ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Кибернетика және ақпараттық технологиялар институты

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

Санатұлы Сәмет

«Криптография саласында Қазақстан Республикасының мемелекеттік стандарттарының өзектілігін талдау»

ДИПЛОМДЫҚ ЖҰМЫС

Мамандығы 5В100200 - Ақпараттық қауіпсіздік жүйелері

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Кибернетика және ақпараттық технологиялар институты

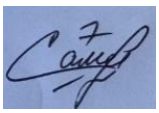
«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
КБОиХИ Кафедра меңгерушісі
тех.ғыл.канд, ассоц. профессор
_____ Н.А.Сейлова
“_____” _____20__ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: “Криптография саласында Қазақстан Республикасының мемелекеттік стандарттарының өзектілігін талдау. ”

Мамандығы 5В100200 - Ақпараттық қауіпсіздік жүйелері

Орындаған  Санатұлы С.

Ғылыми жетекші лектор  Ибраев Р.Б.

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Кибернетика және ақпараттық технологиялар институты

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

БЕКІТЕМІН
КБОиХИ Кафедра меңгерушісі
тех.ғыл.канд, ассоц. профессор
___ Н.А.Сейлова
“_____” _____20__ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы *Санатұлы Сәмет*
Тақырыбы:Криптография саласында Қазақстан Республикасының мемелекеттік стандарттарының өзектілігін талдау.
Университет Ректорының *"27" 01 №762-б* бұйрығымен бекітілген
Аяқталған жұмысты тапсыру мерзімі *2020 жылғы "29"мамыр*
Дипломдық жұмыстың бастапқы берілістері:Криптография саласындағы шетелдік және отандық стандарттар.
Дипломдық жобада әзірленуге жататын мәселелер тізімі:
а) ҚР СТ 1073-2007 және ГОСТ 28147-89 шолу.
б) ҚР СТ 1073-2007 және ГОСТ 28147-89 өзектілігі.
в) ҚР СТ 1073-2007және ГОСТ 28147-89 толықтылығы.
Ұсынылатын негізгі әдебиет: ҚР мемлекеттік стандарттары, "Стандарттау туралы" ҚР Заңы.

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімдері	Ескерту
Ақпараттық қауіпсіздіктің стандарттары	01.03.2020ж.	Орындалды
СТ ҚР 1073-2007 стандартының өзектілігін анықтау	15.03.2020ж.	Орындалды
Гост 28147-89 стандартының өзектілігін анықтау	15.04.2020ж.	Орындалды
ГОСТ 28147-89 және СТ ҚР стандарттарын толықтыруға ұсынылған мәліметтер	06.05.2020ж.	Орындалды

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

Бөлімдератауы	Кеңесшілер, аты, әкесінің аты, тегі (ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Норма бақылау	Магистр тех.ғыл, лектор Зиро А.	01.05.2020ж.	

Ғылыми жетекші лектор _____ Ибраев Р.Б.

Тапсырманы орындауға алған білім алушы _____ Санатұлы С.

Күні «27» қаңтар 2020 ж.

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Санатұлы Самет

Название: «Криптография саласында Қазақстан Республикасының мемелекеттік стандарттарының өзектілігін талдау»

Координатор: Ренат Ибраев

Коэффициент подобия 1:10,4

Коэффициент подобия 2:1,6

Замена букв:1

Интервалы:0

Микропробелы:0

Белые знаки: 0

После анализа Отчета подобия констатирую следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

В данной работе рассмотрены государственные стандарты РК в области криптографической защиты информации, а также нормативные правовые акты, регламентирующие деятельность, связанную с криптографической защитой информации. Следовательно, в данной работе в определенных местах встречаются цитирование указанных НПА.

В работе рассмотрены вопросы, прямо соответствующие тематике работы. Работа выполнена студентом самостоятельно, считаю возможным допустить ее к защите.

Дата 30 мая 2020 года

Подпись Научного руководителя ……

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Санатұлы Самет

Название: «Криптография саласында Қазақстан Республикасының мемелекеттік стандарттарының өзектілігін талдау»

Координатор: Ренат Ибраев

Коэффициент подобия 1:10,4

Коэффициент подобия 2:1,6

Замена букв:1

Интервалы:0

Микропробелы:0

Белые знаки:0

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☐обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;

☐обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

Дата

Подпись заведующего кафедрой /

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

……

……

……

……

……

…… ……

Дата *Подпись заведующего кафедрой* /

АҢДАТПА

Осы жұмыста Қазақстан Республикасы Мемлекеттік стандарттары ҚР СТ 1073-2007 «Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар» талаптарының толықтылығына жүргізілген талдаудың негізгі нәтижелері қарастырылды, сонымен қатар аталған стандартты жетілдіру бойынша негізгі ұсыныстар келтірілген.

Түйін сөздер: ҚР СТ 1073-2007, АКҚҚ, сертификаттау, лицензиялау.

АННОТАЦИЯ

В данной работе рассмотрены основные результаты проведенного анализа полноты и актуальности государственного стандарта Республики Казахстан СТ РК 1073-2007«Средства криптографической защиты информации. Общие технические требования», а также приведены основные предложения по усовершенствованию указанного стандарта.

Ключевые слова: СТ 1073-2007 РК, СКЗИ, сертификация, лицензирование.

ANNOTATION

This paper considers the main results of the analysis of the completeness of the requirements of the state standard of the Republic of Kazakhstan ST RK 1073-2007 “Means of cryptographic information protection. General technical requirements”, as well as the main proposals for improving this standard.

Keywords: ST RK 1073-2007, CIST, certification, licensing.

ЖОСПАР

КІРІСПЕ

Қазақстан Республикасында ақпараттық-коммуникациялық технологиялардың қарқынды дамуы ақпараттық қауіпсіздік проблемаларының өзектілігін растайды.

"Қазақстан Республикасының Ұлттық қауіпсіздік туралы" Қазақстан Республикасы Заңының 4-бабына сәйкес ақпараттық қауіпсіздік Қазақстан Республикасының Ұлттық қауіпсіздік түрлерінің бірі болып саналады .

Қазақстан Республикасының заңнамасында мұндай норманың болуы, Қазақстан Республикасының ұлттық және мемлекеттік органдарының, ақпаратты қорғау құралдарына қойылатын талаптары өте маңызды екендігі, осы талаптарды регламенттеуге, әзірлеуге, іске асыруға, бекітуге негізделген.

