ҳәм т.б. Организмде жүзеге келген бундай өзгерислер жумыс қәбилетиниң көтерилиўин тәмийинлейди.

Азанғы гигиеналық шынығыўлар адамда шаршататуғын дәрежеде аўыр болмаўы керек. Соның ушын спорттың бул түри менен шуғылланыўда адам өзиниң физикалық имканиятын есапқа алған жағдайда шуғылланыўы керек. Азанғы шынығыўларды шаршағанша орынлаў организмниң жумысқа кирисе алыў ўақтын көбейтеди, жумыс қәбилетин төменлетеди, жумыс өнимин кемейтеди.

Азанғы гигиеналық гимнастиканың әҳмийети тек уйқыдан кейин жумыс қәбилетин асырыў, жумысқа кирисип алыў ўақтын қысқартыў менен шегараланбайды. Әсиресе, үлкен жастағы адамлардың саламатлығын, шыдамлылығын, тетиклигин сақлаўда ол үлкен әҳмийетке ийе. Себеби гигиеналық гимнастика менен анық шуғылланғанда, ҳәрекет аппараты ҳәм ишки органлар жумысын басқарыў шөлкемлеседи.

Әдебиятлар

1. Ахмедов.Б.А. Жисмоний машқлар биомеханика. (Кундузги ва сиртқи бўлимда ўқийдиган талабалар учун методик қўлланма). -Тошкент: 1990.
2. Ахмедов. Б.А. Велотренажерда ишлаш. - Тошкент: 1990.
3. Алимбоева Р. Жисмоний машқлар биомеханикаси. -Тошкент: 2008.
4. Содиқов Қ. Ўқувчилар физиологияси ва гигиенаси. -Т.: «Ўқитувчи», 1992.
5. Содиқов Қ. Оилавий ҳаёт - гигиена ва ҳамда жинсий тарбия. –Т.: «Ўқитувчи», 1997.
6. Алматов К.Т. Улғайиш физиологияси. М.Улуғбек номидаги УзМУ босмахонаси. -Т.: 2004.

РЕЗЮМЕ

Организм чидамлилигини оширишнинг энг қулай усули жисмоний машқлар билан шуғулланишдир. Бу мақолада жисмоний машқларнинг организм ҳаракат аппарати (суяклар ва мушаклар) ва ички органлари (ҳазм қилиш, нафас олиш, айириш, юрак-қон томир тизими, нерв тизими, ички секреция безлари) ишларининг фаолиятини яхшилаш, ташқи ва ички муҳитнинг салбий омилларига организм чидамлилигини ошириш ҳақида маълумотлар берилган.

РЕЗЮМЕ

Наиболее эффективный метод развития выносливости организма - это заниматься физическими упражнениями. В статье даётся информация о пользе физических упражнений для улучшения деятельности опорно-двигательных аппаратов (кости и мускулы) и работы внутренних органов (пищеварение, респираторные органы, сердечно-сосудистая система, нервная система, железы внутренней секреции), развития выносливости организма к негативным факторам внешней и внутренней среды.

SUMMARY

The most effective method to develop the endurance of the organism is physical exercises. The article considers information about the benefits of physical exercises for improving the activity of the musculoskeletal system (bones and muscles) and the work of internal organs (digestive, respiratory organs, cardio - vascular system, nervous system, endocrine glands), the development of the endurance of the organism to the negative factors of external and internal environment.

Fizika. Matematika. Informatika

İNFORMACIYALARDÍ SISTEMALASTÍRÍW USÍLLARÍ

A.Abdullaev – *ekonomika ilimleriniń kandidatı, docent*
J.Juginisova - *ulken oqıtıwshı*
Ajiniyaz atındǵı Nókis mámleketlik pedagogikalıq institutı

Tayanch so'zlar: tizim, ma'lumot, ma'lumotlarni yig'ish, ma'lumotlarni saqlash, ma'lumotlarni uzatish, elektron jadval, katakcha manzili, tanlash, saralash.

