«Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамы Басқармасының 2023 жылғы 7 сәуірдегі №02/10 шешімімен бекітілген
№8 сұрақ

«Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамының ақпараттық қауіпсіздік саясаты

4.0 нұсқасы

Құжаттар тобы:	операциялық құжаттама
Әзірлеуші:	Корпоративтік қауіпсіздік қызметі
Құжатты талдау және оған өзекті сипат беру үшін жауапты:	Корпоративтік қауіпсіздік қызметі

Астана-2023 ж.

Мазмұны

1 Жалпы ережелер

1. Осы «Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамының ақпараттық қауіпсіздік саясаты (бұдан әрі - Саясат) «Ақпараттық технологиялар – қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздікті басқару жүйелері – Талаптар» ISO 27001:2013 халықаралық стандартының талаптарына сәйкес әзірленген.

2. Саясат «Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамының (бұдан әрі – «ҚТЖ» ҰК» АҚ) ішкі құжаты болып табылады.

3. Осы Саясаттың күші «ҚТЖ» ҰК» АҚ компаниялар тобына («Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамы) және оның дауыс беретін акцияларының (қатысу үлестері) жүз пайызы тікелей меншік немесе сенімгерлік басқару құқығымен «ҚТЖ» ҰК» АҚ тиесілі еншілес ұйымдарына (бұдан әрі - ЕҰ) және «ҚТЖ» ҰК» АҚ компаниялар тобының мүддесінде әрекет ететін (жасалған шарттар шеңберінде) өзге ұйымдар.

4. «ҚТЖ» ҰК» АҚ басшылығы ақпараттық қауіпсіздікке төнетін қатерлер контекстінде ақпараттық активтерді қорғау шаралары мен құралдарын дамыту, жетілдіру, «ҚТЖ» ҰК» АҚ қызметін реттеу заңнамасы мен нормаларын дамыту үшін қажетті жағдайларды қамтамасыз ете отырып, ақпараттық қауіпсіздікті басқарудың маңыздылығын түсінеді және жүзеге асырады.

5. «ҚТЖ» ҰК» АҚ «Самұрық-Қазына» акционерлік қоғамы активтерінің құрамына кіретін мемлекеттік маңызы бар көлік-логистикалық компания болып табылады. Аталған қызметті жүзеге асыру ақпаратты, оның ішінде «ҚТЖ» ҰК» АҚ-ның маңызды активі болып табылатын мемлекетпен таратылатын ақпаратты басқарумен байланысты және жеке жергілікті актімен бекітілген Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидаларына сәйкес активтердің құпиялылығы, тұтастығы және қолжетімділігі түсінілетін ақпараттық қауіпсіздікті қамтамасыз етуге байланысты.

6. «ҚТЖ» «ҰК» АҚ ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне ерекше көңіл бөледі, ақпараттық қауіпсіздікті басқару жүйесін (бұдан әрі - АҚБЖ), ақпараттық қауіпсіздікке төнетін қатерлерден қорғаудың қолданылатын құралдары мен тәсілдерін ұдайы жетілдіреді, сондай-ақ ақпаратты қорғау саласындағы құзыреттілікті жоғары деңгейде ұстап тұру үшін Компания қызметкерлерін үздіксіз оқытуды қамтамасыз етеді.

7. АҚБЖ «ҚТЖ» ҰК» АҚ басқару жүйесінің бөлігі болып табылады. Саясат ережелері барлық мүдделі тараптардың үміттерін ескереді және инвестициялық жобалар портфелін қалыптастыру процесінде «ҚТЖ» ҰК» АҚ-ның және ЕҰ-ның барлық қызметкерлерінің орындауы үшін міндетті, сондай-ақ «ҚТЖ» ҰК» АҚ ақпараттық жүйелері мен құжаттарына қол жеткізе алатын клиенттер мен өзге де үшінші тұлғалардың назарына «ҚТЖ» ҰК» АҚ-мен және оның қызметімен тікелей байланысты бөлімінде жеткізіледі.

8. Саясат ақпаратты қорғаудың негізгі мақсаттарын, принциптері мен талаптарын қарастырады.

