шынында да, E (m) функциясы детерминистік - кіріс параметрлерінің бірдей мәндері үшін (кілт және хабарлама) бірдей нәтиже береді. Бұл шифрдің практикалық (семантикалық) сенімділігі үшін қажетті шарт орындалмағанын білдіреді. Шифрды ашу үшін қажет Эйлер функциясын *N* санының есептеу қажет, бұл үшін n санының жай сандарға ыдырауын білу қажет. RSA алгоритмін қолдана отырып, сіз 0-ден n-1 дейінгі диапазондағы M сандарымен ұсынылған хабарламаларды шифрлай аласыз. Шифрлау M модуліндегі қалдық сақинадағы n қуатын e-ге дейін көтеруге, d-ге дешифрлеуден тұрады. Көбейту ассоциативті болғандықтан, log (x) операциялары үшін x қуатын көбейтуге болады.

1.8 RSA схемасының қауіпсіздігі.

Схеманың қауіпсіздігі қандай параметлардан құралады. Болат және

Алияның хат жіберуіне Сакен қосылады деп елестетіп көрейікші, Болат қандай хабар жібергенін Сакен қалайды білуге тырысады. Мысалы, бар ашық кілт Алисы (e,N) үшін хабар таратып жазу с білу қажет жабық кілт (d,N). Біз білеміз, $d*e=1(mod\phi(N))$, алайда, Ева білмейді $\phi(N)=(p-1)*(q-1)$, т. е міндет азайтатын іздеу жай сан p және q (бұл емес,) байланысты белгілі N былайша $N=p*q$.

Қорытынды жасаймыз. Алгоритм үшін тұрақты болу үшің қажет:

1) Таңдау екі үлкен қарапайым кездейсоқ санын p және q (мысалы, >= 1024 бит әрбір), тиіс емес, тым әр түрлі және тым жақын.

2) Ең үлкен ортақ бөлгіш (p−1) (q−1) болуы тиіс аз, көп жағдайда тең екі.

3) Таңдауға үлкен мән ашық экспонат e, әдетте жай сандар таңдайды: 17, 257, 65537...

4) Сақталуы құпия жабық кілт.

RSA алгоритмінің қауіпсіздігі үлкен бүтін сандарды факторизациялау өте күрделі және қымбат есептеу процесі екендігіне негізделген. Шифрлаудың қауіпсіздігі үшінші тарап үшін ашық кілттің есігінен есептеу өте қиын болуымен қамтамасыз етіледі (шифрді бұзуға тырысады). Екі батырма да бір нүктеге дейін есептеледі (p және q). Яғни, кілттер өзара байланысты. Бірақ бұл байланысты орнату өте қиын. Негізгі модуль - n модулін p және q қарапайым факторларға бөлу. Егер сан екі өте үлкен жай сандардың көбейтіндісі болса, онда оны факторлау өте қиын. RSA 30 жылдан астам уақыт бойы қолданылып келеді және егер жеткілікті ұзындықтағы (2048 биттен кем емес) кілттер қолданылса, қауіпсіз шифрлау процесі болып саналады.

1.9 Біржақты функциялар. Хэш-функциялар

Біржақты функциялар криптографияның, тұлғалық идентификацияның, аутентификацияның ж/е т.б. ақпарат қорғау аудандарының фундаментальді аспабы болып табылады.

Біржақты функция (one way function) — X Y бейнелеуін жүзеге асыратын функция, мұндағы X ж/е Y — туынды көпмүше, ж/е бұл функция келесі шартты қанағаттандыруы керек:

1) x X үшін (—x-тің X анықталу аймағына тәуелді екенінің белгісі) y = f(x) есептеу оңай.

2) Кез келген y Y (мәндер аймағы) табу, яғни y =f(x) есептеу мүмкін емес болатын x-ті табу.

Біржақты функцияны қолданып парольді жіберу ж/е сақтау әдісі қауіпсіздікті қамтамасыз ету үшін дұрыс. Қолданушылар тізімінде парольді шифрлау кезінде белгілі криптографиялық тұрақты хэш-функцияны қолданады. Қолданушылар тізімінде парольдің өзі емес, хэш-функцияның паролінің нәтижесі болып табылатын парольдің үлгісі сақталады. Хэш-функцияның біржақтылығы парольге парольдің үлгісін қалпына келтіруге мүмкіндік бермейді, бірақ хэш-функцияны есептеп, қолданушы енгізген

парольдің үлгісін ж/е осылайша енгізген парольдің дұрыстығын тексеруге мүмкіндік береді. Хэш функцияларын пайдалану операциялық жүйенің маңызды файлдарының, маңызды бағдарламалар мен маңызды деректердің тұтастығын бақылау үшін жиі қолданылады. Мониторинг қажет болған жағдайда да, тұрақты негізде де жүргізілуі мүмкін. Алдымен сіз басқарғыңыз келетін файлдардың тұтастығын анықтаңыз. Әр файл үшін оның хэш мәні нәтижені сақтай отырып, арнайы алгоритммен есептеледі. Қажетті уақыт өткеннен кейін ұқсас есептеу жүргізіледі және нәтижелер салыстырылады. Егер мәндер әртүрлі болса, онда файлдағы ақпарат өзгерді. Мысалы, бір қолданушы нақты деректер массивін басқасына өткізеді, содан кейін одан хэш шығады. Ақпаратты алушы ақпаратты өзімен бірге жинап, қоқыстарды салыстыра отырып, оның нақты жіберілгеніне көз жеткізе алады.

Blockchain технологиясында хэш деректердің тұтастығын тексеру үшін де қолданылады. Хэш транзакция тізбегінің (төлемдердің) тұтастығының кепілі болып табылады және оны рұқсат етілмеген өзгерістерден қорғайды. Оның арқасында және таратылған есептеу, блокчейнді бұғаттау өте қиын. Мысалы, ұзындығы 1 миллион таңбадан тұратын бірнеше миллион түрлі сызықтардан тұратын массивке, ол әлі жоқ болса, тағы біреуін қосу керек. Әр жолды кейіпкерлермен салыстырумен айналыспас үшін, сіз олардың әрқайсысының хешін алдын-ала есептеп, қазірдің өзінде салыстыра аласыз. Барлық жұмыс кейде жеңілдетіліп, жеделдетіледі. Хэш функциясы көбінесе деректерді жылдам іздеу үшін хэш кестесімен, компьютерлік бағдарламаларда қолданылатын жалпы мәліметтер құрылымымен бірге қолданылады. Хэш - үлкен файлдағы қайталанатын жазбаларды табу арқылы кестені жылдамдату немесе дерекқорды іздеу функциялары. Осындай қосымшалардың бірі - мұндай аймақтарды ДНҚ тізбегінде табу. Олар криптографияда да пайдалы. Криптографиялық хэш функциясы картада берілген хэш мәні үшін кейбір кіріс деректері бар-жоғын тексеруді жеңілдетеді, алайда егер енгізу мәліметтері белгісіз болса, хэш функциясының сақталған мәнін біле отырып, оны қалпына келтіру әдейі қиын болады (немесе кез келген балама нұсқалар). Бұл берілетін деректердің тұтастығын қамтамасыз ету үшін қолданылады және хабарламаның түпнұсқалығын растауды қамтамасыз ететін HMAC үшін негіз болып табылады. Қарапайым жағдайда хэш-функция ретінде парольдегі бірнеше константаларды шифрлеу нәтижесі қолданылады.

Хэш–функциялардың қолданылуы:

1) Сандық қолтаңба механизміне қолданылатын хабардың қысылған бейнесін құру үшін.

2) Парольдерді қорғау үшін.

Хабар аутентификациялары кодын құру үшін. Хэш функцияларға қойылатын негізгі талаптар:

1) h(m) функциясының белгілі мәні бойынша оның m аргументін табу мүмкін емес(өте күрделі) болуы керек.Мұндай хэш функция айналдыру мағынасында берік деп аталады.

2) Берілген m аргумент үшін h(m)= h(m') боладтын h(m') табу мүмкін

емес. Мұндай хэш-функциялар композицияларды есептеу мағынасында берік деп аталады.

3) Практикалық маңыздылық үшін хэш функцияларды алу алгоритмі жылдам есептелінетін болу керек,одан да жақсысы-нақты аппаратты есептеу ортасында ықшамдалған болу керек.

Хэш функциясы қандай сипаттамаларға ие болуы керек?

- Оның криптографиялық беріктігін зерттеу үшін ашық алгоритм болуы керек;
- Ол бір жақты болуы керек, яғни бастапқы деректерді нәтиже бойынша анықтаудың математикалық мүмкіндігі болмауы керек;
- Ол соқтығысуларға «төтеп беруі» керек, яғни әртүрлі енгізілген мәліметтер үшін бірдей мәндерді шығармауы керек;
- Үлкен есептеу ресурстарын қажет етпеуі керек;
- Енгізілген деректер шамалы өзгерген кезде нәтиже айтарлықтай өзгеруі керек.

Сурет 1.6 – Хэш функцияларды есептеудің типтік сызбасы.

Хэш функциялардың ішіндегі ең белгілілері-MD2,MD4,MD5 ж/е SHA. MD2,MD4,MD5 — Ривестпен өңделген MD хэш функцияларын есептеу алгоритмдерінің тобы. 128-битті бейнеге қысылған еркін ұзындықтағы кіріс хабарын түрлендіреді.

2. Модуль бойынша сан келтіру

Қазіргі заманғы көптеген криптожүйелер ашық кілтті шифрлау түрін қолданады [1].

Ашық кілтті криптожүйенің жабық кілтті криптжүйеден басты артықшылығы: ашық кілтті криптожүйе қауіпсіздік ықтималдығы ең жоғары болып табылады, себебі құпия кілтті жіберіп және түпнұсқалығын тексеру қажеті жоқ.

Ашық кілтті криптожүйелердің негізгі кемшілігі төмен жылдамдығы болып табылады, өйткені шифрлау және дешифрлау кезінде күрделі және ауқымды математикалық есептеулер жүргізіледі, оның үстіне өте үлкен сандар пайдаланылады. Осындай криптожүйелердің өнімділігін арттыру үшін базалық операцияларды орындалуын жеделдету керек. Олар: көбейту операциялары, дәрежеге шығару және модуль алу.

Осы уақытқа дейін тез көбейтетің және дәрежеге шығаратын құрылғыларды әзірлеуде үлкен тәжірибеге жеттік. Оларға мыналар жатады: Браун матрица сумматоры, Уоллеса ағашына арналған көбейткіштері және Дадда санауыштары және тағы басқада көбейткіштер ойлап табылды. Олар кеңінен қолданысты әр түрлі компьютерлер үшін операциялық блоктарды құруда тапты.

Көпразрядты сандарды көбейту, есептеу талапына сай келетін O (n^2) қадамнан (биттік операция) тез жұмыс жасайтын әдістер қажет болды, Карацуба әдісі криптографияда кеңінен қолданыс тапты [4], күрделілігі

O ($n^{\log_2 3}$) тең, Тоом-Кук алгоритімі [5] қиындығы O ($n2^{\sqrt{2\log_2 n}}$), Шенхаге-Шрассен алгоритімі [6] екі n-разрядты сандарды O($n\log n \log n$) биттік операцияға көбейтуге мүмкіндік береді.

В. М. Глушков атындағы Кибернетика Институтында бағдарламалар кешені әзірленген, сол жерде ерекше назар жеделдетіп көбейту операцияларына аударды, өйткені ассиметриялық криптожүйелерде негізгі

жүктеме соған түседі [7]. Кешенді бағдарламалар әзірленді, сандарды көбейту жоғарыда аталған алгоритімдер бойынша көп ядролы компьютерлерде [8], онда есептеулер процестері қатар жүреді.

Сандарды модульге келтіру операцияларына келсек, онда бұл операция ең үлкен болып табылады, себебі ол көпразрядты сандардың модулге

бөлінгенен қалдығын алуың білдіреді, ал бөлу операциясы – арифметикалық операциялар ішіндегі ең күрделісі.

Бөлу операциясы шифрлау және дешифрлау процесінде деректер бірнеше рет көбейтумен қайталанады, кейін өте үлкен сан (a^x) модульге бөлінеді, модульге дәрежесің шығаруды жеделдету үшін көп қадамды дәйекті көбейту келтіре отырып, модуль бойынша әр қадам сайын жаңа туындылар жазып отырады. Сондықтан криптожүйелердің жаңа құралдарын жедел модуль бойынша келтіру, әзірлеу және тез істейтін аппараттық шешім бойынша міндеттерді орындау үшін модуль бойынша келтіру өзекті мәселе болып табылады.

Қазіргі қалдықтарды қалыптастыру тәсілдерін болуы үш топқа бөлуге болады:

Бірінші топқа мыналар жатады: қалдықты модуль бойынша қалыптастыру, есептеу арқылы ішінара қалдықтары және кейіннен оларды модуль бойынша жинақтау [10].

Мұндай тәсіл қалыптастыру үшін 2n разрядтық санан қалдық n разрядтық модуль бойынша n-1 қалыптастырғыш ішінара қалдықтары мен модуль бойынша сонша сумматорлар қажет.

Екінші топқа жататындар модуль бойынша қалдықты қалыптастыру тәсілі [11], онда қалдық қалыптастыру үшін қабылдайтын санан параллельді модульдер еселілері есептеледі. Бұл үшін алдымен әр түрлі блоктарда модуліне $P \times i$ (мұнда $i = 1, 2, 3, \ldots, n$) еселі құрылады, содан кейін модуль Р мен модульдер 2р, 3р, ..., nP n сумматорын пайдалана отырып қабылдайтын сандар бір уақытта есептеледі. Мұндай қалыптастырғышта сумматорлар саның анықтау үшін А және Р қалдықтарының арақатынасының байланысымен анықталады.

