«Алматы» ӘКК» АҚ
Басқармасының шешімімен
БЕКІТІЛДІ
2023 жылғы _____ «__»_____
№_____ хаттама

«АЛМАТЫ» ӘКК» АҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Иесі	**Қауіпсіздік қызметі**
Әзірлеуші	**Қауіпсіздік қызметі**
Дананы сақтауға жауапты	**Стратегия және корпоративтік даму департаменті**
Түпнұсқаны қағаз және электрондық тасығышта сақтау орны	**ІНҚ базасы**
Мониторинг және өзектендіру үшін жауапты	**Қауіпсіздік қызметі Ақпараттық технологиялар департаменті**
Жаңасының қабылдануына байланысты күші жойылған ІНҚ туралы мәліметтер	**Жоқ**
Келіспеушілік хаттамасы	**Жоқ**
Қосымшалар мен беттер саны	**Қосымшалар жоқ, 19 беттен тұратын саясат**

Алматы қаласы
2023 жыл

МАЗМҰНЫ:

1-тарау. Жалпы ережелер

1.1. Осы құжат – «Алматы» ӘКК» АҚ ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «Алматы» ӘКК» АҚ (бұдан әрі – Қоғам) жүйелері мен ақпараттық активтеріне тән және маңызды қатерлер болған жағдайда ақпараттық қауіпсіздікті қамтамасыз етудің басымдықтары мен қағидаттарын айқындайтын құжат болып табылады.

1.2. Осы Саясат Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасына, ISO/IEC 27000, COBIT, ITIL ақпараттық қауіпсіздік жөніндегі халықаралық стандарттар сериясына, Қоғамның ақпараттық инфрақұрылымын дамытудың қазіргі жай-күйі мен таяудағы перспективаларына, сондай-ақ ақпаратты қорғаудың қазіргі заманғы ұйымдастырушылық-техникалық әдістерінің мүмкіндіктеріне сәйкес әзірленді.

1.3. Саясат ақпараттың қауіпсіздігін қамтамасыз ету туралы көзқарастар жүйесін анықтайды және ақпараттық қауіпсіздік саласындағы қорғау мақсаттары мен міндеттерін, ережелерді, рәсімдерді, практикалық әдістер мен нұсқаулықтарды, сондай-ақ Қоғамдағы ақпараттың қауіпсіздігін қамтамасыз етудің негізгі қағидаттарын, ұйымдастырушылық, технологиялық және рәсімдік аспектілерін жүйелі түрде баяндайды.

1.4. Саясат Қоғамдағы ақпараттық технологияларды дамытудың қазіргі жағдайы мен таяудағы перспективаларын, оларды пайдаланудың мақсаттарын, міндеттері мен құқықтық негіздерін, жұмыс істеу режимдерін ескереді, сондай-ақ Қоғамның ақпараттық қатынастарының объектілері мен субъектілері үшін қауіпсіздікке төнетін қатерлерді талдауды қамтиды.

1.5. Саясат Қоғам иесі және пайдаланушысы болып табылатын барлық ақпараттық жүйелер мен құжаттарды қамтиды. Ақпараттық қауіпсіздікті қамтамасыз ету – Қоғам қызметін табысты жүзеге асыру үшін қажетті шарт. Ақпарат Қоғамның маңызды активтерінің бірі болып табылады.

1.6. Саясат мыналар үшін әдіснамалық негіз болып табылады:

- Қоғамда ақпараттық қауіпсіздікті қамтамасыз ету саласында бірыңғай саясатты қалыптастыру және жүргізу;
- ақпараттық қауіпсіздік саясатын іске асыру бойынша басқарушылық шешімдер қабылдау және практикалық шаралар әзірлеу және ақпарат қауіпсіздігіне төнетін түрлі қатерлерді іске асыру салдарын анықтауға, көрсетуге және жоюға бағытталған келісілген шаралар кешенін әзірлеу;
- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды сақтай отырып, ақпараттық технологияларды құру, дамыту және пайдалану жөніндегі жұмыстарды жүргізу кезінде Қоғамның құрылымдық бөлімшелерінің қызметін үйлестіру;
- Қоғамдағы ақпараттық қауіпсіздікті құқықтық, нормативтік, техникалық және ұйымдастырушылық қамтамасыз етуді жетілдіру бойынша ұсыныстар әзірлеу.

1.7. Бұл саясатты Қоғамның ақпараттық қауіпсіздігінің кешенді жүйесін құру үшін негіз ретінде пайдалану оны құру шығындарын оңтайландыруға мүмкіндік береді.

1.8. Саясатты әзірлеу кезінде ақпараттың қауіпсіздігін қамтамасыз етудің кешенді жүйелерін құрудың негізгі қағидаттары, ұйымдастырушылық-техникалық

әдістердің сипаттамалары мен мүмкіндіктері және ақпараттың қауіпсіздігіне төнетін қауіп-қатерлерге қарсы тұрудың заманауи аппараттық-бағдарламалық құралдары ескерілді.

1.9. Саясаттың негізгі ережелері ақпараттық қауіпсіздік мәселелерін сапалы түсінуге негізделген және тәуекелдерді экономикалық (сандық) талдау және ақпаратты қорғауға қажетті шығындарды негіздеу мәселелерін қозғамайды.

1.10. Саясаттың ережелерін Қоғамның барлық қызметкерлері орындауға міндетті. Саясат талаптары Қоғамның ақпараттық ресурстары мәселелерімен байланысты басқа ұйымдар мен мекемелерге де қолданылады.

2-тарау. Қоғамның ақпараттық қауіпсіздік жүйесін құру қағидаттары

Қоғам ақпаратының қауіпсіздігін қамтамасыз ету жүйесін құру және оның жұмыс істеуі мынадай негізгі қағидаттарға сәйкес жүзеге асырылуы тиіс:

2.1. Заңдылық.

Ақпарат, ақпараттандыру және ақпаратты қорғау саласындағы қолданыстағы заңнамаға, сондай-ақ ақпаратпен жұмыс істеу кезінде құқық бұзушылықтарды анықтау мен жолын кесудің барлық рұқсат етілген әдістерін қолдана отырып, өз құзыреті шегінде мемлекеттік билік және басқару органдары бекіткен ақпарат қауіпсіздігі жөніндегі басқа да нормативтік актілерге сәйкес қорғау іс-шараларын жүзеге асыруды және Қоғамның ақпараттық қауіпсіздік жүйесін әзірлеуді көздейді.

Қоғамның ақпараттық жүйесінің барлық пайдаланушылары ақпарат саласындағы құқық бұзушылықтар үшін жауапкершілік туралы түсінікке ие болуы тиіс.

Бұл қағидатты іске асыру Қоғамның аты мен беделін қорғау үшін қажет.

2.2. Жүйелілік.

Қоғамдағы ақпаратты қорғау жүйесін құруға жүйелі көзқарас Қоғамның ақпараттық қауіпсіздігін қамтамасыз ету мәселесін түсіну және шешу үшін маңызды барлық өзара байланысты, өзара әрекеттесетін және уақыт бойынша өзгеретін элементтерді, жағдайлар мен факторларды ескеруді қамтиды.