Ключевые слова: система, информация, сбор информации, сохранение информации, передача информации, электронная таблица, адрес ячейки, фильтр, сортировка.

Key words: system, information, collection of information, preservation of the information, transfer of the information, electronic table, address of a cell, filter, sorting.

Hár birimiz kúndelikli turmısta informatika hám informaciyalar menen jumıs alıp baramız. Átirapımızdagı bolıp atırǵan waqıyalardı baqlaw, adamlar menen munásibette bolıw, aktual hám kúndelikli máselelerdi dodalawǵa qatnasıw, izertlew jumısların alıp barıw, hár turli eksperimentler ótkiziw ham t.b. İnformatika páni kompyuter texnologiyasınan paydalanıp informaciyalardı jıynaw, saqlaw, qayta islew hám uzatıw ámellerin uyretedi. Sonday-aq, bul pán oqıwshılardıń logikalıq pikirlewin rawajlandıradı. Mektep oqıwshıları informaciyalar ustinde joqarıdagı ámellerdi orınlaw ushın tómendegilerdi biliwi kerek:

- informaciyalar bazasın jaratıw;
- informaciyalardı tártiplestiriw (sortirovka);
- informaciyalar bazasınan kerekli dizimlerdi ajıratıp alıw (tańlaw);
- informaciyalar bazasınan sorawlar boyınsha informaciyalardı izlew;
- kiritiw hám shıǵarıwǵa tiyisli analitikalıq formalardı jaratıw.

Joqarıda aytılǵanlardı orınlaw metodikasın elektron tablicalar járdeminde ámelge asırıw MS Excel programması tiykarında iske asırıladı.

Tema. « Maǵlıwmatlardı sortlaw hám tańlaw».

Maqset: Elektron tablicada jumıs islew kónlikpelerin rawajlandırıw, bilimdi bekkemlew, sabaq barısında alınǵan nátiyjelerden paydalanıp informatika pánine oqıwshılardıń qızıǵıwshılıǵın arttırıw hám basqa pánler menen baylanıstı kusheytiw, informaciyalardı sistemalastırıw usılların uyretiw.

Metod: Kishi toparlarda ámeliy hám teoriyalıq jumıs alıp barıw.

Oqıtıw quralları: proektor, komp'yuter, elektron tablicalar.

Sabaqtıń barısı:

I. Shólkemlestiriw basqıshı. Oqıwshılar menen sálemlesip hám sabaqqa qatnastı tekserip bolǵannan keyin oqıtıwshı sabaq barısında qoyılatuǵın máselelerdi sheshiwdi hám alınatuǵın nátiyjelerdi tusindiredi. Uyge berilgen tapsırmalardı tekseriw ushın sizler berilgen sorawlarǵa juwap beriwińiz hám qaysı kishi toparǵa tiyisli ekenligińizdi, toparıńızdıń atamasın anıqlap alıw kerek ekenligin tusindiredi.

II. Texnika qáwipsizligi. Kompyuterde jumıs islewden aldın oqıwshılar texnika qáwipsizligi menen tanısıwın «Mumkin-mumkin emes» oyını járdeminde bilip aladı. Hár bir oqıwshı náwbet menen informatika kabinetinde ne islewge mumkin hám ne islewge mumkin emes ekenligin jazıp aladı.