Бұл жұмыста ақпаратты криптографиялық қорғаудың қауіпсіздік шаралары (бұдан әрі – криптографиялық ақпаратты қорғау) үшін, Қазақстан Республикасының мемлекеттік стандарттарының рөлі мен орны қарастырылған, Қазақстан Республикасының қолданыстағы нормативтік құқықтық актілерін ескере отырып, олардың нормаларын анықтап, нәтижесі шығарылды.

1 Ақпараттық қауіпсіздіктің стандарттары

1.1 Ақпараттық қауіпсіздік стандарттарының рөлі

Ақпараттық қауіпсіздік стандарттарының басты міндеті қолжетімділігі шектеулі ақпаратты берудің, сақтаудың және өңдеудің әртүрлі жүйелерін жобалау. Пайдалану шеңберінде жүрген өндірушілер, тұтынушылар және ақпараттық қауіпсіздік жөніндегі сарапшылар өз арасында алмасу үшін негізделген.

Тұтынушылар олардың қажеттіліктеріне жауап беретін ақпараттық қауіпсіздік құралдарын таңдауға мүмкіндік беретін әдіске мүдделі, ол үшін бағалау критерийлерін талап етуі тиіс.

Өндірушілерге өздерінің ақпараттық қауіпсіздік құралдарының мүмкіндіктерін салыстыру үшін стандарттар және олардың қасиеттерін объективті бағалау керек, сондай-ақ қауіпсіздік талаптарының белгілі бір жиынтығын стандарттау үшін стандарттар қажет.

Ақпараттық қауіпсіздік жөніндегі сарапшылар, стандарттарды ақпараттық қауіпсіздік құралдарымен қамтамасыз етілетін, қауіпсіздік деңгейін бағалауға мүмкіндік беретін, құрал ретінде қарастырады.

Бүгінде ақпараттық қауіпсіздік жөніндегі сарапшыларға ақпараттық қауіпсіздік стандарттарын білмей жұмыс істеу мүмкін емес. Оған бірнеше себеп бар. Ресми себеп - кейбір стандарттарды қолдану қажеттілігі заңмен бекітілген. Алайда, ең сенімді себептер:

Біріншіден, стандарттар мен олардың спецификациялары-ақпараттық қауіпсіздік бойынша білім жинақтау нысандарының бірі. Оларда білікті мамандар әзірлеген, сынақтан өткізілген, жоғары сапалы шешімдер мен әдіснамалар тіркелген.

Екіншіден, олардың екеуі де аппараттық-бағдарламалық жүйелер мен олардың компоненттерінің өзара үйлесімділігін қамтамасыз етудің негізгі құралы.

1.3 Стандарттау ерекшеліктері

Ақпаратты қорғаудың криптографиялық жүйелерін синтездеу және талдау процесі жоғары күрделілік пен еңбекқорлықпен сипатталады. Осыған байланысты, дамыған криптографиялық технологиялары бар барлық елдерде ақпаратты қорғаудың криптографиялық технологиясы мемлекеттік реттеу саласына жатады. Мемлекеттік реттеу, әдетте, ақпаратты қорғаудың криптографиялық жүйелерін әзірлеуге және енгізуге, оларды сертификаттауға және стандарттауға байланысты қызметті жекешелендіруді қамтиды.

"Рұқсаттар және хабарламалар туралы" Қазақстан Республикасы Заңының нормаларына сәйкес АКҚҚ-рын әзірлеу мен өткізуге, оның ішінде оны біреуге беруге, байланысты қызметтердің бәрі лицензияланған болып есептеледі.

Сертификаттау сынақтарын жүргізу үшін Қазақстан Республикасының техникалық реттеу саласындағы заңнамасының талаптарына сәйкес, ұлттық аккредиттеу орталығы аккредиттелген органдарға тиісті сынақтарды жүргізуге рұқсат етіледі.

Қазақстан Республикасындағы мемлекеттік және ұлттық стандарттар Қазақстан Республикасы инвестициялар және даму министрінің 2018 жылғы 26 желтоқсандағы № 918 бұйрығымен бекітілген ұлттық стандарттарды (әскери ұлттық стандарттарды қоспағанда), техникалық-экономикалық ақпараттың ұлттық жіктеуіштерін және стандарттау жөніндегі ұсынымдарды әзірлеу, келісу, сараптау, бекіту, тіркеу, есепке алу, өзгерту, қайта қарау, күшін жою және қолданысқа енгізу қағидаларының талаптарына сәйкес әзірленеді.

Көрсетілген Ереженің 3-тармағына сәйкес стандарттарда белгіленетін талаптар ғылыми-зерттеулер, тәжірибелік-конструкторлық және жобалау жұмыстарының, патенттік зерттеулердің нәтижелеріне, халықаралық, өңірлік немесе шетелдік стандарттардың және шет мемлекеттердің стандарттау жөніндегі нормативтік құжаттарының ережелеріне және (немесе) отандық және шетелдік ғылымның, техника мен технологияның өзге де қазіргі заманғы жетістіктеріне негізделеді.

Бұл ретте көрсетілген қағидалардың 11-тармағында мынадай субъектілермен стандарттарды міндеттеу көзделген:

1. Мемлекеттік органдардың құзыреті өз шегінде.

2. Бекітілген стандарттау объектілері немесе қызмет бағыттары бойынша стандарттау жөніндегі техникалық комитеттер.

3. Сәйкестікті растау жөніндегі органдар.

4. Кәсіпкерлік субъектілерінің аккредиттелген салалық бірлестіктері.

5. Ғылыми-зерттеу институттары мен зертханалар.

Қазақстан Республикасында АКҚҚ-на қойылатын талаптар ҚР СТ 1073-2007 "ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар".

2 Нормативтік құқықтық актілер

"Рұқсаттар және хабарламалар туралы" Қазақстан Республикасының Заңында әзірлеу және өткізу, оның ішінде АКҚҚ-ын беру, Қазақстан Республикасының уәкілетті мемлекеттік органының арнайы лицензиялары мен рұқсаттары талап етілетін, лицензияланатын қызмет түріне жатады.

Осы жұмыста Қазақстан Республикасының ақпаратты қорғау саласын реттейтін нормативтік құқықтық актілері ҚР СТ 1073-2007 4.1-тармағын ескере отырып қарастырылды.

2.1 Құпиялылықты қамтамасыз ету

Егер Қазақстан Республикасының заңнамасында белгіленбесе, Қазақстан Республикасында ұлттық және мемлекеттік стандарттардың нормалары ерікті сипатта болады.

ҚР СТ 1073-2007 нормаларын мемлекеттік органдардың, жергілікті атқарушы органдардың, мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйелердің меншік иелері мен иеленушілерінің қолдану міндеттілігі, ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы "Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген.