Қорғау жүйесін құру кезінде Қоғамның ақпараттық жүйесінің барлық әлсіз және неғұрлым осал тұстары, сондай-ақ бұзушылар (әсіресе, жоғары білікті зиянкестер) тарапынан оған шабуылдардың сипаты, ықтимал объектілері мен бағыттары, таратылған жүйелерге ену жолдары және ақпаратқа рұқсатсыз қол жеткізу ескерілуге тиіс. Қорғаныс жүйесі ақпаратқа енудің және рұқсатсыз қол жеткізудің барлық белгілі арналарын ғана емес, сонымен қатар қауіпсіздік қатерлерін іске асырудың түбегейлі жаңа жолдарының пайда болу мүмкіндігін ескере отырып құрылуы керек.

2.3. Кешенділік.

Компьютерлік жүйелерді қорғаудың әдістері мен құралдарын кешенді пайдалану қауіптерді іске асырудың барлық елеулі (маңызды) арналарын жабатын және оның жекелеген құрамдастарының түйіскен жерлерінде әлсіз жерлері жоқ тұтас қорғаныс жүйесін құру кезінде гетерогенді құралдарды келісілген қолдануды қамтиды. Қорғаныс эшелондалған түрде салынуы тиіс. Сыртқы қорғаныс физикалық құралдармен, ұйымдастырушылық және құқықтық шаралармен қамтамасыз етілуі керек.

2.4. Үздіксіздік.

Ақпараттық қауіпсіздікті қамтамасыз ету – Қоғам басшылығы, ақпаратты қорғау бөлімшелері және барлық деңгейдегі қызметкерлер жүзеге асыратын процесс. Бұл – Қоғам ішіндегі барлық деңгейлерде үнемі жүруі тиіс процесс және Қоғамның әрбір қызметкері осы процеске қатысуы керек . Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызмет Қоғамның күнделікті қызметінің құрамдас бөлігі болып табылады. Оның тиімділігі Қоғамның барлық қызметкерлерінің ақпараттық қауіпсіздікті қамтамасыз етуге қатысуына байланысты.

Бұған қоса, физикалық және техникалық қорғаныс құралдарының көпшілігі өз функцияларын тиімді орындау үшін үнемі ұйымдастырушылық (әкімшілік) қолдауды қажет етеді (атауларды, құпия сөздерді, шифрлау кілттерін дұрыс сақтау мен қолдануды уақтылы өзгерту және қамтамасыз ету, өкілеттіктерді қайта анықтау және т.б.). Қорғаныс құралдарының жұмысындағы үзілістерді зиянкестер қолданылатын қорғаныс әдістері мен құралдарын талдау үшін, арнайы бағдарламалық және аппараттық «бетбелгілерді» және қорғауды жеңудің басқа құралдарын енгізу үшін пайдалана алады.

2.5. Уақытылық.

Ақпараттық қауіпсіздікті қамтамасыз ету шараларының алдын алу сипатын, яғни ақпаратты кешенді қорғау жөніндегі міндеттерді қоюды және тұтастай алғанда ақпараттық жүйелерді және олардың ақпаратты қорғау жүйелерін, атап айтқанда, әзірлеудің бастапқы кезеңдерінде ақпарат қауіпсіздігін қамтамасыз ету шараларын іске асыруды көздейді.

Қорғау жүйесін әзірлеу ең қорғалатын ақпараттық жүйені әзірлеумен және дамытумен қатар жүргізілуі тиіс. Бұл жобалау кезінде қауіпсіздік талаптарын ескеруге және, сайып келгенде, жеткілікті қауіпсіздік деңгейіне ие тиімдірек (ресурстардың шығындары бойынша да, төзімділік бойынша да) жүйелерді құруға мүмкіндік береді.

2.6. Жетілдірудің сабақтастығы мен үздіксіздігі.

Ақпаратты ұстау әдістері мен құралдарындағы өзгерістерді, қорғау жөніндегі нормативтік талаптарды, осы саладағы отандық және шетелдік тәжірибені ескере отырып, ұйымдастырушылық және техникалық шешімдердің сабақтастығы, кадрлық құрам, Қоғамның ақпараттық жүйесінің және оны қорғау жүйесінің жұмыс істеуін талдау негізінде ақпаратты қорғау шаралары мен құралдарын ұдайы жетілдіруді көздейді.

2.7. Ақылға қонымды жеткіліктілік (экономикалық орындылық).

Ақпараттық ресурстардың қауіпсіздігін қамтамасыз етуге арналған шығындар деңгейінің және олардың жария етілуінен, жоғалуынан, таралуынан, жойылуынан және бұрмалануынан болатын залалдың шамасына сәйкестігін көздейді.

2.8. Дербес жауапкершілік.

Ақпараттық қауіпсіздікті және оны өңдеу жүйесін қамтамасыз ету үшін жауапкершілікті оның өкілеттігі шегінде әрбір қызметкерге жүктеуді көздейді. Осы қағидатқа сәйкес қызметкерлердің құқықтары мен міндеттерін бөлу кез-келген бұзушылық болған жағдайда кінәлілер шеңбері нақты белгілі немесе минимумға дейін төмендетілетіндей етіп құрылады.

2.9. Өкілеттіктерді азайту.

Бұл пайдаланушыларға қызметтік қажеттілікке сәйкес қолжетімділіктің минималды құқықтарын беруді білдіреді. Ақпаратқа қол жеткізу қызметкерге өзінің лауазымдық міндеттерін орындау үшін қажет болған жағдайда және көлемде ғана берілуі керек.

2.10. Мүдделер қақтығысын жою.

Ақпараттық қауіпсіздікті қамтамасыз етудің тиімді жүйесі қызметкерлердің міндеттерін нақты бөлуді және қызметкерлердің жауапкершілік саласы мүдделер қақтығысына жол беретін жағдайларды жоюды қамтиды. Ықтимал қақтығыстардың салалары анықталуы, азайтылуы және қатаң тәуелсіз бақылауда болуы керек. Бұл қағиданы іске асыру бірде-бір қызметкердің сыни операцияларды жеке-жеке жүзеге асыруға мүмкіндік беретін өкілеттіктері болмауы керек деп болжайды. Қызметкерлерге мүдделер қақтығысын тудыратын өкілеттіктер беру оған өзімшілдік мақсатта немесе проблемаларды немесе шығындарды жасыру үшін ақпаратты бұрмалауға мүмкіндік береді. Ақпаратты манипуляциялау және ұрлау қаупін азайту үшін мұндай өкілеттіктер мүмкіндігінше Қоғамның әр түрлі қызметкерлері немесе бөлімшелері арасында бөлінуі керек.

2.11. Өзара іс-қимыл және ынтымақтастық.

Қоғамның құрылымдық бөлімшелерінде қолайлы атмосфера құруды көздейді. Мұндай жағдайда қызметкерлер белгіленген ережелерді саналы түрде сақтауға және ақпаратты қорғау бөлімшелерінің қызметіне жәрдемдесуі тиіс.

Қоғамдағы ақпараттық қауіпсіздікті қамтамасыз етудің тиімді жүйесінің маңызды элементі ақпаратпен жұмыс істеудің жоғары мәдениеті болып табылады. Қоғам басшылығы кәсіби қызметтің этикалық нормалары мен стандарттарын қатаң сақтауға, барлық деңгейдегі қызметкерлерге қоғамның ақпараттық қауіпсіздігін қамтамасыз етудің маңыздылығын көрсететін және көрсететін корпоративтік мәдениетті құруға жауапты. Қоғамның барлық қызметкерлері ақпараттық қауіпсіздікті қамтамасыз ету үдерісіндегі өз рөлін түсініп, осы үдеріске қатысуы тиіс.

