"Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы

Қазақстан 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 тіркелді.

Ескерту. Бұйрықтың тақырыбы жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.04.2024 № 257/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

"Ақпараттандыру туралы" Қазақстан Республикасы Заңының 7-1-бабының 5) тармақшасына сәйкес **БҰЙЫРАМЫН:**

Ескерту. Кіріспе жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.04.2024 № 257/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1. Мыналар:

1) осы бұйрыққа 1-қосымшаға сәйкес "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі;

2) осы бұйрыққа 2-қосымшаға сәйкес "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары бекітілсін.

Ескерту. 1-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.04.2024 № 257/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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 3 маусымдағы
№111/НҚ бұйрығына
1-қосымша

"Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі

Ескерту. Әдістеме жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.04.2024 № 257/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы ережелер

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

2. Осы Әдістемеде мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) бағдарламалық бетбелгі – ақпараттандыру объектісіне рұқсатсыз қол жеткізуді және (немесе) оған әсер етуді жүзеге асыратын бағдарламалық қамтылымға (бұдан әрі – БҚ) жасырын енгізілген функционалдық объект;

2) бэкдор – аутентификацияны, сондай-ақ қауіпсіздіктің басқа стандартты әдістері мен технологияларын айналып өту арқылы бағдарламалық жасақтамаға рұқсатсыз қол жеткізуге арналған зиянды БҚ;

3) декларацияланбаған мүмкіндіктер (бұдан әрі – ДМ) – техникалық құжаттамада сипатталғандарға сәйкес келмейтін немесе көрсетілмеген БҚ-ның функционалдық мүмкіндіктері;

4) енуге қолмен тестілеу – қауіпсіз және бақыланатын шабуылдарды қолдана отырып, ақпараттандыру объектілерінің қорғалуын заңды бағалау, осалдықтарды анықтау және өтініш берушінің қызметіне нақты зиян келтірместен оларды пайдалану әрекеттері;

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

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

7) осалдық – пайдаланылуы ақпараттандыру объектісі тұтастығының және (немесе) құпиялылығының және (немесе) қолжетімділігінің бұзылуына алып келуі мүмкін ақпараттандыру объектісінің кемшілігі;

8) 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;

9) 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;

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

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

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

13) функционалдық объект – бағдарлама алгоритмінің аяқталған фрагментін іске асыру жөніндегі іс-қимылдарды орындауды жүзеге асыратын БҚ элементі (рәсім, функция, тармақ немесе өзге компонент);

14) функционалды объектілерді орындау бағыты – алгоритммен анықталған функционалды объектілердің реттілігі;

15) 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;

16) SYNAQ интернет-порталы – мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын ақпараттандыру объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынау бойынша қызмет көрсету процесін автоматтандыруға арналған мемлекеттік техникалық қызметтің интернет-порталы.

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 БҚ-ның осалдықтарын анықтау мақсатында жүргізіледі.

Мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілерінің бастапқы кодтарын талдау ДМ және БҚ осалдықтарын 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-қосымшаға сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың 5-тармағы 11) тармақшасының және 12) тармақшасының кестелерінде 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.

Мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілері бойынша БҚ кемшіліктерін анықтау бастапқы кодты талдаудың қолмен әдісімен және өтініш беруші ұсынған бастапқы кодтардың негізінде бастапқы кодты талдауға арналған бағдарламалық құралды пайдалана отырып жүргізіледі.

8. Мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілері бойынша БҚ ДМ анықтау бастапқы кодты егжей-тегжейлі қарап және ашық бастапқы коды бар кітапханаларда бэкдорларды іздеуді жүргізе отырып, бастапқы кодты талдаудың қолмен әдісімен жүргізіледі.

9. Бастапқы кодты талдау мыналарды қамтиды:

1) БҚ осалдықтарын анықтау;

2) мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілері үшін ДМ анықтау;

3) бастапқы кодты талдау нәтижелерін бекіту.

10. БҚ осалдықтарын анықтау мынадай тәртіппен жүзеге асырылады:

1) бастапқы деректерді дайындау ("электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің бастапқы кодтарын жүктеу, сканерлеу режимін таңдау (динамикалық және/немесе статикалық), сканерлеу режимдерінің сипаттамаларын баптау) жүргізіледі;

2) бастапқы кодты талдаудың қолмен әдісі және бастапқы деректерді дайындау (мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілерінің бастапқы кодтарын жүктеу), сканерлеу режимін таңдау (статикалық, тәуелділіктерді талдау және/немесе динамикалық), сканерлеу режимдерінің сипаттамаларын реттеу) жүргізіледі;

3) БҚ осалдықтарын анықтауға арналған БҚ іске қосылады;

4) жалған позитивтердің болуына бағдарламалық есептерге талдау жүргізіледі;

5) олардың сипаттамасы, бағыты (файлға жол) және тәуекел дәрежесі (жоғары, орташа, төмен) көрсетіле отырып, БҚ анықталған осалдықтардың тізбесін қамтитын есеп қалыптастырылады.

11. ДМ анықтау мынадай тәртіппен жүзеге асырылады:

1) сынақ объектісіне арналған техникалық құжаттаманы, оның ішінде ақпараттандыру объектісін құруға (дамытуға) арналған техникалық тапсырманы оның мақсаты, қолдану саласы, қолданылатын әдістер, шешілетін міндеттер сыныбы, қолдану кезіндегі шектеулер, техникалық құралдардың ең аз конфигурациясы, жұмыс істеу ортасы және жұмыс тәртібі туралы мәліметтер бөлігінде талдау;

2) сынақ объектісінің қолмен әдісімен бастапқы кодқа талдау жүргізу:

БҚ-ның модульдік және логикалық құрылымын, сондай-ақ жеке модульдерді зерттеу және осы құрылымдарды техникалық құжаттамада көрсетілгендермен салыстыру;

функционалдық объектілерді орындау бағытын зерделеу және өңдеу деректерін тексеру;

функционалдық объектілер деңгейінде бастапқы мәтіндердің толықтығын және артық болмауын бақылау;

есепте ДМ анықтау нәтижелерін кейіннен ұсыну үшін скриншот көмегімен ДМ-ны тіркеу;

3) олардың сипаттамасын, маршрутын (файлға жол) және скриншотын келтіре отырып, анықталған ДМ тізбесін қамтитын есепті қалыптастыру;

4) ашық бастапқы коды бар кітапханаларда, оның ішінде автоматтандырылған анализатордың көмегімен бэкдорларды іздеуді жүргізу;

5) осалдықтардың халықаралық дерекқорынан сәйкестендіргіш келтіре отырып, осалдықтардың сипаттамасын қамтитын есепті қалыптастыру.

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

13. Бастапқы кодтарды талдау нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың көшірмесін 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.

14. 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.

15. 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

16. 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.

17. Ақпараттық қауіпсіздік функцияларын сынау мыналарды қамтиды:

1) қауіпсіздік функцияларының техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілерінің және Қазақстан Республикасының аумағында қолданылатын ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін, оның ішінде бағдарламалық құралдарды қолдана отырып (қажет болған жағдайда) бағалауды;

2) мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілерінің кіруіне қолмен тестілеу;

3) бағдарламалық қамтылымның жаңартуларға сканерлеуі және конфигурацияны талдау;

4) байқау, сәйкестікті немесе сәйкессіздікті бағалау нәтижелері көрсетілген есепте сынақ нәтижелерін және анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдарды (қажет болған жағдайда) тіркеуді қамтиды.

18. Ақпараттық қауіпсіздік функцияларының тізбесі Әдістемеге 1-қосымшада және қолмен тестілеу функцияларының тізбесі Әдістемеге 2-қосымшада келтірілген.

19. Ақпараттық қауіпсіздік функцияларын сынау Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сауалнаманың 1) тармақшасының және 5-тармағының 4) тармақшасының кестелерінде санамаланған серверлер, виртуалды ресурстар және виртуалдандыру орталары бөлінісінде жүргізіледі.

20. Мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын сынақ объектілерінің енуіне қолмен тестілеуді қамтиды:

1) сынақ объектісіндегі осалдықтарды анықтау;

2) Анықталған осалдықтарды жою бойынша ұсынымдар қалыптастыру.

21. 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.

4-тарау. Жүктемелік сынау

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

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

24. 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.

25. Жүктемелік сынау мынадай тәртіппен жүзеге асырылады:

1) сынауға дайындық жүргізіледі;

2) сынақ жүргізіледі;

3) сынақ нәтижелері тіркеледі.

26. Сынауға дайындық мыналарды қамтиды:

1) сынау сценарийін анықтау;

2) сынаудың уақытша және сандық сипаттамаларын анықтау;

3) сынау жүргізу уақытын тапсырыс берушімен келісу.

27. 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.

28. 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.

29. 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.

5-тарау. Желілік инфрақұрылымды зерттеп-қарау

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

31. Желілік инфрақұрылымды зерттеу мыналарды қамтиды:

1) желілік инфрақұрылымды қорғау функцияларының техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілерінің және Қазақстан Республикасының аумағында қолданылатын ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін бағалау;

2) өтініш берушінің желілік инфрақұрылымын, оның ішінде бағдарламалық құралдарды қолдана отырып тексеру (қажет болған жағдайда);

3) Бағдарламалық құралдың жалпы осалдықтар мен тәуекелдер базасынан бағдарламалық қамтамасыз етудің белгілі осалдықтарының болуына сканерлеуі;

4) байқау, сәйкестікті немесе сәйкессіздікті бағалау нәтижелерін және анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдарды көрсете отырып, есепте алынған сынақ нәтижелерін тіркеуді (қажет болған жағдайда) қамтиды.

32. Желілік инфрақұрылымды қорғау функцияларының тізбесі осы Әдістемеге 3-қосымшада келтірілген.

33. Желілік инфрақұрылымды тексеру жөніндегі жұмыстар Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнаманың 5-тармағының 7) тармақшасының кестесінде көрсетілген сынақ объектісі желісінің (кіші желісінің) әрбір сегменті үшін жүргізіледі.

34. 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.

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

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

36. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеу мыналарды қамтиды:

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

2) байқау нәтижелерін, сәйкестікті немесе сәйкессіздікті бағалауды және анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдарды көрсете отырып, сынақты бағалау нәтижелерін тіркеуді (қажет болған жағдайда) қамтиды.

37. Ақпараттық қауіпсіздікті қамтамасыз ету процестерінің тізбесі және олардың мазмұны Әдістемеге 4-қосымшада келтірілген.

38. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін тексеру бойынша жұмыстар сынақ объектісі үшін жүргізіледі.

39. Ақпараттық қауіпсіздікті қамтамасыз ету процестерін тексеру нәтижелерін өнім берушінің осы жұмыс түрінің жауапты орындаушысы сынақ объектісінің сипаттамалары туралы сауалнама-сауалнаманың көшірмесін қоса бере отырып, ақпараттық қауіпсіздікті қамтамасыз ету процестерін тексеру хаттамасында (еркін нысанда) тіркейді.

Қосымшаларымен және есебімен ақпараттық қауіпсіздікті қамтамасыз ету процестерін тексеру хаттамасы:

1) аккредиттелген зертханамен тігіледі, беттердің өтпелі нөмірленуімен тігіледі және мөрмен (бар болса) мөрленеді;

2) мемлекеттік техникалық қызмет электрондық түрде өтініш берушінің Жеке кабинетінде SYNAQ интернет-порталында орналастырады.

Бағдарламалық құралдың ақпараттық қауіпсіздікті қамтамасыз ету саласындағы стандарттарға сәйкестігіне сканерлеу нәтижелері ақпараттық қауіпсіздікті қамтамасыз ету процестерін тексеру хаттамасына енгізілмейді және ұсынымдық сипатта болады.