Осылайша, аталған қаулының 48-тармағына сәйкес таратылуы шектеулі қызметтік ақпаратты, құпия ақпараттық жүйелерді, құпия электрондық ақпараттық ресурстарды және қолжетімділігі шектеулі дербес деректерді қамтитын электрондық ақпараттық ресурстарды қорғау мақсатында ҚР СТ 1073-2007 талаптарына сәйкес келетін параметрлері бар АКҚҚ (бағдарламалық немесе аппараттық) қолданылады.

2.2 Түпнұсқалық, оның ішінде тұтастықты қамтамасыз ету

Құқықтық қатынастарды белгілеуді, өзгертуді немесе тоқтатуды көздейтін электрондық цифрлық қолтаңба (бұдан әрі – ЭЦҚ) арқылы куәландырылған электрондық құжаттарды жасау және пайдалану, сондай-ақ азаматтық-құқықтық мәмілелер жасауды қоса алғанда, электрондық құжаттар айналымы саласында туындайтын құқықтық қатынастарға қатысушылардың құқықтары мен міндеттері "Электрондық құжат және электрондық цифрлық қолтаңба туралы"Қазақстан Республикасының Заңымен нормативті бекітілген.

ЭЦҚ ашық кілтінің ЭЦҚ жабық кілтіне сәйкестігін куәландыру, тіркеу куәлігінің дұрыстығын растау үшін Қазақстан Республикасында куәландырушы орталықтар (бұдан әрі-КО) жұмыс істейді.

КО қызметінің заңдылығы "куәландырушы орталықтарды аккредиттеуді жүргізу қағидасын бекіту туралы"Қазақстан Республикасы Үкіметінің 2010 жылғы 19 қарашадағы № 1222 қаулысына сәйкес КО аккредиттеу рәсімін арнайы комиссиямен қамтамасыз етіледі.

Көрсетілген қаулының 5-тармағының 7 тармақшасына сәйкес КО мен оның пайдаланушылары пайдаланатын АКҚҚ ҚР СТ 1073-2007 талаптарына сәйкестік сертификаты болуы тиіс.

Бұдан басқа, Қазақстан Республикасы инвестициялау және даму министрінің 2015 жылғы 28 желтоқсандағы № 1261 "куәландырушы орталықтарды, шет мемлекеттердің сенім білдірілген үшінші тараптарын Қазақстан Республикасының сенім білдірілген үшінші тарапымен тіркеу және өзара іс-қимылын тоқтату қағидаларын бекіту туралы" бұйрығының 3-тармағының 3) тармақшасына сәйкес ҚР СТ 1073-2007 талаптарына сәйкес келетін АКҚҚ КО қолдану міндеттілігі белгіленген.

Көрсетілген нормалар сондай-ақ ауыстырады талаптар ҚР СТ 1073-2007 ерікті міндетті.

3 Мемлекеттік стандарттарға шолу

3.1 ГОСТ 2847-89 және ҚР СТ 1073-2007 стандарттарына шолу

Өткен ғасырдың соңынан Қазақстанда, қазіргі әлемде сияқты, әртүрлі ауқымда және мақсатта ақпараттық жүйелер белсенді түрде құрылып, дамып келеді,қоғам өмірінің барлық салаларын ,ғаламдық ақпараттандыру процесі жүріп жатыр. Нәтижесінде құпия емес қызметтік және коммерциялық мәліметтерді, сондай-ақ таратылуы шектелген мәліметтерді қорғауға арналған ақпаратты криптографиялық қорғау құралдары (АККҚ) талап етілді. Сонымен қатар, сатып алушылар мен АККҚ пайдаланушыларын қорғау үшін Қазақстанда осы құралдарды сертификаттау жүйесі дами бастады. Бірінші кезеңде келесі қарама-қайшы факторлармен сипатталатын бір мәнді жағдай қалыптасты.

1. Қолданыстағы криптографиялық стандарттар ГОСТ 28147-89 кеңестік стандарты, сондай-ақ ГОСТ 34.310-95 және ГОСТ 34.311-95 мемлекетаралық стандарттары ғана болды.

2. Көптеген криптографиялық аспектілер, атап айтқанда, ассимметриялық шифрлау, кілттерді генерациялау регламенттелмеген. Шетелдік стандарттар Des, TripleDES, AES, DSA, SHA-1 алгоритмдарын қолданып жүрді.

3. Қазақстанда әзірленген, тіпті жоғарыда көрсетілген қолданыстағы және шетелдік стандарттарды іске асыратын АККҚ-ның көбісі криптографиялық тұрақсыз болып табылды, кілттерді генерациялау мен басқарудың дұрыс іске асырылмауына байланысты.

4. Бізде ГОСТ 28147-89 және ГОСТ 34310-95 және ГОСТ 34311-95 сияқты шетелдік стандарттар пайдаланылды. Отандық стандартты құру үшін уақыт келді және 2002 жылы Қазақстан Республикасының Ұлттық қауіпсіздік комитеті ҚР СТ 1073-2007 құрылды. Қазіргі редакция 2007 жылғы болып табылады.

Осы стандарт отандық және шетелдік өндірістің ақпаратты криптографиялық қорғау құралдарына қолданылады және оларға қойылатын жалпы техникалық талаптарды белгілейді. Стандарт сәйкестікті растау мақсатында жарамды. Осы стандарт Қазақстан Республикасының мемлекеттік шифрлау құралдары болып табылатын ақпаратты криптографиялық қорғау құралдарына қолданылмайды.

ҚР СТ отандық және шетелдік өндірістегі АККҚ-на қолдану саласы және оларға қойылатын жалпы техникалық талаптарды белгілейді Қазақстан Республикасының мемлекеттік шифрлау құралдары болып табылатын АККҚ-на қолданылмайды.

Бұл стандартты әзірлеу негізінде келесі тұжырымдамалық тәсілдер алынды. Сертификаттық зерттеулер барысында АККҚ-на ақпаратты қорғаудың кешенді технологиялық аяқталған құрал ретінде қарастыру қажет. Стандартта қорғалатын ақпаратты жариялаудан, танудан немесе рұқсатсыз өзгертуден

болатын ықтимал залалға байланысты АКҚҚ қауіпсіздігінің төрт деңгейін анықтау.

АКҚҚ басты шарттары :

1. Құпия деректерді шифр арқылы қорғау.
2. Түпнұсқаландыру, ЭЦҚ көмегімен деректердің тұтастығын бақылау.
3. Кілттерді генерациялау, қалыптастыру, бөлу немесе басқару.

