

Қазақстан Республикасының Цифрлық даму,
қорғаныс және аэроғарыш өнеркәсібі министрлігіҚазақстан Республикасының
Цифрлық даму, қорғаныс және
аэроғарыш өнеркәсібі министрінің
2019 жылғы 3 маусымдағы № 111
/НҚ бұйрығы. Қазақстан
Республикасының Әділет
министрлігінде 2019 жылғы 5
маусымда № 18795 болып тіркелдіМинистерство цифрового развития, оборонной и
аэрокосмической промышленности Республики
Казахстан

«Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы

«Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 7-1-бабының 5) тармақшасына және «Мемлекеттік көрсетілетін қызметтер туралы» 2013 жылғы 15 сәуірдегі Қазақстан Республикасы Заңының 10-бабының 1) тармақшасына сәйкес **БҰЙЫРАМЫН:**

Ескерту. Кіріспе жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 01.04.2020 № 121/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1. Мыналар:

1) осы бұйрыққа 1-қосымшаға сәйкес «Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі;

2) осы бұйрыққа 2-қосымшаға сәйкес «Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық



«ЗҚАИ» ШЖҚ РМК лауазымды тұлғаның ЭЦҚ мәліметі бар QR-код



ҚР НҚА ЭББ-гі нақты
құжатқа сілтеу QR-коды

инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары бекітілсін.

2. «Сервистік бағдарламалық өнімнің, «электрондық үкіметтің» ақпараттық-коммуникациялық платформасының мемлекеттік органның интернет-ресурсының және ақпараттық жүйенің олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы» Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 14 наурыздағы № 40/НҚ бұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16694 болып тіркелген, Қазақстан Республикасы Нормативтік құқықтық актілерінің эталондық бақылау банкінде 2018 жылғы 12 сәуірде жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті заңнамада белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық мемлекеттік тіркелген күннен бастап күнтізбелік он күн ішінде оны Қазақстан Республикасы Нормативтік құқықтық актілерінің эталондық бақылау банкіне ресми жариялау және енгізу үшін Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

3) осы бұйрық ресми жарияланғаннан кейін оны Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрлігінің интернет-ресурсында орналастыруды;

4) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрлігінің Заң департаментіне осы тармақтың 1), 2) және 3) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер ұсынуды қамтамасыз етсін.

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

5. Осы бұйрық алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

**Қазақстан Республикасының
Цифрлық даму, қорғаныс және
аэроғарыш өнеркәсібі министрі**

А. Жұмағалиев

«КЕЛІСІЛДІ»

Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

2019 жылғы «__» _____

Қазақстан Республикасы
Цифрлық даму, қорғаныс
және аэроғарыш
өнеркәсібі министрінің
2019 жылғы «__» _____
№ __ бұйрығына
1-қосымша

**«Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса маңызды объектілеріне
жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
әдістемесі**

1-тарау. Жалпы ережелер

1. Осы «Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі (бұдан әрі – Әдістеме) «Ақпараттандыру туралы» Қазақстан Республикасы Заңының 7-1-бабының 5) тармақшасына сәйкес әзірленді.

Ескерту. 1-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

2. Осы Әдістемеде мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) қызмет беруші – мемлекеттік техникалық қызмет немесе аккредиттелген сынақ зертханасы;

2) мемлекеттік техникалық қызмет – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған акционерлік қоғам;

3) осалдық – бағдарламалық қамтылымдағы оның жұмыс қабілеттілігін бұзуға немесе бағдарламалық қамтылымда белгіленген рұқсаттардан тыс қандай да бір заңсыз іс-әрекеттерді орындауға мүмкіндік беретін кемшілік;

4) өтініш беруші – сынақ объектісінің меншік иесі немесе иеленушісі, сондай-ақ сынақ объектісінің меншік иесі немесе иеленушісі өкілеттік берген ақпараттандыру объектісінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізуге өтініш берген жеке немесе заңды тұлға;

5) сенімді арна – сынақ объектілерінің қауіпсіздік функциялары (бұдан әрі – ОҚФ) мен сынақ объектілерінің қауіпсіздік саясатын қолдауда қажетті сенімді деңгейді қамтамасыз ететін ақпараттық технологиялардың алыс орналасқан сенімді өнімі арасындағы өзара іс-қимыл құралы;

6) сенімді бағыт – сынақ объектілерінің қауіпсіздік саясатын қолдауда сенімділікті қамтамасыз ететін пайдаланушы мен ОҚФ арасындағы өзара іс - қимыл құралы;

7) сынақ объектісі – оған қатысты ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтан өткізу жөніндегі жұмыстар жүргізілетін ақпараттандыру объектісі;

8) сынақ объектісі желісінің (ішкі желісінің) сегменті – сынақ объектісі желісінің қисынды бөлінген сегменті;

9) штаттық пайдалану ортасы – ақпараттандыру объектісін тәжірибелік пайдалану (пилоттық жобаны) кезеңінде қолданылатын және өнеркәсіптік пайдалану кезеңінде қолдануға арналған серверлік жабдықтың, желілік инфрақұрылымның, жүйелік бағдарламалық қамтылымның нысаналы жиынтығы;

10) SYNAQ интернет-порталы – «электрондық үкіметтің» ақпараттандыру объектілерін және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерді ақпараттық қауіпсіздік талаптарына сәйкестігіне сынау бойынша қызмет көрсету процесін автоматтандыруға арналған мемлекеттік техникалық қызметтің интернет-порталы.

Ескерту. 2-тармаққа өзгерістер енгізілді - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 01.04.2020 № 121/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); 28.09.2020 № 356/НҚ (алғаш ресми жарияланған күнінен

кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрықтарымен.

3. Сынақтар жүргізу мыналарды қамтиды:

- 1) бастапқы кодтарды талдау;
- 2) ақпараттық қауіпсіздік функцияларын сынау;
- 3) жүктемелік сынау;
- 4) желілік инфрақұрылымды зерттеп-қарау;
- 5) ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау.

2-тарау. Бастапқы кодтарды талдау

4. Сынақ объектілерінің бастапқы кодтарын талдау бағдарламалық қамтылымның (бұдан әрі – БҚ) кемшіліктерін анықтау мақсатында жүргізіледі.

5. Бастапқы кодтарды талдау «Электрондық үкіметтің» ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелердің олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидаларына (бұдан әрі – Қағидалар) 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың 5-тармағы 11) тармақшасының кестесінде аталған БҚ үшін жүргізіледі.

6. Егер сынақтар жүргізу кезінде сынақ мерзімі аяқталғанға дейін бастапқы кодтарды қайта талдау жүргізу қажеттілігі айқындалса, өтініш беруші қызмет берушіге сұрау салумен жүгінеді және Қағидалардың 26-тармағына сәйкес бастапқы кодтарға қайтадан талдау жүргізу туралы қосымша келісім жасалады.

7. БҚ кемшіліктерін айқындау өтініш беруші ұсынған бастапқы кодтардың негізінде бастапқы кодты талдауға арналған бағдарламалық құралды пайдалана отырып жүргізіледі.

8. Бастапқы кодтарды талдау:

- 1) БҚ кемшіліктерін айқындауды;

2) бастапқы кодты талдау нәтижелерін белгілеуді қамтиды.

9. БҚ кемшіліктерін айқындау мынадай тәртіппен жүзеге асырылады:

1) бастапқы деректерді дайындау жүргізіледі («электрондық үкіметтің» ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелердің (бұдан әрі – АО) бастапқы кодтарын жүктеу, сканерлеу режимін (қарқынды және/немесе статикалық) таңдау, сканерлеу режимдерінің сипаттамаларын баптау);

2) БҚ кемшіліктерін айқындауға арналған бағдарламалық құрал іске қосылады;

3) жалған іске қосылулардың болуына бағдарламалық есептерді талдау жүргізіледі;

4) сипаттамасы, бағдары (файлға дейінгі жолы) мен тәуекел деңгейі (жоғары, орташа, төмен) көрсетілген БҚ айқындалған кемшіліктерінің тізбесін қамтитын есеп қалыптастырылады.

10. Бастапқы кодты талдау бойынша жұмыстардың көлемі бастапқы кодтың өлшемімен айқындалады.

11. Бастапқы кодтарды талдау нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін және Қағидаларға 5-қосымшаға сәйкес сынақ объектісінің бастапқы кодтарын қабылдау-беру актісін қоса бере отырып, бастапқы кодтарды талдау хаттамасында (еркін нысанда) тіркейді.

Қосымшаларымен және есеппен берілетін бастапқы кодтарды талдаудың:

1) аккредиттелген зертхана берген хаттамасы парақтарды бірыңғай нөмірлей отырып, тігіледі және мөр басылады (болған кезде);

2) мемлекеттік техникалық қызмет берген хаттамасы электрондық түрде өтініш берушінің SYNAQ интернет-порталының жеке кабинетінде орналастырылады.

Ескерту. 11-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

12. Бастапқы кодтарды талдау жүргізу аяқталғаннан кейін оның нәтижелері оң болған кезде сынақ объектісінің бастапқы кодтары таңбаланады және мөр басылған түрінде қызмет берушінің мұрағатына жауапты сақтауға тапсырылады.

13. Қызмет беруші сынақтар аяқталғаннан кейін олардың құпиялылығын кем дегенде үш жыл сақтай отырып, алынған бастапқы кодтарды сақтауды қамтамасыз етеді.

3-тарау. Ақпараттық қауіпсіздік функцияларын сынау

14. Ақпараттандыру объектілерінің функцияларын ақпараттық қауіпсіздік талаптарына сәйкестігіне бағалау (бұдан әрі – ақпараттық қауіпсіздік функцияларын сынау) олардың техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін бағалау мақсатында жүзеге асырылады.

15. Ақпараттық қауіпсіздік функцияларын сынау мыналарды қамтиды:

1) қауіпсіздік функцияларының техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін, соның ішінде бағдарламалық құралдарды пайдалана отырып (қажет болған кезде) бағалау;

2) сынақ нәтижелерін бақылау, сәйкестікті немесе сәйкессіздікті бағалау нәтижелері мен айқындалған сәйкессіздіктерді түзету жөніндегі ұсынымдар (қажет болған кезде) көрсетілген есепте тіркеу.

16. Ақпараттық қауіпсіздік функцияларының тізбесі осы Әдістемеге 1-қосымшада берілген.

17. Ақпараттық қауіпсіздік функцияларын сынау Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың 5-тармағының 1) тармақшасы мен 4) тармақшасының аталған серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі.

18. Ақпараттық қауіпсіздік функцияларын сынау нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, ақпараттық қауіпсіздік функцияларын сынау хаттамасында тіркейді (еркін нысанда).

Қосымшаларымен және есеппен берілетін ақпараттық қауіпсіздік функцияларын сынаудың:

1) аккредиттелген зертхана беретін хаттамасы парақтарды бірыңғай нөмірлей отырып, тігіледі және мөр басылады (болған кезде);

2) мемлекеттік техникалық қызмет беретін хаттамасы электрондық түрде өтініш берушінің SYNAQ интернет-порталындағы Жеке кабинетінде орналастырылады.

Бағдарламалық құралмен жаңартулардың және конфигурацияны талдаудың болуына сканерлеу нәтижелері Ақпараттық қауіпсіздік функцияларын сынау хаттамасына енгізіледі.

Бағдарламалық құралмен ақпараттық қауіпсіздікті қамтамасыз ету саласындағы стандарттарға сәйкестігіне сканерлеу нәтижелері Ақпараттық қауіпсіздік функцияларын сынау хаттамасына енгізілмейді, өтініш берушінің SYNAQ интернет-порталындағы жеке кабинетінде орналастырылады және ұсынымдық сипатта болады.

Ескерту. 18-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

4-тарау. Жүктемелік сынау

19. Жүктемелік сынау сынақ объектісінің қолжетімділігін, тұтастығын және құпиялылығын сақтауды бағалау мақсатында жүргізіледі.

20. Жүктемелік сынау дербес деректер жалған деректермен алмастырылған сынақ объектісін штаттық пайдалану ортасында автоматтандырылған сценарийлер негізінде мамандандырылған бағдарламалық құралды пайдалана отырып жүргізіледі.

21. Өтініш беруші жүктемелік сынау параметрлерін Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың 5-тармағының 9) тармақшасы мен 10) тармақшасының кестелерінде ұсынады.

Жүктемелік сынау жүргізу кезінде сынақ объектісінің нақты жүктемелік қабілеттілігінің параметрлері айқындалады.

22. Жүктемелік сынау мынадай тәртіппен жүзеге асырылады:

- 1) сынауға дайындық жүргізіледі;
- 2) сынақ жүргізіледі;
- 3) сынақ нәтижелері тіркеледі.

23. Сынауға дайындық мыналарды қамтиды:

- 1) сынау сценарийін анықтау;
- 2) сынаудың уақытша және сандық сипаттамаларын анықтау;
- 3) сынау жүргізу уақытын тапсырыс берушімен келісу.

24. Сынау жүргізу:

- 1) мамандандырылған бағдарламалық құралға сынау сценарийі мен конфигурациясын баптауды;
- 2) мамандандырылған бағдарламалық құралды іске қосуды;
- 3) сынақ объектісіне жүктеуді тіркеуді;
- 4) сынақ объектісінің нақты өткізу қабілетін жоғарылату немесе төмендету жөнінде ұсынымдар көрсете отырып, жүктемелік сынаудың есебін қалыптастыруды және беруді қамтиды.

25. Жүктемелік тестілеу жүргізу жөніндегі жұмыстар Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың 5-тармағының 9) тармақшасы мен 10) тармақшасының кестелерінде көрсетілген

бір сынақ объектісіне пайдаланушыларды қосу нүктелерінің нұсқалары мен сынақ объектісінің интеграциялық өзара іс-қимылын іске қосу нүктелерінің нұсқалар саны бойынша жүргізіледі.

26. Жүктемелік сынау нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, жүктемелік сынау хаттамасында тіркейді (еркін нысанда).

Қосымшаларымен және есеппен берілетін жүктемелік сынаудың:

1) аккредиттелген зертхана беретін хаттамасы парақтарды толассыз нөмірлей отырып, тігіледі және мөр басылады (болған кезде);

2) мемлекеттік техникалық қызмет беретін хаттамасы электрондық түрде өтініш берушінің SYNAQ интернет-порталындағы жеке кабинетінде орналастырылады.

Ескерту. 26-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

5-тарау. Желілік инфрақұрылымды зерттеп-қарау

27. Желілік инфрақұрылымды зерттеп-қарау желілік инфрақұрылымның қауіпсіздігін бағалау мақсатында жүргізіледі.

28. Желілік инфрақұрылымды зерттеп-қарау мыналарды қамтиды:

1) желілік инфрақұрылымның қорғалу функцияларының техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін бағалау;

2) өтініш берушінің желілік инфрақұрылымын, соның ішінде бағдарламалық құралдарды пайдалана отырып (қажет болған кезде) зерттеп-қарау;

3) бағдарламалық құралмен жалпы осалдықтар мен тәуекелдер базасынан бағдарламалық қамтылымның белгілі осалдықтары тұрғысынан сканерлеу;

4) алынған сынақ нәтижелерін бақылау, сәйкестікті немесе сәйкессіздікті бағалау нәтижелері мен айқындалған сәйкессіздіктерді түзету жөніндегі ұсынымдар (қажет болған кезде) көрсетілген есепте тіркеу.

29. Желілік инфрақұрылымның қорғалу функцияларының тізбесі осы Әдістемеге 2-қосымшада берілген.

30. Желілік инфрақұрылымды зерттеп-қарау бойынша жұмыстар Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың 5-тармағы 7) тармақшасының кестесінде көрсетілген сынақ объектісінің әрбір сегментіне (кіші желісіне) жүргізіледі.

31. Желілік инфрақұрылымды зерттеп-қарау нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, желілік инфрақұрылымды зерттеп-қарау хаттамасында тіркейді (еркін нысанда).

