# ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ. БІЛІМ БЕРУДІ АҚПАРАТТАНДЫРУ
# ИНФОРМАТИКА. МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ. ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ

**МРНТИ 21.55:34**
**УДК 004.058.56**

**https://doi.org/10.51889/2020-2.1728-7901.31**

*Ж.Т. Айтуғанова [1], Б.Ә. Талпақова[1], Б.К. Жүсіпбек [2]*

*[1]Алматы технологиялық университеті, Алматы қ., Қазақстан*
*[2]Қ.А. Ясауи атындағы Халықаралық қазақ-түрік университеті, Қазақстан*

## ДЕРЕКТЕР ҚОРЫНДА АҚПАРАТТЫ САҚТАУ ҚАУІПСІЗДІГІН АРТТЫРУДЫҢ ТИІМДІ ӘДІСТЕРІ

*Аңдатпа*

Технологияның қарқында дамығын дәуірінде ақпаратты қорғау мәселесі өте өзекті болып отыр. Мақалада компьютерлік жүйелерде ақпаратты байланыс каналдары бойынша оңай және тез көшіріп алуға байланысты ақпарат қауіпсіздігіне байланысты туындаған мәселелер қарастырылған. Ақпаратты қорғау мәселесі заң шығарушы орындардан бастап нақты техникалық құрылғыға дейін кең ауқымды қамтиды. Бағдарламаны өңдеушілер ақпараттың жоғары деңгейде қорғалуын қамтамасыз ететін қорғаудың техникалық құралдары қажеттігін ұсынады. Тәжірибе көрсеткендей ақпараттың қорғалуына бағдарламалық құралдар кепіл бола алмайды. Сондықтан бағдарламалық құралдар ақпаратқа қол жеткізуді, сақтау ережесін анықтайтын ұйымдастыру шараларымен толықтырылды.

Бағдарламалық құралдарды пайдаланушыларға қорғау құралдары пайдалану саласында қосымша қиындық туғызады. Бұл жұмыста қорғау құралдарының классификациясы мен өзіндік қорғау әдістері және де қосымша ақпаратты сұрау салу арқылы қорғау тәсілдері келтірілген.

**Түйін сөздер:** ақпаратты қорғау, мәліметтер қоры, қауіпсіздік, бағдарламалық құралдар, әдістер.

*Аннотация*

*Ж.Т. Айтуганова [1], Б.А. Талпакова [1], Б.К. Жусипбек[2]*
*[1]Алматинский технологический университет, г.Алматы, Казахстан*
*[2]Международный Казахско-турецкий университет им.Х.А.Ясави, Казахстан*

## ЭФФЕКТИВНЫЕ СПОСОБЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ХРАНЕНИЯ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ

В эпоху бурного технологического развития вопрос информационной безопасности очень актуален. В статье рассматриваются вопросы, связанные с информационной безопасностью в компьютерных системах за счет простого и быстрого копирования информации по каналам связи. Проблема информационной безопасности охватывает широкий круг вопросов, от законодательного органа до конкретного технического устройства. Разработчики программы предполагают необходимость технических средств защиты, обеспечивающих высокий уровень защиты информации. Опыт показывает, что программное обеспечение не может гарантировать защиту информации. Поэтому любое программное обеспечение нужно дополнить организационными мерами, определяющими правила доступа и хранения информации. В практике пользователи программного обеспечения сталкиваются с дополнительными проблемами при использовании инструментов безопасности.

В этой статье представлена классификация гарантий и методов самозащиты, а также методы защиты путем запроса дополнительной информации.

**Ключевые слова:** информационная безопасность, база данных, безопасность, программное обеспечение, методы.

*Abstract*

**EFFECTIVE WAYS TO INCREASE THE SECURITY OF STORING INFORMATION IN A DATABASE**

*Aituganova Zh.T.[1], Talpakova B.A.[1], Zhussipbek B.K.[2]*

*[1] Almaty technological University Almaty, Kazakhstan*

*[2] Akhmet Yassawi International Kazakh-Turkish University, Kazakhstan*

In the era of rapid technological development, the issue of information security is very relevant. The article discusses issues related to information security in computer systems due to the simple and quick copying of information through communication channels. The problem of information security covers a wide range of issues, from the legislature to a specific technical device. Program developers suggest the need for technical means of protection that provide a high level of information security. Experience has shown that software cannot guarantee information security. Therefore, any software must be supplemented by organizational measures that determine the rules for access and storage of information. In practice, software users face additional challenges when using security tools.

This article presents a classification of guarantees and methods of self-defense, as well as methods of protection by requesting additional information.

**Keywords:** information security, database, security, software, methods.

Қазіргі кезде біздің елде ақпараттық қауіпсіздікті қамтамассыз ететін бөлімшелердің жұмыс нәтижесінің бағасы стандартқа сай келмейді және ұйымның интегралды қауіпсіздік деңгейін қамтитын арнайы қадағалайтын факторы жоқ. Нақты мәселеге және азаматтық сектордың қажеттілігіне байланысты көзқарастарды трансформацияланған реттелген ведомстволардың дұрыс белгілері жоқ.

Хабарлар тасымалданатын байланыс арналары көбінесе қорғалмаған болып келеді және осы арнаға қатынас құру құқығы бар кез-келген адам хабарларды қолға түсіре алады. Сондықтан тораптарда ақпаратқа біраз шабуылдар жасау мүмкіндігі бар. Қауіпсіздік өзегі барлық қорғаныш тетіктерінің құрылу негізі болып табылады.

Осы жағдайлардың бәрі ақпарат жүйесінің қауіпсіздік саясатын ұйымдастыруды қажет етіп және келесі факторларға бөлінеді:

- қорғау мақсатын анықтау;
- қорғау объектісін анықтау;
- өзекті ақпараттық қылмыстарды, осы қылмысқа кіретін субъектіні анықтау;
- қорғау сапасын анықтайтын әдістерді өңдеу;
- жүйені қорғау кепілдемесін алу.

Тәжірибелік жұмыста ұйым бойынша және ақпараттық ресурстарға байланысты ақпарат қауіпсіздік саясатының анықталмағандығына және бірдеңгейлі болмауына сәйкес түрлі факторларды қолдануға әкеп соғады. Бірдеңгейлі емес және анықталмаған қауіпсіздік саясаты факторлардың бір-бірімен түйісіп қалуына әкеледі.

Ақпараттық жүйедегі қауіпсіздік мәселесін шешетін ұйым қасиеттері:

- Ұйым өзіне сай келетін байланысқа қатысты азаматтық құқық нормасын қалыптастыруы керек, ал мемлекет басқару органдарына әкімшілік құқығын беру қажет.
- Ұйымның негізгі әрекеттер түріне ақпараттық жүйенің қауіпсіздігін байланыстырмау қажет.
- Ұйымның негізгі алға қойған мақсатына қол жеткізу және негізгі функционалды мәселелерді шешу үшін ақпараттық жүйе қауіпсіздігін қамтамассыз ету керек.
- Қауіпсіздік қызметі ереже бойынша қауіпсіздік тәртібін өзі шығармайды, оны тұтынушы мен тапсырыс беретін адам арасындағы келісім бойынша жүзеге асуы керек.

Жеті қауіпсіздік деңгейі

Әрбір деңгейдегі мамандар сатысы, ақпараттық ресурстармен жұмыс жасайтын мамандар өздеріне тән деңгейлік терминологиясын қолданады. Осыған байланысты қауіпсіздік аймағында түсінікті аппарат қалыптасады. Сол себепті осындай аппарат көрші деңгейде қолданылмайды, ал I және VII деңгейлі мамандар бір-бірлерін түсіне алмайды. Көпдеңгейлі модель ресми қолданушылардың қатысуына және ескеруіне өзінің көп үлесін қосады. Әрбір келесі деңгейлерде берілген факторлар түсінірек болады.

Нақты деңгей моделін анықтамай тұрып, оның қауіпсіздік саясатын қарау мағынасыз. Қажетті қауіпсіздік деңгейін сатылай жоғарлататын болсақ, онда біз қорғаудың тең төзімділігіне көңіл аударуымыз қажет. Қауіпсіздік деңгейі ақпараттық қылмыстардың орындалуына байланысты бара-бара өзінің нәтижесіне, яғни мақсатына жетіп, қорғау құралдарының деңгейіне де тоқталып өтеді. Осындай тұрғыдан қарастырсақ, көп жағдайлар аталған саймандарға қатысты болып келеді.

III деңгейге дейін орындалатын әрекеттер түсініктірек бола бастайды. Бекітілмеген рұқсат техникалық қорғауға байланысты көптеген сұрақтарды туындатқан болатын, яғни өте күшті

сертификацияланған құрылғы қауіпсіздікті қамтамассыз етуді жүзеге асыра алады ма? Сұрақтар оның құндылығына және орналасу аймағына байланысты туындады. Ары қарай жағдайлар күрделене түседі. III деігейден жоғарғы деңгейлерде арнайы сертификацияланған қорғау құрылғысы жоқ, қауіпсіздік толығымен басқару жүйесінің программалық баптауын, программаның бүтіндігін қамтамассыз етуін және бизнес-кезеңінің штаттылығын орналастырады. Қауіпсіздікті қамтамассыз ететін баптау тұрақтылығы екі факторға бөлінеді:

- Әкімшілік жүйенің жұмыс сапасы барлық өзгертулерді бақылап отыру үшін әкімшілік саясат бөлімшелеріне бөлу қажет, өз уақытында енгізілген өзгерістерді басқару жүйесінің баптауынан қадағалап отыру қажет. Осы әрекеттерді практика жүзінде қолдану барысында бұл сапаны әлсіретеді, ал басқару саясат рұқсаты, яғни пайдалануға берілген қолданушы құқығы және паролі әкімшілік саясатқа сәйкес келеді.
- Баптауға қолжетімділік дербес компьютерлерге желіні орналастыруға, жай қолданушыларға әкімшілікке кіруге мүмкіндік бермеу керек.