III. Kishi toparlara bóliw. Oqıtıwshı oqıwshılardıń tórt kishi toparlarǵa bólinetuǵınlıǵın tusindiredi. Bunıń ushın oqıtıwshı A, B, C, D háripleri jazılǵan kartochkalardı tarqatıp beredi. Oqıwshılar tórt kishi toparǵa bólinedi hám ekranda kórsetilgen elektron tablicadan paydalanıp kishi toparlardıń atamaların tómendegishe izleydi:

	A	B	C	D	E
1	A	B	C	D	E
2	F	G	H	I	N
3	J	K	L	M	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z				
7					

a) A1 C3 B2 E3 C4 D2 E4 D3
b) A4 C4 E3 B2 C4 A1 D3 D3 A1
c) A1 D1 C4 E1 D4 D4
d) E5 A1 C1 C2 E1 B3 A1

IV. U'yge tapsırmanı frontal tekseriw.

Oqıtıwshı: Biz sabaq barısında isletiletuǵın tusiniklerdi, anıqlamalardı tákirarlap bilip alıwımız kerek. Ha`r bir ajıratılǵan toparǵa tapsırmalar beriledi.

№1 - tapsırma

Elektron tablica degen ne? Ol qanday elementlerden turadı? Microsoft Excel programması qanday juklenedi? Elektron tablicada baǵanalar qanday belgilenedi? Elektron tablicada qatarlar qanday belgilenedi? Yacheyka degen ne? Aktiv yacheyka degen ne? Yacheyka adresi qanday belgilenedi? Elektron tablica yacheykasına neni kiritiwge boladı?

Oqıwshılar ótilgen temalarǵa baylanıslı berilgen blic – sorawlarǵa kompyuter ekranında kórsetilgen elektron tablicadan paydalanıp juwap izley baslaydı. Durıs alınǵan juwaplar ushın kishi toparlar ball toplaydı.

V. Jańa materialdı tńsindiriw. Aktualizaciyalaw hám motivaciyalaw.

Oqıtıwshı: Elektron tablicada kóp informaciyalar saqlanıwı mumkin. Bul informaciyalar ishinen kerekli informaciyalardı izlep tabıwǵa hám dizim kórinisinde alıwǵa tuwrı keledi. Tómendegi elektron tablicada oqıwshılar haqqında informaciyalar (7 - klass)

kórsetilgen:

	A	B	C	D	E	F	G	H
1	Ana tili bali	Familiyasi,ati	Fizika bali	Informatika bali	Matematika bali	Qatar sani	Shet tili bali	Tuwilg'an jili
2	4	Asembaeva Albina	4	4	4	1	4	2000
3	5	Abdreymov Zakur	4	4	4	2	5	2001
4	4	Bayramov Islam	4	3	4	3	4	2001
5	4	Bisenbaeva Aysanem	5	4	3	4	4	2001
6	5	Dojanova Kamila	4	4	4	5	5	2001
7	5	Juginisov Azamat	3	5	5	6	5	2001
8	5	Ismaylov Nurg'ali	5	5	5	7	4	2001
9	3	Qalbaev Nurlibek	4	4	4	8	3	2001
10	4	Matkarimov Azat	5	5	5	9	4	2001
11	4	Orazimbetova Aqsu'ngil	5	3	4	10	4	2001
12	5	Su'yindikova Ayzada	4	4	4	11	5	2000
13	5	Saparniyazov Allaniyaz	5	5	5	12	5	2001
14	5	Turdimuratov Alpamis	5	5	4	13	5	2001
15	4	Utepbergenova Aziza	5	5	5	14	4	2001

Oqıwshılarǵa tablica kórinisindegi informaciyalar tarqatılǵan. Oqıtıwshı prezentaciya járdeminde informaciyalar ústinde sortlaw hám tańlaw ámelleriniń orınlanıwın kórsetedi.

Sortlaw hám tańlawda joqarıdaǵı elektron tablicadaǵı informaciyalar dizimi paydalanıladı. Bunıń ushın informaciyalar dizimi berilgen qaǵıyda boyınsha duziliwi kerek. Eger bul qaǵıydaǵa ámel qılınbasa, onda sortlaw hám tańlaw ámeli islemeydi.