3.1 кесте - Жалпы техникалық талаптар ҚР СТ 1073-2007

Ұсыныстар	I-деңгей	II-деңгей	III-деңгей	IV-деңгей
Зала,АЕК	100	10 000	1 000 000	100 000 000
Есептеу күрделілігі	2^50	2^80	2^120	2^160
Кілттер генераторы	кездейсоқ оқиғалар	кездейсоқ оқиғалар	физикалық шум	физикалық шум
Симметриялық алгоритм кілтінің ұзындығы	60	100	200	250
Асимметриялық алгоритм кілтінің ұзындығы	500	1500	4000	8000
Кілттің эллиптикалық ұзындығы	120	160	250	400
Хэш код ұзындығы	120	160	250	400
ЭЦҚ ұзындығы	120	200	300	400
Қорғалмаған арна бойынша бөлінетін кілттерді криптқорғау	+	+	+	+
Әрбір кілт үшін алгоритмнің жалғыздығы	+	+	+	+

3.1-і кестенің жалғасы

Ұсыныстар	I-деңгей	II-деңгей	III-деңгей	IV-деңгей
АКҚҚ-ын рұқсатсыз өзгертуден қорғау	+	+	+	+
Техникалық құжаттамадағы алгоритмдердің сипаттамасы+	+	+	+	+
АКҚҚ техникалық құжаттамаға сәйкестігі	+	+	+	+
Пайдалану құжаттамасының толықтығы	+	+	+	+
0,5 ықтималдықтың ауытқуы (кілт биті=1), одан артық емес	0,03	0,01	0,003	0,001
Бұрмаланған кілттерді анықтау		0,9999	0,999999	0,9999999999

ГОСТ 28147-89, 1990 жылы енгізілген симметриялық шифрлау Ресей стандарты, ТМД елдерінде де қолданысқа ие. Толық атауы – "ГОСТ 28147-89 ақпаратты өңдеу жүйелері. Криптографиялық қорғау. Криптографиялық түрлендіру алгоритмі". Блокты шифр алгоритм. Гаммалаумен шифрлау әдісін қолданғанда, ағынды шифр алгоритм функциясын орындай алады.

ГОСТ 28147-89 256-биттік кілтті, 32-түрлендіру циклі бар, 64-биттік блоктармен операция жасайтын блоктық шифр. Алгоритмінің негізінде Фейстель желісі жатыр.

Жұмыс режимдері:

1. Оңай ауыстыру режимі.
2. Гаммалау режимі.
3. Кері байланысы бар гаммалау режимі.
4. Имитовставки жасау режимі.

Осы стандарт электрондық есептеу машиналары (ЭЕМ) желілерінде, жекелеген есептеу кешендері мен ЭЕМ-да ақпаратты өңдеу жүйелері үшін криптографиялық түрлендірудің бірыңғай алгоритмін белгілейді, деректерді

шифрлеу және имитовставканы өңдеу ережелерін айқындайды. Криптографиялық түрлендіру алгоритмі аппаратты немесе бағдарламалы түрде жүзеге асады, криптографиялық талаптарды қанағаттандырады және өзінің мүмкіндіктері бойынша қорғалатын ақпараттың құпиялылық дәрежесіне шектеулер қоймайды. Стандарт ЭЕМ желілерінде, жеке есептеу кешендерінде немесе ЭЕМ-да сақталатын және берілетін деректерді криптографиялық қорғауды қолданатын ұйымдар, кәсіпорындар мен мекемелер үшін міндетті болып саналады.

2010 жылы ГОСТ халықаралық шифрлау стандарты дәрежесіне ие болып, ISO стандартты ретінде мәлімденді. Алгоритмдердің өте аз саны халықаралық стандарттарға айнала алды. TDEA, MISTY1, CAST — 128, HIGHT-және үш 128 биттік Шифр-AES, Camellia, SEED. ГОСТ сол ISO/IEC 18033-3 стандартын қосу ұсынылады.

3.2 кесте - Симметриялық шифрлау алгоритмі ГОСТ және DES салыстыру

ГОСТ	DES
КГБ ішкі дамуы, ол оны жұртшылық үшін ашық етеді.	Корпоративтік даму болып табылады және жария пайдалану үшін ашық.
Бұл бағдарламалық және аппараттық нұсқаларда оңай іске асырылады	Hardware нұсқасында іске асыру үшін қарапайым, soft өнім нұсқасында іске асыру қиын.
Барлық алдыңғы әзірлемелер мен қателерді ескере отырып, неғұрлым озық және қазіргі уақытта пайдаланылатын.	Пайдалану үшін ұсынылмайды. Ол өте танымал болды.
Ол жабық алгоритмге байланысты өте танымал емес,әсіресе s блогы, сұрау бойынша FSB жіберіледі.	Сынық арқылы бұзылды.
Ол жақсы негізгі тұрақтылық бар. Қазіргі уақытта бірде-бір белгілі бұзу оқиғасы жоқ.	Негізгі кеңістіктің тұрақтылығын салыстыру: блок 64, кілт 56-қысқа уақыт ішінде заманауи компьютерлерде қайталауға болады.

ГОСТ 28147-89 кеңес үкіметінен келе жатқан отандық блоктық шифр болып табылады. Яғни, ашық мәтін блоктарға бөлінеді (бұл жағдайда 64 бит) және әрбір блок бөлек түрлендіріледі. Алгоритмнің негізі Фейстель желісі болып табылады.

Алгоритмнің сипаттамасы:

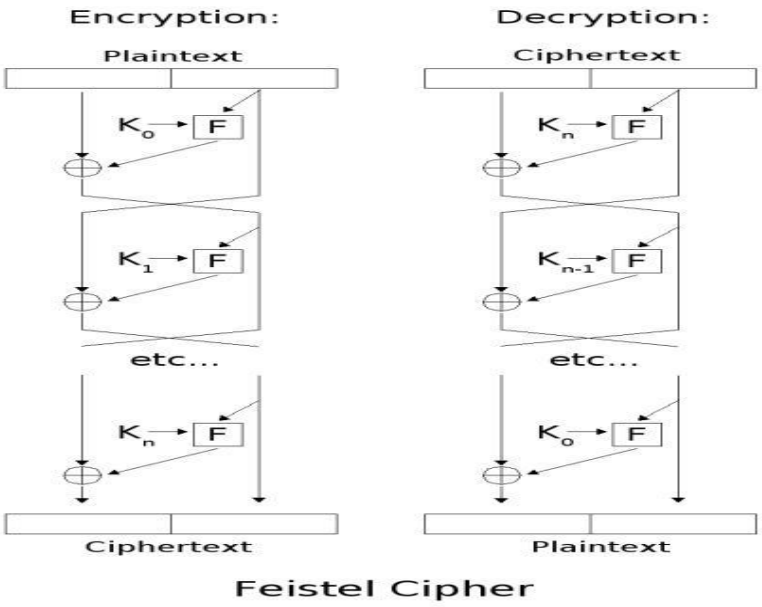
1. Әрбір блок екі "подблокқа" бөлінеді (сол және оң).