2.12. Қорғаныс жүйесінің икемділігі.

Ақпараттық қауіпсіздікті қамтамасыз ету жүйесі сыртқы ортаның өзгеруіне және Қоғамның өз қызметін жүзеге асыру жағдайларына жауап бере алуы керек. Мұндай өзгерістерге мыналар жатады:

- ақпараттық қауіпсіздік саласындағы қатынастарды реттейтін заңнамадағы өзгерістер;
- Қоғамның ұйымдық және штаттық құрылымындағы өзгерістер;
- корпоративтік қайта құрылымдау, кеңейту, бірігу және бірігу;
- қолданыстағы ақпараттық жүйелерді өзгерту немесе түбегейлі жаңа ақпараттық жүйелерді енгізу;
- жаңа техникалық құралдар;
- жаңа қызмет түрлері, жаңа қызметтер, өнімдер.

Икемділік қасиеті мұндай жағдайларда ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің экономикалық тиімділігін қамтамасыз ететін қорғаныс құралдары мен әдістерін жаңаларына толығымен ауыстыру бойынша түбегейлі шаралар қабылдау қажеттілігін жояды.

2.13. Мамандану және кәсібилік.

Әкімшілік шараларды іске асыруды және қорғау құралдарын пайдалануды қоғамның кәсіби даярланған мамандары (ақпаратты қорғау саласында арнайы бейіндік білімі бар қоғамның қызметкері) жүзеге асыруы тиіс. Ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету жөніндегі қызметтің нақты түріне неғұрлым дайындалған және практикалық жұмыс тәжірибесі бар мамандандырылған ұйымдардың немесе мамандардың ақпаратты қорғау шараларын әзірлеуге және іске асыруға тартуға жол беріледі.

2.14. Қызметкерлер үшін алғашқы қорғаныс әдістерінің қарапайымдылығы.

Қорғаудың алғашқы әдістерінің тетіктері мен әдістері түсінікті және қолдануға оңай болуы керек. Қорғаудың бастапқы құралдары мен әдістерін қолдану арнайы тілдерді білумен немесе тіркелген пайдаланушылардың қалыпты жұмысы кезінде айтарлықтай қосымша еңбек шығындарын талап ететін әрекеттерді орындаумен байланысты болмауы керек, сондай-ақ пайдаланушыдан өзіне түсініксіз күнделікті операцияларды орындауды талап етпеуі керек.

2.15. Міндетті бақылау.

Пайдаланылатын жүйелер мен ақпаратты қорғау құралдары негізінде ақпараттың қауіпсіздігін қамтамасыз етудің белгіленген ережелерін бұзу әрекеттерін анықтау мен жолын кесудің міндеттілігі мен уақтылылығын көздейді.

Кез келген пайдаланушының, әрбір қорғау құралының және кез келген қорғау объектісіне қатысты қызметін бақылау жедел бақылау және тіркеу құралдарын қолдану негізінде жүзеге асырылуы тиіс және пайдаланушылардың рұқсатсыз да, санкцияланған да әрекеттерін қамтуы керек. Бұдан басқа, ақпараттық қауіпсіздікті қамтамасыз етудің тиімді жүйесі белгіленген нормативтік талаптардың сақталуы туралы ақпарат пен мәліметтердің қозғалысына байланысты процестердің ағымдағы жай-күйі туралы барабар және жан-жақты ақпараттың, сондай-ақ шешім қабылдауға қатысы бар қосымша ақпараттың болуын талап етеді. Ақпарат сенімді, уақтылы, қолжетімді және дұрыс ресімделген болуы керек.

Қоғам қызметкерлері немесе қауіпсіздікті қамтамасыз ету бөлімшелері анықтаған ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің кемшіліктері дереу тиісті деңгейдегі басшылардың назарына жеткізілуі және жедел жойылуы тиіс. Елеулі кемшіліктер туралы Қоғам басшылығына хабарлау қажет. Басшылыққа тоқсан сайын ақпараттық қауіпсіздікті қамтамасыз ету жүйесі анықтаған барлық проблемаларды қорытындылайтын есептер жіберіледі. Ақпараттық қауіпсіздікке жауапты бөлімше тоқсан сайын есепті кезеңнен кейін күнтізбелік 20 күннен кешіктірмей Қоғам басшылығына ақпараттық қауіпсіздікті қамтамасыз ету жүйесі анықтаған барлық проблемаларды қорытындылайтын есептер жібереді.

3-тарау. Ақпараттық қатынастар субъектілері және қорғау объектілері

3.1. Қоғамның ақпараттық қауіпсіздігін қамтамасыз ету кезіндегі ақпараттық қатынастардың субъектілері:

- ақпараттық ресурстардың иесі ретінде Қоғам;
- ақпараттық алмасуға қатысатын Қоғамның бөлімшелері;

- оларға жүктелген функцияларға сәйкес Қоғамның құрылымдық бөлімшелерінің басшылығы мен қызметкерлері;
- Қоғамның контрагенттері – олар туралы мәліметтер Қоғамның ақпараттық жүйесінде жинақталатын, сақталатын және өңделетін заңды және жеке тұлғалар;
- Қоғамның өз функцияларын орындауын қамтамасыз етуге тартылған басқа заңды және жеке тұлғалар (консультанттар, әзірлеушілер, қызмет көрсетуші персонал, қызмет көрсету үшін тартылатын ұйымдар және т.б.) болып табылады.

3.2. Ақпараттық қатынастардың аталған субъектілері мыналарды қамтамасыз етуге мүдделі:

- қажетті ақпаратқа (оның қолжетімділігіне) уақтылы қол жеткізу;
- ақпараттың сенімділігі (толықтығы, дәлдігі, барабарлығы, тұтастығы);
- ақпараттың белгілі бір бөлігінің құпиялылығы (құпияда сақталуы);
- оларға жалған (дұрыс емес, бұрмаланған) ақпаратты таңудан қорғау;
- ақпаратпен жұмыс істеудің белгіленген ережелерін бұзғаны үшін жауапкершіліктің аражігін ажырату;
- ақпаратты өңдеу және беру процестерін үздіксіз бақылау мен басқаруды жүзеге асыру мүмкіндіктері;
- ақпаратты заңсыз көшіруден қорғау (авторлық құқықтарды, ақпарат иесінің құқықтарын қорғау және т.б.).

