«Nomad Life» ӨСК» АҚ
Директорлар кеңесінің
2024 ж. «30» шілдедегі №300724/1 хаттамасымен
Бекітілді

«NOMAD LIFE» ӨСК» АҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

И - 137

Алматы қ.

КІРІСПЕ

«Nomad Life» ӨСК» АҚ Ақпараттық қауіпсіздік саясаты (бұдан әрі - Саясат) қағаз және электрондық құжат айналымын және сөйлеу құпия ақпаратымен алмасуды қоса алғанда, ақпараттық жүйеде ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған құжатталған басқару шешімдерінің жиынтығы деп түсініледі. Ақпараттық қауіпсіздік саясаты негізгі құжатты – «Ақпараттық қауіпсіздік саясаты» және ақпараттық қауіпсіздікті қамтамасыз ету процестерін, «NOMAD Life» ӨСК» АҚ (бұдан әрі – Қоғам) лауазымды адамдары мен ақпараттық жүйені пайдаланушылардың қызметін регламенттейтін құжаттарды қамтитын құжаттар пакетін білдіреді.

Саясаттың мақсаты - ақпараттың тиісті қорғалуын және қоғамның ақпараттық жүйесінің үздіксіз жұмысын қамтамасыз етуге және ақпараттық қауіпсіздікке төнетін қатерлерге қарсы іс-қимылдың тиімді алдын алу және қалпына келтіру шараларын әзірлеу арқылы оларды пайдаланудан болатын залалды барынша азайтуға қабілетті бірыңғай талаптар мен қағидаларды әзірлеу және бекіту.

1. АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ ЖҰМЫСТЫҢ ЖАЛПЫ БАҒЫТТАРЫ

1.1. Саясат Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 30 шілдедегі № 164 қаулысымен бекітілген сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге рұқсатсыз қол жеткізуден, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігінен ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға қойылатын талаптарға, «Сақтандыру (қайта сақтандыру) ұйымы туралы» Қазақстан Республикасының Заңына сәйкес әзірленді сондай-ақ Қазақстан Республикасының өзге де заңнамалық актілерімен, сондай-ақ Қоғамның ішкі құжаттарымен, ақпаратты қорғауды қамтамасыз ету тәртібіне бірыңғай талаптарды белгілейді, ақпараттық қауіпсіздікті басқару жөніндегі негізгі ұйымдастырушылық шешімдерді (бұдан әрі – АҚ) бекітеді және Қоғамның ақпараттық активтерін қорғау жөніндегі негізгі шараларды айқындайды.

1.2. Саясат ақпараттық қауіпсіздіктің мақсаттары мен міндеттерін сипаттайды, Қоғам өз қызметінде басшылыққа алатын ақ саласындағы ережелердің, талаптардың және басшылық қағидаттардың жиынтығын айқындайды, ақ саясатын іске асыруға және оны өзекті жағдайда ұстауға жауапты Қоғамның лауазымды тұлғалары мен қызметкерлерін, ақпараттық жүйелердің жұмыс қабілеттілігін құруға және қолдауға жауапты қоғамның бөлімшелерін және Қоғамдағы қорғау жүйелері, шаралар, дүлей зілзалалар, аварияләр, өрттер, электр энергиясының өшуі, байланыс желілерінің зақымдануы, жаппай тәртіпсіздіктер, ереуілдер, әскери іс-қимылдар жататын еңсерілмейтін күш жағдайлары туындаған жағдайда ақпараттық жүйелердің қауіпсіздік режимінің бұзылуын болғызбау.

1.3. Саясат талаптары қоғамның барлық құрылымдық бөлімшелеріне, сондай-ақ қоғамның ақпараттық жүйесінің жұмыс істеуін қамтамасыз етуді, қызмет көрсетуді және қамтамасыз етуді жүзеге асыратын қызметкерлерге қолданылады. Саясат ақпарат пен қызметтерді жеткізушілер мен тұтынушылар (пайдаланушылар) ретінде Қоғаммен өзара іс-қимылды жүзеге асыратын басқа ұйымдар мен мекемелерге де қолданылады.