Осы берілген мәселені шешу үшін орталықтандырылған өңдеуге және орталықтанған қауіпсіздік басқаруына өту қажет. Сонымен қатар ақпарат жүйесінің қауіпсіздік төзімділігін бекіте отырып, әкімшілік компоненттер басқаруын жоғарлату керек. Осы шешім кең көлемді АТ-корпорациясын басқаруға кепілдік береді, яғни бұл тек қана толық өңдеуді орталықтандыру болып табылмайды, сонымен қоса әкімшілік ресурстар қолданушылардың әрекеттерін бақылап, әкімшілік аудиттерін тексеріп отырады. Бұл өз кезегінде қауіпсіздіктің логикалық саясатын түсінуге, нақты ұйым үшін ресурстар есебін өндеуге мүмкіндік береді [1].

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

- Бір пайдаланушының екінші пайдаланушыға кедергі келтіруіне жол бермеу;
- 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 (1 сурет).

Мәліметтерді тасымалдауға, бөлмедегі, аумақтағы қорғалған мәліметтерге қол жеткізудің физикалық кедергісі-бұл тосқауыл. Жүйе ресурстарын реттеу әдісімен қорғау арқылы пайдалану қол жеткізуді басқару болып табылады. МБ элементтеріне, тасымалдаушыға бағдарламалық құралдарды пайдаланудың техникалық тұлғасына, пайдаланушыларға арналған жұмыс кестесі белгіленеді [2].

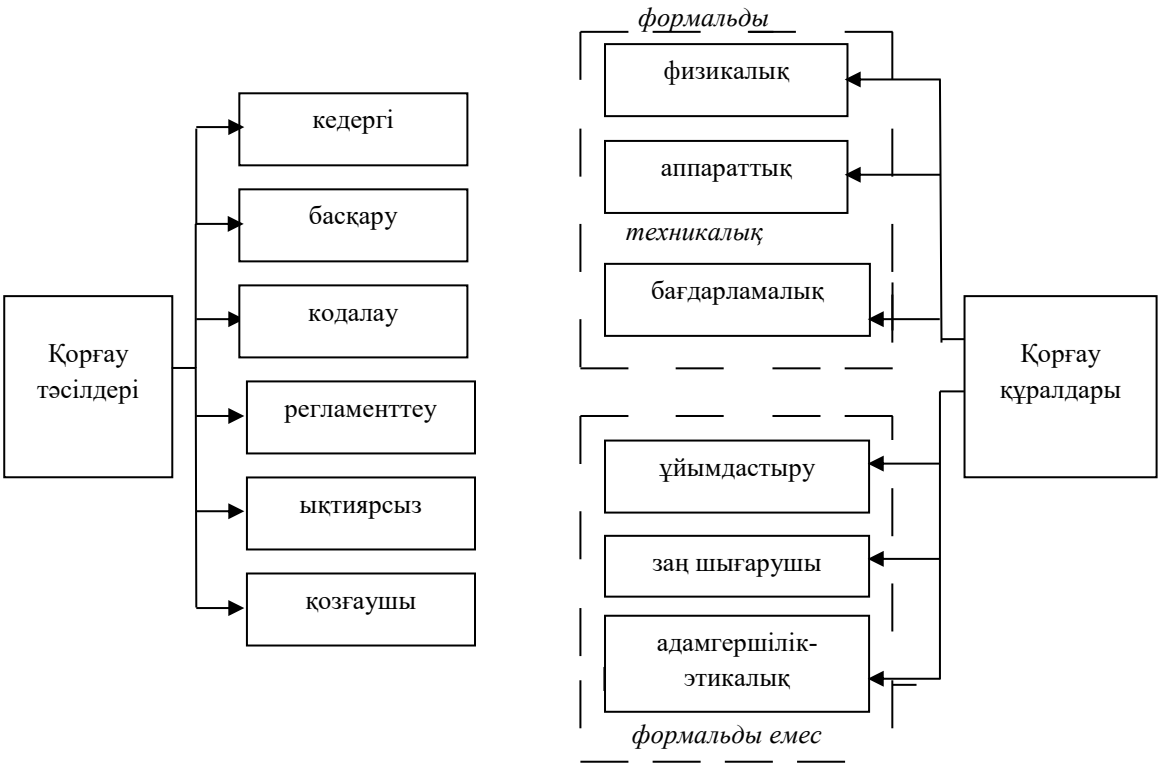
Бұл үшін пайдаланушылардың жұмыс уақыты және қол жеткізу тәртібі мен ресурстар жүйесі тізімінің техникалық персоналға арналған түрін регламенттейді. Берілген, ұсынылған ресурстар тізбесімен пайдаланушылар тізімі жасалынады.

Пайдаланушы тізімінде МБ элементіне арналған қол жеткізуге болатын рәсімдер тізімі белгіленеді. Мәліметтерді тасымалдауға арналған тұлғалар үшін қол жеткізу құқығы бар тұлғалар және оны тұрақты сақтау орны анықталады.