9. Саясат Қазақстан Республикасының ақпараттық жүйелер мен ақпараттық қауіпсіздікті пайдалану мәселелері жөніндегі заңнамасына, сондай-ақ ақпараттық қауіпсіздік басқармасының халықаралық стандарттарының талаптарына сәйкес әзірленді.

10. Саясат иесі және пайдаланушысы «ҚТЖ» ҰК» АҚ және ЕҰ болып табылатын барлық ақпараттық жүйелер мен құжаттарды қамтиды. Ақпараттық қауіпсіздікті қамтамасыз ету «ҚТЖ» ҰК» АҚ қызметін жүзеге асыру үшін қажетті шарт болып табылады.

2 Мақсаттар, талаптар және негізгі принциптер

11. Саясаттың негізгі мақсаты ақпараттың қауіпсіздігіне қауіп төндіретін оқиғалардан болатын залалды олардың алдын алу немесе олардың салдарын барынша азайту арқылы төмендету болып табылады.

12. АҚБЖ негізінде ақпараттық қауіпсіздік оқиғаларын іске асыру ықтималдығын төмендетуге бағытталған тәуекелге бағытталған тәсіл қарастырылған.

13. Ақпараттық қауіпсіздікті қамтамасыз ету «ҚТЖ» ҰК» АҚ мен ЕҰ-ның қолда бар ақпараттық ресурстарына түрлі қауіп-қатерлермен байланысты тәуекелдер мен экономикалық шығындарды азайту үшін қажет. Осы мақсатта ақпараттың негізгі қасиеттерін сақтау қажет, атап айтқанда:

1) қолжетімділік - бұл тиісті өкілеттіктері бар субъектілердің ақпаратына уақтылы кедергісіз қол жеткізу қабілетімен сипатталатын қасиет;

2) құпиялылық - ақпаратқа оның иелері анықтаған шектеулі адамдар ғана қол жеткізе алатынын көрсететін қасиет;

3) тұтастық - бұл ақпараттың бұрмаланбаған түрде сақталуынан тұратын қасиеті (оның кейбір бекітілген күйіне қатысты өзгермейді).

14. Ақпараттық қауіпсіздіктің жеткілікті сенімді жүйесін қамтамасыз ету үшін оның параметрлерін үнемі қайта бағалау, сыртқы және ішкі ортадан шығатын жаңа қауіптерді көрсету үшін бейімделу қажет. Мұндай қажеттілік туындаған кезде стандарттарға, рәсімдерге немесе саясатқа өзгерістер енгізу кезінде ешқандай кедергілер болмауы керек.

Осыған байланысты ақпараттық қауіпсіздікті басқару циклінің келесі кезеңдері анықталады:

1) жоспарлау (әзірлеу) - «ҚТЖ» ҰК» АҚ Директорлар кеңесінің 2019 жылғы 6 қыркүйектегі (№13 хаттама) шешімімен бекітілген «ҚТЖ» ҰК» АҚ-ның 2029 жылға дейінгі даму стратегиясына сәйкес нәтижелер алу үшін тәуекелдерді басқаруға және ақпараттық қауіпсіздікті жетілдіруге жататын тәуекелдерді, мақсаттарды, міндеттерді, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды талдау;

2) іске асыру (енгізу және пайдалану) – бақылау тетіктерін, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды енгізу;

3) тексеру (мониторинг және талдау) - қажет болған жағдайда бағалау, Саясатқа, мақсаттарға және практикалық тәжірибеге сәйкес процестердің орындалу сипаттамаларын өлшеу, ақпараттық ресурстардың қорғалуына әсер ететін сыртқы және ішкі факторлардың өзгеруін талдау, талдау үшін басшылыққа есептер беру;

4) түзету (сүйемелдеу және жетілдіру) – ақпараттық қауіпсіздік жүйесін үздіксіз жетілдіруді қамтамасыз ету мақсатында ақпараттық қауіпсіздіктің жай-күйін ішкі және сыртқы тексерулердің нәтижелеріне, басшылық тарапынан өзге де факторлар талаптарына негізделген түзету және алдын алу шараларын қабылдау.

15. «ҚТЖ» ҰК» АҚ және ЕҰ ақпараттық қауіпсіздікті қамтамасыз ету жүйесін құру, сондай-ақ оның жұмыс істеуі мынадай қағидаттарға сәйкес жүзеге асырылуға тиіс:

1) заңдылық - ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын кез келген іс-әрекеттер «ҚТЖ» ҰК» АҚ және ЕҰ АҚ ақпаратты қорғау объектілеріне теріс әсерлерді анықтау, оқшаулаудың алдын алу және жолын кесу үшін заңнамада рұқсат етілген барлық әдістерді қолдана отырып, Қазақстан Республикасының заңнамасы шеңберінде жүзеге асырылады;

2) іскерлік ақпараттық қауіпсіздікке бағдарлану - негізгі қызметті қолдау процесі ретінде қарастырылады. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі кез келген шаралар «ҚТЖ» ҰК» АҚ және ЕҰ қызметіне елеулі кедергілерге әкеп соқпауы тиіс;

3) үздіксіздік - ақпаратты қорғау жүйелерін басқару құралдарын қолдану, «ҚТЖ» ҰК» АҚ және ЕҰ ақпараттық қорғауды қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру «ҚТЖ» ҰК» АҚ және ЕҰ ағымдағы бизнес-процестерін үзбей немесе тоқтатпай жүзеге асырылуы тиіс;

4) кешенділік - ақпараттық ресурстардың бүкіл өмірлік циклі ішінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және жұмыс істеудің барлық режимдерінде қауіпсіздігін қамтамасыз ету;

5) негізділік және экономикалық орындылық - пайдаланылатын мүмкіндіктер мен қорғау құралдары ғылым мен техниканың тиісті даму деңгейінде іске асырылуы, қауіпсіздіктің белгіленген деңгейі тұрғысынан негізделуі және қойылатын талаптар мен нормаларға сәйкес келуі тиіс. Барлық жағдайларда ақпараттық қауіпсіздік шаралары мен жүйелерінің құны тәуекелдің кез келген түрінен болатын ықтимал залал мөлшерінен аз болуы тиіс.

6) басымдық – «ҚТЖ» ҰК» АҚ-ның барлық ақпараттық ресурстарын және ақпараттық қауіпсіздіктің нақты, сондай-ақ ықтимал қатерлерін бағалау кезіндегі маңыздылық дәрежесі бойынша санаттау (саралау);

7) қажетті білім және артықшылықтардың ең төменгі деңгейі - пайдаланушы артықшылықтары мен өз өкілеттіктері шеңберінде өз қызметін орындау үшін ғана қажетті деректерге қол жеткізе алады;

8) мамандандыру - техникалық құралдарды пайдалану және ақпараттық қауіпсіздік шараларын іске асыруды кәсіби дайындалған мамандар жүзеге асыруы керек;

9) ақпараттандыру және жеке жауапкершілік - барлық деңгейдегі басшылар мен қызметкерлер ақпараттық қауіпсіздіктің барлық талаптары туралы хабардар болуы және осы талаптардың орындалуына және ақпараттық қауіпсіздіктің белгіленген шараларының сақталуына жауапты болуы тиіс;

10) өзара әрекеттестік және үйлестіру - ақпараттық қауіпсіздік шаралары «ҚТЖ» ҰК» АҚ және ЕҰ-ның тиісті құрылымдық бөлімшелерінің өзара байланысы, қойылған мақсаттарға қол жеткізу үшін олардың күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен, кәсіптік қауымдастықтармен және қоғамдастықтармен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыстар орнату негізінде жүзеге асырылады;

11) расталу - ақпараттық қауіпсіздік және оны ұйымдастыру жүйесінің тиімділігі жөніндегі талаптардың орындалғанын растайтын құжаттар Жедел қол жеткізу және қалпына келтіру мүмкіндігімен құрылуы және сақталуы тиіс.