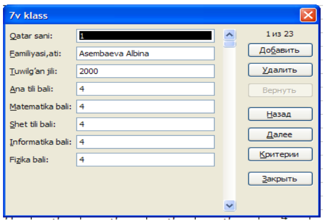
Qaǵıyda boyınsha, dizim jazıwlar (qatar) hám maydan (baǵana) lardan ibarat. Baǵanalar bir tiptegi informaciyalardan turadı. Dizim bos qatar yamasa baǵananı óz ishinde saqlamaydı. Egerde dizimde bas tema qoyılǵan bolsa, onda ol formatlanıp dizim elementlerine tásir etpeytuǵın kóriniste jazıladı.

Sortlaw yamasa tártiplestiriw (ósiw yamasa kemeyiw) sorawlar boyınsha informaciyalardı izlewdi jeńillestiredi. Sortlawdan keyin jazıwlar belgili tártipte baǵananıń mánisi (alfavit, tuwılǵan jıl, reyting ham t.b.) boyınsha ekranda sáwlelendiriledi. İnformaciyalar dizimindegi jazıwlardıń ornalasıw tártibin berilgen qaǵıyda boyınsha ózgerttiw sortlaw dep aytıladı.

Joqarıda keltirilgen elektron tablicadaǵı maǵliwmatlar dızimin Excel diń jumıs betinde payda etiw ushın baǵanalardıń atların A1-H1 adresli yacheykalarına keteklerine sáykes tırde kiritemiz. Dialog ayna járdeminde dizimdegi jaziwlar tómendegishe kiritiledi:

1.Menyudegi **Данные** bóliminen **Форма** komandasın tańlań.

2.Ekranda payda bolǵan soraw aynasınan **OK** tıymesin basıń.



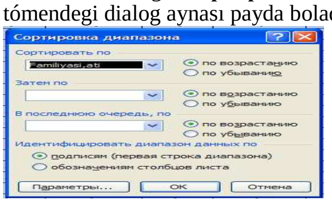
Ekranda *maǵlıwmatlar forması* nıń **7-v klass** atlı dialog aynası payda boladı.

Bul aynada dizimdegi hár bir baǵana atı menen bólimler hám bul bólimler qarsısında maǵlıwmat kiritiw ushın arnawlı aynalar keltirilgen. Aynada bólimlerdiń birewinen ekinshisine ótiw ushın klaviyaturadan [Tab] klavishasınan paydalanıladı.

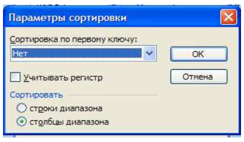
Solay etip, sıwrette keltirilgen dizimdegi maǵliwmatlardı Forma komandasınıń dialog aynası arqalı Excel diń jımıs betinde payda etemiz.

Maǵlıwmatlardı sortlaw

Dizimdegi maǵlıwmatlardıń tártipsiz jaylasıwı kerekli maǵlıwmattı tez tawıp alıwdi qıyınlastıradı. Sonıń ushın dizimdegi maǵlıwmatlardı sortlaw kerek boladı. Bunıń ushın menyuniń **Данные** bólimindegi **Сортировка** komandasın isletemiz, nátiyjede tómendegi dialog aynası payda boladı.



Keltirilgen dizimde sortlawdı **Familiyasi, ati** baǵanası boyınsha orınlaw kerek bolsın. Sortlawdı dizimniń kobi menen ısh baǵana boyınsha orınlaw mımkin. Sortlawda qosımsha parametrler **Сортировка диапозона** dialog aynasındaı **Параметры** tıymesin basıw arqalı payda bolatuǵın dialog aynasında ámelge asırıladı.



Bul jerde sortlaw dawamında bas hám kishi háriplerdi pariqlawdi **Учитывать регистр** bólimine belgi qoyıw arqalı orınlaw mımkin. Sortirovkalaw qatarı yamasa baǵanalar boyınsha ámelge asırıw sáykes turde **Сортировка диапозона** ámellerin aktivlestiriw arqalı orınlanadı. Sonday-aq, **Параметры сортировки** dialog aynası **Порядок сортировки по первому ключи** arqalı paydalanıwshıǵa sortlaw nızamın ózi beriwin támiyinleydi.