7-тарау. "Электрондық үкіметтің" ақпараттандыру объектілерінің бастапқы кодтарынан құрастырылған орындалатын кодтардың өзгермеуін талдау

40. "Электрондық үкіметтің" ақпараттандыру объектілерінің бастапқы кодтарынан құрастырылған орындалатын кодтарды өзгермеуіне талдау жүргізудің (бұдан әрі – өзгермеуге талдау) объектілеріне өнеркәсіптік қолдануға енгізілген ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған "электрондық үкіметтің" ақпараттандыру объектілері жатады.

41. Өзгермеуді талдау жүргізу үшін мемлекеттік техникалық қызмет берген " электрондық үкіметтің" ақпараттандыру объектісінің бастапқы кодтарынан құрастырылған бастапқы және орындалатын кодтарды пайдалана отырып, мемлекеттік техникалық қызмет қызметкерінің бақылауымен өзгермеуге талдау жасау объектісін өнеркәсіптік пайдалану ортасында өрістетуді жүзеге асыру қажет.

42. Өзгермеуді талдау:

1) бағдарламалық қамтылымды орнату;

2) іске қосылған орындалатын кодқа өзгерістер енгізілуін анықтау;

3) бастапқы кодқа өзгеріс енгізілген жағдайда, осы Қағидаларға сәйкес бастапқы кодты талдау кіреді.

43. Өзгермеуге талдау "электрондық үкіметтің" ақпараттандыру объектісі орналасқан жерде мемлекеттік техникалық қызмет белгілеген бағдарламалық қамтылым арқылы тұрақты негізде жүзеге асырылады.

Өзгермейтіндікті талдауға арналған бағдарламалық қамтылым "электрондық үкімет " ақпараттандыру объектісінің оқиғаларын тіркеу журналдарын жинауды жүзеге асырады. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың 38-тармағының 4-тармақшасына сәйкес оқиғаларды тіркеу журналдары ақпараттық қауіпсіздік жөніндегі техникалық құжаттамада көрсетілген, бірақ 3 (үш) жылдан кем емес мерзім бойы сақталады және кем дегенде 2 (екі) ай жедел қолжетімді болады.

44. "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісі өзгермеуге талдау жүргізу үшін мемлекеттік техникалық қызметке:

1) "электрондық үкіметтің" ақпараттандыру объектісінің серверлік жабдықтарына қол жеткізу және мемлекеттік техникалық қызметтің ақпараттық қауіпсіздігінің инциденттері мен оқиғаларын мониторингілеу және басқару жүйесімен желі бойынша қол жеткізуді ұйымдастыруды;

2) оқиғаларды тіркеу журналына өзгермеуге талдау үшін бағдарламалық қамтылыммен болып жатқан оқиғалар туралы ақпаратты жазуды;

3) жұмыс орны, әкімшінің жұмыс орнына, "электрондық үкіметтің" ақпараттандыру объектісінің серверлік жабдығына физикалық қол жеткізуді қамтамасыз етеді.

45. Мемлекеттік техникалық қызмет "электрондық үкіметтің" ақпараттандыру объектісінің бастапқы кодына өзгеріс енгізілген жағдайда 5 (бес) жұмыс күні ішінде ресми хатпен Қазақстан Республикасының Ұлттық қауіпсіздік комитетін (бұдан әрі – ҰҚК), ақпараттық қауіпсіздік саласындағы уәкілетті органды және "электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісін хабардар етеді
.

46. Мемлекеттік техникалық қызмет әр тоқсан сайын, тоқсанның соңғы айының 25 (жиырма бес) күнінен кеш емес мерзімге дейін, ақпараттық қауіпсіздік саласындағы уәкілетті орган және ҰҚК үшін электрондық түрде өзгермеуге талдау нәтижелері жайлы жиынтық ақпаратты SYNAQ интернет-порталында орналастырады.

47. "Электрондық үкіметтің" ақпараттандыру объектісінің бастапқы кодына өзгеріс енгізілген жағдайда "электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісі өзгеріс енгізлген күннен кейін 2 (екі) жұмыс күні ішінде енгізілген өзгерістерді егжей-тегжейлі сипаттай отырып, бастапқы кодқа енгізілген өзгерістер туралы мемлекеттік техникалық қызметті хабардар етеді.

48. "Электрондық үкіметтің" ақпараттандыру объектісінің бастапқы кодына өзгеріс енгізілген жағдайда өтініш беруші Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2024 жылғы 29 ақпандағы № 110/НҚ бұйрығымен (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 34101 болып тіркелген) бекітілген "Электрондық үкіметтің" бірыңғай репозиторийінің жұмыс істеу қағидаларының 10-тармағының 1), 2), 3), 4) және 5) тармақшаларында айқындалған деректерді және "электрондық үкіметтің" ақпараттандыру объектісін құруға және дамытуға ЭҮБР және техникалық тапсырмасын бастапқы кодқа талдау жүргізу үшін мемлекеттік техникалық қызметке SYNAQ интернет-порталы арқылы жіберуді қамтамасыз етеді. Сонымен қатар, бастапқы кодты талдау мерзімі "электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісімен келісіледі.

49. "Электрондық үкіметтің" ақпараттандыру объектісі бойынша жұмыс істеуді қамтамасыз ету серверінде техникалық жұмыстар жүргізуді жоспарлау кезінде " электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісі 2 (екі) жұмыс күні ішінде мемлекеттік техникалық қызметті хабардар етеді.

50. Мемлекеттік техникалық қызмет ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған "электрондық үкіметтің" ақпараттандыру объектісінде өзгермеуге талдау үшін БҚ белгілейді.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса
маңызды объектілерінің
ақпараттық қауіпсіздік

талаптарына сәйкестігіне
сынақтар жүргізу әдістемесіне
1-қосымша

Ақпараттық қауіпсіздік функцияларының тізбесі

р/с №	Функциялардың атауы	Функциялардың мазмұны
1	2	3
Аудит безопасности		
1	Қауіпсіздік аудитінің автоматты әрекет ет әрекет етуі	Ақпараттық қауіпсіздік оқиғаларын жинау және талдау құралдарымен ақпараттық қауіпсіздік мониторингін қамтамасыз ету. 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 (сәттілігі 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.
Криптографиялық қолдау		
7	Криптографиялық кілттерді басқару	Мыналарды қолдаудың болуы: 1) криптографиялық кілттерді құру; 2) криптографиялық кілттерді бөлу; 3) криптографиялық кілттерге қолжетімділікті басқару; 4) криптографиялық кілттерді жою.
8	Криптографиялық операциялар	1. 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. 2. Құпия деректерді, қолжетімділігі шектеулі дербес деректерді немесе таратылуы шектеулі қызметтік ақпаратты қамтитын сынақ объектілері (бұдан әрі – СО) үшін ақпаратты криптографиялық қорғау құралдарын қолдану.
Пайдаланушының деректерін қорғау		
9	Қолжетімділікті басқару саясаты	Қауіпсіздік сервисімен тікелей немесе жанама операцияларды орындайтын пайдаланушылар үшін қолжетімділікті бөлуді жүзеге асыру.
10	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.
11	Деректерді аутентификациялау	Ақпараттың мазмұны айлакерлік жолымен ұқсастырылмағанын немесе түрлендірілмегенін кейін тексеру үшін пайдаланылатын өзіндік деректер жинағының дұрыстығы кепілдігін қолдау.
12	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.
13	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.
14	Ақпараттық ағындарды басқару функциялары	Деректер қоймасында қамтылған ақпаратты бақылаусыз таратуға жол бермеу мақсатында оған қолжетімділікті ұйымдастыру және қамтамасыз ету (бағдарламалық қамтылым (бұдан әрі – БҚ) сенімсіз болған жағдайда жариялаудан немесе түрлендіруден сенімді қорғауды іске асыру үшін ақпараттық ағындарды басқару).
15	Деректерді ОҚФ әрекетінен тыс жерден импорттау	Пайдаланушының деректерін олардың талап етілетін қауіпсіздік және қорғау атрибуттары болатындай етіп СО жіберуге арналған тетіктердің болуы.
16	СО шегінде жіберу	Пайдаланушының деректерін ішкі арна бойынша СО түрлі бөліктері арасында жіберген кезде қорғаудың болуы.
17	Қалған ақпаратты қорғау	Қалған ақпаратты толық қорғауды қамтамасыз ету, яғни ресурс босаған кезде алдыңғы жай-күйінің қолжетімсіздігін қамтамасыз ету.
		Кейбір шектелген (мысалы, уақыт аралығымен) соңғы операцияны немесе бірқатар операцияны жою және алдыңғы белгілі жай-күйге қайту мүмкіндігінің болуы. Кері

18	Ағымдағы жай-күйін кері қалпына келтіру	қалпына қайтару пайдаланушы деректерінің тұтастығын сақтау үшін операцияның немесе бірнеше операция нәтижелерін жоюға мүмкіндік береді.
19	Сақталатын деректердің тұтастығы	Пайдаланушының деректерін ОҚФ шегінде сақтаған кезде олардың қорғалуын қамтамасыз ету.
20	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.
21	ОҚФ арасында жіберген кезде пайдаланушы деректерінің тұтастығын қорға	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		
22	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.
23	Пайдаланушының атрибуттарын айқындау	Әрбір пайдаланушы үшін, ең болмаса, келесі қауіпсіздік атрибуттарын қолдау қажет: - сәйкестендіргіш; - теңестірілген ақпарат (мысалы, пароль); - қол жеткізу құқығы (рөлі).
24	Құпиялардың ерекшелігі	Егер теңестірілген ақпарат криптографиялық операциялармен қамтамасыз етілсе, сондай-ақ ашық және құпия кілттеріне қолдау көрсетілуі қажет.
25	Пайдаланушыны теңестіру	ОҚФ ұсынатын пайдаланушы теңестіру тетіктерінің болуы.

26	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.
27	Пайдаланушы-субъект байланыстырушы	Пайдаланушының тиісті қауіпсіздік атрибуттарын осы пайдаланушы атынан әрекет ететін субъектілермен байланыстыру керек.
Қауіпсіздікті басқару		
28	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.
29	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.
30	ОҚФ деректерін басқару	Тіркелетін оқиғалардың түсіндірілетін мәндерін өзгертуге, сұрастыруға, өзгертуге, жоюға, тазалауға, түрлерін анықтауға, тіркеу журналдарының өлшемін, субъектілердің қол жеткізу құқықтарын, қол жеткізу

		субъектілерінің есептік жазбаларының, парольдерінің, криптографиялық кілттерінің жарамдылық мерзімдерін өзгертуге әкімшінің жеке құқығының болуы.
31	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.
32	Қауіпсіздік атрибутының қолданыс мерзімі	Қауіпсіздік атрибуттарының қолданыс мерзімін белгілеу мүмкіндігін қамтамасыз ету.
33	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		
34	Іркіліс кезіндегі қауіпсіздік	Сервиспен аппараттық кідірістер кезінде (мысалы, электр қуатының іркілісінен орын алған) қауіпсіз жай-күйді сақтау.
35	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.
36	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.
37	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.
38	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.
39	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.
40	Екінші рет пайдалануды анықтау	Сервистің тең естірілген деректердің қайтадан пайдаланылуын айқындауын, қол жеткізуге жол бермеуге, тіркеу журналына жазба енгізуін және әкімшіге қауіпсіздіктің ықтимал бұзылуы туралы сигнал беруін қамтамасыз ету.
41	Өтініштер беру кезіндегі делдалдық	Сервистің қауіпсіздік саясатын жүзеге асыратын функциялар сервистің кез келген басқа функциясын орындауға рұқсат етілгенге дейін шақырылып, сәтті орындалуын қамтамасыз ету.
42	Доменді бөлу	Қауіпсіздік функциялары оларды сенімсіз субъектілердің араласуы мен бұрмалауынан қорғайтын

		меншікті орындауға арналған жеке доменді қолдап отыру.
43	Жай-күйлерді синхрондау хаттамасы	Серверлерде ұқсас функцияларды орындаған кезде жай-күйлерді синхрондауды қамтамасыз ету.
44	Уақыт белгілері	Қауіпсіздік функцияларының пайдалануына сенімді уақыт белгілерін ұсыну.
45	ОҚФ арасындағы деректердің келісілушілігі	Тіркелетін ақпаратты, сондай-ақ қолданылатын криптографиялық операциялар параметрлерін келісімді түсіндіруді қамтамасыз ету.
46	СО шегінде қайталау кезінде ОҚФ деректерінің келісілушілігі	СО түрлі бөліктерінде қайталаған кезде қауіпсіздік функциялары деректерінің үйлесмілігін қамтамасыз ету. Қайталанатын деректерді қамтитын бөліктер ажыратылғанда, үйлесімділік көрсетілген қауіпсіздік функцияларына кез келген сұрауларды өңдеу алдындағы қосылуды қалпына келтіргеннен кейін қамтамасыз етіледі.
47	Сценарийлерді (скриптерді) пайдалану	АИ-де модификациялауға құқықтары бар ықтимал сценарийлердің (скриптердің) болмауы, оларды қолдану ақпараттық қауіпсіздік инциденттерінің туындауына әкеп соғуы мүмкін.
Ресурстарды қолдану		
48	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.
49	Ресурстарды бөлу	1. Басқа пайдаланушылардың немесе субъектілердің ресурстарды монополиялауы себепті қызмет көрсетуден рұқсатсыз бас тартуға жол бермеу үшін пайдаланушылардың және субъектілердің ресурстарды пайдалануын басқаруды қамтамасыз ету. 2. Ақпараттандыру объектісі шеңберінде оның жұмыс істеуін қамтамасыз ететін бағдарламалық өнімдерді ғана пайдалану.