Сонымен, үшінші топқа қалдығын бөлу жолымен қабылдайтын санының Р модулінен қалыптастырғыш [12]. Бұл ретте 2n разрядты сан А бөлінеді n- разрядты модулі Р бөлінеді де n-разрядты R– қалдығы қалыптасады.

Бүтін сандарды бөлудегі белгілі алгоритмдер: қалдық қалпына келтіріп бөлу және қалдықты қалпына келтірмей бөлу.

Қосымша қосу операцияларын қалдықты қалпына келтіру үшін орындау қажеттілігі болғансон бұл алгоритімнің кемшілігі болып табылады

2.1 Көбейткіштің кіші разрядтарын талдай отырып, тізбекті әрекет модулі бойынша сандарды көбейту.

Сандарды тізбектей әсер ету Модулі бойынша көбейтудің функционалдық сұлбасы 2.1 суретте келтірілген. Көбейткіштің құрамына келесілер кіреді: операцияларды бастағанға дейін В саны (көбейткіш) сақталатын РгВ регистрі, мұнда Р модулі сақталатын РгР регистрі; ішінара қалдықтарды жинақтаушы (НФЧО); СММ модулі бойынша жинақтаушы сумматор (НСММ); триггер Т; СчТИ тактілік импульстерінің есептеуіші; кідіру желілері Л.З.1, Л.З.2, Л.З.3; Логикалық схемалар блогы $И_1 \div И_{10}$ және ИЛИ.

2.2 суретінде СМ екілік сумматордан, MS мультиплексорынан және РгЧО ішінара қалдықтарының регистрінен тұратын НФЧО құрылымы келтірілген.

Сумматордың сол жақ кіреберісіне алдыңғы бөліктелген қалдық(r_{i-1}) үлкен разрядқа қарай бір разрядқа жылжи отырып беріледі$(2 * r_{i-1})$. Сумматордың екінші кіруіне $\overline{P}$ модулінің кері кодының разрядтары , ал сумматордың кіші разрядына модульдің кері кодын қосымша кодына ауыстыратын жалғыз сигнал +1 беріледі.

Қосымша кодта $2 * r_{i-1}$ мен $P -$ ны қосу кезінде, егер $2 * r_{i-1} > P$ болса, онда сумматордың үлкен разрядынан П = 1 берілісі туындап, MS мультиплексордың шығысына $r_i = 2r_{i-1} - P$ айырмашылығының берілуін басқарады. Егер $2r_{i-1} < P$ болса, онда MS мултиплексордың шығысна $2r_{i-1}$ кодының берілісін басқаратын, теріс белгісі бар (Зн = 1) $2r_{i-1} - P$ айырмашылығын аламыз және операция нәтижесі РгЧО регистрінде сақталады.

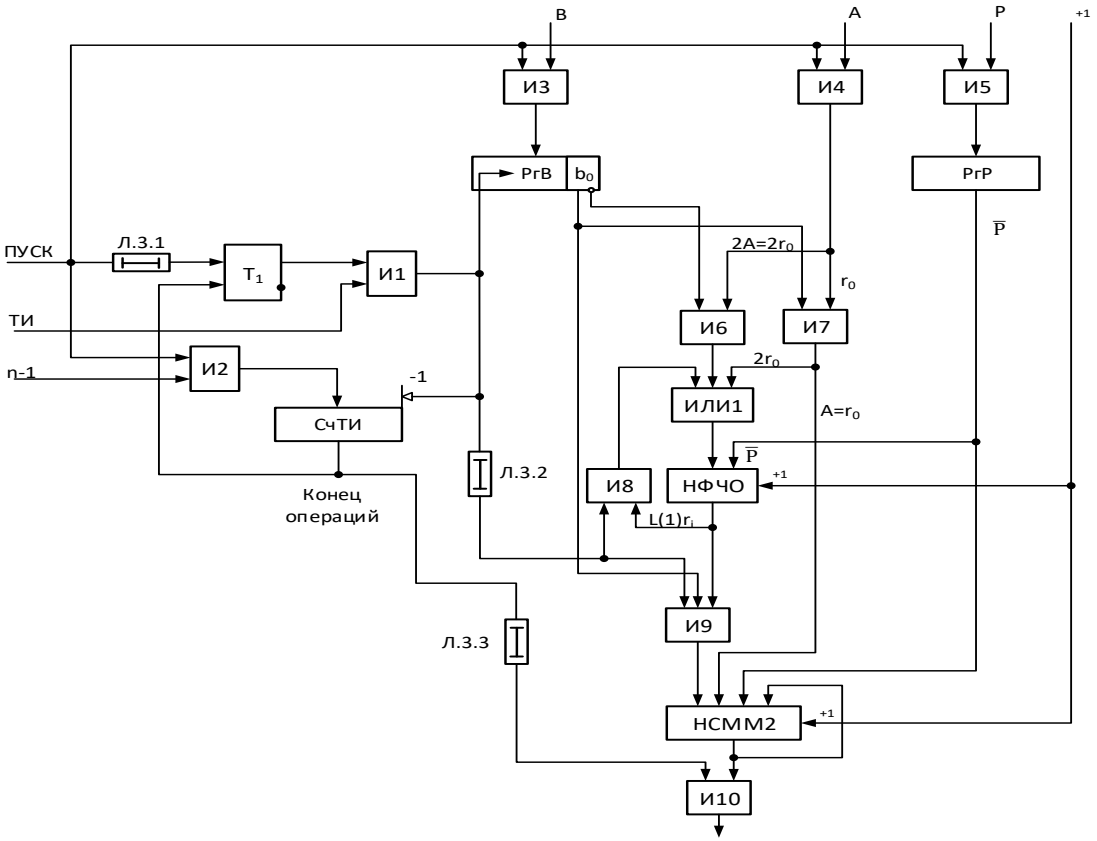
Модуль бойынша жинақталатын сумматордың құрылымы (НСММ) 2.3 суретте келтірілген. НСММ НФЧО-дан тек (R_{i-1}) алдыңғы аралық қалдықтардан r_i ағымдағы ішінара қалдығы жинақталатын СМ сумматормен ғана ерекшеленеді. Содан кейін бұл сумма р модулі бойынша келтіріледі, яғни $R_i = (r_i + R_{i-1}) mod\ P$ және R_i мәні РгR аралық қалдық регистрінде есте қалады.

Көбейткіштің жұмысын қарастырсақ. «ПУСК» сигналына сәйкес В және Р операндалары И3 және И5 логикалық тізбектер блоктары арқылы сәйкесінше РгВ және РгР регистрлеріне қабылданады. Бұл жағдайда В - b_0 көбейткішінің төмен ретті биті РгВ регистрінің төмен ретті битінде белгіленеді. И5 тізбегінің блогының шығуынан көбейткіштің А биттері И7 тізбегі блогының кірістеріне және үлкен бит бағыты бойынша бір битке жылжи отырып И6 тізбектер блогының кірістеріне ауысады.

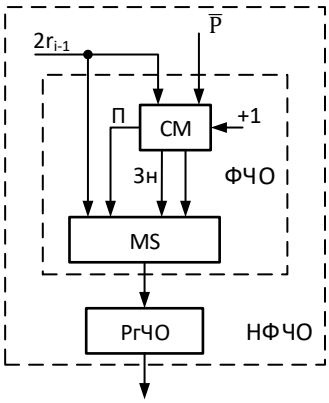
b_0 биттік мәні И7 тізбектер блогының кірістеріне де жеткізіледі, ал оның кері мәні $\overline{b_0}$ И6 тізбектер блогының кірісіне беріледі. «ПУСК» сигналы сонымен қатар жылжу санын - N-1 (мұндағы N – көбейкіштің разрядтығы) СчТИ -нің тактілік импульстік есептегішіне жазады.

В көбейткішін РгВ регистріне жазғаннан кейін, егер $b_0 = 1$ болса, онда көбейтінді разрядтары А = r_0 И7 блогының тізбегі арқылы РгR НСММ аралық қалдық регистріне енгізіледі. Сонымен қатар, И7 және ИЛИ1 тізбектері арқылы үлкен разряд бағыты бойынша бір битке ығысу кезінде А = r_0 мәні НФЧО кірістеріне беріліп, онда $r_1 = 2r_0 mod\ P = 2r_0 + \overline{P} + 1$ қалптасады. r_1 РгЧО НФЧО регистрінде сақталады.

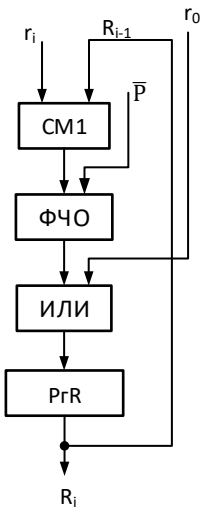
ТИ1 импульсімен бір мезетте РгЧО НФЧО шығысынан И8 және ИЛИ1 блок схемалары арқылы еі еселенген $2r_1$ мәні НФЧО кірісіне беріліп, онда $r_2 = 2r_1 mod\ P$ қалыптасады және и r_2 РгЧО НФЧО регистрінде сақталады. r_2 РгЧО регистрінде және R_1 РгR регистрінде пайда болған кезде, көбейткіштің кірісіне ТИ2 тактілік сигналы беріледі, оның көмегімен РгВ регистрінің мәні бір битке оңға ауысады, СчТИ есептегішінің мәні бір мәнге азаяды, РгЧО-да r_3 ішінара қалдығы және РгR-де R_2 аралық қалдығы қалыптасады, n-1-ші тактілік импульсі берілгеннен кейін «Жұмыстың аяқталуы» сигналы пайда болады, ол Л.З.3-ке кешіктіріліп, нәтиже R_{n-1} тізбектің басқару кірісіне И10-ға беріледі және операция нәтижесі шығысқа беріледі. «Жұмыстың аяқталуы» сигналы Т триггерін бастапқы нөлдік күйге айналдырады және И1 тізбегінен құрылғыға келесі тактілік сигналдың өтуіне жол бермейді. Тактілік сигналдарының параметрлері НСММ сигналдарының кідірісімен анықталады.



Сурет 2.1. Тізбекті әрекет модулі бойынша сандарды көбейтудің функционалдық сұлбасы



Сурет 2.2. НФЧО құрылымы



Сурет 2.3. НСММ құрылымы

2.2 Көбейткіштің жоғарғы разрядтарын талдай отырып, тізбекті әрекет модулі бойынша сандарды көбейту

Сандарды модуль бойынша көбейту N қадамға орындалады, мұнда N – көбейткіштің разрядтылығы. Әрбір қадамда R_i аралық қалдығы қалыптасады. Бірінші кезеңде көбейетін А логикалық түрде b_i үлкен разрядынан бастап көбейткіштің b_i битіне көбейтіледі. А туындысының екінші кезеңінде $R_{(i-1)}$ аралық қалдығының жоғарғы разрядына қарай бір разрядқа жылжытумен жинақталады және $c_i=a*b_i+2R_{(i-1)}$ формуласы есептеледі. Сонда $r_i=(2R_{(i-1)})+A*b_i)\text{mod}P$, мұнда b_i {0,1} және A < P және B < P.

2.4-суретте модуль бойынша көбейтудің функционалдық сұлбасы келтірілген. Көбейту сұлбасы РгА, РГР, РгР, РгР және РГР регистрлерін, екілік сумматор СМ және аралық қалдықтарды қалыптастырушы (ФПО), тактілік импульстерді есептеуіш – триггер Т, кідіру сызығы Л.З.1÷Л.З.3, схемалар блоктары И1÷И8 қамтиды.

РгА регистрлері үлкен разрядқа қарай бір разрядқа жылжу тізбегі бар РГ регистрі көбейетін А сақтау үшін қызмет етеді-көбейткіш в разрядтарын сақтау үшін, ЕСЖ регистрі - р Модулінің разрядтарын сақтау үшін, ЕСЖ регистрі – r_i аралық қалдықтарды сақтау үшін. ФПО аралық қалдықты қалыптастырғышта $r_i=(2r_{(i-1)}+A*b_i)\text{mod}P$ операциясы орындалады және операция нәтижесі ЕСЖ тіркелімінде есте сақталады.

C_i мәні $C_i>2P$ болуы мүмкін болғандықтан, C_i модулі бойынша ФПО кірісіне келтіру үшін Р және 2р қатар , және +1 деңгей беру қажет, бұл $C_i + \bar{P} + 1$ және $C + 2\bar{P} + 1$ операциясын орындай отырып, қосымша кодта қосу операциясымен алмастыруға мүмкіндік береді. СМ сумматор кірісінде схемалар блогы арқылы И7 РгR ішіндегісін бір разрядқа жоғары разрядқа жылжыта отырып беріледі. РгR тіркелімінің шығуы И8 ақпараттық кірулермен байланысты, оның шығуы арқылы "операциялардың аяқталуы" сигналы бойынша нәтиже құрылғының шығуына беріледі.