3 Қорғау объектілері

16. «ҚТЖ» ҰК» АҚ және ЕҰ ақпараттық қауіпсіздікті қамтамасыз етуді қорғаудың негізгі объектілері мынадай элементтер болып табылады:

1) қолданыстағы заңнамаға және "ҚТЖ "ҰК" АҚ және ЕҰ жергілікті актілеріне сәйкес коммерциялық, қызметтік немесе заңмен қорғалатын өзге де құпияға жатқызылған мәліметтерді қамтитын ақпараттық ресурстар, оның ішінде "Цифрлық темір жол" бағдарламаларының жобаларына және "ҚТЖ "ҰК" АҚ-ға трансформациялау бағдарламаларына (бұдан әрі - қорғалатын ақпарат);

2) қорғалатын ақпаратты өңдеу, беру және сақтау жүргізілетін ақпараттандыру құралдары мен жүйелері (есептеу техникасы құралдары, ақпараттық-есептеу кешендері, желілер, жүйелер);

3) «ҚТЖ» ҰК» АҚ және ЕҰ автоматтандырылған жүйелерінің бағдарламалық құралдары (операциялық жүйелер, деректер базасын басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз ету), олардың көмегімен қорғалатын ақпаратты өңдеу жүргізіледі;

4) ақпараттық ресурстарды басқару мен пайдалануға байланысты «ҚТЖ» ҰК» АҚ және ЕҰ процестері;

5) қорғалатын ақпаратты өңдеу құралдары орналасқан үй-жайлар;

6) жабық келіссөздер мен кеңестер жүргізуге арналған «ҚТЖ» ҰК» АҚ және ЕҰ, «ҚТЖ» ҰК» АҚ және ЕҰ қызметкерлерінің жұмыс үй-жайлары мен кабинеттері;

7) қорғалатын ақпаратқа қолжетімділігі бар «ҚТЖ» ҰК» АҚ және ЕҰ қызметкерлері;

8) ашық ақпаратты өңдейтін, алайда қорғалатын ақпарат өңделетін үй-жайларда орналастырылған техникалық құралдар мен жүйелер;

9) серверлік инфрақұрылымды пайдалану кезінде виртуалды орталар (есептеу ресурстары немесе олардың логикалық бірлестігі, аппараттық іске асырудан абстракциялау, бір физикалық ресурста орындалатын есептеу процестерінің бір-бірінен логикалық оқшауланuын қамтамасыз ету).

17. Қорғалатын ақпарат мүмкіндіктері:

1) қағаз тасымалдаушыларда жайғасу;

2) электрондық түрде өмір сүру (есептеу техникасы құралдарымен өңделеді, беріледі және сақталады, техникалық құралдардың көмегімен жазылады және ойнатылады);

3) телефон, телефакс, телекс және т.б. арқылы электр сигналдары түрінде берілу;

4) жиналыстар мен келіссөздер кезінде ауа ортасында және қоршау құрылымдарында акустикалық және діріл сигналдары түрінде қатысу.

4 Ақпараттық қауіпсіздікке төнетін қатерлер

18. Ақпараттық қауіпсіздікке төнетін қатерлер деп ақпаратқа немесе ақпараттық жүйенің компоненттеріне немесе ресурсқа әсер ету арқылы иелер мен пайдаланушылардың мүдделеріне тікелей немесе жанама түрде зиян келтіруі мүмкін ықтимал оқиға, процесс немесе құбылыс түсініледі.

19. Ақпараттық қауіпсіздікке төнетін қатерлер:

1) кездейсоқ, келесі факторларға байланысты болуы мүмкін:

табиғи апаттар;

абайсыз қателіктері;

аппараттық және бағдарламалық құрал қателері;

ақпараттық қауіпсіздік саласындағы қызметкерлердің төмен хабардарлығы;

ақпараттық қауіпсіздік периметрін физикалық қамтамасыз етудің жеткіліксіздігі;

2) қасақана, келесі факторларға байланысты болуы мүмкін:

деректерді бұрмалау немесе жою;

деректерді теріс пайдалану;

ақпаратқа заңсыз қол жеткізу;

компьютерлік шабуылдар (ақпаратқа, электрондық ресурсқа, ақпараттық жүйеге рұқсатсыз әсер ету қатерін іске асырудың немесе бағдарламалық немесе бағдарламалық-аппараттық құралдарды немесе желіаралық өзара іс-қимыл хаттамаларын пайдалана отырып, оларға қол жеткізудің мақсатты әрекеті);