Қосымшаларымен және есеппен берілетін желілік инфрақұрылымды зерттеп-қараудың:

1) аккредиттелген зертхана беретін хаттамасы парақтарды толассыз нөмірлей отырып, тігіледі және мөр басылады (болған кезде);

2) мемлекеттік техникалық қызмет беретін хаттамасы электрондық түрде өтініш берушінің SYNAQ интернет-порталындағы жеке кабинетінде орналастырылады.

Ескерту. 31-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

6-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау

32. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау олардың ақпараттық қауіпсіздікті қамтамасыз ету саласындағы нормативтік құқықтық актілер мен стандарттардың талаптарына сәйкестігін бағалау мақсатында жүзеге асырылады.

33. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау мыналарды қамтиды:

1) ақпараттық қауіпсіздікті қамтамасыз ету процестерінің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы нормативтік құқықтық актілер мен стандарттардың талаптарына сәйкестігін бағалау;

2) бағалау нәтижелерін бақылау, сәйкестікті немесе сәйкессіздікті бағалау нәтижелері мен анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдар (қажет болған кезде) көрсетілген есепте тіркеу;

3) бағдарламалық құралдармен серверлерді, виртуалды ресурстар мен желілік жабдықты белгілі осалдықтар тұрғысынан сканерлеу;

4) жалған іске қосылулардың болуынан анықталған осалдықтарды талдау және олардың аса маңыздылығы деңгейіне байланысты оларды жою жөнінде ұсынымдар (қажет болған жағдайда) қалыптастыру.

Ескерту. 33-тармаққа өзгеріс енгізілді - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 01.04.2020 № 121/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

34. Ақпараттық қауіпсіздікті қамтамасыз ету процестерінің тізбесі және олардың мазмұны Әдістемеге 3-қосымшада берілген.

35. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау бойынша жұмыстар сынақ объектісіне жүргізіледі.

36. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау хаттамасында тіркейді (еркін нысанда).

Қосымшаларымен және есеппен берілетін ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қараудың:

1) аккредиттелген зертхана беретін хаттамасы парақтарды толассыз нөмірлей отырып, тігіледі және мөр басылады (болған кезде);

2) мемлекеттік техникалық қызмет беретін хаттамасы электрондық түрде өтініш берушінің SYNAQ интернет-порталындағы жеке кабинетінде орналастырылады.

Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау хаттамасына айқындалған осалдықтарды талдау нәтижелері енгізілмейді және Өтініш берушіге ұсынымдар нысанында беріледі.

Ескерту. 36-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

**«Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
әдістемесіне
1-қосымша**

Ақпараттық қауіпсіздік функцияларының тізбесі

Р /с №	Функциялардың атауы	Функциялардың мазмұны
1	2	3
Қауіпсіздік аудиті		
1	Қауіпсіздік аудитінің автоматты әрекет етуі	Тіркеу журналына жазба енгізуді, қауіпсіздікті бұзушылықты айқындау туралы әкімшіге локалдық немесе қашықтықтан сигнал беруді жүзеге асыру.
2	Қауіпсіздік аудитінің деректерін генерациялау	Хаттамалаудың, ең болмаса, тіркеу функцияларын іске қосу мен аяқтаудың, сондай-ақ аудиттің базалық деңгейіндегі барлық оқиғалардың болуы, яғни, әрбір тіркеу жазбасында оқиғаның мерзімі мен уақытының, оқиға түрінің, субъектіні сәйкестендіргіш пен оқиға нәтижесінің (сәт-тілігі немесе сәтсіздігі) болуы.
3	Қауіпсіздік аудитін талдау	Сәйкестендіру тетіктерін пайдаланудың ең болмаса, сәтсіз нәтижелерін, сондай-ақ криптографиялық операцияларды орындаудың сәтсіз нәтижелерін жинақтау және/немесе біріктіру арқылы (ықтимал кемшіліктерді айқындау мақсатында) жүзеге асыру.
4	Қауіпсіздік аудитін қарау	Барлық тіркеу ақпаратын қарау (оқу) мүмкіндігін қамтамасыз ету және әкімшіге беру. Өзге пайдаланушыларға тіркеу ақпаратына қолжетімділік айқын ерекше оқиғаларды қоспағанда, жабық болуы тиіс.
5	Қауіпсіздік аудитінің оқиғаларын таңдау	Оқиғаларды тіркеудің, ең болмаса, мынадай атрибуттарға негізделетін іріктеудің болуы: объектіні сәйкестендіргіш; субъектіні сәйкестендіргіш; желі торабының мекенжайы; оқиға түрі; оқиға мерзімі мен уақыты.
6	Қауіпсіздік аудитінің деректерін сақтау	Рұқсатсыз түрлендіруден сенімді қорғау туралы тіркеу ақпаратының болуы.
Байланысты ұйымдастыру		
7	Жіберуден бас тартпаушылық	Жіберуші куәлігі жіберуші мен жіберілген ақпарат арасындағы байланысты (мысалы, цифрлық қолтаңба) дәлелдейтін, ақпаратты жіберу фактісінен бас тартпауы үшін пайдаланушыларға/жіберушінің ұқсастығын куәландыру субъектілеріне кейбір ақпаратты беру.
8	Алудан бас тартпаушылық	Алушының ақпаратты алу фактісінен бас тарту мүмкінсіздігін қамтамасыз ету.

Криптографиялық қолдау		
9	Криптографиялық кілттерді басқару	Мыналарды қолдаудың болуы: 1) криптографиялық кілттерді құру; 2) криптографиялық кілттерді бөлу; 3) криптографиялық кілттерге қолжетімділікті басқару; 4) криптографиялық кілттерді жою.
10	Криптографиялық операциялар	Техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкес сенімді арна арқылы жіберілетін барлық ақпарат үшін тұтастығын шифрлаудың және бақылаудың болуы.
Пайдаланушының деректерін қорғау		
11	Қолжетімділікті басқару саясаты	Қауіпсіздік сервисімен тікелей немесе жанама операцияларды орындайтын пайдаланушылар үшін қолжетімділікті бөлуді жүзеге асыру.
12	Қолжетімділікті басқару функциялары	Қолжетімділікті бөлу функцияларын пайдалану, ең болмаса, мынадай қауіпсіздік атрибуттарына негізделуі тиіс: қол жеткізу субъектілерін сәйкестендіргіштер; қол жеткізу объектілерін сәйкестендіргіштер; қол жеткізу субъектілерінің мекенжайлары; қол жеткізу объектілерінің мекенжайлары; субъектілердің қол жеткізу құқықтары.
13	Деректерді теңестіру	Ақпараттың мазмұны айлакерлік жолымен ұқастырылмағанын немесе түрлендірілмегенін кейін тексеру үшін пайдаланылатын өзіндік деректер жинағының дұрыстығы кепілдігін қолдау.
14	Деректерді СО қауіпсіздік функцияларының (бұдан әрі – ОҚФ) әрекетінен тыс экспорттау	Пайдаланушының деректерін СО экспорттау кезінде оларды қорғау мен сақталуын немесе қауіпсіздік атрибуттарын ескермеуді қамтамасыз ету.
15	Ақпараттық ағындарды басқару саясаты	Пайдаланушының деректерін қауіпсіздік сервисінің физикалық бөлінген бөліктері арасында жіберген кезде оларды ашуға, түрлендіруге және/немесе қолжетімді болуына жол бермеуді қамтамасыз ету.
16	Ақпараттық ағындарды басқару функциялары	Деректер қоймасында қамтылған ақпаратты бақылаусыз таратуға жол бермеу мақсатында оған қолжетімділікті ұйымдастыру және қамтамасыз ету (БҚ сенімсіз болған жағдайда жариялаудан немесе түрлендіруден сенімді қорғауды іске асыру үшін ақпараттық ағындарды басқару).
17	Деректерді ОҚФ әрекетінен тыс жерден импорттау	Пайдаланушының деректерін олардың талап етілетін қауіпсіздік және қорғау атрибуттары болатындай етіп СО жіберуге арналған тетіктердің болуы.
18	СО шегінде жіберу	Пайдаланушының деректерін ішкі арна бойынша СО түрлі бөліктері арасында жіберген кезде қорғаудың болуы.
19	Қалған ақпаратты қорғау	Қалған ақпаратты толық қорғауды қамтамасыз ету, яғни ресурс босаған кезде алдыңғы жай-күйінің қолжетімсіздігін қамтамасыз ету.
20	Ағымдағы жай-күйін кері қалпына келтіру	Кейбір шектелген (мысалы, уақыт аралығымен) соңғы операцияны немесе бірқатар операцияны жою және алдыңғы белгілі жай-күйге қайту мүмкіндігінің болуы. Кері қалпына қайтару пайдаланушы деректерінің тұтастығын сақтау үшін операцияның немесе бірнеше операция нәтижелерін жоюға мүмкіндік береді.
21	Сақталатын деректердің тұтастығы	Пайдаланушының деректерін ОҚФ шегінде сақтаған кезде олардың қорғалуын қамтамасыз ету.
22	ОҚФ арасында жіберген кезде пайдаланушы деректерінің құпиялылығын қорғау	Пайдаланушының деректерін ОҚФ арасында сыртқы арна немесе АТ басқа сенімді өнімі бойынша жіберген кезде олардың құпиялылығын қамтамасыз ету. Құпиялылық деректерді екі соңғы нүкте арасында жіберген кезде оларға рұқсатсыз қол жеткізуді болдырмау жолымен жүзеге асырылады. Соңғы нүктелер ОҚФ немесе пайдаланушы бола алады.

23	ОҚФ арасында жіберген кезде пайдаланушы деректерінің тұтастығын қорғау	Пайдаланушының деректерін ОҚФ және АТ басқа сенімді өнімі арасында жіберген кезде олардың тұтастығы, сондай-ақ айқындалған қателер кезінде оларды қалпына келтіру мүмкіндігі қамтамасыз етілуі тиіс.
Сәйкестендіру және теңестіру		
24	Теңестіруден бас тарту	Сәтсіз теңестіру талаптарының белгілі санына келгенде әкімшінің субъектіге қол жеткізуге рұқсат бермеу, тіркеу журналына жазба енгізуді генерациялау мен әкімшіге қауіпсіздіктің ықтимал бұзушылық туралы сигнал беру мүмкіндігінің болуы.
25	Пайдаланушының атрибуттарын айқындау	Әрбір пайдаланушы үшін, ең болмаса, келесі қауіпсіздік атрибуттарын қолдау қажет: - сәйкестендіргіш; - теңестірілген ақпарат (мысалы, пароль); - қол жеткізу құқығы (рөлі).
26	Құпиялардың ерекшелігі	Егер теңестірілген ақпарат криптографиялық операциялармен қамтамасыз етілсе, сондай-ақ ашық және құпия кілттеріне қолдау көрсетілуі қажет.
27	Пайдаланушыны теңестіру	ОҚФ ұсынатын пайдаланушы теңестіру тетіктерінің болуы.
28	Пайдаланушыны сәйкестендіру	1) Қауіпсіздік сервисі осы пайдаланушының атынан орындайтын кез келген іс-қимыл аяқталғанға дейін әрбір пайдаланушы сәтті сәйкестендірілуге және теңестіруді; 2) Басқа пайдаланушыдан көшіріп алынған немесе ұқсастырып жасалған теңестірілген деректерді пайдалануға жол бермеу мүмкіндіктерін; 3) Пайдаланушының ұсынылған кез келген сәйкестендіргішін теңестіруді; 4) Әкімші белгілеген уақыт интервалы аяқталғаннан кейін пайдаланушыны қайтадан теңестіруді; 5) Теңестіруді орындаған кезде қауіпсіздік функциялары пайдаланушыға тек қана жасырын кері байланысқа рұқсат беруді қамтамасыз ету.
29	Пайдаланушы-субъект байланыстырушы	Пайдаланушының тиісті қауіпсіздік атрибуттарын осы пайдаланушы атынан әрекет ететін субъектілермен байланыстыру керек.
Қауіпсіздікті басқару		
30	ОҚФ жеке функцияларын басқару	Жұмыс істеу, ажырату, қосу, сәйкестендіру мен теңестіру режимдерін түрлендіру, қолжетімділік, хаттамалау және аудит құқығын басқару режимдерін анықтауға әкімшінің жеке құқығының болуы.
31	Қауіпсіздік атрибуттарын басқару	Қауіпсіздіктің түсіндірілетін мәндерін өзгертуге, сұрастыруға, атрибуттарын өзгертуге, жоюға, құруға әкімшінің жеке құқығының болуы. Бұл ретте, қауіпсіздік атрибуттарына тек қана қауіпсіздік мәндер беруді қамтамасыз ету қажет.
32	ОҚФ деректерін басқару	Тіркелетін оқиғалардың түсіндірілетін мәндерін өзгертуге, сұрастыруға, өзгертуге, жоюға, таза-лауға, түрлерін анықтауға, тіркеу журналдарының өлшемін, субъектілердің қол жеткізу құқықтарын, қол жеткізу субъектілерінің есептік жазбаларының, парольдерінің, криптографиялық кілттерінің жарамдылық мерзімдерін өзгертуге әкімшінің жеке құқығының болуы.
33	Қауіпсіздік атрибуттарын жою	Уақыттың кейбір сәттерінде қауіпсіздік атрибуттарын бұзуды жүзеге асырудың болуы. Пайдаланушылармен байланыстырылған қауіпсіздік атрибуттарын бұзу мүмкіндігі тек қана уәкілетті әкімшілерде болуы тиіс. Қауіпсіздік үшін маңызды өкілеттіктер дереу жойылуы тиіс.
34	Қауіпсіздік атрибутының қолданыс мерзімі	Қауіпсіздік атрибуттарының қолданыс мерзімін белгілеу мүмкіндігін қамтамасыз ету.
35	Қауіпсіздікті басқару рөлдері	1) Ең болмаса, мынадай рөлдерді қолдауды қамтамасыз ету: уәкілетті пайдаланушы, қашықтықтан пайдаланушы, әкімші; 2) Қашықтықтан пайдаланушы мен әкімші рөлдерін тек қана сұрау бойынша алуды қамтамасыз ету.
ОҚФ қорғау		
36		