2. ЖАУАПКЕРШІЛІК

2.1. Саясатты әзірлеу мен басқаруға Қоғамның Ақпараттық қауіпсіздік бөлімі жауапты болып табылады.

2.2. Саясатты дұрыс қолданғаны үшін жауапкершілік Қоғамның құрылымдық бөлімшелерінің басшыларына жүктеледі.

3. АНЫҚТАМАЛАР, БЕЛГІЛЕР ЖӘНЕ ҚЫСҚАРТУЛАР

3.1. Саясатта келесі терминдер мен анықтамалар қолданылады:

Авторизация - аутентификация деректері бойынша адамның немесе ақпараттық ресурстың өкілеттіктерін және оларға қол жеткізу қажет элементтерді анықтау;

Аутентификация - жүйеде іске асырылған қол жеткізудің ұсынылатын деректемелерінің сәйкестігін айқындау жолымен қол жеткізу субъектісінің немесе объектісінің түпнұсқалығын растау;

Шабуыл - ақпараттық активті жою, ашу, өзгерту, кіруді шектеу, ұрлау, рұқсатсыз кіру немесе рұқсатсыз пайдалану әрекеті;

Қолжетімділік-ақпараттық активтерді пайдалану мүмкіндігі;

Ақпараттық қауіпсіздік - электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалу жағдайы;

Ақпараттық актив - ақпаратты сақтау және (немесе) өңдеу үшін пайдаланылатын ақпарат пен ақпараттық-коммуникациялық инфрақұрылым объектісінің жиынтығы;

Ақпараттық жүйе (АЖ, ААЖ) - ақпараттық процестерді іске асыруға арналған аппараттық-бағдарламалық кешен;

Ақпараттық ресурстар - ақпараттық жүйелерде қамтылған электрондық түрде сақталатын ақпарат (ақпараттық деректер базасы);

Ақпараттық технологиялар - ақпаратты жинауды, жасауды, сақтауды, жинақтауды, өңдеуді, іздеуді, шығаруды, көшіруді, беруді және таратуды қамтамасыз ететін технологиялық кешенге біріктірілген әдістердің, өндірістік процестердің және бағдарламалық-техникалық құралдардың жиынтығы;

Қоғамның ақпараттық жүйесі - Қоғам мен оның клиенттерінің деректері сақталатын және өңделетін ақпараттық жүйе;

Таратылуы шектеулі ақпарат (қызметтік ақпарат) - таратудың, жинаудың, өңдеудің және пайдаланудың арнайы режимі белгіленген ақпарат;

Ақпараттық қауіпсіздік инциденті - ақпараттық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында олардың тиісінше жұмыс істеуіне қауіп төндіретін жеке немесе сериялық туындайтын іркілістер және (немесе) қоғамның электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, өзгерту, жою немесе бұғаттау үшін жағдайлар;

Деректерді берудің корпоративтік желісі - ақпараттық жүйелер арасындағы немесе олардың құрамдас бөліктері арасындағы өзара іс-қимылды қамтамасыз етудің, сондай-ақ электрондық ақпараттық ресурстарды берудің техникалық және аппараттық-бағдарламалық құралдарының жиынтығы;

Ақпаратқа рұқсатсыз қол жеткізу - құқықтық құжаттарда белгіленген оған қол жеткізу қағидаларын бұза отырып, мүдделі субъектінің қорғалатын ақпаратты алуы;

Ақпараттық-коммуникациялық инфрақұрылым объектілері - Қоғамның ақпараттық жүйелері, технологиялық платформалар, аппараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдар мен ақпараттық қауіпсіздіктің үздіксіз жұмыс істеуін қамтамасыз ету жүйелері;

Сақтық көшірме - қажет болған жағдайда деректерді бастапқы немесе жаңа жерде қалпына келтіруге арналған ақпарат тасығыштағы деректердің көшірмесі;

Ақпараттық-коммуникациялық инфрақұрылым (бұдан әрі - ақпараттық инфрақұрылым) - электрондық ақпараттық ресурстарды қалыптастыру және оларға қол жеткізуді қамтамасыз ету мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

Ақпараттық қауіпсіздікке қатер - ақпараттық қауіпсіздік инцидентінің туындауына алғышарттар жасайтын жағдайлар мен факторлардың жиынтығы;

Ақпараттық қауіпсіздікті қамтамасыз ету - Қоғамның ақпараттық активтерінің құпиялылығын, тұтастығын және қолжетімділігін сақтауға бағытталған процесс;

Нысан - жүйенің пассивті компоненті, қол жетімділікті шектеу ережелерімен реттелетін автоматтандырылған жүйенің ресурс бірлігі (құрылғы, диск, каталог, файл және т. б.);

Қорғау объектісі - ақпаратты қорғау мақсатына сәйкес қорғауды қамтамасыз ету қажет ақпарат немесе ақпарат тасымалдаушы немесе ақпараттық процесс;

Пайдаланушы - өзіне қажетті ақпараттық ресурстарды алу үшін ақпараттық жүйеге жүгінетін және оларды пайдаланатын субъект;

Қолжетімділікті саралау - алдын ала әзірленген және бекітілген қағидаларға сәйкес адамдардың техникалық және бағдарламалық құралдарға, оны есептеу техникасы құралдарында өңдеу кезінде қорғалатын ақпаратқа қол жеткізу тәртібі;

Есептеу техникасы құралдары - ақпаратты өңдеу жүйелерінің бағдарламалық және техникалық элементтерінің жиынтығы, оның ішінде дербес немесе басқа жүйелердің құрамында жұмыс істеуге қабілетті енгізу немесе шығару;

Технологиялық шот - ақпараттық жүйелер арасындағы аутентификацияға арналған ақпараттық жүйедегі шот;

Уәкілетті орган - Қаржы нарығын реттеу және дамыту жөніндегі уәкілетті орган;

АҚБ жауапты тұлғасы - ақпараттық қауіпсіздік бөлімінің қызметкері.

3.2. Саясатта саясаттың 1 кестесіне сәйкес келесі қысқартулар мен белгілер қолданылады.

Кесте №1

№	Анықтамалар, белгілер және қысқартулар	Берілген анықтамаларды, белгілерді және қысқартуларды түсіндіру
1	АҚ	Ақпараттық қауіпсіздік
2	КДЖ	Корпоративтік деректер желісі
3	ҚБ	Құрылымдық бөлімше
4	АЖ	Ақпараттық жүйе
5	ЕТҚ	Есептеу техникасы құралдары
6	ЖТ	Жұмыс тобы
7	ЖЕЖ	Жергілікті есептеу желісі
8	РК	Рұқсатсыз кіру
9	АККҚ	Ақпаратты криптографиялық қорғау құралы
10	ДК	Дербес компьютер
11	ДЕЭМ	Дербес электрондық есептеу машинасы
12	АЖ	Автоматтандырылған жүйелер
13	АҚБ	Ақпараттық қауіпсіздік бөлімі
14	ҚАИС	Қоғамның ақпараттық инфрақұрылымының серверлік және коммуникациялық жабдықтары орналасқан арнайы бөлінген үй-жай.

4. ТАЛАПТАР

4.1. Негізгі талаптар

4.1.1. АЖ ақпараттық жүйелерін пайдаланушыларға мыналар жатады:

4.1.1.1. Қоғам қызметкерлері – өз қызметін қоғамда жүзеге асыратын және Қазақстан Республикасының еңбек заңнамасына сәйкес қызметкердің негізгі құқықтары мен міндеттеріне ие жұмыскерлер;

4.1.1.2. көмекші персонал-ақпарат пен қызметтерді жеткізушілер және тұтынушылар (пайдаланушылар) ретінде қоғаммен өзара іс-қимылды жүзеге асыратын ведомстволық бағынысты және бөгде ұйымдардың қызмет көрсетуші және техникалық персоналы. Оның ішінде:

1) телекоммуникациялық жабдықты сүйемелдеуге жауапты ҚДЖ деректерді берудің Корпоративтік желісінің әкімшілері;

2) жалпы және қолданбалы бағдарламалық қамтамасыз етуді сүйемелдеуге жауапты жүйелік әкімшілер;

3) қолданбалы бағдарламалық қамтамасыз етуді әзірлеушілер;

4) Ақпараттық қауіпсіздік (арнайы қорғау құралдары) жөніндегі мамандар және т. б.

4.1.2 Ақпаратты кешенді қорғау жүйесін құрудың негізгі принциптері

Қоғамның ААЖ ақпаратының қауіпсіздігін қамтамасыз ету жүйесін құру және оның жұмыс істеуі мынадай негізгі қағидаттарға сәйкес жүзеге асырылуға тиіс:

4.1.2.1. Заңдылық

Ақпаратпен жұмыс істеу кезінде құқық бұзушылықтарды анықтау мен жолын кесудің барлық рұқсат етілген әдістерін қолдана отырып, Қазақстан Республикасының Ақпарат, ақпараттандыру және ақпаратты қорғау саласындағы қолданыстағы заңнамасына, Ақпарат қауіпсіздігі жөніндегі басқа да нормативтік актілерге сәйкес қорғау іс-шараларын жүзеге асыруды және қоғамның автоматтандырылған жүйелерінің Ақпарат қауіпсіздігі жүйесін әзірлеуді көздейді.

Қоғамның ААЖ пайдаланушылары мен қызмет көрсетуші персоналында ақпаратты автоматтандырылған өңдеу жүйелері саласындағы бұзушылықтар үшін жауапкершілік туралы түсінік болуы тиіс.

4.1.2.1. Жүйелік

Қоғамның ААЖ-да ақпаратты қорғау жүйесін құруға жүйелі көзқарас қоғамның ААЖ ақпаратының қауіпсіздігін қамтамасыз ету мәселесін түсіну және шешу үшін маңызды барлық өзара байланысты, өзара әрекеттесетін және уақыт бойынша өзгеретін элементтерді, жағдайлар мен факторларды ескеруді көздейді.

Қорғаныс жүйесін құру кезінде ақпаратты өңдеу жүйесінің барлық әлсіз және осал тұстары, сондай-ақ бұзушылар (әсіресе жоғары білікті зиянкестер) тарапынан жүйеге шабуылдардың сипаты, мүмкін объектілері мен бағыттары, таратылған жүйелерге және ақпаратқа РК ену жолдары ескерілуі тиіс. Қорғаныс жүйесі ақпаратқа енудің барлық белгілі арналары мен РК-ді ғана емес, сонымен қатар қауіпсіздік қатерлерін іске асырудың түбегейлі жаңа жолдарының пайда болу мүмкіндігін ескере отырып құрылуы керек.

4.1.2.3. Кешендік

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

шекаралардың бірі - ОЖ-нің барлық ресурстарын пайдалануды басқаратын компьютерлік жүйенің бөлігі болғандықтан, ЕТҚ операциялық жүйелері (ОЖ) деңгейінде жүзеге асырылатын қорғаныс құралдары. Пәндік аймақтың ерекшеліктерін ескеретін қолданбалы қорғаныс деңгейі қорғаудың ішкі шекарасын білдіреді.

4.1.2.4. Қорғаныстың үздіксіздігі

Ақпаратты қорғау-бұл бір реттік іс-шара емес, өткізілген іс-шаралар мен белгіленген қорғаныс құралдарының қарапайым жиынтығы емес, сонымен қатар оны пайдалану кезеңінде ғана емес, жобалаудың алғашқы кезеңдерінен бастап қоғамның ААЖ өмірлік циклінің барлық кезеңдерінде тиісті шаралар қабылдауды көздейтін үздіксіз мақсатты процесс.

Көптеген физикалық және техникалық қорғаныс құралдары өз функцияларын тиімді орындау үшін үнемі ұйымдастырушылық (әкімшілік) қолдауды қажет етеді (атауларды, парольдерді, 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 оның жұмыс істеуі қалпына келтірілгеннен кейін қорғаныс жүйесін жеңудің басқа құралдарын енгізу үшін пайдалана алады.

4.1.2.5. Уақытылық

Ақпараттың қауіпсіздігін қамтамасыз ету шараларының алдын алу сипатын, яғни ААЖ-ны кешенді қорғау жөніндегі міндеттерді қоюды және тұтастай ААЖ-ны және оның ақпаратты қорғау жүйесін, атап айтқанда, әзірлеудің бастапқы кезеңдерінде ақпараттың қауіпсіздігін қамтамасыз ету шараларын іске асыруды көздейді.

Қорғаныс жүйесін дамыту қорғалатын жүйенің өзін дамытумен және дамытумен қатар жүргізілуі керек. Бұл архитектураны жобалау кезінде қауіпсіздік талаптарын ескеруге және сайып келгенде, тиімдірек (ресурстардың құны бойынша да, төзімділік бойынша да) қорғалған жүйелерді құруға мүмкіндік береді.

4.1.2.6. Сабақтастық және жетілдіру

Ұйымдастырушылық және техникалық шешімдердің сабақтастығы, кадр құрамы, ААЖ және оның қорғау жүйесінің жұмыс істеуін талдау негізінде ақпаратты қорғау шаралары мен құралдарын ақпаратты ұстау әдістері мен құралдарындағы өзгерістерді, қорғау жөніндегі нормативтік талаптарды, осы саладағы қол жеткізілген отандық және шетелдік тәжірибені ескере отырып, тұрақты жетілдіруді көздейді.

4.1.2.7. Ақылға қонымды жеткіліктілік

(экономикалық орындылығы, ықтимал залал мен шығындардың салыстырмалылығы)

Ақпараттың қауіпсіздігін қамтамасыз етуге арналған шығындар деңгейінің ақпараттық ресурстардың құндылығына және олардың жария етілуінен, жоғалуынан, ағып кетуінен, жойылуынан және бұрмалануынан болатын залалдың шамасына сәйкестігін көздейді. Ақпараттық ресурстардың қауіпсіздігін қамтамасыз етудің қолданылатын шаралары мен құралдары осы ақпарат айналымда болатын ААЖ жұмысының эргономикалық көрсеткіштерін айтарлықтай нашарлатпауға тиіс.

Уақыт пен қаражаттың жеткілікті мөлшерімен кез-келген қорғанысты жеңуге болады. Шығындар, тәуекел және ықтимал зиян мөлшері қолайлы болатын қорғаныстың жеткілікті деңгейін дұрыс таңдау маңызды (тәуекелді талдау міндеті).

4.1.2.8. Жеке жауапкершілік

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

4.1.2.9. Өкілеттіктерді барынша азайту қағидаты

Бұл пайдаланушыларға өндірістік қажеттілікке сәйкес ең төменгі қол жетімділік құқықтарын беруді білдіреді. Ақпаратқа қол жеткізу қызметкерге өзінің лауазымдық міндеттерін орындау үшін қажет болған жағдайда және көлемде ғана берілуі керек.

4.1.2.10. Өзара әрекеттесу және ынтымақтастық

Қоғамның БҚ ұжымдарында қолайлы атмосфера құруды көздейді. Мұндай жағдайда қызметкерлер белгіленген ережелерді саналы түрде сақтауға және ақпаратты техникалық қорғау бөлімшелерінің қызметіне жәрдемдесуге тиіс.

4.1.2.11.Қорғаныс жүйесінің икемділігі

Қабылданған шаралар мен белгіленген қорғаныс құралдары, әсіресе оларды пайдаланудың бастапқы кезеңінде, қорғаныстың шамадан тыс және жеткіліксіз деңгейін қамтамасыз етуі мүмкін. Қауіпсіздік деңгейінің өзгеру мүмкіндігін қамтамасыз ету үшін қорғаныс құралдары белгілі бір икемділікке ие болуы керек. Бұл қасиет жұмыс істейтін жүйеге қорғаныс құралдарын орнату оның қалыпты жұмыс істеу процесін бұзбай жүзеге асырылуы қажет болған жағдайларда ерекше маңызды. Сонымен қатар, уақыт өте келе сыртқы жағдайлар мен талаптар өзгереді. Мұндай жағдайларда қорғаныс жүйесінің икемділік қасиеті атом электр станциясының иелерін қорғаныс құралдарын жаңаларына толығымен ауыстыру үшін түбегейлі шаралар қабылдау қажеттілігінен құтқарады.

4.1.2.12. Алгоритмдер мен қорғаныс механизмдерінің ашықтығы

Алгоритмдер мен қорғаныс механизмдерінің ашықтығы принципінің мәні мынада: қорғаныс тек құрылымдық ұйымның құпиялылығымен және оның ішкі жүйелерінің жұмыс істеу алгоритмдерімен қамтамасыз етілмеуі керек. Қорғаныс жүйесінің алгоритмдерін білу оны жеңуге мүмкіндік бермеуі керек (тіпті авторларға). Алайда, бұл белгілі бір қорғаныс жүйесі туралы ақпарат жалпыға қол жетімді болуы керек дегенді білдірмейді.

4.1.2.13. Қорғаныс құралдарын қолданудың қарапайымдылығы

Қорғаныс механизмдері интуитивті және пайдалану оңай болуы керек. Қорғаныс құралдарын қолдану Арнайы тілдерді білумен немесе белгіленген тәртіппен тіркелген пайдаланушылардың қалыпты жұмысы кезінде айтарлықтай қосымша еңбек шығындарын талап ететін әрекеттерді орындаумен байланысты болмауы керек, сондай-ақ пайдаланушыдан өзіне түсініксіз әдеттегі операцияларды (бірнеше парольдер мен атауларды енгізу және т. б.) орындауды талап етпеуі керек.

4.1.2.14. Ғылыми негізділігі және техникалық іске асырылуы

Ақпараттық технологиялар, техникалық және бағдарламалық құралдар, ақпаратты қорғау құралдары мен шаралары ғылым мен техниканың қазіргі даму деңгейінде іске асырылуға, Ақпарат қауіпсіздігінің белгіленген деңгейіне қол жеткізу тұрғысынан ғылыми негізделген болуға және ақпарат қауіпсіздігі бойынша белгіленген нормалар мен талаптарға сәйкес келуге тиіс.

4.1.2.15. Мамандандыру және кәсібилік

Тәжірибелік жұмыс тәжірибесі және осы салада қызмет көрсету құқығына тиісті лицензиясы бар ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету жөніндегі қызметтің нақты түріне неғұрлым дайындалған мамандандырылған ұйымдардың ақпаратын қорғау құралдарын әзірлеуге және оларды қорғау шараларын іске асыруға тартуды көздейді.

Әкімшілік шараларды іске асыруды және қорғау құралдарын пайдалануды қоғамның кәсіби дайындалған қызметкерлері (қауіпсіздік бөлімшелерінің мамандары) жүзеге асыруы тиіс.

4.1.2.16. Міндетті бақылау

Осы жүйелер мен құралдардың тиімділігін бағалау критерийлері мен әдістерін жетілдіру кезінде пайдаланылатын жүйелер мен ақпаратты қорғау құралдары негізінде ақпараттың қауіпсіздігін қамтамасыз етудің белгіленген ережелерін бұзу әрекеттерін анықтаудың және жолын кесудің міндеттілігі мен уақтылығын көздейді.

Кез келген пайдаланушының, әрбір қорғау құралының және кез келген қорғау объектісіне қатысты қызметін бақылау жедел бақылау және тіркеу құралдарын қолдану негізінде жүзеге асырылуға тиіс және пайдаланушылардың рұқсатсыз да, санкцияланған да әрекеттерін қамтуға тиіс.