3.3. Қоғамда таралуы шектеулі мәліметтерді (қызметтік, коммерциялық, дербес деректер) және қорғау объектілері болып табылатын ашық мәліметтерді қамтитын құпиялылықтың әр түрлі деңгейлеріндегі ақпарат таралады. Қоғамның ақпараттық ортасында ұсынылуына және орналасуына қарамастан, Қоғамның барлық ақпараты мен ақпараттық ресурстары қорғалуы тиіс:

1) оларды ұсыну нысаны мен түріне қарамастан, Қоғамның жұмысы үшін қажетті ақпараттық активтер;
2) ақпараттық технологияларды, ақпаратты қалыптастыру, өңдеу, беру, сақтау (оның ішінде мұрағатталған) және пайдаланудың техникалық және бағдарламалық құралдарын қоса алғанда, ақпараттық жүйелер,
3) компьютерлік техниканы, кітапханаларды, архивтерді, деректер қорын, серверді қоса алғанда, АТ-инфрақұрылымының элементтері, оның ішінде физикалық және виртуалды, ақпарат алмасу және телекоммуникация арналары, ақпаратты қорғау жүйелері мен құралдары, Қоғамның АТ-инфрақұрылымының қорғалатын элементтері орналасқан объектілер мен үй-жайлар;
4) Қоғамдағы ақпаратты өңдеу процестері, регламенттері мен рәсімдері;
5) Қазақстан Республикасының заңнамасына сәйкес ақпарат меншік иесі қол жеткізуі шектелген коммерциялық құпияны құрайтын мәліметтер;
6) Қоғам қызметкерлері мен контрагенттерінің дербес деректері;
7) Қоғамның қалыпты жұмыс істеуін қамтамасыз ету үшін қажетті ашық ақпарат.

3.4. Негізгі қорғаныс объектілерінің құрылымы, құрамы және орналасуы

Қоғамның ақпараттық ортасының негізгі ерекшеліктеріне мыналар жатады:

- ақпаратты өңдеу мен берудің көптеген техникалық құралдарын бірыңғай жүйеге біріктіру;
- ақпаратты өңдеудің автоматтандырылған жүйелерін пайдалану аясының едәуір кеңеюі, Қоғамда ақпараттық-басқару жүйелерінің алуан түрлілігі және кеңінен таралуы;
- шешілетін міндеттер мен өңделетін деректер түрлерінің алуан түрлілігі, әр түрлі пайдаланушылардың ақпараттық сұраныстарын орындаудың кең үйлесімімен ақпаратты автоматтандырылған өңдеудің күрделі режимдері;
- әр түрлі мақсаттағы, тиесілілiктегі және құпиялылық деңгейлеріндегі ақпараттың бірыңғай деректер қорында біріктіру;
- «сыртқы әлеммен» (ақпарат көздерімен және тұтынушылармен) өзара іс-қимылдың көптеген ақпараттық арналарының болуы;
- Қоғамның ақпараттық жүйесінің үздіксіз жұмыс істеуін қамтамасыз ету қажеттілігі;
- ақпараттық ағындардың жоғары қарқындылығы.

Мұндай жағдайларда ақпараттың осалдығы күрт артады және Қоғамның ақпараттық ортасының маңызды элементтерінің бірі корпоративтік ақпараттық жүйе болып табылады, онда әр түрлі пайдаланушылар бөлісетін ақпараттың едәуір көлемі өңделеді және жинақталады.

4-тарау. Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен міндеттері

4.1. Қорғау мақсаттары.

Осы Саясаттың ережелеріне қол жеткізуге бағытталған негізгі мақсат Қоғамның ақпараттық қатынастары субъектілерін ақпаратқа, оны тасымалдаушыларға, өңдеу және беру процестеріне кездейсоқ немесе қасақана әсер ету арқылы оларға материалдық, моральдық немесе өзге де залал келтіруден қорғау, сондай-ақ операциялық және басқа да тәуекелдер деңгейін (Қоғамның іскерлік беделіне нұқсан келтіру тәуекелі, құқықтық тәуекел және т.б.) барынша азайту болып табылады.

Аталған мақсатқа ақпараттың мынадай қасиеттерін қамтамасыз ету және тұрақты ұстап тұру арқылы қол жеткізіледі:

- заңды пайдаланушылар үшін ақпараттың қолжетімділігі (пайдаланушылар қажетті ақпаратты және олар үшін қолайлы уақыт ішінде міндеттерді шешу нәтижелерін алуға мүмкіндігі бар Қоғамның ақпараттық жүйесінің тұрақты жұмыс істеуі);
- Қоғамның ақпараттық жүйесінде сақталатын және өңделетін және байланыс арналары арқылы берілетін ақпараттың тұтастығы мен түпнұсқалығы (авторлығын растау);
- құпиялылық – сақталған, өңделетін және байланыс арналары арқылы берілетін ақпараттың белгілі бір бөлігін құпия сақтау;

Ақпараттың қолжетімділігінің, тұтастығының және құпиялылығының қажетті деңгейі ақпараттық қауіпсіздікке төнетін қатерлер деңгейіне сәйкес келетін әдістермен және құралдармен қамтамасыз етіледі.

4.2. Ақпараттың көрсетілген қасиеттерін қорғау мен қамтамасыз етудің негізгі мақсатына қол жеткізу үшін қоғамның ақпараттық қауіпсіздігін қамтамасыз ету жүйесі мынадай міндеттерді тиімді шешуді қамтамасыз етуі тиіс:

1) ақпараттық қауіпсіздікке қатер көздерін, мүдделі ақпараттық қатынастар субъектілеріне залал келтіруге, қоғамның ақпараттық жүйесінің қалыпты жұмыс істеуін бұзуға ықпал ететін себептер мен жағдайларды уақтылы анықтау, бағалау және болжау;

2) Қоғам активтерінің осалдығын уақтылы анықтау және жою және сол арқылы бизнес-процестердің қалыпты жұмыс істеуіне нұқсан келтіру және бұзылу мүмкіндігінің алдын алу;

3) ақпараттық қауіпсіздікті қамтамасыз етудің негізгі талаптары мен рәсімдерін айқындау және құжаттау;

4) ақпарат қауіпсіздігінің қатерлеріне және теріс үрдістерге жедел ден қою тетігін құру;

5) жеке және заңды тұлғалардың заңсыз әрекеттерімен келтірілген залалды барынша азайту және оқшаулау үшін жағдайлар жасау, теріс ықпалды әлсірету және ақпараттық қауіпсіздікті бұзу салдарын жою;

6) бөгде адамдар қоғамының ақпараттық жүйесінің жұмыс істеу процесіне араласудан қорғау (ақпараттық ресурстарға қол жеткізуді белгіленген тәртіппен тіркелген пайдаланушылар ғана иеленуі тиіс);

7) пайдаланушылардың Қоғамның ақпараттық, аппараттық, бағдарламалық және өзге де ресурстарына қол жеткізуінің аражігін ажырату (тек сол ресурстарға қол жеткізу және олармен қызметтік міндеттерін орындау үшін нақты пайдаланушыларға қажет операцияларды ғана орындау мүмкіндігі), яғни рұқсатсыз кіруден қорғау;

8) ақпарат алмасуға қатысатын пайдаланушылардың аутентификациясын қамтамасыз ету (ақпарат жіберуші мен алушының түпнұсқалығын растау);

9) Қоғамның корпоративтік ақпараттық жүйесінде пайдаланылатын бағдарламалық құралдарды санкцияланбаған түрлендіруден қорғау, сондай-ақ жүйені компьютерлік вирустарды қоса алғанда, санкцияланбаған бағдарламаларды енгізуден қорғау;

10) шектеулі пайдаланудағы ақпаратты оны өңдеу, сақтау және байланыс арналары арқылы беру кезінде техникалық арналар бойынша таралудан қорғау;

11) ақпаратты қорғаудың криптографиялық құралдарының өміршеңдігін қамтамасыз ету;

12) қоғамның ақпараттық қауіпсіздігін қамтамасыз етуге арналған шығындарды жоспарлау және оңтайландыру.

4.3. Қорғаныс жүйесінің міндеттерін шешудің негізгі жолдары.