20. «ҚТЖ» ҰК» АҚ және ЕҰ ақпараттық қауіпсіздікке төнетін қатерлерге мыналар жатады (бірақ олармен шектелмейді):

1) қорғалатын ақпараттың жоғалуы;

2) қорғалатын ақпаратты бұрмалау (рұқсатсыз өзгерту, қолдан жасау);

3) ақпараттың ағылуы, бөгде адамдардың қорғалатын ақпаратпен рұқсатсыз танысуы (рұқсатсыз кіру, көшіру, ұрлау және т. б.);

4) ақпараттық ресурстарды рұқсатсыз пайдалану (теріс пайдалану, алаяқтық және т. б.);

5) бұғаттау, жабдықтың істен шығуы, деректер базасын басқару жүйелері, таратылған есептеу желілері, вирустардың, дүлей зілзалалардың және өзге де форс-мажорлық мән-жайлардың және зиянды әрекеттердің салдарынан ақпараттың қолжетімсіздігі.

21. Аталған қауіптердің әсері нәтижесінде «ҚТЖ» ҰК» АҚ және ЕҰ-ның ақпараттық қауіпсіздігінің жай-күйіне қалыпты жұмыс істеуіне әсер ететін мынадай жағымсыз салдарлар туындауы мүмкін:

1) қозғалыс қауіпсіздігіне байланысты төтенше жағдайлар;

2) қорғалатын ақпараттың ағылуына немесе жария етілуіне байланысты қаржылық шығындар;

3) жоғалған ақпаратты жоюға және кейіннен қалпына келтіруге байланысты қаржылық шығындар;

4) «ҚТЖ» ҰК» АҚ қызметінің ұйымдастырылмауынан және өз міндеттемелерін орындау мүмкін сстігіне байланысты шығындарға дейінгі залал;

5) бейтарап ақпарат негізінде басқарушылық шешімдер қабылдаудан болатын залал;

6) «ҚТЖ» ҰК» АҚ басшылығының объективті ақпаратқа ие болмауынан болатын залал;

7) «ҚТЖ» ҰК» АҚ және ЕҰ-ның беделіне келтірілген залал;

8) залалдың өзге түрі.

Аппараты қауіпсіздік қатерлерін сәйкестендіруді жүргізу, ақпараттық қауіпсіздік қатерлерін іске асыру ықтималдығын айқындау үшін жекелеген жергілікті актімен бекітілген «ҚТЖ» ҰК» АҚ компаниялар тобы бойынша ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесін басшылыққа алу қажет.

5 Ақпараттық қауіпсіздікті қамтамасыз ету шаралары

22. «ҚТЖ» ҰК» АҚ және ЕҰ ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі негізгі шаралар:

1) әкімшілік-құқықтық және ұйымдастырушылық шаралар;

2) физикалық қауіпсіздік шаралары;

3) бағдарламалық-техникалық шаралар.

23. Әкімшілік-құқықтық және ұйымдастырушылық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):

1) ҚР заңнамасы талаптарының және «ҚТЖ» ҰК» АҚ және ЕҰ ішкі құжаттарының орындалуын бақылау;

2) саясатты қолдайтын қағидалардың, әдістемелер мен нұсқаулықтардың орындалуын әзірлеу, енгізу және бақылау;

3) «ҚТЖ» ҰК» АҚ бизнес-процестерінің саясат талаптарына сәйкестігін бақылау;

4) «ҚТЖ» ҰК» АҚ қызметкерлерін ақпараттық жүйелермен және ақпараттық қауіпсіздік талаптарымен жұмыс істегенге дейін ақпараттандыру және оқыту;

5) ақпараттың рұқсатсыз ағылу арналарына, осыған байланысты оқиғаларға, салдарды оқшаулауға және азайтуға жауап беру;

6) ақпараттық қауіпсіздіктің жаңа тәуекелдерін талдау;

7) ұжымдағы моральдық-іскерлік ахуалды қадағалау және жақсарту;

8) төтенше жағдайлар туындаған кездегі іс-қимылдарды айқындау;

9) «ҚТЖ» ҰК» АҚ қызметкерлерін жұмысқа қабылдау және жұмыстан шығару кезінде алдын алу шараларын жүргізу;

10) БЖ пайдаланудың заңдылығын бақылау жөніндегі іс-шаралар.