Dizimde ushırasatuǵın parametrler (baǵanalar mánisi) boyınsha informaciyalar alıw ushın tańlaw ámeli paydalanıladı. Tańlaw– bul kerek emes informaciyalardı jasırıw, kerek informaciyalardı kórsetiw.

Tańlawdıń sortlawdan ózgesheligi berilgen shárt tiykarında jazıwlar informaciyalar diziminen terip alınadı hám ekranǵa shıǵarıladı. Shártti qanaatlandırmaytuǵın jazıwlar ekranda kórinbeydi.

Dizimdi tańlaw

Dizim baǵanalarındaǵı maǵlıwmatlardı belgili tırleri boyınsha ajiratıp alıw menyudiń **Данные-Фильтр** komandası járdeminde orınlanadı. Kursordı dizimniń qálegen ketegine qoyǵan halda **Данные – Фильтр - Автофильтр** komandasın orınlaymız. Nátiyjede baǵanalar atları keteklerinde tıymeler payda boladı.

	A	B	C	D	E	F	G	H
1	Qatar sani	Familiyasi,ati	Tuwilg'an jili	Ana tili bali	Matematika bali	Shet tili bali	Informatika bali	Fizika bali
2	1	Asembaeva Albina	2000	4	4	4	4	4
3	2	Abdreymov Zakur	2001	5	4	5	4	4
4	3	Bayramov Islam	2001	4	4	4	3	4
5	4	Bisenbaeva Aysanem	2001	4	3	4	4	5
6	5	Dojanova Kamila	2001	5	4	5	4	4
7	6	Juginisov Azamat	2001	5	5	5	5	3
8	7	Ismaylov Nurg'ali	2001	5	5	4	5	5
9	8	Qalbaev Nurlibek	2001	3	4	3	4	4
10	9	Matkarimov Azat	2001	4	5	4	5	5
11	10	Orazimbetova Aqsu'ngil	2001	4	4	4	3	5
12	11	Su'yindikova Ayzada	2000	5	4	5	4	4
13	12	Saparniyazov Allaniyaz	2001	5	5	5	5	5
14	13	Turdimuratov Alpamis	2001	5	4	5	5	5

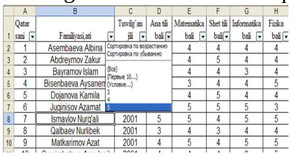
Familiyası, atı baǵanasında **8-v klass** boyınsha tańlawdi orınlap kóreyik.

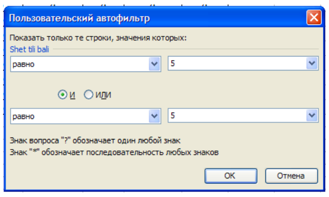
1.D1 ketegindegi tıymeni () basıń.

2.Mirát etilip atirǵan dizimdegi 5 tinıstine kursordı qoyıń.

3.Tishqanshanin shep tıymesin basıń.

Endi oqiwshılardıń ishinde ana tili boyınsha tek 5 ball toplaǵan oqıwshılar dizimi shıǵadı. Shet tilinen 5 ball toplaǵan oqıwshılardı anıqlaw ushın F1 ketegindegi () ni basıń. Kursordı usınıp atırǵan dizimdegi **Условия..** ıstine qoyıp, tishqanshanin shep tıymesin basıń. Natiyjede **Пользовательский автофильтр** atlı dialog aynası payda boladı.





1.Kursordı birinshi qatar birinshi bólimdegi tıyme ustine qoyıp tishqanshanin shep tıymesin basıń.

2.Usınılǵan dizimnen **равно** belgisin tańlań.

3.Kursordi birinshi qatar ekinshi bólimine qoyıń hám 5 dep teriń.

Nátiyjede dizimde ana tili hám shet tili pánlerinen tek 5 ball toplaǵan oqıwshılardin dizimi shıǵadı.