Қорғаудың негізгі мақсаттары мен жоғарыда аталған міндеттерді шешуге мыналар арқылы қол жеткізіледі:

- Қоғамның ақпараттық жүйесінің барлық қорғалатын ресурстарын (ақпарат, міндеттер, құжаттар, байланыс арналары, серверлер, автоматтандырылған жұмыс орындары) қатаң есепке алу;
- корпоративтік ақпараттық жүйенің бағдарламалық және техникалық құралдарына қызмет көрсетуді және модификациялауды жүзеге асыратын персоналдың іс-қимылдарын журналдау;
- ақпараттың қауіпсіздігін қамтамасыз ету мәселелері бойынша Қоғамның ұйымдастырушылық-өкімдік құжаттарының талаптарының толықтығы, нақты орындылығы және дәйектілігі;
- ақпараттың қауіпсіздігін және оны өңдеу процестерін қамтамасыз ету жөніндегі практикалық іс-шараларды ұйымдастыруға және жүзеге асыруға жауапты қызметкерлерді даярлау (оқыту);
- әрбір пайдаланушыға өзінің функционалдық міндеттерін орындау үшін Қоғамның ақпараттық ресурстарына қол жеткізу бойынша ең аз қажетті өкілеттіктер беру;
- Қоғамның ақпараттық жүйесінің барлық пайдаланушыларының ақпарат қауіпсіздігін қамтамасыз ету мәселелері бойынша ұйымдастырушылық-өкімдік құжаттардың талаптарын нақты білуі және қатаң сақтауы;
- Қоғамның ақпараттық ресурстарына қол жеткізе алатын өзінің функционалдық міндеттері шеңберінде әрбір қызметкердің өз іс-әрекеттері үшін дербес жауапкершілік;
- Қоғамның ақпараттық ортасы элементтерінің қорғалуының қажетті деңгейін үздіксіз ұстап тұру, ақпараттық қауіпсіздікке төнетін қатерлерді іске асыру кезінде ықтимал залалды жою, оның ішінде ықтимал үзілістерден кейін бизнес-процестерді қалпына келтіру уақытын қысқарту;
- жүйенің ресурстарын қорғаудың физикалық және техникалық (бағдарламалық-аппараттық) құралдарын қолдану және оларды пайдалануды үздіксіз әкімшілік қолдау;
- ақпараттық қауіпсіздік оқиғалары мен инциденттеріне мониторинг жүргізу және өңдеу;
- Қоғамның ақпараттық ресурстарын пайдаланушылардың ақпарат қауіпсіздігін қамтамасыз ету жөніндегі талаптарды сақтауын тиімді бақылау;
- оның бөлімшелерінің сыртқы ұйымдармен өзара іс-қимылы кезінде (ақпарат алмасуға байланысты) осы ұйымдар тарапынан да, қызмет көрсетуші персонал мен үшінші тұлғалардың рұқсатсыз іс-әрекеттерінен де құқыққа қайшы іс-әрекеттерден Қоғам мүдделерін құқықтық қорғау.

5-тарау. Қоғам ақпаратының қауіпсіздігіне төнетін негізгі қатерлер

5.1. Ақпараттың қауіпсіздігіне төнетін қатерлер және олардың көздері.

Ақпараттың пайда болу табиғаты бойынша қауіпсіздігіне төнетін көптеген ықтимал қауіптер екі сыныпқа бөлінеді: табиғи (объективті) және жасанды (субъективті).

Табиғи қатерлер – ақпараттық жүйеге және оның құрамдастарына техногендік сипаттағы объективті физикалық процестердің немесе адамға тәуелсіз табиғи құбылыстардың әсерінен туындаған қауіптер;

Жасанды қатерлер – адам әрекетінен туындаған қауіптер. Олардың ішінде іс-әрекеттің ынтасына сүйене отырып, мыналарды бөліп көрсетуге болады:

- ақпараттық жүйені және оның элементтерін жобалаудағы қателіктерден, персоналдың іс-әрекетіндегі қателіктерден және т.б. туындаған қасақана емес (байқаусызда, кездейсоқ) қатерлер;
- адамдардың (шабуылдаушылардың) өзімшілдік, идеялық немесе өзге де ұмтылыстарымен байланысты әдейі (қасақана) қатерлер.

Ақпараттық жүйенің өзіне қауіп төндіретін көздер сыртқы және ішкі болуы мүмкін.

5.2. Қоғам ақпаратының қауіпсіздігіне аса маңызды қатерлер (ақпараттық қатынастар субъектілеріне залал келтіру тәсілдері):

- Қоғамның ақпараттық жүйесі құрамдастарының функционалдығын бұзу, ақпаратты бұғаттау, технологиялық процестерді бұзу, міндеттерді уақтылы шешуді бұзу;
- Қоғамның ақпараттық, бағдарламалық және басқа ресурстарының тұтастығын бұзу (бұрмалау, ауыстыру, жою), сондай-ақ құжаттарды бұрмалау (қолдан жасау);
- қызметтік немесе коммерциялық құпияны құрайтын мәліметтердің, сондай-ақ дербес деректердің құпиялылығын бұзу (жария ету, жария ету) болып табылады.

5.3. Ақпарат қауіпсіздігіне абайсызда жасанды (субъективті) қатерлерді іске асыру жолдары.

Қоғамның ақпараттық жүйесін заңды пайдаланушылар ретінде тіркелген немесе оның құрамдастарына қызмет көрсететін Қоғам қызметкерлері кездейсоқ әсердің ішкі көздері болып табылады, өйткені олар ақпаратты өңдеу процестеріне тікелей қол жеткізе алады және қолданыстағы қағидаларды, нұсқаулықтар мен регламенттерді байқаусызда бұзушылықтар мен қателіктер жасай алады.

Қоғам ақпаратының қауіпсіздігіне абайсызда жасанды (субъективті) қатерлерді іске асырудың негізгі жолдары (адамдар кездейсоқ, білместен, немқұрайлылықпен немесе немқұрайлылықпен, қызығушылықпен, бірақ жаман ниетсіз жасаған іс-әрекеттер):

- Қоғамның ақпараттық жүйесі құрамдастарының функционалдығын ішінара немесе толық бұзуға немесе ақпараттық немесе бағдарламалық-техникалық ресурстардың бұзылуына әкеп соқтыратын байқаусызда жасалған әрекеттер;
- таралуы шектеулі ақпаратты жария етуге немесе оны көпшілікке жария етуге әкеп соғатын абайсыз әрекеттер;

- рұқсатты шектеу атрибуттарын (рұқсаттамалар, сәйкестендіру карталары, кілттер, құпия сөздер, шифрлау кілттері және т.б.) жария ету, беру немесе жоғалту;
- ақпараттық ресурстармен жұмыс істеу кезінде ұйымдастырушылық шектеулерді (белгіленген ережелерді) елемеу;
- жүйелерді, деректерді өңдеу технологияларын жобалау, Қоғамның ақпараттық жүйесінің жұмыс істеуі мен ақпарат қауіпсіздігіне қауіп төндіретін мүмкіндіктері бар бағдарламалық қамтамасыз етуді әзірлеу;
- деректер мен құжаттарды қате мекенжайға (құрылғыға) жіберу;
- қате деректерді енгізу;
- ақпарат тасығыштардың абайсызда бүлінуі;
- байланыс арналарының абайсызда зақымдануы;
- жабдықты заңсыз өшіру немесе құрылғылардың немесе бағдарламалардың жұмыс режимдерін өзгерту;
- компьютерлерді вирустармен жұқтыру;
- корпоративтік ақпараттық жүйе құрамдастарының жұмыс қабілеттілігін жоғалтуға әкеп соқтыратын немесе оларда қайтымсыз өзгерістерді жүзеге асыратын (ақпарат тасымалдағыштарды форматтау немесе қайта құрылымдау, деректерді жою және т.б.) технологиялық бағдарламаларды рұқсатсыз іске қосу;
- қорғаныс құралдарын қабілетсіз пайдалану, баптау немесе заңсыз өшіру.