Модуль бойынша көбейту құрылғысы келесідей жұмыс істейді. "Іске қосу" сигналы бойынша көбейткіш А, көбейткіш В және Р модулі И3, И4, И5 схемалары арқылы РгА, РгВ және РгР регистрлеріне сәйкес қабылданады. "Іске қосу" сигналының әрекет ету кезінде $b_{N-1}=1$ бит мәні кезінде көбейткіш А мәні И6 схемалар блогы арқылы сумматордың оң жақтағы кіруіне СМ беріледі. Бұл ретте $C_0 = A$ А < Р болғандықтан, онда ФПО шығуында R_i=А болады, ол РгR тіркелімінде есте қалады. Содан кейін ұсталған Л.З.1сигнал "іске қосу" Т триггерінің жеке кіруіне келіп, оны жеке күйге ауыстырады. Триггердің жеке жағдайы ТИ1 бірінші тактілік импульсінен өтуге рұқсат береді. Бұл ретте ТИ1 СчТИ көрсеткішінен бірлікті шегереді және РгВ регистрінің ішіндегісін бір разрядқа жоғары разрядқа жылжытуды жүзеге асырады. РгВ ти1 регистрін жылжыту кезінде Л.З.2 кідіртіледі. Осыдан кейін ТИ1 тактілік импульсімен жоғары разрядқа қарай жылжыған R_{i-1} РгВ ішіндегіні и7 схемасы арқылы сумматордың сол жақ кіруіне беріледі, ал оның оң жақ кірулеріне үлкен разрядты РгВ (бит b_{N-2}) мәнімен И6 схемалар блогының шығуларынан көбейтудің нәтижесі беріледі. $b_{n-2}=1$ кезінде көбейткіш А мәні $2R_0$-ден жинақталады және шығуда СМ мәні қалыптасады $C_1 = 2R_0 + A$, ол ФПО кіруіне беріледі және ФПО шығуында $R_1 = C_1 mod P$. Осы сәтте И1 сұлбасының шығуында ТИ2 тактілік импульс түседі, ол Ржв тіркелімінің мазмұнын бір разрядқа солға жылжытады және СчТИ мазмұнынан бірлікті шегереді. ТИ2-де ұсталған Л.З.2 ТИ2 сызбалар блогы арқылы $2R_1$ мәнін сумматордың сол жақ кіруіне СМ береді, ал оның оң жақ кіруіне $A \cdot b_{n-3}$ көбейту нәтижесінің И6 шығысынан беріледі. Шығыста СМ $C_2 = 2R_2 + A \cdot b_{n-3}$ мәні қалыптасады, ол Р модулі бойынша R_2 қалыптастыра отырып келтіріледі. Сол сияқты $R_3, R_4, .., R_{N-1}$. аралық қалдықтар қалыптасады.

ТИ N-1 тактикалық импульсінен кейін "операциялардың аяқталуы" сигналын шығарады, ол триггердің нөлдік кіруіне беріледі және оны нөлдік күйге түсіреді. Триггердің нөлдік күйі құрылғы схемасына келесі ТИ өтуін тежейді.

Соңғы ТИ көмегімен РгВ регистрінің мазмұны солға бір битке ауыстырылады және В – b_0 коэффициентінің ең аз биті ең жоғары биттік РгВ В-ге жазылады, ол И6 тізбегінде А мультипликаторымен көбейтіледі, $b_0 = 1$ А болғанда, ол $2R_{N-1}$ және C_{N-1} мәні қосылады, ол Р модулі және қорытынды қалдық $R_{N-1} = R$ түзіледі. Нәтижені PrR регистрінен И8 тізбегі арқылы шығару З-ші уақытқа кешіктірілген ТИ N-1 арқылы жүзеге асырылады. Бұл кідірістің мәні R_{N-1} нәтижесінің қалыптасу уақытымен анықталады.

2.5-суретте аралық қалдықты (ФПО) қалыптастырушының функционалдық сұлбасы келтірілген. Құрастырушы екі екілік СМ2 СМ1 сумматорынан, И1-И3 үш блоктан және ИЛИ схема блогынан. Келтірілген санның мәні $C_i = A * b_i + 2R_{i-1}$ Р Модулінің инверсиялық мәні СМ1 сумматордың оң жақ кірісіне беріледі. СМ2 оң жақ кіріске Р Модулінің кері коды беріледі, ол бір разрядқа жоғары разрядқа, яғни 2Р . СМ1 және СМ2 кіші разрядтарына +1 бірлі-жарым деңгей беріледі, онда модульдің кері кодтары

қосымша кодтарға ауыстырылады, бұл азайту операциясын қосу операциясымен ауыстыруға мүмкіндік береді.

$R_i = C_i mod P$ қалдығының мәнін C_i, 2р және Р мәндерінің арақатынасын талдау жолымен анықтауға болады.

СМ2 сумматорындағы R_i мәнін есептеу үшін C_i – 2Р операциясы орындалады, бұл қосымша $C_i - 2\overline{P} + 1$ кодында қосу операциясына сәйкес келеді. СМ1 сумматорда C_i – Р операциясы орындалады, бұл қосымша $C_i - \overline{P} + 1$ кодында қосу операциясына сәйкес келеді. $C_i < P$ кезінде R_i мәні C_i мәніне сәйкес келеді.

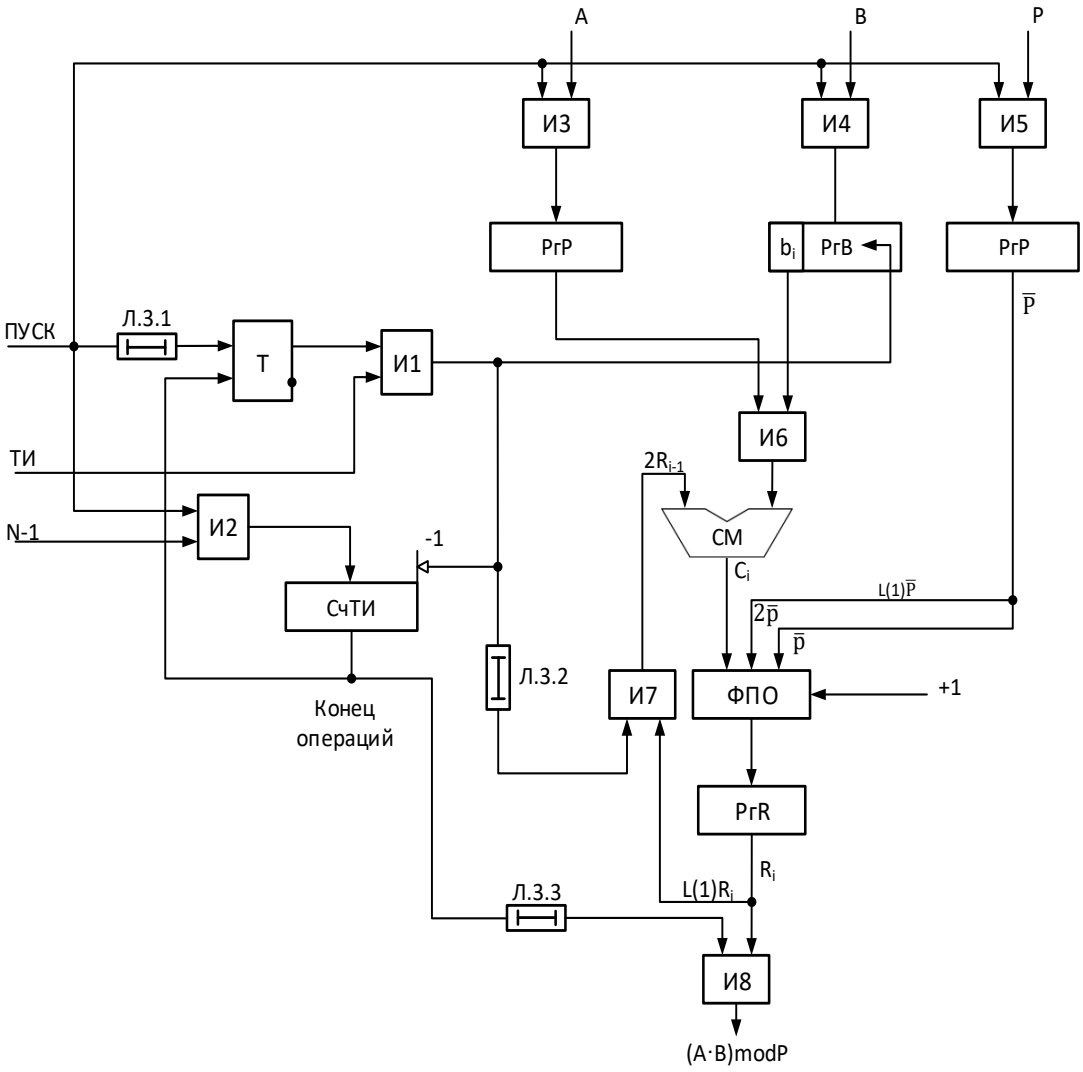
СМ1 және СМ2 сумматорларында қосу операциясы бір уақытта орындалады және бір уақытта СМ1 және СМ2 сумматорларының тиісті шығыстарында П1 және П2 белгілік разрядтарынан және Зн1 және Зн2 белгілерінен ауысу іске асырылады.

С. 3 кестесінде П2, П және Зн2, Зн1 белгілерінің тасымалдау мәніне байланысты R ең аз оң қалдығының қалыптасу шарттары келтірілген.

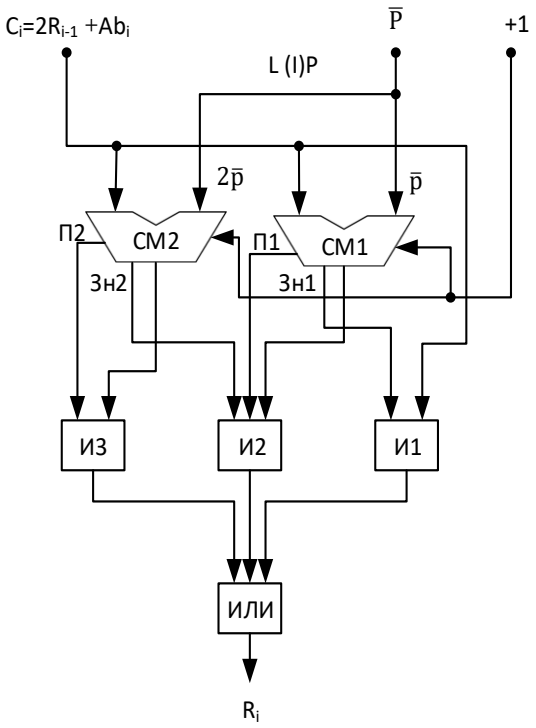
Бұл кестеде П2=П1=1 және Зн2=Зн1=0 кезінде r_i ең кіші оң қалдық ретінде сумматор шығысынан СМ2 C_i-2p айырмашылығын анықтаймыз, оның мәні П2=1 сигналымен И3 схемасының шығысына берілетін. Бір уақытта Зн2=Зн1=0 сигналдарымен И1, И2 және И3 схемаларының шығуынан кодты беру бұғатталады.

П2=0 және П1=1 мәндері кезінде қалдық сумматордың шығуында қалыптасады СМ1. Бұл ретте Зн1=0 C_i мәндерінің И1 схемасының шығуында өтуін тежейді.

П2=П1 = 0 кезінде осы сигналдармен СМ2 және СМ1 шығулары бұғатталады және Зн 1=1 сигналымен C_i мәні схемамен және 1 көбейтгіш шығысына беріледі.



Сурет 2.4. Көбейткіштің үлкен разрядын талдай отырып, көбейтетін тізбекті әрекет модулі бойынша көбейткіштің құрылымдық сұлбасы.

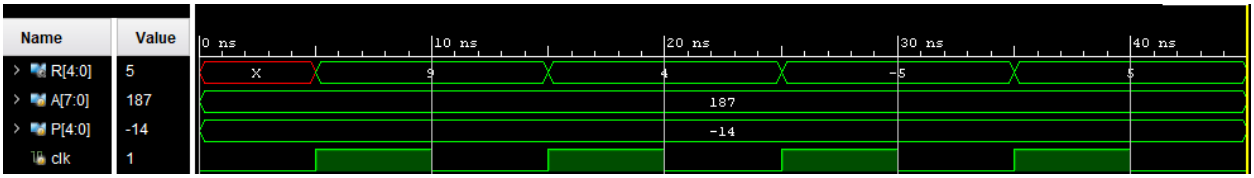


Сурет 2.5. Аралық қалдықты қалыптастырушының функционалдық схемасы

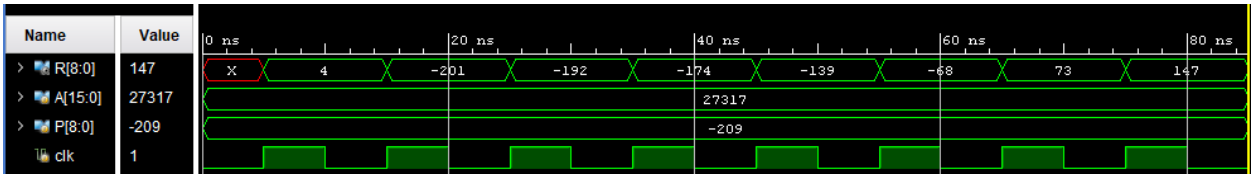
3.Есептеулер

3.1-суретте $A_{a7\div a0} = 187_{10} = 10111011_2$ 8 разрядты санын 4 разрядты $P = 14_{10} = 1110_2$ модулі бойынша келтіру құрылғысының уақытша жұмыс диаграммасы келтірілген. А санының үлкен разрядтары $r_0 = 11_{10} = 1011_2$.
С. 6 суретте ТИ1 тактілік импульстің алдыңғы фронты бойынша А регистрінің мазмұны солға бір разрядқа жылжиды және регистрде $2r_0 + a_3) = 23$ қалыптасады$r_2 = 18 - P = 4$ ішінара қалдық қалыптасады, ол А тіркеліміне беріледі. ТИ2 берілгеннен кейін А тіркелімінің мазмұны солға бір разрядқа жылжытылады және тіркелімде $(2r_1 + a_2) = 18$ қалыптасады. Келесі тактілік импульспен ТИ3 А тіркелімінің мазмұны солға қарай бір разрядқа жылжиды және тіркелімде $2r_2 + a_1) = 9$ қалыптасады, ішінара қалдық $r_3 = 9 - P = -5$ қалыптасады, бұл ретте r_3 а тіркеліміне беру бұғатталады және онда ескі қалдық сақталады (9). Соңғы тактілік импульспен ТИ4 А регистрінің мазмұны сол жаққа бір разрядқа ауысады және регистрде $(2r_3 + a_0) = 19$ қалыптасады, $r_4 = R = 19 - P = 5$ ішінара қалдық қалады.