	Іркіліс кезіндегі қауіпсіздік	Сервиспен аппараттық кідірістер кезінде (мысалы, электр қуатының іркілісінен орын алған) қауіпсіз жай-күйді сақтау.
37	ОҚФ экспортталатын деректерінің қолжетімділігі	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің қолжетімділігін тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер айқындалса, тіркеу журналына жазба енгізуді генерациялауға мүмкіндік беруге тиіс.
38	ОҚФ экспортталатын деректерінің құпиялылығы	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің құпиялылығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер анықталса, тіркеу журналына жазба енгізуді генерациялауға мүмкіндік беру.
39	ОҚФ экспортталатын деректерінің тұтастығы	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің тұтастығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер анықталса, тіркеу журналына жазба енгізуді генерациялауға мүмкіндік беру.
40	ОҚФ деректерін СО шегінде жіберу	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің қолжетімділігін, құпиялылығы мен тұтастығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер анықталса, тіркеу журналына жазба енгізуді генерациялауға мүмкіндік береді.
41	ОҚФ физикалық қорғау	ОҚФ физикалық қорғауды жүзеге асыру.
42	Сенімді қалыпқа келтіру	Кідірулер немесе қызмет көрсету тоқтатылғаннан кейін автоматты түрде қалпына келтіру мүмкін болмаса, сервис қауіпсіз жай-күйге қайтаруға мүмкіндік беретін авариялық қолдау режиміне ауысады. Аппараттық кідірістерден кейін автоматты рәсімдерді қолданумен қауіпсіз жай-күйге кері қайту қамтамасыз етіледі.
43	Екінші рет пайдалануды анықтау	Сервистің теңестірілген деректердің қайтадан пайдаланылуын айқындауын, қол жеткізуге жол бермеуге, тіркеу журналына жазба енгізуін және әкімшіге қауіпсіздіктің ықтимал бұзылуы туралы сигнал беруін қамтамасыз ету.
44	Өтініштер беру кезіндегі делдалдық	Сервистің қауіпсіздік саясатын жүзеге асыратын функциялар сервистің кез келген басқа функциясын орындауға рұқсат етілгенге дейін шақырылып, сәтті орындалуын қамтамасыз ету.
45	Доменді бөлу	Қауіпсіздік функциялары оларды сенімсіз субъектілердің араласуы мен бұрмалауынан қорғайтын меншікті орындауға арналған жеке доменді қолдап отыру.
46	Жай-күйлерді синхрондау хаттамасы	Серверлерде ұқсас функцияларды орындаған кезде жай-күйлерді синхрондауды қамтамасыз ету.
47	Уақыт белгілері	Қауіпсіздік функцияларының пайдалануына сенімді уақыт белгілерін ұсыну.
48	ОҚФ арасындағы деректердің келісілушілігі	Тіркелетін ақпаратты, сондай-ақ қолданылатын криптографиялық операциялар параметрлерін келісімді түсіндіруді қамтамасыз ету.
49	СО шегінде қайталау кезінде ОҚФ деректерінің келісілушілігі	СО түрлі бөліктерінде қайталаған кезде қауіпсіздік функциялары деректерінің үйлесімділігін қамтамасыз ету. Қайталанатын деректерді қамтитын бөліктер ажыратылғанда, үйлесімділік көрсетілген қауіпсіздік функцияларына кез келген сұрауларды өңдеу алдындағы қосылуды қалпына келтіргеннен кейін қамтамасыз етіледі.
50	ОҚФ өзін-өзі тестілеу	Іске қосу кезінде қауіпсіздік функциялары жұмысының дұрыстығын көрсету үшін қылыпты жұмыс процесінде және/немесе әкімшінің сұрауы бойынша мерзімді түрде өзін-өзі тестілеу пакетін орындау. Әкімшінің қауіпсіздік функциялары деректері мен орындалатын кодтың тұтастығын тексеру мүмкіндігі болуы тиіс.
Ресурстарды қолдану		
51	Істен шығуға қарсы тұрушылық	Кідірулер кезінде де сынақ объектісінің функционалдық мүмкіндіктерінің қолжетімділігін қамтамасыз ету. Осындай кідірістердің үлгілері: қуат көзін ажырату, аппаратураның жұмыс істемей қалуы, БҚ іркілісі.
52	Қызмет көрсетудің басымдылығы	Пайдаланушылардың немесе субъектілердің өздерінің әрекет ету аясында ресурстарды пайдалануын сынақ объектісі шегіндегі басымдылығы жоғары операциялар басымдылығы төмен операциялар жағынан кедергісіз және кідіріссіз орындалатын етіп басқаруды қамтамасыз ету.

53	Ресурстарды бөлу	Басқа пайдаланушылардың немесе субъектілердің ресурстарды монополиялауы себепті қызмет көрсетуден рұқсатсыз бас тартуға жол бермеу үшін пайдаланушылардың және субъектілердің ресурстарды пайдалануын басқаруды қамтамасыз ету.
СО-ға қолжетімділік		
54	Таңдалатын атрибуттардың аясын шектеу	Қолжетімділік әдісі немесе орны және/немесе уақыты негізінде (мысалы, тәулік уақыты, апта күні) қол жеткізу жүзеге асырылып отырған порттан пайдаланушы таңдай алатын қауіпсіздік атрибуттарымен қатар пайдаланушы байланыста болуы мүмкін субъектілердің атрибуттарын да шектеу.
55	Қатарлас сеанстарды шектеу	Бір пайдаланушыға ұсынылатын қатарлас сеанстардың барынша көп санын шектеу. Бұл шаманың ұйғарынды мәнін әкімші белгілейді.
56	Сеансты бұғаттау	Пайдаланушы әрекетсіздігі ұзақтығының әкімші белгілеген мәні аяқталғаннан кейін жұмыс сеансы мәжбүрлі аяқтау.
57	СО-ға қол жеткізуге рұқсат беру алдында алдын алу	Сәйкестендіруге және теңестіруге дейін әлеуетті пайдаланушылар үшін сынақ объектісінің пайдаланудың сипатына қатысты ескерту хабарламасын көрсету мүмкіндігін қамтамасыз ету.
58	СО-ға қолжетімділік тарихы	Сеансты сәтті ашқан кезде пайдаланушы үшін осы пайдаланушы атынан қолжетімділікті алудың сәтсіз әрекеттерінің тарихын алу мүмкіндігін қамтамасыз ету. Бұл тарих қол жеткізу мерзімін, уақытын, құралдарын және СО соңғы рет сәтті қолжетімділік портын, сондай-ақ сәйкестендірілген пайдаланушының соңғы сәтті қол жеткізуінен кейінгі СО сәтсіз қол жеткізу әрекеттерінің санын қамтуы мүмкін.
59	СО-мен сеансты ашу	Субъектіні сәйкестендіргішке, субъектінің пароліне, субъектінің қолжетімділік құқықтарына негізделе отырып, сервистің сеансты ашуға жол бермеуге қабілеттігін қамтамасыз ету.
Зиянды кодтан қорғау функциялары		
60	Вирустарға қарсы қорғау құралдарының болуы	Зиянды кодтан қорғану үшін серверлерден, қажеттілік туындаған жағдайда сынақ объектісінің жұмыс станцияларынан зиянды кодты анықтау және бұғаттау немесе жою, мониторинг құралдарын қолдану.
61	Вирустарға қарсы қорғау құралдарына арналған лицензия	Серверлерге және жұмыс станцияларына вирустарға қарсы қорғау құралдарының лицензиялары (сатып алынған, шектелген, еркін таратылатын) болуы тиіс.
62	Вирустарға қарсы қорғау сигнатуралары базасын және бағдарламалық қамтылымды жаңарту	Вирустарға қарсы қорғау құралдарының ұдайы жаңартылып, өзекті күйде болуын қамтамасыз ету.
63	Вирустарға қарсы қорғау құралдарына қолжетімділікті басқару	Вирустарға қарсы қорғау құралдарын орталықтандырылған басқару мен конфигурациялауды жүзеге асыру.
64	Сыртқы электрондық тасығыштардағы ақпаратты зиянды кодтан вирустарға қарсы құралдарымен қорғауды басқару	Сыртқы электрондық тасығыштардағы ақпаратты зиянды кодтан қорғау файлдардың, қажет болса ақпарат тасығыштардың тексерісін және бұғатталуын қамтамасыз ету.
БҚ жаңартылуы кезіндегі қауіпсіздік		
65	БҚ ұдайы жаңартылуы	Серверлер мен жұмыс станцияларының жалпыжүйелік және қолданбалы БҚ ұдайы жаңартылуын қамтамасыз ету.
66	Интернеттегі жаңарту серверлеріне рұқсатсыз желілік ортадағы БҚ жаңартылуы	Интернеттегі жаңарту серверлеріне рұқсатсыз желілік ортадағы БҚ мамандандырылған арнайы жаңарту серверінен жаңартылуын қамтамасыз ету.
Қолданбалы БҚ-ға өзгеріс енгізу кезіндегі қауіпсіздік		
67	Қолданбалы БҚ әзірлеу және тестілеу ортасы	Қолданбалы БҚ-ны өнеркәсіптік пайдалану ортасынан оқшауландырылған қолданбалы БҚ әзірлеу және тестілеу үшін ортаның болуын қамтамасыз ету.

68	Қолданбалы БҚ әзірлеу және тестілеу ортасына қол жеткізудің аражігін ажырату	Бағдарламашылар мен әкімшілер үшін қолданбалы БҚ әзірлеу және тестілеу орталарына қол жеткізуді басқаруын қамтамасыз ету.
69	Қолданбалы БҚ өрістету жүйесі	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ өрістету (тарату) жүйесінің болуы.
70	Қолданбалы БҚ өрістету жүйесіне қол жеткізудің аражігін ажырату	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ ажырату (тарату) жүйесіне қол жеткізуді басқаруды қамтамасыз ету.

**Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
әдістемесіне
2-қосымша**

Желілік инфрақұрылымды қорғау функцияларының тізбесі

р /с №	Функциялардың атауы	Функциялардың мазмұны
1	2	3
1	Сәйкестендіру және теңестіру	Уәкілетті персоналға қосу арқылы қолжетімділікті шектеу жолымен (ұйым ішінде немесе одан тыс жерде) желілік инфрақұрылым ұсынатын сервистердің қауіпсіздігін және тиісті деректердің сақталуын қамтамасыз ету.
2	Аудиттерді белгілеу (желілік қосылулардың қауіпсіздігіне байланысты оқиғалар туралы есептер қалыптастыру және олардың бар болуы)	Күдікті және нақты оқиғаларды мұқият шолу мүмкіндігінің болуы үшін аудитті жүргізу барысындағы іркіліс жағдайлары мен нақты оқиғалары бойынша жеткілікті ақпаратты белгілеу керек.
3	Басып кіруді анықтау	Басып кіруді болжауға (телекоммуникация желілеріне ықтимал басып кіру), оларды нақты уақыт масштабында айқындауға және тиісті алаңдаушылықты туғызуға мүмкіндік беретін құралдардың бар болуын қамтамасыз ету.
4	Желілік қауіпсіздікті басқару	Дистанционды диагностиканың барлық порттарына (виртуалды және физикалық) заңсыз қол жетімділіктен сақтануды қамтамасыз ететін желілік ресурстарды қорғауды басқару бойынша шаралардың болуы. Желілер арасындағы байланыс үшін қауіпсіздік шлюздерінің болуы.
5	Желіаралық экрандар	Әрбір желіаралық экран үшін сервистерге қолжетімділік саясатын (қауіпсіздік) белгілейтін жеке құжат әзірлеу және осы қосылу арқылы тек қана рұқсат етілген трафиктің өтуіне кепілдік беру үшін оны әрбір қосылуда жүзеге асыру қажет.
6	Желілер арқылы жіберілетін деректердің тұтастығын, құпиялығын сақтау	Деректер құпиялығын және тұтастығын сақтау маңызды болған жағдайларда желілік қосылым арқылы өтетін ақпаратты шифрлау үшін қорғаныстың криптографиялық шараларын көздеген жөн.
7	Ақпарат алмасу бойынша жасалған іс-қимылдардан бас тартпаушылық	Ақпаратты желі бойынша жіберудің растауын ұсыну талап етілетін жағдайда, мынадай қорғау шараларын қолданылды: 1) құжатты жіберу фактісін растайтын байланыс хаттамалары; 2) бастапқы адресті немесе сәйкестендіргішті ұсынуды және аталған ақпараттың бар болуын тексеруді талап ететін қосымшалардың хаттамалары; 3) жіберуші мен алушы мекенжайларының форматтары синтаксистің дұрыстығына және тиісті директориалардағы ақпаратпен үйлесімділікке қатысты тексерілетін желіаралық экрандар;

		4) желіаралық өзара іс-қимыл шеңберінде ақпаратты жеткізу фактілерін растайтын хаттамалар; 5) ақпараттың реттілігін белгілеуге рұқсат беретін тетіктерді қамтитын хаттамалар.
8	Үздіксіз жұмыс және қалыпқа келуді қамтамасыз ету	Әрбір іскерлік операцияның үзілуден кейінгі керекті уақыт интервалында қалыпқа келу қабілетін қамтамасыз ету жолымен төтенше жағдайлар кезіндегі үзілген бизнес функцияларының жалғасуын қамтамасыз ететін қорғаныс шараларының болуы.
9	Сенімді арна	1) Қашықтықтағы сенімді АТ-өнімімен байланыс үшін қауіпсіздік функциялары басқалардан логикалық ерекшеленетін және оның тараптарының сенімді теңестірудің, сондай-ақ деректерді түрлендіру мен ашудан қорғауды қамтамасыз ететін арна ұсыну; 2) сенімді арна арқылы екі тараптарда байланыстарды бастамалауға мүмкіндікті қамтамасыз ету.
10	Сенімді бағдар	1) Қашықтықтағы пайдаланушымен байланыс үшін қауіпсіздік функциялары басқалардан логикалық ерекшеленетін және оның тараптарының сенімді теңестіретін, сондай-ақ деректерді түрлендіру мен ашудан қорғауды қамтамасыз ететін арна ұсыну; 2) Пайдаланушының байланыстарды сенімді арна арқылы бастамалауға мүмкіндікті қамтамасыз ету; 3) Қашықтықтағы пайдаланушы мен қашықтықтан басқаруды бастапқы аутентификациялау үшін сенімді бағдарды пайдалану міндетті болып табылады.

**Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
әдістемесіне
3-қосымша**

**Ақпараттық қауіпсіздікті қамтамасыз ету процестерінің тізбесі мен олардың
мазмұны**

Р /с №	Процестердің атауы	АҚ қамтамасыз ету процестерінің мазмұнына қойылатын талап
1	2	3
1	Ақпараттық-коммуникациялық технологиялармен байланысты активтерді басқару	1. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және маркалау қағидаларында айқындалған активтерді сәйкестендіру тәртібіне сәйкес активтерді сәйкестендіру; 2. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және маркалау қағидаларында айқындалған сыныптау жүйесіне сәйкес ақпаратты сыныптау; 3. Ақпараттандыру объектілерін сыныптау қағидаларының талаптарына сәйкес сынақ объектісіне айқындалған сыныпты тексеру; 4. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және маркалау қағидаларында айқындалған маркалау қағидаттарына сәйкес активтерді маркалау; 5. Сәйкестендірілген активтерге жауапты тұлғаларды бекіту; 6. Активтер тізілімін қабылданған тізілім нысанына сәйкес жүргізу және өзектілендіру; 7. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және маркалау қағидаларында айқындалған сыныптау жүйесіне сәйкес активтермен жұмыс істеу (беру, пайдалану, сақтау, енгізу/шығару және қайтару) рәсімдерін айқындау, құжаттау және іске асыру; 8. Есептеу техникасы құралдарын, телекоммуникациялық жабдықты және бағдарламалық қамтылымды паспорттандыру; 9. Ақпараттық-коммуникациялық технологиялармен байланысты активтерді қабылдап алу/тиееу кезінде жұмыстарды қауіпсіз ұйымдастыру; 10. Серверлік және телекоммуникациялық жабдықты, деректерді сақтау жүйелерін, жұмыс станцияларын, ақпарат тасымалдауыштарды қауіпсіз кәдеге жарату (қайта пайдалану).
2	Ақпараттық қауіпсіздікті ұйымдастыру	1. Ақпараттық технологиялар бөлімшесінен жекеленген жоғары басшылыққа тікелей бағынысты ақпараттық қауіпсіздік бөлімшесінің немесе ақпараттық қауіпсіздікке жауапты қызметкердің болуы; 2. Ақпараттық қауіпсіздікті қамтамасыз ету және жұмыстарды үйлестіру мәселелері жөніндегі жұмыс топтарының жұмыс істеуі мен кеңестер өткізу; 3. Ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманы әзірлеу (өзектілендіру), басшылықтың бекітуі, мақұлдауы, олардың мазмұнын қызметкерлерге және сырттан тартылатын орындаушыларға жеткізу;