5.4. Ақпарат қауіпсіздігіне қасақана жасанды (субъективті) қатерлерді іске асыру жолдары.

Жұмысты қасақана ұйымдастырмаудың, Қоғамның ақпараттық жүйесінің құрамдастарын істен шығарудың, жүйеге енудің және ақпаратқа рұқсатсыз қол жеткізудің негізгі мүмкін жолдары (өзімшіл мақсаттармен, мәжбүрлеу арқылы, кек алу ниетінен және т.б.):

- Қоғамның ақпараттық жүйесі құрамдастарының функционалдығын ішінара немесе толық бұзуға немесе ақпараттық немесе бағдарламалық-техникалық ресурстардың бұзылуына әкелетін қасақана әрекеттер;
- Қоғамның ақпараттық жүйесінің жұмыс істеуін ұйымсыздандыру, құжаттар мен ақпарат тасығыштарды ұрлау жөніндегі іс-әрекеттер;
- құжаттар мен ақпарат тасығыштарды рұқсатсыз көшіру, ақпаратты қасақана бұрмалау, дұрыс емес деректерді енгізу;
- ақпараттық жүйелердің (электрмен қоректендіру, салқындату және желдету, байланыс желілері мен аппаратурасы және т б.) жұмыс істеуін қамтамасыз етудің ішкі жүйелерін ажырату немесе істен шығару;
- байланыс арналары арқылы берілетін деректерді ұстап қалу;

- өндірістік қалдықтарды жымқыру (басып шығарылған құжаттар, жазбалар, ақпарат тасығыштар және т.б.);
- қол жеткізуді шектеу атрибуттарын заңсыз алу (агентуралық жолмен, пайдаланушылардың немқұрайлылығын пайдаланып, қолдан жасау, таңдау және т.б.);
- заңды пайдаланушылардың жұмыс станцияларынан корпоративтік ақпараттық жүйенің ресурстарына рұқсатсыз қол жеткізу;
- ақпаратты криптоқорғау шифрларын ұрлау немесе ашу;
- ақпараттық ресурстарға жасырын қол жеткізуді жүзеге асыру немесе Қоғамның корпоративтік ақпараттық жүйесі компоненттерінің жұмыс істеуін ұйымсыздандыру мақсатында аппараттық және бағдарламалық бетбелгілерді енгізу;
- үшінші тұлғалардың құқықтарын бұзатын жабдықты, бағдарламалық құралдарды немесе ақпараттық ресурстарды заңсыз пайдалану;
- ақпаратты рұқсатсыз түсіру үшін тыңдау құрылғыларын қолдану, қашықтықтан фото және бейне түсіру;
- құрылғылар мен байланыс желілерінің жанама электрмагниттік, акустикалық және басқа да сәулеленулерін, сондай-ақ ақпараттық алмасуға (қоректендіру желісіне) тікелей қатыспайтын техникалық құралдарға белсенді сәулелену көздерін ұстап қалу.

5.5. Ақпарат қауіпсіздігінің негізгі табиғи қатерлерін іске асыру жолдары:

- жабдықтардың ақпараттық жүйелердің және оның жұмыс істеуін қамтамасыз ететін жабдықтардың істен шығуы;
- істен шығу немесе байланыс желілерін пайдалану мүмкін еместігі;
- өрт, су тасқыны және басқа да табиғи апаттар.

5.6. Қоғамның ақпараттық қауіпсіздігін қамтамасыз ету жүйесі жүйеде бұзушылардың келесі мүмкін түрлері туралы болжамдарға сүйене отырып құрылуы керек (адамдардың санатын, уәждемесін, біліктілігін, арнайы құралдардың болуын және т.б. ескере отырып):

- біліксіз (ұқыпсыз) пайдаланушы – қателік, қабілетсіздік немесе немқұрайлылық бойынша зұлымдықсыз әрекет ете отырып және бұл ретте тек штаттық (берілген) құралды пайдалана отырып, тыйым салынған әрекеттерді орындауға, ақпараттық жүйенің қорғалатын ресурстарына өз өкілеттіктерін асыра пайдалана отырып қол жеткізуге, дұрыс емес деректерді енгізуге, ақпаратпен жұмыс істеу қағидалары мен регламенттерін бұзуға және т.б. әрекет жасай алатын Қоғамның (немесе Қоғамның ақпараттық жүйесін заңды пайдаланушы болып табылатын басқа ұйым бөлімшесінің) қызметкері;
- әуесқой – Қоғамның (немесе Қоғамның ақпараттық жүйесінің тіркелген пайдаланушысы болып табылатын басқа ұйым бөлімшесінің) пайдакорлық

мақсатсыз немесе зұлымдықсыз немесе өзін-өзі таныту үшін қорғаныс жүйесін бұзуға тырысатын қызметкері. Қорғаныс жүйесін еңсеру және тыйым салынған әрекеттерді орындау үшін ол ресурстарға қол жеткізудің қосымша өкілеттіктерін алудың әр түрлі әдістерін, қорғаныс жүйесін құрудағы кемшіліктерді және оған қолжетімді штаттық құралдарды (рұқсат етілген құралдарды пайдалану өкілеттігін асыра пайдалану арқылы рұқсат етілмеген әрекеттер) пайдалана алады. Бұдан басқа, ол қосымша стандартты емес аспаптық және технологиялық бағдарламалық қамтамасыз етуді, өздігінен жасалған бағдарламаларды немесе стандартты қосымша техникалық құралдарды қолдануға тырысуы мүмкін;

- ішкі қаскүнем – пайдақорлық мүдделерден немесе реніш үшін кек алу үшін мақсатты түрде, мүмкін, Қоғамның қызметкері болып табылмайтын адамдармен келісе отырып әрекет ететін Қоғамның (немесе жүйенің пайдаланушысы ретінде тіркелген басқа ведомство бөлімшесінің) қызметкері. Ол агентуралық әдістерді, пассивті құралдарды (техникалық ұстау құралдары), белсенді әсер ету әдістері мен құралдарын (техникалық құралдарды өзгерту, деректер арналарына қосылу, бағдарламалық бетбелгілерді енгізу және арнайы аспаптық және технологиялық бағдарламаларды пайдалану) қоса алғанда, қорғаныс жүйесін бұзудың барлық әдістері мен құралдарын, сондай-ақ Қоғамның ішінен де, одан тыс та әсерлердің комбинацияларын пайдалана алады;
- сыртқы қаскүнем – пайдақорлық, кек алу немесе қызығушылық үшін мақсатты түрде, мүмкін басқа адамдармен келісе отырып, әрекет ететін әрекет ететін бөгде адам. Ол агентуралық әдістерді, пассивті құралдарды (техникалық ұстау құралдары), белсенді әсер ету әдістері мен құралдарын (техникалық құралдарды өзгерту, деректер арналарына қосылу, бағдарламалық бетбелгілерді енгізу және арнайы аспаптық және технологиялық бағдарламаларды пайдалану) қоса алғанда, қорғаныс жүйесін бұзудың барлық әдістері мен құралдарын, сондай-ақ Қоғамның ішінен де, одан тыс та әсерлердің комбинацияларын пайдалана алады.