3.2 суретте 16 разрядты $A = 27317_{10}$ санын 8 разрядты $P = 209_{10}$ модуліне келтірудің ұқсас диаграммасы берілген. Тактілік сигналдар ТИ1-ТИ8 Арқылы сәйкесінше $r_1 = 4$, $r_2 = -201$, $r_3 = -192$, $r_4 = -174$, $r_5 = -139$, $r_6 = -68$, $r_7 = 73$ и $r_8 =$ 147 – 209 = -62 қалыптасады. Осылайша R = 27317 mod 209 = 147.



Сурет 3.1. 8 биттік сан үшін алгоритм жұмысының диаграммасы



Сурет 3.2. 16 биттік сан үшін алгоритм жұмысының диаграммасы

3.1 кестесі. А және В сандарының көбейтіндісін Р модулі бойынша есептеу

ТИ	b_i	НФЧО	НСММ
ПУСК	$b_0 = 0$ $b_1 = 1$	$r_1 = 2r_0 mod P$= 50-26=24	$R_0 = 0$ $R_1 = (R_0 + r_1)$mod26=24
ТИ1	$b_2 = 1$	$r_2 = 2r_1 mod P$=	$R_2 = (R_1 + r_2)$ mod P

		=48-26=22	=24+22=46 mod 26 = 20
ТИ2	$b_3 = 0$	$r_3 = 2r_2 mod P$= =44-26-18	$R_3 = (R_2 + 0)$ mod P= 20
ТИ3	$b_4 = 1$	$r_4 = 2R_3 mod P$= 36-26=10	$R_4 = (R_3 + r_4)$ mod P =(20+10)mod 26 = 4

Тексереміз $R = (A \cdot B) mod P = (25 \cdot 22) mod\ 26 = 550\ mod\ 26 = 4$.

3.2 кестесі. R қалдығының қалыптасу шарты.

Анализ жасау шарты	**R есептелуі**
C_i< P	C_i
P<C_i<2P	3Х – P C_i – P
2P≤C_i	3Х – 2P C_i – 2P

3.3 кестесі. СМ2, СМ1 сумматорларының шығысындағы ең кішкентай қалдық қалыптасуының шарты

п/п	П2	Зн2	П1	Зн1	Сумматорлардың шығысы		3Х
					СМ2	СМ1	
1	1	0	1	0	R_i	-	-
2	0	1	1	0	-	R_i	-
3	0	1	0	1	-	-	R_i

3.4 кестесі. $R = (75 * 46) mod 143$ есептелуі

1	$b_5 = 1$	ПУСК	$C_0 = 0 + A = 75$	75mod143=75 75mod286=75 R_0 =75
2	$b_4 = 0$	ТИ1	$C_1 = 2r_0 + A = 75 * 2 = 150$	150mod143=7 150mod286=150 R_1 =7
3	$b_3 = 1$	ТИ2	$C_2 = 2r_1 + A = 14 + 75 = 89$	89mod143=89 89mod286=89 R_2 =89

4	$b_2 = 1$	ТИ3	$C_3 = 2r_2 + A = 89 * 2 + 75 = 253$	253mod143=110 253mod286=253 R_3 =110
5	$b_1 = 1$	ТИ4	$C_4 = 2r_3 + A = 220 + 75 = 295$	295mod143=152 295mod286=9 R_4 =9
6	$b_0 = 0$	ТИ5	$C_5 = 2r_4 + 0 = 18$	18mod143=18 18mod286=18 $R_5 = R$ =18

Тексереміз: (75*46)mod143=3450mod143=18

4 Өмір-тіршілік қауіпсіздігі бөлімі

4.1 Еңбек жағдайларын талдау

Дипломдық жобаның бұл бөлімінде "Ақпаратты криптографиялық қорғау процесін жылдамдататын құрылғы құрастырудың" өндірістік тәуекелдерді зерттеу қарастырылады. Қалыпты еңбек жағдайларын анықтауға, сонымен қатар адамның денсаулығы мен өміріне жұмыс ортасында зиян келтіретін факторларды анықтауға бағытталған шаралар кешені.

Ақпараттың криптографиялық қауіпсіздігін жылдамдатуға арналған аппаратық-бағдарламалық құрылғы арнайы компьютер көмегімен жұмыс жасайды. Қарастырылып отырған бөлмеде бір қызметкер жұмыс істейді және оған бір компьютер орнатылған.

Бағдарламалық жасақтаманы құру кезінде әзірлеуші компьютермен ұзақ уақыт жұмыс істеуге мәжбүр. Осы бөлімде адамға кері әсер ететін кейбір факторларға тексеру жүргізілді. Санитарлық-эпидемиологиялық нұсқауларға сәйкес қондырғы көздерімен жұмыс істеу жағдайларына қойылатын физикалық факторлар (ДК) әсер ететін адамдарға жеңіл 1б санатта қолайлы микроклиматтық көрсеткіштер мынадай шарттар болып табылады[9]:

- қыста температура 23-21^{o}С, жылдың ыстық мезгілінде 22-24^{o}С, мұндағы ауа ылғалдылығы 40 - 60%;

- жылдың ыстық мезгілінде ауа айналымының жылдамдығы 0,2 м/с, қыста 0,1 м/с.

Зерттеулерге сәйкес, ДК пайдаланушылардың өздерін нашар сезіну себептерінің бірі монитор экранындағы кескіннің жарықтылығынан пульсациялану болып табылады. Жарықтандырудың пульсациясы жалпақ монитор жарықтану жұмысының ерекшелігіне байланысты. Қазіргі уақытта бұл параметр қалыпқа келтірілмеген, бірақ оған жалпы және жергілікті жарықтандырудың пульсациясы әсер етеді.

Компьютерде жұмысты ұйымдастыру шарттары:

- жұмыс бөлмесінде табиғи және жасанды жарықтандырудың болуы;

- бөлмені кондиционерлеу жүйелерімен жабдықталуы; бөлме сағат сайын желдетіледі;

- күн сәулесінің тікелей түсуінен аулақ болу үшін перделерден немесе жалюздерден пайдалану;

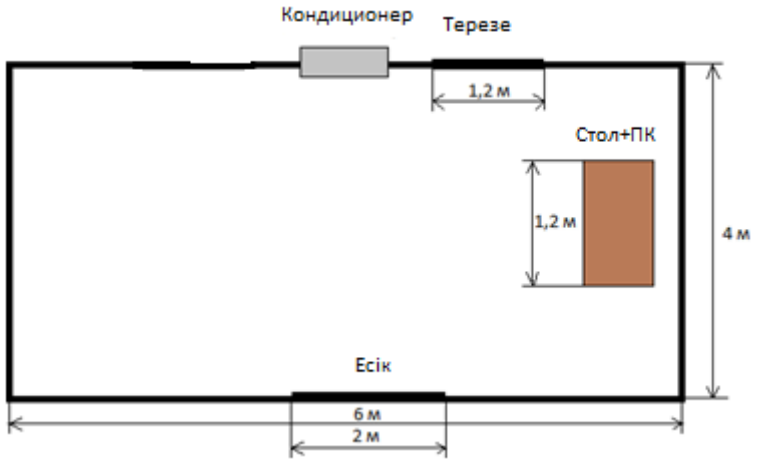
- біркелкі жасанды жарықтандыру.

4.1.1 Жұмыс орнының сипаттамасы

Кеңсені жобалау және құру кезінде ҚР ҚНжЕ 3.02-04-2009 [14] ережелеріне сүйене отырып жасалған.

Жұмыс бөлмесі бір жұмыс орнына жабдықталған. Кеңсе Ауезова көшесіндегі Nurikon бизнес-орталығының, 6 қабатында орналасқан. Кеңсенің тезерелері ғимараттың кері жағында орналасқандықтан әр түрлі шу көздері жұмыс барысына әсер ете алмайды.

Ғимарат жоспары 4.1 суретте көрсетілген.



4.1 сурет – Ғимарат жоспары

Жұмыс орнының мынадай параметрлері бар:

а) сегіз қабатты ғимараттың алтыншы қабатында орналасқан;

б) ұмыс орнының (бөлменің) өлшемдері: ұзындығы 6 м, ені 4 м, биіктігі 3 м;

в) жарық өткізетін материалдың түрі – беттік шыны, қос;

д) күннен қорғайтын құрылғылар-реттелетін жалюздер мен перделер;

е) 1,5*1,2 өлшемдегі екі терезе;

ж) қабырғалардың ішкі әрлеуі-ашық;

3) жұмыстың көру жағдайлары бойынша бөлме жеңіл жұмыс санатына жатады (жеңіл физикалық, Іа санаты, жұмыс отырып жүргізіледі және физикалық кернеуді талап етпейді);

и) жасанды жарықтандыру - екі люминесцентті шамдары бар 2 шам.

к) жұмыста пайдаланылатын жабдықтың сипаттамасы:

л) Intel (R) Core 2 Duo CPU E8400 @ 3.0 GHz 3.0 GHz, 4 ГБ RAM / HDD 1000 Gb;

м) Samsung SyncMaster 932 BF мониторы;

н) электр қорегі: айнымалы кернеуі 220-250 В, жиілігі 50 Гц., қуаты 400 Вт;

о) 2 шам, 4 люминесцентті шамдар;

п) электр қорегі: айнымалы кернеуі 220-250 В, жиілігі 50 Гц, шамның қуаты 2х28 Вт.

4.1.2 Электр қауіпсіздігі

Қоғамдық ғимараттардың электротехникалық құрылғылары Қазақстан Республикасының электр қондырғыларын орнату ережесіне, ҚР ҚНжЕ 2.04-01-2001 [14] талаптарына сәйкес жобаланады.

Электр қауіпсіздігі — адамдарды электр тогының, электр доғасының, электрлі магнит өрісінің және статикалық электрдің зиянды және қауіпті

әсерінен қорғанысын қамтамасыз ететін ұйымдастыру-техникалық шаралардың және құралдардың жүйесі.

Жергілікті электр жарақаттары электр тогының дене ұлпалары мен мүшелерін зақымауы: күюлер, электр таңбалары, терінің электр металдануы және электроофтальмия (көздің қарығуы) болып табылады.

Токтың келесі шектік мәндерін бөліп атауға болады:

− токты сезу шегі –ең аз сезілетін ток (0,5 -1,5мА);

− босатпайтын ток шегі –адам өз бетімен бұлшық еттері электродтармен қамтылған әрекеттен босана алмайтын ең аз ток мөлшері (6-10мА). Бұдан аз токтар босататын болып есептеледі;

− қаза ететін (100 мА және одан астам) ток.

Изоляцияның бүлінуінің әсерінен кернеу астында қалған металды құрылымдарды немесе электр құрылғылардың корпусын ұстау нәтижесінде алынатын электрлік жарақаттарды болдырмау және аппаратураларды қорғау үшін қорғанысты жерлендіру орналастырылады. Ол электр қондырғылардың метал бөліктерін жермен әдейі жалғау арқылы жасалынады.

Жерлендіру құрылғыларын (ЖҚ) жобалау кезінде адамның электр тоғымен жарақат алу ықтималдылығы ескеріледі. Алайда, бірде-бір салада және жалпы өмірде адамдардың толық қауіпсіздігін қамтамасыз ете алмайды.

Сондықтан, ЖҚ-ның аймағында қауіпсіздікті қамтамасыз ету мәселесін адам электр тоғымен жарақат алу қаупі жағдайының болу ықтималдылығын азайтады.

Тиімді жерлендірген желілерде электр қауіпсіздігі қамтамасыз етілген деп жерлендіргіштегі φж потенциалы 10 кВ-тан аспайтын, ал жерлендіргіштің нәтижелі кедергісі жылдың кез-келген мерзімінде 0,5 Ом-нан аспайтын болып саналады.

4.1.3 Өрт қауіпсіздігі

Өрт қауіпсіздігі персоналдың жұмыс ортасының қауіпсіздігін қамтамасыз етудегі ҚР ҚНжЕ 2.02-05-2009 [15] құрылыс проект нормасымен анықталады. Дұрыс жасалған құжат электрлік құрылғылармен жұмыс бөлмесінде сипаты дұрыс емес жағдайлардан туындайтын қауіпті жағдайларды болдырмауға көмектеседі.

Өрт қауіпсіздігі өрттің алдын алу жүйесімен және өрттен қорғау жүйесімен қамтамасыз етілді.

Жұмыс орнындағы өрттер аса қауіпті, себебі үлкен материалдық шығындармен байланысты. Жұмыс орнының ерекшелігі - бөлменің шағын аудандары. Өрт жанғыш заттардың, тотығу мен тұтану көздерінің өзара әрекеттесуі кезінде туындайды. Жұмыс орнында өрт пайда болу үшін қажетті барлық үш негізгі фактор бар.

Жанғыш компоненттерге бөлмені әрлеуге арналған материалдар, қалқалар, есіктер, едендер, кабельдерді оқшаулау және т. б. жатады.

Өртке қарсы қорғаныс - бұл адамдардың қауіпсіздігін қамтамасыз етуге, өрттің алдын алуға, оның таралуын шектеуге, сондай-ақ өртті сәтті сөндіру үшін жағдай жасауға бағытталған ұйымдастырушылық және техникалық іс-шаралар кешені.

От алдыру көздері ЭЕМ-нің электрондық схемалары, техникалық қызмет көрсету үшін қолданылатын аспаптар, жануға қабілетті электрмен қоректендіру құрылғылары болып саналады. Сондай-ақ оларды ӨҚ талаптарына сәйкес келмейтін жағдайда сақтау немесе пайдалану.

