ҚАРАҒАНДЫ ТЕХНИКАЛЫҚ УНИВЕРСИТЕТІ

А.К. ШЕГЕТАЕВА, Е.Л. МУРЫХ, И.Г. МОЛДАВАНОВА

АҚПАРАТ ҚАУІПСІЗДІГІ МЕН ҚОРҒАУДЫ ҚҰҚЫҚТЫҚ ЖӘНЕ АҚПАРАТТЫҚ ҚАМТАМАСЫЗ ЕТУ

Қарағанды 2020

ҚАРАҒАНДЫ ТЕХНИКАЛЫҚ УНИВЕРСИТЕТІ

«Ақпараттық технологиялар және қауіпсіздік» кафедрасы

А.К. ШЕГЕТАЕВА, Е.Л. МУРЫХ, И.Г. МОЛДАВАНОВА

АҚПАРАТ ҚАУІПСІЗДІГІ МЕН ҚОРҒАУДЫ ҚҰҚЫҚТЫҚ ЖӘНЕ АҚПАРАТТЫҚ ҚАМТАМАСЫЗ ЕТУ

Университеттің Ғылыми кеңесі
оқу құралы ретінде бекіткен

Қарағанды 2020

ӘОЖ 004.056 =512.122
КБЖ 32.97 =632.4
Ш93

Университеттің Редакциялық-баспа кеңесі ұсынған

Пікір жазғандар:

ҚарТУ - дың АТҚ кафедрасының доценті, техника ғылымдарының кандидаты ***Г.Т. Даненова***;

Е.А. Бөкетов атындағы Қарағанды университетінің доценті, техника ғылымдарының кандидаты ***Д.Б. Алибиев;***

ҚарТУ - дың АТҚ кафедрасының доценті, техника ғылымдарының кандидаты ***С.Х. Есенбаев***

Шегетаева А.К.

Ш93 Ақпарат қауіпсіздігі мен қорғауды құқықтық және ақпараттық қамтамасыз ету*:* Оқу құралы / А.К. Шегетаева, Е.Л. Мурых, И.Г. Молдаванова; Қарағанды техникалық университеті. -Қарағанды: ҚарТУ баспасы, 2020. -82б.

ISBN 978-601-320-361-4

Оқу құралы оқу жоспарының талаптарына және "Ақпарат қауіпсіздігі мен қорғауды құқықтық және ақпараттық қамтамасыз ету" пәнінің бағдарламасына сәйкес құрылған.

Бұл оқу құралында "Ақпарат қауіпсіздігі мен қорғауды құқықтық және ақпараттық қамтамасыз ету" курсы аясында оқылатын материал бар. Ақпараттық қауіпсіздік саласындағы қатынастарды құқықтық реттеу мәселелері қаралуда және өзінің еңбек қызметінде қауіпсіз ақпараттық технологияларды құрумен және пайдаланумен айналысатын мамандарды құқықтық даярлауды қамтамасыз етуге арналған.

Оқу құралы 5В100200, 6В06301 "Ақпараттық қауіпсіздік жүйелері", 5В070400 "Есептеу техникасы және бағдарламалық қамтамасыз ету", 6В06104 "Есептеу техникасы және бағдарламалық қамтамасыз ету", 5В050600 "Информатика" мамандықтарының студенттеріне арналған, сондай-ақ, ақпаратты қорғаудың құқықтық негіздерін оқитын басқа мамандықтардың студенттеріне де пайдалы болуы мүмкін.

ӘОЖ 004.056=512.122
КБЖ 32.97 =632.4

ISBN 978-601-320-361-4

МАЗМҰНЫ

Кіріспе

Цифрландыру процесі пайдаланушылардың көбеюін қамтиды, бұл құқықтық және заңнамалық нормаларды бұзудың ықтимал проблемаларын тудырады.

Кейде Интернет-ресурстар мен әлеуметтік желілерді пайдалану кезінде Қауіпсіз жұмыстың қарапайым ережелерін сақтамау жеке өмірге басып кіру, жалпыға қолжетімді жеке деректерді рұқсатсыз пайдалану немесе түрлендіру, жеке деректерді жария ету, қылмыстық қауымдастықтар үшін шектеулі қол- жетімділік туралы ақпараттың жоғары қаупіне әкеледі.

Құқықтық шектеулер туралы білімнің болмауы басқа азаматтардың құқықтары мен бостандықтарын, бағдарламалық қамтамасыз етуге авторлық және сабақтас құқықтар иелерінің құқықтарын бұзатын және ақпараттық ресурстардың жұмыс істеуіне әсер ететін іс-әрекеттерге жол берілуінің елесін тудырады.

Бұл оқу құралының негізгі мақсаты - келесі бөлімдерден тұратын "Ақпарат қауіпсіздігі мен қорғауды құқықтық және ақпараттық қамтамасыз ету" курсын меңгеру үшін оқу материалын ұсыну:

1.Ұлттық қауіпсіздік ұғымы;

2. Мемлекеттік құпияларды қорғаудың құқықтық негіздері;

3. Ақпараттық қауіпсіздік;

4. Зияткерлік меншікті қорғау;

5. Дербес деректерді қорғау;

6. Ақпараттық жүйелердің аудиті;

7. Таратылуы шектеулі ақпарат

8. Электрондық құжат және электрондық цифрлық қолтаңба.

9. АКТ саласындағы ҚР заңнамасын бұзғаны үшін жауапкершілік.

10. Ақпаратты қорғау әдістері

Нұсқаулықта студенттер ақпараттық қауіпсіздікті қамтамасыз етудің құқықтық базасы ретінде пайдалана алатын ҚР заңнамалық актілеріне сілтемелер берілген.

Нормативтік-құқықтық және әдістемелік құжаттарға сілтемелер 01.09.2020ж. жағдай бойынша беріледі.

1 Ұлттық қауіпсіздік ұғымы

Қазақстан Республикасының Конституциясына сәйкес, 20-баптың 2-тармағы. "Әркімнің заң жүзінде тыйым салынбаған кез келген тәсілмен еркін ақпарат алуға және таратуға құқығы бар" [1].

1.1 Ұлттық қауіпсіздік саласындағы қатерлер мен мүдделер

Ұлттық қауіпсіздік саласындағы құқықтық қатынастар "Қазақстан Республикасының Ұлттық қауіпсіздігі туралы" 2012 жылғы 6 қаңтардағы № 527-IV Заңымен реттеледі [2].

Қазақстан Республикасының Ұлттық қауіпсіздігі – бұл адамның және азаматтың, қоғам мен мемлекеттің серпінді дамуын қамтамасыз ететін Қазақстан Республикасы Ұлттық мүдделерінің нақты және ықтимал қауіп-қатерлерден қорғалуының жай-күйі.

Қазақстан Республикасының ұлттық қауіпсіздігін қамтамасыз ету ұлттық мүдделерді нақты және ықтимал қауіп-қатерлерден қорғауға бағытталған ұлттық қауіпсіздік субъектілерінің қызметін қамтиды.

Ұлттық қауіпсіздік саласындағы мемлекеттік саясат шеңберінде Ұлттық қауіпсіздік субъектілері іске асыратын құқықтық, ұйымдастырушылық, экономикалық, техникалық және өзге де шаралардың жиынтығы Қазақстан Республикасының ұлттық қауіпсіздігін қамтамасыз ету жүйесі болып табылады.

Қазақстан Республикасының ұлттық мүдделері – іске асырылуына мемлекеттің адам мен азаматтың құқықтарын, Қазақстан қоғамының құндылықтарын және конституциялық құрылыс негіздерін қорғауды қамтамасыз ету қабілеті байланысты болатын, Қазақстан Республикасының заң жүзінде танылған саяси, экономикалық, әлеуметтік және басқа да қажеттіліктерінің жиынтығы.

Қазақстан Республикасының ұлттық мүдделерін іске асыруға кедергі келтіретін сыртқы және ішкі факторлардың (процестер мен құбылыстардың) жиынтығы ұлттық қауіпсіздікке төнетін қатерлер болып табылады.

Ұлттық қауіпсіздік объектілері:

- адам, оның өмірі, құқықтары мен бостандықтары;
- қоғам, оның материалдық және рухани құндылықтары;
- мемлекет, оның конституциялық құрылысы.

Ұлттық қауіпсіздік субъектілері:

- мемлекет;
- Қазақстан Республикасының азаматтары мен ұйымдары.

Ұлттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттары ұлттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті жүзеге асыру кезінде

заңдылықты сақтау; адамның және азаматтың құқықтары мен бостандықтарының басымдығы болып табылады.

Ұлттық қауіпсіздікке төнетін негізгі қатерлер:

- заңдылық пен құқық тәртібі деңгейінің төмендеуі, қылмыстың өсуі, мемлекеттік органдардың криминалдық құрылымдармен, террористік немесе экстремистік ұйымдармен бірігуі, лауазымды адамдардың капиталдың заңсыз айналымына қолдау көрсетуі, сыбайлас жемқорлық;

- демографиялық ахуалдың және халық денсаулығының нашарлауы, оның ішінде бала туудың күрт төмендеуі, өлім-жітімнің артуы;

- елдің денсаулық сақтау, білім беру және зияткерлік әлеуеті деңгейі мен сапасының төмендеуі;

- Қазақстан Республикасы халқының мәдени және рухани мұрасын жоғалту;

- ұлтаралық және конфессияаралық қақтығыстардан, жаппай тәртіпсіздіктерден көрінетін әлеуметтік және саяси жағдайдың ушығуы;

- конституциялық құрылысты күштеп өзгертуге, оның аумағының тұтастығына, қол сұғылмаушылығына, бөлінбестігіне, күзетілетін адамдардың қауіпсіздігіне бағытталған қызмет;

- терроризм, экстремизм және сепаратизм олардың кез келген нысандары мен көріністерінде;

- қаржы жүйесі тұрақтылығының төмендеуі;

- Мемлекеттік шекараға қол сұғылмаушылық және Қазақстан Республикасына қатысты күш қолдану қатері, оған қарсы агрессия, елдің қорғаныс қабілеті деңгейінің төмендеуі;

- Қазақстан Республикасының заңнамасында көзделмеген әскерилендірілген құрамалар құру;

- елдің ақпараттық кеңістігінің, сондай-ақ, ұлттық ақпараттық ресурстардың рұқсат етілмеген қолжетімділіктен қорғалу деңгейін төмендету;

- ұлттық қауіпсіздікке нұқсан келтіре отырып, ақпаратты әдейі бұрмалаумен және дәйексіз ақпаратты таратумен байланысты қоғамдық және жеке санаға ақпараттық ықпал ету;

- экологиялық ахуалдың, оның ішінде ауыз су сапасының күрт нашарлауы, дүлей зілзалалар және табиғи және техногендік сипаттағы өзге де төтенше жағдайлар, эпидемия мен эпизоотия;

- нәсілдік, ұлттық, әлеуметтік, діни төзімсіздікті, тектік-топтық айрықшалықты қоздыру мақсатында жиналыстар, митингілер, шерулер, пикеттер және демонстрациялар өткізу, конституциялық құрылысты күштеп құлату, республиканың аумақтық тұтастығына қол сұғу, сондай-ақ, Қазақстан Республикасы Конституциясының, заңдары мен өзге де нормативтік құқықтық актілерінің басқа да ережелерін бұзу не оларды өткізу қоғамдық тәртіп пен азаматтардың қауіпсіздігіне қатер төндіреді.

ҚР өз аумағында әрбір адам мен азаматтың қауіпсіздігін қамтамасыз етеді. Мемлекет ҚР аумағынан тыс жерлерде жүрген Қазақстан азаматтарын қорғауға және оларға қамқорлық жасауға кепілдік береді.

Ақпараттық қауіпсіздік бағытталған:

- Қазақстанның ақпараттық тәуелділігіне жол бермеу;
- басқа мемлекеттер, ұйымдар мен жеке тұлғалар тарапынан ақпараттық өктемдік пен блокадаға жол бермеу;
- ҚР Президентінің, Парламентінің, Үкіметінің және ұлттық қауіпсіздікті қамтамасыз ету күштерінің ақпараттық оқшауланuына жол бермеу;
- ҚР қауіпсіздігін сақтау мақсатында, оның ішінде ерекше кезеңде және табиғи, техногендік сипаттағы төтенше жағдайлар, карантиндер, өзге де төтенше жағдайлар туындаған кезде байланыс желілерін үздіксіз және тұрақты пайдалануды қамтамасыз ету;
- мемлекеттік құпияларды және заңмен қорғалатын өзге де құпияны құрайтын мәліметтердің жария болуы мен жоғалуын анықтау, олардың алдын алу және жолын кесу;
- ұлттық қауіпсіздікке нұқсан келтіре отырып, ақпаратты әдейі бұрмалаумен және дәйексіз ақпаратты таратумен байланысты қоғамдық және жеке санаға ақпараттық ықпал етуге жол бермеу;
- ұлттық қауіпсіздікке нұқсан келтіре отырып, мемлекеттік шешімдерді әзірлеу және қабылдау процесіне жасырын ақпараттық ықпал ету тетіктерін табу және оларды іріткі салу;
- мемлекеттік, коммерциялық және заңмен қорғалатын өзге де құпияны құрайтын мәліметтер айналымда болатын ақпараттық ресурстарды, Ақпараттық жүйелерді және байланыс инфрақұрылымын қорғаудың тиімді жүйесін қолдау және дамыту.

2. ҚР-да ақпараттық қауіпсіздікті қамтамасыз етудің ұлттық жүйесі, оның ішінде мемлекеттік электрондық ақпараттық ресурстар, ақпараттық жүйелер, ақпараттық-коммуникациялық инфрақұрылым және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері құрылуда және нығайтылуда.

Ұлттық мүдделерді қорғау және ҚР ақпараттық оқшауланuына жол бермеу мақсатында мемлекеттік уәкілетті органдар инвесторларға берілетін кепілдіктерді сақтай отырып, магистральдық байланыс желілерін, сондай-ақ, шетелдік қатысуы бар ұйымдардың басқаруындағы немесе меншігіндегі байланыс желілерін басқаруды және пайдалануды жүзеге асыратын ұйымдардың қызметіне заңнамада айқындалған тәртіппен бақылауды жүзеге асырады.

Ұлттық мүдделерге қайшы келетін шешімдер қабылдауға және іс-әрекеттер жасауға жол берілмейді:

1) ҚР ақпараттық кеңістігін қалыптастыру және үздіксіз жұмыс істеу;

2) Қазақстанның әлемдік байланыс және ақпараттандыру жүйесіне кіруі;

3) ҚР ақпараттық ресурстарын, ақпараттық жүйелерін және байланыс инфрақұрылымын қорғау деңгейін қамтамасыз ету және арттыру.

Мемлекеттік құпияларды және заңмен қорғалатын өзге де құпияны жария етуге тыйым салынады;

Қазақстан Республикасының аумағында заңды тұлға құрмай шетелдіктердің, азаматтығы жоқ адамдардың және шетелдік заңды тұлғалардың магистральдық байланыс желілерін басқаруы немесе пайдалануы;

- ҚР аумағында басқару орталығы оның шегінен тыс орналасқан байланыс желілерін құру және пайдалану;

- жеке және заңды тұлғалардың дербес немесе тұлғалар тобының құрамында дауыс беретін акциялардың, сондай-ақ байланыс және ақпарат саласындағы уәкілетті органның, сондай-ақ ұлттық қауіпсіздік органдарының келісімінсіз қалааралық және (немесе) халықаралық байланыс операторы ретінде байланыс желісін басқару немесе пайдалану жөніндегі қызметті иеленетін және (немесе) жүзеге асыратын ұйымның үлестерін, пайларын сатып алуы немесе меншігіне өзге де алуы;

- байланыс және ақпарат саласындағы уәкілетті органның қорытындысына негізделген Қазақстан Республикасы Үкіметінің оң шешімінсіз қалааралық және (немесе) халықаралық байланыс операторы ретінде телекоммуникациялар саласындағы қызметті жүзеге асыратын, жерүсті (кәбілдік, оның ішінде талшықты-оптикалық, радиорелелік) байланыс желілерін иеленетін заңды тұлғаның дауыс беретін акцияларының, сондай-ақ, үлестерінің, пайларының 49 пайызынан астамын шетелдіктерге, азаматтығы жоқ адамдарға және шетелдік заңды тұлғаларға тікелей және (немесе) жанама иеленуге, пайдалануға, оларға билік етуге және Ұлттық қауіпсіздік органдарымен келісілген;

- жедел-іздестіру, қарсы барлау іс-шараларын қамтамасыз ету жөніндегі нормативтік құқықтық актілердің талаптарына жауап бермейтін байланыс желілерін пайдалануға беру.

Бақылау сұрақтары:

1. Ұлттық қауіпсіздіктің негізгі қауіптері қандай?
2. Ұлттық қауіпсіздіктің негізгі түрлерін атаңыз.
3. Қазақстан Республикасының негізгі ұлттық мүдделері қандай?

2 Мемлекеттік құпияларды қорғаудың құқықтық негіздері

2.1 Негізгі терминдер мен анықтамалар

Қазақстан Республикасының ұлттық қауіпсіздігін қамтамасыз ету мүддесінде мемлекеттік құпияларды қорғаудың құқықтық негізін және бірыңғай жүйесін 1999 жылғы 15 наурыздағы N 349-1 "Мемлекеттік құпиялар туралы" заң реттейді [3].

Мемлекеттік құпиялар-бұл мемлекет қорғайтын және мемлекеттік және қызметтік құпиядан тұратын, әртүрлі қызметті жүзеге асыру мақсатында таралуын мемлекет шектейтін мәліметтер.

Мемлекеттік құпияларды құрайтын мәліметтерді қамтитын электрондық ақпараттық ресурс-бұл мемлекеттік құпияларға жатқызылған, электрондық-цифрлық нысанда берілген және электрондық жеткізгіште қорғалған түрде қамтылған ақпарат;

Мемлекеттік құпия – бұл жария етілуі немесе жоғалуы Қазақстан Республикасының ұлттық қауіпсіздігіне нұқсан келтіретін немесе нұқсан келтіруі мүмкін әскери, экономикалық, саяси және өзге де сипаттағы мәліметтер;

Қызметтік құпия-бұл жария етілуі немесе жоғалуы мемлекеттің ұлттық мүдделеріне, Қазақстан Республикасының мемлекеттік органдары мен ұйымдарының мүдделеріне нұқсан келтіруі мүмкін мемлекеттік құпияның құрамына кіруі мүмкін жекелеген деректер сипаты бар мәліметтер.

Құпиялылық белгісі-бұл жеткізгіштегі мәліметтердің құпиялылық дәрежесін куәландыратын, жеткізгіштің өзінде және (немесе) оған ілеспе құжаттамада қойылатын деректемелер.

Мемлекеттік құпияларды құрайтын мәліметтерге қол жеткізу - бұл белгілі бір адамды мемлекеттік құпияларды құрайтын мәліметтермен өкілетті лауазымды тұлға санкциялаған таныстыру;

Мемлекеттік құпияларға рұқсат беру - бұл азаматтардың мемлекеттік құпияларды құрайтын мәліметтерге қол жеткізу, ал ұйымдардың осындай мәліметтерді пайдалана отырып жұмыстар жүргізу құқығын ресімдеу рәсімі;

Мәліметтер мен олардың көздерін құпияландыру-бұл мемлекеттің ұлттық қауіпсіздігін қамтамасыз ету мүддесінде мемлекеттік құпияларды құрайтын мәліметтерді таратуды және олардың көздеріне қол жеткізуді шектеу жөніндегі іс-шаралар жиынтығы;

Мемлекеттік құпияларды жария ету-бұл мемлекеттік құпияларды олармен танысу құқығы берілмеген заңды және жеке тұлғаларға хабарлау, беру, беру, жіберу, жариялау немесе кез келген басқа тәсілдермен жеткізу;

Мемлекеттік құпияларды жоғалту-бұл мәліметтердің, оның ішінде, мемлекеттік құпияларды құрайтын уақытша мәліметтердің жоғалуы не ұрлануы салдарынан заңды иеленуден немесе пайдаланудан шығуы.

2.2 Қазақстан Республикасының мемлекеттік құпияларына жататын мәліметтер

Мемлекеттік құпиялар және осы мәліметтердің көздері Қазақстан Республикасының меншігі болып табылады.

Мәліметтерді мемлекеттік құпияларға жатқызуды "мәліметтерді мемлекеттік құпияларға жатқызу жөніндегі өкілеттіктер берілген мемлекеттік органдардың лауазымды адамдарының тізбесіне"сәйкес мемлекеттік органдардың басшылары жүзеге асырады.

Аталған лауазымды адамдар басқаратын мемлекеттік органдарға өз құзыреті шегінде Қазақстан Республикасының мемлекеттік құпияларын құрайтын мәліметтерге билік ету өкілеттіктері беріледі.

ҚР Мемлекеттік құпиялары болып табылатын мәліметтер мен олардың жеткізгіштерін құпияландыру қағидаттарға сәйкес жүзеге асырылады:

- заңдылық, яғни Қазақстан Республикасының Конституциясы мен заңдарына сәйкестік;
- негізділігі, яғни нақты мәліметтерді құпияландырудың орындылығын сараптамалық бағалау;
- уақытылы, яғни. осы ақпаратты алған немесе әзірлеген сәттен бастап таратуға шектеулер қою.

Мәліметтерді мемлекеттік құпияларға жатқызу олардың салалық, ведомстволық немесе бағдарламалық-нысаналы тиесілігіне сәйкес жүзеге асырылады.

Мемлекеттік органдар құпияландыруға жататын мәліметтердің ведомстволық (салалық) тізбелерін әзірлейді. Бұл тізбелерді тиісті мемлекеттік органдар мен ұйымдардың басшылары бекітеді. Осы тізбелердің мазмұнымен құпияландырудың орындылығы айқындалады.

Мәліметтерді мемлекеттік құпияларға жатқызу қажеттілігінің негіздемесі осы мәліметтер алынған (әзірленген) мемлекеттік органдар мен ұйымдарға жүктеледі.

Мәліметтерді мемлекеттік құпияларға жатқызудың негізділігіне сот тәртібімен шағым жасалуы мүмкін. Егер сот мәліметтерді құпияландырудың негізсіздігі туралы шешім қабылдаса, онда бұл мәліметтер құпиясыздандыруға жатады.

Мәліметтерді мемлекеттік құпияларға жатқызу жөнінде өкілеттіктер берілген лауазымды адамдар азаматтар мен ұйымдардың меншігіндегі мәліметтер мен олардың көздерін құпияландыру туралы шешімдер қабылдауға құқылы. Көрсетілген мәліметтер көздерін құпияландыру

мәліметтер көздерінің меншік иесі мен осы мәліметтер мен олардың көздері қарамағына өтетін мемлекеттік органдар мен ұйымдар арасындағы осы мәліметтерді иеліктен шығару туралы шарт негізінде жүзеге асырылады.