2. Оң блокты бастапқы толтыру сол блокта жазылады.

3. Оң блоктың үстінде негізгі деректерді қолданумен криптографиялық түрлендіру жүргізіледі.

4. Сол (бастапқы) және оң (түрлендірілген) блоктар 2-модуль бойынша сумматорда жинақталады.

5. Бірнеше рет қайталанады.



Feistel Cipher

3.1 Сурет – Алгоритмнің негізіне Фейстель желісі қосылған

Бұл схема 32 бит бойынша төрт жинақтауыш: N1, N2, N3, N4. Екі 32-разрядты жинақтағыш: N5 және N6, – оларға тиісінше C2 және C1 тұрақты толтырылуы жазылған.

Алгоритмнің құрылымдық сұлбасының сипаттамасы:

1. 256 битке негізгі есте сақтау құрылғысы (КЗУ) ROM 32 разрядты сегіз жинақтан тұрады: X, X1, X2, X3, X4, X5, X6, X7.

2. 32-разрядты сумматор 2 СМ2 модулі бойынша.

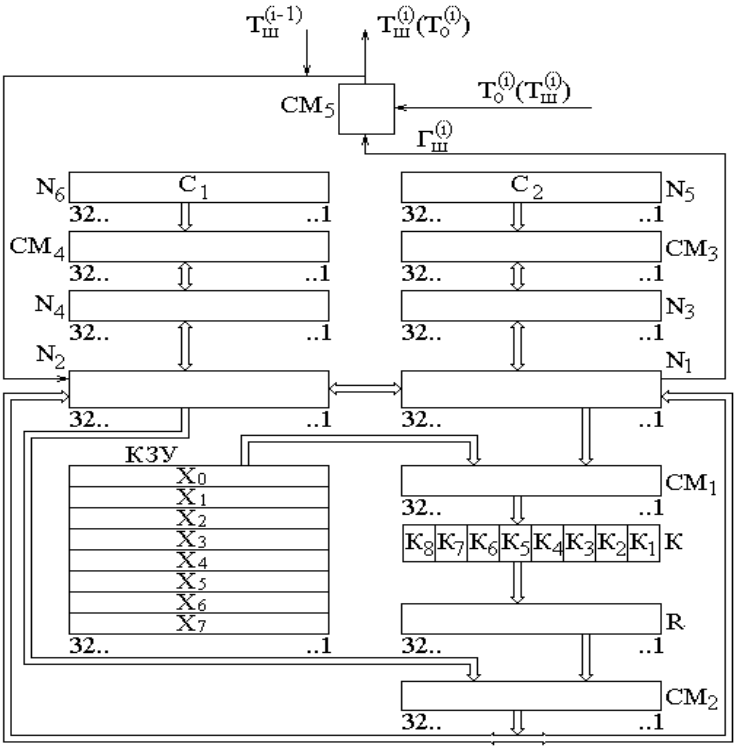
3. 2 модуль бойынша тағы бір сумматор, ол разрядтық шектеулерге ие емес (бірақ 64 бит қолданылады) СМ5.

4. 32 бит 232 разрядтық модулі бойынша екі сумматор: СМ1, СМ3.

5. Модуль бойынша сумматор (232-1) СМ4.

6. К орнату блогы: К1, К2, К3, К4, К5, К6, К7, К8 сегіз ауыстыру тораптары, әрқайсында 64 биттен тұратын жады бар.

7. Циклдық ығысу регистрі солға 11 бит R жылжыйды.



3.2 Сурет – Алгоритмнің құрылымдық сұлбасы

Кілттер. КЗУ 256 бит бөлінген, ГОСТ 28147-89 ұзындығы 256 бит кілті қолданылады. Кілт 32 биттен сегіз блоктарға бөлінеді және әрбір блоктың әрбір биті тиісті ретті х жинағышына жүйелі түрде енгізіледі.

Яғни, кілттің 1-ші биті жинақтауыштың 1-ші разрядына Х, 2-ші жинақтауыштың 2-ші разрядына Х, 33-ші жинақтауыштың 1-ші разрядына Х1, 65-ші жинақтауыштың 1-ші разрядына Х2, және тағы басқа, 224-ші кілт биті жинақтауыштың 1-ші разрядына Х7, 256-ші кілт биті жинақтауыштың 32-ші разрядына енгізіледі.

К орналастыру блогында, орнату блогында 16х8 өлшемдік ауыстыру кестесі бар, ол ұзақ уақыт кілт болып саналады. Қысқаша айтқанда кесте жолдары ауыстыру талап етіледі (он алтылық есептеу жүйесінде 0-ден 15-ке дейінгі сан). Бағандар не алмастыратынын көрсетеді. Сонымен қатар, 32-биттік векторға түсетін вектор сегіз 4 биттік бөлікке бөлінеді,олардың әрқайсысы ауыстыру кестесіне сәйкес өзгертіледі. КЗУ-дегі, сондай-ақ К блогындағы кілттер құпия болып табылады және олардың ымыраласуына жол бермеу шараларын қолдану талап етіледі.

3.2 ҚР СТ 1073-2007 өзектілігін талдау

Жоғарыда көрсетілген нормативтік құқықтық актілерде ҚР СТ 1073-2007 талаптарына сәйкестік түрінде қолданылатын АКҚҚ қауіпсіздігіне қойылатын талаптар келтірілген, бұл ретте өзге де талаптар белгіленбеген.

ҚР СТ 1073-2007 қойылатын өзге де талаптар:

1. ҚР СТ 1073-2007 құралдардың өзіне қойылатын талаптарды белгілейді, бұл ретте АКҚҚ-ын әзірлеу, өндіру, өткізу, жөндеу және кәдеге жарату процестеріне қойылатын талаптарды белгілемейді.

2. ҚР СТ 1073-2007 оның криптографиялық тұрақтылығына тікелей әсер ететін АКҚҚ негізгі көрсеткіштеріне нақты талаптарды, атап айтқанда криптографиялық түрлендіру алгоритмдерінің негізгі параметрлеріне (кілттің ұзындығы, қалыптастырылатын ЭЦҚ ұзындығы, хэш-кодтың ұзындығы, статистикалық көрсеткіштер қойылатын талаптарды белгілейді, демек, оларды "жалпы" деп атау дұрыс емес.