Қысқа тұйықталу, желінің шектен тыс жүктелуі, үлкен ауысу кедергісі салдарынан болатын өрттердің алдын-алу үшін электр құрылғыларын дұрыс монтаждау, эксплутациялау ережелері сақталынады.

4.1.4 Жұмыс орнының микроклиматы

Жұмыс орнының микроклиматы қамтамасыз етудегі ҚР ҚНжЕ 2.02-05-2009 [14] құрылыстық климатология нормасымен анықталады. 4.1-кестеде тұрғын үй, қоғамдық және әкімшілік-тұрмыстық үй-жайлардың қызмет көрсетілетін аймағындағы температураның, салыстырмалы ылғалдылықтың және ауа қозғалысының жылдамдығының оңтайлы нормалары

Жыл мезгілі	Жұмыс санаты	Ауа температурасы , °С	Ауаның салыстырмалы ылғалдылығы, %	Ауаның қозғалыс жылдамдығы, м/с
Салқын	Жеңіл - 1а Жеңіл – 1б	22-24 21-23	40-60 40-60	0,1 0,1
Жылы	Жеңіл - 1а Жеңіл – 1б	23-25 22-24	40-60 40-60	0,1 0,2

Кеңсенің кеңістігін желдету үшін ғимараттың құрылысы кезінде жазда желдетілетін табиғи терезелер қолданылады. Жылы мезгілде, кеңсе температурасы 4.2 кестеде көрсетілгеннен жоғары болған кезде оңтайлы микроклиматты ұстап тұру үшін кондиционер қолданылады. Кеңседегі қалыпты микроклимат жылдың кез келген уақытында қызметкерлердің әл-ауқатын қамтамасыз етеді, сәйкесінше өнімділік жоғарылайды. Осылайша, бөлмедегі микроклиматты сақтау үшін оны ауа баптағыш жүйесімен жабдықтаған жөн.

Кондиционер жұмыс орнындағы климаттың сақталуын қамтамасыз етеді

4.2 Есептеу бөлімі

4.2.1 Жерлендіру есебі

Есеп әдістемелік нұсқауларымен жүргізілді [18]. Жұмысты электр қондырғыларын техникалық пайдалану ережелеріне сәйкес жүргізеді. Сонымен қатар электр құралдарымен жұмыс істеу кезінде қауіпсіздік техникасы бойынша кіріспе және мерзімді нұсқамалар сақталды, еңбек тәртібін орындалды , жұмыс орнын дұрыс ұйымдастыралды. Жерлендіру шиналары қол жетімді жерлерде орналасқан. Қорғау үшін жабдық пен аспаптардың ток өткізгіш бөліктеріне жанасу оқшаулауды, ток өткізгіш бөліктерінің орналасуы мен қоршауын пайдаланады. Жабдықтың металл бөліктеріне жанасу кезінде кездейсоқ кернеу астында болуы мүмкін электр тогының зақымдануынан қорғау үшін, қондырғы корпусын қорғағыш жерге қосылды.

4.2 кесте- жерлендіруді есептеу үшін бастапқы деректер

Топырақтың меншікті кедергісі, Ом*м	Жерлендіруді диаметрі, d, м	Жерлендіруді ұзындығы, L, м	Жерлендіруді орналасу тереңдігі, h, м	Жерлендіруді арасындағы қашықтық,	Жолақтың ені, b, м
300	0,05	2,0	0,7	6,0	0,02

Бір жерлендірудің кедергісі мына формула бойынша анықталады:

$$R_{тк} = p * (\lg (2 * L / d) + 0,5 * \lg ((2 * 4 * t + L) / (4t * L))) / 2 * п * L \quad (5.1)$$

мұндағы Rтк - жерлендірудің кедергісі;

ρ – топырақтың меншікті кедергісі;

L – жерлендірудің ұзындығы;

t – жерлендірудің орналасу тереңдігі;

d – жерлендірудің диаметрі.

$$Rтк = 300 * (\lg (2 * 3 / 0,05) + 0,5 * \lg ((4 * 2,2 + 3) / (4 * 2,2 * 3))) / 2 * 3,14 * 3 = 15,57 \text{ Ом}.$$

Жерлендірудің саны мына формуламен есептеледі:

$$n = R_{тк} / R_{нк}, \quad (5.2)$$

мұндағы, n - жерлендірудің саны;

Rтк - жерлендірудің кедергісі;

Rнк - нормалар бойынша жерлендірудің кедергісі (4 Ом).

Жерлендірудің арасындағы қашықтық мынадай формула бойынша есептеледі:

$$a = 2 * L \quad (5.3)$$

мұндағы, а - жерлендірудің арақашықтық;

L - жерлендірудің ұзындығы.

$$a = 2 * 3 = 6 \text{ м}$$

Олардың өзара экрандалуын ескере отырып, жерлендірудің саны мынадай формула бойынша анықталады:

$$n_Э = n/\eta_{жс} \qquad (5.4)$$

мұндағы, $n_Э$ - өзара экрандалуын ескергендегі жерлендірудің саны;

n - өзара экрандалуын ескермегендегі жерлендірудің саны;

$\eta_{жс}$ - жерлендіргіштерді өзара экрандалуын ескеретін пайдалану коэффициенті.

$$n_Э = 4/0{,}88 = 5$$

Жерлендірудің өткізгіштерінің ұзындығы мынадай формула бойынша анықталады:

$$Ln = 1{,}05 * a * n_э \qquad (5.5)$$

мұндағы, Ln – жерлендіру өткізгіштердің ұзындығы;

a - жерлендірудің арақашықтығы;

$n_э$ - өзара экрандалуын ескергендегі жерлендірудің саны;

$$Ln = 1{,}05 * 6 * 5 = 31{,}5 \text{ м}$$

Жерлендірудің өткізгішінің кедергісі мынадай формула бойынша болады:

$$R_П = \rho * (lg (2 * Ln / b * t)) / 2 * п * L \qquad (5.6)$$

мұндағы, Rж - жолақтық болаттан жасалған жерлендірудің өткізгішінің кедергісі;

Ln - жерлендірудің өткізгіштердің ұзындығы;

b - жерлендірудің өткізгіш жолағының ені;

t - жерлендірудің орналасу тереңдігі.

$R_Ж = 300 * (lg (2 * 31{,}5 / 0{,}02 * 0{,}7)) / 2{,}5 * 3{,}14 * 2 = 30{,}03$ Ом

Барлық токтың ағуына кедергі жерлендірудің құрылғысының мынадай формула бойынша есептеледі:

$$R_{ЖТ} = R_{ТК} * R_Ж / (R_{ТК} * \eta * n + R_Ж * \eta_{жс} * n) \qquad (5.7)$$

мұндағы Rжт - барлық жерлендірудің токқа ағу кедергісі.

$$R\text{жт} = 30{,}03 * 15{,}57/(5 * 30{,}03 * 0{,}8 + 15{,}57 * 1{,}1) = 3{,}41 \text{ Ом}$$

Жерлендірудің нақты саны мынадай формула бойынша анықтадым:

$$n = R\text{ж} / \eta\text{жс} * R\text{жт} \qquad (5.8)$$

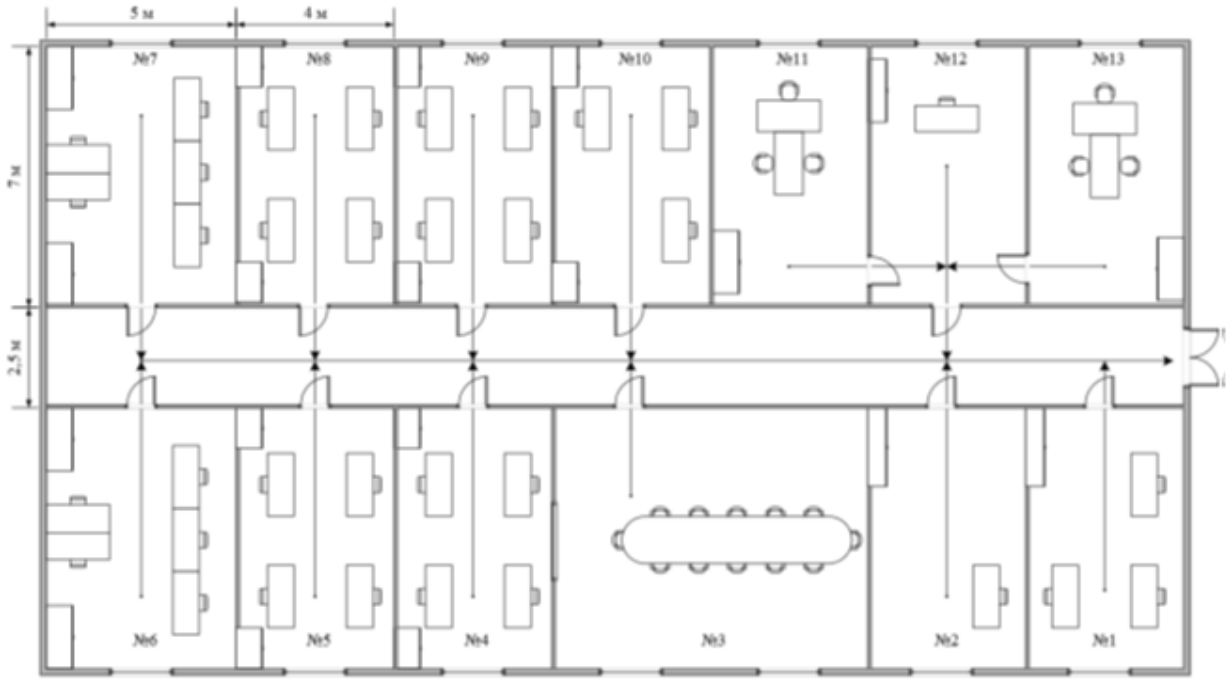
мұндағы, n - жерлендірудің нақты саны.

$$n = 15{,}57 / (0{,}88 * 3{,}41) = 5$$

4.2.2 Эвакуация жолдарын есептеу

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [18]. Адамдарды эвакуациялаудың есептік уақыты ғимараттан соңғы адамның шыққан уақытымен белгіленеді.

Эвакуация процесін модельдеудің алдында ғимараттағы эвакуация жолдарының схемасы беріледі. Эвакуация жолдарының барлығы ұзындығы l және ені d эвакуациялық учаскелерге бөлінеді. Жобаланатын ғимараттар үшін эвакуация жолдарының әрбір бөліктің ұзындығы мен ені жоба бойынша, ал салынған ғимараттар үшін факт бойынша қабылданады. Эвакуациялық учаскелер жазық және еңіс (төмен түсетін баспалдақ, жоғары көтерілетін баспалдақ және пандус) болуы мүмкін. Есік ойығындағы жол ұзындығы нөлге тең деп қабылданады [15].



4.2-сурет – Ғимараттың бірінші қабатының эвакуациялық жолдарының жоспары

Жалпы ғимараттан эвакуациялау уақытын табу үшін эвакуациялау жолын екі учаскеге бөлеміз. Бірінші учаскеде бөлмеден шығу уақытын, екінші учаскеде дәліз бойымен қозғалыс уақытын тауып, бір-біріне қосамыз.

Жалпы ғимараттан эвакуациялау уақыты мынадай формула бойынша анықталады:

$$t = t_1 + t_2 + ... + t_i \tag{4.2}$$

Әр бөлікті жүріп өту уақыты келесі формула бойынша анықталады:

$$t_i = \frac{l_i}{\vartheta_i} \tag{4.3}$$

мұндағы, D – адам ағынының тығыздығы, төмендегі формула бойынша есептеледі:

$$D = N\frac{f}{ld} \tag{4.4}$$

мұндағы, N – адам саны;

l – жолдың ұзындығы;

d – жолдың ені;

f – адамның көлбеу проекциясының орташа ауданы, ол 0,1-қа тең.

Бөлме ішіндегі адам ағынының тығыздығы:

$$D_1 = N_1\frac{f}{l_1 d_1} = 5\cdot\frac{0{,}1}{5\cdot 1{,}5} = 0{,}066 \quad \text{м}^2/\text{м}^2$$

4.3-кесте – Адам ағынының тығыздығы бойынша оның жылдамдығы және қарқындылығы

Адам ағынының тығыздығы D, $\text{м}^2/\text{м}^2$	Көлденең жол		Есіктің ойығы
	Жылдамдық ϑ, м/мин	Қарқындылық q, м/мин	Қарқындылық q, м/мин
0,01	100	1	1
0,05	100	5	5
0,1	80	8	8,7
0,2	60	12	13,4
0,3	47	14,1	16,5
0,4	40	16	18,4
0,5	33	16,5	19,6
0,6	27	16,2	19
0,7	23	16,1	18,5
0,8	19	15,2	17,3
0,9	15	13,5	8,5

4.3-кесте бойынша 0,066 $м^2/м^2$ адам ағынының тығыздығына горизонтальды жолда адам ағынының 100 м/мин-ге тең жылдамдық және 5 м/мин-ге қарқындылық сәйкес келеді [18].