24. Физикалық қауіпсіздік шаралары мыналарды қамтиды (бірақ олармен шектелмейді):

1) өткізу және объектішілік режимдерді ұйымдастыру;

2) қорғалатын объектілердің қауіпсіздік периметрін құру;

3) күзетілетін объектілерді тәулік бойы күзетуді, оның ішінде техникалық қауіпсіздік құралдарын пайдалана отырып ұйымдастыруды;

4) күзетілетін объектілердің өртке қарсы қауіпсіздігін ұйымдастыру;

5) «ҚТЖ» ҰК» АҚ және ЕҰ қызметкерлерінің режимдік үй-жайларға және қолжетімділігі шектеулі үй-жайларға кіруін бақылау.

25 Бағдарламалық-техникалық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):

1) лицензиялық бағдарламалық жасақтама және сертификатталған ақпаратты қорғау құралдарын пайдалану;

2) периметрлік қорғаныс құралдарын пайдалану (firewall, IPS және т. б.);

3) кешенді антивирустық қорғауды қолдану;

4) ақпараттық жүйелерге енгізілген ақпараттық қауіпсіздік құралдарын пайдалану;

5) ақпараттың тұрақты резервтік көшірмесін қамтамасыз ету;

6) бірінші кезекте артықшылықты пайдаланушылардың құқықтары мен іс-әрекеттерін бақылау;

7) нормативтік құқықтық актілерде белгіленген тәртіппен ақпаратты криптографиялық қорғау құралдарын қолдану;

8) аппараттық құралдардың ақаусыз жұмысын қамтамасыз ету;

9) ақпараттық жүйенің маңызды элементтерінің жай-күйін мониторингтеу.

6 Жауапкершілік және заңнама талаптарына сәйкестік

26. «ҚТЖ» ҰК» АҚ және ЕҰ нормативтік құқықтық актілердің талаптарын сақтауды, зияткерлік меншік құқықтарын сақтауды, заңмен қорғалатын дербес ақпаратты қорғауды, криптографиялық құралдарды пайдалану бойынша шектеулерді сақтауды қамтамасыз ету үшін тиісті процестерді енгізді.

27. ISO/IEC 27001 халықаралық стандартының барлық талаптары мен ережелері тиісті құжаттармен айқындалатын оларды қолдану саласында орындау үшін міндетті болып табылады.

28. Ақпараттық қауіпсіздік құралдары мен әдістерін әзірлеу және қолдану кезінде «ҚТЖ» ҰК» АҚ және ЕҰ үшінші тараптармен жасасқан шарттық міндеттемелер мен келісімшарттардың талаптары ескеріледі.

29. Үшінші тараптың «ҚТЖ» ҰК» АҚ және ЕҰ ақпараттық ресурстарына қолжетімділігі осындай қолжетімділік берілген кезде туындауы мүмкін тәуекелдерді талдағаннан және барабар қорғау шараларын қабылдағаннан кейін ғана жүзеге асырылады. Қажет болған жағдайда (атап айтқанда, нормативтік құқықтық актілердің немесе халықаралық стандарттардың талаптары болған кезде), «ҚТЖ» ҰК» АҚ және ЕҰ контрагенттердің (тауарлар мен көрсетілетін қызметтерді жеткізушілердің) белгілі бір талаптарға сәйкестігіне тексеру жүргізеді.

30. Саясат негізінде ақпараттық қауіпсіздікті, стандарттарды және т.б. қамтамасыз ету тәртібі мен әдістерін реттейтін жергілікті актілер әзірленеді.

31. Осы Саясатты сақтау үшін жауапкершілік «ҚТЖ» ҰК» АҚ және ЕҰ қызметкерлеріне жүктеледі.

7 Саясатты қайта қарау

32. Саясат қажеттілігіне қарай, алайда кемінде 24 айда бір рет қайта қаралады.