3. ҚР СТ 1073-2007 аппараттық және аппараттық-бағдарламалық АКҚҚ жұмыс істеуі кезінде туындайтын ақпараттың таралып кетуінің техникалық арналарынан АКҚҚ-ын қорғауға, атап айтқанда, құпия, оның ішінде кілттік ақпараттың техникалық арналары бойынша қойылатын талаптарды белгілемейді.

4. ҚР СТ 1073-2007 қорғалатын, оның ішінде негізгі ақпараттың қауіпсіздігіне қатер төндіретін АКҚҚ-ның аппараттық және бағдарламалық декларацияланбаған мүмкіндіктеріне қойылатын талаптарды белгілемейді.

5. ҚР СТ 1073-2007 сәйкестігін "тексеру қиын" АКҚҚ-ға қойылатын талаптарды белгілейді, атап айтқанда, АКҚҚ-дан негізгі ақпаратты жоюға және криптографиялық қорғауды ашудың "қолданыстағы" алгоритмдерінің еңбек сыйымдылығына кепілдік беруге қатысты талаптарды белгілейді, бұл ретте мүмкін болатын шабуылдардың ең аз тізбесі келтірілмейді.

6. ҚР СТ 1073-2007 кілттік ақпараттың қолданылу мерзімін шектеуге, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз етудің ұйымдастырушылық шараларын негізге ала отырып жұмыс режимдерін таңдауға бағытталған, АКҚҚ-ға қойылатын талаптарды белгілемейді, атап айтқанда ҚР СТ 1073-2007 бір кілтте қорғалған ақпараттың құны бойынша АКҚҚ-ға қойылатын талаптар келтіріледі, бұл ретте криптографиялық талдау жүргізуге мүмкіндік беретін ақпараттың сыни көлемі ақпараттың бір кілттегі сыни құнынан бұрын асып түсуі мүмкін.

7. ҚР СТ 1073-2007 ең үздік криптографиялық шабуылдардың еңбек сыйымдылығы түрінде АКҚҚ криптографиялық тұрақтылығына қойылатын талаптарды белгілейді, бұл ретте жад көлеміне және бір кілтте шифрланған сыни ақпараттың көлеміне қойылатын талаптарды ескермейді.

3.3 ҚР СТ 1073-2007 толықтығын талдау

Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің міндетін атқарушы 2019 жылғы 22 шілдедегі № 169/НҚ бұйрығымен бекітілген "Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің ақпараттық қауіпсіздік комитеті" мемлекеттік мекемесі ережесінің 1-тармағына сәйкес Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің ақпараттық қауіпсіздік комитеті Қазақстан Республикасының ақпараттандыру

және байланыс жөніндегі агенттігі болып табылады, Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба туралы заңнамасын сақтау, ақпараттандыру саласындағы ақпараттық қауіпсіздікті қамтамасыз ету, сондай-ақ электрондық құжат және электрондық цифрлық қолтаңба саласындағы министрліктің стратегиялық функцияларын орындауға қатысатын іске асыру және бақылау функциялары.

Жүргізілген жұмыстың нәтижелері бойынша Қазақстан Республикасында ақпаратты криптографиялық қорғау жөніндегі қызметті жетілдіруге мүмкіндік беретін мынадай ұсыныстар әзірленді:

1. Қазақстан Республикасы инвестициялар және даму министрінің 2018 жылғы 26 желтоқсандағы № 918 бұйрығымен бекітілген ұлттық стандарттарды (әскери ұлттық стандарттарды қоспағанда), техникалық-экономикалық ақпараттың ұлттық жіктеуіштерін және стандарттау жөніндегі ұсынымдарды әзірлеу, келісу, сараптау, бекіту, тіркеу, есепке алу, өзгерту, қайта қарау, күшін жою және қолданысқа енгізу қағидаларының 3-тармағының тармақшасына сәйкес стандарттар ғылыми зерттеулер нәтижелері негізінде әзірленеді. Осыған байланысты стандарттың жаңа редакциясын әзірлеуге мүмкіндік беретін тиісті ғылыми-зерттеу жұмыстарын ұйымдастыру, сондай-ақ "бір мәнді емес түсіндіруді" болдырмайтын нақты талаптарды енгізу, атап айтқанда, әр түрлі тасымалдағыштардан ақпаратты жою әдістерін нақты жазу (әр түрлі тасымалдағыштардан ақпаратты жою мен жоюдың ғылыми негізделген әдістеріне жаңа стандартты бастамашылық ету мүмкін), криптографиялық шабуылдардың базалық тізімін ақпаратты криптографиялық түрлендіру алгоритмдерінің кең таралған типтеріне келтіру ұсынылады, шабуылдардың еңбек сыйымдылығын, критикалық ақпараттың көлемін, криптографиялық шабуыл және т. б. үшін талап етілетін жад көлемін ескере отырып криптографиялық төзімділікті бағалау.

2. Ақпараттық қауіпсіздік қатерлерінің туындау тәуекелдерін азайту мақсатында Қазақстан Республикасының мемлекеттік органдарына Қазақстан Республикасында АККҚ-ны әзірлеу, өндіру, іске асыру, жөндеу және кәдеге жарату процестерін бекітуге мүмкіндік беретін нормативтік құқықтық актіні әзірлеуге бастамашылық жасау ұсынылады.

3. Қазақстан Республикасы Үкіметінің "ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы" 2016 жылғы 20 желтоқсандағы № 832, "куәландырушы орталықтарды аккредиттеуді жүргізу қағидаларын бекіту туралы" 2010 жылғы 19 қарашадағы № 1222 және "уәландырушы орталықтарды тіркеу және олардың өзара іс-қимылын тоқтату қағидаларын бекіту туралы" 2015 жылғы 28 желтоқсандағы № 1261 қаулыларына, "Қазақстан Республикасының Ақпаратты техникалық қорғау, ақпаратқа рұқсатсыз қол жеткізуден қорғау саласындағы Қазақстан Республикасының басқа да мемлекеттік және ұлттық стандарттарына сілтемелер түрінде тиісті толықтырулар енгізсін.

4. Жүзеге асырылатын қызметтің сапасын арттыру мақсатында "Рұқсаттар және хабарламалар туралы" Қазақстан Республикасының Заңында қолдану мерзімін шектей отырып, түрлері бойынша АКҚҚ-на қатысты рұқсат беру құжаттарын бөлу ұсынылады: АКҚҚ-ны әзірлеуге арналған лицензия, АКҚҚ-ын өндіруге арналған лицензия, АКҚҚ-ын өткізуге арналған рұқсат, АКҚҚ-ын жөндеуге арналған лицензия, АКҚҚ-ын кәдеге жаратуға арналған рұқсат.