4.1.3. Ақпараттық қауіпсіздік саясатының мақсаттары мен міндеттері

4.1.3.1. Мақсаттар

Саясаттың барлық тармақтары қол жеткізуге бағытталған негізгі мақсат қоғамның ақпараттық қауіпсіздігін сенімді қамтамасыз ету және соның салдарынан қоғамның ақпараттық активтерінің құпиялылығын, тұтастығы мен қолжетімділігін, қоғамның ақпараттық саладағы мүдделерін қорғауды қамтамасыз ету болып табылады.

Аталған мақсатқа деректерді берудің Корпоративтік желісінің келесі жай күйін қамтамасыз ету және тұрақты қолдау арқылы қол жеткізіледі:

- тіркелген пайдаланушылар үшін өңделетін ақпараттың қолжетімділігі;
- Қоғамның КДЖ тұрақты жұмыс істеуі;
- ЕТҚ-да сақталатын, өңделетін және байланыс арналары арқылы берілетін ақпараттың құпиялылығын қамтамасыз ету;
- қоғамның АЖ-да сақталатын және өңделетін және байланыс арналары арқылы берілетін ақпараттың тұтастығы мен түпнұсқалығы.

4.1.3.2. Міндеттер

Осы мақсатқа жету үшін келесі міндеттер кешенін шешу қажет:

1) қоғамның ақпараттық инфрақұрылымының қорғалуын қамтамасыз етуге мүмкіндік беретін ақпараттық қауіпсіздікті басқару жүйесін дамыту;

2) АҚ Ақпараттық қауіпсіздігін қамтамасыз ету саласында бірыңғай техникалық саясатты әзірлеу және іске асыру, оның ішінде ақпаратты қорғау жүйесін дамыту және нығайту;

3) қызметкерлердің құқықтары мен қоғамның ақпараттық саладағы мүдделерін қорғау;

4) қоғамның ақпараттық ресурстарының жұмыс істеу процесіне бөгде адамдардың араласуынан қорғау;

5) тіркелген пайдаланушылардың қоғамның АЖ-да пайдаланылатын ақпаратқа, аппараттық, бағдарламалық және криптографиялық қорғау құралдарына қол жеткізуінің аражігін ажырату;

6) бағдарламалардың орындалу ортасының тұтастығын бақылау (өзгермейтіндігін қамтамасыз ету) және бұзылған жағдайда оны қалпына келтіру;

7) ақпаратты рұқсатсыз өзгертуден, бұрмалаудан қорғау;

8) пайдаланылатын бағдарламалық құралдардың тұтастығын бақылау, сондай-ақ жүйені зиянды бағдарламалық қамтамасыз етуді енгізуден қорғау;

9) қызметтік құпияны және дербес деректерді оны өңдеу, сақтау және байланыс арналары арқылы беру кезінде ағып кетуден, рұқсатсыз жария етуден немесе бұрмалаудан қорғау;

10) ақпарат алмасуға қатысатын пайдаланушыларды авторизациялауды және аутентификациялауды қамтамасыз ету;

11) АҚ ақпараттық қауіпсіздігіне төнетін қатерлерді, зиян келтіруге ықпал ететін себептер мен жағдайларды уақтылы анықтау;

12) АҚ ақпараттық қауіпсіздігіне төнетін қатерлерге және теріс үрдістерге жедел ден қою тетігін құру;

13) Жеке және заңды тұлғалардың заңсыз әрекеттерімен келтірілген залалды барынша азайту және оқшаулау үшін жағдайлар мен нұсқаулықтар жасау, теріс ықпалды әлсірету және АҚ Ақпараттық қауіпсіздігін бұзу салдарын жою.

14) электрондық құжат айналымының үздіксіз жұмысын құру және қамтамасыз ету.

15) қоғамның ішкі Ішкі аудит қызметінің қауіпсіздік саясатының тұрақты аудиті жылына кемінде 1 рет.