СО-ға қолжетімділік		
50	Таңдалатын атрибуттардың аясын шектеу	Қолжетімділік әдісі немесе орны және/немесе уақыты негізінде (мысалы, тәулік уақыты, апта күні) қол жеткізу жүзеге асырылып отырылған порттан пайдаланушы таңдай алатын қауіпсіздік атрибуттарымен қатар пайдаланушы байланыста болуы мүмкін субъектілердің атрибуттарын да шектеу.
51	Қатарлас сеанстарды шектеу	Бір пайдаланушыға ұсынылатын қатарлас сеанстардың барынша көп санын шектеу. Бұл шаманың ұйғарынды мәнін әкімші белгілейді.
52	Сеансты бұғаттау	Пайдаланушы әрекетсіздігі ұзақтығының әкімші белгілеген мәні аяқталғаннан кейін жұмыс сеансы мәжбүрлі аяқтау.
53	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.
54	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.
55	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		
		Зиянды кодтан қорғану үшін серверлерден, қажеттілік туындаған жағдайда сынақ объектісінің жұмыс

56	Вирустарға қарсы қорғау құралдарының болуы	станцияларынан зиянды кодты анықтау және бұғаттау немесе жою, мониторинг құралдарын қолдану.
57	Вирустарға қарсы қорғау құралдарына арналған лицензия	Серверлерге және жұмыс станцияларына вирустарға қарсы қорғау құралдарының лицензиялары (сатып алынған, шектелген, еркін таратылатын) болуы тиіс.
58	Вирустарға қарсы қорғау сигнатуралары базасын және бағдарламалық қамтылымды жаңарту	Вирустарға қарсы қорғау құралдарының ұдайы жаңартылып, өзекті күйде болуын қамтамасыз ету.
59	Вирустарға қарсы қорғау құралдарына қолжетімділікті басқару	Вирустарға қарсы қорғау құралдарын орталықтандырылған басқару мен конфигурациялауды жүзеге асыру.
60	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		
61	БҚ-ның ұдайы жаңартылуы	Серверлер мен жұмыс станцияларының жалпыжүйелік және қолданбалы БҚ ұдайы жаңартылуын қамтамасыз ету.
62	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		
63	Қолданбалы БҚ әзірлеу және тестілеу ортасы	Қолданбалы БҚ-ны өнеркәсіптік пайдалану ортасынан оқшауландырылған қолданбалы БҚ әзірлеу және тестілеу үшін ортаның болуын қамтамасыз ету.
64	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.
65	Қолданбалы БҚ өрістету жүйесі	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ өрістету (тарату) жүйесінің болуы.
		Өнеркәсіптік пайдалану ортасындағы серверлер мен

66	Қолданбалы БҚ өрістету жүйесіне қол жеткізудің аражігін ажырату	жұмыс станцияларындағы қолданбалы БҚ ажырату (тарату) жүйесіне қол жеткізуді басқаруды қамтамасыз ету.
Мемлекеттік органдардың ақпараттандыру объектілерінде, жергілікті атқарушы органдарда және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінде "құпия ақпараттың таралып кетуінен қорғау"		
67	Қол жеткізуді басқару саясаты	Құпия ақпараттың таралып кетуінен қорғау жүйесін басқару
68	Жүйе компоненттерін жаңарту	Ақпараттың таралып кетуінен қорғау жүйесін үнемі жаңартып отыруды және жаңартып отыруды қамтамасыз ету.
69	Бөлім қауіпсіздігі атрибуты	Аутентификация рәсімдерін ұйымдастыру қағидаларына сәйкес пароль саясатын қолдануды қамтамасыз ету.
70	Деректерді сақтау	Құпия ақпараттың таралып кетуінен қорғау жүйесінің оқиғалар журналдарын кемінде үш жыл және жедел қолжетімділікте кемінде екі ай сақтау.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық- коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу әдістемесіне
2-қосымша

Қолмен тестілеу функцияларының тізбесі

№	Функциялардың атауы	Функциялардың мазмұны
1	Сәулет, дизайн және қауіп-қатер моделі (Architecture, Design and Threat Modeling)	Қолданба дизайны мен сынақ объектісінің архитектурасының қауіпсіздігін және осалдықтардың болмауын қамтамасыз ету.
2	Аутентификация (Authentication)	Сынақ объектісінде пайдаланушылардың аутентификациясының дұрыс жұмыс істеуін қамтамасыз ету (логин/пароль, көп факторлы авторизация, хэштеу және басқа криптографиялық әдістер).
		Әрбір пайдаланушы үшін бірегей сессия құруды және сессияны ортақ пайдалануға техникалық тыйым салуды (бұғаттауды)

3	Сессияны басқару (Session Management)	қамтамасыз ету. Әрекетсіздік уақыты аяқталғаннан кейін пайдаланушы сеансын бұғаттау (Timeout session).
4	Қол жеткізуді басқару (Access Control)	Пайдаланушылардың құқықтарының аражігін ажыратуды қамтамасыз ету және сынақ объектісіне рұқсатсыз кіруді болдырмау.
5	Тексеру, сүзу және кодтау (Validation, Sanitation and Encoding)	Енгізу арқылы шабуылдардың алдын алу үшін пайдаланушының кіріс деректерін сүзуді қамтамасыз ету, сондай-ақ олардың контекстін зиянкестерден қорғауға кепілдік беретін дұрыс Шығыс кодтауын қамтамасыз ету.
6	Сақталған криптография (Stored Cryptography)	Сенімді шифрлау алгоритмдерін қолдану және криптографиялық кілттерді қауіпсіз басқару мен сақтауды қамтамасыз ету.
7	Қателерді өңдеу және логинг (Error Handling and Logging)	Қауіпсіздік талаптарына сәйкес оларды қорғауды ескере отырып, сынақ объектісі пайдаланушыларының іс-әрекеттерін және ақпараттық қауіпсіздік оқиғаларын журналдауды қамтамасыз ету. Құпия деректері бар жиналған журналдар сынақ объектісінің серверлерінде ұзақ уақыт сақталмауы керек және белгілі бір уақыт өткеннен кейін жойылуы керек.
8	Деректерді қорғау (Data Protection)	Жіктеушіге сәйкес ақпаратты криптографиялық қорғау құралдарын пайдалана отырып, сынақ объектісінде деректерді беру және сақтау кезінде құпиялылықты қамтамасыз ету.
9	Байланыс (Communication)	Қауіпсіз байланыс хаттамалары мен шифрлау алгоритмдерін пайдалана отырып, деректерді беру кезінде сынақ объектісінің қауіпсіздігін қамтамасыз ету.
10	Зиянды код (Malicious Code)	Сынақ объектісінде зиянды кодтың орындалуын болдырмау үшін қорғау құралдарын қолдану.
11	Бизнес-логика (Business Logic)	Техникалық тапсырмаға сәйкес сынақ объектісінің логикалық жұмысының дұрыс жұмысын қамтамасыз ету.

12	Файлдар мен ресурстар (Files and Resources)	Қолданба серверлерінен тыс үшінші тарап және сенімсіз көздерден алынған деректерді сақтауды қамтамасыз ету.
13	Қолданбаның бағдарламалық интерфейсі (API)	API келесі талаптарға сәйкестігін қамтамасыз ету: - API-де барлық веб-қызметтерге қол жеткізу үшін дұрыс авторизация, сеансты басқарудың негізгі параметрлері және аутентификация болуы керек; - API интерфейстері олардың параметрлері төменнен жоғары сенім деңгейіне ауысқан жағдайда енгізілген деректерді тиісті түрде тексеруі керек; - бұлтты және серверсіз сияқты әртүрлі API-де барлық қажетті қауіпсіздік басқару элементтері болуы керек.
14	Конфигурация (Configuration)	Қауіпсіз конфигурация параметрлерін, үшінші тарап кітапханаларын пайдалануды, сондай-ақ қауіпті компоненттерді сүзуді және сынақ объектісін пайдалану кезінде конфигурация файлдарындағы құпия деректерді сенімді қорғауды қамтамасыз ету.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздік талаптарына
сәйкестігіне сынақтар жүргізу
әдістемесіне
3-қосымша

Желілік инфрақұрылымды қорғау функцияларының тізбесі

№ п/п	Функциялардың атауы	Функциялардың мазмұны
1	2	3
		1. Пайдаланушының жүзеге асырылған әрекеттермен байланысын орнату үшін есептік жазбалардың бірегей сәйкестендіргіштерін пайдалану. 2. Артықшылықты қол жеткізу құқықтары оларды пайдалану қажеттілігі негізінде есептік жазбаларға арналуы тиіс.