3.4 ГОСТ 28147-89 өзектілігін талдау

Қандай да бір модификациясыз ГОСТ 28147-89-ға толық раунды шабуылдар бар. Алгоритмге талдау жүргізілген алғашқы ашық жұмыстардың бірі, белгілі шифрлау алгоритмдерінің бірқатар кілттерін кеңейту рәсімдерінің әлсіздігін пайдаланды. Атап айтқанда, ГОСТ 28147-89 толықанды алгоритм байланысқан кілттерде дифференциалды криптоанализдің көмегімен, бірақ ауысудың әлсіз кестелерін қолданған жағдайда ғана ашылуы мүмкін. Алгоритмнің 24-раунды нұсқасы (онда алғашқы 8 раунд жоқ) кез келген ауысым кестелерінде ұқсас түрде ашылады, алайда, күшті ауысым кестелері мұндай шабуылды мүлдем тиімсіз етеді.

Ресей ғалымдары Г.Ростовцев пен Э.Б.Маховенко 2001 жылы криптанализдің түбегейлі жаңа әдісін ұсынды (менің ойымша, анағұрлым тиімді, сызықты және дифференциалды криптанализ) мәтін шифріне сәйкес келетін белгілі ашық мәтіннің объективті функциясының мәні, қажетті кілт мәні және кілттің шын мәніне сәйкес келетін экстремумын табу. ГОСТ 28147-89 әлсіз кілттердің үлкен класын қамтиды, бұл барлық таңдалған 4 ашық мәтінді және күрделілігі төмен тиісті шифрмәтінді қолдана отырып алгоритм ашуға мүмкіндік береді.

2004 жылы Кореяның мамандар тобы тағы бір шабуыл түрін ұсынды,оның көмегімен байланысқан кілттердегі дифференциалды криптоанализді пайдалана отырып, 91,7% 12 бит құпия кілтті алуға болады. Шабуыл үшін 2^35 таңдалған ашық мәтін және 2^36 шифрлау операциясы қажет. Бұл шабуыл алгоритмді нақты ашу үшін пайдасызекендігі анықталды.

ГОСТ артықшылықтары:

1. Күш шабуылының перспективасыздығы.

2. Іске асыру тиімділігі және қазіргі компьютерлердегі жоғары жылдамдығы.

3. Жалған деректерді тануы және одан қорғауы (имитовставканы өндіру) және ГОСТ барлық төрт алгоритмі бірдей циклде шифрлауы.

ГОСТ бойынша бар мәліметтердің ешқайсысы шифр қауіпті болуы мүмкін деп пайымдауға негіз бермейді. Керісінше, кілттің үлкен өлшемі мен раундтардың үлкен саны ГОСТ-ты, он жылға қолайлы деп айтуға болады. Мур заңымен таныс адамдардың барлығы, теорияда 256-биттік кілттер кем дегенде 200 жыл қауіпсіз болып қалатынын түсінеді.

Шнайер, Бирюков, Данкельман, Вагнер, көптеген австралиялық, жапондық және ресейлік ғалымдар, криптография жөніндегі сарапшылар, блоктық шифрларды талдау саласында жүрген танымал жетекші мамандар кеңінен зерттді және олардың айтуы бойынша бұл алгоритм қауіпсіз болуы мүмкін немесе әлсіз кілттер кестесіне байланысты өте қауіпті болуы мүмкін деп есептеді.

Мысалы, DES алгоритмімен салыстырғанда, диффузия соншалықты мықты емес, бірақ бұл әрдайым раундтардың үлкен санымен (32), сондай-ақ модуль бойынша қосумен қамтамасыз етілетін қосымша сызықтықпен және диффузияның арқасында жақсы болып тур.

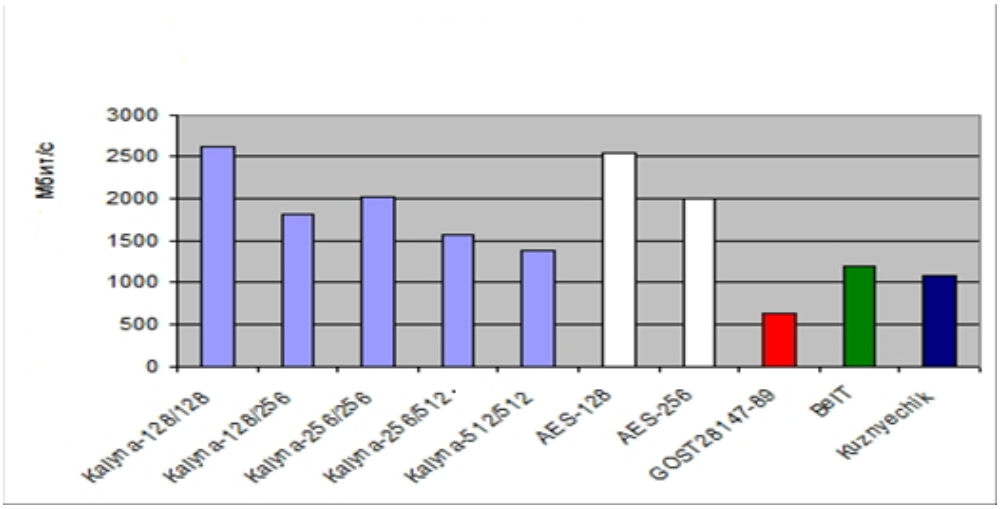
ГОСТ негізгі проблемалары кілттер мен ауысым кестелерін генерациялау бөлігінде, яғни стандарттың толық еместілігімен байланысты. "Әлсіз" кілттер мен ауысым кестелері бар екендігі тривиальды дәлелденеді, бірақ стандартта "әлсіз" таңдау және өлшемдері сипатталмайды. Сонымен қатар, стандарт ауысым кестелерін (S-блоктарды) генерациялау алгоритмін спецификияламайды. Бір жағынан, бұл қосымша құпия ақпарат болуы мүмкін, ал екінші жағынан, бірқатар проблемаларды көтереді:

1. Алдын ала алмасу кестесін білмей алгоритмнің криптотөзімділігін анықтауға болмайды.
2. Әр түрлі өндірушілерден алгоритмді жүзеге асыру әр түрлі ауысым кестелерін пайдалана алады және өзара сыйыспайтын болуы мүмкін.
3. Потенциалды мүмкінлік (стандартта тыйымның болмауы) алмастырулар үшін кестені пайдалану, онда түйіндер алмастыру болып есептелмейді, осылайша шифрдың беріктігінің төмендеуіне әкелуі мүмкін.

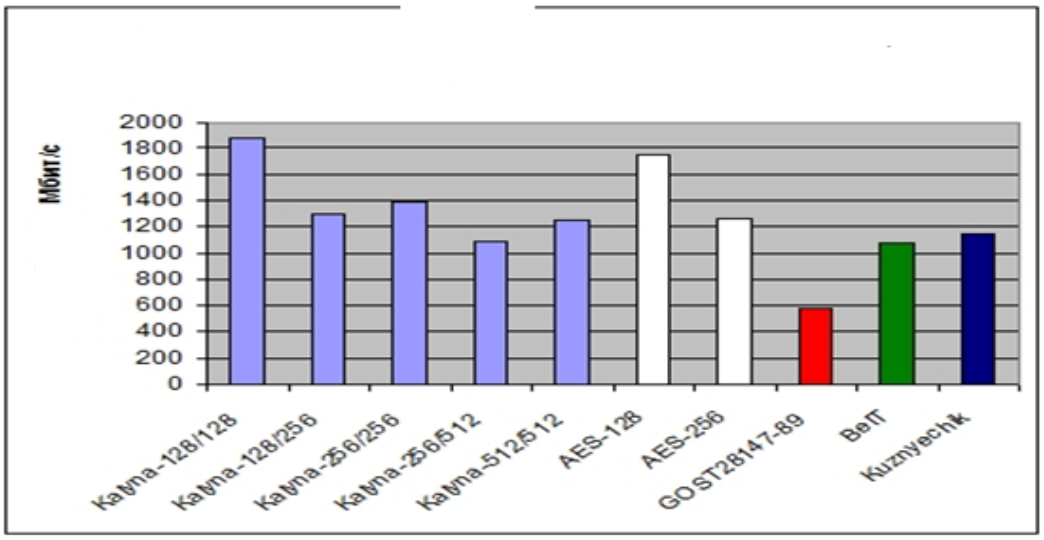
3.5 ГОСТ 28147-89 толықтығын талдау

ГОСТ 28147-89 ТМД-ның көптеген елдерінде негізгі шифр ретінде қолданылды. Ол әлі де практикалық төзімділікті қамтамасыз етіп отырса да, ол үшін криптоанализдің теориялық әдістері белгілі, кілттердің толық аралығына қарағанда күрделілігі айтарлықтай аз. Бұл стандартты Беларустар әрекеттен шығарды және Ресейде модификациялауға жоспарлады (онда негізгісі ретінде 128-биттік шифр "Кузнечик" қолданылатын болады), Украина өзінің ДСТУ 7624:2014 стандартын құрды. Өнімділігі тұрғысынан, ГОСТ 28147-89 басқа да тең сипаттамалар кезінде криптографиялық қорғау құралдарының күрделенуіне және қымбаттауына алып келетін AES сияқты қазіргі заманғы аналогтардан айтарлықтай кем түседі. ГОСТ-тың басқа ұлттық стандарттармен салыстырмалы талдауын қарастырайық.

Тестілеу өнімділігі бағдарланған модельдеу ерекшеліктерін криптографиялық қорғау құралдарын қажет ететін жоғары тез өзгерістерді. Салыстыру "Калина" блоктық шифрі, AES-128, AES-256, ГОСТ 28147-89, СТБ 34.101.31-2011 (Беларусь ұлттық стандарты және "Кузнечик" алгоритмі Ресей мемлекеттік стандарт жобасы үшін жүргізілді.)



3.5 Сурет –Intel Core i5, Ubuntu Linux бағдарламалық іске асырудың оңтайландырылған нұсқаларының тез әрекет етуін салыстыру



3.6 Сурет – Intel Core i7, iMac 13.2 бағдарламалық жүзеге асырудың оңтайландырылған нұсқаларының тез әрекет етуін салыстыру

Қазіргі заманғы жабдықта бағдарламалық жүзеге асыру кезінде Украинаның ұлттық стандарты әрекеті және Беларусь пен Ресей жаңа стандарттары ГОСТ 28147-89 қарағанда айтарлықтай жоғары. Қабылданған стандарт Украинада басқа шифрларды, атап айтқанда, AES, TripleDES қолдануды шектемейді және сонымен бірге қазіргі заманғы ұлттық жоғары өнімді және тұрақты криптографиялық қорғау жүйелерін құруға мүмкіндік береді.

Біз көріп отырғанымыздай, ГОСТ 28147-89 кеңестік стандарты барлық параметрлер бойынша ТМД елдері арасында басқа стандарттарына жол береді, сондықтан осы стандарттан бас тартуды және ҚР СТ 1073-2007 отандық стандартын жақсартуды ұсынамын.

ҚОРЫТЫНДЫ

Бұл жұмыста криптография саласындағы ҚР екі стандарттарын талдау арқылы олардың өзектілігі анықталды. Жұмыс барысында, ҚР СТ 1073-2007 көптеген келіспеушіліктер пайда болды және оның параметрлері қазіргі талаптарға сай емес болғандықтан бұл стандартты қайта қарау мәселесін қарастыру керек деп ойлаймын. Шет елдің стандантарттармен салыстыра отырып, өзіміздің отандық стандартты, конкурс ұйымдастыру арқылы немесе білікті мамандардың басын бірге қосып, қазіргі заманға сай стандартты жасауды ұсынамын. Менің ұстазым айтқандай: "ешқандай ел өзінің криптографиялық қорғанысын, жұмыс принциптерін, өз құпияларымен бөліспейді, бөлісседе олар өзекті емес болып шығады".

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 "ҚР Ұлттық қауіпсіздігі туралы"Қазақстан Республикасының Заңы

2 "Стандарттау туралы" ҚР Заңы

3 СТ РК 1073-2007 ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар. - Астана: мемлекеттік стандарт 2008.-30 Б.

4 Хеллман М. Е. "Криптоаналитический ымыраға арасындағы уақыт және жады бар". Ақпарат теориясы. Шілде 1980.- 401,406 Б

5 Николай Т. Куртуаның Баяндамасы. Қауіпсіздікті бағалау ГОСТ 28147-89. Халықаралық стандарттауды ескере отырып

6 Бирюков А., Шамир А. Ағынды шифрларға арналған уақыт / жад / деректердің Криптоаналитикалық компромиссері / / компьютерлік ғылымдар саласындағы дәрістер жинағы, криптология саласындағы жетістіктер - Азиякрипт 2000, 1976, 1-13 Б