		4. Уәкілетті органдармен, кәсіптік қоғамдастықтармен, кәсіптік қауымдастықтармен немесе ақпараттық қауіпсіздік жөніндегі мамандардың форумдарымен байланыстарды қолдап отыру; 5. Сыртқы ұйымдарды тарту кезінде ақпараттық қауіпсіздікті қамтамасыз ету рәсімдерін айқындау мен құжаттау; 6. Ақпаратты қорғау қажеттілігі көрсетілетін құпиялылық немесе жарияламау туралы келісімдерді әзірлеу (қайта қарау); 7. Ақпараттық қауіпсіздік және қызмет көрсету деңгейі жөніндегі талаптарды айқындау мен сыртқы ұйымдармен жасалатын келісімдерге енгізу. Келісім ережелерінің іске асырылуын бақылау.
3	Персоналға байланысты қауіпсіздік	1. Жұмысқа қабылдау кезінде үміткерлерді алдын ала тексеру; 2. Жұмыспен қамту, еңбек қатынастарын өзгерту немесе тоқтату кезеңінде қызметкерлердің және сырттан тартылатын орындаушылардың ақпараттық қауіпсіздікке байланысты рөлдерін, міндеттері мен жауапкершілігін және сынақ объектісі иеленушісінің міндеттемелерін айқындау, тағайындау және олардың лауазымдық нұсқаулықтарында және (немесе) еңбек шартының талаптарында көрсету; 3. Ақпараттық қауіпсіздікті қамтамасыз ету саласында міндеттемелері бар қызметкерлерді жұмыстан босату рәсімдерін анықтау және құжаттау; 4. Ақпараттық қауіпсіздік қағидаларын бұзушыларға қолданылатын іс-әрекеттерді айқындау мен регламенттеу; 5. Қызметкерлерді ақпараттық қауіпсіздікті қамтамасыз ету саясаттарындағы, қағидаларындағы және рәсімдеріндегі олардың қызметтік міндеттерін орындауды қозғайтын өзгерістер туралы хабардар ету; 6. Жұмыспен қамту, еңбек қатынастарын өзгерту немесе тоқтату кезеңінде қызметкерлердің және сырттан тартылатын орындаушылардың ақпараттық қауіпсіздікті қамтамасыз етуге байланысты міндеттері мен жауапкершілігі туралы хабардарлығы және оларды орындауы; 7. Ақпараттық қауіпсіздік саласында қызметкерлерді оқыту және даярлау; 8. Қызметкерлердің және сырттан тартылатын орындаушылардың ақпараттық қауіпсіздікке қатысты міндеттемелерін орындау мүмкіндігін қамтамасыз ету үшін басшылықтың жауаптылығы.
4	АҚ оқиғаларының мониторингі және АҚ оқыс оқиғаларын басқару	1. Пайдаланушылардың, операторлардың, әкімшілердің іс-қимылдарын және операциялық жүйелердің, дерекқорын басқару жүйелерінің, вирусқа қарсы БҚ, қолданбалы БҚ, телекоммуникациялық жабдықтың, шабуылдарды айқындау мен болдырмау жүйелерінің, контентті басқару жүйесінің оқиғаларын тіркеу; 2. Оқиғаларды тіркеу журналдарын жүргізу, сақтау және қорғау; 3. Оқиғаларды тіркеу журналдарының талдауын жүзеге асыру; 4. Тіркелген оқиғалардың мониторингін жүргізіп, ақпараттық қауіпсіздік үшін маңыздылық дәрежесі жоғары және аса маңызды оқиғалар туралы хабарлау; 5. Ақпараттық қауіпсіздік оқиғасын бағалау және ол бойынша шешім қабылдау; 6. Ақпараттық қауіпсіздік оқыс оқиғаларына әрекет ету рәсімдерін әзірлеу, құжаттау, қызметкерлердің және сырттан тартылатын орындаушылардың назарына жеткізу, орындау; 7. Ақпараттық қауіпсіздік оқыс оқиғаларының талдауын жүргізу.
5	АҚ үздіксіздігін басқару	1. Ақпараттық қауіпсіздіктің үздіксіздігін жоспарлау; 2. Ақпараттық қауіпсіздікті қамтамасыз ету процесінің немесе бизнес процестердің үздіксіздігін бұзудың ықтимал себебі болып табылатын оқиғаларды сәйкестендіру; 3. Штаттан тыс (дағдарысты) жағдайларда ақпараттық қауіпсіздік үздіксіздігінің қажетті деңгейін қолдап отыру процестері мен рәсімдерін әзірлеу (өзектілендіру) және енгізу; 4. Штаттан тыс (дағдарысты) жағдайлар кезіндегі рәсімдерді айқындау, құжаттау, қызметкерлердің және сырттан тартылатын орындаушылардың назарына жеткізу, орындау; 5. Ақпараттық қауіпсіздіктің үздіксіздігін қамтамасыз ету процестері мен рәсімдерін тексеру (тестілеу), талдау және бағалау; 6. Заңнама талаптарын ескере отырып, ақпаратты өңдеу құралдарын, ақпараттандыру объектісін резервілеу.
6	Желілік қауіпсіздікті басқару	1. Желілік қауіпсіздікті басқару рәсімдерін айқындау, құжаттау, қызметкерлердің және сырттан тартылатын орындаушылардың назарына жеткізу, орындау;

		2. Барлық желілік қызметтер мен сервистердің қауіпсіздігін, қолжетімділік деңгейлерін қамтамасыз ету механизмдерін анықтау және желілерге қызмет көрсету мен ақпаратты беру жөніндегі келісімдерге енгізу; 3. Желілер мен желілік қызметтерді пайдалану, ақпаратты жіберу, Интернетке, телекоммуникация және байланыс желілеріне қосылу мен желілік ресурстарға сымсыз қолжетімділікті пайдалану саясаттарын және рәсімдерін айқындау, құжаттау, қызметкерлердің және сырттан тартылатын орындаушылардың назарына жеткізу, орындау; 4. Желі арқылы жіберілетін ақпарат пен электрондық хабарламаларды қорғау құралдарын қолдану бойынша рәсімдерді айқындау, құжаттау және орындау; 5. Желіні құрылымдау мен сегменттеу; 6. Желіні қосу және өзара іс-қимылының заңнама талаптары ескерілген әдістері.
7	Криптографиялық қорғау әдістері	1. Криптографиялық кілттерді жасау, есепке алу, сақтау, беру, пайдалану, қайтару (жою), қорғау мәселелерін қамтитын криптографиялық кілттерді басқарудың заңнама талаптары ескеріліп реттелуі; 2. Аутентификация деректерін қоса алғанда, ақпаратты сақтау және беру кезінде криптографиялық құралдарды пайдалану.
8	Ақпараттық қауіпсіздік тәуекелдерін басқару	1. Тәуекелдерді басқару әдістемесін таңдау; 2. Сәйкестендірілген және сыныпталған активтердің қатерлерін (тәуекелдерін) сәйкестендіру және ақпараттық қауіпсіздік қатерлерінің (тәуекелдерінің) каталогын қалыптастыру (өзектілендіру). Ақпараттық қауіпсіздікті қамтамасыз ету процестеріне байланысты тәуекелдерді қатерлер (тәуекелдер) каталогында көрсету; 3. Сәйкестендірілген тәуекелдерді бағалау (қайта бағалау); 4. Тәуекелдерді өңдеу, тәуекелдерді өңдеу жоспарын қалыптастыру және бекіту (өзектілендіру); 5. Тәуекелдердің мониторингін жүргізу және қайта қарау.
9	Қолжетімділікті басқару	1. Ақпаратқа, қолданбалы жүйелердің функцияларына, қызметтерге, жүйелік БҚ, желілер мен желілік сервистерге қол жеткізу құқықтарын бөлу қағидаларын әзірлеу (өзектілендіру), құжаттау, пайдаланушыларды таныстыру; 2. Пайдаланушыларды авторландырудың және аутентификациялаудың, сәйкестендірудің қолданыстағы әдістері мен рәсімдері; 3. Электрондық ақпараттық ресурстарға қол жеткізу құқығының аражігін ажырату қағидаларында белгіленген қол жеткізу рұқсатының аражігін ажырату қағидаларын жүзеге асыру; 4. Пайдаланушыларды тіркеу және тіркеуді (бұғаттауды) жою рәсімдері; 5. Қол жеткізу құқықтары артықшылықты есептік жазбаларды басқару; 6. Пайдаланушылардың аутентификациясы рәсімдерінде криптографиялық әдістерді қолдану және басқару; 7. Қол жеткізу құқықтарын өзгертулерді басқару; 8. Парольдерді басқару; 9. Артықшылықты утилиталарды пайдалану; 10. Сынақ объектісінің бастапқы кодына қол жеткізуді басқару.
10	Физикалық қауіпсіздік және табиғи қатерлерден қорғау	1. Заңнама талаптарын ескере отырып, серверлік, телекоммуникациялық жабдықты, деректерді сақтау жүйелерін орналастыру; 2. Ақпараттық-коммуникациялық технологиялармен байланысты активтер орналастырылған орынжайлардың қауіпсіздік периметрін физикалық қорғау; 3. Негізгі және резервтік серверлік орынжайлардың заңнама талаптары ескеріліп ұйымдастырылуы; 4. Негізгі және резервтік серверлік орынжайлардың қамтамасыз ету жүйелерімен заңнама талаптары ескеріліп жаратқандырылуы; 5. Серверлік орынжайларға бақыланбалы кіруді ұйымдастыру; 6. Серверлік орынжайдағы жұмысты ұйымдастыру; 7. Серверлік және телекоммуникациялық жабдықты, деректерді сақтау жүйелері мен қамтамасыз ету жүйелерін техникалық қолдап отыру және қызмет көрсету жөніндегі жұмыстарды ұйымдастыру;

		8. Электр энергиясымен жабдықтау жүйесіндегі тоқтап қалулар мен коммуналдық қызметтердің жұмысындағы кідірулерден туындайтын басқа да бұзылулардан жабдықты қорғау тәсілдері; 9. Кәбіл жүйесінің қауіпсіздігін қамтамасыз ету.
11	АҚ қамтамасыз етуді пайдалану рәсімдері	1. Ақпараттық қауіпсіздікті қамтамасыз етуді пайдалану рәсімдерін регламенттейтін нұсқалуықтарды әзірлеу (өзектілендіру), құжаттау, пайдаланушыларды таныстыру; 2. Ақпараттық қауіпсіздікті қамтамасыз ету құралдары мен жүйелерін пайдалану; 3. Ақпаратты резервтік көшіру рәсімдері және көшіру нәтижелерін тестілеу. Резервтік көшірмелерді сақтау орындарының қауіпсіздігі; 4. Оқиғаларды тіркеу журналдарының уақытын бірыңғай уақыт көзімен синхрондау; 5. Пайдаланылатын жүйелерде қолданбалы және жүйелік БҚ жаңа нұсқаларын орнату кезінде өзгерістерді басқару рәсімдері; 6. БҚ осалдықтарын бақылау және басқару; 7. Қызметкерлерді мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану қағидаларының ережелерімен таныстыру және оларды іске асыру; 8. Қашықтықтан жұмыс істеуді ұйымдастыру жөніндегі нұсқаулықты әзірлеу (өзектілендіру), қызметкерлерді таныстыру, оның ережелерін іске асыру; 9. Сынақ объектісінің жұмысқа қабілеттілігін мониторингтеу; 10. Әзірлеу, тестілеу және пайдалану орталарын бөлу; 11. Электрондық пошта хабарламаларын және ақпаратты Интернет арқылы жіберу кезінде құпиялықты қамтамасыз ету; 12. Заңнама талаптарына сәйкес Интернетті беру және сыртқы электрондық пошталық жүйелермен өзара іс-қимыл әдістері; 13. Интернет ресурстарына қол жеткізу кезіндегі шектеулер және фильтрлеу тәртібі.
12	Заңнама және шарттық талаптарға сәйкестік	1. Сынақ объектісіне қойылатын заңнама, нормативтік, өзге міндетті, шарттық талаптарды айқындау (өзектілендіру), құжаттау; 2. Зияткерлік меншікке берілетін құқықтарға байланысты заңнама, нормативтік және шарттық талаптарға сәйкестікті іске асыратын рәсімдерді енгізу; 3. Заңнама талаптарына сәйкес келетін құпия және дербес деректерді қорғау саясаттарын әзірлеу мен іске асыру; 4. Қолданылатын криптографиялық әдістер мен құралдардың заңнама талаптарына және келісімдерге (шарттарға) сәйкестігі; 5. Ақпараттық қауіпсіздік аудитін жүргізу; 6. Сынақ объектісіне ақпараттық қауіпсіздік бойынша заңнама, стандарттар мен техникалық құжаттама талаптарына сәйкестігіне талдау жүргізу; 7. Заңнама, нормативтік және шарттық талаптарға сәйкес жазбаларды зақымдаудан, бұрмалаудан, заңсыз қол жеткізуден және заңсыз шығарудан қорғау.
13	Жүйелерді сатып алу, әзірлеу және оларға қызмет көрсету	1. Сынақ объектісіне арналған техникалық құжаттаманың құрамына ақпараттық қауіпсіздікке байланысты және қолданыстағы заңнама мен стандарттарға сәйкес келетін талаптарды енгізу (өзектілендіру); 2. Пайдаланылатын жүйелерге арналған БҚ (жүйелік және қолданбалы) өзгерістерін басқарудың қауіпсіз рәсімдерін айқындау және қолдану; 3. Сыртқы ұйым жүзеге асыратын сынақ объектісінің БҚ әзірлеу процесін бақылау; 4. Сыртқы ұйым жүзеге асыратын жүйені техникалық қолдап отыру процесін бақылау; 5. Жүйенің қауіпсіздік функцияларын тестілеу.

Қазақстан Республикасы
Цифрлық даму, қорғаныс
және аэроғарыш
өнеркәсібі министрінің
2019 жылғы 3 маусымдағы
№ 111 бұйрығына
2-қосымша

«Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары

Ескерту. Қағидалар жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 01.04.2020 № 121/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы «Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары (бұдан әрі – Қағидалар) «Ақпараттандыру туралы» Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 5) тармақшасына және «Мемлекеттік көрсетілетін қызметтер туралы» Қазақстан Республикасы Заңының (бұдан әрі – «Мемлекеттік көрсетілетін қызметтер туралы» Заң) 10-бабының 1) тармақшасына сәйкес әзірленді және «электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібін айқындайды.

Ескерту. 1-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

2. Осы Қағидаларда мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) ақпараттық жүйе – ақпараттық өзара іс-қимыл арқылы белгілі технологиялық іс-қимылдарды іске асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсететін персонал мен техникалық құжаттаманың ұйымдастырушылық ретке келтірілген жиынтығы;

2) ақпараттық жүйенің кіші жүйесі – ақпараттық жүйенің мақсатына қол жеткізу үшін қажетті, оның белгілі бір функцияларын іске асыратын, ақпараттық жүйенің жиынтық бөлігі (кұрауышы);

3) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – АҚ) – электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалу жай-күйі;

4) ақпараттық қауіпсіздік жөніндегі техникалық құжаттама (бұдан әрі – АҚ жөніндегі ТҚ) – Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға сәйкес әзірленген және сынақ объектісінің ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жалпы талаптарды, қағидаттар мен қағидаларды регламенттейтін құжаттар жиынтығы;

5) бағдарламалық қамтылым – бағдарламаларды, бағдарламалық кодтарды, сондай-ақ техникалық құжаттамаларды пайдалану үшін қажетті өнімдердің жиынтығы;

6) бағдарламалық өнім – әзірлеушілеріне қарамастан, техникалық құжаттамада белгіленген жүйелік талаптарға сәйкес көзделген мақсаттарда пайдаланылуы мүмкін, тауар болып табылатын дербес бағдарлама немесе бағдарламалық қамтылымның бір бөлігі;

7) бастапқы кодтар – сынақ объектісінің компакт-дискіде сәтті компиляциялануы үшін файлдар мен кітапханаларды қоса алғанда сынақ объектісінің модульдері мен компоненттерінің бастапқы кодтары;

8) бөлінген сынақ объектісі – бірдей архитектура бойынша құрылған, бірдей мақсаттарға арналған, бірдей функциялар атқаратын және бірдей қолданбалы бағдарламалық қамтылымды пайдаланатын көптеген, соның ішінде белгісіз, тораптардан тұратын сынақ объектісі;

9) интернет-ресурс – бірегей желілік мекенжайы және (немесе) домендік атауы бар және Интернетте жұмыс істейтін аппараттық-бағдарламалық кешенде орналастырылған ақпарат (мәтіндік, графикалық, аудиовизуалды немесе өзге түрде).

10) қызмет беруші – мемлекеттік техникалық қызмет немесе аккредиттелген сынақ зертханасы;

11) мемлекеттік техникалық қызмет – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған акционерлік қоғам;

12) өтініш беруші – сынақ объектісінің меншік иесі немесе иеленушісі, сондай-ақ сынақ объектісінің меншік иесі немесе иеленушісі өкілеттік берген ақпараттандыру объектісінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізуге өтініш берген жеке немесе заңды тұлға;

13) сынақ зертханасы – сынақтарды жүзеге асыратын, техникалық реттеу туралы заңнамаға сәйкес аккредиттелген заңды тұлға немесе оның атынан әрекет ететін заңды тұлғаның құрылымдық бөлімшесі;

14) сынақ объектісі – оған қатысты ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтан өткізу жөніндегі жұмыстар жүргізілетін ақпараттандыру объектісі;

15) штаттық пайдалану ортасы – ақпараттандыру объектісін тәжірибелік пайдалану (пилоттық жоба) кезеңінде қолданылатын және өнеркәсіптік пайдалану кезеңінде қолдануға арналған серверлік жабдықтың, желілік инфрақұрылымның, жүйелік бағдарламалық қамтылымның нысаналы жиынтығы;

16) «электрондық үкіметтің» ақпараттық-коммуникациялық платформасы – мемлекеттік органның қызметін автоматтандыруға, оның ішінде мемлекеттік функцияларды автоматтандыруға және олардан туындайтын мемлекеттік

қызметтерді көрсетуге, сондай-ақ мемлекеттік электрондық ақпараттық ресурстарды орталықтандырылған жинауға, өңдеуге, сақтауға арналған технологиялық платформа;

17) SYNAQ интернет-порталы – «электрондық үкіметтің» ақпараттандыру объектілерін және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерді ақпараттық қауіпсіздік талаптарына сәйкестігіне сынау бойынша қызмет көрсету процесін автоматтандыруға арналған мемлекеттік техникалық қызметтің интернет-порталы.

Ескерту. 2-тармаққа өзгеріс енгізілді - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 28.09.2020 № 356/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрықтарымен.

3. Ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтар міндетті түрде немесе меншік иесінің немесе иеленушінің бастамасы бойынша жүргізіледі.

4. Ақпараттық қауіпсіздік талаптарына сәйкестігін міндетті сынауға жататын сынақ объектілеріне:

1) «электрондық үкіметтің» ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылым (бағдарламалық өнім);

2) «электрондық үкіметтің» ақпараттық-коммуникациялық платформасы;

3) мемлекеттік органның, мемлекеттік заңды тұлғаның, квазимемлекеттік сектор субъектісінің интернет-ресурсы;

4) мемлекеттік органның, мемлекеттік заңды тұлғаның, квазимемлекеттік сектор субъектісінің ақпараттық жүйесі;

5) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері;

6) мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға, мемлекеттік функцияларды жүзеге асыруға және мемлекеттік қызметтерді көрсетуге арналған мемлекеттік емес ақпараттық жүйе жатады.

Ескерту. 4-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

5. Қазақстан Республикасы ұлттық куәландырушы органының электрондық цифрлық қолтаңбаның түпнұсқалылығын тексеру бойынша сервистерін пайдалануға арналған мемлекеттік органның ақпараттық жүйесі мен мемлекеттік емес ақпараттық жүйесіне ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтан өту талап етілмейді.

6. Объектілерді АҚ талаптарына сәйкестікке сынақтар (бұдан әрі – сынақтар) өткізу объектілерінің техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін бағалау бойынша жұмыстарды қамтиды және сынақтар объектісін пайдаланудың штаттық ортасында жүргізіледі.

7. «Электрондық үкіметтің» ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (бағдарламалық өнімді) және «электрондық үкіметтің» ақпараттық-коммуникациялық платформасын қоспағанда, сынақ объектілерін сынақтан өткізудің құрамына мынадай жұмыс түрлері кіреді:

- 1) бастапқы кодтарды талдау;
- 2) ақпараттық қауіпсіздік функцияларын сынау;
- 3) жүктемелік сынау;
- 4) желілік инфрақұрылымды зерттеп-қарау;
- 5) АҚ қамтамасыз ету процестерін зерттеп-қарау.

Ескерту. 7-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

8. Сынақ объектісінің бастапқы коды болмаған немесе сынақтардың басқа түр(лер)ін жүргізу мүмкін болмаған жағдайда, сынақ объектісінің бастапқы кодына талдау немесе сынақтардың басқа түр(лер)ін жүргізудің міндетті еместігі

туралы шешім өтінім берушінің сұрау салуы Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті (бұдан әрі – Комитет) шешімімен белгіленеді.

Комитет орган осы Қағидаларға 7-тармаққа сәйкес сынақтардың басқа түрлерін жүргізу кезеңінде өтініш берушінің сынақ объектісінің бастапқы кодына талдау немесе сынақтардың басқа түр(лер)ін жүргізбеу туралы сұрау салуының негізділігін тексеру туралы қызмет берушіге тапсырма беруге құқылы.

9. «Электронды үкіметтің» ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (бағдарламалық өтінімді) сынауға:

- 1) бастапқы кодтарды талдау;
- 2) ақпараттық қауіпсіздік функцияларын сынау;
- 3) жүктемелік сынау кіреді.

Ескерту. 9-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

10. «Электрондық үкіметтің» ақпараттық-коммуникациялық платформасын сынақтан өткізуге:

- 1) бастапқы кодтарды талдау;
- 2) ақпараттық қауіпсіздік функцияларын сынау;
- 3) желілік инфрақұрылымын зерттеп-қарау;
- 4) АҚ қамтамасыз ету процестерін зерттеп-қарау кіреді.

11. Біртекті бөлінген сынақ объектілеріне сынақтар бөлінген сынақ объектісінің орталық торап(тар)ы мен бөлінген сынақ объектісі тораптарының жалпы санының оннан бір бөлігінен кем емес санын құрайтын кейбір (өтініш берушімен келісу бойынша) жеке тораптары үшін жүргізіледі.

Біртекті бөлінген сынақ объектісінің орталық торап(тар)ы үшін сынақтар жұмыс түрлерінің толық құрамымен жүргізіледі.

Біртекті бөлінген сынақ объектісінің тораптары үшін жүргізілетін сынақтардың құрамына:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау кіреді.

12. Мемлекеттік техникалық қызмет «электрондық үкіметтің» ақпараттандыру объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақ жүргізеді.

13. Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне («электрондық үкіметтің» ақпараттандыру объектілері болып табылатындарды қоспағанда) жатқызылған ақпараттық жүйенің және «электрондық үкіметтің» ақпараттандыру объектілеріне жатқызылмаған өзге ақпараттандыру объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтарды аккредиттелген сынақ зертханалары жүргізеді.

14. Сынақ объектісінің басқа ақпараттандыру объектісімен интеграциялануы (қолданыстағы немесе жоспарлы) жағдайында, сынақтар сынақ объектісінің құрамына интеграциялауды қамтамасыз ететін компоненттер енгізу (интеграциялау модулі, ішкі интеграциялау жүйесі, интеграциялық шина немесе басқа) арқылы жүргізіледі.

2-тарау. Ақпараттандыру объектілеріне ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтарды мемлекеттік техникалық қызметте жүргізу тәртібі

15. Сынақтарды жүргізу үшін өтініш беруші SYNAQ интернет-порталында осы Қағидаларға 1-қосымшаға сәйкес нысан бойынша сынақтар жүргізуге өтінімді (бұдан әрі – өтінім) толтырады, электрондық цифрлық қолтаңбамен (бұдан әрі – ЭЦҚ) қол қояды және мынадай құжаттарды қоса бере отырып, мемлекеттік техникалық қызметке береді:

1) SYNAQ интернет-порталында сынақ объектісі меншік иесінің (иеленушісінің) ЭЦҚ арқылы куәландырылған осы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық;

2) шарттарға қол қоюға өкілеттік берілген тұлғаның атына сенімхаттың немесе заңды тұлғаның басшысын тағайындау туралы құжаттың электрондық көшірмесі (заңды тұлғалар үшін);

3) меншік иесі немесе иеленушісі бекіткен ақпараттандыру объектісіне арналған техникалық тапсырма немесе техникалық ерекшелігінің электрондық көшірмесі;

4) сәтті компиляция үшін қажетті сынақ объектісінің компоненттері мен модульдерінің бастапқы кодтары кітапханалармен және файлдармен (қажет болған жағдайда);

5) осы Қағидаларға 3-қосымшаға сәйкес сынақ объектісінің бекітілген ақпараттық қауіпсіздік жөніндегі техникалық құжаттамасының электрондық көшірмелері (қажет болған кезде);

6) иеленушісі (меншік иесі) сынақтар жүргізуге өтінім беруге өтініш берушіге уәкілеттік беретін құжаттың электрондық көшірмесі (қажет болған кезде).

Ескерту. 15-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

16. Өтініш беруші сатып алуды мемлекеттік сатып алу веб-порталы арқылы жүзеге асырған жағдайда, сынықтар жүргізуге өтінім ағымдағы жылдың 1 қарашасынан кешіктірмей қабылданады.

17. Мемлекеттік техникалық қызмет өтінімді алған күнінен бастап үш жұмыс күні ішінде осы Қағидаларға 15-тармақта көрсетілген құжаттардың толықтығын тексеруді жүзеге асырады.

18. Осы Қағидаларға 15-тармақта көрсетілген талаптарға сәйкес өтінім және қоса берілген құжаттар сәйкес келмеген жағдайда, өтінім қайтару себептерін көрсете отырып, өтініш берушіге кері қайтарылады.

19. Мемлекеттік техникалық қызмет осы Қағидалардың 15-тармағына сәйкес құжаттар топтамасының толық болуына өтінімді тексергеннен кейін үш жұмыс күні ішінде өтініш берушіге:

1) сатып алуды өтініш беруші мемлекеттік сатып алу веб-порталы арқылы жүзеге асырған кезде, сынақтар жүргізуге арналған шартқа техникалық ерекшеліктің жобасын жібереді. Өтініш беруші техникалық ерекшеліктің жобасын алған күнінен бастап үш жұмыс күні ішінде мемлекеттік сатып алу веб-порталына мемлекеттік сатып алу туралы шартты тікелей жасау арқылы бір

көзден алу тәсілімен мемлекеттік сатып алу туралы шарттың жобасын орналастырады;

2) сатып алуды өтініш беруші мемлекеттік сатып алу веб-порталын қолданусыз жүзеге асырған кезде, сынақтар жүргізуге арналған шарттың екі данасын жібереді. Өтініш беруші жоғарыда көрсетілген шарттың екі данасын алған күнінен бастап бес жұмыс күні ішінде оларға қол қояды және шарттың бір данасын мемлекеттік техникалық қызметке қайтарады.

Ескерту. 19-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

20. Егер өтініш беруші сатып алуды мемлекеттік сатып алу веб-порталы арқылы жүзеге асырған болса және 15 қарашаға дейінгі мерзімде мемлекеттік сатып алу веб-порталында мемлекеттік сатып алу туралы шартты орналастырмаған жағдайда, өтінім жойылады және өтініш берушіге қайтарылады

21. Сынақтар мерзімі өтініш берушімен келісіледі және сынақтар жүргізу бойынша жұмыстардың көлемі мен сынақ объектісінің сыныптау сипаттамаларына байланысты болады.

Сынақтар мерзімін келісу мүмкін болмаған жағдайда, өтінім сынақтар мерзімін айқындау үшін Комитетке жүгіну мүмкіндігі көрсетіліп, қанағаттандырусыз өтініш берушіге кері қайтарылады.

22. Сынақтар жүргізу үшін өтініш беруші мемлекеттік техникалық қызметке мыналарды қамтамасыз етеді:

1) жұмыс орнын, пайдаланушының жұмыс орнына, серверлік және желілік жабдыққа, фото және бейне тіркеуді жүргізе отырып, сынақ объектісінің телекоммуникация желісіне және сынақ объектісіне арналған құжаттамаға және ілеспе құжаттамаға, оның ішінде сынақ объектісін және сынақ объектісінің құрамына кіретін компоненттерді сүйемелдеуге және техникалық қолдап отыруға арналған шарттарға физикалық қолжетімділік;

2) сынақ объектісінің функцияларын техникалық құжаттама талаптарына сәйкес көрсету.

Ескерту. 22-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

23. Өтініш берушінің осы Қағидаларға 22-тармақта көрсетілген талаптарын қамтамасыз ету мүмкінсіздігі жағдайында, шартқа оны орындау мерзімін ұзарту туралы қосымша келісімге қол қоюды ескере отырып, сынақтар Өтініш берушіге оларды қамтамасыз ету үшін қажетті уақытқа тоқтатылады.

24. Сынақтар «Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне сәйкес жүргізіледі.

25. Сынақтар жүргізу кезінде осы Қағидалардың 15-тармағының 1) тармақшасына сәйкес берілген сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың деректері мен сынақ объектісінің нақты жай-күйі арасында алшақтық анықталған жағдайда, өтініш беруші SYNAQ интернет-порталында сынақ объектісі меншік иесінің (иеленушісінің) ЭЦҚ-мен куәландырылған сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сұраулықты мемлекеттік техникалық қызметке жібереді. Сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сұраулық (қажет болған жағдайда) сынақтар мерзімін ұзартуға және сынақтар жүргізу құнын өзгертуге қосымша келісім жасасу үшін негіз болады.

Ескерту. 25-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

26. Қажет болған кезде, сынақтар кезінде сынақ мерзімі аяқталғанға дейін жұмыстардың бір немесе бірнеше түрі бойынша қайтадан сынақтар жүргізу қажеттілігі айқындалса, өтініш беруші сұрау салумен мемлекеттік техникалық қызметке жүгінеді және осы жұмыс түрлері бойынша қайтадан сынақ жүргізу туралы қосымша келісім жасалады.

27. Сынақтарға кіретін жұмыстардың нәтижелері және анықталған сәйкессіздіктерді жою жөніндегі ұсынымдар барлық жұмыс түрлері аяқталғаннан кейін өтініш берушінің SYNAQ интернет-порталындағы жеке кабинетінде орналастырылатын жеке хаттамаларға енгізіледі.

Ескерту. 27-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

28. Мемлекеттік техникалық қызметтің сынақтарға кіретін жұмыстардың әрбір түрін жүргізуінің бағалары Заңның 14-бабының 2-тармағына сәйкес белгіленеді.

29. Сынақтар жүргізу құнын есептеу үшін өтініш беруші мемлекеттік техникалық қызметке SYNAQ интернет-порталында сынақ объектісі меншік иесінің (иеленушісінің) ЭЦҚ-мен куәландырылған сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықты жібереді.

Ескерту. 29-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

30. Өтініш беруші жүргізілген жұмыстар бойынша сынақтардың хаттамалары SYNAQ интернет-порталында орналастырылған күнінен бастап жиырма жұмыс күні ішінде сынақтар кезінде анықталған сәйкессіздіктерді жойса және анықталған сәйкессіздіктерді түзету нәтижелерімен салыстыру кестесін қоса бере отырып, SYNAQ интернет-порталы арқылы қайта сынақтар жүргізуге сұрау салуды мемлекеттік техникалық қызметке жіберсе, мемлекеттік техникалық қызмет өтініш берушіден сұрау салуды алған күннен бастап он бес жұмыс күні ішінде аталған жұмыс түрлері бойынша тиісті құжаттарды рәсімдей отырып, ақысыз негізде қайтадан сынақтар жүргізеді.

Белгіленген мерзімді өткізіп алу сынақтарды осы Қағидаларда белгіленген жалпы тәртіпте жүргізу үшін негіздеме болып табылады.

Ескерту. 30-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

31. Сынақ объектісінің бағдарламалық қамтылымына өзгерістер енгізуге байланысты сәйкессіздіктерді жойғаннан кейін қайтадан сынақ жүргізген кезде бастапқы кодқа талдау жүргізіледі.

Бұл ретте өтініш беруші қайтадан сынақтар жүргізу туралы сұрау салуға сынақ объектісінің сәтті компиляциясы үшін қажетті кітапханалары мен

файлдары бар сынақ объектісі компоненттерінің және модульдерінің бастапқы кодтарын қоса береді.

Ескерту. 31-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

32. Қайтадан сынақтар жүргізген кезде сәйкессіздіктер анықталған жағдайда, мемлекеттік техникалық қызмет теріс қорытынды бар хаттаманы ресімдейді, одан кейін сынақтар осы Қағидаларға 2-тарауда белгіленген тәртіппен жүргізіледі.

33. Сынақ хаттамаларын жоғалтқан, бүлдірген немесе олар зақымдалған, сондай-ақ сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтағы деректер өзгерген кезде, бұрын сынақтар жүргізу кезінде бір немесе бірнеше жұмыс түрлері бойынша теріс нәтижемен қағаз жеткізгіште хаттамалар алған сынақ объектілері үшін сынақ объектісінің меншік иесі немесе иеленушісі мемлекеттік техникалық қызметке себептерін көрсете отырып, хабарлама жібереді.

Мемлекеттік техникалық қызмет хабарламаны алған күннен бастап бес жұмыс күні ішінде бұрын берілген сынақ хаттамасының (лардың) телнұсқасын не сынақ объектісінің сипаттамалары туралы өзектілендірілген сауалнама-сұраулығы бар сынақ хаттамасының (лардың) телнұсқасын береді.

Ескерту. 33-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

3-тарау. Ақпараттандыру объектілеріне ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтарды сынақ зертханаларында жүргізу тәртібі

34. Сынақтарды сынақ зертханаларында жүргізуге шарттар жасау тәртібі Қазақстан Республикасының Азаматтық кодексіне сәйкес айқындалады.

35. Сынақтар жүргізу үшін өтініш беруші мынадай құжаттарды ұсына отырып, мемлекеттік техникалық қызметке қағаз тасымалдауышта ілеспе хатпен

осы Қағидаларға 1-қосымшаға сәйкес нысан бойынша сынақтар жүргізуге өтінім (бұдан әрі – өтінім) береді:

1) шарттарға қол қоюға уәкілеттік берілген тұлғаның атына сенімхаттың немесе заңды тұлғаның басшысын тағайындау туралы құжаттың көшірмесі (заңды тұлғалар үшін);

2) сынақ объектісінің меншік иесі немесе иеленушісі бекіткен қағаз тасымалдауышта осы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық;

3) меншік иесі немесе иеленушісі бекіткен компакт-дискіде ақпараттандыру объектісіне арналған техникалық тапсырма немесе техникалық ерекшелігі (қажет болған кезде);

4) сәтті компиляция үшін қажетті сынақ объектілері компоненттерінің және кітапханалары мен файлдары бар модульдерінің бастапқы кодтары компакт-дискіде (қажет болған кезде);

5) осы Қағидаларға 3-қосымшаға сәйкес сынақ объектісінің ақпараттық қауіпсіздік жөніндегі техникалық құжаттамасының тізбесінің бекітілген көшірмелері электрондық түрде компакт-дискіде (қажет болған кезде);

6) иеленуші немесе меншік иесі сынақтар жүргізу туралы өтінім беруге өтініш берушіге өкілеттік беретін құжат (қажет болған кезде).

36. Сынақтар «Электрондық үкіметтің» ақпараттандыру объектілеріне және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне сәйкес жүргізіледі.

37. Егер өтініш беруші сынақ кезінде анықталған сәйкессіздіктерді атқарылған жұмыстар бойынша сынақ хаттамаларын алған күнінен бастап жиырма жұмыс күні ішінде жойса және айқындалған сәйкессіздіктерді түзету нәтижелерімен салыстыру кестесін қоса бере отырып, қызмет берушіге қайтадан сынақтар жүргізуге сұрау салу жіберсе, қызмет беруші өтініш берушіден хабарламаны алған күннен бастап он бес жұмыс күні ішінде аталған жұмыс түрлері бойынша тиісті құжаттарды ресімдей отырып, өтеусіз негізде қайтадан сынақтар жүргізеді.

Белгіленген мерзімді өткізіп алу осы Қағидаларда белгіленген жалпы тәртіпте сынақтар жүргізу үшін негіздеме болып табылады.

38. Қайтадан сынақтар жүргізген кезде сәйкессіздіктер анықталған жағдайда, қызмет беруші теріс қорытынды бар хаттаманы ресімдейді, одан кейін сынақтар осы Қағидалардың 3-тарауында белгіленген тәртіппен жүргізіледі.

39. Сынақтар хаттамалары жоғалған, бүлінген немесе зақымдалған кезде сынақ объектісінің меншік иесі немесе иеленушісі себептерін көрсете отырып, қызмет берушіге хабарлама жібереді.

Қызметті беруші хабарламаны алған күнінен бастап бес жұмыс күні ішінде сынақтар хаттамаларының телнұсқасын береді.

4-тарау. Ақпарттық қауіпсіздік талаптарына сәйкестікке сынақтардың нәтижелері бойынша акт беру тәртібі

40. Осы Қағидаларға 4-қосымшаға сәйкес нысан бойынша ақпарттық қауіпсіздік талаптарына сәйкестікке сынақтардың нәтижелері бойынша актіні (бұдан әрі – сынақтар актісін) Комитет (бұдан әрі – көрсетілетін қызметті беруші) береді.

Ақпараттық қауіпсіздік талаптарының сәйкестігіне сынақ нәтижелері бойынша актіні беру» мемлекеттік көрсетілетін қызмет (бұдан әрі – мемлекеттік көрсетілетін қызмет) болып табылады.

Мемлекеттік қызмет көрсету ерекшеліктері ескеріле отырып, қызмет көрсету процесінің сипаттамаларын, нысанын, мазмұны мен нәтижесін, сондай-ақ өзге де мәліметтерді қамтитын мемлекеттік қызмет көрсетуге қойылатын негізгі талаптар тізбесі мемлекеттік қызмет көрсету стандартында осы Қағидаларға 6-қосымшаға сәйкес жазылған.

41. Көрсетілетін қызметті алушы «электрондық үкіметтің» веб-порталы (бұдан әрі – портал) арқылы осы Қағидаларға 6-қосымшаның 8-тармағына сәйкес мемлекеттік қызметті көрсетуге қойылатын негізгі талаптар тізбесінде көрсетілген мемлекеттік қызмет көрсету үшін қажетті құжаттар тізбесін ұсынады.

Ескерту. 41-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

42. Сынақтар актісін алу үшін өтініш беруші (бұдан әрі – көрсетілетін қызметті алушы) көрсетілетін қызметті берушіге портал арқылы осы Қағидалардың 7-11-тармақтарында айқындалған хаттамалардың толық жиынтығымен, сынақ объектісінің меншік иесі немесе иеленушісі бекіткен осы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықты қоса бере отырып, осы Қағидаларға 7-қосымшаға сәйкес нысан бойынша өтініш жібереді.

Көрсетілетін қызметті алушы көрсетілетін қызметті берушіге барлық қажетті құжаттарды тапсырған кезде көрсетілетін қызметті алушының «жеке кабинетінде» өтінішті қабылдаудың растауы мемлекеттік көрсетілетін қызмет нәтижесін алу күнін көрсете отырып, мемлекеттік қызметті көрсету үшін сұрау салудың қабылданғаны туралы мәртебе көрсетіледі.

Көрсетілетін қызметті беруші өтініш келіп түскен күні оларды қабылдауды және тіркеуді жүзеге асырады (өтініш беруші жұмыс уақыты аяқталғаннан кейін, Қазақстан Республикасының еңбек заңнамасына сәйкес демалыс немесе мереке күндері жүгінген кезде өтініштерді қабылдау келесі жұмыс күні жүзеге асырылады).

Көрсетілетін қызметті беруші құжаттарды алған күннен бастап екі жұмыс күні ішінде ұсынылған құжаттардың толықтығын тексереді.

Ұсынылған құжаттардың толық емес және (немесе) қолданылу мерзімі өтіп кеткен құжаттар фактісі анықталған кезде, көрсетілетін қызметті беруші көрсетілген мерзімдерде өтінішті одан әрі қараудан дәлелді бас тартады.

Бұл ретте сынақтар актісіне енгізу үшін сынақтың жекелеген түрі бойынша хаттаманың қолданылу мерзімі хаттама берілген күннен бастап бір жылдан аспайды.

Жеке басты куәландыратын құжаттар туралы мәліметтерді, заңды тұлғаны мемлекеттік тіркеу (қайта тіркеу) туралы куәлікті көрсетілетін қызметті беруші «электрондық үкімет» шлюзі арқылы тиісті мемлекеттік ақпараттық жүйелерден алады.

Ескерту. 42-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

43. Сынақтар хаттамаларының оң нәтижелері кезінде өтініш тіркелген күнінен бастап он жұмыс күні ішінде қаралады. Осы Қағидалардың 7-11-тармақтарында айқындалған сынақтар хаттамаларының толық жиынтығы негізінде көрсетілетін қызметті беруші жеті жұмыс күні ішінде сынақтар хаттамаларын зерделейді және көрсетілетін қызметті берушіге ұсынылған сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың деректері мен сынақтар хаттамаларына қоса берілген сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтардың деректері арасындағы айырмашылықтарды белгілейді.

Мемлекеттік қызметті көрсетуден бас тарту үшін негіздемелер анықталған кезде көрсетілетін қызметті беруші көрсетілетін қызметті алушыны мемлекеттік қызметті көрсетуден бас тарту туралы алдын ала шешімі, сондай-ақ Қазақстан Республикасы Әкімшілік рәсімдік-процестік кодексінің 73-бабына сәйкес, көрсетілетін қызметті алушыға алдын ала шешім бойынша ұстанымын білдіру мүмкіндігі үшін тыңдау өткізу уақыты мен орны (тәсілі) туралы хабардар етеді.

Тыңдау туралы хабарлама мемлекеттік қызмет көрсету мерзімі аяқталғанға дейін кемінде үш жұмыс күні бұрын жіберіледі. Тыңдау хабардар етілген күннен бастап екі жұмыс күнінен кешіктірілмей жүргізіледі.

Тыңдау нәтижелері бойынша көрсетілетін қызметті беруші сынақтар актісін немесе мемлекеттік қызметті көрсетуден дәлелді бас тартуды береді.

Сынақтар актісін беру туралы оң шешім қабылданған кезде көрсетілетін қызметті беруші көрсетілетін қызметті алушыға сынақтар актісінің ажырамас бөлігі болып табылатын сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, сынақтар актісін көрсетілетін қызметті берушінің уәкілетті адамының ЭЦҚ-сы қойылған электрондық құжат нысанында «жеке кабинетке» жібереді.

Ескерту. 43-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

44. Бір немесе бірнеше сынақ хаттамаларының теріс нәтижелері кезінде өтініш тіркелген күннен бастап он бес жұмыс күні ішінде қаралады.

Осы Қағидалардың 7-11-тармақтарында айқындалған сынақ хаттамаларының толық жиынтығы негізінде көрсетілетін қызметті беруші сегіз жұмыс күні ішінде сынақ хаттамаларын зерделейді және көрсетілетін қызметті берушіге ұсынылған сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың деректері мен сынақ хаттамаларына қоса берілген сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтарының деректері арасындағы айырмашылықтарды белгілейді.

Туындаған келіспеушіліктерді жою үшін тыңдау туралы хабарлама мемлекеттік қызмет көрсету мерзімі аяқталғанға дейін кемінде үш жұмыс күні бұрын жіберіледі. Тыңдау хабардар етілген күннен бастап екі жұмыс күнінен кешіктірілмей жүргізіледі.

Көрсетілетін қызметті беруші көрсетілетін қызметті алушының және қызмет беруші (қызмет берушілердің) өкілдерін талқылауға шақырады және олардың қатысуымен мынадай:

- 1) сынақ актісін беру туралы;
- 2) сынақ актісін беруден бас тарту туралы шешімдердің бірін қабылдайды.

Сынақтар актісін беру туралы оң шешім қабылданған кезде көрсетілетін қызметті беруші көрсетілетін қызметті алушыға сынақтар актісінің ажырамас бөлігі болып табылатын сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, сынақтар актісін көрсетілетін қызметті берушінің уәкілетті адамының ЭЦҚ-сы қойылған электрондық құжат нысанында «жеке кабинетке» жібереді.

Сынақтар актісін беруден бас тарту туралы шешім қабылданған кезде көрсетілетін қызметті беруші көрсетілетін қызметті алушыға сынақтар актісін беруден бас тарту туралы дәлелді жауапты көрсетілетін қызметті берушінің уәкілетті адамының ЭЦҚ-сы қойылған электрондық құжат нысанында «жеке кабинетке» жібереді.

Ескерту. 44-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

45. Мемлекеттік қызмет көрсету үшін қажетті мәліметтерді қамтитын ақпараттық жүйенің ақаулығы жағдайда, көрсетілетін қызметті беруші

техникалық ақаулардың туындауын анықтаған сәттен бастап sd@nitech.kz электрондық почтасы бойынша бірыңғай қолдау қызметіне сұрау салу жолдау арқылы авторизация сәтінен бастап қателік туындаған сәтке дейін қателік болған нақты уақытты көрсете отырып, қадамдық скриншоттарды қоса бере отырып, мемлекеттік көрсетілетін қызметтің атауы, әкімшілік құжаттың нөмірі және коды немесе өтініштің бірегей сәйкестендіру нөмірі, әкімшілік құжаттың нөмірі және коды немесе рұқсат беру құжатының бірегей сәйкестендіру нөмірі, көрсетілетін қызметті алушының жеке сәйкестендіру нөмірі/бизнес сәйкестендіру нөмірі бойынша міндетті түрде ақпарат ұсына отырып, «электрондық үкімет» ақпараттық-коммуникациялық инфрақұрылымның операторын хабардар етеді.

46. Қағаз нысанда берілген сынақтар актісі (актілері) жоғалған, бүлінген немесе зақымдалған кезде сынақ объектісінің меншік иесі немесе иеленушісі себептерін көрсете отырып, сынақ актісінің телнұсқасын алуға көрсетілетін қызметті берушіге өтініш жібереді.

Телнұсқаны беру үшін өтініш түскен кезде көрсетілетін қызметті беруші өтініш келіп түскен күні бұрын алынған құжаттардың электрондық көшірмелерін қоса тіркеп, оны портал арқылы рәсімдейді және өтінішті алған күннен бастап бес жұмыс күні ішінде көрсетілетін қызметті алушыға сынақтар актісінің ажырамас бөлігі болып табылатын сынақтар объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін қоса бере отырып, сынақтар актісін жібереді.

Ескерту. 46-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

47. Сынақтар актісінің жарамдылық мерзімі «электрондық үкіметтің» ақпараттық-коммуникациялық платформасын қоспағанда, сынақ объектісін өнеркәсіптік пайдалану мерзімімен немесе сынақ объектісін жаңғыртуды бастау сәтіне дейін шектеледі.

«Электрондық үкіметтің» ақпараттық-коммуникациялық платформасының сынақтар актісі бір жылға жарамдылық мерзімімен беріледі.

48. Ақпараттандыру объектісінің жұмыс істеу жағдайлары мен функционалдығына өзгерістер енгізген кезде ақпараттандыру объектісінің меншік иесі немесе иеленушісі өзгерістерге әкелген жұмыстарды аяқтағаннан кейін көрсетілетін қызметті берушіге барлық жүргізілген өзгерістердің сипаттамасын

және сынақтар объектісінің меншік иесінің немесе иеленушісімен бекітілген сынақтар объектісінің сипаттамалары туралы жаңартылған сауалнама-сұраулықты қоса беріп, хабарлама жібереді.

Ескерту. 48-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

49. Көрсетілетін қызметті беруші ақпараттандыру объектісіне енгізілген өзгерістерді бес жұмыс күнінен аспайтын мерзімде қарайды және сынақтар актісін қайтарып алу және ақпараттандыру объектісінің жұмыс істеу жағдайлары және (немесе) функционалдығы өзгерген кезде функциялары бұзылған сынақтар түрін жүргізу қажеттілігі туралы шешім қабылдайды.

Шешім осы Қағидаларға 8-қосымшаға сәйкес Ақпараттандыру объектісінің жұмыс істеуі және (немесе) функционалдығы өзгерістерінің тізбесін ескере отырып қабылданады.

Ескерту. 49-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

50. Сынақтар актісін қайтарып алу кезінде меншік иесі немесе иеленуші үш ай мерзімде осы Қағидалардың 49-тармағының талаптарын ескере отырып, осы Қағидалардың 2 немесе 3-тарауында белгіленген тәртіппен сынақтардан өту туралы қызмет берушілерге өтінім беру үшін шаралар қолданады.

Ескерту. 50-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

51. Көрсетілетін қызметті беруші мынадай негіздер:

1) Көрсетілетін қызметті берушіге ұсынылған сынақтар объектісінің сипаттамалары туралы сауалнама-сұраулықтың деректері мен сынақтар хаттамаларына қоса берілген сынақтар объектісінің сипаттамалары туралы сауалнама-сұраулықтың деректері арасындағы айырмашылықты анықтау;

2) көрсетілетін қызметті алушының және (немесе) мемлекеттік қызмет көрсету үшін қажетті ұсынылған материалдардың, объектілердің, деректердің және мәліметтердің Қазақстан Республикасының нормативтік құқықтық

актілерінде белгіленген талаптарға сәйкес келмеуі бойынша сынақтар актісін беруден бас тартады.

52. Ақпараттық қауіпсіздік талаптарына сәйкестікті сынау нәтижелері бойынша акт беру орталық мемлекеттік органдар, облыстардың, республикалық маңызы бар қалалардың, астананың, аудандардың, облыстық маңызы бар қалалардың жергілікті атқарушы органдарын, қаладағы аудандардың, аудандық маңызы бар қалалардың, кенттердің, ауылдардың, ауылдық округтердің әкімдері үшін осы тарауда көзделген тәртіпте іске асырылады.

53. Мемлекеттік қызмет көрсету мәселелері бойынша шағымды қарауды Қазақстан Республикасы Әкімшілік рәсімдік-процестік кодексінің 91-бабына сәйкес, мемлекеттік қызметті көрсету мәселелері жөніндегі жоғары тұрған әкімшілік орган, лауазымды адам, мемлекеттік қызметтер көрсету сапасын бағалау және бақылау жөніндегі уәкілетті орган (бұдан әрі – шағымды қарайтын орган) жүргізеді.

Шағым шешіміне, әрекетіне (әрекетсіздігіне) шағым берілетін көрсетілетін қызметті берушіге және (немесе) лауазымды адамға беріледі.

Шешіміне, әрекетіне (әрекетсіздігіне) шағым берілген көрсетілетін қызметті беруші, лауазымды адам шағым келіп түскен күннен бастап үш жұмыс күнінен кешіктірмей оны және әкімшілік істі шағымды қарайтын органға жолдайды.

Бұл ретте шешіміне, әрекетіне (әрекетсіздігіне) шағым берілген көрсетілетін қызметті беруші, лауазымды адам үш жұмыс күні ішінде шағымда көрсетілген талаптарды толық қанағаттандыратын шешім немесе өзге әкімшілік іс-қимыл қабылдаса, ол шағымды қарайтын органға шағымды жібермеуге құқылы.

Көрсетілетін қызметті берушінің мекенжайына келіп түскен көрсетілетін қызметті алушының шағымы «Мемлекеттік көрсетілетін қызметтер туралы» 2013 жылғы 15 сәуірдегі Қазақстан Республикасы Заңының 25-бабының 2-тармағына сәйкес ол тіркелген күннен бастап бес жұмыс күні ішінде қаралуға жатады.

Мемлекеттік қызметтер көрсету сапасын бағалау және бақылау жөніндегі уәкілетті органның атына келіп түскен көрсетілетін қызметті алушының шағымы тіркелген күнінен бастап он бес жұмыс күні ішінде қаралуға жатады.

«Мемлекеттік көрсетілетін қызметтер туралы» Заңда өзгесі көзделмесе, сотқа дейінгі тәртіппен шағымданғаннан кейін сотқа жүгінуге жол беріледі.

Ескерту. 53-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
қағидаларына
1-қосымша

Нысан

(қызмет берушінің атауы)

(сынақтар жүргізу объектісінің атауы)

Ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізуге өтінім

1. _____
(өтініш беруші ұйымның атауы, өтініш берушінің Т.А.Ә. (болған кезде)
бизнес-идентификациялық номер, банктік деректемелері)

_____ (өтініш берушінің пошта мекенжайы, e-mail және телефоны, облыс, қала, аудан)

мынадай жұмыстар құрамымен:

1)

2)

3)

4)

5) _____
(осы Қағидалардың 7/8/9/10/11 тармағына сәйкес жұмыс түрлерінің тізбесі
(қажетті тармақты көрсету))

_____ (сынақтар жүргізу объектісінің атауы, нұсқасының нөмірі, әзірлеу күні)

сынақтар жүргізуді сұрайды.

2. Сыналатын сынақ объектісінің иеленушісі (меншік иесі) туралы мәліметтер

(атауы немесе Т.А.Ә. (болған кезде))

(облыс, қала, аудан, пошта мекенжайы, телефоны)

3. Сыналатын сынақ объектісінің әзірлеушісі туралы мәліметтер

(әзірлеуші туралы ақпарат, авторлар атауы немесе Т.А.Ә. (болған кезде))

(облыс, қала, аудан, пошта мекенжайы, телефоны)

4. Қызмет берушімен байланысуға жауапты тұлғаның деректері:

1) тегі, аты, әкесінің аты:

_____;

2) лауазымы:

_____;

3) жұмыс телефоны: _____, ұялы телефоны :

_____;

4) электрондық пошта мекенжайы: E-mail: _____@_____.

Өтініш беруші ұйымның басшысы/өтініш берушінің Т.А.Ә. (болған кезде)

_____ (қолы, күні)

(мөрдiң орны) болған кезде

«Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
қағидаларына
2-қосымша

Ескерту. 2-тармаққа өзгеріс енгізілді - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 28.09.2020 № 356/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

Нысан

1. Сынақ объектісінің атауы:

2. Сынақ объектісіне қысқаша аңдатпа

(мақсаты мен пайдалану аясы)

3. Сынақ объектісінің сыныпталуы:

1) қолданбалы бағдарламалық қамтылымның сыныбы _____.

2) Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 28 қаңтардағы № 135 бұйрығымен (Нормативтік құқықтық актілерді мемлекеттік тіркеу тіркелімінде № 13349 болып тіркелген) бекітілген Ақпараттандыру объектілерін сыныптау қағидаларына 2-қосымшаның нысаны бойынша сыныптау схемасы.

4. Сынақ объектісінің архитектурасы:

1) сынақ объектісінің:

сынақ объектісінің компоненттері, модульдері және олардың IP-мекенжайлары;

компоненттері немесе модульдері арасындағы байланыстары және ақпараттық ағындардың бағыттары;

басқа ақпараттандыру объектілерімен интеграциялық өзара іс-қимылды қосу нүктелері; пайдаланушылар қосылған нүктелер;

деректерді сақтау орындары мен технологиялары;

қолданылатын резервтік жабдық;

пайдаланылатын терминдер мен аббревиатуралардың түсіндірмелері көрсетілген функционалдық схемасы (қажет болған кезде);

2) сынақ объектісінің:

желінің архитектурасы мен сипаттамалары;

серверлік және коммуникациялық жабдық;

адресеу мен қолданылатын желілік технологиялар;

пайдаланылатын локалдық, ведомстволық (корпоративтік) және жаһандық желілері;

жұмыс істемей қалу болмаушылығын қамтамасыз ету және резервтеу жөніндегі шешім(дер);

пайдаланылатын терминдер мен аббревиатуралардың түсіндірмелері көрсетілген деректерді беру желісінің схемасы (қажет болған кезде);

5. Сынақ объектісі туралы ақпарат:

1) серверлерлік жабдық туралы ақпарат (кестені толтыру):

р /с №	Сервердің немесе виртуалды ресурстың атауы (сервердің домендік атауы, желілік атауы немесе логикалық атауы)	Мақсаты (орындайтын функционалдық міндеттері)	Саны	Сервердің немесе мәлімденген пайдаланылатын виртуалды ресурстардың сипаттамалары	Серверлерде орнатылған ОЖ, ДҚБЖ, БҚ, ко-сымшалар, кітапханалар мен қорғау құралдары немесе пайдаланатын виртуалды сервистер (нұсқалардың нөмірлері көрсетілген бағдарламалық ортаның құрамы)	Пайдаланылатын IP-мекенжайлары
1	2	3	4	5	6	7

2) желілік жабдық туралы ақпарат (кестені толтыру):

р /с №	Желілік жабдықтың атауы (маркасы/моделі)	Мақсаты (орындайтын функционалдық міндеттері)	Саны	Пайдаланылатын желілік технологиялар	Пайдаланылатын желіні қорғау технологиялары	Пайдаланылатын IP-мекенжайлары, соның ішінде басқару порты

1	2	3	4	5	6	7

3) серверлік және желілік жабдық орналасқан орны (кестені толтыру):

р /с №	Серверлік орынжайдың иеленушісі	Серверлік орынжайдың иеленушісінің заңды мекенжайы	Серверлік орынжайдың нақты орналасқан орны -мекенжайы	Қолжетімділікті ұйымдастыруға жауапты тұлғалар (Т.А. Ә. (болған кезде)	Жауапты тұлғалардың телефондары (жұмыс, ұялы)
1	2	3	4	5	6

4) резервтік серверлік жабдықтың сипаттамалары (кестені толтыру):

р /с №	Сервердің немесе виртуалды ресурстың атауы (сервердің домендік атауы, желілік атауы немесе логикалық атауы)	Мақсаты (орындайтын функционалдық міндеттері)	Саны	Сервердің немесе мәлімденген пайдаланылатын виртуалды ресурстардың сипаттамалары	Серверлерде орнатылған ОЖ, ДҚБЖ, БҚ, қосымшалар, кітапханалар мен қорғау құралдары немесе пайдаланылатын виртуалды сервистер (нұсқалардың нөмірлері көрсетілген бағдарламалық ортаның құрамы)	Пайдаланылатын IP-мекенжайлары	Резервтеу әдісі
1	2	3	4	5	6	7	8

5) резервтік желілік жабдықтың сипаттамалары (кестені толтыру):

р /с №	Желілік жабдықтың атауы (маркасы/моделі)	Мақсаты (орындайтын функционалдық міндеттері)	Саны	Пайдаланылатын желілік технологиялар	Пайдаланылатын желіні қорғау технологиялары	Пайдаланылатын IP-мекенжайлары, соның ішінде басқару порты	Резервтеу әдісі
1	2	3	4	5	6	7	8

6) резервтік серверлерлік және желілік жабдық орналасқан орны (кестені толтыру):

р /с №	Серверлік орынжайдың иеленушісі	Серверлік орынжайдың иеленушісінің заңды мекенжайы	Серверлік орынжайдың нақты орналасқан орны -мекенжайы	Қолжетімділікті ұйымдастыруға жауапты тұлғалар (Т.А. Ә. (болған кезде)	Жауапты тұлғалардың телефондары (жұмыс, ұялы)
1	2	3	4	5	6

7) сынақ объекті желісінің құрылымы (кестені толтыру) (қажет болған кезде):

р/с №	Желі сегментінің атауы	Желінің IP-мекенжайы / желі маскасы
1	2	3

8) әкімшілердің жұмыс станциялары бойынша ақпарат (кестені толтыру):

р /с №	Әкімшілердің есептік жазбаларының саны	Интернетке қолжетімділіктің болуы	Серверге қашықтықтан қолжетімділіктің болуы	Әкімші жұмыс станциясының IP-мекенжайы	Нақты орналасқан орны - жұмыс орнының мекенжайы

	Әкім-ші-нің рөлі					
1	2	3	4	5	6	7

9) мобильдік және интернет қосымшаларын пайдалануды қоса алғанда, қолданбалы бағдарламалық қамтылымды пайдаланушылар туралы ақпарат (кестені толтыру):

Р /с №	Пайдаланушының рөлі	Пайдаланушының іс-қимылдарының тізбесі	Сынақ объектісіне пайдаланушыларды қосу нүктесінің мекенжайы және порты	Сынақ объектісіне пайдаланушыларды қосу нүктесінің хаттамасы	Сынақ объектісін құруға немесе дамытуға арналған техникалық құжатқа сәйкес пайдаланушылар саны	Секундына өңделетін сұраулардың (пакеттердің) барынша көп саны	Сұраулар арасында күтудің ең ұзақ уақыты
1	2	3	4	5	6	7	8

10) сынақ объектісінің интеграциялық өзара іс-қимылы, соның ішінде болжамды, туралы ақпарат (кестені толтыру):

р /с №	Интеграциялық байланыстың (ақпараттандыру объектісінің) атауы	Интеграциялау объектісінің меншік иесі немесе иеленушісі	Қолданыстағы /жоспарлы	Интеграциялау модулінің болуы	Қосу нүктесінің мекенжайы	Қосу нүктесінің хаттамасы	Секундына сұраулардың (пакеттердің) барынша көп саны	Сұраулар арасында күтудің ең ұзақ уақыты
1	2	3	4	5	6	7	8	9

11) қолданбалы БҚ бастапқы кодтары (кестені толтыру) (қажет болған кезде):

р /с №	Дискінің маркалауы	Дискідегі каталогтың атауы	Файлдың атауы	Файлдың көлемі, Мбайт	Пайдаланылатын бағдарламалау тілі	Бағдарламалау тілінің нұсқасы	Әзірлеу ортасы	Әзірлеу ортасының нұсқасы	Файлдың түрлендірілген күні
1	2	3	4	5	6	7	8	9	10

12) пайдаланылатын кітапханалар мен бағдарламалық платформаның (лардың) бастапқы кодтары және орындалатын файлдары (қажет болған кезде):

р /с №	Дискінің маркалауы	Дискідегі каталогтың атауы	Кітапхана/бағдарламалық платформа/файл атауы	Көлемі, Мбайт	Бағдарламалау тілі (қажет болған кезде)	Кітапхана нұсқасы
1	2	3	4	5	6	7

6. Сыналатын объектіні құжаттау (кестені толтыру) (қажет болған кезде):

	Құжаттың атауы				

Р /с №		Бар бо-луы	Парақтар са-ны	Бе-кіті-лен-ген күні	Оған сәйкес құжат әзірленген стандарт немесе нормативтік құжат
1	2	3	4	5	6
1	Ақпараттық қауіпсіздік саясаты;				
2	Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және маркалау қағидалары;				
3	Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;				
4	Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмыс істеуін қамтамасыз ету қағидалары;				
5	Есептеу техникасы құралдарын, телекоммуникациялық жабдықты және бағдарламалық қамтылымды түгендеу мен паспорттандыру қағидалары;				
6	Ішкі ақпараттық қауіпсіздік аудитін жүргізу қағидалары;				
7	Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;				
8	Электрондық ресурстарға қол жеткізу құқықтарын бөлу қағидалары;				
9	Интернетті және электрондық поштаны пайдалану қағидалары;				
10	Аутентификация рәсімін ұйымдастыру қағидалары;				
11	Вирусқа қарсы бақылауды ұйымдастыру қағидалары;				
12	Мобильдік құрылғыларды және ақпарат тасымалдаушыларды пайдалану қағидалары;				
13	Ақпаратты өңдеу құралдарын физикалық қорғауды және ақпараттық ресурстардың қауіпсіз жұмыс істеу ортасын ұйымдастыру қағидалары;				
14	Ақпаратты резервтік көшіру және қалпына келтіру регламенті;				
15	Әкімшінің ақпараттандыру объектісін сүйемелдеу жөніндегі басшылығы;				
16	Пайдаланушылардың ақпараттық қауіпсіздіктің оқыс оқиғаларына және штаттан тыс (дағдарысты) жағдайларда әрекет етуі бойынша іс-қимыл тәртібі туралы нұсқаулық.				

7. Бұрын өткен жұмыс түрлері немесе сынақтар туралы мәліметтер (хаттаманың нөмірі, күні):

8. Сыналатын объектіге лицензияның болуы (авторлық құқықтың болуы, бастапқы кодты ұсынуға әзірлеуші ұйыммен келісімнің болуы)

9. Қосымша ақпарат:

**«Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
қағидаларына
3-қосымша**

**Сынақ объектісінің ақпараттық қауіпсіздік жөніндегі техникалық
құжаттамасының тізбесі**

1. Ақпараттық қауіпсіздік саясаты;
2. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру,
сыныптау және маркалау қағидалары;
3. Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;
4. Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмыс
істеуін қамтамасыз ету қағидалары;
5. Есептеу техникасы құралдарын, телекоммуникациялық жабдықты және
бағдарламалық қамтылымды түгендеу мен паспорттандыру қағидалары;
6. Ішкі ақпараттық қауіпсіздік аудитін жүргізу қағидалары;
7. Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;
8. Электрондық ресурстарға қол жеткізу құқықтарын бөлу қағидалары;
9. Интернетті және электрондық поштаны пайдалану қағидалары;
10. Аутентификация рәсімін ұйымдастыру қағидалары;
11. Вирусқа қарсы бақылауды ұйымдастыру қағидалары;
12. Мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану
қағидалары;
13. Ақпаратты өңдеу құралдарын физикалық қорғауды және ақпараттық
ресурстардың қауіпсіз жұмыс істеу ортасын ұйымдастыру қағидалары;
14. Ақпаратты резервтік көшіру және қалпына келтіру регламенті;

15. Әкімшінің ақпараттандыру объектісін сүймелдеу жөніндегі басшылығы;

16. Пайдаланушылардың ақпараттық қауіпсіздіктің оқыс оқиғаларына және штаттан тыс (дағдарысты) жағдайларда әрекет етуі бойынша іс-қимыл тәртібі туралы нұсқаулық.

**«Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
қағидаларына
4-қосымша**

Нысан

**Ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтар жүргізу
нәтижелері бойынша**

20 __ жылғы «__» _____ № ____ сынақтар актісі

«Ақпараттандыру туралы» Қазақстан Республикасы Заңының 7-1-бабының
11-1) тармақшасы негізінде 20 __ жылғы «__» _____ Өтінімге сәйкес
Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш
өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті ақпараттық қауіпсіздік
талаптарына сәйкестікке сынақтар жүргізу нәтижелері бойынша

(СО атауы)

(серверлік және желілік жабдықтың нақты орналасқан орны)

(сынақтар объектісі өтініш берушісінің атауы)

(өтініш беруші ұйымның атауы, өтініш берушінің Т.А.Ә. (болған кезде))

сынақ түрлері бойынша келесі хаттамалар негізінде:

1) 20 __ жылғы «__» _____ № ____ бастапқы кодтарды талдау
хаттамасы, қызмет берушінің атауы;

2) 20 __ жылғы «__» _____ № ____ ақпараттық қауіпсіздік
функцияларын сынау хаттамасы, қызмет берушінің атауы;

3) 20 __ жылғы «__» _____ № ____ жүктемелік сынау хаттамасы,
қызмет берушінің атауы;

4) 20 __ жылғы «__» _____ № ____ желілік инфрақұрылымды зерттеп-
қарау хаттамасы, қызмет берушінің атауы;

5) 20__ жылғы «__» _____ № _____ ақпараттық қауіпсіздікті
қамтамасыз ету процестерін зерттеп-қарау хаттамасы, қызмет берушінің атауы

Қорытынды

Жүргізілген сынақтар негізінде _____
(сынақтар объектісінің атауы)

ақпараттық қауіпсіздік талаптарына сәйкес.

Қосымша: Сынақтар объектісінің сипаттамалары туралы сауалнама-
сұраулықтың көшірмесі

Қазақстан Республикасы Цифрлық
даму, инновациялар және аэроғарыш
өнеркәсібі министрлігінің

Ақпараттық қауіпсіздік комитетінің төрағасы _____
(қолы) Т.А.Ә. (болған кезде)

20__ жылғы «__» _____

«Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
қағидаларына
5-қосымша

Нысан

*Ескерту. 5-қосымша алып тасталды - ҚР Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап
қолданысқа енгізіледі) бұйрығымен.*

**«Электрондық үкіметтің»
ақпараттандыру объектілеріне
және ақпараттық-коммуникациялық
инфрақұрылымның аса маңызды
объектілеріне жатқызылған
ақпараттық жүйелерге олардың
ақпараттық қауіпсіздік талаптарына
сәйкестігіне сынақтар жүргізу
қағидаларына 6-қосымша**

Мемлекеттік қызмет көрсетуге қойылатын негізгі талаптардың тізбесі

Ескерту. 6-қосымша жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ (01.01.2023 бастап қолданысқа енгізіледі) бұйрығымен.

«Ақпараттық қауіпсіздік талаптарына сәйкестікті сынау нәтижелері бойынша акт беру» мемлекеттік көрсетілетін қызмет стандарты		
1	Көрсетілетін қызметті берушінің атауы	ЦДИАӨМ Ақпараттық қауіпсіздік комитеті (бұдан әрі – көрсетілетін қызметті беруші)
2	Мемлекеттік қызмет көрсету тәсілдері (қол жеткізу арналары)	Өтінішті қабылдау және мемлекеттік қызметті көрсету нәтижесін беру «электрондық үкіметтің» веб-порталы (бұдан әрі – портал) арқылы жүзеге асырылады.
3	Мемлекеттік қызметті көрсету мерзімі	Көрсетілетін қызметті берушіге портал арқылы құжаттар топтамасын тапсырған сәттен бастап: 1) сынақ хаттамаларының оң нәтижелері кезінде – 10 (он) жұмыс күні. 2) бір немесе бірнеше сынақ хаттамаларының теріс нәтижелері кезінде – 15 (он бес) жұмыс күні.
4	Мемлекеттік қызмет көрсету нысаны	Электрондық (толық автоматтандырылған).
5	Мемлекеттік қызметті көрсетудің нәтижесі	Сынақ объектілерінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесі қоса берілген сынақтар актісі не мемлекеттік қызметті көрсетуден бас тарту туралы дәлелді жауап болып табылады; Мемлекеттік қызметті ұсыну нысаны электрондық.
6	Мемлекеттік қызмет көрсету кезінде көрсетілетін қызметті алушыдан алынатын төлем мөлшері және Қазақстан Республикасының заңнамасында көзделген жағдайларда оны алу тәсілдері	Мемлекеттік қызмет жеке және заңды тұлғаларға (бұдан әрі – көрсетілетін қызметті алушы) тегін көрсетіледі.
7	Көрсетілетін қызметті берушінің жә	1) көрсетілетін қызметті берушінің – Қазақстан Республикасының еңбек заңнамасына сәйкес демалыс және мереке күндерінен басқа, дүйсенбіден бастап жұманы қоса алғанда сағат 9.00-ден 18.30-ға дейін, сағат 13.00-ден 14.30-ға дейін түскі үзіліс.

	не ақпарат объектілерінің жұмыс кестесі	2) порталдың – тәулік бойы, жөндеу жұмыстарын жүргізуге байланысты техникалық үзілістерді қоспағанда (Қазақстан Республикасының еңбек заңнамасына сәйкес демалыс және мереке күндері, жұмыс уақыты аяқталғаннан кейін көрсетілетін қызметті алушы жүгінген кезде, мемлекеттік қызмет көрсету өтінішін қабылдау және нәтижесін беру келесі жұмыс күні жүзеге асырылады). Мемлекеттік қызмет көрсету орындарының мекенжайы www.egov.kz . порталында орналастырылды.
8	Мемлекеттік қызметті көрсету үшін қажет құжаттардың тізбесі:	Портал үшін: «Электрондық үкіметтің» ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (бағдарламалық өтінімді) және «электрондық үкіметтің» ақпараттық-коммуникациялық платформасын қоспағанда, сынақ объектілерін сынау кезінде: Қағиданың 7-қосымшаға сәйкес нысан бойынша сынақтар актісін алуға өтініш; бастапқы кодтарды талдау хаттамасының электрондық көшірмесі; ақпараттық қауіпсіздік функцияларын сынау хаттамасының электрондық көшірмесі; жүктемелік сынау хаттамасының электрондық көшірмесі; желілік инфрақұрылымды зерттеп-қарау хаттамасының электрондық көшірмесі; ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау хаттамасының электрондық көшірмесі; сынақ объектісінің меншік иесі немесе иеленушісі бекіткен Қағидалардың 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың электрондық көшірмесі. «Электрондық үкіметтің» ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (бағдарламалық өтінімді) сынау кезінде: Қағидаларға 7-қосымшаға сәйкес нысан бойынша сынақтар актісін алуға өтініш; бастапқы кодтарды талдау хаттамасының электрондық көшірмесі; ақпараттық қауіпсіздік функцияларын сынау хаттамасының электрондық көшірмесі; жүктемелік сынау хаттамасының электрондық көшірмесі; сынақ объектісінің меншік иесі немесе иеленушісі бекіткен Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың электрондық көшірмесі. «Электрондық үкіметтің» ақпараттық-коммуникациялық платформасын сынау кезінде: Қағидаларға 7-қосымшаға сәйкес нысан бойынша сынақтар актісін алуға өтініш; бастапқы кодтарды талдау хаттамасының электрондық көшірмесі; ақпараттық қауіпсіздік функцияларын сынау хаттамасының электрондық көшірмесі; желілік инфрақұрылымды зерттеп-қарау хаттамасының электрондық көшірмесі; ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау хаттамасының электрондық көшірмесі; сынақ объектісінің меншік иесі немесе иеленушісі бекіткен Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың электрондық көшірмесі. Біртекті бөлінген сынақ объектісінің тораптарын сынау кезінде: Қағидаларға 7-қосымшаға сәйкес нысан бойынша сынақтар актісін алуға өтініш; бастапқы кодтарды талдау хаттамасының электрондық көшірмесі; ақпараттық қауіпсіздік функцияларын сынау хаттамасының электрондық көшірмесі; сынақ объектісінің меншік иесі немесе иеленушісі бекіткен Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың электрондық көшірмесі.
9	Қазақстан Республикасының заңнамасында белгіленген мемлекеттік қызметті көрсетуден бас тарту негіздері	1) мемлекеттік көрсетілетін қызметті алу үшін көрсетілетін қызметті алушы ұсынған құжаттардың және (немесе) ондағы деректердің (мәліметтердің) дұрыс еместігін анықтау; 2) көрсетілетін қызметті алушының және (немесе) мемлекеттік қызмет көрсету үшін қажетті ұсынылған материалдардың, объектілердің, деректердің және мәліметтердің Қазақстан Республикасының нормативтік құқықтық актілерінде белгіленген талаптарға сәйкес келмеуі.
10	Мемлекеттік қызмет көрсетудің ерекшеліктерін ескере отырып, оның ішінде электрондық түрде және Мемлекеттік корпорация арқылы мемлекеттік қызмет көрсетуге қойылатын өзге де талаптар	Көрсетілетін қызметті алушының ЭЦҚ-сы болған жағдайда, мемлекеттік көрсетілетін қызметті электрондық нысанда портал арқылы алуына мүмкіндігі бар. Көрсетілетін қызметті алушы мемлекеттік қызмет көрсету тәртібі туралы ақпаратты порталдағы «жеке кабинеті» арқылы, сондай-ақ Бірыңғай байланыс орталығы арқылы қашықтықтан қол жеткізу режимінде алуға мүмкіндігі бар. Мемлекеттік қызмет портал арқылы көрсетілген кезде нашар көретіндерге арналған нұсқасы қолжетімді. Мемлекеттік қызмет көрсету мәселелері бойынша анықтама қызметтерінің байланыс телефондары порталда көрсетілген. Бірыңғай байланыс орталығы: 1414, 8- 800- 080- 7777.

**«Электрондық үкіметтің» ақпараттандыру
объектілеріне және ақпараттық-
коммуникациялық инфрақұрылымның аса
маңызды объектілеріне жатқызылған ақпараттық
жүйелерге олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне сынақтар жүргізу
қағидаларына
7-қосымша**

Нысан

**Сынақтар актісін алуға
Өтініш**

(өтініш берушінің атауы, БСН/ЖСН*, Т.А.Ә. (болған кезде))

(өтініш берушінің пошталық мекенжайы, e-mail және телефоны, облыс, қала, аудан)

(сынақтар объектісінің атауы)

ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтар нәтижелері
бойынша акт беруді сұрайды.

Қоса беріліп отырған құжаттар:

1. сынақтар объектісінің иесі (меншік иесі) бекіткен сынақ объектінің сипаттамасы туралы сауалнама-сұраулық;
2. бастапқы кодтарды талдау хаттамасы (нөмір, күні, қызмет берушінің атауы);
3. ақпараттық қауіпсіздік функцияларын сынау хаттамасы (нөмір, күні, қызмет берушінің атауы);
4. жүктемелік сынау хаттамасы (нөмір, күні, қызмет берушінің атауы);
5. желілік инфрақұрылымды зерттеп-қарау хаттамасы (нөмір, күні, қызмет берушінің атауы);
6. ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау хаттамасы (нөмір, күні, қызмет берушінің атауы);

Ақпараттық жүйелердегі заңмен қорғалатын құпияны құрайтын қол жеткізу
шектеулі дербес деректерді пайдалануға келісім беремін.

(қолы) М.О. (болған кезде)

20__ ЖЫЛҒЫ «__» _____

* бизнес сәйкестендіру нөмірі/жеке сәйкестендіру нөмірі

«Электрондық үкіметтің»
ақпараттандыру объектілеріне
және ақпараттық-коммуникациялық
инфрақұрылымның аса маңызды
объектілеріне жатқызылған
ақпараттық жүйелерге олардың
ақпараттық қауіпсіздік талаптарына
сәйкестігіне сынақтар жүргізу
қағидаларына 8-қосымша

Ақпараттандыру объектісінің жұмыс істеуі және (немесе)
функционалдығы өзгерістерінің
тізбесі

*Ескерту. Қағидалар 8-қосымшамен толықтырылды - ҚР Цифрлық даму,
инновациялар және аэроғарыш өнеркәсібі министрінің 30.09.2022 № 361/НҚ
(01.01.2023 бастан қолданысқа енгізіледі) бұйрығымен.*

Р /с №	Жүргізілген өзгерістер	Бастапқы кодтарды талдау	Ақпараттық қауіпсіздік функциялары	Жүкте-мелік сынау	Желілік инфрақұрылымды зерттеп-қарау	Ақпараттық қауіпсіздікті қамтамасыз ету процесін зерттеу
1	2	3	4	5	6	7
1.	Өзірлемелерортасын өзгерту (бағдарламалау тілі)	+	-	-	-	-
2.	ҚБҚ функциясын өзгерту	+	+	+	-	-
3.	Серверлік жабдықты ауыстыру	-	+	+	+	+
4.	Желілік жабдықты ауыстыру	-	-	+	+	-
5.	ОЖ, ДҚБЖ түрінің өзгеруі	-	+	+	-	-
6.	Сынақ объектісінің орналасу орнын өзгерту	-	+	-	+	+
7.	Сынақ объектісінің ішкі контурдан сыртқы контурға немесе керісінше көшуі	-	+	+	+	+
8.	Жаңа компонентті (серверді) қосу	-	+	-	+	+
9.	Басқа АЖ-лармен жаңа интеграция	+	+	+	+	+
10.	Ақпараттандыру объектісі сыныбының өзгеруі	-	+	-	+	+

Ескертпе:

«+» - сынақтар жүргізу қажет;

«-» - сынақтар жүргізудің қажеті жоқ.