Бөлмеден шығу уақыты:

$$t_i = \frac{l_i}{\vartheta_i} = \frac{5}{100} = 0{,}05 \text{ мин}$$

Есіктер алдында адамдар жиналып, қозғалыс ақырындайды. Кідіру уақыты мынадай формула бойынша анықталады:

$$\Delta t_i = N_{эв} f \left(\frac{1}{q_{ec} d_{ec}} - \frac{1}{q_i d_i} \right) \quad (4.5)$$

$$\Delta t_i = N_{эв} f \left(\frac{1}{q_{ec} d_{ec}} - \frac{1}{q_i d_i} \right) = 5 \cdot 0{,}1 \left(\frac{1}{5 \cdot 1} - \frac{1}{5 \cdot 1{,}5} \right) = 0{,}93 \text{ мин}$$

Дәліз бойымен қозғалатын адам ағынының тығыздығы:

$$D_2 = N_2 \frac{f}{l_2 d_2} = 37 \cdot \frac{0{,}1}{29 \cdot 2{,}5} = 0{,}051 \text{ } м^2/м^2$$

4.3- кесте бойынша ϑ_2=5 м/мин, q_2=5 м/мин.

$$t_2 = \frac{l_2}{\vartheta_2} = \frac{29}{100} = 0{,}29 \text{ мин}$$

Басты есік алдында кідіру уақыты:

$$\Delta t_i = N_{эв} f \left(\frac{1}{q_{ec} d_{ec}} - \frac{1}{q_i d_i} \right) = 37 \cdot 0{,}1 \left(\frac{1}{5 \cdot 2} - \frac{1}{5 \cdot 2{,}5} \right) = 0{,}074 \text{ мин}$$

Жалпы ғимараттан эвакуациялау уақыты:

$$t = 0{,}05 + 0{,}93 + 0{,}29 + 0{,}074 = 1{,}344 \text{ мин}$$

Есептеу нәтижесінде жалпы ғимараттан эвакуациялау уақыты 1,344 мин болатыны анықталды. Бұл эвакуациялауға қажетті 2 мин уақыттан аспайды, демек талап орындалады.

Өмір тіршілік бөлімі бойынша қорытынды

Тіршілік әрекетінің қауіпсіздігі бөлімінде компанияның кеңсесіндегі жұмыс жағдайына талдау жасалды және олардың жағдайын тексеру үшін микроклимат параметрлерін есептеу жүргізілді. Еңбек жағдайларының деңгейі рұқсат етілген деп танылады, есептеулерден алынған мәліметтер өмір қауіпсіздігі стандарттарының талаптарына сәйкес келеді.

Есептеулер нәтижелері бойынша ауа ағынының жылдамдығын L = 145.9 м3 / сағ қамтамасыз ету үшін 1 Samsung HA 85 кондиционері максималды ауа шығыны 195 м3 / сағ, R22 моделін қолдануға болады

Samsung HA 85 R22 моделінің қысқа сипаттамалары
- шатырдың моноблокты өндірістік кондиционері
- номиналды салқындату қуаттылығы, Вт - 23200
- қуаттың номиналды шығыны, Вт - 9400
- ауа шығыны (мин-макс), м3 / сағ - 100-195

5 Тәуекелді бағалау

5.1. Тәуекелдерді талдау және бағалау

Дипломдық жұмыстың осы бөлігінде біз объектіні қорғаудың дамыған жүйесі үшін тәуекелдерді бағалаймыз.

Тәуекелді бағалау - сәйкестендіруді, тәуекелді талдауды және салыстырмалы тәуекелді бағалауды біріктіретін процесс. Тәуекелділік бүкіл ұйым үшін, оның бөлімшелері, жеке жобалары, қызметі немесе нақты қауіпті оқиға үшін бағалануы мүмкін. Сондықтан әр түрлі жағдайларда тәуекелдерді бағалаудың әр түрлі әдістерін қолдануға болады.

Тәуекелді бағалау ықтимал қауіпті оқиғаларды, олардың себептері мен салдарын, олардың туындау ықтималдығын түсінуді және шешім қабылдауды қамтамасыз етеді:

- тиісті іс-қимыл жасау қажеттілігі;
- тәуекелді азайтудың барлық мүмкіндіктерін барынша іске асыру тәсілдері;
- тәуекелді өңдеу қажеттілігі;
- түрлі тәуекел түрлері арасында таңдау;
- тәуекелді өңдеу бойынша іс-қимылдың басымдылығы;
- тәуекелді қолайлы деңгейге дейін төмендетуге мүмкіндік беретін тәуекелді өңдеу стратегиясын таңдау.

Маңызды объектілердің тәуекелдерін есептеу үшін екі фактор бойынша тәуекелді бағалау әдістемесі қолданылды. Бұл әдістеме ISO-27005 стандартының Е қосымшасы негізінде жүргізіледі.

Қарапайым жағдайда екі факторды бағалау қолданылады: оқиғаның ықтималдығы және ықтимал салдардың ауырлығы. Әдетте, оқиға ықтималдығы мен зардаптардың ауырлығы көп болған сайын тәуекел соғұрлым көп деп есептеледі. Жалпы идея формуламен көрсетілуі мүмкін:

Тәуекел = оқиғалар * шығын бағасы

Егер айнымалы сандық шамалар болса-тәуекел-бұл жоғалтудың математикалық күтуін бағалау.

Егер айнымалылар сапалы шамалар болса, онда метрикалық көбейту операциясы анықталмаған. Осылайша, айқын түрде бұл формула пайдаланылмауы тиіс. Сапалы шамаларды пайдалану нұсқасын қарастырайық (ең жиі кездесетін жағдай).

Алдымен шкалалар анықталуы тиіс.

Шкалалардың мәндері нақты анықталуы (сөздік сипаттамасы) және сараптамалық бағалау рәсімдерінің барлық қатысушылары бірдей түсінілуі тиіс.

Таңдалған кестенің негіздемесі қажет. Тәуекел факторларының бірдей үйлесімімен сипатталатын әр түрлі инциденттердің сарапшылар тұрғысынан тәуекелдердің бірдей деңгейі бар екеніне көз жеткізу қажет.

5.1 кесте-қауіптің туындау ықтималдығы шкаласы

Қауіптердің туындау ықтималдығы шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
0 – өте төмен	Шамамен 2-3 рет 10 жылда
1 – төмен	Шамамен бірнеше рет 5 жылда
2 – орташа	Шамамен бірнеше рет 1 жылда
3 – жоғары	Шамамен 1 рет 1 айда
4 – өте жоғары	Шамамен бірнеше рет 1 айда

Содан кейін осы қауіп төнуі мүмкін залалды бағалайды. Алынған мәндерге сүйене отырып, қауіп деңгейі бағаланады.

5.2 кесте-залал шамасының шкаласы

Шығын көлемінің шкаласы	
Мәні	Анықтамасы
0 - өте төмен	бағасы 50 000 тг дейін
1 – төмен	бағасы 200 000 тг дейін
2 – орташа	бағасы 500 000 тг дейін
3 – жоғары	бағасы 1 000 000 тг дейін
4 – өте жоғары	бағасы 1 000 000 тг жоғары

Ақпаратты криптографиялық қорғауды жылдамдататын құрылғыны әзірлеу кезінде біздің пайдаланылатын ресурстарымызды негізге ала отырып, мынадай активтерді бөлді:

- Бастапқы коды;
- Аспаптық құралдар – жобалауды және әзірлеуді немесе конфигурацияны басқару құралдары, кодтар талдағыштары, баптау бағдарламалары, тестілік талдағыштар, датчиктер, генерациялайтын және құрастыратын бағдарламалық құралдар, бағдарламалар кодын оңтайландыру құралдары, кітапханалар жиынтығы;
- Қызметкер;
- Nexys4 - бағдарламаланатын логикалық интегралдық схема.

5.3 кесте – тәуекелдерді бағалаудың қорытынды кестесі

№	Қауіптер	Осалдық	Тәуекелдің ең жоғары деңгейі	Тәуекелді өңдеу жөніндегі шаралар	Тәуекелдің қалдық ...	Күні
1 Бағдарламаның бастапқы коды						
1.1	Бастапқы кодқа осалдықтарды енгізу қаупі	Аспаптық құралдарды пайдалану саясатының болмауы және БҚ конфигурациясын басқару шараларының жеткіліксіздігі	12	Бағдарлама архитектурасының нақтыланған жобасы негізінде бағдарламаны жасау;бағдарламаның бастапқы кодын статистикалық талдау, бағдарламаның бастапқы кодын сараптау, бағдарламаның осалдығын жүйелі түрде іздеу жүргізу	9	
1.2	Бағдарламаның жаңартуларына осалдықтарды енгізу қаупі	Рұқсатсыз өзгерістерді анықтау мүмкіндігінің болмауы	9	Пайдаланушыға жіберу процесінде тұтастықтың бұзылуына байланысты ақпараттың қауіпсіздігіне қауіп-қатерден БҚ қорғауды қамтамасыз ету; бағдарламаның осалдықтарын жүйелі түрде іздестіруді жүргізу; конфигурация элементтерін резервтік көшіру	7	

1.3	Деректер модификациясы	АҚ шабуылдары мен қатерлерінің типтік сценарийлерін ескерілмеуі	4	Қолжетімділікті шектеу, парольдік қорғау; конфигурация элементтерін резервтік көшіру	2	
2 Аспаптық құралдар						
2.1	Температуралық режимнің бұзылуы	Жабдықтың температуралар ауытқуына ұшырауы	2	Реттелетін жұмыс режимі	1	
2.2	Ақпаратты жоғалту	Физикалық қорғаудың , резервтік көшіру рәсімдерінің болмауы	9	Кіруді бақылау жүйелері, қоршау және физикалық оқшаулау, конфигурация элементтерін резервтік көшіру	7	
2.3	Қызмет көрсетуде бас тарту	Алмасу буферінің өзгеруін, толып кетуін барабар емес бақылау	12	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтір	9	
3 Қызметкер						
3.1	Жүйенің ақпараттарына немесе бағдарламаға рұқсатсыз қол жеткізу	БҚ әзірлеу ортасының объектілеріне қолданылатын және сыни ақпаратқа рұқсаты бар тұлғалар шеңберін және әзірлеу ортасының объектілерімен орындалуы мүмкін операцияларды шектеуге бағытталған қол жеткізуді	12	Қолжетімділікті шектеу, парольдік қорғау; басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	8	

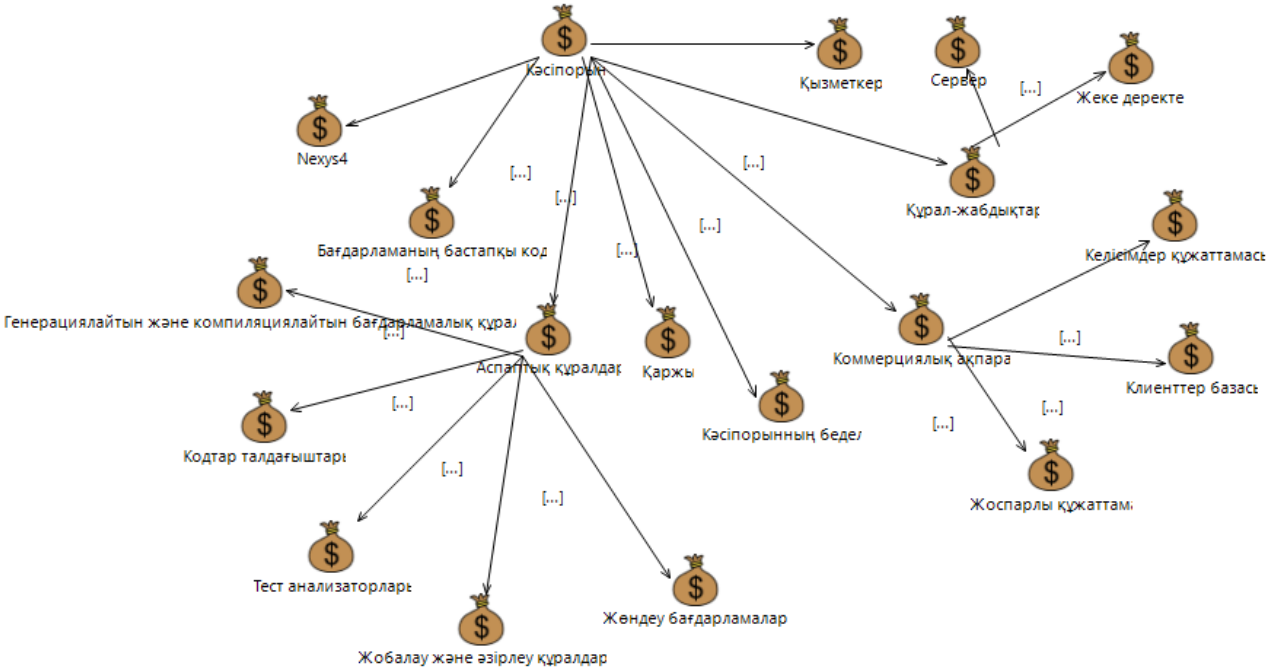
		бақылау шараларындағы кемшіліктер				
3.2	Деректерді өзгерту	Өңделетін деректерді тексерудің болмауы, қолжетімділікті шектеудің дұрыс болмауы	6	Конфигурация элементтеріне рұқсатсыз қолжеткізуден қорғау; конфигурация элементтерін резервтік көшіру; оқиғаларды тіркеу	4	
3.3	Бағдарламалық қате	Қызметкердің біліксіздігі, құралдардың дұрыс жұмыс істемеуі	9	Қызметкерлерді мерзімді оқыту	6	
4 Nexys4						
4.1	Бағдарламаның осалдығын бастапқы кодқа енгізу қаупі	Аспаптық құралдарды пайдалану саясатының болмауы және БҚ конфигурациясын басқару шараларының жеткіліксіздігі	6	Бағдарлама архитектурасының нақтыланған жобасы негізінде бағдарламаны жасау;бағдарламаның бастапқы кодын статистикалық талдау, бағдарламаның бастапқы кодын сараптау, бағдарламаның осалдығын жүйелі түрде іздеу жүргізу	3	
4.2	БҚ жаңартуға осалдықтарды енгізу қаупі	Рұқсатсыз өзгерістерді анықтау мүмкіндігінің болмауы	2	Пайдаланушыға беру процесінде тұтастықтың бұзылуына байланысты ақпараттың	1	

				қауіпсіздігіне қауіп-қатерден БҚ қорғауды қамтамасыз ету; бағдарламаның осалдықтарын жүйелі түрде іздестіруді жүргізу; конфигурация элементтерін резервтік көшіру		
4.3	Бағдарламалық жаңылыс	Тиімді бақылаудың кемшіліктері енгізу	6	Конфигурациялық деректер мониторингі; конфигурация элементтерін резервтік көшіру	4	

5.2 CORAS құралы бар тәуекелдерді талдау

Coras бағдарламалық жасақтамасы бағдарламалық жасақтама бағдарламалық жасақтаманы әзірлеу саласында объектілі модельдеу үшін UML – графикалық сипаттау тілін қолданады.