Мемлекеттік құпияларды құрайтын мәліметтерді құпияландыру мерзімі отыз жылдан аспауға тиіс. Ерекше жағдайларда бұл мерзім мемлекеттік құпияларды қорғау жөніндегі уәкілетті мемлекеттік органның қорытындысы бойынша ұзартылады.

Бюджет қаражаты есебінен өткізілетін Ұлттық бірыңғай тестілеуді, кешенді тестілеуді және тестілеудің басқа да түрлерін өткізу кезінде пайдаланылатын тестілердің мазмұнын және олардың дұрыс жауаптарының кодтарын ашатын мәліметтерге қатысты мәліметтерді құпияландыру мерзімдері тестілердің мазмұнын және олардың дұрыс жауаптарының кодтарын қалыптастыру кезінен бастап тестілеу рәсімі аяқталғанға дейін жыл сайын белгіленеді.

2.3 Мәліметтердің құпиялылық дәрежелері және осы мәліметтер көздерінің құпиялылық белгілері

Мемлекеттік құпияларды құрайтын мәліметтердің құпиялылық дәрежесін айқындау кезінде көрсетілген мәліметтерді тарату салдарынан Қазақстан Республикасының ұлттық қауіпсіздігіне немесе ұйымдардың мүдделеріне нұқсан келтірудің ықтимал дәрежесі ескерілуге тиіс.

Ақпараттың құпиялылығының үш деңгейі белгіленген:

- «аса маңызды»;
- «өте құпиялы»;
- «құпия».

Мемлекеттік құпияны құрайтын мәліметтерге «аса маңызды» және «өте құпия» құпия белгілері беріледі.

Қызметтік құпияны құрайтын мәліметтер «құпия» болып табылады.

Мемлекеттік құпияға жатпайтын мәліметтерді құпиялау үшін осы құпияларды пайдалануға жол берілмейді. Көрсетілген ақпаратқа басқа белгілерді тағайындауға жол берілмейді.

Мемлекеттік құпияларды құрайтын ақпарат тасымалдаушыларда мәліметтер, оның ішінде келесі мәліметтер қолданылады:

- қолданыстағы мемлекеттік органда немесе ұйымда құпиялануға жататын мәліметтер тізімінің тиісті тармағына сілтеме жасай отырып, тасымалдаушыда қамтылған ақпараттың құпиялылық дәрежесі;
- бұқаралық ақпарат құралдарын жіктеген мемлекеттік органның немесе ұйымның атауы;
- тіркеу нөмірі;

- мәліметтерді құпиясыздандыру күні немесе шарттары не ол басталғаннан кейін мәліметтер құпиясыздандырылатын оқиға туралы ақпарат беріледі.

Егер деректерді тасымалдаушыларға мұндай мәліметтерді қолдану мүмкін болмаса, онда бұл мәліметтер ілеспе құжаттамада көрсетілген.

Мемлекеттік құпияларды құрайтын мәліметтері бар мемлекеттік органдар мен ұйымдар осы ақпаратты және оларды тасымалдаушыларды қорғауды қамтамасыз ету бойынша шаралар қабылдауға міндетті.

«Мемлекеттік құпиялар туралы» [2] заңда лауазымды адамдар мен азаматтарды мемлекеттік құпияларға жіберудің үш нысаны белгіленген, олар мемлекеттік құпияларды құрайтын мәліметтердің үш дәреже құпиялылығына сәйкес келеді: «аса маңызды», «өте құпия» немесе «құпия». Шенеуніктер мен азаматтардың құпиялылықтың неғұрлым жоғары деңгейдегі ақпаратқа қол жеткізуі олардың төменгі деңгейдегі ақпаратқа қол жеткізуінің негізі болып табылады.

Лауазымды адамдар мен азаматтардың мемлекеттік құпияларға кіруін тіркеу немесе қайта ресімдеу мерзімдері, мән-жайлары мен тәртібін Қазақстан Республикасының Үкіметі белгілейді.

Шетел азаматтарына мемлекеттік құпияларға тек Қазақстан Республикасымен халықаралық шарттарды орындау шеңберінде қол жеткізуге рұқсат етіледі.

Қазақстан Республикасының лауазымды адамдары мен азаматтарын мемлекеттік құпияларға жіберу мемлекет алдындағы жазбаша міндеттемелерді, кез-келген жұмысты орындау барысында өздеріне белгілі болған мемлекеттік құпияларды құрайтын мәліметтерді жария етпеу, сондай-ақ, олардың құқықтарын ішінара, уақытша шектеуге келісім беруді көздейді.

Мемлекеттік органның немесе ұйымның, сондай-ақ, олардың мемлекеттік құпияларды қорғау жөніндегі құрылымдық бөлімшелерінің басшысы лауазымды адамның мемлекеттік құпияларды құрайтын ақпаратқа қолжетімділігін ұйымдастыруға жауапты.

Еңбек шарты тоқтатылған кезде лауазымды адамның мемлекеттік құпияларды құрайтын ақпаратқа қол жетімділігі тоқтатылады.

Мемлекеттік құпияларды құрайтын мәліметтерді пайдалануға, мемлекеттік құпияларды қорғау құралдарын жасауға, сондай-ақ, мемлекеттік құпияларды қорғау жөніндегі іс-шараларды жүзеге асыруға және (немесе) қызметтер көрсетуге байланысты ұйымдардың қызметі Қазақстан Республикасы Ұлттық қауіпсіздік комитеті және оның органдары берген рұқсат негізінде жүзеге асырылады.

Рұқсат Қазақстан Республикасының Үкіметі айқындайтын тәртіппен жүзеге асырылатын ұйымдарды арнайы тексеруден өткізу және олардың басшыларын аттестаттау нәтижелері негізінде беріледі.

Мемлекеттік құпияларды құрайтын ақпаратты қорғау құралдарында олардың құпиялылықтың тиісті дәрежесіндегі ақпаратты қорғауға қойылатын талаптарға сәйкестігін растайтын куәлігі болуы керек.

Бақылау сұрақтары:

1. «Мемлекеттік құпияларға» анықтама беріңіз.
2. Мемлекеттік құпияларға жататын мәліметтерді атаңыз.
3. «Қызметтік құпия» анықтамасын беріңіз.
4. Әскери саладағы Қазақстан Республикасының мемлекеттік құпияларына қатысты мәліметтерді атаңыз.
5. Қазақстан Республикасының экономика, білім, ғылым және техника саласындағы мемлекеттік құпияларына қатысты мәліметтерді тізімдеңіз.
6. Құпияландыруға жатпайтын ақпаратты тізімдеңіз.
7. Құпиялылықтың қанша деңгейі бар?
8. Құпия белгілері қандай?
9. Лауазымды адамның мемлекеттік құпияларды құрайтын мәліметтерге қолжетімділігі қашан тоқтатылады?

3 Ақпараттық қауіпсіздік

3.1 Ақпараттық қауіпсіздіктің пайда болуы мен даму тарихы

Ақпараттық коммуникациялардың дамуымен кжәне олардың көмегімен сақталатын және берілетін ақпаратқа зиян келтіру мүмкіндігі негізінде ақпараттық қауіпсіздік (АҚ) пайда болды. Ақпараттық қауіпсіздіктің 1816 жылға дейінгі негізгі міндеті субъект (ұйым немесе белгілі бір адам) үшін ерекше маңызы бар әртүрлі ақпараттарды қорғау болды. Радиобайланыс мүмкіндіктерін енгізу мен қолдану радиоэлектрондық байланыстың бөгеттерден қорғанысын кодтау мен сигналдың декодтауын қолдану арқылы қорғауды қамтамасыз ету қажеттілігін анықтады. Кейін радиолокациялық және гидроакустикалық құрылғылар пайда болды (1935), олардың ақпараттық қауіпсіздігі радиолокациялық құрылғыларды электронды интерференциялардың әсерінен қорғауды күшейту арқылы қамтамасыз етілді. 1946 жылдан бастап іс жүзінде электронды есептеуіш машиналарды (компьютерлерді) кеңінен қолдана отырып, ақпараттық қауіпсіздікке негізінен қорғалатын ақпаратты қамтыған немесе өңдейтін жабдыққа физикалық қол жетімділікті шектеу арқылы қол жеткізілді. 1965 жылдан бастап жергілікті желілер дамып келеді, оның ақпараттық қауіпсіздігі негізінен әкімшілендіру және желілік ресурстарға қол жеткізуді бақылау арқылы жүзеге асырылды. Ұялы байланыс құралдарының енгізілуімен ақпараттық қауіпсіздікке қатысты қауіптер едәуір күрделі және күрделі бола бастады. Қауіпсіздіктің жаңа әдістерін әзірлеу қажет болды, өйткені ақпаратты беру және сақтау үшін сымсыз деректерді беру желілері кеңінен қолданылды. Мақсаты әр түрлі көлемдегі (жеке қолданушылардан бастап бүкіл елдерге дейін) ақпараттық қауіпсіздікке зиян келтіру болатын адамдар қауымдастық - хакерлер пайда болды. Содан бері ақпараттық қауіпсіздік ел қауіпсіздігінің маңызды және міндетті компонентіне айналды. Ақпараттық қауіпсіздік мәселесін шешуге арналған ғаламдық желілер дамыған кезде бүкіл адамзаттың ақпараттық қауіпсіздігінің макрожүйесін құру арқылы шешу керек. Ақпаратты беру, өңдеу, сақтау бүгінде тек ақпараттық жүйелердің көмегімен жүреді. Жаһандық желілер байланыс саласындағы (мысалы, электронды пошта, ұялы телефондар), ойын-сауық (MP3, сандық теледидар, ойындар), көлік (қозғалтқыштар, навигация), сауда (несиелік карталар, интернет- дүкендер), медицина (жабдық, медициналық материалдардың мұрағаттары) және т.б салаларында көптеген қызмет атқаруға мүмкіндік береді.

Сонымен, ақпараттық қауіпсіздіктің міндеттері шабуылдарды анықтау, алдын алу және оларға жауап беру әдістерімен ақпаратты қорғау болып табылады.

3.2 Ақпараттық қауіпсіздік мәселелері

Ақпараттық қауіпсіздік кез-келген қауіпсіздік деңгейінің маңызды аспектілерінің бірі болып табылады - ұлттық, салалық, корпоративті немесе жеке. Ақпараттық қауіпсіздіктің басты проблемасы - бұл ақпараттық технологияның ажырамас бөлігі. Бағдарламалау технологиялары қатесіз бағдарламалар құра алмайды, сондықтан ақпараттық қауіпсіздікті қамтамасыз ете алмайды. Яғни, сенімсіз бағдарламаларды қолдана отырып, сенімді ақпараттық қауіпсіздік жүйелерін құру қажеттілігі туындайды. Бұл қажеттілік сәулет принциптерін сақтауды және IP пайдалану кезінде қауіпсіздікті бақылауды талап етеді. Сондай-ақ, ақпараттық-коммуникациялық технологиялардың дамуымен, желілерді үнемі қолданумен шабуылдардың саны айтарлықтай өсті. Бірақ мұны ақпараттық қауіпсіздіктің ең үлкен мәселесі деп атауға болмайды, өйткені бағдарламалық жасақтаманың жаңа әлсіз тұстарын үнемі анықтаумен және соның салдарынан шабуылдардың жаңа түрлерінің пайда болуымен байланысты мәселелер анағұрлым маңызды болып табылады. Мұндай осалдықтарды жою үшін операциялық жүйелердің барлық типтерін әзірлеушілер жұмыс жасайды, өйткені киберқылмыскерлер жаңа қателіктерді белсенді пайдаланады.

Мұндай жағдайларда ақпараттық қауіпсіздік жүйелерінде әртүрлі шабуылдарға қарсы тұру құралдары болуы керек. Шабуылдар бірнеше секундқа немесе бірнеше сағатқа созылуы мүмкін, осал тұстарын баяу тексереді (бұл жағдайда зиянды әрекет көрінбейді). Шабуылшылардың әрекеттері жеке қабылданған ақпаратты және ақпараттық қауіпсіздіктің барлық компоненттерін - қол жетімділікті, тұтастық пен құпиялылықты бұзуға бағытталуы мүмкін.

3.3 Ақпараттық қауіпсіздік әдістері

АЖ-дағы ақпараттың қауіпсіздігін қамтамасыз ету үшін келесі әдістер қолданылады: кедергі; қатынасты басқару; криптографияның әдістері; зиянды бағдарламалардың шабуылдарына қарсы әрекет; реттеу; мәжбүрлеу; ынта-ландыру.

Олардың әрқайсысын толығырақ қарастырайық.

1. Кедергі - бұл қорғалатын ақпаратқа (техникалық жабдықтарға, ақпарат тасымалдаушыларға және т.б.) баратын жолдың физикалық тосқауылы.

Қолжетімділікті басқару - ақпараттық технологиялар мен ақпараттық жүйені пайдалануды реттеу арқылы ақпаратты қорғау әдістері. Қолжетімділікті бақылау қорғалатын ақпаратқа рұқсатсыз қол жеткізудің барлық мүмкін жолдарын болдырмауы қажет.

Ақпаратты қорғау қолжетімділікті басқару: пайдаланушылар мен персоналды сәйкестендіру (жеке идентификатор тағайындау); идентификатор бойынша объектіні сәйкестендіру; ақпаратқа немесе объектіге қол жеткізу құқығын тексеру; ақпаратқа сілтемелерді тіркеу; рұқсат етілмеген әрекеттерді жасау кезінде жауап беру (дабыл, өшіру, жұмыстың кешігуі, сұраудан бас тарту және т.б.) арқылы жүзеге асырады. Криптографиялық қорғау әдістері - ақпаратты шифрлау. Шифрлау әдістері ақпаратты өңдеу мен сақтау кезінде кеңінен қолданылады.

Бұл әдіс желі арқылы ақпарат беру кезінде сенімді болып табылады. Зиянды бағдарламалардың шабуылдарынан қорғаныс ұйымдастыру-шылық сипаттағы әр түрлі әдістер жиынтығын және антивирустық бағдарламаларды қолдануды қамтамасыз етуге арналған, нәтижесінде IP-мен инфекция ықтималдығының төмендеуіне, жүйенің жұқтыру фактілерін анықтауға мүмкіндік береді; ақпараттық инфекциялардың салдарын азайту немесе алдын-алу, вирустарды жою; ақпаратты кейіннен қалпына келтіру орын алады.

2. Реттеу - жұмыс уақытының шектелуі, адамдардың ақпаратқа қол жетімділігінің шектеулі болуы, белгілі бір күндерде, тәулік уақытында, сағаттар бойынша қол жетімділікті шектеу және т.б.

Қорғалатын ақпараттар нормалары мен қорғанас стандарттарымен осындай жағдайдағы жұмыс барынша орындалатын болады.

3. Мәжбүрлеу - бұл пайдаланушылар мен АЖ қызметкерлері жауапкершілікке қауіп төніп тұрған (материалдық, әкімшілік немесе қылмыстық) қорғалатын ақпаратпен жұмыс істеу ережелерін сақтайтын ақпарат.

4. Ынталандыру - (бұрыннан қалыптасқан моральдық-этикалық стандарттардың сақталуына байланысты) IP субъектілерін белгіленген процедураларды бұзбауға шақыратын әдіс.

Ақпаратты қорғаудың техникалық құралдары аппараттық және физикалық болып бөлінеді. Аппараттық құрал деп АЖ-нің техникалық жабдықтарына тікелей салынған немесе онымен стандартты интерфейс арқылы байланысатын құрылғыларды айтады. Физикалық құралдарға қорғаныс объектілеріне физикалық енудің алдын алатын және персоналды, материалды, ақпаратты және басқа құндылықтарды (мысалы, құлыптар, сейфтер, дабыл сигналдары және т.б.) қорғайтын инженерлік құрылғылар мен құрылымдар жатады. АЖ-де ақпаратты қорғауға арналған бағдарламалық құралдар кеңінен қолданылады. Оларға құпия сөз бағдарламалары, антивирустық бағдарламалар, кіруді шектеу бағдарламалары, шифрлау (криптография) бағдарламалары жатады. Ұйымдастыру құралдары ақпаратты ашуға, жария етуге, заңсыз негізде ақпаратқа рұқсатсыз қол жеткізуге мүмкіндік бермейтін немесе қиындататын шараларды ұсынады. Заңнамалық құралдар ақпаратпен жұмыс істеу ережелерін реттейді және оларды бұзғаны үшін

жауапкершіліктің тәртібін белгілейді. Құқықтық қорғау құралдары сол мемлекеттің заңдарымен анықталады. Моральдық этикалық кепілдіктерге жазылуға болмайтын мінез-құлық нормалары жатады (мысалы, адалдық) немесе ережелер мен ережелер түрінде ресімделуі мүмкін. Әдетте, олар заңмен бекітілмеген, бірақ міндетті болып саналады. Мұндай ережелердің мысалы ретінде желідегі қарым-қатынастың этикалық ережелерінің жиынтығы және т.с.с. жатады.

3.4 Ақпаратты қорғау және ақпараттық қауіпсіздік

Ақпаратты кез-келген түрде ұсынылатын процестердің объектілері болып табылатын түрлі типтегі ақпарат ретінде анықтау «Ақпарат, ақпараттық технологиялар және ақпаратты қорғау туралы» заңдағы «ақпаратты қорғау» ұғымының келесі түсіндірмесіне сәйкес келеді.

Ақпаратты қорғау дегеніміз: құқықтық, ұйымдастырушылық және техникалық шараларды қабылдауға арналған әрекеттер:

1) ақпаратты рұқсат етілмеген қолжетімділіктен, жойылудан, өзгертуден, бұғаттаудан, көшіруден, ұсынудан, таратудан, сондай-ақ, осындай ақпаратқа қатысты өзге де заңсыз әрекеттерден қорғауды қамтамасыз ету;

2) қолжетімділігі шектеулі ақпараттың құпиялылығын сақтау;

3) ақпаратқа қол жеткізу құқығын жүзеге асыру.

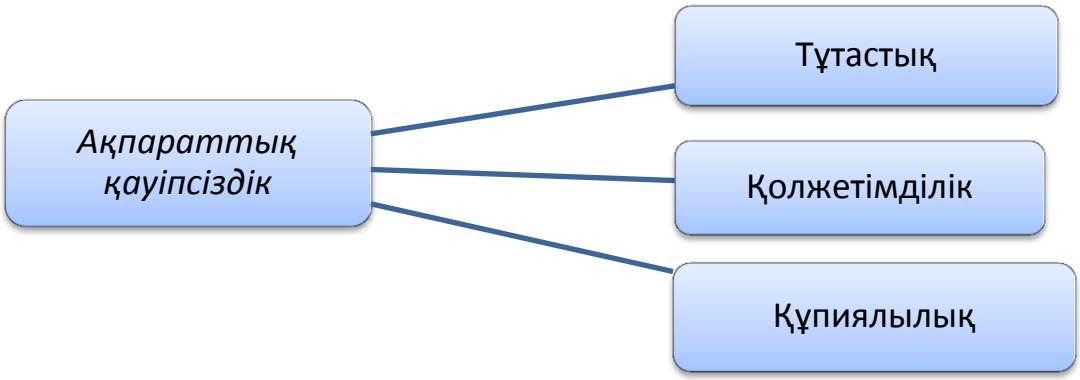
Ақпаратты қорғау дегеніміз ақпараттың таралуын , қорғалатын ақпаратқа рұқсат етілмеген және кездейсоқ әсер етуді болдырмайтын қызмет *болып табылады* [27].

Бұл жерде қауіп-қатердің екі түрі көрсетілген - қорғалатын ақпаратты рұқсатсыз алу (ағыны) және қорғалатын ақпаратқа әсер ету.

Сонымен, ақпаратты қорғау деп оны жинау, беру, өңдеу және сақтау процесінде оның қауіпсіздігін қамтамасыз етуге бағытталған шаралар мен әрекеттер жиынтығы түсіндіріледі.

Кең таралмаған мағынасында «ақпаратты қорғау» ұғымының жоғарыда келтірілген анықтамасы ең алдымен «ақпараттық қауіпсіздік» ұғымымен бірдей (3.1-сурет).

Ақпараттық қауіпсіздік дегеніміз - сыртқы ортаның (адам мен табиғаттың) тұрақсыздандырушы әсерінен және ол орналасқан жүйеге немесе желіге ішкі қауіп-қатерлерден қорғану жағдайы, яғни, ақпараттың құпиялылығы, тұтастығы және қолжетімділігі.



3.1–сурет-Ақпараттық қауіпсіздік түрлері

Ақпараттың құпиялылығы оның иесі анықтайтын және оны қорғаудың қажетті дәрежесін анықтайтын мәртебе (талап) екенін тағы бір рет атап өтеміз. Шын мәнінде, ақпараттың құпиялылығына қойылатын талап тексерілген, сенімді адамдарға ғана (уәкілетті) белгілі болуы керек.

Ақпараттың тұтастығы дегеніміз - (ақпаратқа қойылатын талап) мағыналық мазмұнды өзгеріссіз (бастапқы деректерге қатысты) сақтай алуы, яғни оның кездейсоқ немесе қасақана бұрмалауға немесе жоюға төзімді болып келетін ақпараттың мүмкіндігі.

Ақпараттың қолжетімділігі дегеніміз - объектінің - ақпараттық жүйенің (желінің) - уәкілетті субъектілерге (пайдаланушыларға, абоненттерге) өздерін қызықтыратын ақпаратқа уақтылы кедергісіз қол жеткізуді қамтамасыз ету немесе олардың арасында уақытылы ақпарат алмасуды жүзеге асыру мүмкіндігі (қажеттілігі).

Субъект - бұл жүйенің белсенді компоненті, ол объектіден тақырыпқа ақпарат ағынының қалыптасуын немесе жүйе күйінің өзгеруін тудыруы мүмкін. *Объект* - бұл ақпаратты өңдейтін, сақтайтын, қабылдайтын немесе тарататын жүйенің пассивті компоненті. Нысанға қол жетімділік дегеніміз, оның құрамындағы ақпаратқа қолжетімділік.

Яғни, *ақпаратқа қол жеткізу дегеніміз* - ақпаратты алу және пайдалану мүмкіндігі, оны қабылдау, ақпаратпен танысу, өңдеу, атап айтқанда ақпаратты көшіру, өзгерту немесе жою мүмкіндігі.

Ақпаратқа рұқсатсыз қол жетімділікті саралаудың белгіленген ережелерін бұзумен сипатталады.

Ақпаратқа рұқсатсыз қол жеткізуді қамтамасыз ететін пайдаланушы, бағдарлама немесе процесс қолжетімділікті бақылау ережелерін бұзады (қауіпсіздік саясатының элементтерінің бірі). Рұқсат етілмеген қатынас - бұл компьютер мен желіні бұзудың ең көп тараған түрі.

Ақпараттық қауіпсіздік - бұл құпиялылықты (ақпаратқа тек авторизацияланған пайдаланушылар үшін қолжетімділікті), тұтастықты (ақпараттың сенімділігі мен толықтығы және оны өңдеу әдістері) және қол- жетімділікті (ақпаратқа және онымен байланысты активтерге

қолжетімділікті) қамтамасыз ететін қорғаныс механизмі қажет болған жағдайда авторизацияланған пайдаланушылар).