	A	B	C	D	E	F	G	H
1	Qatar sani	Familiyasi,ati	Tuwilg'an jili	Ana tili bali	Matematika bali	Shet tili bali	Informatika bali	Fizika bali
3	2	Abdreymov Zakur	2001	5	4	5	4	4
7	6	Juginisov Azamat	2001	5	5	5	5	3
13	12	Saparniyazov Allaniyaz	2001	5	5	5	5	5
14	13	Turdimuratov Alpamis	2001	5	4	5	5	5
18	17	Sharapova Juldiz	2001	5	5	5	5	4

Dizimnen filtrdi alıp taslap, onı jáne dáslepki halına keltiriw ushın qaytadan **Данные-Фильтр-Автофильтр** komandasın beriw jetkilikli.

№2-tapsırma.

Oqıtıwshı: Sizlerge aq qaǵaz berilgen. Usı qaǵazǵa topardı sıpatlap beretuǵın tablica jaratıń hám onı Microsoft Excel de teriń. Ajıratılǵan waqıt ishinde tez orınlaǵan kishi toparǵa ball beriledi.

VI. Bekkemlew

№3-tapsırma.

Komp'yuterge kiritilgen tablicalar tiykarında oqıwshılar ámeliy jumıstı orınlawǵa kirisedi. Proektor járdeminde oqıwshılar ózleri jaratqan tablicalar ustinde sortlaw hám fil'trlew ámellerin orınlay baslaydı. Durıs hám tez orınlaǵanı ushın toparǵa ball beriledi.

№4-tapsırma.

Taza tema boyınsha soraw. Oqıtıwshı blic-turnir isletedi: İnformaciyalardı sortirovkalaw degen ne? Fil'trlestiriw qanday orınlanadı? İnformaciyalardı sortirovkalaw hám fil'trlew ushın baǵanada

qanday informaciyalar bolıw kerek? Dizimde bos qatar yamasa baǵana bolıwı mumkin be? Durıs juwaplar ushın toparlarǵa ball beriledi.

VII. Juwmaqlaw. Sabaqtı bahalaw.

Oqıwshılar kóp ball toplaw ushın háreket etedi. Oqıtıwshı toplanǵan ballardı esaplap shıǵadı. Jeńimpaz kishi topardı hám sabaq dawamında aktiv qatnasqan oqıwshılardı xoshametleydi.

Oqıtıwshı sabaqtı juwmaqlastıradı: oqıwshılar elektron tablicada jazılǵan sózlerden ózine tiyislisin jazıp aladı hám ózine tiyisli sózlerin yacheyka adresi menen belgileydi. Ol tómendegishe:

	A	B	C	D
1	Men bildim...	Qi'zi'qli' boldi'..	Qi'yi'n boldi...	Men tapsirmani' ori'nladi'm...
2	Men o'zlestirdim...	Men sezdim, onda...	Endi men isleyin...	Men tu'sindim, onda...
3	Men u'yrendim...	Mende islendi...	Men ta'wekelshimen...	Menin' qoli'mnan keledi...
4	Meni tan' qaldi'rdi'...	Mag'an kerekli...		

VIII. tapsırma.

Temanıń tiykarǵı tusiniklerin yadlaw, sabaqlıqtaǵı temaǵa tiyisli materiallar menen islew, pánler boyınsha ulgeriw elektron tablicasın jaratıw.

Ádebiyatlar

1. Boltayev B., Azamatov A., Asqarov A., Sodiqov M., Azamatova G. Informatika va hisoblash texnikasi asoslari. -T.: «Tafakkur». 2011.
2. Ro`zieva D., Usmonboeva M., Xoltqova Z. Interfaol metodlar: mohiyati va qo`llanilishi. Metodik qóllanma. Nizomiy nomidagi TDPU. -T.: 2013.
3. Qasımov M., JuginisovaJ., Il yasova Z. MS Excel dástńrinde funkciyalardıń grafiklerin jasaw metodikası. Metodikalıq qollanba. -N.: 2015.