Тәуекелдерді талдаудың көрнекілігі үшін Coras бағдарламалық құралдарын пайдаланған. Жоғарыда сипатталған активтер диаграммасын және олардың арасындағы байланысты құрдық (5.1-сурет)



5.1 сурет-активтер диаграммасы

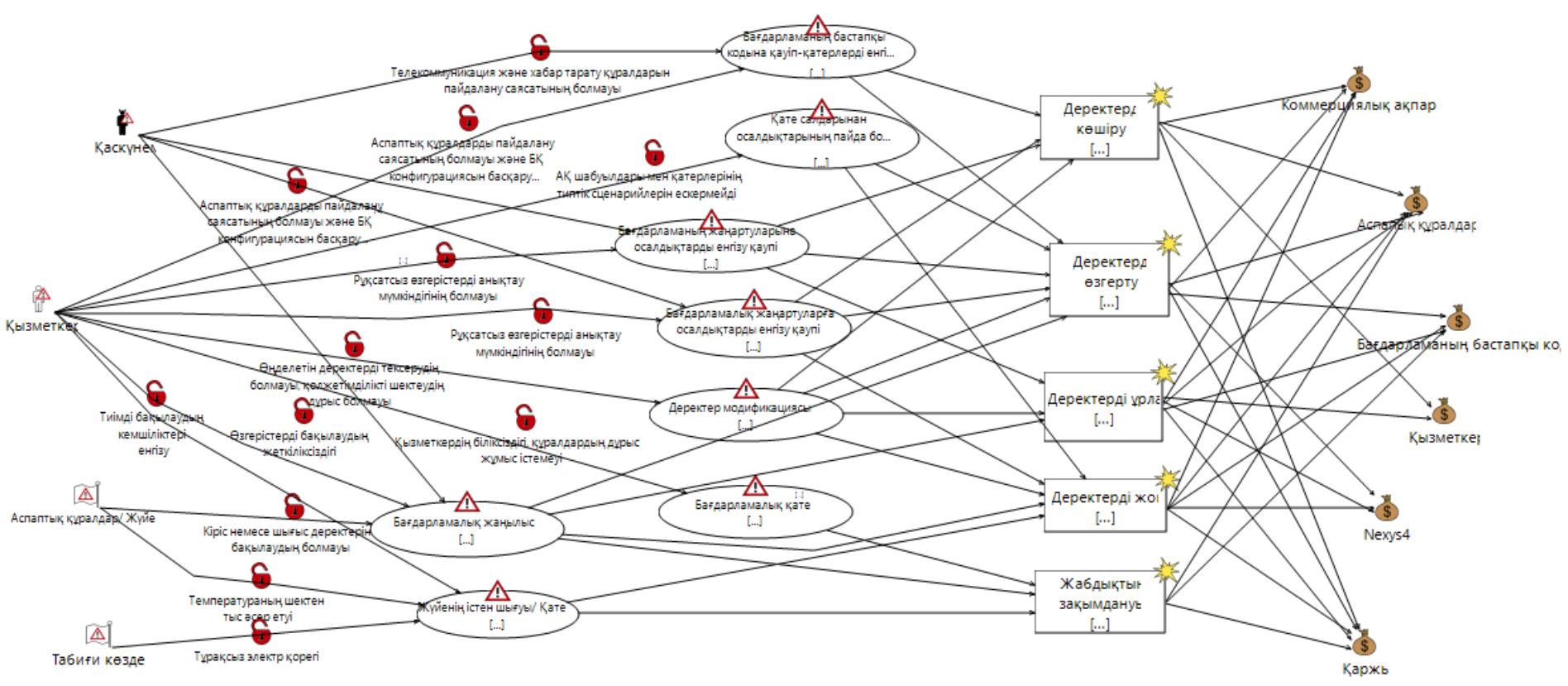
5.4 кестені пайдалана отырып, қауіптер моделін құрайық. Тәуекелдер диаграммасын генерациялаймыз,бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.4 суретте көрсетілген.

Элементтер пайдаланылады:

- Адам факторымен байланысты қасақана қауіп-қатерлерді белгілеу үшін Threat Human Accident;
- Адам факторына байланысты қасақана қауіп-қатерлерді белгілеу үшін Threat Human Deliberate;
- Адам факторымен байланысты емес қауіп-қатерлерді белгілеу үшін Threat Non Human;
- Қатерлерді сипаттау үшін Threat Scenario;
- Осалдықтарды сипаттау үшін Vulnerability;

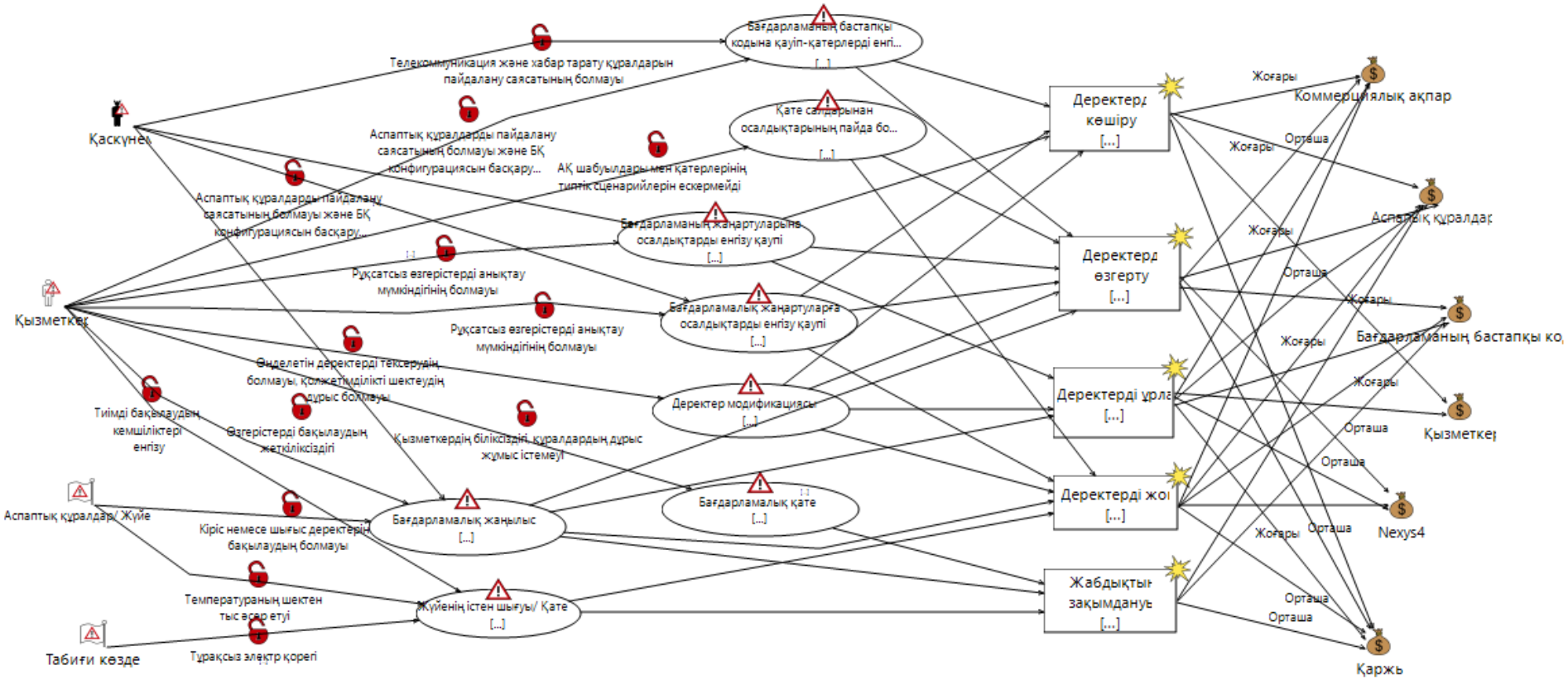
- Жағымсыз оқиғаларды белгілеу үшін Unwanted Incident.

5.4 кестені пайдалана отырып, қауіптер моделін құрайық. Тәуекелдер диаграммасын генерациялаймыз,бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.4 суретте көрсетілген.



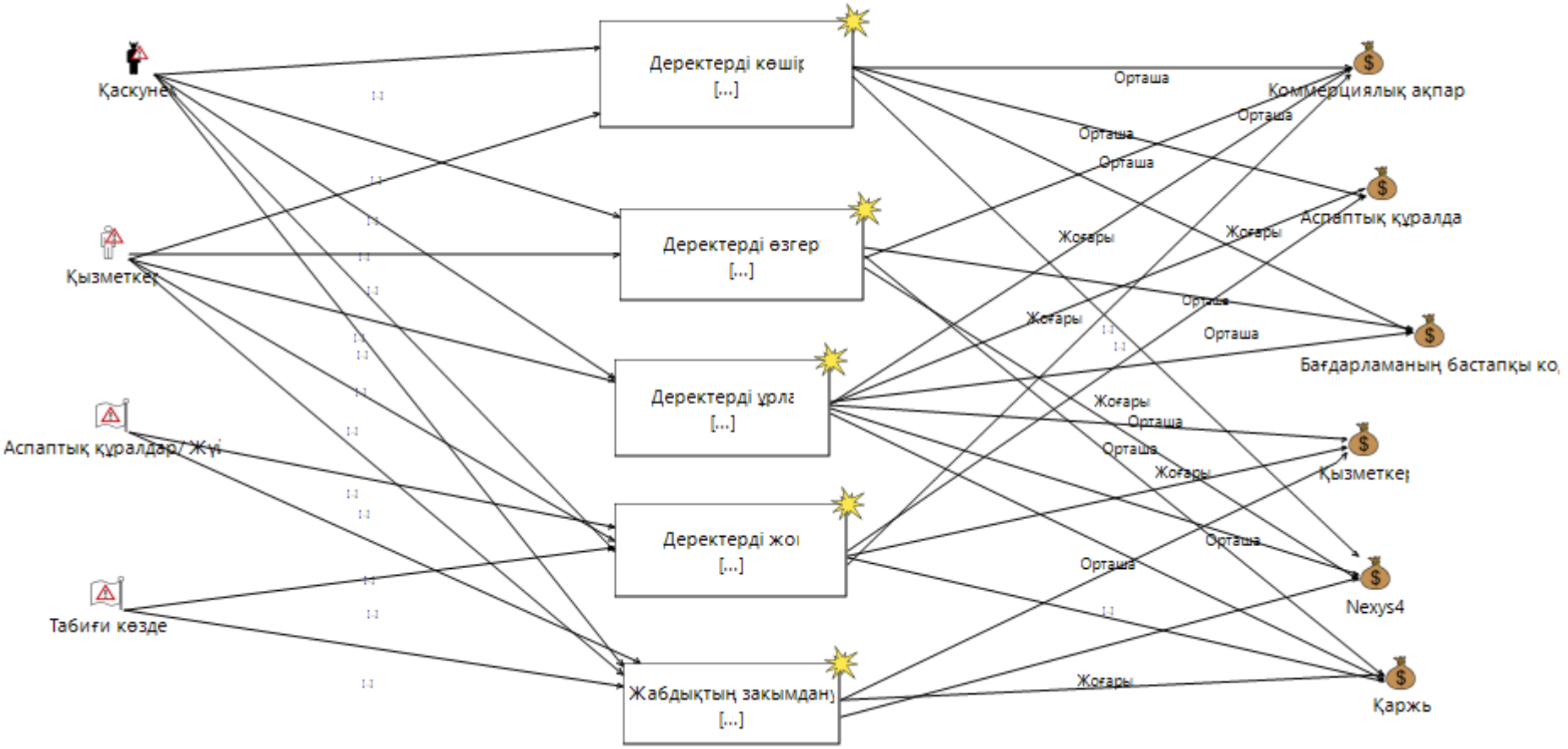
5.2 сурет-қауіптер моделі

Әрбір актив үшін өмірлік цикл кезеңінде әрбір қауіптің туындау ықтималдығын белгіледі.