Қол жеткізуді басқару қорғаудың мынадай қызметінен тұрады:

- ресурсты, дербес пайдаланушыны сәйкестендіру бесаспап идентификатор тағайындау және оны таңдау арқылы жүреді;
- өкілеттігі, яғни қабілеттігін тексеру іске қосқан уақытынан бастап ресурстарды сұрағанмен аяқталады;
- белгіленген регламент негізінде ақпаратқа қол жеткізуге рұқсат беру және жағдай жасау;
- сақталған ренсурстардың айналымын тіркеу;
- бекітілмеген жұмыстар түріне әрекет жасаудың нәтижесі.

*Қорғау құралдарының классификациясы*




*Сурет 1. Қорғау құралдарының классификациясы*

Кодалау-бұл мәліметтерді криптографиялық түрлендіру әдісімен қорғаудың бір түрі. Қорғау әдісі пайдаланушы үшін тиімді болып саналса, онда ақпараттарды өңдеу және сақтау барысында, әрі мәліметті байланыс желісімен тарату кезінде пайдаланылып, ақпаратты қорғаудағы тиімді әдіс болып есептеледі.

Регламенттеу-мәліметтерді өңдеу және сақтаудың, бекітілмеген мәліметке қол жеткізудің мүмкіндігі болатындай жағдай туғызатын шаралар жиынтығын тарату және өңдеу болып табылады.

Мәжбүрлеу-бұл дербес және пайдаланушының мәліметтерді қылмыстық, әкімшілік, материалдық жауапкершілік қауіптен сақтаудың, өңдеудің ережесі, яғни пайдаланушыларды әкімшілік, құқықтық, материалдық жауапкершілік қаупінен ақпаратты қорғауға, сақтауға мәжбүрлеу.

Ұйымдастыру құралы дегеніміз – деректердегі ақпаратты өңдеу жүйесін пайдалану және оның қызметі барысында (жобалау, монтаждау, сынау, тексеру, пайдалану) жүзеге асатын ұйымдастыру-құқықтық және ұйымдастыру-техникалық шаралары.

Заң шығарушы құралдарға қол жеткізуді шектеуші мәліметтерді өңдеу, пайдалану ережелері және ережені бұзған жағдайдағы жауапкершілік шаралары қарастырылатын еліміздің құқықтық актілері жатады. Мысалы, Қазақстан Республикасының ақпараттандыру туралы заңы, Байланыс туралы заң, Интегралдық микросхемалар топологияларын құқықтық қорғау туралы заң, Қазақстан Республикасының патент заңы, Бұқаралық апарат құралдары туралы заң, және т.б.

Моральдық (адамгершілік)-этикалық құралдарға даму кезеңінде қалыптасқан және қоғамдағы ақпарат технологиясы таратқан дәстүрлік норма жатады. Бұл нормаларды сақтау міндетті емес, бірақ оны сақтамау телуге әкеліп соғады. Ұйғарымдама ережелер жинағы түрінде болады.

Барлық қорғау құралдары формальды және формальды емес болып бөлінеді. Қорғаудың формальды формаларына адамның қатысуынсыз алдын-ала жұмыста қарастырылған қорғау қызметін атқаратын құралдар жатады. Формальды емес қорғау құралдарына адамдардың мақсаткерлік қызметтері немесе сондай қызметті регламенттеу жатады.

Қорғау тұжырымдамасының дамуын мынадай кезеңдерге бөледі:

1. Бағдарламалық құралдар дамуының артықшылығы.
2. Қорғаныс құралдарының барлық кластарының қарқынды дамуы.
3. Қорғау құралдарының 3 даму тенденциясы:

а) қорғаудың негізгі қызметін аппараттық тарату;

ә) қорғаудың бірнеше қызметін атқаратын қорғаныс құралдарының жиынтығын құру;

б) қорғаныс құралдарын бірыңғайлау және стандарттау.

Қорғаудың техникалық құралдарын қолдану өзіндік, яғни өз бетімен атқарылған шаралар сипатында болады. Көптеген бағдарламалық құралдар (ОЖ, МББЖ) қамтамасыздандарудың жалпы жүйелік компонеттері құрамына кіреді. Ұйымдастыру компонеттерінің жиынтығы деректердегі ақпаратты өңдеу жүйесіндегі ақпараттарды қорғаудың жалпы ұйымдастыру жұмысынан тұрады.

Ақпаратты қорғау мәселесі заң шығарушы орындардан бастап нақты техникалық құрылғыға дейін кең ауқымды қамтиды. Бағдарламаны өңдеушілер ақпараттың жоғары деңгейде қорғалуын қамтамасыз ететін қорғаудың техникалық құралдары қажеттігін ұсынады. Бағдарламалық құралдарды пайдаланушыларға қорғау құралдары пайдалану тарихында қосымша қиындық туғызады. Бірден-бір қорғау құралы болып табылатын – авторлық құқықты мойындау – яғни бағдарламалық құралдарды сату экономикалық жағынан тиімсіз. Бұдан басқа сақтайтын ақпараттардың ашылу деңгейін көтеру және оны өңдеу әдісін (ноу-хау) жоғарылату тағы бар.

Сауда-саттық қатынасында қорғалатын ақпараттың көшірмесін алуға қол сұғуды азайту, пайдаланушымен сәйкестендіру, көшірме жасауға тиым салу, қорғау құралдарына қызмет көрсететін ЕЖ ресурстарынның бөлігін пайдалану шектеулі.