Ақпараттық қауіпсіздігі деп адамның, қоғамның және мемлекеттің тепе-теңдік мүдделерінің жиынтығымен анықталатын ақпарат саласындағы ұлттық мүдделерді қорғау жағдайы деп түсінеді.

Ақпараттық салада ұлттық мүдделерінің негізгі төрт компоненті бар:

1) ақпарат алу және оны пайдалану, халықтың рухани жаңғыруын қамтамасыз ету, қоғамның адамгершілік құндылықтарын, патриотизм мен гуманизм дәстүрлерін, елдің мәдени және ғылыми әлеуетін сақтау мен нығайту саласындағы конституциялық құқықтар мен бостандықтарды сақтау;

2) азаматтардың ашық мемлекеттік ақпараттық ресурстарға қол-жетімділігін қамтамасыз етумен байланысты мемлекеттік саясатты ақпараттық қолдау;

3) қазіргі заманғы ақпараттық технологияларды, отандық ақпараттық индустрияны дамыту, ішкі нарықтың қажеттіліктерін өз өнімдерімен қанағаттандыру және осы өнімдерді әлемдік нарыққа шығару; отандық ақпараттық ресурстарды жинақтауды, сақтауды және тиімді пайдалануды қамтамасыз ету;

4) ұлттық ақпараттық ресурстарды рұқсат етілмеген қолжетімділіктен қорғау, ақпараттық және телекоммуникациялық жүйелердің қауіпсіздігін қамтамасыз ету.

Сонымен, ақпараттық қауіпсіздікті қамтамасыз етудің мақсаты, ең алдымен, ақпараттық саладағы ақпараттық қатынастардың субъектілері - азаматтар, адамдар қауымдастығы, кәсіпорындар, ұйымдар, корпорациялар, мемлекеттің өмірлік теңгерімді мүдделерін қорғау болып табылады.

Ұйымдар түрлерінің, бағыттарының және масштабтарының барлық алуан түрлілігімен, қатысушылардың саны, олардың маңызды активтері оның процестері, ақпараттық жүйелері мен желілік инфрақұрылымын қолдайтын ақпарат болып табылады, яғни. ақпараттық активтер. Ақпараттың құпиялылығы, тұтастығы және қол жетімділігі бәсекеге қабілеттілікке, өтімділікке, кірістілікке, заңды сәйкестікке және ұйымның іскери беделіне айтарлықтай ықпал етуі мүмкін.

Олардың ақпараттық қауіпсіздігінің мазмұны ақпарат пен ақпараттық инфрақұрылыммен, көрсетілетін ақпараттық қызметтер және ұйымның басқа ақпараттық активтерімен байланысты мақсатты іс-шаралардың қауіпсіздігінде жатыр. Оларға ақпараттық жүйелер мен ресурстар, зияткерлік меншік объектілері, осы объектілерге меншік құқығы, ұйым мүшелерінің мүліктік емес жеке құқықтары, заңмен қорғалатын құпияны құрайтын ақпаратқа қол жетімділіктің белгіленген режимін сақтау құқығы, мысалы, коммерциялық құпия және жеке

мәліметтер жатады. Ұйымның бұл компоненттері ақпараттық қауіпсіздік объектісі ретінде сыртқы және ішкі қауіптерден қорғалған.

Ұйымның, корпорацияның, кәсіпорынның ақпараттық қауіпсіздігі ақпараттық активтердің (ресурстар) сыртқы және ішкі, кездейсоқ және әдейі қатерлер жағдайында, ақпарат және ақпараттық инфрақұрылымның, басқа да ақпараттық активтердің қорғау және қолайлы жағдайын білдіреді.

Ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етудің басты мақсаты - ақпараттық қауіпсіздікті бұзу, оның құпиялылығына қол сұғу, тұтастық пен қолжетімділікті бұзу жағдайында ықтимал тәуекелді немесе экономикалық шығындарды азайту.

Тұтастай алғанда ұйымның қауіпсіздігі және оның «ақпараттық өлшемінің» қауіпсіздігі - ақпараттық қауіпсіздік, қауіпсіздікті талдау және бағалау, ұйымның ақпараттық қауіпсіздігін басқару бойынша талаптарды әзірлеу кезінде ұйым қызметінің қолайлы (немесе қабылданбайтын) тәуекелінің әдістемесі қолданылады. Тәуекел шамасы қолайсыздықтың туындауынан күтілетін қауіптілігімен анықталады.

Ұйымның, корпорацияның, кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз етудің негізгі міндеттеріне:

- ең маңызды, сонымен қатар, әлсіз және ақпараттық тұрғыдан осал объектілерді анықтау;
- ақпараттық қауіпсіздікке қауіп-қатер көздерін бағалау, болжау және оларды жүзеге асыру әдістері;
- корпоративті ақпараттық қауіпсіздік саясатын, оны жүзеге асырудың шаралары мен механизмдерінің жиынтығын әзірлеу;
- корпорацияның ақпараттық қауіпсіздігін қамтамасыз ететін, басқару органдарының ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметін үйлестіретін нормативтік құқықтық базаны әзірлеу;
- қауіп немесе төтенше жағдайлар туындаған кезде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шараларды әзірлеу;
- ақпараттық қауіпсіздікті қамтамасыз етудің иерархиялық жүйесін құру, оның ұйымдастырылуын, ақпараттық қауіпсіздікке төнетін қатерлердің алдын алу, қарсы тұру және бейтараптандыру нысандары, әдістері мен құралдарын жетілдіру;
- корпоративті жүйенің немесе желінің ғаламдық ақпараттық желілер мен жүйелерге қауіпсіз интеграциясын қамтамасыз ету жатады.

«Ақпаратты қорғау» ұғымын кеңінен түсіндіру кез келген материалдық нысанда ұсынылған ақпараттың қауіпсіздігін, ақпараттық жүйелер мен телекоммуникация желілері жұмысының қауіпсіздігін және ақпараттық технологияларды қолдануды қамтамасыз ететін шаралар кешенін қарастырады. Бұл мағынада ол жаңа қалыптасып келе жатқан ақпараттық немесе телекоммуникациялық жүйелердің «ақпараттық қауіпсіздігі» тұжырымдамасымен сәйкес келеді (қазіргі уақытта заңнамалық актілермен анықталмаған).

Ақпараттық қауіпсіздіктің қазіргі заманғы интерпретациясы (кең мағынада - ақпараттық және ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету ретінде - ақпараттық жүйелер мен технологиялар) ақпараттық қауіпсіздікті қамтамасыз ету үдерісімен жеткілікті айқын шекараға ие емес [17].

Сонымен бірге, ақпараттық қауіпсіздік пен ақпаратты қорғауды қамтамасыз ету процестерінің мазмұны (және сәйкесінше, ақпараттық қауіпсіздік және ақпараттық қауіпсіздік ұғымдары) қорғалатын объектілерді ұйымдастырудың иерархиясы мен күрделілігі деңгейінде және қауіптердің сипатымен ерекшеленеді. Объектілердің ақпараттық қауіпсіздігін қамтамасыз ету қауіптердің көрінуінен ақпараттық және ақпараттық инфрақұрылымның қауіпсіздігін (қорғалуын) қамтамасыз ететін «ақпаратты қорғау» мен «ақпараттық қауіпсіздікті» білдіреді. Екі тұжырымдама, сол немесе басқа топтарға баса назар аудара отырып, шаралар жиынтығы мен қорғау құралдарын - құқықтық, ұйымдастырушылық және технологиялық (техникалық) пайдалануды білдіреді.

«Ақпараттық қауіпсіздік» және «ақпараттық қауіпсіздікпен қамтамасыз ету» ұғымдарының келесі түсіндірмесін қабылдайық.

Біріншіден, *қауіпсіздік* тұжырымдамасы «ешқандай қауіп жоқ, қауіптен қорғану бар», ал жалпы жағдайда қауіптің көрінуіне байланысты біреуге немесе бір нәрсеге зиян келтіру мүмкін еместігі ретінде анықталғанын атап өтеміз, яғни олардың *қауіп-қатерден қауіпсіздігі (қауіпсіздік жағдайы). Қауіпсіздік түсінігі* қызметі және қызмет құралы ретінде - екі жолмен қарастырылады, сондай-ақ қауіпсіздік пәндерін қамтиды.

Жұмысқа сәйкес [23], «ақпараттық қауіпсіздік» тұжырымдамасының құрылымында біз ақпараттық қауіпсіздік объектісін, осы объектке төнетін қатерлерді және оның ақпараттық қауіпсіздігін қауіптердің көрінуінен қамтамасыз етеміз.

Қауіпсіз дамудың жаһандық проблемасы аясында жеке адамдар, қоғам (адамдар қауымдастықтары, ұйымдар, оның ішінде корпорацияларды, кәсіпорындарды және т.б.) және ақпараттық қауіпсіздіктің негізгі объектілері ретінде қарастырылады.

Ақпараттық қауіпсіздік осы объектілер үшін ең жалпы түрде қауіпсіздік объектісінің немесе оның құрылымдық компоненттерінің қасиеттеріне зиян келтірудің мүмкін еместігі ретінде анықталуы мүмкін, ақпараттық және ақпараттық инфрақұрылыммен шарт қойылған, яғни, олардың «ақпараттық өлшемінің» қауіпсіздігі (қауіпсіздік жағдайы) ретінде көрініс табады.

Жоғарыда айтылғандардың негізінде адамның, қоғамның және мемлекеттің ақпараттық қауіпсіздігінің мазмұнын, олардың «ақпараттық өлшемінің» қауіпсіздігі ретінде анықтауға болады.

Адамның ақпараттық қауіпсіздігі оған адам ретінде зиян келтіру мүмкін еместігіне, оның әлеуметтік қызметі негізінен алынған ақпаратты түсінуге негізделген.

Қоғамның ақпараттық қауіпсіздігі оның рухани саласына, мәдени құндылықтарына, адам тәртібін әлеуметтік реттеушілерге, оның көмегімен берілетін ақпараттық инфрақұрылымға және хабарламаларға зиян келтіру мүмкін еместігімен тұжырымдалады.

Мемлекеттің ақпараттық қауіпсіздігі - қоғамның ақпараттық және ақпараттық инфрақұрылымын пайдалануға байланысты мемлекеттік істерді басқару функцияларын орындау кезінде оның қызметіне зиян келтіру мүмкін еместігінде. Кейде адамның психикасы мен санасына және қоғамдық санаға әсер етумен байланысты ақпараттық қауіпсіздік компонентінің маңыздылығын қабылдай отырып, онда ақпараттық және психологиялық қауіпсіздік бөлініп шығады.

Ақпараттық қауіпсіздікті қамтамасыз ету ақпараттық және ақпараттық инфрақұрылымның, сондай-ақ осы қызметтің құралдары мен субъектілерінің әсерінен қауіпсіздік объектісінің қасиеттеріне зиян келтіруге жол бермейтін іс-әрекеттермен сипатталады.

Сонымен, ақпараттық қауіпсіздікті қамтамасыз ету, ең алдымен , әлемдік өркениеттің, мемлекеттердің, адамдар қауымдастығының, жеке тұлғаның, табиғаттың қауіпсіз дамуының ғаламдық проблемасын шешім ретінде қарастырылады. Сонымен бірге, «ақпараттық қауіпсіздік» ұғымы жалпыланған қатерлердің екі түрінің мүмкін әрекеті жағдайында адамды, қоғамды, мемлекетті, табиғатты қорғау жағдайын сипаттайды: олардың құпияларын ымыраға келтіру (ашу), сондай-ақ, олардың ақпараттық ішкі жүйелеріне (санаға) теріс (кездейсоқ немесе әдейі) әсер ету және жеке тұлғаның психикасы, бұқаралық сана, ақпараттық сфера (қоршаған орта), қоғам және мемлекет, табиғи объектілердің ақпаратқа сезімтал элементтері) жағдайларын көрсетеді.

Ақпараттық қауіпсіздік ұғымының астарында адамның, қоғам мен мемлекеттің, олардың «ақпараттық өлшеу» (ақпарат саласында жеке адамның, қоғам мен мемлекеттің өмірлік маңызды мүдделері; ұйымның ақпараттық активтері, корпорациялар, бизнес, қорғау күйін білдіреді тиісті ақпарат және ақпараттық инфрақұрылым) сыртқы және ішкі көріністері, кездейсоқ және қасақана қорқыту жағдайлары түсіндіріледі.

Арнайы тұжырым келесі абзацта келтіріледі.

Соңғы жылдары «ақпараттық қауіпсіздік» ұғымы ақпараттық және автоматтандырылған жүйелер, корпоративті және телекоммуникациялық желілер сияқты ақпараттық қауіпсіздік объектілеріне таралды (бірақ заңнамада бекітілмеген). Олар үшін «ақпараттық қауіпсіздік» түсінігінің келесі түсіндірмесін қарастырайық [17].

Корпоративті ақпараттық жүйенің немесе желінің ақпараттық қауіпсіздігі дегеніміз - тұрақсыздандырушы факторлар (қауіптер) жағдайында жүйенің немесе желінің тұрақты жұмысын қамтамасыз ететін, онда орналасқан немесе «айналатын» ақпараттың және оның ақпараттық инфрақұрылымының қауіпсіздігі.

Бақылау сұрақтары:

1. Ақпараттық қауіпсіздіктің пайда болуын түсіндіріңіз?
2. Ақпараттық қауіпсіздіктің қандай әдістері бар?
3. Ақпараттық қауіпсіздік қатеріне мысал келтіріңіз?
4. Ақпараттың құпиялылығын түсіндіріңіз?
5. Компьютерлік шабуыл дегеніміз не?

4 Зияткерлік меншікті қорғау

Зияткерлік меншік саласындағы ғылым, әдебиет және өнер туындыларын (авторлық құқық), туындыларды, спектакльдерді, фонограммаларды, эфирлік және кабельдік хабар тарату ұйымдарының хабарларын (сабақтас құқықтар) жасауға және пайдалануға байланысты туындайтын қатынастар «Авторлық құқық және сабақтас құқықтар туралы» Заңмен реттеледі. 10 маусым 1996 ж. № 6 [5].

4.1 Негізгі ұғымдар мен анықтамалар

Автор - шығармашылық еңбегі ғылым, әдебиет, өнер туындысын жасаған жеке тұлға;

Авторлық құқық - автордың жеке мүліктік емес және мүліктік құқықтары;

Қоғаммен байланыс - авторлық және сабақтас құқықтар объектілерінің сым арқылы немесе сымсыз байланыс құралы арқылы хабарлануы, бұнда көпшілік оларға кез келген жерден және кез келген уақытта өз қалауы бойынша қол жеткізе алады;

Иесі - автор (оның мұрагерлері) авторлық құқыққа қатысты, орындаушыға (оның мұрагерлеріне), фонограмма жасаушыға, байланысты құқықтарға қатысты, эфирлік немесе кабельдік хабар таратуды ұйымдастыруға, сондай-ақ, туындыны және (немесе) объектіні пайдалануға айрықша құқық алған басқа заңды тұлғаларға қатысты, шарт бойынша осы Заңда көзделген кез келген басқа негізде байланысты құқықтар;

Пайдаланушы - авторлық және сабақтас құқықтар объектілерін жүзеге асыратын немесе пайдалануды ұйымдастыратын жеке немесе заңды тұлға;

Шығарманы жариялау - автордың келісімімен туындыны алғаш рет жариялау, көпшілік назарына ұсыну, көпшілік алдында орындау, оны көпшілікке ұсыну және басқа тәсілдер арқылы қолжетімді ететін іс-әрекетті жүзеге асыру.

Авторлық құқық Қазақстан Республикасының аумағында жария етілген немесе жарияланбаған, кез-келген объективті түрде, авторлар мен олардың ізбасарларының азаматтығына қарамастан туындыларға таралады.

Егер Қазақстан Республикасынан тыс жерлерде алғашқы жарияланған күннен бастап отыз күн ішінде ол Қазақстан Республикасының аумағында жарық көрген болса, онда туынды Қазақстан Республикасында жарияланған болып саналады.

Шығарма Қазақстан Республикасы ратификациялаған халықаралық шарттарға сәйкес қорғалады.

Авторлық құқық объектісі.

Авторлық құқық олардың мақсатына, мазмұны мен құндылығына, сондай-ақ, оларды білдіру әдісі мен формасына қарамастан шығармашылық қызметтің нәтижесі болып табылатын ғылым, әдебиет және өнер туындыларына таралады.

Авторлық құқық кез-келген объективті нысанда бар жарияланған (көпшілік алдында орындалған, көпшілікке көрсетілген) және жарияланбаған жұмыстарға да таралады:

- жазбаша (қолжазба, мәтіндік басылым, музыкалық нота және т.б.);
- ауызша (көпшілік алдында сөйлеу, көпшілік алдында өнер көрсету және т.б.);
- дыбыстық немесе бейнежазба (механикалық, сандық, магниттік, оптикалық және сол сияқтылар);
- суреттер (сурет, эскиз, кескіндеме, жоспар, сурет, фильм, теледидар, видео немесе фото кадр және т.б.);
- көлемдік-кеңістіктік (мүсін, модель, модель, құрылым және т.б.);

Туындының бір бөлігін өз бетінше пайдалануға болады, авторлық құқыққа жатады.

Авторлық құқық нақты идеяларға, тұжырымдамаларға, принциптерге, әдістерге, жүйелерге, процестерге, ашылуларға, фактілерге қолданылмайды.

Шығармаға авторлық құқық туынды көрсетілген материалдық объектіге меншік құқығымен байланысты емес.

Авторлық құқық объектілері:

- әдеби шығармалар;
- драмалық және музыкалық-драмалық шығармалар;
- сценарийлер;
- хореография және пантомима шығармалары;
- мәтіні бар немесе мәтінсіз музыкалық шығармалар;
- аудиовизуалды жұмыстар;
- кескіндеме, мүсін, графика және басқа бейнелеу өнерінің туындылары;
- қолданбалы өнер туындылары;
- сәулет, қала құрылысы, дизайн және бақ пен саябақ өнері;
- фотографиялық жұмыстар және фотосуретке ұқсас әдістермен алынған жұмыстар;
- география, топография және басқа ғылымдарға қатысты карталар, жоспарлар, эскиздер, иллюстрациялар және көлемді жұмыстар;
- компьютерлік бағдарламалар.

Компьютерлік бағдарламаларды қорғау кез-келген тілде және кез-келген формада, соның ішінде бастапқы мәтін мен объект кодын білдіруге болатын компьютерлік бағдарламалардың барлық түрлеріне қолданылады (соның ішінде амалдық жүйелер).

Авторлық құқық объектілеріне:

- туынды шығармалар (аудармалар, бейімделулер, аннотациялар, рефераттар, конспектілер, шолулар, қойылымдар, музыкалық аранжировкалар және ғылым, әдебиет және өнер туындыларының басқа түрлендірулері);

- материалдарды іріктеу және (немесе) орналастыру кезінде шығармашылық жұмыстардың нәтижелері болып табылатын жинақтар (энциклопедиялар, антологиялар, мәліметтер базасы) және басқа да композициялық жұмыстар.

Авторлық құқыққа жатпайды:

- ресми құжаттар (заңдар, сот шешімдері, заңнамалық, әкімшілік, сот және дипломатиялық сипаттағы басқа мәтіндер), сондай-ақ, олардың ресми аудармалары;

- мемлекеттік рәміздер мен белгілер (жалаулар, эмблемалар, ордендер, банкноттар және басқа мемлекеттік рәміздер мен белгілер);

- халық шығармашылығы;

- ақпараттық сипаттағы оқиғалар мен фактілер туралы хабарламалар.

Ғылым, әдебиет және өнер туындысына авторлық құқық оны құру фактісінен туындайды. Авторлық құқықтың пайда болуы және оны жүзеге асыру үшін туындыны тіркеу, туындының басқа арнайы дизайны немесе кез-келген формальдылық талаптарына сәйкес келмейді.

Автор және (немесе) авторлық құқық иесі өздерінің ерекше меншік құқықтары туралы хабарлау үшін туындының әр данасында орналастырылған және міндетті түрде үш элементтен тұратын авторлық құқықты қорғау белгісін пайдалануға құқылы:

1) латынша «С» әрпі шеңбер түрінде;

2) айрықша авторлық құқық иесінің атауы (атауы);

3) туындының алғашқы жарияланған жылы.

Жарияланбаған туындыға мүліктік емес жеке құқықтарды растау үшін автор осы Заңға сәйкес авторлық құқықты қорғау мерзімінің кез келген уақытында авторлық құқықпен қорғалатын объектілерге құқықтардың мемлекеттік тізіліміне қажетті ақпаратты енгізуге құқылы.

Егер басқа дәлелдемелер болмаса, туындының түпнұсқасында немесе көшірмесінде автор ретінде көрсетілген адам шығарманың авторы болып саналады - авторлық презумпциясы.

Авторлық презумпция тек автордың өзіне ғана қатысты.

Шығарма анонимді немесе бүркеншік атпен жарияланған кезде (егер автордың бүркеншік аты оның жеке басына күмән тудырмаса), шығармада аты немесе атауы көрсетілген баспагер, егер басқа дәлелдер болмаса, осы Заңға сәйкес автордың өкілі болып саналады және осы сипатта оның құқығы бар автордың құқықтарын қорғау және олардың орындалуын

қамтамасыз ету. Бұл ереже осындай туындының авторы өзінің жеке басын ашқанға дейін және оның авторлығын жарияламағанға дейін қолданылады.

Қызметтік міндеттерді орындау кезінде немесе жұмыс берушінің қызметтік тапсырмасын орындау кезінде жасалған туындыға автордың жеке мүліктік емес құқығы (қызметтік жұмыс) сервистік жұмыстың авторына тиесілі.

Қызметкердің жұмысына меншіктік (айрықша) құқықтар, егер ол мен автор арасындағы келісімшартта өзгеше көзделмесе, жұмыс берушіге тиесілі.

Жұмыс беруші өзінің жұмысын кез келген пайдалану кезінде көрсетуге немесе осындай нұсқау талап етуге құқылы.

Шығарманың түпнұсқасын немесе көшірмелерін оларды жалға беру (және жалпыға жалға беру) арқылы тарату құқығы, осы даналардың меншігіне қарамастан, авторға немесе авторлық құқық иесіне:

1) музыкалық мәтін түріндегі музыкалық шығармаға;

2) фонограммада жазылған шығарма;

3) аудиовизуалды жұмыс;

4) мәліметтер базасы;

5) компьютерлік бағдарлама.