6-тарау. Ақпараттық ресурстардың қорғалуының талап етілетін деңгейін қамтамасыз ету шаралары, әдістері мен құралдары

6.1. Қоғамның ақпараттық жүйесінің қауіпсіздігін қамтамасыз етудің барлық шаралары мыналарға бөлінеді:

6.1.1. Құқықтық (заңнамалық) қорғау шаралары.

Құқықтық қорғау шараларына ақпаратпен жұмыс істеу қағидаларын регламенттейтін, ақпараттық қатынастарға қатысушылардың құқықтары мен міндеттерін оны өңдеу және пайдалану процесінде бекітетін, сондай-ақ осы қағидаларды бұзғаны үшін жауапкершілікті белгілейтін елдегі қолданыстағы

заңдар, жарлықтар мен нормативтік актілер жатады. Құқықтық қорғау шаралары негізінен алдын алу, профилактикалық сипатта болады және Қоғамның ақпараттық жүйесін пайдаланушылармен және қызмет көрсетуші персоналмен тұрақты түсіндіру жұмыстарын талап етеді.

6.1.2. Технологиялық қорғау шаралары.

Қорғау шараларының бұл түріне артықтықтың кейбір түрлерін (құрылымдық, функционалдық, ақпараттық, уақытша және т.б.) пайдалануға негізделген және қызметкерлердің өздеріне берілген құқықтар мен өкілеттіктер шеңберінде қателіктер мен бұзушылықтар жасау мүмкіндігін азайтуға бағытталған технологиялық шешімдер мен әдістер жатады. Мұндай шаралардың мысалы ретінде жауапты ақпаратты екі рет енгізу, жауапты операцияларды инициализациялау рәсімдерін бірнеше адамның келісімі болған жағдайда ғана, шығыс және кіріс хабарламалардың деректемелерін тексеру рәсімдерін және т.б. пайдалану болып табылады.

6.1.3. Ұйымдастырушылық (әкімшілік) қорғау шаралары.

Ұйымдастырушылық (әкімшілік) қорғау шаралары – бұл деректерді өңдеу жүйесінің жұмыс істеу процестерін, оның ресурстарын пайдалануды, қызмет көрсетуші персоналдың қызметін, сондай-ақ қауіпсіздікке төнетін қатерлерді іске асыру мүмкіндігін барынша қиындататын немесе болдырмайтындай немесе оларды іске асырған жағдайда шығындар мөлшерін азайтатындай пайдаланушылардың жүйемен өзара іс-қимыл жасау тәртібін реттейтін ұйымдастырушылық сипаттағы шаралар.

6.2. Қызметкерлерді ақпараттық ресурстарды пайдалануға рұқсат беруді регламенттеу.

Рұқсат беру жүйесі шеңберінде: кім, кімге, қандай ақпарат және қол жеткізудің қандай түрі үшін және қандай жағдайда бере алатындығы анықталады.

Пайдаланушылардың Қоғамның ақпараттық жүйесімен жұмыс істеуге рұқсаты және оның ресурстарына қолжетімділігі қатаң регламенттелуі тиіс. Ішкі жүйелерді пайдаланушылардың құрамы мен өкілеттіктеріне кез келген өзгерістер пайдаланушыларға қол жеткізуді ұсыну регламентіне сәйкес белгіленген тәртіппен жүргізілуі тиіс.

Корпоративтік ақпараттық жүйедегі ақпараттың негізгі пайдаланушылары Қоғамның құрылымдық бөлімшелерінің қызметкерлері болып табылады. Әр пайдаланушының өкілеттік деңгейі жеке анықталады. Әрбір қызметкер лауазымдық міндеттеріне сәйкес жұмыс істеуі қажет ақпаратқа қатысты өзіне белгіленген құқықтарды ғана пайдаланады. рҚол жеткізу құқықтарын кеңейту және қосымша ақпараттық ресурстарға қол жеткізуді ұсыну міндетті түрде осы ресурсты ақпараттық сүйемелдеуге жауапты Қоғамның бөлімшесімен келісілуі тиіс.

6.3. Аппараттық және бағдарламалық ресурстарға қызмет көрсету және түрлендіру процестерін регламенттеу.

Жүйенің қорғалатын ресурстары (құжаттар, міндеттер, серверлер, бағдарламалар) қатаң есепке алынуға жатады (тиісті формулярларды немесе мамандандырылған дерекқорларды пайдалану негізінде).

Ақпараттық қауіпсіздік режимін сақтау мақсатында корпоративтік ақпараттық жүйенің ресурстарына қол жеткізуге болатын Қоғам қызметкерлерінің автоматтандырылған жұмыс орындарының аппараттық-бағдарламалық конфигурациясы осы пайдаланушыларға жүктелген функционалдық міндеттер шеңберіне сәйкес келуі тиіс. Құпия ақпаратпен жұмыс істейтін қызметкерлердің жұмыс орындарында пайдаланылмаған барлық ақпаратты енгізу-шығару құрылғылары мүмкіндігінше өшірілуі керек, жұмыс үшін қажет емес бағдарламалық құралдар мен дискілердегі деректер де жойылуы керек. Қосымша ақпарат алмасу құрылғыларын тек ерекше жағдайларда және уақытша құрал ретінде пайдалануға болады. Мұндай құрылғыларды орнату Қоғамның ақпараттық қауіпсіздігін қамтамасыз ету бөлімшелерімен келісілуі тиіс.

Корпоративтік ақпараттық жүйенің құрамдастарында және пайдаланушылардың жұмыс орындарында тек ақпараттық технологиялар департаментінен алынған бағдарламалық құралдар орнатылып, пайдаланылуы тиіс. Тексерілмеген және Қоғамда ескерілмеген бағдарламалық қамтамасыз етуді пайдалануға тыйым салынуы керек.

Қоғамның ақпараттық желісінің қорғалуын бағалау және Қоғам желісінде ақпаратты қорғау жүйесін құру жөніндегі арнайы міндеттерді шешу үшін арнайы бағдарламалық қамтамасыз ету қолданылуы мүмкін.

6.4. Аппараттық ресурстардың физикалық тұтастығын (конфигурацияның өзгермейтіндігін) қамтамасыз ету және бақылау.

Пайдалану процесінде қызмет көрсетуші персоналдың кіруі талап етілмейтін құпия ақпаратқа қол жеткізу үшін пайдаланылатын корпоративтік ақпараттық жүйенің жабдығы оның компоненттеріне кіруге байланысты баптау, жөндеу және өзге де жұмыстардан кейін жабылуы және мөрленуі (пломбалануы) тиіс. Мөрлердің (пломбалардың) тұтастығы мен сәйкестігін күнделікті бақылауды жабдықты пайдаланушылар, мерзімді бақылауды Қоғамның қауіпсіздік қызметі жүзеге асыруы тиіс.

6.5. Қоғамның ақпараттық жүйесін пайдаланушылар, сондай-ақ басшы және қызмет көрсетуші персонал өздерінің өкілеттік деңгейімен, сондай-ақ Қоғамдағы ақпаратты өңдеу талаптары мен тәртібін айқындайтын ұйымдастырушылық-өкімдік, нормативтік, техникалық және пайдалану құжаттамасымен танысуы тиіс.

7-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету бөлімшелері

7.1. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі жұмысты тікелей ұйымдастыру қоғамның қауіпсіздік қызметіне және ақпараттық технологиялар департаментіне жүктеледі.

7.2. Ақпараттық қауіпсіздікті қамтамасыз ету бөлімшелерінің негізгі функциялары:

- Қоғамның ақпараттық қауіпсіздік саясатын іске асыру;
- ақпаратты кешенді қорғау бойынша Қоғамның барлық бөлімшелерінің іс-шараларын ұйымдастыру және жұмыстарын үйлестіру;
- ақпараттың қауіпсіздігін қамтамасыз етудің ағымдағы жай-күйін талдау;

- Қоғамның ақпараттық жүйесін пайдаланушылардың қызметін реттейтін құжаттарды қоса алғанда, ақпараттың қауіпсіздігін қамтамасыз ету мәселелеріне қатысты нормативтік құжаттарды әзірлеу;
- Қоғамның ақпараттық жүйесінің қолданыстағы құрамдастарын құру және одан әрі дамыту процесінде ақпараттық қауіпсіздік пен қорғау жүйесіне қойылатын талаптарды қалыптастыру;
- қорғау жүйелері мен бағдарламаларын жобалауға, оларды сынауға және пайдалануға қабылдауға қатысу;
- криптографиялық жүйелерді басқаруды қоса алғанда, ақпаратты қорғаудың белгіленген жүйелерінің жұмыс істеуін қамтамасыз ету;
- пайдаланушылар арасында Қоғамның ақпараттық жүйесінің ресурстарына қол жеткізудің қажетті атрибуттарын бөлу;
- қорғау жүйесінің және оның элементтерінің жұмыс істеуін бақылау;
- қорғау жүйесінің жұмыс істеу сенімділігін тексеру;
- ықтимал шабуылдардың үлгілерін бейтараптандыру шараларын әзірлеу;
- пайдаланушылар мен қызмет көрсетуші персоналды ақпаратты қауіпсіз өңдеу ережелеріне үйрету;
- Қоғам қызметкерлеріне ақпараттық қауіпсіздікті қамтамасыз ету мәселелерінде әдістемелік көмек көрсету;
- деректер қоры әкімшілерінің, серверлердің және желілік құрылғылардың әрекеттерін бақылау;
- пайдаланушылардың ақпаратпен жұмыс істеудің белгіленген ережелерін сақтауын бақылау;
- қабылданған шаралар мен қолданылатын ақпаратты қорғау құралдарының тиімділігін бақылау және бағалау;
- ақпараттық ресурстарға және жүйенің құрамдастарына рұқсатсыз қол жеткізу әрекеттері кезінде немесе қорғау жүйесінің жұмыс істеу қағидалары бұзылған кезде шаралар қабылдау;
- ақпараттық қауіпсіздік мәселелері бойынша ақпаратты жинау, жинақтау, жүйелеу және өңдеу;
- ақпараттық қауіпсіздік талаптарын бұзу фактілері бойынша қызметтік тексерулер мен тергеулер жүргізу.

7.3. Оларға жүктелген міндеттерді шешу үшін ақпараттық қауіпсіздікті қамтамасыз ету бөлімшелерінің құқықтары:

- ақпараттық қауіпсіздіктің кез келген аспектілері бойынша Қоғамның ақпараттық жүйесін пайдаланушылардан ақпарат алу;
- оған тікелей қауіп төнген кезде ақпаратты өңдеуді тоқтату;
- жаңа ақпараттық технологияларды жобалау және әзірлеу кезінде ақпараттың қауіпсіздігін қамтамасыз ету мәселелері бойынша техникалық шешімдерді пысықтауға қатысу;
- ақпараттың қауіпсіздігін қамтамасыз ету жөніндегі талаптарды іске асыру сапасын бағалау мәселелері бойынша әзірленген ақпараттық технологияларды сынауға қатысу;
- ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша Қоғамның ақпараттық жүйесін пайдаланушылардың қызметін бақылау;

- ақпараттық қауіпсіздік талаптарын бұзуға жол беретін қызметкерлерді жауапкершілікке тартуға бастамашылық жасау.

8-тарау. Ақпараттық қауіпсіздік талаптарын бұзғаны үшін жауапкершілік

Қоғамның қызметкерлері ақпаратты өңдеудің белгіленген тәртібін, жүйенің өз иелігіндегі қорғалатын ресурстарын сақтау, пайдалану және беру қағидаларын бұзғаны үшін дербес жауапты болады. Әрбір қызметкер жұмысқа қабылдау кезінде қызметтік және коммерциялық құпияны сақтау жөніндегі белгіленген талаптарды, сондай-ақ Қоғамдағы ақпаратпен жұмыс істеу қағидаларын бұзғаны үшін сақтау және жауапкершілік туралы міндеттемеге қол қоюы тиіс. Қоғам қызметкерлерінің ақпараттық қауіпсіздіктің белгіленген қағидалары мен талаптарын бұза отырып жасалған іс-әрекеттері үшін жауапкершілік шарасы келтірілген залалмен, зұлым ниеттің болуымен және Қоғам басшылығының қалауы бойынша басқа да факторлармен айқындалады.

9-тарау. Ақпараттық қауіпсіздікті қамтамасыз етудің ұйымдық-құқықтық режимі

Қоғамда ақпараттық қауіпсіздікті қамтамасыз етудің ұйымдық-құқықтық режимін енгізу қажетті нормативтік құжаттарды әзірлеуді және бекітуді көздейді:

- ақпараттық қауіпсіздікке қатысты Қазақстан Республикасының заңнамасында айқындалған және орындауға міндетті;
- Қоғамның коммерциялық құпиясын құрайтын мәліметтерге қатысты (коммерциялық құпия туралы ереже, Қоғамның коммерциялық және қызметтік құпиясын құрайтын мәліметтер тізбесі);
- Қоғам басшылығының қауіпсіздік режиміне қатысты бұйрықтары мен өкімдері.

10-тарау. Қорытынды ережелер

10.1. Осы Саясатпен реттелмеген мәселелер Қазақстан Республикасының заңнамасына сәйкес реттеледі.

10.2. Саясат Қазақстан Республикасы заңнамасының талаптарына қайшы келген жағдайда, Саясат Қазақстан Республикасының заңнамалық және нормативтік құқықтық актілеріне қайшы келмейтін бөлігінде қолдануға жатады.

10.3. Саясат талаптары Қоғамның барлық қызметкерлеріне таралады. Бөлімше қызметкерлерінің Саясат талаптарын орындауын бөлімше басшылары және жетекшілік ететін басшылар қамтамасыз етеді.

10.4. Осы Саясат Қоғам Басқармасы бекіткен күннен бастап күшіне енеді.

10.5. Осы Саясатқа өзгерістер мен толықтырулар Қоғам Басқармасының шешімі бойынша енгізіледі.