1	Сәйкестендіру және аутентификация	3. Сәтсіз және сәтті аутентификация әрекеттерін тіркеу. 4. Сеанс уақытын шектеу. 5. Аутентификациядан бас тарту (аутентификацияның сәтсіз әрекеттерінің белгілі бір санына қол жеткізу кезінде субъектіге кіруден бас тарту мүмкіндігінің болуы). 6. Күшті құпия сөздерді пайдалану және таңдау. 7. Парольді тұрақты ауыстыруды жүргізу, сондай-ақ – қажетіне қарай.
2	Аудиттерді белгілеу (желілік қосылулардың қауіпсіздігіне байланысты оқиғалар туралы есептер қалыптастыру және олардың бар болуы)	1. Ақпараттық қауіпсіздік жағдайына байланысты оқиғаларды тіркеу, бұл ретте оқиғалар журналдары мыналарды қамтуы тиіс: пайдаланушылардың идентификаторлары; жүйелік әрекеттер; кіру және шығу сияқты негізгі оқиғалардың күні, уақыты және мәліметтері; сәтті және қабылданбаған қол жеткізу әрекеттері туралы есептер ; жүйе конфигурациясының өзгерістері; артықшылықтарды пайдалану; желілік мекенжайлар мен хаттамалар. 2. Ақпараттық қауіпсіздікті бұзумен байланысты оқиғаларға мониторинг жүргізу және мониторинг нәтижелерін талдау. 3. Оқиғаларды тіркеу журналдарын ақпараттық қауіпсіздік жөніндегі техникалық құжаттамада көрсетілген мерзім бойы, бірақ үш жылдан кем емес мерзімге сақтау және олардың екі айдан кем емес мерзімге оперативтік сақтауда болуы. 4. Оқиғаларды тіркеу журналдарын араласудан және рұқсатсыз кіруден қорғауды қамтамасыз ету, бұл ретте: жүйелік әкімшілерде журналдарды өзгертуге, жоюға

		және өшіруге өкілеттіктердің болуына жол берілмейді; құпия Ақпараттық жүйелер журналдардың резервтік қоймасын құруды және жүргізуді талап етеді. 5. Ақпараттық қауіпсіздік оқиғаларының сыни түрлері туралы хабарландырудың болуы. 6. Оқиғаларды тіркеу журналдарының уақытын UTC(kz) ДҮНИЕЖҮЗІЛІК ҮЙЛЕСТІРІЛГЕН уақыттың ұлттық шкаласын жаңғыртатын уақыт пен жиілік эталонымен синхрондауды қамтамасыз ету.
3	Басып кіруді анықтау	1. Басып кірулерді (желілік инфрақұрылымға ықтимал басып кірулерді) болжауға, оларды нақты уақыт ауқымында анықтауға және тиісті дабылды көтеруге мүмкіндік беретін қаражаттың болуын қамтамасыз ету. 2. Қағидалар базасын автоматтандырылған жаңарту мүмкіндігі.
4	Желілік қауіпсіздікті басқару	1. Жергілікті желінің кабельдік жүйесінің пайдаланылмаған интерфейстері белсенді жабдықтан физикалық түрде ажыратылуы тиіс. 2. Мемлекеттік органдар мен жергілікті атқарушы органдардың ішкі контурының жергілікті желісін Интернетке қосуды болдырмау, сондай-ақ ішкі контурдың жергілікті желісін және мемлекеттік органдар мен жергілікті атқарушы органдардың сыртқы контурының жергілікті желісін өзара ұштастыруды болдырмау. 3. Мемлекеттік органдар мен жергілікті атқарушы органдардың ақпараттық жүйесін бағдарламалық-аппараттық қамтамасыз етуді басқару ақпараттық жүйе иесінің ішкі жергілікті желісінен жүзеге асырылуы тиіс.

		4. Жергілікті желіні логикалық және/немесе физикалық сегменттеу құралдарын қолдану. 5. Ақпараттандыру объектісінің компоненттері арасындағы, сондай-ақ ақпараттандыру объектісі мен оның жұмыс істеу ортасы арасындағы уақыт бойынша синхрондауды қамтамасыз ету.
5	Желіаралық экрандар	1. Әр интерфейсте кіріс және шығыс пакеттерді сүзуді қамтамасыз ету. 2. Жабдық параметрлерінде пайдаланылмаған порттар бұғатталуы тиіс. 3. Желілік мекенжайларды түрлендіру.
6	Желілер арқылы жіберілетін деректердің тұтастығын, құпиялығын сақтау	Жергілікті желілерді біріктіретін арнайы байланыс арнасын ұйымдастыру кезінде ақпаратты криптографиялық қорғау құралдарын пайдалана отырып, ақпаратты қорғаудың бағдарламалық-техникалық құралдары, оның ішінде криптографиялық шифрлау қолданылуы тиіс.
7	Ақпарат алмасу бойынша жасалған іс-қимылдардан бас тартпаушылық	Желілік трафикті бақылау және талдау құралдарын қолдану.
8	Үздіксіз жұмыс және қалыпқа келуді қамтамасыз ету	Қол жетімділік пен ақаулыққа төзімділікті қамтамасыз ету үшін деректерді өңдеудің аппараттық-бағдарламалық құралдарын, деректерді сақтау жүйелерін, деректерді сақтау желілерінің компоненттерін және деректерді беру арналарын резервтеу пайдаланылуы тиіс.
9	Сенімді арна	Басқалардан қисынды түрде ерекшеленетін және оның тараптарының сенімді аутентификациясын, сондай-ақ деректерді өзгертуден және ашудан қорғауды қамтамасыз ететін қашықтағы сенімді арна өнімімен байланысу үшін қамтамасыз ету. Екі жақтың да сенімді арна арқылы байланыс орнатуға мүмкіндік беруін қамтамасыз ету.

10	Сенімді бағдар	Қашықтағы пайдаланушымен байланысу үшін басқалардан қисынды түрде ерекшеленетін және оның тараптарының сенімді аутентификациясын, сондай-ақ деректерді өзгертуден және ашудан қорғауды қамтамасыз ететін маршрутты ұсыну. Пайдаланушының сенімді маршрут арқылы байланыс орнатуға мүмкіндік беруін қамтамасыз ету. Қашықтағы пайдаланушының бастапқы аутентификациясы және қашықтан басқару үшін сенімді маршрутты пайдалану міндетті болып табылады.

"Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне 4-қосымша

Ақпараттық қауіпсіздікті қамтамасыз ету процестерінің тізбесі мен олардың мазмұны

№ п/п	Процестердің атауы	АҚ қамтамасыз ету процестерінің мазмұнына қойылатын талап
1	2	3
		1. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидаларында айқындалған активтерді сәйкестендіру тәртібіне сәйкес активтерді сәйкестендіру. 2. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау ережелерінде айқындалған жіктеу жүйесіне сәйкес ақпаратты жіктеу. 3. Тестілеу объектісі үшін анықталған сыныптың ақпараттандыру объектілерін жіктеу қағидаларының талаптарына сәйкестігін тексеру. 4. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидаларында

1	Ақпараттық-коммуникациялық технологиялармен байланысты активтерді басқару	айқындалған таңбалау қағидаттарына сәйкес активтерді таңбалау. 5. Сәйкестендірілген активтерге жауапты тұлғаларды бекіту. 6. Қабылданған тізілім нысанына сәйкес активтер тізілімін жүргізу және өзектендіру. 7. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидаларында айқындалған жіктеу жүйесіне сәйкес активтермен жұмыс істеу рәсімдерін айқындау, құжаттау және іске асыру (беру, пайдалану, сақтау, енгізу/шығару және қайтару). 8. Есептеу техникасы, телекоммуникациялық жабдық және бағдарламалық қамтамасыз ету құралдарын паспорттау. 9. Ақпараттық-коммуникациялық технологиялармен байланысты активтерді қабылдау / жөнелту кезінде жұмыстарды қауіпсіз ұйымдастыру. 10. Серверлік және телекоммуникациялық жабдықтарды, деректерді сақтау жүйелерін, жұмыс станцияларын, ақпарат тасығыштарды қауіпсіз кәдеге жарату (қайта пайдалану).
		1. Ақпараттық қауіпсіздік бөлімшесінің немесе ақпараттық қауіпсіздікке жауапты, ақпараттық технологиялар бөлімшесінен оқшауланған, тікелей жоғары басшылыққа бағынатын қызметкердің болуы. 2. Жұмыс топтарының жұмыс істеуі және жұмыстарды үйлестіру және ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша кеңестер өткізу. 3. Ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманы әзірлеу (өзектендіру), бекіту, басшылықтың мақұлдауы, олардың мазмұнын қызметкерлер мен орындаушылар тарапынан тартылатын қызметкерлерге жеткізу.

2	Ақпараттық қауіпсіздікті ұйымдастыру	4. Ақпараттық қауіпсіздік мамандарының өкілетті органдарымен, кәсіби қауымдастықтарымен, кәсіби қауымдастықтарымен немесе форумдарымен байланыста болу. 5. Ақпараттық қауіпсіздікті қамтамасыз ету рәсімдерін, оның ішінде бөгде ұйымдарды тарту кезінде айқындау және құжаттау. 6. Ақпаратты қорғау қажеттіліктерін көрсететін құпиялылық немесе жарияламау туралы келісімді әзірлеу (қайта қарау). 7. Ақпараттық қауіпсіздік және қызмет көрсету деңгейі жөніндегі талаптарды айқындау және үшінші тарап ұйымдарымен келісімдерге енгізу. Келісім ережелерінің іске асырылуын бақылау.
3	Қызметкерлермен байланысты қауіпсіздік	1. Жұмысқа қабылдау кезінде кандидаттарды алдын ала тексеру. 2. Қызметкерлердің лауазымдық нұсқаулықтарында және (немесе) еңбек шартының талаптарында және орындаушылар тарапынан тартылатын жұмыспен қамту, еңбек қатынастарын өзгерту немесе тоқтату кезеңіндегі ақпараттық қауіпсіздікке байланысты рөлдерді, міндеттер мен жауапкершіліктерді және сынақ объектісі иесінің міндеттемелерін айқындау, тағайындау және көрсету. 3. Ақпараттық қауіпсіздікті қамтамасыз ету саласында міндеттемелері бар қызметкерлерді жұмыстан шығару рәсімдерін айқындау және құжаттау. 4. Ақпараттық қауіпсіздік ережелерін бұзушыларға жасалатын іс-қимылдарды айқындау және регламенттеу. 5. Қызметкерлерге олардың қызметтік міндеттерін орындауды қозғайтын ақпараттық қауіпсіздікті қамтамасыз ету саясаттарындағы, қағидаларындағы және

		рәсімдеріндегі өзгерістер туралы хабарлау. 6. Қызметкерлердің және тараптан тартылатын орындаушылардың жұмыспен қамту, еңбек қатынастарын өзгерту немесе тоқтату кезеңінде ақпараттық қауіпсіздікті қамтамасыз етуге байланысты міндеттер мен жауапкершіліктер туралы хабардар болуы және орындауы. 7. Ақпараттық қауіпсіздік саласындағы қызметкерлерді оқыту және даярлау. 8. Қызметкерлердің және орындаушылар тарапынан тартылатын ақпараттық қауіпсіздікке қатысты міндеттемелерді орындау мүмкіндігін қамтамасыз ету үшін басшылықтың жауапкершілігі.
4	АҚ оқиғаларының мониторингі және АҚ инциденттерін басқару	1. Пайдаланушы, оператор, әкімші және операциялық жүйелердің оқиғаларын, дерекқорды басқару жүйелерін, антивирустық бағдарламаларды, қолданбалы бағдарламаларды, телекоммуникациялық жабдықтарды, шабуылдарды анықтау және алдын алу жүйелерін, мазмұнды басқару жүйелерін тіркеу. 2. Оқиғаларды тіркеу журналдарын жүргізу, сақтау және қорғау. 3. Оқиғаларды тіркеу журналдарын талдауды жүзеге асыру. 4. Тіркелген оқиғаларды бақылау және ақпараттық қауіпсіздік үшін маңыздылығы жоғары және маңызды оқиғалар туралы ескерту . 5. Ақпараттық қауіпсіздік оқиғасын бағалау және шешім қабылдау. 6. Қызметкерлерді және тараптан тартылатын орындаушыларды әзірлеу, құжаттау, олардың назарына жеткізу, ақпараттық қауіпсіздік инциденттеріне ден қою рәсімдерін орындау.