REZYUME

Maqolada ma’lumotlarni tizimlashtirishning ilmiy metodik muammolari ko`rib chiqilgan. MS Excel dasturi yordamida ma’lumotlarni elektron jadval ko’rinishida saqlash usuli ko`rib chiqilgan. Amalda 8-sinfda o’qitiladigan mavzularga doir dasturlashtirish ko’rib chiqilgan. Unda saralash va tanlash usullari kiritilgan. Maqolada ma’lumotlarni tizimlashtirishning innovatsion texnologiyasi yaratilgan.

РЕЗЮМЕ

В статье излагаются вопросы научно-методического обеспечения систематизации информации. Описывается алгоритм сохранения информации в виде электронной таблицы на базе MS Excel. Полученные результаты используются в 8-классе, которые соответствуют теме сортировки и фильтрации информации. В работе разработаны инновационные технологии систематизации информации.

SUMMARY

The article deals with the issues of scientific-methodical supply of the information systematization. The author describes the algorithm of preservation of the information in the form of an electronic table on the basis of MS Excel. The received results are used in the 8-th form, they correspond to themes of sorting and filtration of the information. There have been worked out innovative technologies of systematization of the information.

ЗАМОНАВИЙ КРИПТОГРАФИК АЛГОРИТМЛАР УЧУН КАТТА ТУБ СОНЛАРНИ ГЕНЕРАЦИЯЛАШ МАСАЛАЛАРИ

Ш.Б.Норматов - *катта ўқитувчи*

ТАТУ Қарши филиали

Таянч сўзлар: ахборот хавфсизлиги, криптография, туб сонлар, шифрлаш алгоритмлари, сонларни тубликка текшириш.
Ключевые слова: информационная безопасность, криптография, простые числи, алгоритмы шифрование, проверка числа на простоту.
Key words: information security, cryptography, prime numbers, encryption algorithms, verification of the simplicity.

Кириш. Ахборот-коммуникацион технологияларининг кун сайин ривожланиб бориши ахборот хавфсизлиги муаммосининг долзарблилигини янада ошириб юбормоқда. Бу эса ахборот хавфсизлигини таъминлашга қаратилган турли хил янги усуллар ва воситаларни яратиб боришни тақозо этади. Маълумки, ахборот хавфсизлигини ишончли таъминлаш бу масалага комплекс ёндашувни талаб қилади. Яъни, ахборотларни ҳимоялашнинг ҳуқуқий, ташкилий ва муҳандислик-техник таъминотларидан самарали фойдаланиш зарурлигини кўрсатади.

Жумладан, ахборотларни ҳимоялашда криптографик усулларнинг ҳам салмоқли ўрни бор. Бу соҳада ҳам мамлакатимизда қатор ислоҳотлар амалга оширилмоқда. Бунинг тасдиғи сифатида Ўзбекистон Республикаси Президентининг 2007 йил 3 апрелдаги «Ўзбекистон Республикасида ахборотни криптографик муҳофазасини ташкил қилиш чора-тадбирлар тўғрисида» ПҚ 614-сонли, Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги «Ахборотни криптографик муҳофаза қилиш воситаларини лойиҳалаштириш, ишлаб чиқиш, сотиш, таъмирлаш ва ишлатишни лицензиялаштириш тўғрисидаги низомни тасдиқлаш тўғрисида» ВМҚ 242-сонли қарорлари, маълумотларни шифрлаш, хэш функциялар бўйича давлат стандартларининг қабул қилинишида кўриш мумкин.

Мавжуд криптотизимларнинг барчаси бирор бир криптографик алгоритм асосида ишлайди. Ҳозирда кўпгина криптографик стандартларга асос сифатида олинаётган *RSA*, *El-Gamal* алгоритмлари асосида амалий жиҳатдан ечиш етарли даражада мушкул бўлган берилган сонни иккита туб кўпайтувчи шаклида ифодалаш ва чекли майдонда дискрет логарифмни ҳисоблаш масалалар ётади.