Қорғау құралдары пайдаланушыға ол көшірмесін жасағанша, орындағанға дейін белгісіз болуы керек. Мұндай әрекет ету әдісін АҚШ-тағы өңдеу жүйесіне қызмет көрсетудің Ассоциациясы бойынша қорғау комитеті қабылдады, бұл комитет “үнді перне” атағын алған қорғау аппаратурасының стандартын ұсынды.

Қорғау әдістері деректер мен ЭЕМ-ді қорғаудың әдістері және бағдарламалық жабдықтарды (БЖ) қорғау әдістері болып бөлінеді [3].

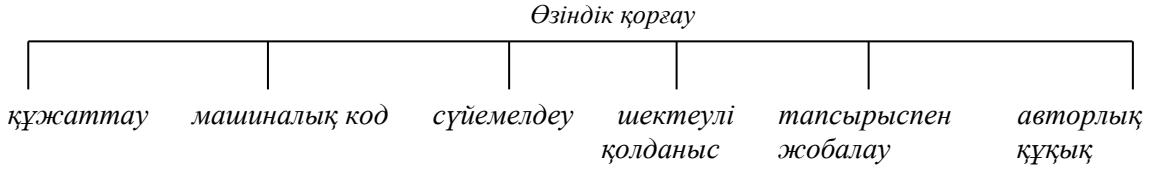
Электронды есептеу машинасын (ЭЕМ) қорғау – аппаратураға физикалық қол жеткізуді шектеуге және парольдер пайдалануға негізделген. ЭЕМ-ді шағын бөлмеге орналастырып оның сақталу, қорғалуына мүмкіндік береді. Жекелей сатылатын бағдарламалық қамтамасыздандыруды поштамен салып, қорғау құралдарын меңгеретіндігін ұзақ мерзімде сынауға болады.

Қорғау құралдары төмендегі категорияларға ажыратылады:

- өзіндік қорғау;
- ЕЖ құрамында қорғау;
- сұрау салу арқылы ақпаратты қорғау;
- активті қорғау;
- пассивті қорғау.

*Өзіндік қорғау құралдары*

Өзіндік қорғау құралдарын төмендегідей сұлба арқылы бейнелеуге болады (2 сурет).




*Сурет 2. Өзіндік қорғау*

Бағдарламалық жабдықты сүйемелдеуші құжат авторлық құқық субъектісі болып саналып, қорғау функцияларын орындай алады. Бағдарламалық жабдық құжатсыз толық бағалы түрде қолданыла алмайды. Бағдарламалық жабдыққа есептеуіш жүйенің бейімделуі қажет болған кезде бағдарламаны өңдеуші тарапынан сүйемелдеудің маңызы ерекше.

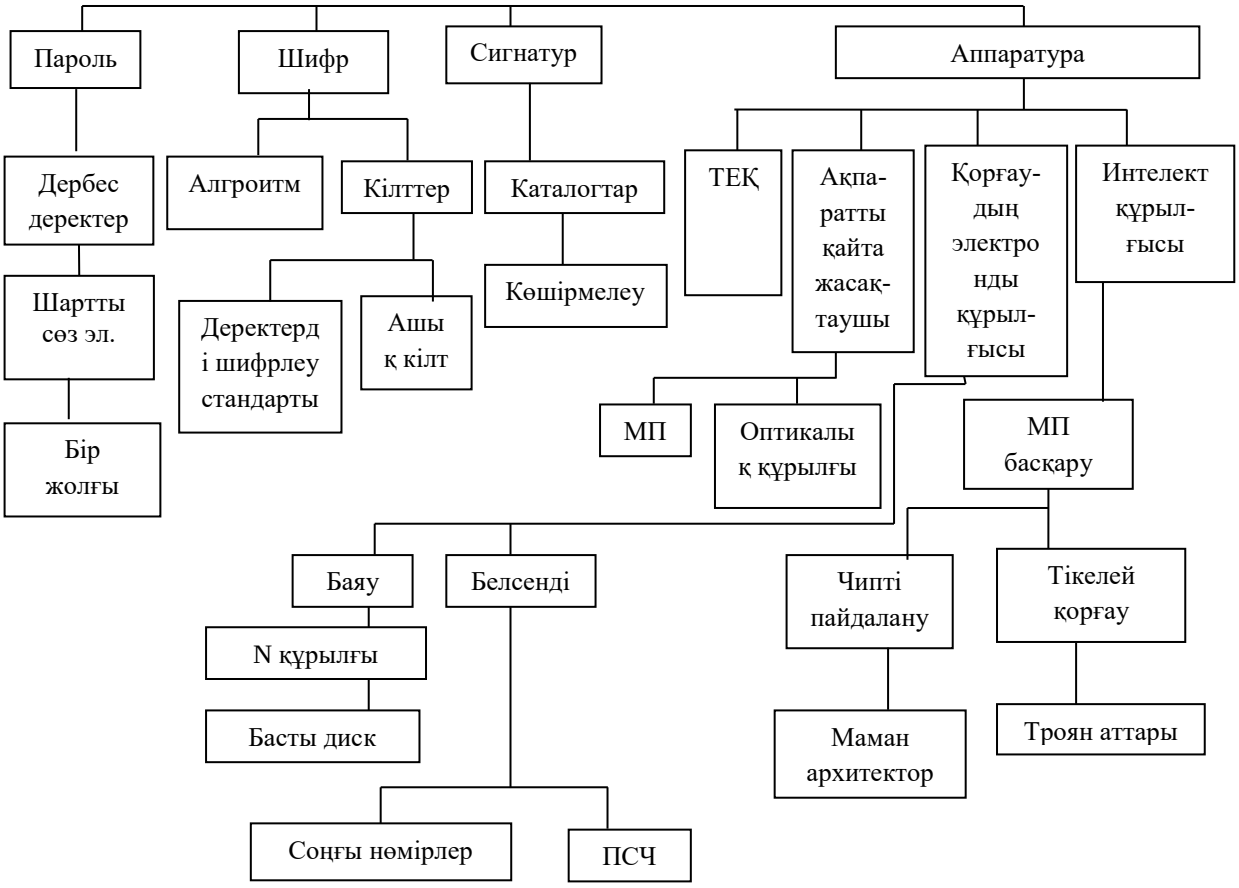
Шектеулі қолданыс пайдаланушылар шеңберін шектейді, бағдарламалық жабдық санаулы қолданушылар шеңберінде пайдаланылады. Тапсырыспен жобалау – бағдарламалық жабдықты арнаулы мақсатқа өңдеу. Егер бағдарлама сирек қолданылатын болса, онда бағдарламаның коммерциялық мақсатта ұрлану қаупі де аз болады. Стандартты бағдарламалық модульдер бағдарламаны сәйкестендіретін, авторлық құқық беретін ерекше белгімен жабдықталады. Жеке таңбалау құны сауда-саттық түсімінен күтілетін түсіммен шамалас болуы керек.