		7. Ақпараттық қауіпсіздік инциденттеріне талдау жүргізу.
5	АҚ үздіксіздігін басқару	1. Ақпараттық қауіпсіздіктің үздіксіздігін жоспарлау. 2. Ақпараттық қауіпсіздікті немесе бизнес-процестерді қамтамасыз ету процесінің үздіксіздігінің бұзылуының ықтимал себебі болып табылатын оқиғаларды идентификациялау. 3. Штаттан тыс (дағдарыстық) жағдайларда ақпараттық қауіпсіздіктің үздіксіздігінің қажетті деңгейін ұстап тұру процестері мен рәсімдерін әзірлеу (өзектендіру), енгізу. 4. Қызметкерлерді және орындаушылар тарапынан тартылатын қызметкерлерді анықтау, құжаттау, олардың назарына жеткізу, штаттан тыс (дағдарыстық жағдайларда) рәсімдерді орындау. 5. Ақпараттық қауіпсіздіктің үздіксіздігін қамтамасыз ету процестері мен рәсімдерін тексеру (тестілеу), талдау және бағалау. 6. Заңнаманың талаптарын ескере отырып, ақпаратты өңдеу құралдарын, ақпараттандыру объектісін резервтеу.
6	Желілік қауіпсіздікті басқару	1. Қызметкерлерді және орындаушылар тарапынан тартылатын қызметкерлерді анықтау, құжаттау және олардың назарына жеткізу, желілік жабдықты басқару рәсімдерін орындау. 2. Желілерге қызмет көрсету және ақпарат беру жөніндегі келісімдерге қауіпсіздікті қамтамасыз ету тетіктерін, барлық желілік қызметтер мен сервистер үшін қолжетімділік деңгейлерін айқындау және енгізу. 3. Қызметкерлерді және орындаушылар тарапынан тартылатын қызметкерлерді анықтау, құжаттау, олардың назарына жеткізу, желілер мен Желілік қызметтерді пайдалану, ақпарат беру, Интернетке, телекоммуникация және байланыс

		желілеріне қосылу және желілік ресурстарға сымсыз қол жеткізуді пайдалану саясаттары мен рәсімдерін орындау. 4. Желі және электрондық хабарламалар арқылы берілетін ақпаратты қорғау құралдарын қолдану жөніндегі рәсімдерді айқындау, құжаттау және орындау . 5. Заңнама талаптарын ескеретін желілерді қосу және өзара іс-қимыл жасау тәсілдері.
7	Криптографиялық қорғау әдістері	1. Заңнаманың талаптарын ескеретін криптографиялық кілттерді дайындау, есепке алу, сақтау, беру, пайдалану, қайтару (жою), қорғау мәселелерін қамтитын криптографиялық кілттерді басқаруды регламенттеу. 2. Аутентификациялық деректерді қоса алғанда, ақпаратты сақтау және беру кезінде криптографиялық құралдарды қолдану.
8	Ақпараттық қауіпсіздік тәуекелдерін басқару	1. Тәуекелдерді бағалау әдістемесін таңдау; 2. Сәйкестендірілген және жіктелген активтер үшін қатерлерді (тәуекелдерді) сәйкестендіру және ақпараттық қауіпсіздік қатерлерінің (тәуекелдерінің) каталогын қалыптастыру (өзектендіру). Ақпараттық қауіпсіздікті қамтамасыз ету процестерімен байланысты қатерлерді (тәуекелдерді), тәуекелдерді каталогта көрсету. 3. Анықталған тәуекелдерді бағалау (қайта бағалау). 4. Тәуекелдерді өңдеу, тәуекелдерді өңдеу жоспарын қалыптастыру және бекіту (өзектендіру). 5. Тәуекелдерді бақылау және қайта қарау.
		1. Пайдаланушыларды ақпаратқа, қолданбалы жүйелердің функцияларына, қызметтерге, жүйелік БҚ, желілер мен желілік сервистерге қол жеткізу құқықтарының аражігін ажырату

9	Қол жеткізуді басқару	қағидаларымен әзірлеу (өзектендіру), құжаттандыру, таныстыру. 2. Пайдаланушыларды сәйкестендіру, аутентификациялау және авторизациялаудың қолданылатын әдістері мен рәсімдері. 3. Электрондық ақпараттық ресурстарға қол жеткізу құқықтарының аражігін ажырату қағидаларында белгіленген қол жеткізу құқықтарының аражігін ажырату қағидаларын іске асыру. 4. Пайдаланушыларды тіркеу және тіркеуден шығару (бұғаттау) рәсімдері. 5. Артықшылықты кіру құқығымен есептік жазбаларды басқару. 6. Пайдаланушының аутентификация процедураларында криптографиялық әдістерді қолдану және басқару. 7. Қол жеткізу құқықтарының өзгеруін басқару. 8. Құпия сөздерді басқару. 9. Артықшылықты утилиталарды пайдалану. 10. Сынақ объектісінің бастапқы кодына қол жеткізуді басқару.
10		1. Заңнама талаптарын ескере отырып, серверлік, телекоммуникациялық жабдықтарды, деректерді сақтау жүйелерін орналастыру. 2. Ақпараттық-коммуникациялық технологиялармен байланысты активтер орналастырылған үй-жайлардың қауіпсіздік периметрін физикалық қорғау. 3. Заңнаманың талаптарын ескеретін негізгі және резервтік серверлік үй-жайларды ұйымдастыру. 4. Негізгі және резервтік серверлік үй-жайларды заңнаманың талаптарын ескеретін қамтамасыз ету жүйелерімен жарақтандыру. 5. Серверлік үй-жайларға бақыланатын қол жеткізуді ұйымдастыру.

	Физикалық қауіпсіздік және табиғи қауіптерден қорғау	6. Серверлік үй-жайда жұмыстарды ұйымдастыру. 7. Серверлік және телекоммуникациялық жабдықтарды, деректерді сақтау жүйелерін және қамтамасыз ету жүйелерін техникалық сүйемелдеу және оларға қызмет көрсету жөніндегі жұмыстарды ұйымдастыру. 8. Жабдықты электрмен жабдықтау жүйесіндегі ақаулардан және коммуналдық қызметтердің жұмысындағы ақаулардан туындаған басқа да бұзылулардан қорғау тәсілдері. 9. Кабельдік жүйенің қауіпсіздігін қамтамасыз ету. 10. Кросс үй-жайларының қауіпсіздігін қамтамасыз ету.
11	АҚ қамтамасыз етудің пайдалану рәсімдері	1. Ақпараттық қауіпсіздікті қамтамасыз етудің пайдалану рәсімдерін регламенттейтін нұсқаулықтарды әзірлеу (өзектендіру), құжаттау, пайдаланушыларды таныстыру. 2. Ақпараттық қауіпсіздікті қамтамасыз ету құралдары мен жүйелерін қолдану. 3. Ақпараттың сақтық көшірмесін жасау процедуралары және көшіру нәтижелерін тексеру. Сақтық көшірмелерді сақтау орындарының қауіпсіздігі. 4. Оқиғаларды тіркеу журналдарының уақытын бір уақыт көзімен синхрондау. 5. Қолданыстағы жүйелерде қолданбалы және жүйелік бағдарламалық қамтылымның жаңа нұсқаларын орнату кезіндегі өзгерістерді басқару процедуралары. 6. Осалдықтарды бақылау және басқару. 7. Қызметкерлерді таныстыру және мобильді құрылғылар мен ақпарат тасығыштарды пайдалану ережелерін ережелерін іске асыру. 8. Қашықтан жұмысты ұйымдастыру жөніндегі

		нұсқаулықтың ережелерін әзірлеу (өзектендіру), қызметкерлерді таныстыру, іске асыру. 9. Сынақ объектісінің жұмыс қабілеттілігінің мониторингі. 10. Әзірлеу, тестілеу және пайдалану орталарын бөлу. 11. Электрондық пошта хабарламалары мен ақпараттарды Интернет арқылы беру кезінде құпиялылықты қамтамасыз ету. 12. Заңнаманың талаптарына сәйкес интернетті ұсыну және сыртқы электрондық пошта жүйелерімен өзара іс-қимыл жасау тәсілдері. 13. Интернет ресурстарына қол жеткізу кезіндегі шектеулер мен сүзу тәртібі.
12	Заңнамалық және шарттық талаптарға сәйкестігі	1. Сынақ объектісі үшін заңнамалық, нормативтік, өзге де міндетті, шарттық талаптарды айқындау (өзектендіру), құжаттау. 2. Зияткерлік меншік құқықтарына байланысты заңнамалық, нормативтік және шарттық талаптарға сәйкестікті іске асыратын рәсімдерді енгізу. 3. Заңнаманың нормаларына сәйкес келетін құпия және дербес деректерді қорғау саясатын әзірлеу және іске асыру. 4. Қолданылатын криптографиялық әдістер мен құралдардың заңнама талаптарына және келісімдерге (шарттарға) сәйкестігі. 5. Ақпараттық қауіпсіздік аудитін жүргізу. 6. Ақпараттық қауіпсіздік жөніндегі заңнаманың, стандарттардың және техникалық құжаттаманың талаптарына сәйкестігі тұрғысынан сынақ объектісіне талдау жүргізу. 7. Жазбаларды жоғалтудан, бүлінуден, бұрмалануден, рұқсатсыз кіруден және заңнамалық, нормативтік, шарттық талаптарға сәйкес рұқсатсыз шығарудан қорғау.
		1. Ақпараттық қауіпсіздікке байланысты және қолданыстағы

13	Жүйелерді сатып алу, әзірлеу және қызмет көрсету	заңнамаға және стандарттарға сәйкес келетін талаптарды сынақ объектісіне техникалық құжаттаманың құрамына енгізу (өзектендіру). 2. Пайдаланылатын жүйелер үшін БҚ (жүйелік және қолданбалы) өзгерістерін басқарудың қауіпсіз рәсімдерін айқындау және қолдану. 3. Сынақ объектісі бойынша, оның ішінде бөгде ұйым жүзеге асыратын әзірлеу процесін бақылау. 4. Бөгде ұйым жүзеге асыратын жүйені техникалық сүйемелдеу процесін бақылау. 5. Жүйенің қауіпсіздік мүмкіндіктерін тексеру.

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

"Электрондық үкіметтің" ақпараттандыру объектілері және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары

Ескерту. Қағидалар жаңа редакцияда – ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 30.04.2024 № 257/НҚ (қолданысқа енгізілу тәртібін 4 -т. қараңыз) бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы "Электрондық үкіметтің" ақпараттандыру объектілері мен ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары (бұдан әрі – Қағидалар) "Ақпараттандыру туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 5) тармақшасына сәйкес әзірленді және "электрондық үкіметтің " ақпараттандыру объектілері мен ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай негізгі ұғымдар мен қысқартулар пайдаланылады:

1) ақпараттық жүйе – ақпараттық өзара іс-қимыл арқылы белгілі бір технологиялық әрекеттерді іске асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсетуші персоналдың және техникалық құжаттаманың ұйымдық реттелген жиынтығы;

2) ақпараттық жүйенің кіші жүйесі – ақпараттық жүйенің мақсатына жету үшін қажетті оның белгілі бір функцияларын іске асыратын ақпараттық жүйенің жиынтық бөлігі (құрамдас бөлігі) ;

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

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

5) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның интернет-порталы – "электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынау бойынша қызмет көрсету процесін автоматтандыруға арналған ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның интернет-порталы;

6) бағдарламалық қамтылым – бағдарламалардың, бағдарламалық кодтардың, сондай-ақ оларды пайдалану үшін қажетті техникалық құжаттамасы бар бағдарламалық өнімдердің жиынтығы;

7) "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының бағдарламалық өнімі (бұдан әрі – платформалық бағдарламалық өнім) – "электрондық үкіметтің" ақпараттық-коммуникациялық платформасында әзірленген және орналастырылған бағдарламалық қамтылым;

8) бастапқы кодтар – сынақ объектісінің компакт-дискідегі сәтті компиляциясы үшін қажетті кітапханалары мен файлдары бар сынақ объектісінің компоненттері мен модульдерінің бастапқы кодтары;

9) үлестірілген сынақ объектісі – бірдей мақсаттарға арналған, бірдей функцияларды орындайтын және бірдей қолданбалы бағдарламалық қамтылымды пайдаланатын, бірдей архитектура бойынша салынған көптеген, оның ішінде белгісіз тораптардан тұратын сынақ объектісі;

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

11) өнім беруші – мемлекеттік техникалық қызмет немесе аккредиттелген сынақ зертханасы;

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

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

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

15) сынақ объектісі – ақпараттық қауіпсіздік талаптарына сәйкестігін сынау жөніндегі жұмыстар жүргізілетін ақпараттандыру объектісі;

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

17) "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы – мемлекеттік органның қызметін автоматтандыруға, оның ішінде мемлекеттік функцияларды автоматтандыруға және олардан туындайтын мемлекеттік қызметтер көрсетуге, сондай-ақ мемлекеттік электрондық ақпараттық ресурстарды орталықтандырылған жинауға, өңдеуге, сақтауға арналған технологиялық платформа;

18) SYNAQ интернет-порталы – мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын ақпараттандыру объектілерінің 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 м.а. 27.09.2024 № 605/НҚ (08.01.2025 бастап қолданысқа енгізіледі) бұйрығымен.

3. Объектілердің АҚ талаптарына сәйкестігін сынау (бұдан әрі – сынақтар) сынақ объектілерінің техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілерінің және Қазақстан Республикасының аумағында қолданылатын ақпараттық қауіпсіздік саласындағы стандарттардың талаптарына сәйкестігін бағалау жөніндегі жұмыстарды қамтиды және сынақ объектісін штаттық пайдалану ортасында жүргізіледі.

4. "Электрондық үкіметтің" ақпараттық-коммуникациялық платформасында және " электрондық үкіметтің" ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (бағдарламалық өнімді) қоспағанда, сынақ объектісінің сынақтарының құрамына мынадай жұмыс түрлері кіреді:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) жүктеме сынағы;

4) желілік инфрақұрылымды зерттеу;

5) АҚ қамтамасыз ету процестерін тексеру.

5. Сынақ объектісінің бастапқы коды (мемлекеттік орган меншік иесі (иеленуші) және (немесе) тапсырыс беруші болып табылатын ақпараттандыру объектілерін қоспағанда) болмаған немесе сынақтардың басқа түрін (түрлерін) жүргізу мүмкін болмаған жағдайда, сынақ объектісінің бастапқы кодына немесе сынақтарының басқа түріне (түрлеріне) талдау жүргізудің міндетті остігі туралы ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның шешімімен өтініш берушінің сұрау салуы бойынша белгіленеді.

Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган осы Қағидалардың 7-тармағына сәйкес басқа түрлері бойынша сынақтар жүргізу кезеңінде бастапқы кодты немесе сынақ объектісінің сынақтарының басқа түрін (түрлерін) талдауды алып тастау туралы өтінім берушінің сұрау салуының негізділігін тексеру туралы Өнім берушіге сұрау салуды жібереді.

6. "Электрондық үкіметтің" ақпараттық-коммуникациялық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (платформалық бағдарламалық өнімді) сынауға мыналар кіреді:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) жүктеме сынағы;

4) АҚ қамтамасыз ету процестерін зерттеп-қарау.

Ескерту. 6-тармаққа өзгеріс енгізілді - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 27.09.2024 № 605/НҚ (08.01.2025 бастап қолданысқа енгізіледі) бұйрығымен.

7. "Электрондық үкіметтің" ақпараттық-коммуникациялық платформасының сынақтарына мыналар кіреді:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) желілік инфрақұрылымды зерттеу;

4) АҚ қамтамасыз ету процестерін тексеру.

8. Біртекті үлестірілген сынау объектілері үшін сынақтар үлестірілген сынау объектісі түйіндерінің жалпы санының кемінде оннан бір бөлігін құрайтын жалпы санында үлестірілген сынау объектісінің орталық(тар) торабы(тары) үшін және кейбір (өтініш берушінің келісімі бойынша) жекелеген тораптары үшін жүргізіледі.

Біртекті үлестірілген сынақ объектісінің орталық торабы (тары) үшін сынақтар жұмыс түрлерінің толық құрамында жүргізіледі.

Біртекті үлестірілген сынақ объектісінің тораптары үшін сынақтар құрамына мыналар кіреді:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау.

9. Сынақ объектісі басқа ақпараттандыру объектісімен интеграцияланған (қолданыстағы немесе жоспарланған) жағдайда сынақтар сынақ объектісінің құрамына интеграцияны қамтамасыз ететін компоненттерді (интеграция модулі, интеграцияның кіші жүйесі, интеграциялық автобус немесе басқа) енгізе отырып жүргізіледі.

2-тарау. Ақпараттандыру объектілерінің мемлекеттік техникалық қызметтегі ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібі

10. 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 объектісінің меншік иесінің (иеленушісінің) ЭЦҚ-мен куәландырылған осы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнама;

2) шарттарға немесе заңды тұлғаның басшысын тағайындау туралы құжатқа қол қоюға уәкілетті тұлғаға сенімхаттың электрондық көшірмесі (заңды тұлғалар үшін);

3) ақпараттандыру саласындағы уәкілетті органмен және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органмен келісілген ақпараттандыру объектісіне техникалық тапсырманың электрондық көшірмесі;

4) сәтті құрастыру үшін қажетті кітапханалары мен файлдары бар сынақ объектісінің компоненттері мен модульдерінің бастапқы кодтары (қажет болған кезде);

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

6) иеленуші (меншік иесі) сынақтар жүргізуге өтінім беруге өтінім берушіге уәкілеттік беретін құжаттың электрондық көшірмесі (қажет болған жағдайда):

7) сынақ объектісінің меншік иесі (иеленуші) және (немесе) тапсырыс беруші мемлекеттік орган болып табылатын растайтын құжат.

11. Егер өтініш беруші сатып алуды мемлекеттік сатып алу веб-порталы арқылы жүзеге асырған жағдайда, сынақтар жүргізуге өтінім ағымдағы жылдың 1 қарашасынан кешіктірілмей қабылданады.

12. Мемлекеттік техникалық қызмет өтінімді алған күннен бастап үш жұмыс күні ішінде осы Қағидалардың 10-тармағында көрсетілген құжаттардың толықтығын тексеруді жүзеге асырады.

13. Өтінім мен қоса берілген құжаттар осы Қағидалардың 10-тармағында көрсетілген талаптарға сәйкес келмеген жағдайда, өтінім қайтару себептері көрсетіле отырып, он жұмыс күні ішінде өтініш берушіге қайтарылады.

14. Мемлекеттік техникалық қызмет осы Қағидалардың 10-тармағына сәйкес құжаттардың толық топтамасының болуына өтінімді тексергеннен кейін үш жұмыс күні ішінде өтініш берушіге жібереді:

1) мемлекеттік сатып алу веб-порталы арқылы сатып алуды жүзеге асыру кезінде сынақтар жүргізуге арналған шартқа техникалық ерекшеліктің жобасы. Өтініш беруші техникалық ерекшелік жобасын алған күннен бастап үш жұмыс күні ішінде мемлекеттік сатып алу туралы шартты тікелей жасасу арқылы бір көзден алу тәсілімен мемлекеттік сатып алу туралы шарттың жобасын мемлекеттік сатып алу веб-порталында орналастырады;

2) мемлекеттік сатып алу веб-порталын қолданбай сатып алуды жүзеге асыру кезінде сынақтар жүргізуге арналған шарттың екі данасы. Өтініш беруші жоғарыда көрсетілген шарттың екі данасын алған күннен бастап бес жұмыс күні ішінде оларға қол қояды және шарттың бір данасын мемлекеттік техникалық қызметке қайтарады.

15. Егер өтініш беруші сатып алуды мемлекеттік сатып алу веб-порталы арқылы жүзеге асырса және 15 қарашаға дейінгі мерзімде мемлекеттік техникалық қызмет атына мемлекеттік сатып алу туралы шартты мемлекеттік сатып алу веб-порталы арқылы жібермеген жағдайда, өтінім жойылады және өтініш берушіге қайтарылады.

16. Сынақ мерзімі Өтініш берушімен келісіледі және сынақ бойынша жұмыс көлеміне және сынақ объектісінің жіктеу сипаттамаларына байланысты болады.

Сынақ жүргізу мерзімдерін келісу мүмкін болмаған жағдайда, өтінім қанағаттандырусыз өтініш берушіге сынақ мерзімдерін айқындау үшін ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға жүгіну мүмкіндігін көрсете отырып қайтарылады.

17. Сынақтарды өткізу үшін өтініш беруші мемлекеттік техникалық қызмет үшін:

1) жұмыс орнын, пайдаланушының жұмыс орнына, серверлік және желілік жабдыққа, фото және бейне тіркеуді жүргізе отырып, сынақ объектісінің телекоммуникация желісіне және сынақ объектісіне құжаттамаға және ілеспе құжаттамаға, оның ішінде сынақ объектісінің құрамына кіретін сынақ объектісі мен компоненттерді сүйемелдеу және техникалық қолдау шарттарына физикалық қол жеткізуді;

2) техникалық құжаттама талаптарына сәйкес сынақ объектісінің функцияларын көрсетуді қамтамасыз етеді.

18. Өтініш беруші осы Қағидалардың 17-тармағының талаптарын қамтамасыз ете алмаған жағдайда, сынақтар оның орындалу мерзімін ұзартуға арналған шартқа қосымша келісімге қол қоюды ескере отырып, оларды қамтамасыз ету үшін өтініш берушіге қажетті уақытқа тоқтатыла тұрады.

19. Сынақтар "Электрондық үкіметтің" ақпараттандыру объектілері және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне сәйкес жүргізіледі.

20. Сынақтарды жүргізу кезінде осы Қағидалардың 10-тармағының 1) тармақшасына және сынақ объектісінің нақты жай-күйіне сәйкес берілген сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнаманың деректері арасында алшақтық анықталды, өтініш беруші мемлекеттік техникалық қызметке SYNAQ интернет-порталында сынақ объектісінің меншік иесінің (иесінің) ЭЦҚ-мен куәландырылған сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сұрақнаманы жібереді. Сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сауалнама (қажет болған жағдайда) сынақ мерзімін ұзартуға және сынақ жүргізу құнын өзгертуге қосымша келісім жасасу үшін негіз болады.

21. Қажет болған жағдайда, егер сынақ жүргізу кезінде сынақ мерзімі аяқталғанға дейін сынақтардың бір немесе бірнеше түрі бойынша қайта сынақ жүргізу қажеттілігі анықталса, өтініш беруші мемлекеттік техникалық қызметке сұрау салады және өтеусіз негізде осы жұмыс түрлері бойынша қайта сынақ жүргізу туралы қосымша келісім жасалады.

22. Сынақтарға кіретін жұмыстардың нәтижелері және анықталған сәйкессіздіктерді жою жөніндегі ұсынымдар жұмыстардың барлық түрлері аяқталғаннан кейін өтініш берушінің Жеке кабинетінде SYNAQ интернет-порталында орналастырылатын жекелеген хаттамаларға енгізіледі.

23. Мемлекеттік техникалық қызметтің сынақтарға кіретін жұмыстардың әрбір түрін жүргізуіне бағалар Заңның 14-бабының 2-тармағына сәйкес белгіленеді.

24. Сынақтарды өткізу құнын есептеу үшін өтініш беруші мемлекеттік техникалық қызметке SYNAQ интернет-порталында сынақ объектісінің меншік иесінің (иесінің) ЭЦҚ-мен куәландырылған сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнама жібереді.

25. Өтініш беруші сынақтар кезінде анықталған сәйкессіздіктерді SYNAQ интернет-порталында жүргізілген жұмыстар бойынша сынақтар хаттамаларын орналастырған күннен бастап алпыс жұмыс күні ішінде жойған және мемлекеттік техникалық қызметке SYNAQ интернет-порталы арқылы анықталған сәйкессіздіктерді түзету нәтижелерімен салыстыру кестесін қоса бере отырып, қайталама сынақтар

жүргізуге сұрау салуды жіберген кезде, мемлекеттік техникалық қызмет өтеусіз негізде өтініш берушіден сұрау салуды алған күннен бастап жиырма жұмыс күні ішінде тиісті құжаттарды ресімдей отырып, осы жұмыс түрлері бойынша қайта сынақтар жүргізеді.

Өтініш беруші белгіленген мерзімде екі реттен артық емес қайталама сынақтарға өтінім бере алады.

Қажет болған жағдайда, өтініш беруші қайталама сынақтарды өткізу мерзімін ұзартуға қосымша өтінім беру арқылы, бірақ 20 жұмыс күнінен аспайтын мерзімін бір рет ұзарта алады.

Белгіленген мерзімді өткізу осы Қағидаларда белгіленген жалпы тәртіппен сынақтар жүргізу үшін негіз болып табылады.