Юқорида келтирилган ҳар иккала алгоритмда ҳам маълумотларни шифрлашда, электрон рақамли имзони яратишда 1024 битли ва ундан ҳам катта туб сонлардан фойдаланилади. Шунинг учун ҳам катта туб сонлар билан ишлаш, уларни генерация қилиш криптографиянинг асосий масалаларидан бирига айланиб улгурган. Умуман криптографияда туб сонларнинг кенг қўлланилишини улар сир тутилганда топишнинг қийинчилиги билан боғлаш мумкин.

Асосий қисм. Фақат ўзига ва 1 га бўлинадиган сонлар туб сонлар дейилади [4]. Қадимдан натурал сонлар қаторида туб сонларни топиш йўллари билан кўпгина олимлар шуғулланганлилига қарамасдан ханузгача борор оралиқдан фақатгина туб сонларни генерация қиладиган функция топилмаган [1]. Чунки туб сонларни бошқа сонлар асосида ифодалаб бўлмайди. Яъни, уларни бир неча соннинг кўпайтмаси шаклида ёзиш мумкин эмас. Бундан ташқари туб сонлар натурал сонлар қаторида текис тақсимланмаган. Туб сонларнинг сони чексиз кўп. Яъни улардан исталганча фойдаланиш мумкин. Лекин сонлар қаторида кам учрайди.

Бирор оралиқдаги барча сонлар ҳамда шу оралиқдаги туб сонларнинг сонини баҳолаб кўрайлик. Мисол сифатида иккилик саноқ системасидаги 32 разрядли сонларни қараймиз.

32 разрядли энг катта сон $2^{32}-1$. 31 разрядли энг катта сон $2^{31}-1$. Барча 32 разрядли сонлар сонини қуйидагича ҳисоблаш мумкин:

$$(2^{32}-1)-(2^{32}-1)=2^{32}-1-2^{31}+1=$$

$$=2^{32}-2^{31}=2^{31}(2^{1}-1)=2^{31}=2147483648$$

Энди бу сонлар орасидаги туб сонлар сонини ҳисоблаймиз. Лежандр формуласига асосан [2] n разряддан ошмаган туб сонлар сонини қуйидагича баҳолаш мумкин:

$$\frac{n}{\ln n}=\frac{(n-1)}{\dfrac{\log_2(n-1)}{\log_2 e}}=\frac{\log_2 e\times(n-1)}{\log_2(n-1)}$$

32 разряддан ошмаган туб сонлар сони қуйидагича ҳисоблаш мумкин:

$$\frac{2^{32}}{\ln(2^{32})}=\frac{2^{32}}{\dfrac{\log_2(2^{32})}{\log_2 e}}=\frac{\log_2 e\times 2^{32}}{\log_2(2^{32})}=$$

$$=1.44\times\frac{2^{32}}{2^{5}}\approx 193273528$$

(Бу ерда $2^{32}-1$ ни 2^{32} деб ҳисобладик).

31 разряддан ошмаган туб сонлар сони эса қуйидагича:

$$\frac{2^{31}}{\ln 2^{31}}=\frac{2^{31}}{\dfrac{\log_2(2^{31})}{\log_2 e}}=\frac{\log_2 e\times 2^{31}}{\log_2(2^{31})}=1.44\times\frac{2^{31}}{31}=$$

$$=1.44\times\frac{2^{31}}{2^{5}}\approx 99754079$$

Демак, 32 разрядли туб сонлар сони $193273528-99754079=93519449$ га тенг экан. Бундан оралиқдаги ҳар 30 та сонинг биттаси туб сон бўлади деган хулосага келиш мумкин.

32 битли сонни қуйидагича ифодалашимиз мумкин: