



**Коммерциялық емес  
акционерлік  
қоғам**

АЛМАТЫ ЭНЕРГЕТИКА  
ЖӘНЕ БАЙЛАНЫС  
УНИВЕРСИТЕТІ

Қазақ және орыс тілдері  
кафедрасы

## **КӘСІБИ ҚАЗАҚ ТІЛІ**

5В100200- Ақпараттық қауіпсіздік жүйесі мамандығының студенттеріне  
арналған әдістемелік нұсқаулықтар

Алматы 2014

Құрастырушы: Ахметова Эльмира Тұрсыновна, Әлмұхаметова Гүлмира Сатыбалдиевна. Кәсіби қазақ тілі. 5В100200 – Ақпараттық қауіпсіздік жүйесі мамандығының студенттеріне арналған әдістемелік нұсқаулықтар. - Алматы: АЭЖБУ, 2014. - 33 б.

Ұсынылып отырған әдістемелік нұсқаулық «Кәсіби қазақ тілі» пәні бойынша «Ақпараттық қауіпсіздік жүйелері» мамандығында оқитын студенттерге арналған. Әдістемелік нұсқаулықты жазудағы басты мақсат – мемлекеттік тілді кәсіби бағдарлы үйрету арқылы техникалық терминдердің мағынасын түсіндіріп меңгерту және оларды қолдану дағдысын қалыптастыру.

Кесте - 3. Сурет-2.

Пікір беруші: аға оқытушы С.Б.Абдрешова

«Алматы энергетика және байланыс университеті» коммерциялық емес акционерлік қоғамының 2014 жылғы жоспары бойынша басылады.

## Алғы сөз

Бүгінде жоғары оқу орындарында, әсіресе техникалық жоғары оқу орындарында мемлекеттік тілді оқыту сапасының деңгейін көтеруге, кәсіби тілді меңгеруге байланысты жұмыстар жүргізу күн тәртібіндегі өзекті мәселеге айналды.

Ұсынылып отырған әдістемелік нұсқаулық «Кәсіби қазақ тілі» пәні бойынша «Ақпараттық қауіпсіздік жүйелері» мамандығында оқитын студенттерге арналған. Әдістемелік нұсқаулықты жазудағы басты мақсат – мемлекеттік тілді кәсіби бағдарлы үйрету арқылы техникалық терминдердің мағынасын түсіндіріп меңгерту және оларды қолдану дағдысын қалыптастыру. Әдістемелік нұсқаулықта мамандыққа қатысты терминдердің жасалу жолдары, терминдердің мағынасын түсіндіруге септігін тигізетін тапсырмалар, кәсіби сала мәтіндері берілген. Сөздіктермен, салалық сөздіктермен жұмыс жасау дағдыларын қалыптастыру, лексикалық, синтаксистік оралымдарды танып, дұрыс аудару білу дағдыларын меңгерту, техникалық мәтіндерді қазақшадан орысшаға және орысшадан қазақшаға аудару тәсілдерін нақты мәтіндер үлгісін қолдана отырып игертудің тиімді жақтары қарастырылды. Әдістемелік көрсеткіште берілген материалдар студенттердің кәсіптік мамандығын ескере отырып қазақ тілін қарым-қатынас құралы ретінде меңгертуге септігін тигізеді деген ойдамыз.

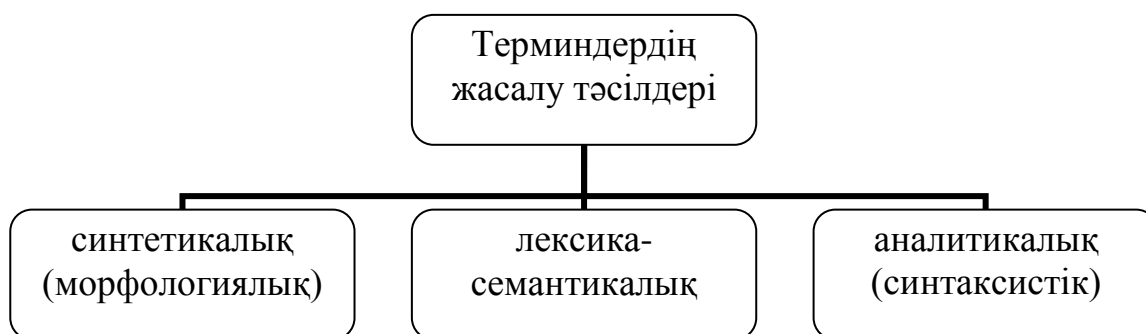
## 1 Терминдер және олардың жасалу тәсілдері

Термин (лат. *terminus* шек, шекара) – ғылым, техника, өндіріс, өнер саласындағы белгілі бір ұғымды атау үшін қолданылатын сөздер мен сөз тіркестері.

Терминжасам тілдің сөзжасам жүйесінің бір тармағы болғандықтан, ол сөзжасамның жалпы заңдылықтарын сақтайды. Олай болса терминжасамда сөзжасамның тәсілдері қолданылады.

Техника терминдерінің сөзжасамдық тәсілдері төмендегідей бөлінеді (1-кестені қараңыз).

1 кесте –Техника терминдерінің сөзжасамдық тәсілдері



1-тапсырма. Мәтіннен термин сөздерді теріп жазыңыз (7-8 термин), олардың түсіндірме сөздігін жасаңыз .

*Үлгі: Ақпаратты қорғау- ақпаратты қорғауға бағытталған кешен.*

### 1.2 Ақпараттық қауіпсіздік және оның құрамдас бөліктері

Ақпарат (лат. *informatio* — түсіндіру, мазмұндау) ұғымы күнделікті өмірден бастап техникалық салада пайдаланылатын көп мағыналы ұғым. Жалпы алғанда бұл ұғым шектеу, байланыс, бақылау, форма, инструкция, білім, мағына, құрылым, бейнелеу, сезіну тағы басқа ұғымдармен тығыз байланысты. Ақпараттық қоғам, ақпараттық технологиялар, тіпті информатика, ақпарат ғылымы және компьютер ғылымы назарға көп түсуде, ал "ақпарат" сөзі білдіре бастаған мағыналары ұқыпсыз пайдаланылуда. Ақпараттық технологиялардың дамуы, оларды адам қызметтерінде кең пайдалануы жыл сайын ақпараттық қауіпсіздік проблемаларының өзектілігін және бірегей күрделілігін анықтайды.

Ақпаратты өңдеу технологиялары үздіксіз жетілдірілуде, ал сонымен бірге күнделікті ақпараттық қауіпсіздікті қамтамасыз ету әдістері де өзгеруде. Шынында, әмбебапты қорғау әдістері жоқ, нақты жүйеге қауіпсіздік механизмдерді жасау барысында жетістіктер жүйенің ерекшеліктеріне байланысты. Практикада қорғау жүйелерін жасауда оларды іске асыру кезінде техникалық ерекшеліктеріне тәуелді емес жалпы заңдылықтар есепке

алынады. Осындай әмбебапты принциптер ақпараттық қауіпсіздікті жеке ғылыми пән ретінде ерекшелейді.

Ақпаратты шындығында да ғылыми ұғым ретінде қарастыруға болады. Өйткені бұған дейін ақпараттың құрылымы мен қасиеттері барлық ғылым салаларында зерттелді. Мысалы, физика - ақпарат таситын сигналдардың қасиеттерін зерттейді. Табиғаттағы көптеген құбылыстардың сигнал шығаратыны белгілі.

Сонымен ақпарат — бұл ақпараттық процесс барысында түзілетін қозғалыстағы объект. Ақпараттың қасиеттері мәліметтердің қасиеттеріне де, әдістердің қасиеттеріне де тікелей тәуелді.

Ақпаратты қорғау — ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп деректерді енгізу, сақтау, өңдеу және тасымалдау үшін қолданылатын ақпарат пен қорлардың тұтастығын, қол жеткізулік оңтайлығын және керек болса, жасырындылығын қолдауды түсінеді.

2-тапсырма. Берілген сөз тіркестерінен сөйлем құраңыз.

*Ақпараттық қозғам, ақпараттық технологиялар, ақпараттық қауіпсіздік, қауіпсіздікті қамтамасыз ету, тәжірибе жүзінде, қорлардың тұтастығы, проблеманың өзектілігі.*

## 2 Синтетикалық тәсіл

Техника саласына байланысты терминдердің *синтетикалық тәсілі*, яғни сөз тудырушы жұрнақтар арқылы термин жасау маңызды орын алады. Сол себептен болар сөзжасамның бұл тәсілі қазақ тіл білімінде кеңінен зерттелген.

Техника терминдерін тудырушы жұрнақтардың белсенділік деңгейі әртүрлі. Мәселен:

*-ғыш, -гіш, -қыш, -кіш* жұрнақтары арқылы көптеген терминдер қалыптасқан. Бұл жұрнақтар термин жасауда өнімді жұрнақтардың қатарынан табылды. Мысалы: *сақтандырғыш, көрсеткіш, түрлендіргіш*. Атаулы жұрнақтардың көмегімен жасалған терминдер жоғарыда келтірілген мысалдардан орыс тіліндегі *-тель* суффиксімен жасалған қосымшаларға сәйкес келетінін байқау қиын емес.

*-лық, -лік, -дық, -дік, -тық, -тік* жұрнақтары арқылы *қолжетерлік, оңтайлық, тұтастық, жасырындылық, қауіпсіздік, ақпараттық* т.б. терминдер қалыптасқан. Бұл жұрнақтар зат есім, сын есім тұлғалы сөздерге жалғану арқылы жаңа термин атауы жасалып тұр.

1-тапсырма. Мәтіннен синтетикалық тәсіл арқылы жасалған термин сөздерді тауып, жасалу жолдарына назар аударыңыз.

## 2.1 Ақпарат қорғау жүйесін жобалау негіздері

Ақпаратты қорғау – ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп деректерді енгізу, сақтау, өңдеу және тасымалдау үшін қолданылатын ақпарат пен қорлардың тұтастығын, қол жеткізулік оңтайлығын және керек болса жасырындылығын қолдауды түсінеді. Сонымен, ақпаратты қорғау – ақпараттың сыртқа кетуінің, оны ұрлаудың, жоғалтудың, рұқсатсыз жоюдың, өзгертудің, маңызына тимей түрлендірудің, рұқсатсыз көшірмесін алудың, бұғаттаудың алдын алу үшін жүргізілетін шаралар кешені. Қауіпсіздікті қамтамасыз ету кезі қойылатын шектеулерді қанағаттандыруға бағытталған ұйымдастырушылық, бағдарламалық және техникалық әдістер мен құралдардан тұрады.

Ақпараттық қауіпсіздіктің өте маңызды 3 жайын атап кетуге болады: қол жеткізерлік (оңтайлық), тұтастық және жасырындылық.

*Қол жетерлік (оңтайлық)* – саналы уақыт ішінде керекті ақпараттық қызмет алуға болатын мүмкіндік. Ақпараттың қол жеткізерлігі – ақпараттың, техникалық құралдардың және өңдеу технологияларының ақпаратқа кедергісіз қол жеткізуге тиісті өкілеттігі бар субъектілердің оған қол жеткізуін қамтамасыз ететін қабілетімен сипатталатын қасиеті.

*Тұтастық* – ақпараттың бұзудан және заңсыз өзгертуден қорғанылуы. Ақпарат тұтастығы деп ақпарат кездейсоқ немесе әдейі бұрмаланған кезде есептеу техника құралдарының немесе автоматтандырылған жүйелердің осы ақпараттың өзгермейтіндігін қамтамасыз ететін қабілетін айтады.

*Жасырындылық* – заңсыз қол жеткізуден немесе оқудан қорғау.

*Қауіпсіз жүйе* – белгілі бір тұлғалар немесе олардың атынан әрекет жасайтын үрдістер ғана ақпаратты оқу, жазу құрастыру және жою құқығына ие бола алатындай етіп ақпаратқа қол жеткізуді тиісті құралдар арқылы басқаратын жүйе.

*Сенімді жүйе* - әр түрлі құпиялық дәрежелі ақпаратты қатынас құру құқығын бұзбай пайдаланушылар тобының бір уақытта өңдеуін қамтамасыз ету үшін жеткілікті аппаратық және бағдарламалық құралдарды қолданатын жүйе. Жүйенің сенімділігі (немесе сенім дәрежесі) екі негізгі өлшеме бойынша бағаланады: қауіпсіздік саясаты және кепілділік.

2-тапсырма. Дұрыс сәйкестігін табыңыз.

1	қолжетерлік	1	Целостность
2	жасырындылық	2	Надежная система
3	тұтастық	3	Информационная безопасность
4	сенімді жүйе	4	Доступность
5	қауіпсіз жүйе	5	Блокировка информации
6	ақпараттық қауіпсіздік	6	Конфиденциальность
7	ақпараттың жасырындылығы	7	Безопасная система
8	ақпараттың сыртқа кетуі	8	Утечка информации
9	ақпаратты бұғаттау	9	Обеспечение безопасности

### 3 Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен міндеттері

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі мақсаттары: ақпарат қорғаудың ұлттық жүйесін, оның ішінде мемлекеттік ақпараттық ресурстарды құру және нығайту; мемлекеттік ақпараттық ресурстарды, сондай-ақ ақпарат саласында адам құқықтары мен қоғам мүдделерін қорғау.

Қазақстанның ақпараттық тәуелділігін, басқа мемлекеттер тарапынан ақпараттық өктемдікті немесе тосқауылды, Президенттің, Парламенттің, Үкіметтің және басқа да мемлекеттік органдар мен ұйымдардың ақпараттық оқшаулануын төмендету немесе оған жол бермеу болып табылады. Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі негізгі міндеттер:

- ақпараттық қауіпсіздік саласында ұлттық заңнаманы жетілдіру;
- ақпараттық қауіпсіздік қатерлерінің көздерін анықтау, бағалау, болжау;
- ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік органдар мен ұйымдардың қызметін құқықтық реттеу және үйлестіру;
- Қазақстанның жаһандық ақпараттық желілер мен жүйелерді құру және пайдалану процестеріне белсенді қатысуын қамтамасыз ету.

1-тапсырма. Берілген мәтінді аударыңыз.

2-тапсырма. Мәтінге сұрақтар қойыңыз.

3- тапсырма. Берілген сөздер мен сөз тіркестерін қатыстырып сөйлем құраңыз:

Ұлттық жүйе, мемлекеттік ақпараттық ресурстар, адам құқығын қорғау, қауіпсіздік шаралары.

### 4 Лексика-семантикалық тәсіл

*Лексика-семантикалық тәсілде* сөздің құрамы, тұлғасы ешбір өзгеріске түспейді, өзгеріс тек сөздің мағынасында ғана болады. Сөз дыбыстық, морфемдік құрамын сақтай отырып, тілдегі бұрынғы қолданылып жүрген мағынасының үстіне жаңа мағына қосып алады, тілде жаңа мағынасында да қолданыла бастайды. Сөздің тек мағынасында өзгеріс болғандықтан, бұл тәсіл лексика-семантикалық тәсіл аталған. Мысалы, ақпарат саласындағы *көз*, *қор*, *шама*, *өріс*, *желі* т.б. терминдердің мағыналары тілдегі түрлі қолданыста қалыптасқан (2 кесте).

2кесте – Терминжасамның лексика-семантикалық тәсілі

Мысал	Мағыналары	Ақпарат қауіпсіздігі саласына байланысты мысалдар
көз	1) көру мүшесі; 2) бір нәрсенің шығар жері, қойнауы.	Ақпарат көзі, жарық көзі
қор	1) мол жиналған қазына, байлық; 2) бір нәрсенің жиналып қалған запасы.	ұлттық қор, деректер қоры
желі	1) негіз, арқау, өзек; 2) байланыс, жалғастық, сабақтастық.	ақпарат желісі, компьютерлік желілер

#### **4.1 Қазақстан Республикасының ақпараттық қауіпсіздігінің жай-күйі**

Қазіргі уақытта Қазақстанның саяси өміріндегі және экономикасындағы болып жатқан қайта құру процестері оның ақпараттық қауіпсіздігінің жай-күйіне тікелей әсерін тигізеді. Бұл ретте ақпараттық қауіпсіздіктің нақты жай-күйін бағалау және осы саладағы негізгі проблемалар мен бағыттарды айқындау кезінде ескеруді қажет ететін жаңа факторлар туындайды.

Көрсетілген факторларды саяси, экономикалық және ұйымдастырушылық-техникалық деп бөлуге болады.

Саяси факторлар:

Әлемнің түрлі өңірлерінде геосаяси жағдайдың өзгеруі; әлемдік саяси, экономикалық, әскери, экологиялық және басқа да процестердің жаһандық мониторингін жүзеге асыратын, ақпаратты тарататын әлемнің дамыған елдерінің ақпараттық өктемдігі; ішкі саяси дағдарыстардың туындауы: билік тармақтары арасындағы, аумақтық мемлекеттік құрылым субъектілері арасындағы жанжалдар, қорғалатын тұлғаларға қастандық жасалуы; реформалар жүргізу процесінде Қазақстанның шетелдермен неғұрлым тығыз ынтымақтастық жасауға ұмтылуы; терроризм және экстремизм, криминогенді жағдайдың ушығуы, әсіресе кредит-қаржы саласында компьютерлік қылмыстар санының өсуі болып табылады.

Экономикалық факторлар арасында:

Қазақстанның дүниежүзілік экономикалық кеңістікке белсенді кіруі, көптеген отандық және шетелдік мемлекеттік емес құрылымдардың - ақпаратты өндірушілер мен тұтынушылардың, ақпараттандыру және ақпаратты қорғау құралдарының пайда болуы, ақпараттық өнімнің тауарлық қатынастар жүйесіне қосылуы; бүкіл әлемдегі экономикалық процестердің дамуына әсерін тигізетін коммуникациялық жаһандану.

Ұйымдастырушылық-техникалық факторлардың ішінен мыналар айқындаушы болып табылады: ақпараттық қатынастар саласында, оның ішінде ақпараттық қауіпсіздікті қамтамасыз ету саласында, нормативтік құқықтық базаның жеткіліксіздігі; мемлекеттің Қазақстандағы



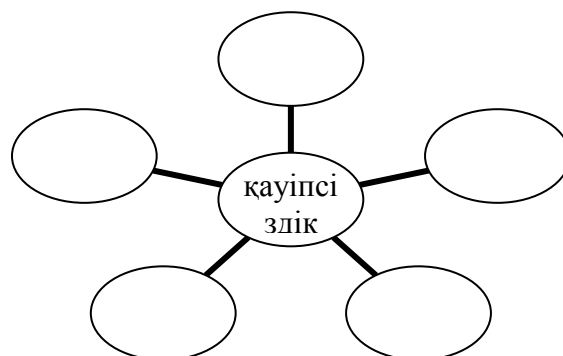
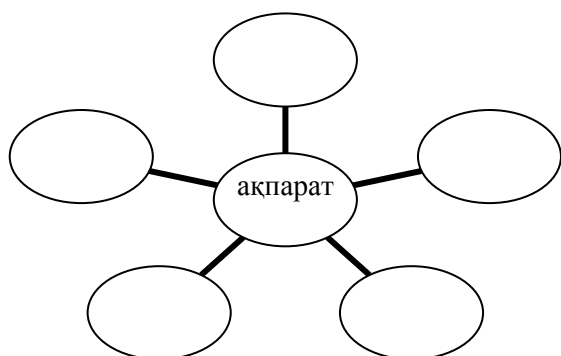
ақпараттандыру құралдары, ақпараттық өнімдер мен қызмет көрсетулер нарығының жұмыс істеу және даму процестерін нашар реттеуі; ақпаратты сақтау, өңдеу, беру және қорғау үшін мемлекеттік басқару саласында, кредит-қаржы және басқа салаларда ақпараттың сыртқа шығып кетуінен және сыртқы әсерден қорғалмаған импорттық техникалық және бағдарламалық құралдардың кеңінен пайдаланылуы; Қазақстандағы ақпараттық қауіпсіздіктің қазіргі жай-күйін талдау оның қазіргі заманғы деңгейінің адам, қоғам және мемлекет қажеттіліктеріне сәйкес келмейтінін көрсетті.

Ақпаратты қорғау саласында кәсіби мамандар сандарының жеткіліксіздігі республикада ақпараттық қауіпсіздікті ұйымдастыруға кері әсерін тигізеді.

1-тапсырма. Мәтіннен синтетикалық тәсіл арқылы жасалған термин сөздерді табыңыз, аударыңыз.

2-тапсырма. Сөз тіркестерін құрастырыңыз.

Үлгі: ақпарат көзі; қауіпсіздік техникасы.

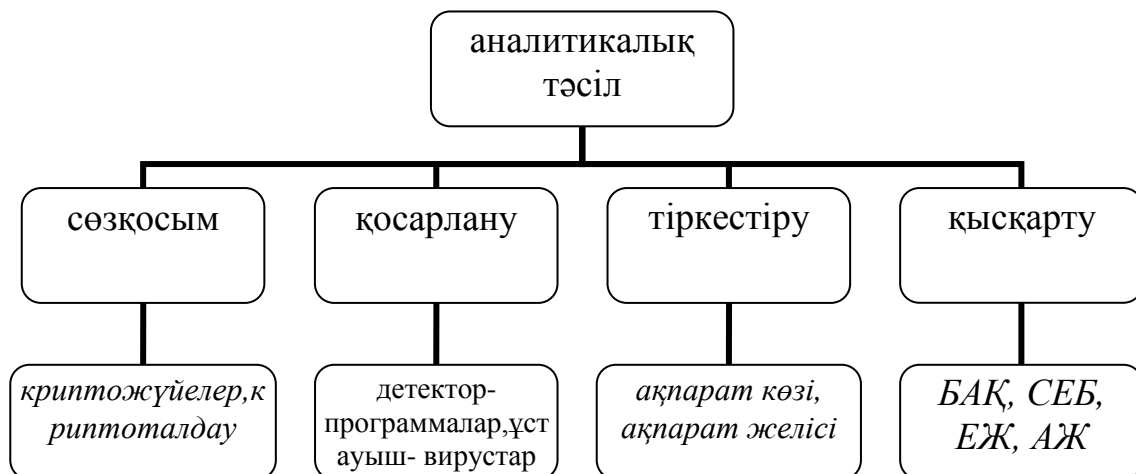


## 5 Аналитикалық тәсіл

Сөзжасамның аналитикалық тәсілі, яғни сөздердің тіркесуі, бірігуі, қосарлануы, қысқартылуы арқылы термин атауын жасау терминологияда өнімді тәсілдердің бірі болып табылады.

Техника терминдерінің *аналитикалық тәсілі* тірек-сызба негізінде берілді (3 кесте).

3 кесте – терминжасамның аналитикалық тәсілі



## 5.1 Ақпараттық қауіпсіздіктің жай-күйін бағалау

Ел президентінің 1997 жылдың 10 қазандағы « Қазақстан 2030 », барлық қазақстандықтардың өсіп - өркендеуі, қауіпсіздігі және әл – ауқатының артуы атты Қазақстан халқына жолдауында ұзақ мерзімді басымдық ретінде ұлттық қауіпсіздік айқындалды, оның құрамының бірі ақпараттық қауіпсіздік болып табылады.

Қазіргі уақытта Қазақстанның саяси өміріндегі және экономикасындағы болып жатқан қайта құру процестері оның ақпараттық қауіпсіздігінің жай-күйіне тікелей әсерін тигізеді. Бұл ретте ақпараттық қауіпсіздіктің нақты жай-күйін бағалау және осы саладағы негізгі проблемалар мен бағыттарды айқындау кезінде ескеруді қажет ететін жаңа факторлар туындайды.

Компьютерлер – ақпараттық жүйені қалыптастырушылардың бірі, бірақ біздің назарымыз бірінші орында ақпаратқа негізделеді, компьютердің көмегімен сақталатын, өңделетін және жіберілетін ақпараттарды қарастыра аламыз.

Қазақстанның ақпараттық қауіпсіздігіне төнген қауіп-қатер деңгейі өте жоғары. XX ғасырдың соңындағы ақпарат кеңістігіне қарағанда XXI ғасырдағы ақпарат кеңістігін айтарлықтай үлкен дәрежеде өсті. Бұрындары «ақпарат ағымы» дейтін болсақ, бүгін «ақпарат тасқыны», «ақпарат мұхиты» деп жиі атайтын болдық. ҚР 1998 жылғы заңында «Ақпараттық қауіпсіздік – мемлекеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай-күйі» деп аталса, 2012 жылғы заңда «*Ақпараттық қауіпсіздік – елдің орнықты дамуы және ақпараттық тәуелсіздігі қамтамасыз етілетін, ақпарат саласындағы нақты және ықтимал қауіп-қатерлерден Қазақстан Республикасы ақпараттық кеңістігінің, сондай-ақ адамның және азаматтың құқықтары мен мүдделерінің, қоғам мен мемлекеттің қорғалуының жай-күйі*» деп көрсетіледі.

1-тапсырма. Мәтін мазмұнын өз сөзіңізбен баяндаңыз, мәтінде берілген ақпаратқа пікіріңізді білдіріңіз.

2-тапсырма. Мәтінді қазақ тіліне аударыңыз.

*Информационная безопасность сегодня стала стратегической категорией, состоящей из таких комплексных понятий, как «международная безопасность» и «национальная безопасность». Она может рассматриваться в аспекте социально-экономического развития как политика, проводимая в целях сохранения и защиты технической и языковой информации, влияния информационных потоков на массовое и индивидуальное сознание, мониторинга и классификации компьютерных и сетевых угроз и предупреждения информационных войн.*

## **6 Аббревиатуралар**

Аббревиатура (лат. *ab* – бастапқыдан, *brevio* – қысқарту) – қысқартылып жазылатын сөз тіркесі. Аббревиатураның 2 түрі бар.

*Инициалдық аббревиатура.* Бұл – қысқартылып жазылған сөз тіркесіндегі басқы әріптерден немесе дыбыстардан ғана құралған аббревиатура. Мысалы: *БАҚ* (Бұқаралық апарат құралдары), *АЖ* (Ақпараттық жүйелер), *СЕБ* (Сенімді есептеу базасы).

*Буындық аббревиатура* (күрделі қысқартылған сөз). Бұл – сөз тіркесіндегі сөздердің бастапқы буындарынан немесе алғашқы сөздегі бастапқы буын мен соңғы сөздің тұтастай тіркестірілуінен құралатын, басқа да жолдармен жасалатын аббревиатура. Мысалы: *ұжымшар* (ұжымдық шаруашылық), *ҚазТАГ* (Қазақ телеграф агенттігі), *автокөлік* (автомобиль көлігі).

### **6.1 ХХІ ғасыр – ақпарат ғасыры**

Бүгінде кейбір мемлекеттер экспериментті түрде ақпарат арқылы кез келген елді қарусыз санасын жаулап, өлтірмей жанын алуға әбден болатынын дәлелдеді. Адамдар қайда жүрсе де ақпараттың құрсауына оралуда. Қоғам бар жерде, мемлекет бар жерде ақпараттық шабуыл үнемі жасалады. Бір қарағанда, бұқаралық ақпарат құралдарымен құлаққа кіріп, санаға сіңген ақпарат кішігірім қоғамда, мемлекетте, тіпті тұтастай әлемде қаруы жоқ соғыстың өршуіне себепкер болатынына куә болдық.

Ақпараттық соғыстың басты мақсаты–қарсы жақты өз ыркына мәжбүрлеп көндіру арқылы өз мүддесіне сәйкес келетін саяси, экономикалық, әскери, әлеуметтік ұтысқа қол жеткізу. Мұндай соғыс мемлекеттер, одақтар, қоғамдық, экономикалық және әскери құрылымдардың арасында жүргізіледі. Ақпараттық соғысты кейбір ғалымдар «психологиялық соғыспен» де теңестіріп жатады. Ең қызығы, бұл қарусыз майданда «кімнің жау» екенін ажырату өте қиынға түседі. Психологиялық шаралар, электрондық соғыс шаралары, теріс ақпарат тарату мен қарсы үгіт-насихат шаралары, қарсы

әрекет ету мен қауіпсіздікті қамтамасыз ету шаралары, тікелей ақпараттық шабуылдар мемлекеттер мен ірі державалар арасындағы ақпараттық теке-тірестің өршуіне негізгі себеп болады.

Ақпараттық қауіпсіздікті қамтамасыз етпеудің зардабы зор.

Ақпараттық тәуелсіздік - бұл ақпараттық қауіпсіздікке жетудің бірден-бір жолы. Бүгінгі ақпараттық ғасырымыздың талабы осы болып тұр. Әлемдік тәжірибеге сүйенсек, өркениетті елдерде әр ел өз аумағына сырттан таралатын БАҚ-ты мемлекеттік заң тұрғысынан реттеп отырады. Өзге елдік БАҚ-ты 20 пайыздық шектен асырмайды. Егер, одан асса мемлекеттің ақпараттық қауіпсіздігіне нұқсан келтірілген болып саналады.

1-тапсырма. Сөздіктің көмегімен мәтінді аударыңыз.

2-тапсырма. Мәтіндегі аббревиатураларды теріп жазыңыз, қосымша аббревиатураның екі түрі бойынша өз мысалдарыңызды келтіріңіз (5- 10 мысал).

## **7 Әлеуметтік желілер – мемлекеттің ақпараттық қауіпсіздігінің объектісі**

Қазіргі елімізде ақпараттық қорғау құру процесі қарқынды жүріп жатқан жағдайда ақпарат, ақпараттық байланыстар қоғамның кез-келген саласының негізгі өзегіне айналып отыр. Ақпараттық байланыстар саяси жүйенің қан тамыры секілді, оның құрамдас бөліктері мен элементтеріне нәр береді, өзара байланысын, іс-қимылын қамтамасыз етіп отырады. Басқаша айтқанда, саяси жүйенің, оның құрамдас бөліктерінің дұрыс қызмет атқаруы ақпараттың объективтілігіне, нақтылығына, дер кезінде жетуіне тікелей тәуелді.

Демек, кез-келген мемлекеттің, ондағы мемлекеттік басқару формаларына қарамастан, оның саяси жүйесінің барлық құрамдас бөліктерінде (саяси институттар, саяси қатынастар, саяси нормалар мен принциптер, саяси сана мен саяси мәдениет) ақпараттың қалыптастырушы, үйлестіруші, байланыс факторы ретінде алатын орны ерекше болмақ және ол дами бермек. Өйткені ақпараттық технологиялардың, ақпарат таратудың жана әдістерінің, соның ішінде бүгінгі күні Қазақстанда ресми түрде бұқаралық ақпарат құралдарына теңестірілген Интернет желісінің дамуымен бірге саяси жүйенің коммуникативтік қызметі де жандана түседі.

Мемлекеттік билік те бұл жаңалықтарға қызығушылық танытып, соның нәтижесінде «электрондық үкімет», «электрондық әкімдік», «электрондық партия», «электрондық университет» сияқты жаңа жобалар, ақпараттық-коммуникациялық саяси институт туындады. Сонымен бірге ақпаратты өндіру-тарату процесі мен компьютерлік техниканың шапшаң дамуы мемлекеттік басқарудың құрылымы мен механизмдеріне айтарлықтай әсер етуде. Бүгінгі ақпарат тасқыны толассыз күшке айналған, бүкіләлемдік ақпараттық кеңістік қалыптасқан жағдайда қоғамдағы ақпараттың рөлі мен орны ерекше артып отыр. Бұл өз кезегінде мемлекеттің, қоғамның және жеке

адамдардың ақпараттық қауіпсіздігін қамтамасыз ету мәселелерінің күрделенуіне ықпал етуде.

Қазақстан демократиялық бағыт ұстанған, зайырлы, құқықтық, әлеуметтік мемлекет ретінде өзінің қауіпсіздігін, оның ішінде ақпараттық қауіпсіздігін қамтамасыз етуге мүдделі. Сондықтан да ақпараттық қауіпсіздіктің нормативтік-құқықтық қамтамасын дамыту мақсатында «Ақпараттандыру туралы», «Мемлекеттік құпиялар туралы», «Бұқаралық ақпарат құралдары туралы», «Электрондық құжат және электрондық цифрлық қолтаңба туралы», «Жарнама туралы», «Байланыс туралы», т.б. заңдар, «Ақпараттық қауіпсіздік тұжырымдамасын қабылдады».

Қазіргі таңда ақпарат тарату мүмкіншілігі бойынша Интернет торабы алдыңғы қатарға шығып отыр. Газет, теледидар, радионың түгелге жуығы Интернет торабында сайт немесе өз парақшаларын ашып, электронды ақпарат құралдарының саны күннен-күнге өсуде. Ал Интернеттегі әлеуметтік желілердің қолданушыларының орта жасы 7-ден 48-ге дейін болып отыр.

Қазір кез-келген ұялы телефонда әлеуметтік желілерге қосылу үшін қосымша бағдарламалар орнатылатын болды. Кез-келген компанияның өз тауарларын жарнамалау мақсатында әлеуметтік желіде парақшалары бар. Тіпті Үкімет мүшелері, көптеген лауазымды тұлғалар Интернетте өз парақшалары, блогтарын ашып, сол арқылы өздерінің қызметіне байланысты ақпарат беріп отырады.

Әлеуметтік желілердің жеке тұлғаның өзін-өзі дамытуға пайдасы зор. Интернеттен музыка, фильм, ойындардан басқа ғылыми мақалалар, аудиокітаптар, тіл үйрену курстарын, тамақ істеу, би үйрену, дене шынықтыру тәсілдерін көшіріп алуға, қарауға болады. Көптеген оқулықтар мен рефераттар, түрлі суреттер де Интернетте жетерлік. Кез-келген мемлекеттік органдар, түрлі компаниялар мен дүкендер, кафе, мейрамханалар туралы ақпарат алу, олардан анықтама алу, тапсырыс беру сияқты көптеген жұмыстарды үйде отырып Интернет арқылы бітіре беруге болады. Сонымен қатар, әлеуметтік желілер арқылы кез-келген адам өзінің пікір алмасатын, мүдделестер ортасын қалыптастыруға, жаңа таныс, дос табуға да мүмкіншілігі бар. Сол сияқты кез-келген фирма өзінің өнімдеріне қызығушылық танытқан клиенттерін топтастыра алады. Алайда, әлеуметтік желілердің адамзатқа, әсіресе жас ұрпаққа әсері соңғы кезде барлық елдерде ғалымдарды, билік өкілдерін, жастар тәрбиесімен айналысатын ұстаздарды аландатып отыр.

1-тапсырма. Мәтінді мағыналық бөліктерге бөліп, оларға ат қойыңыз.

2-тапсырма. Мәтіннен мамандыққа қатысты терминдерді теріп жазыңыз, оларды қатыстырып сөйлем құраңыз.

Үлгі: Біздің жұмысымыздың ең басты мақсаты *құпиялылықты* сақтау болып табылады.

## 8 Ақпаратты қорғау жүйесі

Қолдануға қажетті кез-келген басқа программаның тұжырымдамасы сияқты қорғаныс жүйесін құру тұжырымдамасы да мынадай сұрақтарды қарастырады: ақпаратты қорғау аймағындағы практикалық зерттемелердің өзектілігі, қорғаныс жүйесін құрудың негізгі кезеңдері және қорғаныс мәселесін шешудің әр түрлі әдістемелерінің салыстырмалы талдауы.

Қорғаныс жүйесін құрудың негізгі кезеңдері төмендегідей болып жіктеледі (1 сурет):



1 сурет- Қорғаныс жүйесін құру кезеңдері

1) Мүмкін болатын қауіп-қатердің талдауы келесі қауіп-қатерден қорғанудың негізгі түрлерін зерттеумен айналысады:

- Ақпараттың құпиялылығының бұзылуының қауіп-қатері;
- Ақпараттың бүтінділігінің бұзылуының қауіп-қатері.

Бұл кезең шындығында да барлық қауіп-қатердің жиынтығынан қарапайым зиян (вирус, ұрлық) келтіретіндерін таңдаумен аяқталады.

2) Қорғаныс жүйесін жоспарлау кезеңі қорғалатын құрылымдар тізімінен және оларға мүмкін болатын қауіп-қатерден тұрады. Бұл кезде қорғанысты қамтамасыз етудің келесі бағыттарын назарға алу қажет:

- құқықтық-этикалық;
- моральды-этикалық;
- қорғанысты қамтамасыз етудің әкімшіліктік шаралары;
- қорғанысты қамтамасыз етудің аппараттық-программалық шаралары.

3) Қорғаныс жүйесін іске асыру ақпаратты өндеудің жоспарланған ережелерін іске асыруға қажетті құралдарды орнату мен баптауды қамтамасыз етеді.

4) Қорғаныс жүйесін сүйемелдеу кезеңі жүйенің жұмысын бақылау, ондағы болып жатқан оқиғаларды тіркеу, қорғанысты бұзуды айқындау мақсатымен оларды талдау және қажетінше қорғаныс жүйесін түзетумен сипатталады.

- 1-тапсырма. Сөздіктің көмегімен мәтінді аударыңыз.  
2-тапсырма. Берілген мәтінді қазақ тіліне аударыңыз.

*В современных условиях наличие развитой системы информационной безопасности становится одним из важнейших условий конкурентоспособности любой компании. Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.*

## 9 Ақпаратты қорғау әдістері



2 сурет - Ақпаратты қорғау әдістерінің жіктелуі

Қорғаныстың аппараттық әдістерін қолдану мынадай техникалық құралдарды пайдалануды ұсынады:

- 1) Тыңдалатын және жазылатын құрылғылардан қорғайтын TRD-800 категориялы радиохабарлағыштар мен магнитофондар детекторы;
- 2) Жасырын бейне бақылау құратын модульдік нөмірлер;
- 3) Ақпаратты жеткізудің дұрыстылығын қамтамасыз ететін ақпаратты анықтылыққа тексеру сызбалары;
- 4) Күпиялы құжаттарды жіберуге арналған SAFE-400 категориялы факстік хабардың скремблері.

Қорғаныстың аппараттық әдістері ресурстардың үлкен шығынын талап етеді.

Программалық әдістер есептеуіш алгоритмдер мен қатынауды шектеуді қамтамасыз ететін программаларды және ақпаратты рұқсатсыз пайдаланудан шығаруды ұсынады. Программалық әдістер келесі функцияларды іске асырады:

- 1) Идентификация, аутентификация, авторизация (Pin кодтар, парольдер жүйелері арқылы);

- 1) Резервті көшіру және қалпына келтіру процедуралары;
- 2) Антивирустық программаларды белсенді қолдану және антивирустық қорларды жиі жаңартып отыру;
- 3) Транзакцияны өңдеу.

1-тапсырма. Сөздіктің көмегімен мәтінді аударыңыз.

2-тапсырма. Мәтіндегі термин сөздерді теріп жазып, олардың жасалу жолын анықтаңыз.

Үлгі: ұйымдастырушы-лық жұрнағы арқылы жасалған синтетикалық тәсіл; радиохабар - аналитикалық тәсіл арқылы жасалған сөз тіркесі; құпия құжаттар- лексика-семантикалық тәсіл арқылы жасалған сөз тіркесі.

## **10 Ақпаратты қорғаудың криптографиялық әдісі**

Ақпаратты қорғаудың криптографиялық әдісі—бұл ақпаратты шифрлаудың, кодтаудың немесе басқаша түрлендірудің арнайы әдісі, мұның нәтижесінде ақпарат мазмұнына криптограмма кілтінсіз және кері түрлендірмей шығу мүмкін болмайды. Криптографиялық қорғау – ең сенімді қорғау әдісі, өйткені ақпаратқа шығу емес, оның тікелей өзі қорғалады, (мысалы, әуелі тасуыш ұрланған жағдайдың өзінде ондағы шифрланған файлды оқу мүмкін емес).

Мұндай қорғау әдісі стандартты операциялар немесе программалар дестесі түрінде жүзеге асырылады. Операциялық жүйенің негізіндегі қорғау көбінесе қатынас құруды басқарудың процедураларын жүзеге асыруға мүмкіндік беретін мәліметтер қорын басқару жүйелері деңгейіндегі қорғау құралдарымен толықтырылуы керек.

Қазіргі кезде ақпарат қорғаудың криптографиялық әдісінің көпшілік қабылдаған жіктеуі жоқ. Дегенмен, жіберілетін хабарламаның әрбір символы шифрлауға түскенде шартты түрде 4 негізгі топқа бөлуге болады:

- ауыстыру шифрланушы мәтіннің символдары сол немесе басқа алфавит символдарымен алдын ала белгіленген ережеге сәйкес ауыстырылады;

- аналитикалық түрлендіруде шифрланушы мәтін қандай да бір аналитикалық ереже бойынша түрлендіріледі;

- орын ауыстыру шифрланушы мәтіннің символдарының орны жіберілетін мәтіннің берілген блогының шегінде қандай да бір ереже бойынша шифрланады.

Ақпаратты шифрлаудың сенімділік дәрежесі бойынша көптеген программалық өнімдер бар. Кең таралған программалардың бірі болып Циммерменн құрған Pretty Good Privacy (PGP) болып табылады. Оның криптографиялық қорғау құралы өте күшті. Танымдылығы мен ақысыз таратылуы іс жүзінде PGP-ны дүние жүзінде электрондық хат алысу стандартына айналдырды. PGP программасына желіде көпшіліктің шығуына мүмкіндігі бар.



Ақпаратты қорғаудың ұйымдастырушылық әдісі келесі іс-шаралардың ұйымдастырылуы мен іске асырылуын қарастырады:

- 1) өртке қарсы қорғаныс;
- 2) жанбайтын сейфтерде аса қажетті құжаттарды сақтау;
- 3) өту жүйесі арқылы қатынау регламенті;
- 4) бақылау жүйесін ұйымдастыру;
- 5) қолданушылардың әр түрлі категорияларының қорғаныс объектілері мен олардың орындалу талаптарына қатынауды регламентациялайтын көмекші нұсқамаларды даярлау;
- 6) мамандарды таңдау мен даярлау;
- 7) қауіпсіздік мәселесі бойынша семинарларға, конференцияларға қатысуды қамтасыз ету мен ұйымдастыру.

1-тапсырма. Мәтінді аударыңыз.

2-тапсырма. Сөздіктің көмегімен берілген мәтінді қазақ тіліне аударыңыз.

*Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации. Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в зашифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию. Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных. Криптография — одна из старейших наук, её история насчитывает несколько тысяч лет.*

## **11 Жаһандық ақпараттық кеңістік**

Ғаламдық ақпараттық қоғамның қалыптасу ортасы және негізі. Ғаламдық ақпараттық кеңістікті қалыптастыруда технологиялық түп қазық болып табылатын, ақпараттық қоғам дамып, қызмет ететін қазіргі компьютерлік технологиялардың маңызы зор. Қазіргі компьютерлік технологиялардың дамуында ғаламдық компьютерлік желі Интернеттің құрылуы аса маңызды кезең болды. Интернет желісі — бүкіл әлемде бірнеше миллион адамдарды қамтып, біріктіретін біртұтас ақпарат кеңістігі.

Интернетті қолданушылар өте кең көлемдегі ақпараттық қызметтерге қол жеткізе алады: баспасөз сайттарын, радио, теледидар, электронды пошта, электрондық коммерция, телеконференциялар, хабарландырулар тақтасын, жаңалықтар топтамасын, чаттарды және т.б. көптеген қызмет түрлерін қолдана алады.

Ақпараттық қауіпсіздік — мемлекеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай-күйі. Ақпаратты қорғау — ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп деректерді енгізу, сақтау, өңдеу және тасымалдау үшін қолданылатын ақпарат пен қорлардың тұтастығын, қол жеткізулік оңтайлығын және керек болса, жасырындылығын қолдауды түсінеді.

ҚР Конституциясы әр адамға қажетті ақпаратты алуға және оны заңмен тыйым салынбаған, кез келген жолмен жариялауға кепілдік береді.

1-тапсырма. Мәтінді аударыңыз.

2-тапсырма. Мәтінде берілген ақпаратқа өз ойыңызды білдіріп, мәтінді толықтырыңыз.

## **12 Ақпаратты қорғау әдістері мен құралдары**

Қорғау дегеніміз-жалпы түсінік. Қорғау-жүйенің объектілерін қоршаған ортадан қорғайтын механизмдерді сипаттау. Қорғау тетіктеріне тән белгілер:

1) Бір пайдаланушының екінші пайдаланушыға кедергі келтіруіне жол бермеу;

2) Пайдаланушының бағдарламасымен деректеріне қорғаныс құралдарын ұсыну.

Қорғау тетіктері (механизмы) төмендегідей бірқатар мәселелерді шешеді:

1) Заң шығару нормаларымен анықталатын, дербес қол жеткізуді реттеуші жеке ақпарат құпиясын қорғау.

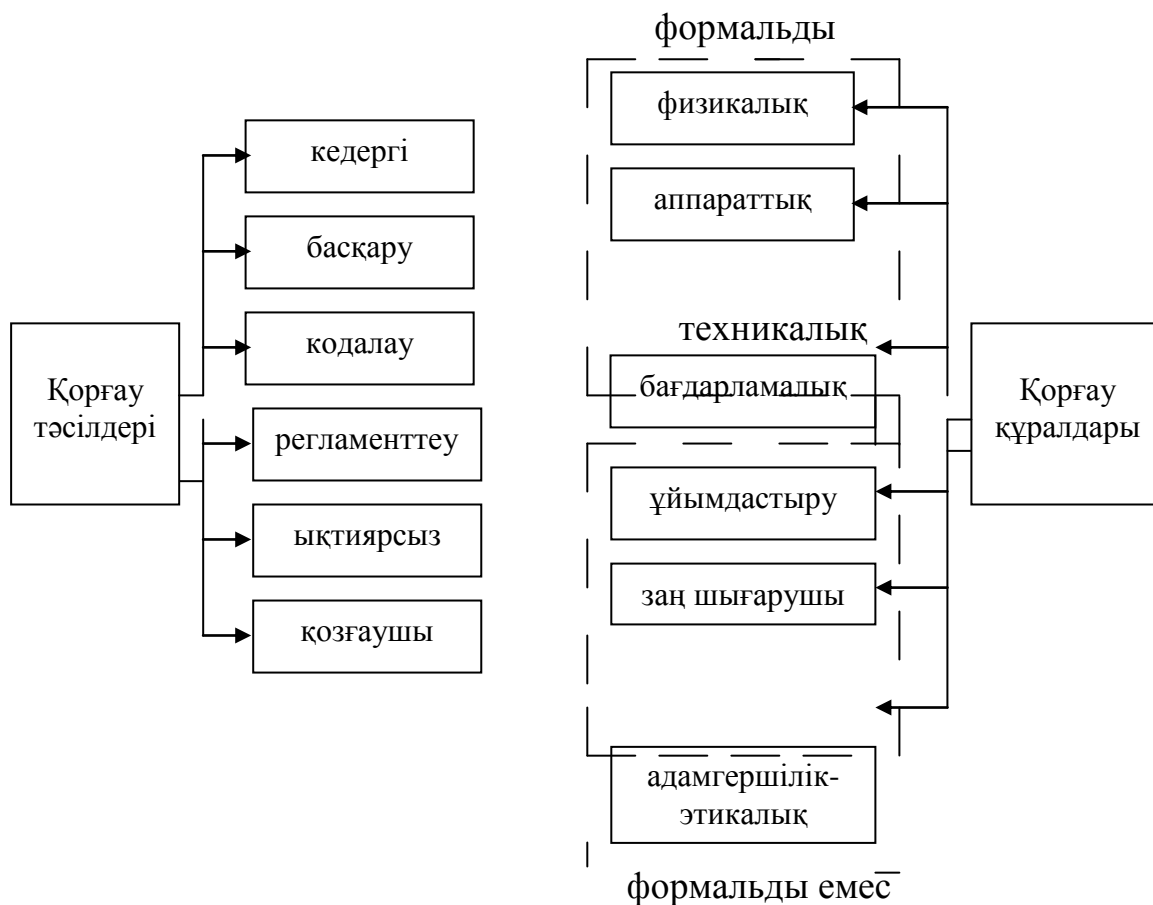
2) Ақпаратқа қол жеткізу ережесін анықтайтын ақпарат құпиялылығын сақтау.

3) Құпиялылықтың сақталуын қамтамасыз ететін әдістер мен құралдардың ақпарат қауіпсіздігіне жол ашуы.

Алғашқы сатыда ақпараттың қорғалуы бағдарламалық әдіспен шешіледі. Тәжірибе көрсеткендей ақпараттың қорғалуына бағдарламалық құралдар кепіл бола алмайды. Сондықтан бағдарламалық құралдар ақпаратқа қол жеткізуді, сақтау ережесін анықтайтын ұйымдастыру шараларымен толықтырылды.

Келесі саты-мәліметтерді қорғау бойынша жүйе және техникалық құралдар құру болып табылады. Қорғаудың кешенді әдісі жоғары нәтиже береді. Ақпаратты қорғаудың барлық әдістері мен құралдарының жиынтығын төмендегідей түрде топтастыруға болады.

### 13 Қорғау құралдарының классификациясы



1-тапсырма. Сөздіктің көмегімен мәтінді аударыңыз.

2-тапсырма. Берілген сұлба бойынша қорғау тәсілдеріне түсініктеме беріңіз.

### 14 Аударма туралы

Аударма дегеніміз – бір тілде берілген ақпаратты екінші тілдің тәсілдерімен басқа тілге жеткізу. Аударманың бірнеше түрлері бар.

Сөзбе-сөз дәлдік немесе сөзбе-сөз аударма дегеніміз – грамматикалық оралымдарды механикалық түрде көшіру, жеке тілдік бірліктерінің мағынасын беру, терминологиялық және лексикалық тәсілдерді дұрыс таңдамау, түпнұсқа сөйлемдерінің құрылымын өзгертпей сақтау, аудармашыға еркіндік бермеу. Мұндай аударма сапасыз аударма ретінде саналуы мүмкін. Бірақ сөзбе-сөз аударманың артықшылығы да бар, ол аударманың ең объективті түрі болып есептеледі. Бастапқы мәтіннің жеке тілдік бірліктерінің мағынасын бере отырып, синтаксистік конструкцияларды көшіріп бере отырып, аудармашы өзіне еркіндік бере алмайды. Сөзбе-сөз

аударманың кемшілігі – аударманы қолданатын адамның коммуникативтік мүмкіндіктерін ескермеу.

Мағыналық дәлдікке немесе мағыналық аудармаға екі тілдің стильдік ерекшеліктерін терең біліп, сөйлемдегі сөздердің орын тәртібі мен сөйлемдер құрылымындағы айырмашылықтарды біліп, керек кезінде түпнұсқаның мағынасын сақтау үшін сөзбе-сөз аударудан аулақ болғанда ғана қол жеткізуге болады.

Мағынасын сақтап аударуды еркін аударма деп те атайды. Еркін аударма аудармашыға түпнұсқа мәтінін түсіндірулер мен қосымшалар, түбегейлі өзгертулер арқылы жеткізуге шексіз мүмкіндіктер береді. Сол себептен еркін аударма объективті емес, өйткені аударылатын мәтінді жазған адамның дәл солай дегеніне ешкім кепілдік бере алмайды. Көптеген жағдайларда, мысалы, келісімшарттарды, маңызды құжаттарды аударғанда ол жарамсыз болып қалады.

Нағыз аударма сөзбе-сөз аударма мен еркін аударманың жиынтығы болып табылады. Сөзбе-сөз аудармадан бастапқы мәтінге мүмкіндігінше мағыналық және құрылымдық жағынан жақындықты алады, бірақ бұл тілдік норманы бұзбауы және түсініксіздік туғызбауы керек. Түсініксіздік туған жағдайда және барабарлық болмаған жағдайда бейімдеуді қолдануға болады, бірақ ол шектеулі көлемде болуы керек. Түпнұсқаға мағыналық-құрылымдық жақындықтан шегіну, яғни бейімделу қажеттіліктен туындаған амалсыз шара ретінде қарастырылады.

1-тапсырма. Мәтіннің сөзбе-сөз аудармасын жасаңыз.

#### **14.1 Компьютерлер мен желілердегі ақпаратты қорғаудың бағдарламалық құралдары**

Компьютерлік вирустарды жіктеу, өмір сүру ортасына жұғу тәсілдері. Вирустарды белсенді ету тәсілдері. Вирустардың бұзушылық әрекеттері. Вирустардың болу белгілері. Басқа қауіпті бағдарламалар. Антивирустық құралдар. Вирустармен күресудің болашақтағы тиімді бағыттары.

Есептеу жүйесіне немесе желісіне бағдарламалық өніммен танысу, орындау, жою, ұрлау мақсатында рұқсатсыз ену талаптары -компьютерлік қарақшылық деп аталады. Мұндай құбылыстың алдын-алу үшін операциялық жүйені, бағдарламалық жабдықты қорғауға, рұқсатсыз енуді бақылауға, бұзушылар категориясын және қолданылатын әдістерді анықтауға арналған қорғаныс түрлері бар.

Хакерлер категориясы:

- 1) Хакер –дилетанттар;
- 2) Хакер-мамандар(маманданған хакерлер) болып бөлінеді.

Дилетант хакерлер:

- 1) бағдарламаның тағайындалу мақсатын анықтау үшін қол жеткізуге тырысады;

- 2) ойын бағдарламаларына қол жеткізуге ұмтылады;
- 3) бұзақылық мақсатпен із қалдырып деректерді жойып жібереді.

Бұл категориядағы хакерлерге түрткі болған нәрсе, эмоциялық тілегін қанағаттандырудан бастап, жүйені басқаруды жүзеге асыру.

Хакерлер ісіне түрткі болатын жағдайлар:

- 1) басшылық тарапынан олардың ісіне көзқарас;
- 2) фирмадағы еңбегін құрметтеу жүйесіне көңілінің толмауы;
- 3) ашудан туған қасақаналық.

Хакердің болуының өзі жүйені қорғау мәселесіне жауапты қарауды, жүйеге рұқсатсыз ерудің алдын-алып, оларды тауып жазалауды талап етеді.

Хакерлер-мамандар – төмендегі мақсатты көздейтін қылмысты топтар:

- 1) саяси;
- 2) өндірістік тыңшы;
- 3) пайдакүнем.

Компьютерлік айла –шарғымен олар фирмаға үлкен материалдық залал әкеледі. Мұндай әрекеттер алдын-ала жоспарланып істі білетіндермен жүзеге асады. Қарақшылар- маманданғандар олар өзі іс әрекетіне фирманың бұрынғы және қазіргі қызметкерлерін тартады.

## **15 Аудармаға қойылатын талаптар**

Аудармаға мынадай талаптар қойылады:

1) *Дәлдік (точность)*. Аудармашы автордың ойын толығымен аудармада жеткізуі тиіс. Мәтіндегі ойлардың негізгі сипаты ғана сақталмауы тиіс, сонымен бірге айтылған ойдың ньюанстары мен белгілері де сақталуы тиіс. Автордың айтқан ойларын жеткізе отырып, сонымен бірге аудармашы өз жанынан ештеңе қосуға, толықтыруға және оны түсіндіруге тиіс емес;

2) *Ықшамдылық (краткость)*. Аудармашы көп сөзді болмауы керек, ойлары барынша ықшамды және мәнерлі (үйлесімді) түрде мазмұндалуы тиіс;

3) *Айқындылық (ясность)*. Аудармада тілдің жеңілдігі мен ықшамдылығы аса қажет. Қабылдауға қиындық туғызатын күрделі және екі ұшты оралымдардан бас тартқан жөн. Ой қарапайым әрі айқын, баршаға түсінікті тілмен жеткізілуі тиіс;

4) *Әдебилік (литературность)*. Аударма әдеби тілдің жалпыға бірдей тұтастай нормасына сай жасалуы қажет. Әрбір сөйлем түпнұсқаның синтаксистік құрылымындағы аударма тіліне жат ешқандай тұспалдау байқатпай, нақты және табиғи түрде айшықталып тұруы тиіс. Шетелдік сөздерге калька жасаудан бойды аулақ салып, сөздіктер мен анықтамалық әдебиеттің көмегіне сүйене отырып, аударма тілінде балама терминдер табуға тырысу керек.

1-тапсырма. Мәтіннің мағыналық аудармасын жасаңыз.

## **15.1 Бағдарламалық қамтамасыздандырылуды рұқсатсыз қолданудан қорғау**

Пайдаланушыларды идентификациялау және аутентификациялау. ДЭЕМ-ді идентификациялау. Рұқсатсыз қолданудан және көшіруден қорғаудың бағдарламалық құралдары. Электронды кілттер көмегімен көшіруден бағдарламалық қамтамасыздандыруды қорғау. Қорғауды құру сызбалары.

Қорғаудың техникалық құрылғысы – бұл деректер мен ақпараттарды қорғауға тағайындалған негізгі және қосымша құрал – жабдықтар.

Ол келесі түрге бөлінеді:

- 1) электрондық қорғау құрылғылары (ЭҚК);
- 2) оптикалық қорғау құрылғылары.

Ақпаратты қорғаудың техникалық құрылғыларын құру (АҚТК) - аз танымал физикалық құбылыстағы қорғау кілтіне нақты негізделген. Мұндай кілтті жаңғырту өте қиын, сондықтан оны тек лицензиясын төлеген иемденушілер ғана пайдалана алады.

ЭҚК пайдалану барысында көшіруден қорғау үшін қосымша шара қажет емес. Қорғау кілтінің болуы бағдарламалық өнімді өндірумен қатарлас жетілген кілттің бар болуын тағайындайды. Жүйе бір ғана жалғыз құлыппен және қос кілтке ажыратылады. Қорғау деңгейі санының артуына байланысты жүйенің қорғалу дәрежесі артады. Бір кілт қорғаудың қарапайым құрылғысының кілтін алу үшін, екіншісі бағдарламаны шифрдан шығаруға немесе жүйеде жасырулы ІІІ кілтті алуға негізделген. Қосымша қорғау деңгейлері көшірмелеу жұмысын қиындатады.

Жоғарыда аталған қорғау құрылғыларының міндеті - деректер базасын, компьютерлік бағдарламаларды рұқсатсыз пайдаланудың алдын алу. Қызметкерлердің сенімділік дәрежесін әртүрлі қорғау кілттері арқылы қамтамасыз етуге болады.

## **16 Ғылыми-көпшілік және ғылыми техникалық аударма**

Ғылыми аударма және ғылыми-техникалық аударманы жасау үшін аудармашының алдымен ғылыми-техникалық ақпараттан хабардар болуы тиіс.

Ғылыми-техникалық ақпарат 3-ке бөлінеді:

1) патенттік әдебиет – ақпарат алмасудың негізгі түрі, қалай болғанда да ол ғылым мен техника саласындағы жаңа дүниенің бәрі патент сипатында және оның туындылық түрінде ресми құжатталынып тіркеледі;

2) ғылыми-техникалық ақпарат алмасу үшін арнайы тағайындалған мерзімдік кезең, мәселен, салалық бюллетеньдер, мазмұнды рефераттар, түйіндеме және атауы, салалық ғылыми-техникалық журналдар, арнайы сипаттағы пікірталастық өзекті мәселе көтерген және есептік мақалалар, тақырып атаулары тізімделген библиографиялық көрсеткіштер,

өнертапқыштық және өндіріс өнімдерінің заттары, сондай-ақ аталған сала бойынша мазмұндағы түйіндеме мен тақырыптық шолу;

3) әртүрлі мерзімдік және мерзімдік емес басылымдар және басқа да ғылыми-техникалық алмасу үшін арнайы бекітілмеген, алайда осы мақсатта пайдалана беруге болатын ақпарат көздері, мысалы: арнайы кітаптар мен журналдар, жарнамалық материалдар, нұсқаулар және сол тектес арнайы ақпараттық көздер.

1-тапсырма. Аударыңыз:

- 1) қатынас құру-
- 2) ерікті басқару-
- 3) қадағалау жұмысы-
- 4) сүйемелдеу-
- 5) әдістері-
- 6) маңызды құралы-
- 7) сенімді есептеу базасы-
- 8) қорғаныш тетігі-
- 9) жүйенің сенімділігі-
- 10) ақпаратқа талдау жасау-
- 11) іс - әрекеттер тізімі-
- 12) талап етіледі-
- 13) даярлық кезеңі-
- 14) қатерді талдау-
- 15) қорғаныш жоспары-
- 16) негізін құру-

### **16.1 Ақпараттық қауіпсіздік саясаты**

Қауіпсіздік саясаты - мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны. Бұл ережелер пайдаланушының қайсы кезде белгілі бір деректер жинағымен жұмыс істей алатынын көрсетеді. Қауіпсіздік саясатын құрамына мүмкін болатын қауіптерге талдау жасайтын және оларға қарсы әрекет шаралары кіретін қорғаныштың белсенді сыңары деп санауға болады.

Қауіпсіздік саясатының құрамына ең кемінде мына элементтер кіруі керек: қатынас құруды ерікті басқару, объектілерді қайтадан пайдаланудың қауіпсіздігі, қауіпсіздік тамғасы және қатынас құруды мәжбүрлі басқару.

Кепілдік - жүйенің сәулетіне және жүзеге асырылуына көрсетілетін сенім өлшемі. Ол қауіпсіздік саясатын іске асыруға жауапты тетіктердің дұрыстығын көрсетеді. Оны қорғаныштың, қорғаушылар жұмысын қадағалауға арналған, белсенсіз сыңары деп сипаттауға болады. Кепілдіктің екі түрі болады: операциялық және технологиялық. Біріншісі жүйенің сәулеті

және жүзеге асырылу жағына, ал екіншісі - құрастыру және сүйемелдеу әдістеріне қатысты.

Есепберушілік (немесе хаттамалау тетігі) қауіпсіздікті қамтамасыз етудің маңызды құралы болып табылады. Сенімді жүйе қауіпсіздікке байланысты барлық оқиғаларды тіркеп отыруы керек, ал хаттаманы жазу-жүргізу тексерумен (аудитпен - тіркелу ақпаратына талдау жасаумен) толықтырылады.

Сенімді есептеу базасы (СЕБ) - компьютерлік жүйенің қауіпсіздік саясаты жүзеге асыруға жауапты қорғаныш тектерінің жиынтығы. Компьютерлік жүйенің сенімділігіне баға беру үшін тек оның есептеу базасын қарастырып шықса жеткілікті болады. СЕБ негізгі міндеті - қатынасым монитормының міндетін орындау, яғни, объектілермен белгілі бір операциялар орындау болатындығын бақылау.

Қатынасым монитормы - пайдалынушының программаларға немесе деректерге әрбір қатынасының мүмкін болатын іс - әрекеттер тізімімен келісімдігі екендігін тексеретін монитор. Қатынасым монитормынан үш қасиеттің орындалуы талап етіледі:

- оңашаландық. Монитор өзінің жұмысы кезінде аңдудан қорғалуға тиісті;

- толықтық. Монитор әрбір қатынасу кезінде шақырылады. Бұл кезде оны орай өтуге мүмкіндік болмау керек;

- иландырылатындық. Мониторды талдауға және тестілеуге мүмкін болу үшін ол жинақы болуы керек.

## **17 Техникалық аударма**

Техникалық аударма – әртүрлі тілде сөйлейтін адамдар арасында арнайы ғылыми-техникалық ақпарат алмасу үшін қолданылатын аударма. Техникалық аударманы жүзеге асыратын адам екі тілді білуге міндетті. Түпнұсқаның мазмұнын сауатты, нақ, дәл беру үшін аудармашы екі тілдің біреуін еркін меңгеруі керек. Техникалық аударманы жүзеге асырушы адам жаңа материалдарды пайдаланады, сондықтан оны қабылдау үшін белгілі дайындығы және арнайы білімі болуы керек. Кез келген екі тілді білетін адам техникалық аударманы жүзеге асыра алмайды.

Техникалық аударма жасай алу үшін ғылыми-техникалық ақпарат алмасуда аудармашы (делдал) қызметін атқаратын адам қандай қасиеттерге, білімге, біліктілікке, дағдыға ие болуы керек?

Бұл жерде әңгіме қазақ тілі мен орыс тілі туралы болып отырғандықтан, біріншіден, аударып отырған тілін (мысалы, аудармашы орыстілді болып, түпнұсқа қазақша немесе керісінше болса), яғни қазақ тілін түсіне алатындай деңгейде немесе керісінше; екіншіден, басқа тілді (бұл жерде орыс немесе қазақ тілін) ақпаратты сауатты бере білу үшін жеткілікті деңгейде білуі; үшіншіден, ақпарат көздерін пайдалана білуі; төртіншіден, әртүрлі



техникалық аудармалар жасай алуы; бесіншіден, терминологиялық минимумды білуі керек.

Аудармашы өзіне қажет арнайы мәліметтерді тез табу үшін қандай ақпарат көздері бар екенін, олардан не табуға болатынын, оларды қандай тәртіппен қолдануға болатынын білуі керек.

Барлық ақпарат көздерін жалпы, арнайы ақпарат көздері деп бөлуге болады. Жалпы ақпарат көздеріне жалпы қолданыстағы сөздіктер және жалпы энциклопедиялар жатады. Сөздіктер екітілді және бір тілді болады. Біртілді сөздіктер: түсіндірме, синонимдер, омонимдер, антонимдер, орфографиялық, фразеологиялық болып келеді. Арнайы ақпарат көздеріне: арнайы сөздіктер, арнайы энциклопедиялар, ғылым мен техниканың әртүрлі салалары бойынша анықтамалықтар, арнайы әдебиеттер жатады.

Жалпы екітілді сөздіктерді табысты пайдалану үшін мыналарды есте сақтау керек:

1) кез келген жалпы екітілді сөздік (фразеологиялық сөздіктен басқасы) сөздің аудармасын емес, әрбір сөздің мүмкін болатын баламаларын ғана береді, сөздік сөздің белгілі контекстегі мағынасын тұспалдап қана көрсетеді;

2) қажет сөзді жылдам табу үшін алфавитті жақсы білу керек. Сөздікпен жиі жұмыс жасаған кезде алфавитті жақсы білу жұмыс уақытын едәуір үнемдеуге мүмкіндік береді;

3) барлық шартты белгілердің, қысқартулардың, сөздік мақалаларында кездесетін тыныс белгілерінің мағыналарын жақсы білу керек. Ол үшін сөздікті пайдаланбас бұрын сөздікті пайдалану туралы мақаланы зерде қойып оқып шығу және қысқартулар тізімімен танысу керек.

1-тапсырма. Мәтінді сөздіктің көмегімен аударыңыз.

### **17.1 Қауіпсіздік саясатының негізгі элементтері**

Қауіпсіздік саясаты (ұйымдастыру тұрғысынан қарағанда) есептеу және қатынас қорларын пайдалану тәсілін, сондай - ақ, қауіпсіздік режимін бұзудың алдын алу және мән беру процедураларын дұрыс анықтайды. Қауіпсіздік саясатын қалыптастыру іс - әрекетін келесі кезеңдер түрінде қарастыруға болады:

*Ұйымдастыру мәселелерін шешу.* Бұл кезеңде ақпараттық қауіпсіздік қызметі құралады, ақпараттық қауіпсіздік тұрғысынан қарағанда пайдаланушылардың санаттары, пайдаланушылардың барлық санаттарының жауаптылық деңгейлері, құқықтары және міндеттері анықталады.

*Қатерге талдау жасау.* Қатерді талдау үрдісі нені қорғау керек, неден қорғау керек және қалай қорғау (істеу) керек деген сияқты сұрақтардың жауабын анықтайды. Мүмкін болатын қатерлердің бәрін қарастырып шығу керек және оларды келтіретін зиянының ықтимал мөлшеріне байланысты жіктеу керек. Қорғанышқа жұмсалатын қаржы қорғалынатын объектінің құнынан аспауға тиісті.

*Жеңілдіктерді анықтау.* Қорларды пайдалану құқықтары, қорларды қолдану ережелері, әкімшілік жеңілдіктер пайдаланушылардың құқықтары мен міндеттері, жүйелік әкімшілердің құқықтар мен міндеттері, жасырын ақпаратпен жұмыс істеу тәртіптері және тағы басқа анықталады.

*Қауіпсіздік саясатының бұзылуына жауап қайтару шараларын анықтау.* Қауіпсіздік режимін бұзушыларды табуға және жауапкершілікке тартылуға бағытталған әрекеттер, сонымен қатар, ақпаратты бұрынғы қалпына келтіру және бұзулардың зардаптарын жою шаралары анықталады.

*Ұйымдастыру-өкімгерлік құжаттарды дайындау.* Қауіпсіздік саясатының негізгі жайлары әр түрлі нұсқауларда, қағидаларда, ережелерде және өкімдерде келтіріледі.

Қауіпсіздік саясаты ақпарат қорғау жүйесінің қауіп-қатерлерге қарсы әрекет жасауға бағатталған құқықтық нормалардың, ұйымдастырушылық (құқықтық) шаралардың, программалық-техникалық құралдар және процедуралық шешімдер кешенінің жиынтығын анықтайды.

## **18 Ғылыми-техникалық әдебиетті аудару**

Ғылыми-техникалық әдебиетті аударушының ең негізгі міндеті – автордың ойын бұрмаламай, толық беру, аудармада қажетті терминологияны қолданып, сауатты әдеби тілмен аудару. Ғылыми-техникалық әдебиеттің аудармасына қойылатын негізгі талап - аударманың түпнұсқаға толық сәйкес келуі, оны орысша «адекватность перевода» дейді. «Адекватный» - латын сөзі. Қазақ тіліндегі мағынасын: тең, толық сәйкес келетін, барабар, ұқсас, бірдей, тепе-тең, теңбе-тең деген сөздер береді. Ғылыми-техникалық мәтіннің бірдейлігіне ақпараттық, ғылыми-техникалық дәлдікті сақтай отырып және түпнұсқаның стилистикалық ерекшеліктерін ескере отырып, қол жеткізуге болады. Мұндай аударманы басқаша эквивалентті (лат. тең, тең мағыналы) және аутентивті (грек тілінде - түпнұсқаға сәйкес, дұрыс, шын) деп те атайды.

Аударманың өн бойында бір затты немесе ұғымды білдіретін бір ғана термин қолданылуы керек. Белгілі бір кәсіпорында ғана қолданылатын жергілікті сөздерді, архаизм-терминдерді қолданбау керек. Қазіргі кезде аудармада бір сөзді бір мәтіндік бірліктің өзінде бірнеше құбылтып қолдану жағдайлары кездеседі. Мысалы, «схема» деген сөзді бір мәтінде немесе бір ақпараттық бірлікте «сұлба», «схема», «сұлбе» деп немесе «сеть» сөзін бірде «желі», бірде «торап» деп аударатын жағдайлар жиі кездеседі.

Тілдің барлық грамматикалық нормаларын сақтап, күрделі грамматикалық конструкцияларды көп қолданбай, аударылатын ақпаратты қарапайым және түсінікті етіп беру керек.

1-тапсырма. Мәтінді оқыңыз, таныс емес сөздерді сөздіктен қараңыз, сөздік түзіңіз.

2-тапсырма. Мамандыққа қатысты сөз тіркестерінің баламасын табыңыз:

- 1) адамның құқықтары-
- 2) шаралар кешені-
- 3) деректерді енгізу-
- 4) қол жеткізу оңтайлығы-
- 5) қойылатын шектеулер-
- 6) жасырындылық-
- 7) ақпарат кедергісі-
- 8) қабілеттілігі-
- 9) заңсыз қол жеткізу-
- 10) кепілділік-
- 11) ақпаратты өңдеу-
- 12) Қауіпсіздік саясаты-

### **18.1 Компьютерлік және желілік ақпараттарды қорғауды ұйымдастыру және техникалық құралдары**

Ақпараттық жүйелерде қауіпсіздік деңгейін бағалаудың әдістері. Ақпаратты қорғау мен бақылауды басқарудың ұйымдастырушылық шаралары. Ақпаратты қорғаудың заң жүзіндегі шаралары. Ақпаратты қорғаудың техникалық құралдары.

Есептеуіш жүйе құрамындағы қорғау құралдары.

Бұл қорғау әдістерінің категориясына дисклермен аппаратураларды қорғау, қорғау кілттері, штаттық құрылғы функцияларының өзгерулері жатады. Бұндай әдістерді қолдану кезінде қорғауға кепілдеме беретін бағдарлама орындалуы белгілі бір әрекеттерге, арнайы қауіпсіздік ережелері және шарттарына тәуелді болғандықтан есептеуіш жүйесінің операциялық ортасы штаттық режимге қарағанда әрдайым өзгеріп отырады. ЕЖ құрамындағы қорғаныс құралдарын төмендегі сұлба арқылы ұсынамыз:

МД қорғау.

МД-ны арнайы тәсілмен пішіндеу ОЖ-ні көшірмелеуден сақтайды. Бұл – деректер, каталогтар пішімін стандартты емес жолмен анықтау, секторлар өлшемін өзгерту, синхрондаушы сигналдар санын арттыру, ақпараттар тақырыбын ауыстыру.

DOS стандартты құралдары арқылы көшірмелеу барысында секторлардың орналасуы өзгереді және кешігу қортынды көшірменің кешігуімен сәйкес келмейді. Мұндай әдіс биттік көшірмелеуге тиімсіз.

ЕЖ құрылғысының қорғаныс тетіктері. Дискінің магниттік беті жолдың жеке секцияларына жазуға тиым салады (диск бетінен элементтердің механикалық сүртілуі немесе лазерлік ағынды пайдалану), яғни әр дискінің пішімі бесаспап. Оқылу жылдамдығын салыстыра отырып көшірмеден диск түпнұсқасын ажыратуға болады.

Қорғауға бір ЧИП-ті микропроцессор пайдаланылады. Көшіру немесе қарау үшін бағдарламаны деректер құрында (шинасында) салыстырудан сақтайтын МП-архитектурасы дайындалуда. Бағдарламаның орындалуы ЧИП

арқылы жүреді. ЧИП – бұл шифрлеуді қорғауды талап ететін жұмысты таратушы аппараттық зерделі модуль.

Қорғау құлыптары. Егер барлық тексерулер жүргізілмесе (мерзімі, уақыты, пайдаланушының идентификаторы, компьютердің сериялық нөмірі т.б.) бағдарламаға қол жеткізуге тиым салынады. Бұл – мобильдік құлып деп аталады. Бағдарлама тек қана сериялық нөмірі лицензияға кіргізілген компьютерде ғана жұмыс істейді. Мұндай қорғауды объектік кодтқа өзгеріс енгізу әдісімен айналып өтуге болады. Бірегей, сирек мінездемені жазбасы есте сақтауында ішінара бұзылған компьютерге ғана береді. Динамикалық есте сақтауда ақпараттың сақталуы периодты түрде қайта жазу арқылы жүреді. Бұл өзгергіштік қасиетті сәйкестендіруге пайдалануға болады. Бағдарламаның жұмыс жасау жағдайын есте сақтаудың бірегей құрылымымен байланыстыруға болады. Ішінара бұзылған жазу – басқа компьютерде қорғалған бағдарламаға керемет кілт бола алады.

Ақпараттың қызметінің өзгеруі бағдарламаны көшірмелеу жұмысын тоқтататын, ашып қарау жұмысын үзіп тастайтын қызметтер жүйесіне немесе кілттерді ауыстыруға негізделген. Сондықтан мұндай жағдайда жасалған көшірме жұмысқа жарамсыз болады.

## **19 Баламасыз лексиканы аудару тәсілдері**

Аудармада кейде сөздікте жоқ, яғни баламасыз лексика деп аталатын сөздер кездеседі. Мұндай жағдайда аударманы баламасыз лексиканы жеткізудің тәсілдерін қолданып, іске асырады.

Баламасыз лексиканы жеткізудің бірнеше тәсілдері бар:

1) *Транслитерация*. Шетел сөзін алып, оны аударма тілдің әріптерімен бейнелеу. Ондай сөздерге зауыт, пошта, станса т.б. сөздер жатады, бұл сөздер қазақ тіліне сіңіп кеткен. Ал орыс тіліне шетел тілінен енген жаңа сөздер қазақ тілінде де өзгертілмей алынып жүр: дисплей, ноу-хау, программа, модем т.б. сөздер. Бұл тәсілдің артықшылығы - оның сенімділігі. Транслитерация - таныс емес, жеткіліксіз зерттелген сөздің тек дыбыстық сыртқы қабығын ғана көрсету. Мұндай сөздердің мазмұны контекст арқылы ашылады. Аудармашы осы тәсілді қолдана отырып, жаңа сөзді түсіндіруде қателік жіберіп алудан қашады.

2) *Калькілеу*. Бұл тәсілдің мәні баламасыз сөздің құрылымдық бөліктері олардың аударма тілдегі сөзбе-сөз нұсқаларымен ауыстырылады: іскерлік банк, қызметтік автомашина, жоғарғы палата, директорлар кеңесі, Қауіпсіздік Кеңесі т.б.

3) *Баламасыз лексиканың өзіндік сонылығын сақтап, аударма тілдің мүмкіндігін пайдаланып, жаңа сөз немесе сөз тіркесін жасау*. Зейнеткер, тіркелім, бағдаршам, іссапар, тікұшақ, күнтізбе т.б.

4) *Сипаттама (түсіндірме) аударма тәсілі* - баламасыз лексиканы тілдік бірліктің мағынасын кеңінен сипаттау (сөз тіркестері, фразалар) арқылы жеткізу. Оның артықшылығы сипатталатын құбылыстың мәнін толық ашу

мүмкіндігін береді. Түпнұсқа тіліндегі сөз беріледі де, оның беретін мағынасы аударма тілдің тәсілдерімен түсіндіріледі.

1-тапсырма. Мәтінді аударыңыз.

2-тапсырма. Сөздердің баламасын табыңыз, оларды қатыстырып сөйлем құраңыз:

- 1) ақпараттық қорлар-
- 2) ақпараттық ағындар-
- 3) қатерді бағалау-
- 4) қатердерді бейтараптау-
- 5) жабдықтарды орнату-
- 6) мамандарды көздейді –
- 7) кең ауқымды –
- 8) негізгі талап –
- 9) мамандандырылған жоғары оқу орны—
- 10) заманауи техника—
- 11) ғылыми-зерттеу саласы –
- 12) сырттай оқу –
- 13) кәсіпорын –
- 14) бірегей –

### **19.1 Ақпараттық қауіпсіздігін қамтамасыз ету жұмыстары**

Объектінің ақпараттық қауіпсіздігін қамтамасыз етуге арналған жұмыстар бірнеше кезеңге бөлінеді: даярлық кезеңі, ақпараттық қорларды түгендеу, қатерді талдау, қорғаныш жоспарын жүзеге асыру. Осы аталған кезеңдер аяқталған соң эксплуатациялау кезеңі басталады.

*Даярлық кезең.* Бұл кезең барлық келесі шаралардың ұйымдастырушылық негізін құру, түпқазық құжаттарды әзірлеу және бекіту, сондай-ақ, үрдіске қатысушылардың өзара қарым - қатынастарын анықтау үшін қажет. Даярлық кезеңде ақпарат қорғау жүйесінің ақпараттың міндеттері анықталады.

*Ақпараттық қорларды түгендеу.* Бұл кезеңде, әдетте, объект, ақпараттық ағындар автоматтандырылған жүйелердің құрылымы серверлер, хабар тасышулар, деректер өңдеу және сақтау тәсілдері жайында мәлімет жиналады. Түгендеу анықталған соң олардың осалдылығына талдау жасалынады.

*Қатерді талдау.* Келесі шаралардың нәтижелерді ақпараттық қорлардың қорғанылу күй - жағдайның қаншалықты толық және дұрыс талдануына тәуелді болады. Қатерді талдау мыналардан тұрады: талданатын объектілерді және оларды қарастырудың нақтылану дәрежесін таңдау; қатерді бағалау әдіснамасын таңдау; қауіптерді және олардың салдарын талдау; қатерлерді бағалау; қорғаныш шараларын талдау; таңдап алынған шараларды жүзеге асыру және тексеру; қалдық қатерді бағалау.

Қауіп бар жерде қатер пайда болады. Қауіптерді талдау кезеңі қатерді талдаудың орталық элементі болып табылады. Қауіптердің алдын алу үшін қорғаныш шаралары мен құралдары қажет. Қауіптерді талдау, біріншіден, мүмкін болатын қауіптерді анықтаудан (оларды идентификациялаудан) және, екіншіден, келтірілетін болашақ зиянды болжау - бағалаудан тұрады.

Бұл кезеңнің орындалу нәтижесінде объектідегі қауіп - қатерлер тізбесі және олардың қауіптік дәрежесі бойынша жіктемесі құрастырылады. Бұлар бәрі ақпарат қорғау жүйесіне қойылатын талаптарды айқындауға, қорғаныштың ең әсерлі шаралары мен құралдарын таңдап алуға, сондай - ақ, оларды жүзеге асыруға қажетті шығындарды анықтауға мүмкіндік береді.

*Қорғаныш жоспарын құрастыру.* Бұл кезеңде осының алдында жүргізілген талдаудың нәтижесінде анықталған қатерлерді бейтараптау үшін қорғаныштың тиісті ұйымдастырушылық және техникалық шаралары таңдап алынады.

Қорғаныш жоспарын құру ақпарат қорғау жүйесінің функционалдық сұлбасын әзірлеуден басталады. Ол үшін қорғаныш жүйесінің атқаратын міндеттері анықталады және нақты объектінің ерекшеліктерін ескере отырып жүйеге қойылатын талаптар талқыланады.

*Қорғаныш жоспарын жүзеге асыру.* Бұл кезеңде қорғаныш жоспарында келтірілген шаралармен қоса жабдықтаушылармен келісім - шарттар жасасу жабдықтарды орнату және баптау, қажетті құжаттарды әзірлеу және т.б. осы сияқты шаралар іске асырылады.

*Өз бетімен аударуға берілетін қосымша мәтіндер.*

1) Ақпарат қауіпсіздігінің жоғарғы дәрежесіне қол жеткізу тек тиісті ұйымдастыру шараларын қолдану негізінде ғана мүмкін болады. Ұйымдастырушылық шаралар кешенінің құрамына ақпараттық қауіпсіздік қызметін құру, жасақтау және оның іс-әрекеттерін қолдау, ұйымдастыра-өкімгерлік құжаттар жүйесін дайындау жұмыстары, сонай-ақ, қорғаныш жүйесін құруға және оның жұмысын сүйемелдеуге арналған бірқатар ұйымдастырушылық және ұйымдастыру-техникалық шаралар кіреді.

Ұйымдастырушылық және ұйымдастыру-техникалық шаралар жүргізу ақпараттың сыртқа кететін жаңа арналарын дер кезінде табуға, оларды бейтараптандыру шараларын қолдануға, қорғаныш жүйелерін толық жетілдіруге және қауіпсіздік режимін бұзу әрекеттеріне жедел қарсы шара қолдануға мүмкіндік береді. Қатерге талдау жүргізу қауіпсіздік саясатын қалыптастырудың негізгі кезеңі болып табылады.

2) Қауіпсіздік саясаты мынадай элементтерден тұрады: қатынас құруды ерікті басқару, объектілерді қайтадан пайдаланудың қауіпсіздігі, қауіпсіздік тамғасы және қатынас құрудың мәжбүрлі басқару.

Қатынас құрудың ерікті басқару - жеке субъект немесе құрамына осы субъект кіретін топтың тұлғасын ескеру негізінде жасалған объектілерге қатынас құруды шектеу. Ерікті басқару - белгілі бір тұлға (әдетте, объектінің

иесі) өзінің қарауынша басқа субъектілерге өзінің шешімі бойынша объектігі қатынас құру құқығын бере алады.

Қатынас құрудың ағымдағы жағдайы ерікті басқару кезінде матрица түрінде көрсетіледі. Қатарларында - субъектілер, бағандарында - объектілер, ал матрицаның түйіндерінде қатынас құру құқығының (оқу, жазу, орындау және т.б.) кодасы көрсетіледі.

3) Қауіпсіздік саясаты – мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны. Бұл ережелер пайдаланушының қайсы кезде белгілі бір деректер жинағымен істей алатынын көрсетеді. Қауіпсіздік саясатын құрамына мүмкін болатын қауіптерге талдау жасайтын және оларға қарсы әрекет шаралар кіретін қорғаныштың белсенді сыңары деп санауға болады.

Қауіпсіздік саясатының құрамына ең кемінде мына элементтер кіруі керек: қатынас құруды ерікті басқару, объектілерді қайтадан пайдаланудың қауіпсіздігі, қауіпсіздік тамғасы және қатынас құруды мәжбүрлі басқару.

4) Кепілділік – жүйенің сәулетіне және жүзеге асырылуына көрсетілетін сенім өлшемі. Ол қауіпсіздік саясатын іске асыруға жауапты тетіктердің дұрыстығын көрсетеді. Оны қорғаныштың, қорғаушылар жұмысын қадағалауға арналған, белсенсіз сыңары деп сипаттауға болады. Кепілділіктің екі түрі болады: операциялық және технологиялық. Біріншісі жүйенің сәулеті және жүзеге асырылу жағына, ал екіншісі – құрастыру және сүйемелдеу әдістеріне қатысты.

Есепберушілік (немесе хаттамалау тетігі) қауіпсіздік қамтамасыз етудің маңызы құралы болып табылады. Сенімді жүйе қауіпсіздікке байланысты барлық оқиғаларды тіркеп отыруы керек, ал хаттаманы жазу – жүргізу тексерумен (аудитпен – тіркелу ақпаратына талдау жасаумен) толықтырылады.

5) Сенімді есептеу базасы (СЕБ) – компьютерлік жүйенің қауіпсіздік саясатты жүзеге асыруға жауапты қоршаған тетіктерінің жиынтығы. Компьютерлік жүйенің сенімділігіне баға беру үшін тек оның есептеу базасын қарастырып шықса жеткілікті болады. СЕБ негізгі міндеті – қатынасым мониториның міндетін орындау, яғни, объектілерімен белгілі бір операциялар орындау болатындығын бақылау.

б) Қауіпсіздік саясаты және негізгі элементтері.

Қауіпсіздік саясаты (ұйымдастыру тұрғысынан қарағанда) есептеу және қатынас қорларын пайдалану тәсілін, сондай-ақ, қауіпсіздік режимін бұзудың алдын ала және мән беру (жауап қайтару) процедураларын дұрыс анықтайды. Қауіпсіздік саясатының қалыптастыру іс-әрекетін келесі кезеңдер түрінде қарастыруға болады:

1) *Ұйымдастыру мәселелерін шешу.* бұл кезеңде ақпараттық қауіпсіздік қызметі (АҚК) құрылады, ақпараттық қауіпсіздік тұрғысынан қарағанда пайдаланушылардың санаттары, пайдаланушылардың барлық санаттарының жауаптылық деңгейлері, құқықты және міндеттері анықталады.

2) *Қатерге талдау жасау*. Қатерді талдау үрдісі нені қорғау керек, неден қорғау керек және қалай қорғау (істеу) керек деген сияқты сұрақтардың жауабын анықтайды. Мүмкін болатын қатерлердің бәрін қарастырып шығу керек және оларды келтіретін зиянының ықтимал мөлшеріне байланысты жіктеу қажет. Қорғанышқа жұмсалатын қаржы қорғанылатын объектінің құнынан аспауға тиісті.

7) Конфиденциальность (от англ. *confidence* — доверие) — необходимость предотвращения утечки (разглашения) какой-либо информации.

С этимологической точки зрения, слово «конфиденциальный» происходит от латинского *confidentia* — доверие. В современном русском языке это слово означает «доверительный, не подлежащий огласке, секретный». Слово «секрет», заимствовано из французского *secret* означает — «тайна». В словаре В. Даля также названы аналогичные значения: «конфиденциальная» — «откровенная, по особой доверенности, неоглашаемая, задушевная»; «тайна» — «кто чего не знает, то для него тайна, все сокрытое, неизвестное, неведомое». Исходя из определений понятия конфиденциальная информация, тайна, секрет являются равнозначными.

С развитием информационных технологий проблема конфиденциальности и конфиденциальной информации приобретает большую значимость. И в различных областях и различных странах конфиденциальность и информация относящаяся к конфиденциальной определяется по разному.

8) Понятие конфиденциальности используется практически во всех областях, как в коммерческих структурах, так и государственных. Когда речь заходит о конфиденциальности на предприятиях, то чаще всего имеется в виду коммерческая или государственная тайна.

*Конфиденциальность* — обязательство неразглашения информации, полученной от испытуемого (в общем случае, от делового партнера, от участника переговоров, собеседника), или в общем случае ограничение её распространения кругом лиц, о которых испытуемый был заранее извещен.

*Государственная тайна* — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности.



## Әдебиеттер тізімі

1. Алдажаров Қ.С. Ақпараттық қауіпсіздік негіздері: Оқу құралы. – Алматы: Эконормика, 2011.
2. Аяжанов Қ.С., Есенова А.С. Ақпараттық қауіпсіздік және ақпаратты қорғау: Оқулық. - Алматы: ЖШС РПБК «Дәуір», 2011.
3. Әлметова Ә., Дәркенбаева Ж., Хамимұльдинова Л., Тұңғатова Ғ. Қазақ тілі: Оқу құралы (С<sub>1</sub> – негізгі стандарттан жоғары деңгейге арналған және С<sub>2</sub> – туризм мамандығы үшін). - Алматы, 2013. - 117 б.
4. Әлметова Ә., Тұңғатова Ғ., Хамимұльдинова Л., Дәркенбаева Ж. Қазақ тілі: Оқу құралы (В<sub>2</sub> – негізгі стандартты деңгей). - Алматы, 2013. - 102 б.
5. Төлеуп М.М. Кәсіби қазақ тілі: 5В071800 – Электр энергетикасы бағыты студенттеріне арналған әдістемелік нұсқаулар. - Алматы: АЭЖБУ, 2013. - 35 б.
6. Тілембекова А.И. Кәсіби қазақ тілі: 5В071900 – Радиотехника, электроника және телекоммуникациялар бағыттары студенттеріне арналған әдістемелік нұсқаулар. - Алматы: АЭЖБУ, 2013. - 35 б.
7. Советова З.С. Кәсіби қазақ тілі: 5В071700 мамандығы студенттеріне арналған әдістемелік нұсқаулар. - Алматы: АЭЖБУ, 2014. - 42 б.

## Мазмұны

1 Алғы сөз.....	3
2 Терминдер және олардың жасалу тәсілдері.....	
3 Синтетикалық тәсіл.....	4
4 Лексика-семантикалық тәсіл.....	6
5 Аналитикалық тәсіл.....	8
6 Аббревиатуралар.....	10
7 Аударма туралы.....	18
8 Аудармаға қойылатын талаптар.....	20
9 Ғылыми-көпшілік және ғылыми техникалық аударма.....	21
10 Техникалық аударма.....	23
11 Ғылыми-техникалық әдебиетті аудару.....	25
12 Баламасыз лексиканы аудару тәсілдері.....	28
Әдебиеттер тізімі.....	

Эльмира Тұрсынқызы Ахметова  
Гүльмира Сатыбалдықызы Әлмұхаметова

КӘСІБИ ҚАЗАҚ ТІЛІ

5В100200 – Ақпараттық қауіпсіздік жүйесі мамандығының  
студенттеріне арналған әдістемелік нұсқаулықтар

Редактор Б. Қасымжанова  
Стандарттау бойынша маман Н. К. Молдабекова

Басуға қол қойылды \_\_\_\_ . \_\_\_\_ . \_\_\_\_ .  
Таралымы 30 дана.  
Көлемі 2,1 оқу-басп.т.

Пішімі 60x84 1/16  
№1 типографиялық қағаз  
Тапсырыс \_\_\_\_ . Бағасы 1050

±

«Алматы энергетика және байланыс университеті»  
коммерциялық емес акционерлік қоғамының  
көшірмелі-көбейткіш бюросы  
050013, Алматы, Байтұрсынов көшесі, 126