26. Объектінің бағдарламалық қамтамасыз етуіне өзгерістер енгізуге байланысты сәйкессіздіктер түзетілгеннен кейін қайталама сынақтар жүргізу кезінде бастапқы кодқа талдау жүргізіледі.

Бұл ретте өтініш беруші қайталама сынақтар жүргізуге сұрау салуға сынақ объектісінің құрамдас бөліктері мен модульдерінің бастапқы кодтарын сынақ объектісін сәтті құрастыру үшін қажетті кітапханалармен және файлдармен қоса тіркейді.

27. Қайта сынақтар жүргізу кезінде сәйкессіздіктер анықталған жағдайда мемлекеттік техникалық қызмет теріс қорытындысы бар хаттаманы ресімдейді, одан кейін сынақтар осы Қағидалардың 2-тарауында белгіленген тәртіппен жүргізіледі.

28. Сынақ хаттамалары жоғалған, бүлінген немесе бүлінген кезде, сондай-ақ сынақ объектісінің сипаттамалары туралы сауалнама-сауалнамадағы деректер өзгерген жағдайда, бұрын теріс нәтижесі бар қағаз тасығышта хаттамалар алған сынақ объектілері үшін жұмыстардың бір немесе бірнеше түрі бойынша сынақтар жүргізу кезінде сынақ объектісінің меншік иесі немесе иесі себептерін көрсете отырып, мемлекеттік техникалық қызметке хабарлама жібереді.

Мемлекеттік техникалық қызмет хабарламаны алған күннен бастап бес жұмыс күні ішінде бұрын берілген сынақтар хаттамасының (ларының) телнұсқасын не сынақ объектісінің сипаттамалары туралы өзектендірілген сауалнама-сұрақнамасы бар сынақтар хаттамасының (ларының) телнұсқасын береді.

3-тарау. Ақпараттандыру объектілерінің сынақ зертханаларында ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібі

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

30. 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 немесе заңды тұлғаның басшысын тағайындау туралы құжатқа қол қоюға уәкілетті тұлғаға сенімхаттың көшірмесі (заңды тұлғалар үшін);

2) сынақ объектісінің меншік иесі немесе иеленуші қағаз жеткізгіште бекіткен осы Қағидаларға 2-қосымшаға сәйкес сынақ объектісінің сипаттамалары туралы сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнама;

3) меншік иесі немесе иеленуші бекіткен, мемлекеттік заңды тұлғаның ақпараттық жүйесі және мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйені қоспағанда, ақпараттандыру объектісіне техникалық тапсырма немесе техникалық ерекшелік, мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған, компакт-дискіде (қажет болған жағдайда);

4) библиотекам дискіде сәтті компиляциялау үшін қажетті кітапханалары мен файлдары бар сынақ объектісінің компоненттері мен модульдерінің бастапқы кодтары (қажет болған жағдайда);

5) осы Қағидаларға 3-қосымшаға сәйкес сынақ объектісінің ақпараттық қауіпсіздігі жөніндегі техникалық құжаттаманың бекітілген тізбесінің көшірмелері электронам дискіде электрондық түрде (қажет болған жағдайда);

6) өтініш берушіге меншік иесі немесе иеленушісі сынақтар жүргізуге өтінім беруге (қажет болған жағдайда) уәкілеттік беретін құжат.

31. Сынақтар "Электрондық үкіметтің" ақпараттандыру объектілері мен ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне сәйкес жүргізіледі.

32. Егер өтініш беруші жүргізілген жұмыстар бойынша сынақ хаттамаларын алған күннен бастап жиырма жұмыс күні ішінде сынақтар кезінде анықталған сәйкессіздіктерді жойған және анықталған сәйкессіздіктерді түзету нәтижелерімен салыстыру кестесін қоса бере отырып, өнім берушіге қайталама сынақтар жүргізуге сұрау салуды жіберген жағдайда, өнім беруші өтініш берушіден хабарлама алған күннен бастап жиырма жұмыс күні ішінде өтеусіз негізде тиісті құжаттарды ресімдей отырып, осы жұмыс түрлеріне.

Өтініш беруші белгіленген мерзімде екі реттен артық емес қайталама сынақтарға өтінім бере алады.

Қажет болған жағдайда, өтініш беруші қайталама сынақтарды өткізу мерзімін ұзартуға қосымша өтінім беру арқылы, бірақ 20 жұмыс күнінен аспайтын мерзімін бір рет ұзарта алады.

Белгіленген мерзімді өткізу осы Қағидаларда белгіленген жалпы тәртіппен сынақтар жүргізу үшін негіз болып табылады.

33. Қайталама сынақтар жүргізу кезінде сәйкессіздіктер анықталған жағдайда өнім беруші теріс қорытындысы бар хаттаманы ресімдейді, содан кейін сынақтар осы Қағидалардың 3-тарауында белгіленген тәртіппен жүргізіледі.

34. Сынақ хаттамалары жоғалған, бүлінген немесе бүлінген кезде сынақ объектісінің меншік иесі немесе иеленушісі өнім берушіге себептерін көрсете отырып хабарлама жібереді.

Өнім беруші хабарламаны алған күннен бастап бес жұмыс күні ішінде сынақ хаттамаларының телнұсқасын береді.

4-тарау. Ақпараттық қауіпсіздік талаптарына сәйкестігін сынау хаттамаларын беру және кері қайтарып алу тәртібі

35. Ақпараттық қауіпсіздік талаптарына сәйкестігін сынау хаттамаларын қызмет беруші береді.

36. Сынақ хаттамаларының жарамдылық мерзімі "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын қоспағанда, сынақ объектісін өнеркәсіптік пайдалану мерзімімен немесе сынақ объектісін жаңғыртуды бастау сәтіне дейін шектеледі.

Бұл ретте ақпараттандыру объектісін өнеркісіптік пайдалануға енгізу үшін сынақтың жекелеген түрі бойынша хаттаманың қолданылу мерзімі хаттама берілген күннен бастап бір жылдан аспайды.

"Электрондық үкіметтің" ақпараттық-коммуникациялық платформасын сынау хаттамалары бір жыл қолданылу мерзімімен беріледі.

37. Қызмет беруші тұрақты негізде тізімнің ақпараттық қауіпсіздігін қамтамасыз ету саласындағы уәкілетті органға мынадай деректерді ұсынады:

1) сынақтар жүргізуге өтінім;

2) сынақ зертханаларында сынақтар жүргізуге арналған шарт туралы ақпарат (күні, нөмірі);

3) сынақ объектісінің атауы;

4) сынақ объектісінің меншік иесінің және (немесе) иесінің атауы;

5) нәтижесін көрсете отырып, жұмыстың әрбір түрі бойынша ақпараттық қауіпсіздік талаптарына сәйкестігін сынаудың тізілімдік нөмірі, берілген күні және хаттамасы;

6) сынақ объектісінің серверлік және желілік жабдықтың нақты орналасқан орны;

7) сынақ объектісінің меншік иесі немесе иеленушісі бекіткен сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық.

Аккредиттелген сынақ зертханасы жоғарыда көрсетілген деректерді ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның интернет-порталына енгізуді қамтамасыз етеді.

Есеп түріндегі ақпарат аккредиттелген сынақ зертханасының ЭЦҚ-сын пайдалана отырып қалыптастырылады.

Жоғарыда көрсетілген деректерді беру үшін мемлекеттік техникалық қызмет SYNAQ интернет-порталының ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның интернет-порталымен интеграциялануын қамтамасыз етеді.

38. Ақпараттандыру объектісінің жұмыс істеу жағдайлары мен функционалдығына өзгерістер енгізген кезде ақпараттандыру объектісінің меншік иесі немесе иеленушісі өзгерістерге әкелген жұмыстарды аяқтағаннан кейін көрсетілетін қызмет берушіге барлық жүргізілген өзгерістердің сипаттамасын және сынақтар объектісінің меншік иесінің немесе иеленушісімен бекітілген сынақтар объектісінің сипаттамалары туралы жаңартылған сауалнама-сұраулықты қоса беріп, хабарлама жібереді.

39. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган осы Қағидалардың талаптарына сәйкессіздіктер анықталған кезде, анықталған сәйкессіздіктерді қоса бере отырып, қызмет берушіге ақпарат жібереді.

40. Қызмет беруші ақпараттандыру объектісіне енгізілген өзгерістерді және (немесе) анықталған сәйкессіздіктер туралы ақпаратты және (немесе) өзгермеуге талдау нәтижелері бойынша бастапқы кодтың өзгерістері туралы ақпаратты он жұмыс күнінен аспайтын мерзімде қарайды және тестілеу хаттамаларын кері қайтарып алу және ақпараттандыру объектісінің жұмыс істеу және (немесе) функционалдығы жағдайлары өзгерген кезде функциялары бұзылған сынақтардың сол түрін жүргізу қажеттілігі туралы шешім қабылдайды.

Шешім осы Қағидаларға 4-қосымшаға сәйкес ақпараттандыру объектісінің жұмыс істеуі және (немесе) функционалдығы өзгерістерінің тізбесі ескеріле отырып қабылданады.

41. Сынақ хаттамаларын қайтарып алу кезінде меншік иесі немесе иеленуші үш ай мерзімде осы Қағидалардың 2 немесе 3-тарауында белгіленген тәртіппен сынақтардан өту туралы қызмет берушілерге өтінім беру үшін шаралар қолданады.

42. Шағымды қарау өтініш беруші ақпараттық қауіпсіздік талаптарына сәйкестігін сынау хаттамаларының нәтижелерімен келіспеген жағдайда жүзеге асырылады және оны Қазақстан Республикасы Әкімшілік рәсімдік-процестік кодексінің 91-бабына сәйкес ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган жүргізеді.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздік талаптарына
сәйкестігіне сынақтар жүргізу
қағидаларына
1-қосымша
Нысан

_____
(өнім берушінің атауы)
Сынақтарды өткізуге өтінім

_____
(сынақ объектісінің атауы)
ақпараттық қауіпсіздік талаптарына сәйкестігіне (бұдан әрі – сынақтар)
1._____
(өтініш беруші ұйымның атауы, аты-жөні (бар болса),
бизнес-сәйкестендіру нөмірі, өтініш берушінің банктік деректемелері)

_____
_____
(өтініш берушінің пошталық мекенжайы, e-mail және телефоны, облыс, қала, аудан)
сынақтарды өткізуді сұрайды

_____
(сынақ объектісінің атауы, нұсқа нөмірі, әзірленген күні)
мынадай жұмыс түрлерінің құрамында:
1) _____
2) _____
3) _____
4) _____
5) _____
(Қағидалардың 7 / 8 / 9 / 10 / 11 тармақтарына сәйкес жұмыс түрлерінің тізбесі
(қажетті элементті көрсетіңіз)
2. Сыналатын сынақ объектісінің меншік иесі (иеленуші) туралы мәліметтер

_____
(атауы немесе аты-жөні (бар болса)

_____
_____
(облыс, қала, аудан, пошта мекенжайы, телефон)
3. Сыналатын сынақ объектісін әзірлеуші туралы мәліметтер

_____
(әзірлеуші туралы ақпарат, авторлардың атауы немесе аты-жөні (бар болса))

_____
(қала, аудан, пошта мекенжайы, телеф)
4. Өнім берушімен байланыс үшін жауапты тұлғаның деректері:
1) тегі, аты, әкесінің аты: _____;
2) лауазымы: _____;
3) жұмыс телефоны:_____, ұялы
телефон:_____;

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

Өтініш беруші ұйымның басшысы/ аты-жөні (бар болса),

өтініш берушінің _____ (өтініш берушінің)

(Мөр орны) болған жағдайда

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу қағидаларына
2-қосымша
Нысан

Сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық

1. Сынақ объектісінің атауы:_____

_____

2. Сынақ объектісіне қысқаша аннотация _____

_____

(мақсаты және қолдану саласы)

3. Сынақ объектісінің жіктелуі:

1) қолданбалы бағдарламалық қамтылым класы _____.