24-бап. Компьютерлік бағдарламалар мен мәліметтер базасын ақысыз көбейту. Компьютерлік бағдарламалардың декомпиляциясы [5]

1. Компьютерлік бағдарламаның немесе мәліметтер базасының көшірмесін заңды түрде иеленуші тұлға автордың немесе ерекше құқықтардың басқа иесінің рұқсатынсыз және қосымша ақы төлемей-ақ:

1) компьютерлік бағдарламаға немесе мәліметтер базасына қосуға құқылы пайдаланушының техникалық құралдарында оның жұмыс істеуі үшін, оның мақсатына сәйкес компьютерлік бағдарламаның немесе мәліметтер базасының жұмысына қажетті кез келген әрекеттерді, оның ішінде компьютердің жадына жазуды және сақтауды (бір компьютерде немесе бір желі қолданушысында) сақтау үшін жүзеге асырылатын өзгерістер; сонымен қатар, егер автормен келісімде өзгеше көзделмесе, айқын қателіктерді түзету;

2) компьютерлік бағдарламаның немесе мәліметтер базасының көшірмесін жасау немесе оған нұсқау беру, егер бұл көшірме тек мұрағаттық мақсатқа арналған болса және компьютерлік бағдарламаның немесе мәліметтер базасының түпнұсқасы жоғалған, жойылған немесе жарамсыз болып қалған жағдайда заңды түрде алынған көшірмені ауыстыру қажет. Бұл жағдайда компьютерлік бағдарламаның немесе мәліметтер базасының көшірмесін 1) тармақшасында көрсетілгеннен басқа мақсаттарда пайдалану мүмкін емес және осы компьютерлік

бағдарламаның немесе мәліметтер базасының көшірмесі заңды болып табылмаса, жойылуы керек.

2. Компьютерлік бағдарламаның көшірмесіне заңды түрде иелік ететін тұлға автордың немесе ерекше құқықтардың басқа иесінің келісімінсіз және қосымша сыйақы төлемей-ақ, объект кодын түпнұсқа мәтінге көбейтуге және түрлендіруге (компьютерлік бағдарламаны декомпиляциялауға) немесе қажет болған жағдайда басқа адамдарға осы әрекеттерді орындауға нұсқауға құқылы. осы адам жасаған компьютерлік бағдарлама келесі шарттарды сақтай отырып, декомпиляцияланған бағдарламамен өзара әрекеттесе алатын басқа бағдарламалармен дербес өзара әрекеттесу қабілетіне қол жеткізу:

1) өзара әрекеттесу қабілетіне жету үшін қажетті ақпарат осы адамға бұрын басқа көздерден қолжетімді болмаған;

2) көрсетілген әрекеттер декомпиляцияланған компьютерлік бағдарламаның өзара әрекеттесу мүмкіндігіне қол жеткізуге қажетті бөліктеріне қатысты ғана жүзеге асырылады;

3) декомпиляциялау нәтижесінде алынған ақпараттарды тек тәуелсіз дамыған компьютерлік бағдарламамен басқа бағдарламалармен өзара әрекеттесу мүмкіндігіне қол жеткізу үшін ғана пайдалануға болады, басқа адамдарға берілмейді, тек өз бетінше дамыған компьютерлік бағдарламамен өзара әрекеттесу мүмкіндігіне қол жеткізу қажет болған жағдайларды қоспағанда басқа бағдарламалар, сонымен қатар, сыртқы түрі бойынша декомпиляцияланған компьютерлік бағдарламаға ұқсас компьютерлік бағдарламаны жасау үшін немесе авторлық құқықты бұзатын кез келген басқа әрекеттерді орындау үшін қолдануға болмайды.

3. Осы баптың ережелерін қолдану компьютерлік бағдарламаның немесе мәліметтер базасының қалыпты пайдаланылуына негізсіз зиян келтірмеуге және автордың немесе компьютерлік бағдарламаға немесе мәліметтер базасына ерекше құқықтардың басқа иесінің заңды мүдделерін негізсіз бұзбауы тиіс.

28-бап. Авторлық құқықтың қолданылу мерзімі [5]

1. Авторлық құқық автордың бүкіл өмірінде және ол қайтыс болғаннан кейін жетпіс жыл өткен соң жарамды.

2. Авторлық құқық, автордың атын және беделін қорғау құқығы шексіз қорғалады.

48-бап. Авторлық және сабақтас құқықтарды бұзу [5]

1. Осы Заңда көзделген авторлық және (немесе) сабақтас құқықтарды бұзғаны үшін жауаптылық Қазақстан Республикасының заңдарына сәйкес жүзеге асырылады.

2. Шығармаларға немесе сабақтас құқықтар объектілеріне қатысты мыналарға жол берілмейді:

1) автордың немесе басқа құқық иеленушінің рұқсатынсыз авторлық құқық пен сабақтас құқықтарды қорғаудың техникалық құралдарын пайдалану арқылы белгіленген туындыларды немесе сабақтас құқықтар объектілерін пайдалану бойынша шектеулерді жоюға бағытталған іс-әрекеттер;

2) кез келген құрылғыны немесе оның компоненттерін жасау, тарату, жалға беру, импорттау, жарнамалау, оларды табыс табу мақсатында пайдалану немесе қызметтер көрсету, егер мұндай әрекеттер нәтижесінде авторлық құқықты қорғаудың техникалық құралдарын пайдалану мүмкін болмай қалса және сабақтас құқықтар немесе осы техникалық құралдар аталған құқықтардың тиісті қорғалуын қамтамасыз ете алмайды;

3) құқықтарды басқару туралы ақпаратты автордың немесе басқа құқық иеленушінің рұқсатынсыз алып тастау немесе өзгерту;

4) көбейту, тарату, тарату мақсатында әкелу, көпшілік алдында орындау, кабельдік немесе эфирлік хабар тарату арқылы көпшілікке хабарлау, туындылар немесе сабақтас құқықтар объектілері туралы олар туралы мәліметтер автордың немесе басқа құқық иесінің рұқсатынсыз жойылған немесе өзгертілген көпшілікке мәлімет беру. меншік құқығын басқару.

4.2 Патент

Меншік және өнеркәсіптік меншік объектілерін құруға, құқықтық қорғауға және пайдалануға байланысты туындайтын жеке мүліктік емес қатынастар 1999 жылғы 16 шілдедегі № 427 «Қазақстан Республикасының Патент Заңы» заңымен реттеледі [6].

Өнеркәсіптік меншік объектілері - өнертабыстар, пайдалы модельдер және өнеркәсіптік үлгілер.

Өнертабысқа, пайдалы модельге және өнеркәсіптік үлгіге құқықтар патентпен қорғалады.

Патент өнеркәсіптік меншік объектісіне басымдылықты, авторлықты және айрықша құқықты куәландырады.

Өнертабысқа патент өтінім берілген күннен бастап жиырма жыл ішінде жарамды.

Пайдалы модельге арналған патент өтінім берілген күннен бастап бес жыл ішінде жарамды. Өнеркәсіптік үлгінің патенті өтінім берілген күннен бастап он бес жыл ішінде жарамды.

Патентпен қамтамасыз етілген құқықтық қорғаудың көлемі анықталады: өнертабыс пен пайдалы модель үшін - олардың формуласы бойынша, ал өнеркәсіптік үлгі үшін - өнімнің сыртқы түрінің бейнелерінде ұсынылған оның маңызды белгілерінің жиынтығы. Сипаттама мен

сызбалар пайдалы модель талаптарын түсіндіру үшін пайдаланылуы мүмкін.

Өнертабысқа жаңа, егер өнертабыстық сатысы болса және өнеркәсіпте қолданылатын болса, оған құқықтық қорғау беріледі.

5-бапқа сәйкес [6] мыналар өнертабыс болып танылмайды:

1) жаңалықтар, ғылыми теориялар және математикалық әдістер;

2) экономиканы ұйымдастыру және басқару әдістері;

3) конвенциялар, кестелер, ережелер;

4) ақыл-ой операцияларын жасау, ойын ойнау ережелері мен әдістері;

5) компьютерлерге арналған бағдарламалар және сол сияқты алгоритмдер;

6) құрылыстардың, ғимараттардың, аумақтардың жобалары мен сызбалары;

7) өнімнің тек сыртқы түріне қатысты ұсыныстар;

8) қоғамдық тәртіпке, ізгілік пен адамгершілік қағидаларына қайшы келетін ұсыныстар.

Пайдалы модель өнімге (құрылғыға, субстанцияға, микроорганизм штаммына, өсімдік немесе жануарлар клеткаларының дақылына), әдіске (материалды құралдардың көмегімен материалды заттарға әсер ету процесін), сондай-ақ, белгілі өнімді немесе әдісті қолдануға байланысты кез келген саладағы техникалық шешімдерді қамтиды, яғни, адамдарды немесе жануарларды емдеудің диагностикалық, терапиялық және хирургиялық әдістерін қоспағанда, белгілі бір мақсаттағы жаңа кездесу немесе жаңа өнім.

Пайдалы модель, егер ол жаңа және өнеркәсіпте қолданылатын болса, құқықтық қорғауға ие болады.

Өнеркәсіптік үлгі дегеніміз - өнімнің сыртқы түрін анықтайтын өнеркәсіптік немесе қолөнер бұйымдарының көркемдік дизайны. Өнеркәсіптік үлгі жаңа, түпнұсқа болса, оған құқықтық қорғау беріледі.

8-бапқа сәйкес [6], келесі шешімдер өнеркәсіптік үлгілер деп танылмайды:

1) тек өнімнің техникалық қызметіне байланысты;

2) сәулеттік нысандар (шағын сәулет нысандарын қоспағанда), өндірістік, гидротехникалық және басқа стационарлық құрылыстар;

4) сұйық, газ тәрізді, сусымалы немесе ұқсас заттардан жасалған тұрақсыз пішіндегі заттар;

5) қоғамдық мүдделерге, ізгілік пен адамгершілік қағидаларына қайшы келетін өнімдер.

Өнеркәсіптік меншік объектісінің авторы - ол өзінің шығармашылық еңбегін жасаған жеке тұлға. Авторлық құқық - бұл ажырамас жеке құқық және ол шексіз қорғалады.

Патент иесінің қорғалатын өнеркәсіптік меншікті өз қалауы бойынша пайдалануға айрықша құқығы бар.

Патент иесі өнеркәсіптік меншік объектісін пайдалануға міндетті.

Патент иеленуші қорғау құжатын сақтау үшін жыл сайын өтінім берілген күнге сәйкес күнде төлеуге міндетті.

4.3 Лицензиялау

Қазақстан Республикасындағы барлық рұқсаттар мен хабарламалар «Рұқсаттар және хабарламалар туралы» Қазақстан Республикасының 2014 жылғы 16 мамырдағы № 202-V ҚРЗ заңына бағынады [7].

Келесі салалардағы қызметтің немесе әрекеттердің (операциялардың) жекелеген түрлері лицензиялануға жатады, оның ішінде:

- білім;
- ақпараттандыру және байланыс;
- ақпараттық қауіпсіздікті қамтамасыз ету.

2014 жылғы 16 мамырдағы № 202-V ҚРЗ «Рұқсаттар және хабарламалар туралы» Заңына 1-қосымшада бірінші санаттағы рұқсаттардың (лицензиялардың) тізімі келтірілген. Ақпараттық қауіпсіздік саласындағы ақпараттандыру және коммуникация саласындағы қызметті лицензиялау (4.1- кесте).

4.1-кесте

№ р / р	Атауы және лицензиясы үшін лицензияны қажет ететін қызметтің түрі, лицензияны қажет етеді	Жүзеге асыру үшін лицензияның болуы талап етілетін қызметтің кіші түрінің атауы	Ескерту
Ақпарат және байланыс саласындағы лицензиялау қызметі			
12.	Байланыс қызметтерінің лицензиясы	1. Қалааралық телефон байланысы. 2. Халықаралық телефон байланысы. 3. Спутниктік ұялы байланыс. 4. Ұялы байланыс.	Бөлінбейтін; 1 сынып
Ақпараттық қауіпсіздік саласындағы қызметті лицензиялау			
27.	Криптографиялық қорғау құралдарын жасауға лицензия		Бөлінбейтін; 1 сынып
28.	Ақпараттың таралып кетуінің техникалық арналарын және жедел-іздестіру қызметін жүзеге асыруға арналған арнайы техникалық құралдарды анықтау бойынша қызметтерді ұсынуға лицензия		Бөлінбейтін; 1 сынып

Бақылау сұрақтары:

1. Зияткерлік меншікті қорғаудың қандай формалары бар?
2. Патент дегеніміз не?
3. Патенттердің қандай түрлері бар?
4. Қандай қызмет түрлері лицензиялануға жатады?

5 Дербес деректерді қорғау

«Дербес деректер және оларды қорғау» 2013 жылғы 21 мамырдағы № 94-V [8] заңы, дербес деректер саласындағы қоғамдық қатынастар, сондай-ақ дербес деректерді жинауға, өңдеуге және қорғауға байланысты қызметтің мақсатын, қағидаттарын және құқықтық негіздерін анықтайды және реттейді.

5.1 Негізгі ұғымдар

Дербес деректер дегеніміз - олардың негізінде анықталған электрондық, қағаз және (немесе) өзге де ақпараттық тасымалдағыштарда жазылған дербес деректер субъектісіне қатысты ақпарат.

Дербес деректерді қорғау - кешенді, оның ішінде құқықтық, ұйымдастырушылық және техникалық шаралар.

Дербес деректерді өңдеу - жеке деректерді жинауға, сақтауға, өзгертуге, толықтыруға, пайдалануға, таратуға, иесіздендіруге, бұғаттауға және жоюға бағытталған әрекеттер;

Дербес деректерді сақтау - жеке мәліметтерге кез келген тәсілмен қол- жетімділікті қамтамасыз ету жөніндегі іс-шаралар. Дербес деректерге:

- тегі, аты және әкесінің аты (бар болса);
- ұлты;
- жынысы;
- туған күні мен орны;
- жеке сәйкестендіру нөмірі жатады;
- жеке куәліктің нөмірі;
- заңды мекен-жайы;
- тұрғылықты жері;
- байланыс құралдарының абоненттік нөмірі;
- отбасылық және әлеуметтік жағдайы.

5.2 Дербес деректерді жинау, өңдеу және қорғау

Дербес деректер қолжетімділігі бойынша жалпыға қолжетімді және қолжетімділігі шектеулі болып бөлінеді.

Қазақстан Республикасының заңнамасына сәйкес құпиялылықты сақтау талаптары қолданылмайтын, субъектінің келісімімен еркін қол жеткізуге болатын дербес деректер немесе мәліметтер жалпыға бірдей қолжетімді дербес деректер болып табылады.

Халықты ақпаратпен қамтамасыз ету үшін жалпыға қол жетімді жеке дерек көздері (өмірбаяндық анықтамалықтар, телефон, мекен-жай кітаптары, жалпыға қолжетімді электрондық ақпараттық ресурстар, бұқаралық ақпарат құралдары қоса) қолданылады.

Жинау және өңдеу Қазақстан Республикасының заңнамасын бұза отырып жүзеге асырылған субъект туралы ақпарат субъектінің немесе оның заңды өкілінің өтініші бойынша немесе соттың шешімі бойынша немесе басқа да уәкілетті мемлекеттік органдардың кез келген уақытта жеке деректердің жалпыға қолжетімді көздерінен алынып тасталады.

Дербес деректерді жинауды, өңдеуді меншік иесі және (немесе) оператор, сондай-ақ, үшінші тұлға субъектінің немесе оның заңды өкілінің келісімімен уәкілетті орган айқындайтын тәртіппен жүзеге асырады.

Жеке деректерді өңдеу нақты, алдын-ала анықталған және заңды мақсаттарға қол жеткізумен шектелуі керек. Дербес деректерді жинау мақсаттарына сәйкес келмейтін дербес деректерді өңдеуге жол берілмейді. Мазмұны мен көлемі, оларды өңдеу мақсаттарына қатысты шамадан тыс көп болатын жеке деректер өңдеуге жатпайды.

Субъект немесе оның заңды өкілі жеке деректерді жинауға, өңдеуге жазбаша түрде, электрондық құжат түрінде немесе жеке деректердің қауіпсіздігін қамтамасыз ету қызметі арқылы немесе басқа жолмен Қазақстан Республикасының заңнамасына қайшы келмейтін қорғаныс әрекеттерінің элементтерін қолдана отырып келісім береді (алып тастайды).

Жеке деректерді жинау, өңдеу келесі жағдайларда субъектінің немесе оның заңды өкілінің келісімінсіз жүзеге асырылады:

- құқық қорғау органдары мен соттардың қызметін, атқарушылық іс жүргізуді жүзеге асыру;
- мемлекеттік статистикалық қызметті жүзеге асыру;
- мемлекеттік органдардың дербес деректерді оларды иесіздендірудің міндетті шартымен статистикалық мақсаттарда пайдалануы.

Кәсіби, іскерлік қажеттілікке, сондай-ақ, еңбек қатынастарына байланысты шектеулі қолжетімділіктің дербес деректері туралы хабардар болған адамдар олардың құпиялылығын қамтамасыз етуге міндетті.

Заң жеке деректерді өңдеу бойынша келесі іс-әрекеттерді (операцияларды) көздейді:

Дербес деректерді өңдеуге арналған әрекеттер (операциялар)	Дербес деректерді өңдеуге арналған әрекеттерді (операцияларды) сипаттау
Дербес деректерді жинақтау	Деректерді алуға бағытталған әрекеттер
Жеке деректерді жинақтау	Дербес деректерді дерекқорға енгізу арқылы дербес деректерді жүйелеу бойынша әрекеттер
Жеке деректерді өңдеу	Дербес деректерді жинауға, сақтауға,

	өзгертуге, қосуға, пайдалануға, таратуға, иесіздендіруге, бұғаттауға және жоюға бағытталған әрекеттер
Жеке деректерді өзгерту және қосу	Жеке деректерді өзгерту мен толықтыруды меншік иесі және (немесе) оператор субъектінің немесе оның заңды өкілінің өтініші (сұранысы) негізінде жүзеге асырады.
Жеке деректерді бұғаттау	Жеке деректерді жинау, жинақтау, өзгерту, қосу, пайдалану, тарату, иесіздендіру және жоюды уақытша тоқтату жөніндегі іс-шаралар
Жеке деректерді жою	Нәтижесінде жеке деректерді қалпына келтіру мүмкін емес әрекеттер
Жеке деректерді жасыру	Нәтижесінде дербес деректердің дербес деректер субъектісіне жататындығын анықтау мүмкін емес әрекеттер
Жеке деректерді пайдалану	Меншік иесінің, оператордың және үшінші тұлғаның мақсаттарына қол жеткізуге бағытталған дербес деректермен іс-әрекеттер
Жеке деректерді сақтау	Жеке деректердің тұтастығын, құпиялылығын және қолжетімділігін қамтамасыз ететін іс-шаралар
Жеке мәліметтерді тарату	Жеке деректерді беруге, соның ішінде, бұқаралық ақпарат құралдары арқылы немесе кез-келген тәсілмен жеке деректерге қол жеткізуді қамтамасыз ететін әрекеттер
Дербес деректерді трансшекаралық тасымалдау	Дербес деректерді шет мемлекеттердің аумағына беру.

Дербес деректерді қорғау іс-шаралар кешенін қолдану арқылы жүзеге асырылады, оның ішінде, құқықтық, ұйымдастырушылық және техникалық.

Бапқа сәйкес [8]**.**

1. Меншік иесі және (немесе) оператор, сондай-ақ, үшінші тұлға:

1) дербес деректерге рұқсатсыз қол жеткізуді болдырмау;

2) дербес деректерге рұқсатсыз қол жеткізу фактілерін уақытылы анықтау, егер мұндай рұқсатсыз кірудің алдын алу мүмкін болмаса;

3) дербес деректерге рұқсат етілмеген қолжетімділіктің жағымсыз салдарын азайту.

Бақылау сұрақтары:

1. Жеке мәліметтерге анықтама беріңіз.
2. Жеке мәліметтерді құрайтын мәліметтерді келтіріңіз.
3. Жеке мәліметтер қолжетімділігіне қарай қандай мәліметтерге бөлінеді?
4. Жеке мәліметтерді қорғау үшін қандай шаралар қолданылады?
5. Шектелген жеке деректер туралы білетін адамдар не істеуі керек?

6 Ақпараттық жүйелер аудиті

6.1 Ақпараттық жүйенің аудитіне жалпы сипаттама

Ережеге сәйкес [9] ақпараттық жүйелер аудиті:

- ақпараттық жүйенің ағымдағы жағдайына, оларда болатын іс-шаралар мен оқиғаларға баға алу, олардың ақпараттандыру саласындағы техникалық регламенттерге, стандарттарға сәйкестік деңгейін анықтай алу;
- нормативтік-техникалық құжаттаманың тұтынушы талаптарына, сондай-ақ, ақпараттық қауіпсіздік талаптарына сәйкестігін белгілеу.

Ақпараттық жүйелер аудитінің міндеттері:

- Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 қаулысымен бекітілген ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы бірыңғай талаптарға сәйкестігін бағалау [10].
- ақпараттық жүйелерді қорғауға арналған қауіпсіздік саясатын және басқа ұйымдастырушылық-әкімшілік құжаттарды әзірлеуді талдау және бағалау;
- ақпараттық жүйелердің ресурстарына қатысты қауіпсіздікке қатер төндіру мүмкіндігімен байланысты тәуекелдерді талдау;
- персоналға ақпаратты қорғауды қамтамасыз етуге байланысты міндеттер қоюды бағалау;
- ақпараттық қауіпсіздікті бұзумен байланысты оқиғаларды талдауға қатысуды бағалау;
- ақпараттық жүйелерді қорғау жүйесіндегі осалдықтарды оқшаулау;
- ақпараттық жүйелерді пайдаланушыларды және техникалық қызмет көрсету персоналын оқытуға қатысу дәрежесін анықтау;
- ақпараттық жүйелердің қауіпсіздігін қамтамасыз етудің жаңа тетіктерін енгізу және тиімділігін арттыру бойынша ұсыныстар әзірлеу;
- ақпараттық жүйе функцияларының оның мақсаттары мен міндеттеріне сәйкестігін бағалау;
- ақпараттық жүйені құрудың, енгізудің және пайдаланудың ақпараттандыру саласындағы техникалық регламенттерге, стандарттарға сәйкестігін бағалау;
- қолданбалы бағдарламалық жасақтама мен мәліметтер базасын қоса, ақпараттық жүйелердің қауіпсіздік деңгейін бағалау;
- ақпараттық-коммуникациялық инфрақұрылым жағдайын, оның техникалық жағдайы мен топологиясын бағалау;
- нормативтік-техникалық құжаттаманың ақпараттандыру саласындағы Қазақстан Республикасы заңнамасының талаптарына сәйкестігін бағалау.

6.2 Ақпараттық жүйелердің аудитін жүргізу тәртібі

Ақпараттық жүйелер аудиті ақпараттық жүйелерді құру, енгізу және пайдалану кезеңінде ақпараттық жүйелер иесінің немесе иесінің бастамасы бойынша жүзеге асырылады.

Ақпараттық жүйелер аудитін АКТ саласында арнайы білімі мен тәжірибесі бар жеке (немесе) заңды тұлғалар жүзеге асырады.

Мемлекеттік құпияларға жататын қорғалатын ақпараттық жүйелерде аудит жүргізілмейді.

Ақпараттық жүйелер аудитінің тапсырыс берушісі ақпараттық жүйенің иесі және (немесе) иесі болып табылады.

Ақпараттық жүйені тексеру уақыты ақпараттық жүйенің функционалдық күрделілігіне және тапсырыс беруші тарапынан ақпараттық жүйе аудитінің нақты міндеттеріне байланысты.

Мемлекеттік заңды тұлғалардың ақпараттық жүйелеріне аудит жүргізу кезінде аудиторды таңдау «Мемлекеттік сатып алу туралы» 2015 жылғы 4 желтоқсандағы Қазақстан Республикасының Заңына сәйкес жүзеге асырылады.

Ақпараттық жүйелер аудиті бойынша жұмыс (сараптамалық әдіспен талдау, ақпараттық қауіпсіздік стандарттарының ұсынымдарына және бірыңғай талаптарға сәйкестігін бағалау, ақпараттық жүйенің компоненттерін инструменталды сараптау) бірқатар дәйекті кезеңдерді қамтиды:

- ақпараттық жүйелер аудитінің рәсімін бастау;
- ақпараттық жүйелер аудитінің жиынтығы;
- ақпараттық жүйелер аудитінің деректерін талдау;
- ұсыныстар әзірлеу;
- қорытынды дайындау және қол қою.

Сараптамалық әдіспен талдау барысында ақпаратты қорғау шаралары жүйесіндегі кемшіліктер сауалнама процедурасына қатысатын сарапшылардың тәжірибесі негізінде анықталады.

Қазақстан республикасының стандарттары «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару құралдары туралы ережелер кодексі» және әкімшілік, процедуралық және физикалық қорғау шараларын қоса, ұйымдық деңгейде қауіпсіздік тетіктерін бағалау критерийлері ретінде қолданылады.

Жүйенің аппараттық және бағдарламалық жасақтамасындағы осалдықтарды анықтау және жою ақпараттық жүйелер компоненттерінің инструменталды сараптамасы кезінде жүзеге асырылады.

Ақпараттық жүйенің аудиті аяқталғаннан кейін аудиторлық есеп жасалады, екі данада, оның біреуі тапсырыс берушіге беріледі, екіншісі аудиторда қалады (Қосымша F). Бұл табиғатта кеңес беру сипатына ие.

«Мемлекеттік техникалық қызмет» АҚ 2015 жылғы 24 қарашадағы «Ақпараттандыру туралы» Қазақстан Республикасы Заңының 14-бабы 1-тармағының 7) тармақшасы негізінде «электрондық үкіметтің» ақпараттандыру объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақ жүргізеді.

Тестілерге сынақ объектілерінің техникалық құжаттама талаптарына, Қазақстан Республикасының нормативтік құқықтық актілеріне және Қазақстан Республикасының аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттарға сәйкестігін бағалау бойынша жұмыстар кіреді және сынақ объектісінің қалыпты жұмысы жағдайында жүзеге асырылады.

Бақылау сұрақтары:

1. Ақпараттық жүйенің аудитіне анықтама беріңіз.
2. Ақпараттық жүйенің аудиті туралы қай заңнамада сипатталған?
3. Ақпараттық жүйелер аудитін жүргізу тәртібін түсіндіріңіз.

7 Таратылуы шектеулі ақпарат

Қазақстан Республикасы Үкіметінің **«Ақпаратты шектеулі таратудың ресми ақпаратына жатқызу және онымен жұмыс істеу ережесін бекіту туралы»** 2015 жылғы 31 желтоқсандағы № 1196 қаулысымен ақпаратты түріне және / немесе ақпарат тасымалдаушысына қарамастан шектеулі таратудың ресми ақпаратына жатқызу және онымен жұмыс істеу тәртібі айқындалды.

Шектелген таратудың ресми ақпараты - бұл шешім қабылдау кезінде мемлекеттік органның тәуелсіздігін қамтамасыз ету қажеттілігіне байланысты әкімшілік рәсімдерді сақтау тәртібін бұзуы мүмкін мемлекеттік органның қызметіне қатысты ақпарат.

Ашық жарияланым - бұл материалдарды ашық баспасөзде жариялау, интернет-ресурста орналастыру, оларды радио мен теледидарда беру, ашық конференцияларда, кездесулерде, симпозиумдарда хабарландыру, фильмдерде демонстрациялау, мұражайларда, көрмелерде көрмелер, ғылыми-зерттеу және эксперименталды жария қорғау -жобалық жұмыс, қолжазба депозиті.

7.1 Мәліметті шектеулі таратудың ресми ақпаратына жатқызу тәртібі

Шектеулі таратылатын ресми ақпаратты қамтитын құжаттар, істер мен басылымдарда «Қызметтік пайдалану үшін» (бұдан әрі - «ҚПҮ» белгісі) деген белгі қойылады.

Ақпаратты шектеулі тарату ақпараттарына беруді мердігер мен құжатқа қол қойған тұлға мемлекеттік органда әзірленген қызметтік пайдалану үшін ақпарат тізбесі (бұдан әрі - ақпарат тізімі) негізінде жүзеге асырады.

Ақпарат тізбесі (оған толықтырулар мен өзгерістер) мемлекеттік орган басшысының бұйрығымен бекітіледі.

Ақпарат тізбесін әзірлеу келесі өлшемдер негізінде жүзеге асырылады:

1) құпиялылық режимін ұйымдастыруға және сақтауға байланысты мемлекеттік құпияларды қамтымайтын мәліметтер, сондай-ақ, тіркеу формаларын қоса, оның сақталуын бақылау;

2) жариялануы немесе жария етілуі мемлекеттік органдардың жұмысына, соның ішінде электрондық ақпараттық ресурстарға, оның ішінде, қол жеткізу парольдеріне рұқсатсыз қол жеткізу нәтижесінде ақпаратты жоюдан, бұғаттаудан немесе өзгертуден қорғау процесіне тікелей әсер ететін ақпарат;

3) ақпараттың заңды иесі мемлекеттік органға құпия негізде берген ақпарат;

4) жариялау немесе жариялау жеке және заңды тұлғалардың заңды құқықтары мен мүдделерін бұзатын мәліметтер;

5) шешімдер қабылдау процесінде жүзеге асырылатын ведомствоаралық және ведомствоішілік хат-хабарлар туралы ақпаратты қамтитын, шешімдер қабылдау кезінде мемлекеттік органдардың тәуелсіздігін қамтамасыз ету қажеттілігімен байланысты әкімшілік рәсімдерді сақтау тәртібін бұзуы мүмкін шешімдер қабылдау кезінде өткізілетін мемлекеттік органдардағы кездесулер, «Ақпаратқа қол жеткізу туралы» Қазақстан Республикасы Заңының 6-бабында көрсетілген мәселелер бойынша нөмір;

6) түпкілікті шешім қабылданбаған мемлекеттік бақылау және қадағалау шеңберінде жүргізілген тексерулердің нәтижелері туралы ақпарат;

7) шет мемлекеттерден немесе халықаралық ұйымдардан алынған, оларды жария ету шарттары туралы өзара келісім қабылданбаған ақпарат.

7.2 "Қызметтік пайдалану үшін (ҚПҮ)" деген белгісі бар қызметтік ақпаратпен жұмыс істеу тәртібі

Таратылуы шектелген қызметтік ақпаратты ашық байланыс түрлерінің техникалық арналары арқылы беруге (жалпы пайдаланудағы телефон, факсимильді байланыс, радиобайланыс, спутниктік және ұялы (жылжымалы (ұтқыр) байланыс, Интернет желісі) жол берілмейді.

"ҚПҮ" деген белгісі бар құжаттар мен басылымдарды қабылдауды және есепке алуды (тіркеуді) мемлекеттік органның құжаттамалық қызметі жүзеге асырады.

"ҚПҮ" деген белгісі бар хат-хабар қағаз түрінде келіп түскен жағдайда, ол конвертте (пакетте) жапсырылуға тиіс. Бұл ретте орамның бүтіндігі, құжаттар мен басылымдардың парақтары мен даналарының саны, сондай-ақ, ілеспе хатта көрсетілген қосымшалардың болуы тексеріледі.

Қате келіп түскен "ҚПҮ" деген белгісі бар құжаттар мен басылымдар жөнелтушіге қайтарылады.

"ҚПҮ" деген белгісі бар құжаттар мен басылымдар электрондық жеткізгіштерде келіп түскен кезде зиянды бағдарламалардың болуы тексеріледі.

Жұмыстан тыс уақытта "ҚПҮ" деген белгісі бар құжаттар мен басылымдарды Мемлекеттік орган бойынша кезекші қабылдайды, ол оларды ашпай, құжаттамалық қызмет басшысына береді.

"ҚПҮ" деген белгісі бар құжаттар мен басылымдарды тұрақты кезекшілері жоқ мемлекеттік органдарға жұмыстан тыс уақытта жеткізуге жол берілмейді.

Барлық кіріс, шығыс және ішкі құжаттар, сондай-ақ "ҚПҮ"деген белгісі бар басылымдар тіркелуге жатады. Құжаттар парақтардың, басылымдардың (кітаптар, журналдар, брошюралар), даналардың саны бойынша есепке алынады.

Журналдардың парақтары нөмірленеді, тігіледі және соңғы парақта нөмірленген парақтардың саны (санмен және жазумен), қызметкер лауазымының атауы, оның қойған қолдары және қойылған қолдың толық жазылуы көрсетіле отырып, мөрмен бекітіледі.

Журналдар аяқталғаннан кейін соңғы параққа бірінші және соңғы тіркелген құжаттың нөмірі, сондай-ақ, литерлік және өткізіп алған нөмірлердің саны көрсетіле отырып, тіркелген құжаттардың саны (санмен және жазумен) қосымша қойылады. Көрсетілген деректерден кейін қызметкер лауазымының атауы, оның қолы және қолының толық жазылуы қойылады.

Журналдың соңғы парағына қосымша, бірінші және соңғы тіркелген құжаттың нөмірі, сондай-ақ әріптер мен жетіспейтін сандар көрсетіледі. Көрсетілген мәліметтерден кейін қызметкердің лауазымының атауы, оның қолы және қолдың шифры ашылады.

"ҚПҮ" деген белгісі бар құжаттар мен басылымдардың қозғалысы тиісті тіркеу-есепке алу нысандарында уақтылы көрсетілуге тиіс.

Құжаттың бірінші парағында жоғарғы оң жақ бұрышында "қызметтік пайдалану үшін" деген белгі немесе "ҚПҮ" деген аббревиатура басылады және басылған данасының нөмірі көрсетіледі.

Құжаттың және ілеспе хаттың әрбір данасының соңғы парағының сырт жағында жөнелтілген құжаттың даналары қайда жіберілгені және оның жіберілгені (жіберілімнің есебі), құжатты орындаушының тегі көрсетіледі.

«ҚПҮ» белгісі бар құжаттарды, файлдарды және басылымдарды Қазақстан Республикасының шегіндегі басқа ұйымдарға жіберу, әдетте, курьерлік қызметпен немесе курьерлермен жүзеге асырылады. «ҚПҮ» белгісі бар құжаттарды, файлдарды және басылымдарды жіберу қалың қағаз конверттеріне салынуы немесе оралуы керек. Пошта арқылы жіберу үшін мөлдір терезелері бар конверттерді пайдалануға жол берілмейді.

Іс қағазымен аяқталған істің мұқабасында келесі деректемелер болуы керек:

1) «ҚПҮ» белгісі;

2) мемлекеттік органның ресми атауы;

3) мемлекеттік орган орналасқан елді мекеннің атауы;

4) мемлекеттік органның құрылымдық бөлімшесінің атауы;

5) істер номенклатурасына сәйкес істің индексі;

6) істің тақырыбы;

7) іс көлемінің нөмірі;

8) істі қарау мерзімі (әкімшілік құжаттар, хаттамалар, стенограммалар, хат-хабарлар үшін), әкімшілік құжаттар, хаттамалар, стенограммалар үшін - бірінші және соңғы құжаттың реттік нөмірлері;

9) файлды сақтау мерзімі.

Істің басында құжаттардың ішкі тізімдемесі, соңында аттестаттау парағы орналастырылады.

Лауазымды тұлғаларға құжаттама қызметінің басшылары бекіткен тізімдерге сәйкес «ҚПҮ» белгілері бар істермен, ал шектеулі тарату құжаттарымен - мемлекеттік органдар басшыларының қаулыларындағы нұсқауларға сәйкес жұмыс істеуге рұқсат етіледі.

Рұқсат етілмейді:

1) ақпараттарды халықаралық (ғаламдық) тарату желілерінде, Интернетте таралуы шектеулі құжаттар мен басылымдардан ақпарат орналастыруға;

2) оларды көпшілік алдында сөйлеу немесе ашық баспасөзде, радио мен телевизиялық хабарларда жариялау үшін пайдалануға;

3) «ҚПҮ» белгілері бар құжаттар мен басылымдарды ашық көрмелерде көрсетуге, оларды стендтерде, витриналарда немесе көпшілік көретін басқа жерлерде көрсетуге.

Жою үшін таңдалған «ҚПҮ» белгісі бар істер бөлек актіде жасалуы немесе жою үшін таңдалған басқа жіктелмеген құжаттармен бірге жалпы актіге (6-қосымша) енгізілуі мүмкін. Бұл жағдайда актінің 2-бағанында «ҚПҮ» белгісі бар істердің тақырыптарынан кейін «ҚПҮ» белгісі қойылады.

Мемлекеттік органның ведомстволық архиві (ведомстволық кітапхана) қызметкерлерінің қатысуымен «ҚПҮ» белгісі бар құжаттарды, іс қағаздарын және басылымдарды өртеп жіберіп жоюға жол беріледі.

«ҚПҮ» белгісімен аяқталған іс қағаздары мемлекеттік органның құрылымдық бөлімшелерінің кеңсе үй-жайларында олар ведомстволық мұрағатқа өткізілгенге дейін сақталуы керек.

«ҚПҮ» деп белгіленген басылымдар, әдетте, ведомстволық кітапханада, ол болмаған жағдайда - ведомстволық мұрағатта сақталады.

Сақтау сенімді құлыпталған және мөрленген металл шкафтарда немесе сейфтерде жүзеге асырылады. Сонымен бірге олардың физикалық қауіпсіздігін қамтамасыз ету үшін тиісті жағдайлар жасалуы керек.

«ҚПҮ» белгісі бар құжаттардың, файлдардың және басылымдардың болуын тексеруді жылына кемінде бір рет мемлекеттік орган басшысының

бұйрығымен тағайындалған комиссия жүзеге асырады. Комиссияның құрамына оларды есепке алу мен сақтауды жүргізу сеніп тапсырылған адамдар кіруі керек.

«ҚПҮ» белгісі бар құжаттардың, істер мен басылымдардың жоғалу фактісі бойынша қызметтік тергеу жүргізу немесе олардағы мәліметтердің жария етілу фактісін анықтау үшін мемлекеттік орган басшысының әкімшілік құжатымен комиссия тағайындалады.

Тергеу нәтижелері бойынша комиссияның қорытындысын осы комиссияны құрған басшы бекітеді.

Жоғалған құжаттарға, құжаттарға және «ҚПҮ» белгісімен басылымдарға акт жасалады және тіркеу жазбаларына тиісті жазбалар енгізіледі.

«Қызметтік пайдалану үшін» деген белгісі бар таратылған шектеулі таратылымдық ақпаратпен жұмыс істеу тәртібін бұзу, бұл ақпараттың ашылуына немесе жоғалуына әкелмеген және себеп болмады, кінәлілерді қолданыстағы заңнамаға сәйкес тәртіптік жауапкершілікке тартуға негіз бола алады.

Бақылау сұрақтары:

1. Ақпаратты шектеулі таратудың ресми ақпаратына жатқызу тәртібін түсіндіріңіз.
2. «Қызметтік пайдалану үшін» белгісі бар қызметтік ақпаратпен жұмыс істеу тәртібін түсіндіріңіз.

8 Электрондық құжат және электрондық цифрлық қолтаңба

«Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370 Заңы құқықтық қатынастарды орнатуды, өзгертуді немесе тоқтатуды көздейтін, электрондық цифрлық қолтаңбалармен куәландырылған электрондық құжаттарды жасау мен пайдаланудан туындайтын қатынастарды, сондай-ақ құқықтар мен міндеттерді реттейді. электрондық құжаттардың айналымы, соның ішінде азаматтық-құқықтық мәмілелерді жасау саласында туындайтын құқықтық қатынастарға қатысушылар [12].

«Электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру ережелері» 2015 жылғы 9 желтоқсандағы № 1187 [13] ақпараттық жүйені құру және пайдалану кезеңінде ақпараттық жүйемен электрондық цифрлық қолтаңбаның дұрыстығын тексеру тәртібін анықтайды.

8.1 Негізгі терминдер мен анықтамалар

Электрондық құжат айналымы - бұл мемлекеттік органдар, жеке және заңды тұлғалар арасында электрондық құжаттармен алмасу.

Электрондық цифрлық қолтаңбаэлектрондық цифрлық қолтаңба – бұл арқылы жасалған және электрондық құжаттың дұрыстығын, оның меншігі мен мазмұнының өзгермейтіндігін растайтын электрондық цифрлық белгілер жиынтығы.

Электрондық цифрлық қолтаңбаның құралдарыэлектрондық цифрлық қолтаңбаның - бұлжасалуы мен дұрыстығын тексеру үшін қолданылатын бағдарламалық-техникалық құралдар жиынтығы.

Электрондық цифрлық қолтаңбаның ашық кілті – кез келген адамға қолжетімді және электрондық құжатта электрондық цифрлық қолтаңбаның дұрыстығын растауға арналған электрондық цифрлық белгілердің кезектілігі;

Электрондық цифрлық қолтаңбаның құпия кілті - бұл электрондық цифрлық қолтаңбаны пайдалану арқылы электрондық цифрлық қолтаңба жасауға арналған электрондық цифрлық белгілердің реттілігі.

Қазақстан Республикасының Ұлттық сертификаттау орталығы - жеке және заңды тұлғаларға мемлекеттік және мемлекеттік емес ақпараттық жүйелерде электрондық құжаттарды қалыптастыру үшін электрондық цифрлық қолтаңбалар мен тіркеу куәліктерін ұсынатын сертификаттау орталығы.

Мемлекеттік және мемлекеттік емес ақпараттық жүйелерде электрондық құжат айналымы келесі принциптер негізінде жүзеге асырылады:

- әр түрлі электронды құжат айналымы жүйелерін қолдану;

- электронды құжаттар АКТ деректерді құру, өңдеу, сақтау және беру үшін қолданылатын кез-келген қызмет саласында қолданылады;

- электрондық құжаттарды беру кез-келген ақпараттық жүйені қолдану арқылы жүзеге асырылады.

8.2 Электрондық құжат айналымына қойылатын талаптар

Электрондық цифрлық қолтаңба арқылы куәландырылған электрондық құжат, оған қол қоюға құқығы бар адам қағаз жеткізгіште қол қойылған құжатқа тең.

Электрондық құжат телекоммуникация желілері арқылы берілген сәттен бастап жіберілген болып саналады.

Кіріс электрондық құжат адресаттың ақпараттық жүйесінде жазылғаннан кейін алынған болып саналады.

Түбіртек туралы хабарламада электрондық құжатты алу фактісі мен уақыты және оны жіберуші туралы ақпарат болуы керек. Егер хабарламаны оның авторы алмаған болса, онда құжат адресат алған жоқ деп саналады.

Электрондық құжат айналымының тәртібін Қазақстан Республикасының Үкіметі айқындайды.

Электрондық құжаттар мемлекеттік және (немесе) мемлекеттік емес ақпараттық жүйелерде сақталады.

Мемлекеттік құпияларды құрайтын, қорғалатын нұсқадағы ақпараттық жүйелерді қолдана отырып, электрондық құжаттарды және мемлекеттік құпияларды құрайтын мәліметтерді қамтитын басқа деректерді жинау, өңдеу, сақтау, беру, іздеу, тарату, пайдалану, қорғау, тіркеу және жою тәртібін Қазақстан Республикасының Ұлттық қауіпсіздік комитеті айқындайды құпияларды, сондай-ақ арнайы сертификаттау орталығын құру, аккредиттеу және қызметін тоқтату тәртібі.

8.3 Электрондық цифрлық қолтаңба

Электрондық цифрлық қолтаңба қол қоюшының өз қолымен қойылған қолымен баламалы болып табылады және сол заңды салдарға әкеп соқтырады, егер:

- электрондық цифрлық қолтаңбаның шынайылығы тіркеу куәлігі бар ашық кілтпен тексерілсе;

- электрондық құжатқа қол қойған тұлға заңды түрде электрондық цифрлық қолтаңбаның жеке кілтіне ие болса;

- электрондық цифрлық қолтаңба тіркеу куәлігінде көрсетілген мәліметтерге сәйкес қолданылады;

- электрондық цифрлық қолтаңба жасалып, Қазақстан Республикасының аккредиттелген сертификаттау орталығы немесе Қазақстан Республикасының сенімді үшінші тұлғасында тіркелген шетелдік сертификаттау орталығы берген тіркеу куәлігі.

Электрондық цифрлық қолтаңбаның жеке кілттері оларға заңды түрде иелік ететін адамның меншігі болып табылады. Адамда әртүрлі ақпараттық жүйелер үшін электрондық цифрлық қолтаңбаның жеке кілттері болуы мүмкін. Электрондық цифрлық қолтаңбаның жеке кілттерін басқа адамдарға беруге болмайды.

Электрондық цифрлық қолтаңбаны мемлекеттік органдардың лауазымды адамдары өз өкілеттіктері шегінде берген электрондық құжаттарды куәландыру кезінде пайдалана алады.

Сертификаттау орталығының функциялары:

- электрондық цифрлық қолтаңбаның жабық кілттерін рұқсат етілмеген қолжетімділіктен қорғау бойынша шаралар қабылдай отырып, электрондық құжат айналымы жүйесіне қатысушылардың өтініштері бойынша электрондық цифрлық қолтаңбалардың кілттерін жасайды;
- тіркеу куәліктерін береді, тіркейді, қайтарып алады, сақтайды, белгіленген тәртіппен берілген тіркеу куәліктерінің тізілімін жүргізеді;
- тіркеу куәліктерін қолдану ережелерін бекітеді;
- жарамды және қайтарып алынған тіркеу куәліктерінің есебін жүргізеді;
- сертификаттау орталығында Қазақстан Республикасының заңнамасында белгіленген тәртіппен тіркелген электрондық цифрлық қолтаңбаның ашық кілтіне меншік құқығы мен жарамдылығын растайды;

Сертификаттау орталығы сақтаудағы ашық және (немесе) электрондық цифрлық қолтаңбалардың жеке кілттерін жоғалтудың, өзгертудің және қолдан жасаудың алдын алу үшін барлық қажетті шараларды қабылдауға міндетті. Осы міндеттемелерді орындамағаны үшін Қазақстан Республикасының заңнамасына сәйкес жауап береді.

Сертификаттау орталығы тіркеу куәліктерінің иелері туралы ақпараттың қорғалуын қамтамасыз етеді. Тараптардың келісімі бойынша құпия болып табылатын тіркеу куәліктерінің иесі туралы мәліметтер тіркеу куәліктерінің қоғамдық тізіліміне енгізілмеген.

8.4 Электрондық цифрлық қолтаңбаның түпнұсқалылығын тексеру тәртібі

ЭЦҚ-ның түпнұсқалылығын ақпараттық жүйені құру және жұмыс істеу кезеңінде тексеру, қоюшының тіркеу куәлігі бар электрондық

құжатты алғаннан кейін, ақпараттық жүйе келесі тексерулерді жүзеге асыратын функционалдығын жүзеге асырады:

- электрондық құжатта ЭЦҚ тексеріледі;
- қол қоюшының тіркеу куәлігі тексеріліп жатыр.

Ақпараттық жүйе қол қоюшының тіркеу куәлігінде болатын ашық ЭЦҚ кілтін қолдана отырып, электрондық құжаттағы ЭЦҚ тексереді. Электрондық құжат, өз кезегінде, қол қоюшының тіркеу куәлігін қамтуы керек.

ЭЦҚ -ны тексеру кері тәртіпте жүзеге асырылады, оған сәйкес құжатқа қол қойылды, келесі схема бойынша:

- жіберушінің ЭЦҚ ашық кілтін пайдалану арқылы хабарлама хэші (жіберушінің қолы) шифры шешіледі;
- хэш функциясын қолдану арқылы бастапқы хабарламаның бақылау сомасы есептеледі.

Бұл кезеңде екі бақылау сомасы салыстырылады, егер олар тең болса, онда ЭЦҚ дұрыс деп саналады (ЭЦҚ тексеруінің оң нәтижесі анықталады), егер тең болмаса, онда ЭЦҚ жарамсыз болып саналады (ЭЦҚ тексеруінің теріс нәтижесі анықталады).

Ақпараттық жүйе ЭЦҚ -ны техникалық енгізу және тіркеу куәлігінің аутентификациясы үшін жауап береді.

Егер криптографиялық ақпараттық жүйені қолдана отырып ЭЦҚ түпнұсқалығын тексеру рәсімін өткізгеннен кейін ЭЦҚ сәйкессіздіктері анықталса (ЭЦҚ тексерудің теріс нәтижесі анықталса), ақпараттық жүйе арқылы алынған электрондық құжат қолмен қол қойылған құжатқа балама деп танылмайды.

Бақылау сұрақтары:

1. «Электрондық цифрлық қолтаңба» анықтамасын беріңіз.
2. Электрондық цифрлық қолтаңбаның мақсаты неде?
3. Электрондық цифрлық қолтаңба құралдарына мысал келтіріңіз.
4. Электрондық цифрлық қолтаңбаның жабық кілтінің мақсатын түсіндіріңіз.
5. Электрондық цифрлық қолтаңбаның ашық кілтінің мақсатын түсіндіріңіз.
6. Қазақстан Республикасының ұлттық сертификаттау орталығы қандай қызметтерді атқарады?

9 АКТ саласындағы ҚР заңнамасын бұзғаны үшін жауапкершілік

9.1 Әкімшілік құқық бұзушылық

Әкімшілік құқық бұзушылық - жеке немесе заңды тұлғаның құқыққа қарсы, қасақана немесе абайсызда жасаған әрекеті не әрекетсіздігі не әкімшілік жауаптылық көзделген тұлғалардың әрекетсіздігі.

Әкімшілік жауапкершілік - егер құқық бұзушылықтар өз сипаты бойынша ҚР заңнамасына сәйкес қылмыстық жауаптылыққа әкеп соқпаса, басталады.

Негізгі әкімшілік жазалар ретінде ескерту, әкімшілік айыппұл, қызметті тоқтата тұру немесе оған тыйым салу, әкімшілік қамаққа алу қолданылады.

Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V ҚРЗ "Әкімшілік құқық бұзушылық туралы" Кодексімен ақпараттық қауіпсіздікті қамтамасыз ету үшін [14] әкімшілік құқық бұзушылық жасағаны үшін әкімшілік жауапкершілік шаралары, оның ішінде электрондық ақпараттық ресурстарды қорғау құралдарын пайдалану жөніндегі талаптарды бұзу түрінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі міндеттерді орындамайтын лауазымды тұлғалармен, сондай-ақ "бірыңғай талаптарды" орындамауы, ақпараттық жүйелердің меншік иесінің немесе иеленушісінің ақпаратты қорғау, дербес деректері бар, жөнінде шаралар оларды қорғау.

Әкімшілік Кодексте мынадай құқық бұзушылықтар бойынша жазалар көзделген:

- 14-бап. Жеке басқа қол сұғылмаушылық;
- 15-бап. Жеке адамның ар-намысы мен қадір-қасиетін құрметтеу;
- 16-бап. Жеке өмірге қол сұғылмаушылық және құпияны қорғау;
- 78-бап. Жеке тұлғаға ақпарат беруден бас тарту;
- 79-бап. Қазақстан республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу;
- 185-бап. Коммерциялық, банктік құпияны, кредиттік есептердің мәліметтерін немесе кредиттік бюроның кредиттік тарихының деректер базасынан алынған ақпаратты сақтау міндетін бұзу;
- 186-бап. Сақтандыру немесе зейнетақы жинақтарының құпиясын не микрокредит беру құпиясын сақтау міндетін бұзу;
- 240-бап. Бухгалтерлік ақпараттың құпиясын жария ету;
- 456-1-бап. Ақпаратқа қол жеткізу құқығын заңсыз шектеу;
- 473-бап. Салық құпиясын құрайтын мәліметтерді жария ету;

− 504-бап. Мемлекеттік құпияларды қорғау саласындағы, сондай-ақ, таратылуы шектелген қызметтік ақпаратпен жұмыс істеудегі белгіленген талаптарды бұзу.

9.2 Қылмыстық құқық бұзушылықтар

Қазақстан Республикасы Қылмыстық кодексінің 4-бабына [15] сәйкес, "қылмыстық құқық бұзушылық, яғни қылмыс құрамының не осы Кодексте көзделген қылмыстық теріс қылықтың барлық белгілері бар іс-әрекет жасау қылмыстық жауаптылықтың жалғыз негізі болып табылады".

Қазақстан Республикасы Қылмыстық кодексінің 10-бабына сәйкес, қылмыстық құқық бұзушылықтар қоғамдық қауіптілік және жазаланушылық дәрежесіне қарай қылмыстар және қылмыстық теріс қылықтар болып бөлінеді.

"Осы кодексте айыппұл салу, түзеу жұмыстары, қоғамдық жұмыстарға тарту, бас бостандығын шектеу, бас бостандығынан айыру немесе өлім жазасы түріндегі жазалау қатерімен тыйым салынған айыпты жасалған қоғамға қауіпті іс-әрекет (әрекет немесе әрекетсіздік) қылмыс деп танылады" [15].

"Қылмыстық теріс қылық деп қоғамға зор қауіп төндірмейтін, жеке адамға, ұйымға, қоғамға немесе мемлекетке болмашы зиян келтірген не зиян келтіру қатерін туғызған, оны жасағаны үшін айыппұл салу, түзеу жұмыстары, қоғамдық жұмыстарға тарту, қамаққа алу, шетелдікті немесе азаматтығы жоқ адамды Қазақстан Республикасының шегінен тысқары жерге шығарып жіберу түріндегі жаза көзделген, айыпты жасалған іс-әрекет (әрекет не әрекетсіздік) танылады" [15].

Елеусіз болуына байланысты қоғамдық қауіп төндірмейтін іс-әрекет немесе әрекетсіздік қылмыстық құқық бұзушылық болып табылмайды.

Қылмыстық Кодексте мынадай құқық бұзушылықтар бойынша жазалар көзделген:

− 138-бап. Бала асырап алу құпиясын жария ету;

− 148-бап. Хат жазысу, телефон арқылы сөйлесу, пошта, телеграф немесе өзге де хабарлар құпиясын заңсыз бұзу;

− 223-бап. Коммерциялық немесе банктік құпияны, деңгейлес мониторинг барысында алынған салықтық құпияны, микрокредит беру құпиясын, коллекторлық қызмет құпиясын құрайтын мәліметтерді, сондай – ақ, мүлікті жария етуге байланысты ақпаратты заңсыз алу, жария ету немесе пайдалану;

− 321-бап. Медицина қызметкерінің құпиясын жария ету;

− 175-бап. Мемлекеттік опасыздық;

− 176-бап. Тыңшылық;

− 185 - бап. Мемлекеттік құпияларды заңсыз жинау, тарату, жария ету;

− 186-бап. Мемлекеттік құпиялары бар мәліметтер жеткізгіштерді жоғалту;

− 213-бап. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абоненттің сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай – ақ, абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды жасау, пайдалану, тарату;

− 458-бап. Әскери сипаттағы құпия мәліметтерді жария ету немесе әскери сипаттағы құпия мәліметтер жеткізгіштерді жоғалту.

ҚР ақпараттандыру және байланыс саласында жасалатын қылмыстарға арналған жеке тарауды да көздейді. Біліктілік жағдайларын ескере отырып, онда электрондық ақпараттық ресурстар мен телекоммуникация жүйелеріне немесе желілеріне қарсы қылмыстардың 38 құрамы бар.

Бақылау сұрақтары:

1. Әкімшілік құқық бұзушылық дегеніміз не?
2. Ақпараттандыру және байланыс саласындағы әкімшілік құқық бұзушылықтар қандай?
3. Қылмыстық теріс қылық дегенді қалай түсінесіз?
4. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар қандай қылмыс түріне жатады?

10 Ақпаратты қорғау әдістері

10.1 Ақпаратқа заңсыз қол жеткізу тәсілдері

Табысты күресудің кепілі, ол ақпаратқа рұқсатсыз қолжеткізу және деректерді ұстап алу ақпараттың таралып кету арналары туралы нақты түсінік.

Компьютерлерге қуат беретін интегралды микросхемалар кернеу мен ток деңгейінің жоғары жиіліктегі өзгерістерін жасайды. Тербелістер сымдар бойымен таралады және оларды түсінікті формаға айналдырып қана қоймай, оны арнайы құрылғылар ұстап алады. Мониторда көрсетілетін немесе пернетақтадан енгізілген ақпаратты ұстап қалу үшін құрылғыларды компьютерге немесе мониторға орнатуға болады. Ақпаратты беру сыртқы байланыс каналдары арқылы, мысалы, телефон желісі арқылы беру кезінде де мүмкін.

Іс жүзінде қорғау әдістерінің бірнеше тобы қолданылады, соның ішінде:

− ақпаратты ұрлаушының жолында физикалық және бағдарламалық құралдармен жасалатын кедергі;

− қорғалатын жүйенің элементтерін бақылау немесе әсер ету;

− деректерді криптографиялық құралдармен жасыру;

− дерекқорлармен өзара әрекеттесетін пайдаланушыларды өзін-өзі дұрыс ұстауға шақыруға бағытталған реттеу немесе нормативтік құқықтық актілерді әзірлеу және шаралар жиынтығы;

− мәжбүрлеу немесе пайдаланушы деректерді өңдеу ережелерін сақтауға мәжбүр болатын осындай жағдайлар жасау;

− пайдаланушыларға өзін дұрыс ұстауға итермелейтін жағдайлар жасау немесе жағдай жасау.

Ақпаратты қорғау әдістерінің әрқайсысы әртүрлі санаттағы құралдарды қолдану арқылы жүзеге асырылады. Негізгі құралдар - ұйымдастырушылық-техникалық.

Ақпараттық қауіпсіздікті реттеу - бұл бизнес-процестер мен ақпараттық инфрақұрылымның ерекшеліктерін, сонымен қатар, жүйелік архитектураны ескеретін ұйымның ішкі құжаты.

Ұйымдық ақпараттық қауіпсіздік

Ақпаратты қорғаудың ұйымдастырушылық құралдарының кешенін әзірлеу қауіпсіздік қызметінің құзыретіне кіруі керек.

Көбінесе қауіпсіздік мамандары:

− компьютерлік техникамен және құпия ақпаратпен жұмыс істеу ережелерін белгілейтін ішкі құжаттаманы әзірлеу;

− жеке құрамды брифингтер мен персоналды мерзімді тексерулерден өткізу;

− жұмыстан белгілі болған ақпаратты жария еткені немесе оны дұрыс пайдаланбағаны үшін жауапкершілікті белгілейтін еңбек шарттарына қосымша келісімдерге қол қоюды бастау;

− маңызды мәліметтер жиынтығы қызметкерлердің біреуінің қарамағында болған жағдайларды болдырмау үшін жауапкершілік салаларын шектеу;

− жалпы жұмыс процесі бағдарламаларында жұмысты ұйымдастыру және маңызды файлдардың желілік дискілерден тыс сақталмауын қадағалау;

− кез келген пайдаланушының деректерін көшіруден немесе жоюдан, соның ішінде ұйымның жоғарғы басшылығынан қорғайтын бағдарламалық өнімдерді енгізу;

− қандай да бір себептермен істен шыққан жағдайда жүйені қалпына келтіру жоспарларын құру.

Егер компанияда арнайы ақпараттық қауіпсіздік қызметі болмаса, шешім аутсорсингке қауіпсіздік маманын шақыру болып табылады. Қашықтағы қызметкер компанияның IT-инфрақұрылымын тексеріп, оны сыртқы және ішкі қауіп-қатерлерден қалай қорғауға болатындығы туралы ұсыныстар бере алады. Сондай-ақ, ақпараттық қауіпсіздікті аутсорсингке корпоративті ақпаратты қорғаудың арнайы бағдарламаларын қолдану жатады.

Ақпараттық қауіпсіздік техникасы

Ақпаратты қорғаудың техникалық құралдар тобы аппараттық және бағдарламалық жасақтаманы біріктіреді, негізгілері:

− компьютерлік жүйеде маңызды мәліметтер жиынтығының сақтық көшірмесін жасау және қашықтықтан сақтау;

− деректердің қауіпсіздігі үшін маңызды барлық желілік ішкі жүйелердің қайталануы және сақтық көшірмесі алу;

− жекелеген элементтер жұмыс істемей қалған жағдайда желілік ресурстарды қайта бөлу мүмкіндігін құру;

− резервтік қуат жүйелерін пайдалану мүмкіндігін қамтамасыз ету;

− жабдықтың өрттен немесе судан зақымдануынан қауіпсіздікті қамтамасыз ету;

− мәліметтер базасын және басқа ақпараттарды рұқсатсыз қол жеткізуден қорғайтын бағдарламалық жасақтаманы орнату.

Техникалық шаралар кешеніне сонымен қатар компьютерлік желілер объектілерінің физикалық қол жетімсіздігін қамтамасыз ету шаралары кіреді, мысалы, бөлмені камералармен және дабылды құрылғылармен жабдықтау сияқты практикалық әдістер.

Аутентификация және идентификация

Ақпаратқа заңсыз қолжеткізуді болдырмау үшін идентификация және аутентификация сияқты әдістер қолданылады.

Идентификация - ақпаратпен өзара әрекеттесетін пайдаланушыға өзінің ерекше атауы немесе суретін беру тетігі.

Аутентификация - пайдаланушының қабылданған кескінге сәйкестігін тексеру тәсілдерінің жүйесі.

Бұл қаражат деректерге қолжеткізуді қамтамасыз етуге немесе керісінше бас тартуға бағытталған.

Түпнұсқалық, әдетте, үш жолмен анықталады: бағдарламамен, аппаратпен, адаммен. Бұл жағдайда аутентификацияның объектісі тек адам ғана емес, сонымен қатар техникалық құрылғы (компьютер, монитор, тасымалдаушылар) немесе мәліметтер бола алады. Өзіңізді қорғаудың ең қарапайым тәсілі – құпия сөзге жасыру (пароль беру).

10.2 Ақпаратты таралып кетуден қорғау

Компанияны қаржылық және басқа құпия ақпараттың таралып кетуінен қалай қорғауға болады?

Ақпараттың таралып кетуіне қатысты ең осал бөліктердің бірі - бухгалтерлік есеппен тікелей байланысты ақпарат: қаржылық құжаттама, есеп беру, бизнес жоспарлар, келісімшарттар, қызметкерлердің еңбек ақысы, жеке деректері.

Ақпарат компаниядан кететін көптеген ақпарат көздері бар: әртүрлі мессенджерлер (Skype, ICQ және т.б.), электрондық пошта, ашық көздер (әлеуметтік желілер, форумдар), қағаз, флэш-дискілер, дискілер, сақтық көшірмелер. Оның үстіне, кездейсоқ таралып кету жағдайында таралу көздер бірдей.

Айтпақшы, құпия ақпаратты алудың бүкіл саласы бар - заңсыз және бәсекеге қабілетті барлау. Біріншісі шпиондықты қамтиды: ақпарат қажет адамдар компанияның қызметкерлерін жалдайды немесе қызметкерлер құрамына өз адамын енгізеді. Бәсекелестік интеллект ашық түрде жұмыс істейді - әлеуметтік желілер, сұхбаттар, ашық ақпарат көздері арқылы.

«Компания құпиялары» деген сауда белгілер бар:

Біріншіден, клиенттер компаниядан кеткен жағдайда немесе клиенттердің бірі базасын бәсекелестерге жіберіп алуы мүмкін.

Екіншіден, кейбір қызметкерлердің мінез-құлқындағы айқын өзгеріс: олардың қаржылық жағдайының кенеттен жақсаруы, жұмысқа деген қызығушылықтың төмендеуі, Интернеттегі хат-хабарлардың күшеюі, графикалық немесе парольмен қорғалған архивтік файлдардың жиі жіберілуі.

Үшіншіден, «кластерлеу». Осылайша, бір компанияда келісімшарт жасасуға қатысқан 40 жұмысшының 30-ы келісім бойынша өз ұйымын

тіркеп, нақты жұмыс істеген. Қызметкерлер өздері тікелей байланысқан клиенттерге бірдей қызметтерді ұсынады, бірақ сәл арзан бағамен және өз ұйымының атынан олармен келісім шарттарды ұзартады.

10.3 Ақпарат таралып кетуінің алдын алудың тиімді әдістері

Еңбек шарты. Онда жұмыс берушінің қызметкерлердің компьютерлеріндегі ақпаратқа толық қолжетімділігі және коммерциялық құпия ашылған жағдайда шығындардың орнын толтыруды талап ететіндігі туралы тікелей айтуға болады. Бұл шаралар мықты психологиялық тежеу болып табылады.

Жоғары жалақы. Оны жоғалтудан қорқу, ең алдымен, қызметкерді өз компаниясына опасыздық жасаудан бас тартады.

Бақылау және тыңдау. Компьютерде болатын барлық нәрсені басқаратын бағдарламалар бар. Егер қызметкерлер оны орнатқанын білсе, олар жұмыс компьютерінен құпия ақпаратты беруді қалауы екіталай. Сондай-ақ, олар өздерінің «қателерін» кеңселерде немесе мәжіліс бөлмелерінде орнатады, ал шпиондардың «қателіктерін» сигналды бөгейтін генераторлар жауып тастайды.

Оқыту. Олар арандатушылықты ұйымдастырады: қызметкерлерге вирустар бар хаттар жіберіледі, олардан құпия ақпаратты телефон арқылы беруді сұрайды, т.с.с. Тест нәтижесінде қызметкерлердің мұндай әрекеттерге қалай қарайтындығы анықталады және қорғау шаралары әзірленеді.

DLP жүйесі. (деректердің таралып кетуіне жол бермеу). Ол файлдардың тасымалдануын және басып шығарылуын, Интернеттегі байланыстың кенеттен пайда болуын, жұмыс үшін типтік емес сайттарға кіруді және т.б. бақылайды, сонымен қатар хат-хабарлар мен құжаттарға лингвистикалық талдау жүргізеді және кілт сөздерді қолдану арқылы таралып кету қаупін анықтайды. DLP жүйесімен жұмысты құзыретті маманға тапсыру өте маңызды. Егер компанияда ақпараттық қауіпсіздік бөлімі болмаса, аутсорсингке алынған қызметкер жүйені орнатып, инциденттерді тоқтата алады.

Қағаз құжаттары. Қағаздың көмегімен құпия ақпарат басқаларға жиі қол жетімді болады. Сонымен қатар, біреу оны әдейі таратып жатқанына немесе таралып кетуі кездейсоқ пайда болғанына қарамастан, қағаз құжаттарын сату электронды сатудан гөрі қауіпсіз, өйткені олардың кімнен алынғандығын дәлелдеу қиын (егер әрине жазба болмаса).

Компьютерлер. Компьютерлер (стационарлық дегенді білдіреді) инсайдерлер құпия ақпаратты жанына жіберетін екінші кең таралған арна. Бірақ, шын мәнінде, компьютер енді құпия деректерді беру арнасы емес, оларды қабылдауға арналған арна болып табылады. Ол арқылы инсайдер компанияның серверінде сақталған корпоративті ақпаратқа қол жеткізе

алады, оны алынбалы медиаға жүктей алады немесе электронды пошта арқылы жібере алады.

Ғаламтор. Қаржы туралы ақпарат Интернетте жұмыс істейтін компания бағдарламаларында болған кезде, кездейсоқ таралып кетулер орын алуы мүмкін және оларға кіру кезінде алғашқы парольдер бар. Бұл пернетақта бойындағы сандық немесе әріптік парольдер болып саналады: 123456, 123123, 12345678, qwerty, сонымен қатар abc123, dragon, 111111, iloveyou, sunshine, passw0rd, superman, football және т.б.

Электрондық пошта. Қызметкерлер құпия деректерді корпоративті емес, жеке поштадан жіберу қауіпсіз деп санайды. Бұл қате түсінік: кімнің мекен-жайын шоттардан анықтау оңай. Сондай-ақ, «электронды» вирусты жұқтырған хаттардың көмегімен компания құпияларына енуге көмектеседі. Тыңшылар қызметкердің қызығушылығын зерттейді (әлеуметтік желілерде және т.б.), содан кейін оған тақырып бойынша хат жіберіліп, оны міндетті түрде ашады.

Смартфондар, ноутбуктар. Смартфондар мен ноутбуктер сонымен қатар, құпия ақпараттың таралуының ең көп таралған арнасы емес, бірақ оларды көбінесе аға менеджерлер пайдаланады. Қатысушыларда жиналыс материалдары бар смартфондар немесе көбінесе ноутбуктар бар. Қазіргі инсайдер кіріктірілген микрофонды іске қосып, содан кейін жабық отырыста айтылғандардың бәрі сыртқы әлемге таратылады.

Алынатын тасымалдаушылар және сақтық көшірме. Ақпаратты тасымалдау үшін ыңғайлы болғандықтан, флэш-дискілер, портативті қатты дискілер де қолданылады. Сонымен қатар, инсайдер өзінің әдеттегі шығынына оңай сілтеме жасай алады. Мысалы, қызметкер флэш-дискте қаржылық көрсеткіштері бар есептерді үйде, ал үйде қорғалмаған интернет байланысын аяқтау үшін алды. Сақтық көшірмелер туралы айтатын болсақ, онда сіз Интернеттегі деректерді сақтай аласыз (мысалы, iCloud).

Коммерциялық құпия ақпаратты қорғау. Коммерциялық компаниялар өзі үшін де, бәсекелестер үшін де құнды көптеген ақпарат шығарады. Іскерлік маңызды ақпарат технологияны, ноу-хауды, өнертабыс пен дамуды, нарықты зерттеуді, стратегиялық жоспарларды және тәуелсіз активті құрайтын мәліметтердің басқа түрлерін қамтиды. Бәсекелес фирмалар үшін клиенттер мен контрагенттер туралы ақпарат та қызығушылық тудырады.

Мемлекет ақпаратты актив ретінде таниды және оны материалдық-құқықтық құндылықтарды қорғау шараларына баламалы белгілі бір қорғау шараларын белгілей отырып, оны азаматтық-құқықтық айналымға енгізеді.

10.4 Коммерциялық құпияны қорғау жолдары

Екі тең емес ұғымдарды ажырату керек. «Коммерциялық құпия» және «коммерциялық құпияны құрайтын ақпарат» заңнамада бір уақытта пайда болады, бірақ сәл өзгеше құбылыстар көзделеді.

«Коммерциялық құпия» термині құпиялылық режимінде, ақпаратты қылмыстық кіріп кетуден немесе сыртқа шығып кетуден қорғау үшін компанияда орнатылған қорғаныс ұйымдастырушылық шаралар жүйесін білдіреді. Құпиялылық режимі компанияға нарықтағы өз позициясын сақтауға, бәсекелестік артықшылығын сақтауға және құпия ақпаратты жариялау немесе тарату нәтижесінде шайқалған беделін қалпына келтіру шығындарынан аулақ болуға көмектеседі.

«Коммерциялық құпия ақпарат» - бұл компанияның өз еркімен анықтайтын ақпарат мөлшері. Ақпарат ғылыми, өндірістік, маркетингтік қызметке қатысты болуы мүмкін. Мұндай ақпараттың нақты немесе ықтимал коммерциялық құны үшінші тұлғаларға қол жетімсіз болғандықтан жоғарылайды. Ақпаратқа қатысты коммерциялық құпия режимі орнатылған.

Коммерциялық құпияны құрайтын ақпарат массивтері төрт топқа бөлінеді:

1. **Ғылыми-техникалық сипаттағы ақпарат:**

− өнертабыстар, ноу-хау, патенттер;
− рационализаторлық ұсыныстар;
− өндіріс тиімділігін арттыру әдістері;
− компьютерлік желілердің жұмысына, қауіпсіздік стандарттарына, бағдарламалық жасақтамаға, парольдерге қатысты барлық нәрсе.

2. **Технологиялық және өндірістік сипаттағы ақпарат:**

− сызбалар;
− модельдер;
− жабдықтың құжаттамасы;
− өндіріс рецептері;
− әдістемелер;
− бизнес-процестердің сипаттамасы;
− өндірістік және маркетингтік жоспарлар, стратегиялар, бизнес жоспарлар;
− инвестициялық ұсыныстар.

3. **Қаржы сипатындағы ақпарат,** ол жалпыға қолжетімді болып табылмайды:

− басқару және қаржылық есепке алу туралы мәліметтер;
− есептер;
− өнімнің өзіндік құны туралы ақпарат;
− ақша ағындарын есептеу;
− бағаны қалыптастыру тетіктері;

- болжамды салықтық шегерімдер.

4. **Әскери ақпарат:**

- жеткізушілер мен мердігерлер туралы ақпарат;
- тұтынушы туралы ақпарат; сату жоспарлары;
- әр түрлі стратегиялар;
- консультациялық ұсыныстар;
- нарықты талдау деректері және ұқсас ақпарат.

Әр топ үшін құпиялылық дәрежесін бағалауға мыналар кіреді:

- ұйымның жоғарғы басшылығына ғана қол жетімді құпиялылықтың ең жоғары дәрежесі;
- қатаң құпия ақпарат;
- құпия ақпарат;
- қолжетімділігі шектеулі ақпарат.

Құпиялылық деңгейі бойынша рейтинг қолжетімділік жүйесін жақсы ұйымдастыруға көмектеседі және таралып кету қаупін азайтады. Мысалы, компания қызметкерлерінің кең ауқымы үшін ең жоғары мәнді мәліметтерге қолжетімсіз болады, бұл оның қасақана немесе кездейсоқ таралып кету қаупі аз болатындығын білдіреді.

Коммерциялық құпияны қорғаудың заңды мүмкіндіктерін пайдалану үшін бірінші кезеңде компания коммерциялық құпия режимімен қамтылған ақпарат тізімін анықтауы керек. Болашақта контрагенттері бар қызметкерлерден деректерді қорғау шараларын сақтауды және коммерциялық құпияны құрайтын ақпаратты жариялағаны үшін оларды жауапкершілікке тартуды талап ету орынды.

Анықтамалық ақпаратпен қатар сіз құпиялылық режимін орнату қажет, бұл дегеніміз - ақпаратты әдейі немесе кездейсоқ жария етудің немесе таратудың алдын алуға көмектесетін әкімшілік, ұйымдастырушылық және техникалық шаралар жүйесін әзірлеу және енгізу болып табылады.

Азаматтық және қылмыстық заңнама саласындағы коммерциялық құпия режимін құқықтық реттеу. Құқықтық қатынастар құпия қорғау объектісі ретінде анықталған Азаматтық кодексте реттеледі. Коммерциялық құпия режимін сақтауға қатысты жеке нормалар Еңбек кодексінде қамтылған. Қылмыстық кодекс ақпаратты қасақана жария еткені үшін жауаптылық енгізеді. Осылайша, компания қандай мәліметтер коммерциялық құпияны құрайтын мәліметтерді дербес анықтауға құқылы және оны қорғауға мемлекеттік мәжбүрлеу шараларымен кепілдік беріледі.

Қауіп-қатер - ақпараттың құпиялылығын сақтау бойынша қорғаныс шаралары жүйесін жасамас бұрын және компанияға коммерциялық құпия режимді енгізбес бұрын, қауіпсіздікке қауіп төндіретін қауіпті анықтау. Қауіптер ішкі және сыртқы болып жіктеледі.

Сыртқы қауіп-қатерлерге коммерциялық құпияны құрайтын ақпарат алуға мүдделі болуы мүмкін субъектілердің үш тобы кіреді:

− бір нарықта жұмыс істейтін тікелей бәсекелестер немесе сол нарықтарға шығуды жоспарлап, компанияның жағдайына нұқсан келтірудің түрлі сценарийлерін жүзеге асыратын компаниялар;

− кәсіпорындағы акцияларды қайта бөлуге мүдделі субъектілер, рейдерлік топтар, миноритарлық акционерлер және активтер үшін күресте алынған ақпаратты пайдалана алатын басқа адамдар;

− компанияға тиесілі активтерге қол сұғатын субъектілер: жылжымайтын мүлік, жер учаскелері, акциялар және акциялар. Активтер туралы мәліметтер алу процесті жеңілдетеді.

Ішкі қауіп-қатерлер ең алдымен компанияның персоналымен, оның ішінде топ-менеджерлермен байланысты. Корпоративті ақпараттық жүйелерге қол жеткізетін қызметкерлер коммерциялық құпияны құрайтын ақпаратты сату, өзінің коммерциялық жобаларында пайдалану немесе компанияға зиян келтіру мақсатында шексіз кең ауқымды адамдарға тарату мақсатында заңсыз пайдалануы мүмкін.

Қорғау жүйесі барлық ықтимал қатерлерді анықтап, нақты қауіп-қатерлермен күресу механизмдерін қамтуы керек.

Коммерциялық құпияны құрайтын ақпарат алу әдістері

Ақпаратты коммерциялық құпия деп тану көп жағдайда сөздің қатаң мағынасында құпиялылықты білдірмейді, өйткені қызметкерлер, әзірлеушілер, тапсырыс берушілер мен мердігерлер деректерге қол жеткізе алады. Компанияның ішкі құжаттарында құпияға жататын ақпарат контрагенттердің әрекеттеріне байланысты көпшілікке қол жетімді болуы мүмкін. Құпия деп танылған ақпараттың екі жақты мәні деректерді алудың заңсыз ғана емес, сонымен қатар заңды тәсілдерін тудырады.

Коммерциялық құпияны алудың заңсыз жолдар:

− телекоммуникациялық желілерден ақпараттардың түсуін немесе ұйымдастырылуы;

− құжаттарды тікелей ұрлануы;

− қызметкерлерге пара берілуі.

Коммерциялық құпияны құқықтық жолдар:

− бұқаралық ақпарат құралдарын, мәліметтерді ашудың ресми көздерін, мысалы, қаржылық есептілік жарияланған веб-сайттарды, аралық соттардың істерін зерттеу. Ашық ақпарат көздері компанияның қаржылық жағдайы мен контрагенттермен қарым-қатынасы туралы жеткілікті дәл көрініс жасауға мүмкіндік береді;

− мақсатты компанияның қызметі туралы кең көлемді ақпаратқа ие және әңгімелесушілерге коммерциялық құпияны құрайтын мәліметтерді жария ету туралы ойланбай жауап беретін бәсекелес компаниялардың қызметкерлерімен жұмыс жасауы;

− егер компания ашық сауда жасайтын компания болса, оның проспектісінде коммерциялық құпияға жататын ақпараттың көп бөлігі бар. Сонымен қатар, егер консультанттар босату кезінде тарату шектеулерімен байланысты болмаса, олардың жұмысында ақпараттың едәуір мөлшері болады;

− компания қызметкерлерімен сұхбаттасу, қызметке тікелей қатысы жоқ сұрақтарға жауап беру кезінде құпиялылық режимін бұзбайды, бірақ сізге пайдалы ақпараттың көп мөлшерін алуға мүмкіндік береді;

− компания қызметкерлеріне жұмыс ұсынысы, кейде адамды жалдауды көздемейді. нақты қамтамасыз ету. Қабылдау нақты жұмыс орны, міндеттері, өнімдері туралы кең көлемді мәліметтер алуға мүмкіндік береді;

− өнімнің өзін, сондай-ақ шикізат пен компоненттерді жеткізушілердің жұмысын зерттеу;

− компания мен қызметкерлерді қадағалаудың барлық түрлері;

− нақты келісім жасамай-ақ мүмкін болатын келісім-шарт туралы келіссөздер жүргізу. әдіс мәліметтердің көп мөлшерін жинауға ғана емес, сонымен қатар өндіріс процесін іштен зерттеуге мүмкіндік алуға мүмкіндік береді. Осылайша алынған ақпарат коммерциялық құпияны құрайды, бірақ өз еркімен беріледі.

Деректерді жинаудың осы әдістерімен күресу, олардың заңдылығын қиындатады. Қарсы шараларға қызметкерлерге нұсқау беру, әлеуетті мердігерлерді мұқият тексеру және компанияның орналасқан жерінен тыс жерлерде келіссөздер жүргізу кіреді.

Коммерциялық құпияны қорғау шаралары

Коммерциялық құпияны құрайтын ақпаратты қорғаудың негізгі шарасы коммерциялық құпия режимін орнату болады. Негізгі қызмет түрлері әкімшілік-ұйымдастырушылық сипатта болады. Мысалы, жүйенің негізгі элементтерінің бірі құпиялылықты бұзғаны үшін қызметкерлердің жауапкершілігін қарастыратын еңбек шарты болып табылады. Сыртқы қауіптер компанияның компьютерлік желілерінен коммерциялық құпияны құрайтын мәліметтерді ұрлау түрінде көрінетіндігін ескере отырып, қорғаудың толықтығына кепілдік беретін техникалық шараларды енгізу қажет.

Әкімшілік-ұйымдастырушылық шаралар

Ең алдымен, әкімшілік және ұйымдастырушылық шаралар қызметкерлерге қандай ақпарат коммерциялық құпияға жататындығы және персоналға жария етілмеген қандай міндеттемелер жүктелгені туралы хабарлауға бағытталған.

Тағы бір мақсат - компанияның барлық заңды талаптарды орындағанына және сақтық танытқанына көз жеткізу. Бұл қылмыстық іс-

әрекеттен пайда тапқан коммерциялық құпияны ұрлаушыға немесе ұрлауға тапсырыс берушіге қарсы мүмкін сот ісі туындаған жағдайда позицияны күшейтеді.

Әкімшілік шараларға жатады:

− коммерциялық құпия режимін енгізу туралы бұйрық шығару;

Құжат қорғаныс жүйесінің негізгі параметрлерін және қорғау шараларын ұйымдастыруға жауапты адамдарды анықтайды.

− коммерциялық құпияға қатысты мәліметтер тізімін анықтау;

Көбінесе құжаттардың авторлары тізімге өздері білетін барлық ақпаратты енгізеді. Бұл дұрыс емес жол, өйткені жария етілген есеп беру сияқты көптеген мәліметтер жалпыға қол жетімді. Сот ісі қаралған жағдайда, мәліметтер тізімі тым кең болуы бүкіл тізімді коммерциялық құпия режимге сәйкес емес деп тануға негіз бола алады. Шынайы құнды ақпарат тізімін шектеген жөн. Құрылтай құжаттарынан алынған мәліметтер, штат кестесі, еңбек режимі, экологиялық және өртке қарсы талаптардың сақталуы туралы мәліметтердің көпшілігі құпияға жатқызыла алмайды.

− құпиялылық режимінің сақталуын және коммерциялық құпияны құрайтын ақпараттарды қорғауды қамтамасыз ететін жергілікті нормативтік құқықтық актілер жүйесін құру.

Негізгі құжатқа қосымша - «коммерциялық құпиялар туралы» ережелер - электронды компьютерлермен жұмыс туралы, контрагенттер мен мемлекеттік органдарға ақпарат беру тәртібі, құжаттарды көшіру тәртібі, контрагенттермен типтік келісімшарттар, еңбек келісім шарттарының қосымшалары және басқалары туралы ережелер әзірленуі мүмкін.

Ереже коммерциялық құпия ретінде анықталған мәліметтер тізіміне арналған бөлімдерді қамтуы керек; ақпарат коммерциялық құпия деп танылатын тізбеге немесе жалпы өлшемдерге өзгерістер енгізу тәртібі; құпия ақпаратпен жұмыс істеу құқығына ие адамдардың дәрежелері мен қабылдау деңгейлерінің тізбесі; коммерциялық құпияны құрайтын ақпараттың тасымалдаушылары болып табылатын құжаттармен және ақпараттық базалармен жұмыс істеу тәртібі; қарапайым пайдаланушылардың және құпиялылықты қамтамасыз ету функциялары сеніп тапсырылған адамдардың құқықтары мен міндеттері; әртүрлі тасымалдағыштарды сақтау, есепке алу және жою тәртібі.

Сонымен қатар, ережеде талаптарды орындамағаны үшін жауапкершілік шаралары болуы керек. Ережеге сәйкес әзірленуге қалған құжаттар оған қайшы келмеуі керек. Компания қызметкерлері лауазыммен таныс болуы керек. Заңнама құжатты әзірлеуге кәсіподақ немесе еңбек ұжымының басқа өкілдік органдарын тартуды міндеттемейді, бірақ қажет болған жағдайда олардың пікірі ескерілуі мүмкін.

Коммерциялық құпияны құрайтын мәліметтерден тұратын материалдармен жұмыс істеуге құқығы бар адамдар шеңберін және рұқсаттың деңгейін анықтау. Осы кезеңде ұйымдастыру шаралары техникалық шаралармен өзара әрекеттесуі керек, өйткені клиренс деңгейлері компанияның АТ құрылымында жүзеге асырылады. Неғұрлым сенімді қорғаныс үшін қауіпсіздікті рұқсат етуді тек ақпараттық құндылық дәрежесі бойынша ғана емес, сонымен қатар салалық сипатта да тағайындау орынды болады. Атқарушы органның бұйрығы деңгейінде анықталған уәкілетті адамдарға, оларға сеніп тапсырылған ақпарат коммерциялық құпия болып табылатындығы туралы ескертіліп, жұмыстан босату мүмкіндігі және оны жария еткені үшін басқа санкциялар туралы ескертілуі керек.

Коммерциялық құпияны қорғау туралы ережені қамтитын контрагенттермен еңбек келісім-шарттарын және келісімшарттарды әзірлеу. Қызметкерлермен жасалған келісімшартта құпия ақпаратты жариялағаны үшін жауапкершілік және компанияның қызметкерге материалдық зиянды өтеуге міндеттеу құқығы туралы ескертетін тармақ болуы керек. Сондай-ақ, заң еңбек шартында еңбек шарты тоқтатылғаннан кейін басталатын кезеңді көрсетуге мүмкіндік береді, оның барысында қызметкер еңбек міндеттерін орындауға байланысты белгілі болған ақпаратты жария етуге құқылы емес. Әдетте мерзімі үш жыл. Қызметкер қол қойылған мәліметтер тізімімен танысуы керек. Жеке қолының болуы қызметкердің жауапкершілікті толық білетіндігін және ақпарат ашылған жағдайда жазалауға дайын екендігін куәландырады.

Қосу контрагенттермен келісім шарт талаптарын орындауға байланысты контрагентке немесе оның қызметкерлеріне сеніп тапсырылған ақпарат коммерциялық құпияны құрайтын жағдайларда құпиялылық шарттарын жасасады. Мұндай контрагенттер аудиторлық, консалтингтік, бағалаушы және басқа компаниялар бола алады. Келісімшарттағы тармақ құпияларды жария етуден келтірілген зиянды толығымен өтеуге міндеттелуі керек.

Құпия ақпаратты және құжаттардың көшірмелерін сәйкестендіру құралдарын қорғау үшін «коммерциялық құпия» мөртабанының жұмыс істеуі. Бұл ықтимал тұтынушыларға ақпарат беру үшін құжаттарды көшіруден сақтамайды, бірақ қоғамдық домендегі кең ауқымды адамдарға таратуды шектейді.

Телекоммуникациялық жабдықты, көшіру құрылғыларын, сыртқы электрондық поштаны, Интернетті пайдаланудың арнайы режимдері. Қызметкердің ресурстарға қол жетімділігі пайдалану қажеттілігін негіздейтін сұраныстарға негізделуі керек. Сұраныстарды қызметкердің басқару және қауіпсіздік қызметі деңгейінде үйлестіру керек.

Желідегі шоттарды тек шот иелерінің парольді беру «коммерциялық құпияны ашуына» байланысты жұмыстан шығаруға негіз бола алатындығын ескертумен қатаң бақылау.

Коммерциялық құпияны қорғаудың техникалық шаралары

Коммерциялық құпияны құрайтын ақпаратты қорғаудың техникалық шаралары арасында, ең алдымен, ақпараттың периметрін таралып кетуден, рұқсатсыз көшіруден немесе деректерді жіберуден толық қорғауға мүмкіндік беретін бағдарламалар қарастырылған. Бұл құралдарға DLP жүйелері мен SIEM жүйелері кіреді.

DLP класының жүйелері мүмкіндігінше ішкі пайдаланушылардың ақпаратты ұрлауы мүмкін болмайтындай етіп конфигурацияланған. SIEM-сынып жүйелері қауіп-қатерлерді анықтайды және сыртқы қауіпсіздік периметрі арқылы тәуекелдерді толық басқаруға және кіріптардан қорғауға мүмкіндік береді.

Қорғаудың техникалық шаралары деректерді кодтау мен шифрлаудың барлық әдістерін, көшіруге тыйым салуды, қызметкерлердің компьютерлерін басқаруды және шоттарды пайдалануды бақылауды қамтиды.

Коммерциялық құпияны қорғаудың заңды жолдары

Егер барлық ақпараттар орын алса және құпия ақпараттың таралуын болдырмау мүмкін болмаса, кінәліні жауапқа тарту және зиянды өтеу қажет болады. Бұл сот арқылы ғана мүмкін болады. «Коммерциялық құпияны жариялау» негізінде жұмыстан шығаруға сот тәртібімен шағым жасалуы мүмкін.

Бақылау сұрақтары:

1. Коммерциялық құпияны қорғаудың заңды жолдарын атаңыз.
2. Коммерциялық құпияны құрайтын ақпарат алу әдістері қандай?
3. Коммерциялық құпияны алудың заңсыз жолдарын атаңыз.

Пайдаланылған әдебиеттер тізімі

1. Қазақстан Республикасының 1995 жылғы 30 тамыздағы Конституциясы
2. Қазақстан Республикасының Ұлттық қауіпсіздігі туралы. Қазақстан Республикасының 2012 жылғы 6 қаңтардағы № 527-IV Заңы
3. Мемлекеттік құпиялар туралы. Қазақстан Республикасының 1999 жылғы 15 наурыздағы N 349-1 Заңы.
4. Киберқауіпсіздік тұжырымдамасын ("Қазақстан киберқалқаны") бекіту туралы. Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы
5. "Авторлық құқық және сабақтас құқықтар туралы" Қазақстан Республикасының 1996 жылғы 10 маусымдағы № 6 Заңы
6. "Қазақстан Республикасының патенттік Заңы" Қазақстан Республикасының 1999 жылғы 16 шілдедегі № 427 Заңы .
7. "Рұқсаттар және хабарламалар туралы" Қазақстан Республикасының Заңы 2014 жылғы 16 мамырдағы № 202-V ҚРЗ.
8. Дербес деректер және оларды қорғау туралы. Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы.
9. Ақпараттық жүйелердің аудитін жүргізу қағидаларын бекіту туралы. Қазақстан Республикасы Ақпарат және коммуникациялар министрінің 2018 жылғы 13 маусымдағы № 263 бұйрығы.
10. Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы.
11. Мәліметтерді таратылуы шектелген қызметтік ақпаратқа жатқызу және онымен жұмыс істеу қағидаларын бекіту туралы. Қазақстан Республикасы Үкіметінің 2015 жылғы 31 желтоқсандағы № 1196 қаулысы.
12. Ақпаратқа қол жеткізу туралы. Қазақстан Республикасының Заңы 2015 жылғы 16 қарашадағы № 401-V ҚРЗ.
13. Электрондық құжат және электрондық цифрлық қолтаңба туралы. Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370 Заңы
14. Электрондық цифрлық қолтаңбаның төлнұсқалығын тексеру қағидаларын бекіту туралы. Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 9 желтоқсандағы № 1187 бұйрығы.
15. Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V ҚРЗ "Әкімшілік құқық бұзушылық туралы" Кодексі
16. Қазақстан Республикасының Қылмыстық кодексі Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ.
17. Ақпараттық қауіпсіздік саласындағы Менеджмент. М.: Интернет-Ақпараттық Технологиялар Университеті, 2017

18. Шангин В. Ақпараттық қауіпсіздік: М., DMK Press, 2014 \ \ ЭБС Lan.

19. ҚР СТ ИСО / МЭК 27002-2015 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару құралдары бойынша қағидалар жиынтығы"

20. Сыртқы және өзара сауданың интеграцияланған ақпараттық жүйесін құру, пайдалану және дамыту кезінде қолданылатын ақпараттық-телекоммуникациялық технологиялар мен ақпараттық қауіпсіздік саласындағы стандарттар мен ұсынымдардың тізбесі туралы. Еуразиялық экономикалық комиссия Алқасының 2015 жылғы 3 ақпандағы № 2 ұсынымы

21. "Мемлекеттік техникалық қызмет" ақ [сайт]. URL http://sts.kz

А қосымшасы

Қосымша
аудит жүргізу қағидаларына
Ақпараттық жүйелер
Пішіні

Аудит жүргізу нәтижелері бойынша аудиторлық қорытынды
ақпараттық жүйе

_____
(ақпараттық жүйенің атауы)
_____
(Тапсырыс беруші ұйымның атауы)
саласындағы
_____
(аудит жүргізу саласы)
бастап "___" _____ 20__ жыл
_____
(ақпараттық жүйелердің аудитін жүзеге асыратын жеке тұлғаның тегі, аты, әкесінің аты (ол болған кезде) және (немесе) заңды тұлғаның атауы) "___" _____ 20__ аудит ақпараттық жүйелердің аудитін жүргізу ережелеріне сәйкес жүргізілді, аудиторлық тексеру барысында осы ақпараттық жүйенің келесі бағалау көрсеткіштері бар екендігі анықталды:
1. _____
2. _____
3. _____
облыста белгіленген талаптар мен стандарттарға не сәйкес келеді/сәйкес келмейді
_____
(аудит жүргізу саласы)
Ақпараттық жүйені сүйемелдеу және дамыту бойынша ұсынымдар
_____
_____
_____
(Тегі, Аты, Әкесінің аты (бар болса), қолы)
"___" _____ 20__ жыл
Мөрге арналған орын
(бар болған кезде)

Б қосымшасы

Сыртқы және өзара сауданың интеграцияланған ақпараттық жүйесінің интеграциялық сегментінде және сенім білдірілген үшінші тараптың бағдарламалық-аппараттық кешенінде ақпаратты қорғау және оның қауіпсіздігін қамтамасыз ету құралдарын әзірлеу

1. ISO/IEC 15408-1: 2009 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпарат қауіпсіздігін бағалау критерийлері. 1 бөлім. Кіріспе және жалпы модель " (Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model).

2. ISO/IEC 15408-2: 2008 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпарат қауіпсіздігін бағалау критерийлері. 2 бөлім. Қауіпсіздіктің функционалдық талаптары " (Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components).

3. ISO/IEC 15408-3:2008 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ат қауіпсіздігін бағалау критерийлері. 3 бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар" (Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components).

4. ISO/IEC 27001:2013 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" (Information technology – Security techniques – Information security management systems – Requirements).

5. ISO/IEC 27002:2013 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы" (Information technology – Security techniques – Code of practice for information security controls).

6. ISO/IEC 27003:2010 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік менеджменті жүйесін енгізу бойынша нұсқаулық" (Information technology – Security techniques – Information security management system implementation guidance).

7. ISO/IEC 27004:2009 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті. Өлшеу " (Information technology – Security techniques – Information security management – Measurement).

8. ISO/IEC 27005:2011 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік тәуекелін басқару" (Information technology-Security techniques-Information security risk management).

9. ISO/IEC 27033-1:2009 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Желілік қауіпсіздік. 1 бөлім. Шолу және тұжырымдамалар" (Information technology – Security techniques – Network security – Part 1: Overview and concepts).

10. ISO/IEC 18028-4:2005 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық желінің қауіпсіздігі. 4 бөлім. Қашықтықтан қол жеткізу қауіпсіздігін қамтамасыз ету" (Information technology-Security techniques-IT network security –

Part 4: Securing remote access).

11. ГОСТ 28147-89 "Ақпаратты өңдеу жүйелері. Криптографиялық қорғау. Криптографиялық түрлендіру алгоритмі".

12. ITU-T X. 842 "Ақпараттық технологиялар. Қорғау әдістері. Сенім білдірілген үшінші тарап қызметтерін қолдану және басқару жөніндегі басшылық нұсқаулар" (Information technology – Security techniques – Guidelines for the use and management of trusted third party services).

13. ITU-T x. 509 "Ақпараттық технологиялар. Ашық жүйелердің өзара байланысы. Анықтама: ашық кілттер мен атрибуттар сертификаттарының құрылымы" (Information technology – Open Systems Interconnection – the Directory: Public-key and attribute certificate frameworks).

14. XML синтаксисі және электрондық қолтаңбаны өңдеу (XML Signature Syntax and Processing (Second Edition) (XML-DSig)).

15. Электрондық қолтаңбаны XML-ге кеңейту (XML advanced Electronic Signatures (XAdES)).

16. "Құрылымдық хабарламалардың қауіпсіздігі" веб-сервистерінің қауіпсіздік сипаттамасы (Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)).

В қосымшасы

ҚР АК 31-тарауы "Ақпараттандыру және байланыс саласындағы әкімшілік құқық бұзушылықтар»

Мақала атауы	Жауапкершілік нормасы
639-бап Электрондық ақпараттық ресурстарды қорғау құралдарын пайдалану жөніндегі талаптарды бұзу	«1. Электрондық ақпараттық ресурстарды қорғау құралдарын пайдалану жөніндегі талаптарды мемлекеттік техникалық қызметтің бағдарламалық (бағдарламалық-техникалық) құралдарының жұмысына кедергі келтіру немесе бұғаттау, сол сияқты мемлекеттік техникалық қызмет қызметкерлерінің мемлекеттік техникалық қызметпен өзара іс-қимыл жасайтын ақпараттандыру объектілерімен жұмысына кедергі келтіру түрінде жасалған бұзу, –» "Ескерту жасауға немесе жеке тұлғаларға – он, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – жиырма, орта кәсіпкерлік субъектілеріне – қырық, ірі кәсіпкерлік субъектілеріне бір жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.» «2. Осы баптың бірінші бөлігінде көзделген, қайталап жасалған немесе ақпараттық қауіпсіздіктің оқыс оқиғасының туындауына әкеп соққан әрекеттер (әрекетсіздік), –» "Жеке тұлғаларға – жиырма, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – елу, орта кәсіпкерлік субъектілеріне – бір жүз, ірі кәсіпкерлік субъектілеріне екі жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.» "Ескерту жасауға немесе жеке тұлғаларға – он, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – жиырма, орта кәсіпкерлік субъектілеріне – қырық, ірі кәсіпкерлік субъектілеріне бір жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады».
640-бап Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба туралы заңнамасын бұзу	«1. Қазақстан Республикасының заңдарында көзделген жағдайларда электрондық құжаттарды қабылдаудан бас тарту, –лауазымды адамдарға – жиырма, заңды тұлғаларға елу айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады». «2. Куәландырушы орталықтың сақтауда тұрған электрондық цифрлық қолтаңбаның ашық кілттерінің жоғалуын, түрлендірілуін және қолдан жасалуын болдырмау үшін қажетті шараларды қабылдамауы –

	жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады». «3. Куәландырушы орталықтың тіркеу куәліктерінің иелері туралы мәліметтерді қорғауды қамтамасыз етпеуі – жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады». «4. Тіркеу куәлігі иесінің электрондық цифрлық қолтаңбаның өзіне тиесілі жабық кілтін заңсыз қол жеткізуден және пайдаланудан қорғау үшін, сондай-ақ ашық кілттерді сақтау бойынша Қазақстан Республикасының заңнамасында белгіленген тәртіппен шаралар қолданбауы, – елу айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады». «5. Электрондық цифрлық қолтаңбаның жабық кілтін басқа тұлғаларға заңсыз беру – Жеке тұлғаларға – он, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – он бес, орта кәсіпкерлік субъектілеріне – отыз, ірі кәсіпкерлік субъектілеріне бір жүз елу айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады».
Мақала атауы	Жауапкершілік нормасы
641-бап Қазақстан Республикасының Ақпараттандыру туралы заңнамасын бұзу	1. Қазақстан Республикасының заңдарында көзделген жағдайларда электрондық құжаттарды қабылдаудан бас тарту, – лауазымды адамдарға – жиырма, заңды тұлғаларға елу айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 2. Куәландырушы орталықтың сақтауда тұрған электрондық цифрлық қолтаңбаның ашық кілттерінің жоғалуын, түрлендірілуін және қолдан жасалуын болдырмау үшін қажетті шараларды қабылдамауы – жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 3. Куәландырушы орталықтың тіркеу куәліктерінің иелері туралы мәліметтерді қорғауды қамтамасыз етпеуі – жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 4. Тіркеу куәлігі иесінің электрондық цифрлық қолтаңбаның өзіне тиесілі жабық кілтін заңсыз қол жеткізуден және пайдаланудан қорғау үшін, сондай-ақ ашық кілттерді сақтау бойынша Қазақстан Республикасының заңнамасында белгіленген тәртіппен шаралар қолданбауы, – елу айлық есептік

	көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 5. Электрондық цифрлық қолтаңбаның жабық кілтін басқа тұлғаларға заңсыз беру – Жеке тұлғаларға – он, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – он бес, орта кәсіпкерлік субъектілеріне – отыз, ірі кәсіпкерлік субъектілеріне бір жүз елу айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. Ескерту. 640-бап жаңа редакцияда-ҚР 24.11.2015 № 419-V Заңымен (01.01.2016 бастап қолданысқа енгізіледі). 641-бап. Қазақстан Республикасының Ақпараттандыру туралы заңнамасын бұзу 1. Қазақстан Республикасының Ақпараттандыру туралы заңнамасын: 1) меншік иесі немесе иеленушісі дербес деректерді қамтитын ақпараттық жүйелерді, дербес деректерді қамтитын базаның меншік иесі және (немесе) операторы, сондай-ақ үшінші тұлға оларды қорғау жөніндегі шараларды жүзеге асырмаған немесе тиісінше жүзеге асырмаған жағдайларда жол берілмейді; 2) ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бұзу; 3) Алып тасталды-ҚР 18.03.2019 № 237-VI Заңымен (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); 4) "электрондық үкіметтің" сервистік интеграторына әзірленген бағдарламалық қамтылымды, бастапқы бағдарламалық кодтарды (болған кезде), "электрондық үкіметтің" ақпараттандыру объектілерінің лицензиялық бағдарламалық қамтылымының күйге келтіру кешенін ұсынбау"; 5) қағаз жеткізгіштердегі техникалық құжаттаманың түпнұсқаларын жоғалту; 6) Ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтардың оң нәтижелері бар акт болмаса, "электрондық үкіметтің" ақпараттандыру объектісін өнеркәсіптік пайдалану қағидаттарына негізделеді – Жеке тұлғаларға – он, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық

	емес ұйымдарға – он бес, орта кәсіпкерлік субъектілеріне – отыз, ірі кәсіпкерлік субъектілеріне бір жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 2. Мемлекеттік электрондық ақпараттық ресурстардың резервтік көшірмесін әзірлемеу – лауазымды адамдарға – отыз, заңды тұлғаларға сексен айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 3. Осы баптың бірінші және екінші бөліктерінде көзделген, әкімшілік жаза қолданылғаннан кейін бір жыл ішінде қайталап жасалған әрекеттер (әрекетсіздік), – Жеке тұлғаларға – жиырма, лауазымды адамдарға – елу, заңды тұлғаларға жүз елу айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 4. Жеке тұлғалар туралы дербес деректерді қамтитын электрондық ақпараттық ресурстарды оларға мүліктік және (немесе) моральдық зиян келтіру, Қазақстан Республикасының заңдарында кепілдік берілген құқықтар мен бостандықтарды іске асыруды шектеу мақсатында пайдалану, – ескерту жасауға немесе жеке тұлғаларға – он, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – жиырма, орта кәсіпкерлік субъектілеріне – қырық, ірі кәсіпкерлік субъектілеріне екі жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады. 5. Егер Қазақстан Республикасының заңнамалық актілерінде өзгеше белгіленбесе, ақпараттық қауіпсіздікті ұлттық үйлестіру орталығының ақпараттық-коммуникациялық инфрақұрылымының аса маңызды объектілері меншік иесінің немесе иеленушісінің ақпараттық қауіпсіздіктің оқыс оқиғалары туралы және оларға ден қою нәтижелері туралы "электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларында айқындалған тәртіппен және мерзімдерде хабарламауы, – жеке және лауазымды адамдарға – жиырма, шағын кәсіпкерлік субъектілеріне – қырық, орта кәсіпкерлік субъектілеріне – алпыс, ірі кәсіпкерлік субъектілеріне бір жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.

	6. Осы баптың бесінші бөлігінде көзделген, әкімшілік жаза қолданылғаннан кейін бір жыл ішінде қайталап жасалған іс-әрекет, – жеке және лауазымды адамдарға – қырық, шағын кәсіпкерлік субъектілеріне сексен, орта кәсіпкерлік субъектілеріне бір жүз жиырма, ірі кәсіпкерлік субъектілеріне екі жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.

Г қосымшасы

ҚР ҚК 7-тарауы "Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар" мынадай баптар көзделген:

Мақала атауы	Жауапкершілік нормасы
205 бап Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу	1. Азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделерін елеулі түрде бұзуға әкеп соққан, электрондық жеткізгіштегі заңмен қорғалатын ақпаратқа ақпараттық жүйеге немесе телекоммуникациялар желісіне қасақана құқыққа сыйымсыз қол жеткізу, – бір жүз алпыс айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір жүз алпыс сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан айыра отырып немесе онсыз қырық тәулікке дейінгі мерзімге қамаққа алуға жазаланады. 2. Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне қатысты жасалған дәл сол іс-әрекет, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан екі жылға дейінгі мерзімге айыра отырып немесе онсыз, екі жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не екі жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не елу тәулікке дейінгі мерзімге қамаққа алуға жазаланады. 3. Осы баптың бірінші немесе екінші бөліктерінде көзделген, абайсызда ауыр зардаптарға әкеп соққан іс-әрекеттер, – үш жылға дейінгі мерзімге белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан айыра отырып немесе онсыз, екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.
206 бап. Ақпаратты заңсыз жою немесе түрлендіру	1. Электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникация желілері арқылы берілетін, заңмен қорғалатын ақпаратты қасақана құқыққа сыйымсыз жою немесе түрлендіру, сол сияқты, егер бұл азаматтардың немесе ұйымдардың

құқықтары мен заңды мүдделерін не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделерін елеулі түрде бұзуға әкеп соқса, ақпараттық жүйеге көрінеу жалған ақпарат енгізу, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан екі жылға дейінгі мерзімге айыра отырып немесе онсыз, екі жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не екі жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не елу тәулікке дейінгі мерзімге қамаққа алуға жазаланады.

2. Жасалған дәл сол әрекеттер:
1) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне қатысты;
2) адамдар тобының алдын ала сөз байласуымен, –
үш жылға дейінгі мерзімге белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан айыра отырып немесе онсыз, екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

3. Осы баптың бірінші немесе екінші бөліктерінде көзделген іс-әрекеттер:
1) қылмыстық топ жасаған;
2) ауыр зардаптарға әкеп соққан, –
белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

207 бап. Ақпараттық жүйенің немесе телекоммуникация желілерінің жұмысын бұзу

1. Ақпараттық жүйенің немесе телекоммуникация желілерінің жұмысын бұзуға бағытталған қасақана әрекеттер (әрекетсіздік), –
екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

2. Жасалған дәл сол әрекеттер:
1) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне қатысты;
2) адамдар тобының алдын ала сөз байласуымен, –

белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз, төрт мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір мың сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не төрт жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

3. Осы баптың бірінші немесе екінші бөліктерінде көзделген іс-әрекеттер:

1) қылмыстық топ жасағаң;

2) ауыр зардаптарға әкеп соққан, –

белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан бес жылға дейінгі мерзімге айыра отырып немесе онсыз бес жылдан он жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

208 бап. Ақпаратты заңсыз иелену

1. Егер бұл азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделерін елеулі түрде бұзуға әкеп соқса, электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникациялар желілері арқылы берілетін, заңмен қорғалатын ақпаратты қасақана құқыққа сыйымсыз көшіру немесе өзге де құқыққа сыйымсыз иемдену, –

белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан екі жылға дейінгі мерзімге айыра отырып немесе онсыз, екі жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не жүз сексен сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не елу тәулікке дейінгі мерзімге қамаққа алуға жазаланады.

2. Жасалған дәл сол әрекет:

1) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне қатысты;

2) адамдар тобының алдын ала сөз байласуымен, –

үш жылға дейінгі мерзімге белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан айыра отырып немесе онсыз, екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

3. Осы баптың бірінші немесе екінші бөліктерінде көзделген іс-әрекеттер:
1) қылмыстық топ жасаған;
2) ауыр зардаптарға әкеп соққан, –
белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

209 бап. Ақпаратты беруге мәжбүрлеу

1. Электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникация желілері арқылы берілетін заңмен қорғалатын ақпаратты күш қолдану не мүлікті жою немесе бүлдіру қатерін төндіру арқылы, сол сияқты жәбірленушіні немесе оның жақындарын масқаралайтын мәліметтерді тарату қатерін төндіру арқылы не жариялануы жәбірленушінің немесе оның жақындарының мүдделеріне елеулі зиян келтіруі мүмкін өзге де мәліметтерді беруге мәжбүрлеу, –
екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

2. Сол әрекет:
1) адамға немесе оның жақындарына күш қолданумен ұштасқан;
2) адамдар тобы алдын ала сөз байласу арқылы жасаған іс-әрекеттер;;
3) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінен ақпарат алу мақсатында жасалған, –
белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

3. Осы баптың бірінші немесе екінші бөліктерінде көзделген іс-әрекеттер:
1) қылмыстық топ жасаған;
2) ауыр зардаптарға әкеп соққан, –
белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан бес жылға дейінгі мерзімге айыра отырып немесе онсыз бес жылдан он жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.

210-бап Зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату	1. Электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникация желілері арқылы берілетін ақпаратты құқыққа сыйымсыз жою, бұғаттау, түрлендіру, көшіру, пайдалану, компьютердің, абоненттік құрылғының, компьютерлік бағдарламаның, ақпараттық жүйенің немесе телекоммуникация желілерінің жұмысын бұзу мақсатында компьютерлік бағдарламаны, бағдарламалық өнімді жасау немесе қолданыстағы бағдарламаға немесе бағдарламалық өнімге өзгерістер енгізу, сол сияқты осындай бағдарламаны немесе бағдарламалық өнімді қасақана пайдалану және (немесе) тарату – үш мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не сегіз жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не үш жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады. 2. Жасалған дәл сол әрекеттер: 1) адамдар тобының алдын ала сөз байласуымен; 2) адам өзінің қызмет бабын пайдалана отырып жасаған іс-әрекеттері; 3) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне қатысты, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз, үш жылдан жеті жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады. 3. Осы баптың бірінші немесе екінші бөліктерінде көзделген іс-әрекеттер: 1) қылмыстық топ жасаған; 2) ауыр зардаптарға әкеп соққан, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан бес жылға дейінгі мерзімге айыра отырып немесе онсыз бес жылдан он жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.
211 бап. Қолжетімділігі шектеулі электрондық ақпараттық ресурстарды құқыққа сыйымсыз тарату	«1. Азаматтардың дербес деректерін немесе Қазақстан Республикасының заңдарында немесе олардың меншік иесінде немесе иеленушісінде қолжетімділігі шектелген өзге де мәліметтерді қамтитын электрондық ақпараттық ресурстарды құқыққа сыйымсыз тарату, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз, екі жүз айлық

	есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не жүз сексен сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не елу тәулікке дейінгі мерзімге қамаққа алуға жазаланады. 2. Жасалған дәл сол әрекет: 1) адамдар тобының алдын ала сөз байласуымен; 2) пайдакүнемдік ниетпен; 3) адам өзінің қызмет бабын пайдалана отырып жасаған іс-әрекеттері, – бір мың екі жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не бес жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз жазаланады. 3. Осы баптың бірінші немесе екінші бөліктерінде көзделген іс-әрекеттер: 1) қылмыстық топ жасаған; 2) ауыр зардаптарға әкеп соққан, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан бес жылға дейінгі мерзімге айыра отырып немесе онсыз үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.»
212 бап. Құқыққа қайшы мақсаттарды көздейтін интернет-ресурстарды орналастыру үшін қызметтер көрсету	«1. Ашық ақпараттық-коммуникациялық желіде жұмыс істейтін аппараттық-бағдарламалық кешендерді құқыққа қарсы мақсаттарды көздейтін интернет-ресурстарды орналастыру үшін ұсыну бойынша көрінеу құқыққа қайшы қызметтер көрсету, – екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады. 2. Адамдар тобының алдын ала сөз байласуы бойынша немесе қылмыстық топ жасаған дәл сол әрекет, – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып, үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады.»
213 бап. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын,	«1. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын өзгерту, егер бұл әрекеттер өндірушінің немесе заңды иесінің келісімінсіз жасалса,

абоненттің сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды жасау, пайдалану, тарату	ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасау, – бір жүз алпыс айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір жүз алпыс сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не қырық тәулікке дейінгі мерзімге қамаққа алуға жазаланады. 2. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын өзгертуге немесе ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасауға мүмкіндік беретін бағдарламаларды құқыққа сыйымсыз жасау, пайдалану, тарату, – екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады. 3. Осы баптың бірінші немесе екінші бөліктерінде көзделген, қылмыстық топ жасаған іс-әрекеттер - бес жылға дейін мерзімге бас бостандығынан айыруға жазаланады».

Оқу басылымы

ШЕГЕТАЕВА АЙЖАН КАЙРГЕЛЬДИЕВНА,
МУРЫХ ЕЛЕНА ЛЬВОВНА,
МОЛДАВАНОВА ИННА ГРИГОРЬЕВНА

АҚПАРАТ ҚАУІПСІЗДІГІ МЕН ҚОРҒАУДЫ ҚҰҚЫҚТЫҚ ЖӘНЕ АҚПАРАТТЫҚ ҚАМТАМАСЫЗ ЕТУ

Редакторы Жақыпханова Г.Қ.

Басуға қол қойылды 13.10.2020ж. Пішімі 60×90/16
Есептік баспа табағы 5,2. Таралымы 100 дана. Тапсырыс 251.
ҚарТУ баспасы. 100027, Қарағанды, Н.Назарбаев даңғылы, 60.