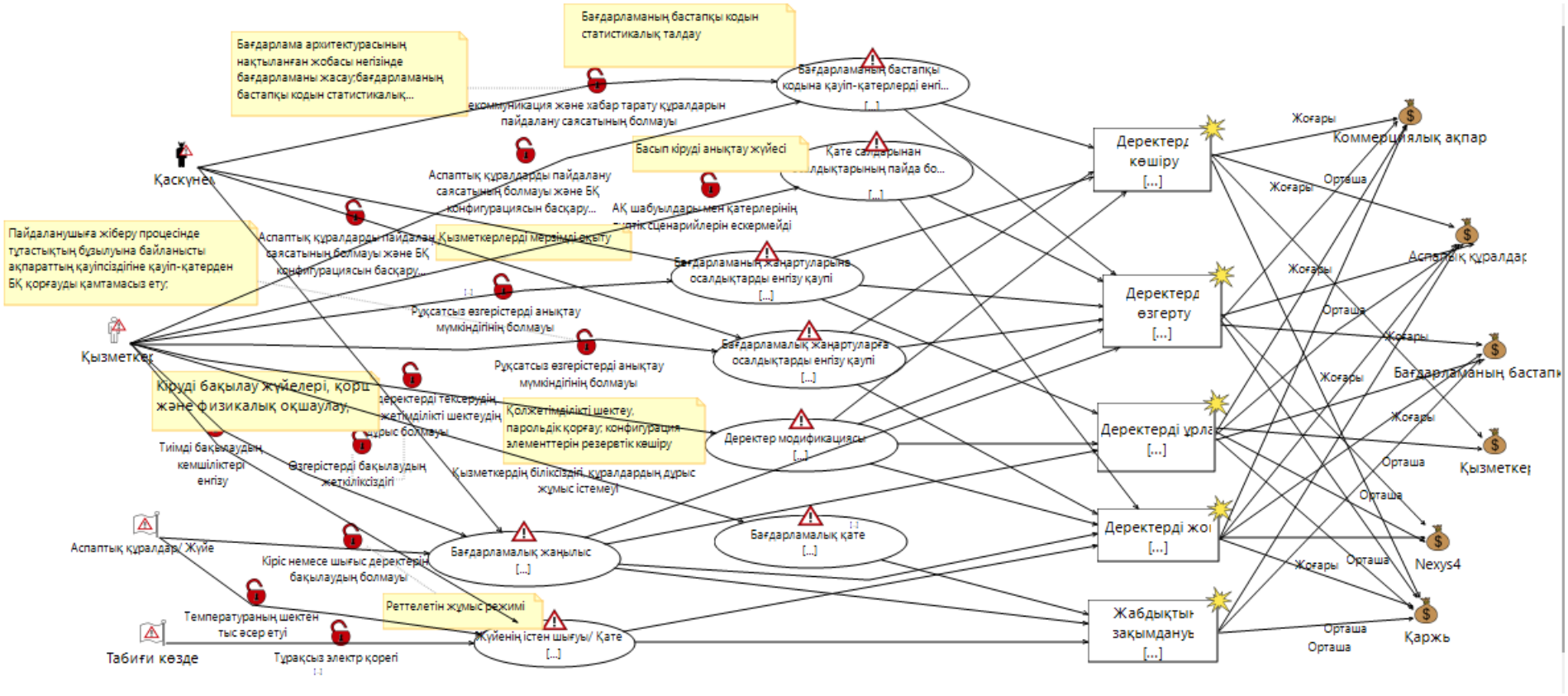
5.3 сурет-ықтимал сипаттамалары бар қауіптер моделі

Шараларды таңдау және нақтылау ақпарат қауіпсіздігіне төнетін қауіп-қатерлерге жүргізілген талдау нәтижелеріне негізделуі тиіс. Бағдарламаның тіршілік циклінің процестерінде осалдықтарының пайда болуын болдырмау және жою мақсатында қауіптерді іске асыруға жататын қорғау шараларының тізбесін анықтаймыз (сурет.5.5).Әсер ету дәрежесін, әрбір актив үшін қауіп-қатерді іске асырудың салдарын анықтады.



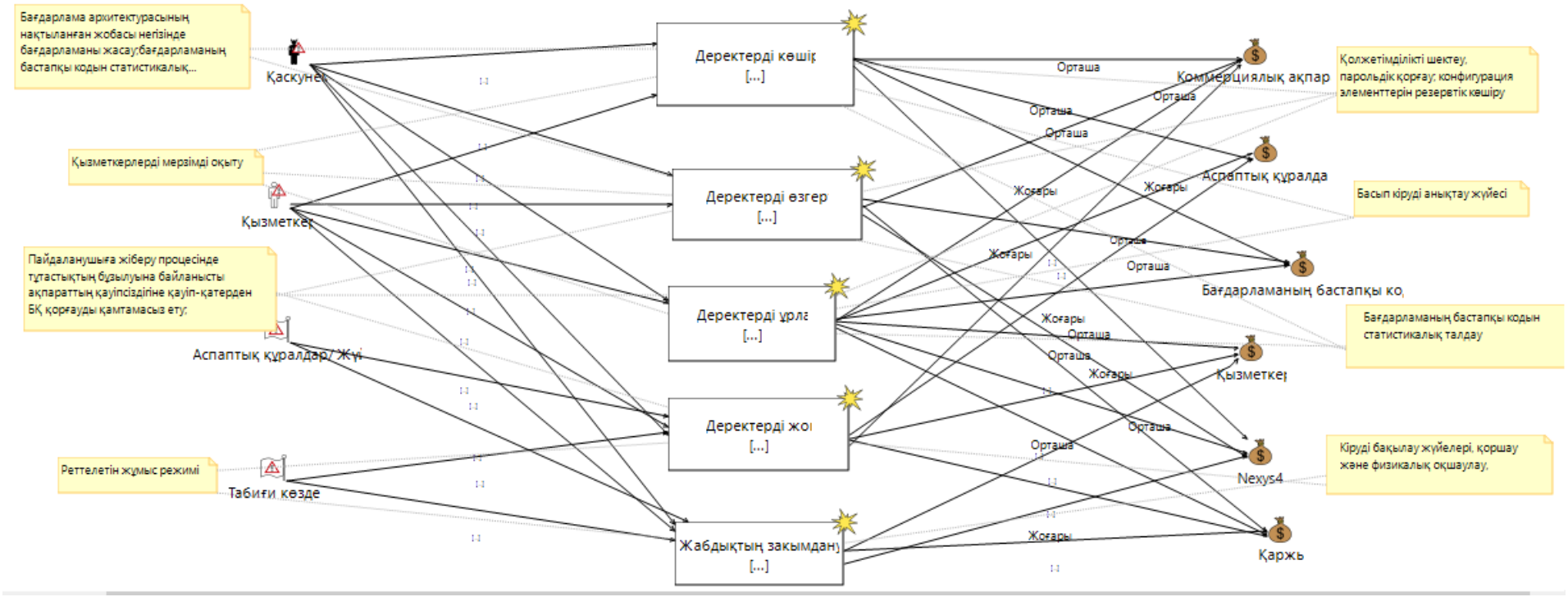
5.4 сурет-қауіпті жүзеге асыру салдарларының сипаттамасы бар тәуекелдер диаграммасы

Тәуекел деңгейін азайту үшін әрбір осалдыққа арналған қорғаныс шаралары, іс-шаралар қабылданды.



5.5 сурет-қорғаныс шараларын қосқаннан кейінгі қауіптер диаграммасы

Бұл диаграммада қорғаныс шараларын қосқан кезде де қалуы мүмкін тәуекелдерді көрсетеді. Жүйелердің толық мониторингі кезінде қауіптердің пайда болуы азайтылуы тиіс.



5.6 сурет-қолайсыз тәуекелдер диаграммасы

Тәуекелдерді бағалау бөлімі бойынша қорытынды

Дипломдық жұмыстың осы бөлігінің мақсаты (тәуекелдерді бағалау) объектіні қорғаудың әзірленетін жүйесі үшін тәуекелдер сипаттамаларын анықтаудан тұрады.

Қорытынды жасай отырып, барлық анықталған ресурстар бойынша тәуекелдер деңгейі есептелді және ақпараттық жүйені қорғау шаралары анықталды. Таңдалған активтердің негізгі қатерлері мен осалдықтары қаралды. Тәуекелдерді бағалау екі фактор бойынша есептеу әдісін қолдана отырып жүргізілді. Тәуекелдердің жоғары деңгейі анықталды,осыған байланысты қорғау шараларын пайдалану туралы шешім қабылданды. Қорғаныс іс-шараларын өткізгеннен кейін тәуекелдерге қайта есептеу жүргізілді. Бастапқы есепте тәуекелдердің мәні 7,5 болды және контрмерді қолданғаннан кейін мәні 5,2-ге дейін төмендеді, бұл қорғаныс құралдарының тиімділігін көрсетеді.

Екінші бөлімде CORAS көмегімен ақпараттық тәуекелдерге талдау жүргізілді және активтерді сәйкестендіруден бастап, қауіптер мен осалдықтар моделінен бастап, қарсы өлшемдерді енгізумен аяқталатын UML диаграммалары салынды.

Қорытынды

Бұл дипломдық жобада барлық қойылған мақсаттар іске асырылды. Ақпаратты криптографиялық қорғау процесін жылдамдататын құрылғы жасалды. Криптожүйені құру барысында барлық нюанстар ескерілді. Беріліп отырған бағдарламалық өнім екі үлкен санды тез көбейтуге мүмкіндік береді.Аппаратты біз тізбекті әрекет ету схема бойынша жасаймыз.

Өміртіршілік қауіпсіздігі бөлімінде жұмыс аймағындағы жұмыс жағдайына талдау жүргізілді. Еңбек жағдайларының деңгейі жұмысшылар үшін қолайлы деп танылды. Ғимараттағы эвакуациялау жолдарын есептеу және жерлендіру есебі орындалды.

Тәуекелдерді бағалау бөлімінде барлық анықталған ресурстар бойынша тәуекелдер деңгейі есептелді және ақпараттық жүйені қорғау шаралары анықталды. Таңдалған активтердің негізгі қатерлері мен осалдықтары қаралды. Тәуекелдерді бағалау екі фактор бойынша есептеу әдісін қолдана отырып жүргізілді.

Пайдаланылған әдебиеттер тізімі

4. Рябко Б.Я., Фионов А.И. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2014. – 173 с.

5. Ахметов Б.С., Корченко А.Г., Сиденко В.В., Дренс Ю.А., Сейлова Н.А. Прикладная криптология: методы шифрования. – Алматы: КазНИТУ им.К.И.Сатпаева, 2015. -496 с.:ил.

6. Айтхожаева Е.Ж., Тынымбаев С.Т. Аспекты аппаратного приведения по модулю в асимметричной криптографии. Журнал Вестник НАН РК.- №5(2014). Алматы, 2014. –с.88-93.

7. Орлов С.А., Цилькер Б.Я. Организация ЭВМ систем: Учебник для вузов, 3-изд.-.СПб.:Питер, 2015. -688 с.

8. Карацуба А.А., Офман Ю.П. Умножение многоразрядных чисел на автоматах. ДАНССР. 1962. Т.145.с.293-314.

9. Cook S.A., Aanderaa S.O. On the minimum computation time of functions. Trans. AMS, 142(1969), p.291-314.

10. Шенхаге А., Штрассен В. Быстрое умножение больших чисел. Кибернетический сборник. 1973. Вып 2. с.87-98.

11. Ковтун М., Ковтун В. Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений [Электронный ресурс.] – http://docplayer.ru/30671408-Obzor-i-klassaifikaciya-algoritmov-privedeniys-po-modulyu-bolshih-chisel-dlya-kriptograficheskih-prilozheniy.html

12. Комбинационный рекуррентный формирователь остатков: пат. 2029435 РФ: МПК H03M7/18/ Петренко В.И., Чипига А.Ф.; заявитель и патентообладатель Петренко В.И., Чипига А.Ф. – №5032302/24; зааявл.16.03.1992; опубл.20.02.1995, – 3с.

13. Устройство для формирования остатка по произвольному модулю от числа: пат. 236942 РФ: МПК H03M7/18, G06F 7/72 / Петренко В.И., Сидорчук А.В., Кузьминов Ю.В.; заявитель и патентообладатель ГОУ ВПО Ставролопольский военный институт связи РВ.– №20101066858/08; зааявл.10.01.2009; опубл.27.09.2009, Бюл.№27– 9 с.

14. S.Tynymbayev, Y.ZH.Aitkhozhayeva, S.Adilbekkyzy. High speed device for modular reduction. Bulletin of National Academy of Sciences of the Republic of Kazakhstan. Volume 6, number 376 (2018)

15. Тынымбаев С.Т., Айтхожаева Е.Ж. формирователь остатка по произвольному модулю. Патент РК №30983 от 19.02.2016, опубликован бюллетень №3 от 16.03.2016, МПК G06F.

16. Тынымбаев С.Т., Бердибаев Р.Ш., Омар Т, Шайкулова А.А., Магауин Б. Быстродействующие устройства приведения числа по модулю. Материалы XIV Международной Азиатской школы – семинара «Проблемы оптимизации сложным систем». 20-31 июля 2018, часть 2, Алматы 2018.

17. https://www.scopus.com/results/authorNamesList.uri?sort=count-

f&src=al&affilName=almaty&sid=062324577e720b6409442ad1f630e2a7&sot=al&sdt=al&sl=36&s=AUTHLASTNAME%28omar%29+AND+AFFIL%28almaty%29&st1=omar&orcidId=&selectionPageSearch=anl&reselectAuthor=false&activeFlag=true&showDocument=false&resultsPerPage=20&offset=1&jtp=false&currentPage=1&previousSelectionCount=0&tooManySelections=false&previousResultCount=0&authSubject=LFSC&authSubject=HLSC&authSubject=PHSC&authSubject=SOSC&exactAuthorSearch=false&showFullList=false&authorPreferredName=&origin=searchauthorfreelookup&affiliationId=&txGid=cd75844c2b83ad6b73fd49ceb7e0565d

18. ҚР ҚНжЕ 3.02-04-2009 – «Әкімшілік және тұрмыстық ғимараттар» - **Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2010.**

19. ҚР ҚНжЕ **2010**2.04-01-2001. «Құрылыстық климатология» - **Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер,** Астана, 2002**.**

20. ҚР ҚНжЕ 2.02-05-2009 – «Ғимараттар мен имараттардың өрт қауіпсіздігі» - **Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана,**.

21. ҚР ҚНжЕ 4.04-10-2002 Қазақстан Республикасы Индустрия және сауда министрлігінің Құрылыс комитеті Астана, 2002.

22. Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800 - «Электроэнергетика» - Алматы: АУЭС, 2013 - 22с.

23. Н.Г. Приходько, Ф.Р. Жандаулетова. Основы пожарной безопасности. Методические указания к выполнению курсовой работы для студентов специальности 5В073100 – Безопасность жизнедеятельности и защита окружающей среды. - Алматы: АУЭС, 2013 - 31 с**.**

24. Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009. - 32 с.