*Сұрау салу арқылы ақпаратты қорғау.* Қосымша ақпараттың жұмысына парольдер, нөмірлер, кілттер түрінде талап етілетін бағдарламалар сұрау салу арқылы ақпаратты қорғау түріне жатады (3 срует).

Парольдер – жүйеге ену үшін қажетті кілттер ретінде қарастырылады және ақпарат тұтастығын сақтауды қамтамасыз етеді бірақ, олар басқа мақсаттар үшін де қолданылады, мысалы, дискіенгізгіште жазуды бұғаттауда, мәліметтерді шифрлеу командаларында, т.б. [4].

Парольдерді 7 негізгі топтарға бөледі:

- қолданушы орнататын парольдер;
- жүйемен генерацияланатын парольдер;
- енудің кездейсоқ кодтары;
- жартылай сөз;
- кілттік фазалар;
- “сұрақ -жауап” түріндегі интерактивті тізбек;
- “қатаң ” парольдер.




*Сурет 3. Қосымша ақпаратты сұрау салу арқылы қорғау*

Шифрлер - ақпаратты түрлендіруге арналған криптографиялық әдістерді пайдалану. Шифрлер криптоаналитиктер үшін қарапайым болу керек, бірақ кәдімгі пайдаланушылар үшін файлға қол жеткізуді қиындатады. Бағдарламаларды, идентификациялық белгілерді шифрлеуге болады. Бағдарламаны қорғауға арналған шифрдың негізгі сипаттамасы - кілттік шифрдың үзындығы болып саналады.

Сигнатуралар – қорғаныс үшін пайдаланылатын және бағдарламалық тәсілмен тексерілетін электронды есептеуіш машинаның бесаспап сипаттамасы.

Қорғау аппаратурасының көмегімен бағдарламны қорғаудың негізгі принципі – тұрақты есте сақтау құрылғысымен оперативті есте сақтау құрылғысынан бағдарламаларды рұқсатсыз көшіру кезінде бағдарламның өздігінен жойылып кетуіне арналған сигналдарды өндіру.

Арнайы микропроцессорлар (МП) – арнайы оптикалық құрылғы, стандартты интерфейс арқылы қосылады, сұрау салуға кейбір сандық реттілікпен үндеседі. Кемшілігі – бағдарламамен басқарылады.

Электр интеллектісімен қорғау – күрделі қорғаныс алгоритмін таратушы арнайы микропроцессоры бар электронды қорғаныс құрылғыларының бірі [5].

Тікелей қорғау құралдары-егер құпия ақпараттардан тұратын модульды бұзатын болса, тікелей қорғау динамикалық жады қорегін бұғаулайды да, құпия ақпараттарды жояды.

Ақпараттық қауіпсіздік режимін қалыптастыру кешендік мәселе болып табылады. Қазіргі таңда бұл өзекті мәселені шешуде криптогрфиялық әдісті пайдалану тиімді болып отыр. Бұл ақпараттың бүтіндігімен және қауіпсіздігімен қамтамасыз ететін өте тиімді әдіс болып табылады. Криптографиялық әдісті техникалық және ұйымдастыру шараларымен біріктіріп қолдану ақпарат қауіпсіздігін кең спектрінен сенімді қорғауларды қамтамасыз етеді.

Криптографиялық хаттамалардың (басты алмасу, электрондық-цифрлық қолтаңба (ЭЦҚ) негізгі типтерін дамыту ашық кілттерді және олардың негізінде шифрлеудің ассиметриялық хаттамаларысыз мүмкін емес.

Асимметриялық криптоалгоритмдердің негізгі идеясы хабарламаны шифрлеу үшін бір кілт, ал шифрлеудің мағынасын ашқан кезде - басқасы пайдаланылады. Одан басқа шифрлеудің рәсімі, шифрлеудің белгілі кілті бойынша тіпті тұрақты болып таңдалған – бұл асимметриялық криптографияның екінші қажетті шарты. Яғни, шифрлеу кілті мен шифрленген мәтінді біле тұрып шығыс хабарламаны қалпына келтіру мүмкін емес – оны тек екінші кілттің – шифрлеудің мағынасын ашатын кілттің көмегімен ғана оқуға болады. Егер ондай болса, онда шифрлеу кілті қандай да бір тұлғаға хаттарды жөнелту үшін - бәрібір оқудың мүмкін еместігін біле тұрып шифрленген хабарламаны ашпауға да болады.

Сондықтан шифрлеу кілтін асимметриялық жүйелерде «ашық кілт» деп атайды, ал шифрлеудің мағынасын ашу кілтін хабарламаны алушыға құпияда ұстау қажет – ол «жабық кілт» деп аталады. Осылай, біз құпия кілттермен алмасудың күрделі міндетін шешу қажеттілігінен құтыламыз. «Неге ашық кілтті біле тұра, жабық кілтті есептеп шығаруға болмайды?» деген сұрақ сұранады – бұл асимметриялық криптографияның үшінші қажетті шарты – шифрлеу және шифрлеудің мағынасын ашу алгоритмдері ашық кілттің жабық кілтті есептеп шығарудың мүмкін еместігін біле тұра құрылады.

Жалпы асимметриялық шифрлеуді пайдаланған кезде хат жазысу жүйесі былайша өрбиді. Хат жазысуды жүргізуші N абоненттердің әрбірі үшін өзінің кілттер жұбы: «ашық» Ej және j – абоненттің нөмірі бар жерде «жабық» Dj таңдап алынған. Барлық ашық кілттер пайдаланушылардың барлығына белгілі, әрбір жабық кілт керісінше ол тиесілі абонентте ғана сақталады. Егер абонент, 7 нөмірлі деп алсақ, 9 нөмірлі абонентке ақпарат бермекші болса, ол деректерді E9 шифрлеу кілтімен шифрлейді және оны 9 абонентіне жөнелтеді. Желіні пайдаланушылардың барлығы E9 кілтін білетіндіктеріне және шифрленген жіберілім жүріп жатқан арнаға қол жеткізу мүмкіндігіне ие екеніне қарамастан олар шығыс хабарламаны оқи алмайды, өйткені шифрлеу рәсімі ашық кілт бойынша тұрақты. Және тек 9 абонент ғана жіберілімді алып, тек өзіне ғана белгілі D9 кілтінің көмегімен оған түрлендіру жүргізеді және жіберілім мәтінін қалпына келтіреді. Егер хабарламаны қарама қарсы бағытта (9 абонентінен 7 абонентіне) жөнелту керек болса, онда басқа кілттер жұбын (шифрлеу үшін E7 кілті, ал дешифрлеу үшін D7 кілті) пайдалану керектігін ескеріңіз.

Көріп тұрғанымыздай, біріншіден асимметриялық жүйелердегі бар кілттер саны абоненттердің симметриялық жүйелердегі сияқты шаршы емес, сызықтық (N пайдаланушыдан жүйеде 2N кілттер пайдаланылады) санымен байланысты. Екіншіден k жұмыс станциясы бұзылған кезде қасқүнем тек Dk кілтті ғана біледі: бұл оның k абонентіне келетін барлық хабарламаларды оқуға мүмкіндік береді, алайда хаттарды жіберген кезде оның орнына өзін қоюға мүмкіндік бермейді.

RSA асимметриялық шифрлеу стандарты.

Асимметриялық шифрлеудің ең таралған алгоритмі RSA алгоритмі болып табылады. Ол үш зерттеуші-математик Рональдом Ривестпен (R.Rivest), Ади Шамирмен (A.Shamir) және Леонард Адльманмен (L.Adleman) ұсынылған болатын. Осы алгоритмнің әзірлеушілеріне құпиямен бір тараптық жұмыс істеу идеясын тиімді асыру мүмкін болды.

RSA төзімділігі үлкен тұтас сандардың күрделілігіне базаланады. 1993 жылы RSA әдісі халыққа берілді және стандарт (PKCS #1: RSA Encryption standart) ретінде қабылданды, RSA шифрлеу/мағынасын ашу үшін сияқты электрондық цифрлық қолтаңбаны туындату/тексеру үшін де қолдануға болады [6].

ЭЦҚ сызбаларының көпшілігінің төзімділігі шифрлеудің және хэш-функциялардың асимметриялық алгоритмдерінің төзімділігіне байланысты. ЭЦҚ сызбаларына шабуылдардың, белгілі және ашық кілтпен шабуылдау түрлері бар. Шабуыл және белгілі қол қойылған хабарламаларымен – қарсылас, ашық кілттен басқа қол қойылған хабарламалар жиынтығына да ие. Қол қойылған хабарламаларды таңдаумен қарапайым шабуыл – қарсылас хабарламаларды таңдау мүмкіндігіне ие, бұл ретте ашық кілт ол хабарламаны таңдағаннан кейін алады. Хабарламаны таңдаумен бейімделген шабуыл.

Әрбір шабуыл бірнеше топтарға бөлуге болатын белгілі бір мақсатты көздейді:

1) толық ашылу. Қарсылас пайдаланушының құпия кілтін табады;

2) әмбебап қолдан жасалған. Қарсылас ЭЦҚ туындату алгоритміне функционалды ұқсас алгоритмді табады;

3) селективті қолдан жасау. Таңдалған хабарламамен қолтаңбаны қолдан жасау;

4) экзистенциалды қолдан жасау. Ең болмаса бір кездейсоқ таңдалған хабарламаның қолтаңбасын қолдан жасау [7].

Практикада ЭЦҚ қолдану мынадай іс-қимылдарды бұзушыларды айқындауға немесе алдын алуға арналған:

1) құжаттың авторлығына қатысушылардың бірінің бас тартуына;

2) қабылданған электрондық құжатты түрлендіруге;

3) құжатты қолдан жасауға мүмкіндік береді;

4) беру үрдісінде хабарламаларды тықпалау – қарсылас хабарламалар алмасуды ұстап алады және оларды түрлендіреді;

5) хабарлама жіберуді қайталау [8].

Сонымен қатар хабарлама алмасу жүйесін олардан қорғау мүмкін емес бұзушылықтар бар – бұл хабарламаны жіберуді қайталау және хабарламаны жіберу уақытын қолдан жасау. Осы бұзушылықтарға қарсы әрекет уақытша қосымшалар мен кіріс хабарламаларды қатаң есепте пайдалануға негізделуі мүмкін.

Қазіргі таңда ақпарат технологиясында апарат қауіпсіздігімен қамтамасыз ету мәселесіннің өз шешімін табуы көптеген салалардағы өзекті мәселелерді шешкен болар еді. Ақпаратты криптографиялық қорғау қазіргі таңда ақпарат қауіпсіздігін қамтамасыз ету мен мемлекет мүдесін қорғауда ең тиімді жол болмақ.

*Пайданылған әдебиеттер тізімі:*


1 *Анин Б. Ю. Защита компьютерной информации. СПб.: БХВ - Санкт-Петербург, 2010.*

2 *Утепбергенов И.Т., Сағындыкова Ш.Н. ақпараттық жүйелердегі деректер қоры. Оқу құралы.2016. 76 бет.*

3 *Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Энергоатомиздат. 2012.*

4 *Гусманова Ф.Р., Абдулкаримова Г.А. Ақпаратты қорғаудың криптографиялық әдістерін оқытудың өзекті аспектілері. //Абай атындағы ҚазҰПУ-нің Хабаршысы. «Физ.-мат. ғылымдары» сериясы, 2019, №4(68), 201 б.*

5 *Домарев В. В. Безопасность информационных технологий. Системный подход - К.: ТИД Диа Софт, 2011. 992 с.*

6 *Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 2013.*

7 *Хоффман Л. Дж. Современные методы защиты информации: Пер. с англ. М.: Сов. радио, 2008.*

8 *Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2014.*


*References:*


1. *Anin B. Ju. (2010) Zashhita komp'juternoj informacii. SPb: BHV - Sankt-Peterburg,.*
2. *Utepbergenov I.T., Sagyndykova Sh.N. (2016) akparattyk zhujelerdegi derekter qory. Oku kuraly. 76.*
3. *Gerasimenko V. A. (2012) Zashhita informacii v avtomatizirovannyh sistemah obrabotki dannyh. V 2-h kn. M: Jenergoatomizdat.*
4. *Gusmanova F.R., Abdulkarimova G.A. (2019) Akparatty korgaudyn kriptografijalyk adisterin okytudyn ozekti aspektileri. Abaj atyndagy KazUPU-nin Habarshysy. «Fiz.-mat. gylymdary» serijasy, №4(68), 201.*
5. *Gusmanova F.R., Abdulkarimova G.A. (2019) Akparatty korgaudyn kriptografijalyk adisterin okytudyn ozekti aspektileri. Abaj atyndaғy KazUPU-nin Habarshysy. «Fiz.-mat. gylymdary» serijasy, №4(68), 201.*
6. *Rastorguev S. P. (2013) Programmnye metody zashhity informacii v komp'juterah i setjah. M. Jahtsmen,.*
7. *Hoffman L. Dzh. (2008) Sovremennye metody zashhity informacii: Per. s angl. M.: Sov. Radio*
8. *Lapina M. A., Revin A. G., Lapin V. I. (2014). Informacionnoe pravo. M.: JuNITI-DANA, Zakon i pravo,*