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

4. Сынақ объектісінің архитектурасы:

1) сынақ объектісінің функционалдық схемасы (қажет болған жағдайда):

сынақ объектісінің компоненттерін, модульдерін және олардың IP-мекенжайларын;

компоненттер немесе модульдер арасындағы байланыстар және ақпараттық ағындардың бағыттары;

басқа объектілермен интеграциялық өзара әрекеттесудің қосылу нүктелері ақпараттандыру;

пайдаланушылардың қосылу нүктелері;

деректерді сақтау орындары мен технологиялары;

қолданылатын резервтік жабдық;

қолданылатын терминдер мен аббревиатураларды түсіндіру;

2) сынақ объектісінің деректерін беру желісінің сызбасы (қажет болған жағдайда):

желінің архитектурасы мен сипаттамалары;
серверлік желілік және коммуникациялық жабдықтар;
адресации и применяемых сетевых технологий;
пайдаланылатын жергілікті, ведомстволық (корпоративтік) және жаһандық желілер;
ақауларға төзімділікті қамтамасыз ету және резервтеу жөніндегі шешімдер(лар).
қолданылатын терминдер мен аббревиатураларды түсіндіру;
5. Сынақ объектісі туралы ақпарат:
1) серверлік жабдық туралы ақпарат (кестені толтыру):

№ п/п	Сервердің немесе виртуалды ресурстың атауы (домендік атау, желі атауы немесе логикалық Сервер атауы)	Мақсаты (орындалатын функционалдық міндеттер)	Саны	Сервердің сипаттамалары немесе қолданылатын мәлімделген виртуалды ресурстар	ОЖ, ДҚБЖ, БҚ, қосымшалар, кітапханалар және серверлерде орнатылған немесе пайдаланылатын виртуалды сервистер қорғау құралдары (нұсқа нөмірлері көрсетілген бағдарламалық ортаның құрамы)	Қолданылатын IP мекенжайлары
1	2	3	4	5	6	7

2) желілік жабдық туралы ақпарат (кестені толтыру):

№ п/п	Желілік жабдықтың атауы (бренд / модель)	Мақсаты (орындалатын функционалдық міндеттер)	Саны	Қолданылатын желілік технологиялар	Желіні қорғаудың қолданылатын технологиялары	Пайдаланылған IP мекенжайлары, соның ішінде басқару порты
1	2	3	4	5	6	7

3) серверлік және желілік жабдықтың орналасқан жері (кестені толтыру):

№ п/п	Серверлік үй-жайдың иесі	Серверлік үй-жай иесінің заңды мекенжайы	Нақты орналасқан жері – сервер бөлмесінің мекен-жайы	Қолжетімділікті ұйымдастыруға жауапты тұлғалар (Т.А.Ә. (бар болса)	Жауапты тұлғалардың телефондары (жұмысшылар, ұялы)
1	2	3	4	5	6

4) резервтік серверлік жабдықтың сипаттамалары (кестені толтыру):

					ОЖ, ДҚБЖ, БҚ,		

№ п/п	Сервердің немесе виртуалды ресурстың атауы (домендік атау, желі атауы немесе логикалық Сервер атауы)	Мақсаты (орындалатын функционалдық міндеттер)	Саны	Сипаттамалары сервер немесе пайдаланылған мәлімделген виртуалды ресурстар	қосымшалар , кітапханалар және серверлерде орнатылған немесе пайдаланылатын виртуалды сервистер қорғау құралдары (нұсқа нөмірлері көрсетілген бағдарламалық ортаның құрамы)	Қолданылатын IP мекенжайлары	Брондау әдісі
1	2	3	4	5	6	7	8

5) резервтік желілік жабдықтың сипаттамалары (кестені толтыру):

№ п/п	Желілік жабдықтың атауы (бренд / модель)	Мақсаты (орындалатын функционалдық міндеттер)	Саны	Қолданылатын желілік технологиялар	Желіні қорғаудың қолданылатын технологиялары	Пайдаланылған IP мекенжайлары, соның ішінде басқару порты	Брондау әдісі
1	2	3	4	5	6	7	8

6) резервтік серверлік және желілік жабдықтың орналасқан жері (кестені толтыру):

№ п/п	Серверлік үй-жай иесінің заңды мекенжайы	Серверлік үй-жайдың иесі	Нақты орналасқан жері – сервер бөлмесінің мекен-жайы	Қолжетімділікті ұйымдастыруға жауапты тұлғалар (аты-жөні. (бар болса)	Жауапты тұлғалардың телефондары (жұмысшылар, ұялы)
1	2	3	4	5	6

7) сынақ объектісі желісінің құрылымы (кестені толтыру) (қажет болған жағдайда):

№ п/п	Желі сегментінің атауы	Желінің IP мекенжайы / желі маскасы
1	2	3

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

№ п/п	Әкімші рөлі	Әкімші есептік	Интернетке қол	Жабдыққа қашықтан қол	Әкімші жұмыс	Нақты орналасқан

		жазбаларының саны	жетімділіктің болуы	жеткізудің болуы	станциясының IP мекенжайы	жері-жұмыс орнының мекен-жайы
1	2	3	4	5	6	7

9) қолданбалы бағдарламалық қамтылымды пайдаланушылар туралы, оның ішінде мобильді және интернет қосымшаларды қолдана отырып ақпарат (кестені толтыру):

№ п/п	Пайдаланушының рөлі	Пайдаланушының үлгілік әрекеттерінің тізбесі	Пайдаланушылардың сынақ объектісіне қосылу нүктесінің мекенжайы мен порты	Пайдаланушыларды сынақ объектісіне қосу хаттамасы	Сынақ объектісін құруға немесе дамытуға арналған техникалық құжаттамаға сәйкес пайдаланушылар саны	Секундына өңделетін сұраулардың (пакеттердің) ең көп саны	Сұраулар арасындағы максималды күту уақыты
1	2	3	4	5	6	7	8

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

№ п/п	Интеграциялық байланыстың (ақпаратты ндыру объектісінің)атауы	Интеграцияланатын объектінің иесі немесе иесі	Қолданыстағы / жоспарланған	Интеграция Модулінің болуы	Қосылу нүктесінің мекенжайы	Қосылу хаттамасы	Секундына сұраныстардың (пакеттердің) максималды саны	Сұраулар арасындағы максималды күту уақыты
1	2	3	4	5	6	7	8	9

11) қолданбалы бағдарламаның бастапқы кодтары (кестені толтыру) (қажет болған жағдайда):

№ п/п	Дискінің маркалауы (қажет болған жағдайда)	Каталог атауы / дискідегі каталог атауы	Файл атауы	Файл өлшемі, Мбайт	Қолданылатын бағдарламалау тілі (қажет болған жағдайда)	Бағдарламалау тілінің нұсқасы	Қолданылатын жақтау, жақтау нұсқасы	Даму ортасының нұсқасы	Файлды өзгерту күні
1	2	3	4	5	6	7	8	9	10

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

№ п/п	Дискінің маркалауы (		Кітапхана / бағдарламалы			

	қажет болған жағдайда)	Каталог атауы / дискідегі каталог атауы	қ платформа / файл атауы	Өлшемі, Мбайт	Бағдарламалау тілі	Кітапхана нұсқасы
1	2	3	4	5	6	7

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

№ п/п	Құжаттың атауы	Болуы	Беттер саны	Бекітілген күні	Құжат әзірленген Стандарт немесе нормативтік құжат
1	2	3	4	5	6
1	Ақпараттық қауіпсіздік саясаты;				
2	Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидалары;				
3	Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;				
4	Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар;				
5	Есептеу техникасы, телекоммуникациялық жабдық және бағдарламалық қамтамасыз ету құралдарын түгендеу және паспорттау қағидалары;				
	Ақпараттық қауіпсіздіктің				

6	ішкі аудитін жүргізу қағидалары;				
7	Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;				
8	Электрондық ақпараттық ресурстарға қол жеткізу құқықтарының аражігін ажырату қағидалары;				
9	Интернет және электрондық поштаны пайдалану қағидалары;				
10	Аутентификация рәсімін ұйымдастыру қағидалары;				
11	Антивирустық бақылауды ұйымдастыру қағидалары;				
12	Мобильді құрылғылар мен ақпарат тасымалдағыштарды пайдалану қағидалары;				
13	Ақпаратты өңдеу құралдарын және ақпараттық ресурстардың жұмыс істеуінің қауіпсіз ортасын физикалық қорғауды ұйымдастыру қағидалары;				
14	Ақпаратты резервтік көшіру және қалпына келтіру регламенті;				

15	Ақпараттандыру объектісін сүйемелдеу бойынша әкімшінің нұсқауы;				
16	Ақпараттық қауіпсіздік инциденттеріне және штаттан тыс (дағдарыстық) жағдайларға денқою бойынша пайдаланушылардың іс-қимыл тәртібі туралы нұсқаулық.				

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

_____

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

_____

_____

9. Қосымша ақпарат:

_____

_____

_____

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу қағидаларына
3-қосымша
Нысан

Сынақ объектісінің ақпараттық қауіпсіздігі жөніндегі техникалық құжаттаманың тізбесі

1. Ақпараттық қауіпсіздік саясаты;

2. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидалары;

3. Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;

4. Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар;

5. Есептеу техникасы, телекоммуникациялық жабдық және бағдарламалық қамтылым құралдарын түгендеу және паспорттау қағидалары;

6. Ақпараттық қауіпсіздіктің ішкі аудитін жүргізу қағидалары;

7. Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;

8. Электрондық ақпараттық ресурстарға қол жеткізу құқықтарының аражігін ажырату қағидалары;

9. Интернет және электрондық поштаны пайдалану қағидалары;

10. Аутентификация рәсімін ұйымдастыру қағидалары;

11. Антивирустық бақылауды ұйымдастыру қағидлары;

12. Мобильді құрылғылар мен ақпарат тасымалдағыштарды пайдалану қағидалары;

13. Ақпаратты өңдеу құралдарын және ақпараттық ресурстардың жұмыс істеуінің қауіпсіз ортасын физикалық қорғауды ұйымдастыру қағидалары;

14. Ақпаратты резервтік көшіру және қалпына келтіру регламенті;

15. Ақпараттандыру объектісін сүйемелдеу бойынша әкімшінің нұсқауы;

16. Ақпараттық қауіпсіздік инциденттеріне және штаттан тыс (дағдарыстық) жағдайларға ден қою бойынша пайдаланушылардың іс-қимыл тәртібі туралы нұсқаулық.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу қағидаларына
4-қосымша

Ақпараттандыру объектісінің жұмыс істеуі және (немесе) функционалдығы өзгерістерінің тізбесі

№ р/	Жасалған өзгерістер	Бастапқы кодтарды талдау	Ақпараттық қауіпсіздік функциялары	Жүктеме сынағы	Желілік инфрақұрылымды зерттеу	Ақпараттық қауіпсіздікті қамтамасыз ету процестерін зерттеу
1	2	3	4	5	6	7
1.	Даму ортасын өзгерту (бағдарламалау тілі)	+	-	-	-	-

2.	Қолданбалы бағдарламалық қамтылмның функциясын өзгерту	+	+	+	-	-
3.	Серверлік жабдықты ауыстыру	-	+	+	+	+
4.	Желілік жабдықты ауыстыру	-	-	+	+	-
5.	Операциялық жүйе, деректер базасын басқару жүйесі түрінің өзгеруі	-	+	+	-	-
6.	Сынақ объектісінің орналасқан жерін өзгерту	-	+	-	+	+
7.	Сынақ объектісінің ішкі контурдан сыртқы контурға немесе айналымға көшуі	-	+	+	+	+
8.	Жаңа компонентті (серверді)қосу	-	+	-	+	+
9.	Басқалармен жаңа интеграция	+	+	+	+	+
10.	Ақпараттандыру объектісінің сыныбын өзгерту	-	+	-	+	+

Ескерту:

"+" – сынақтар жүргізу қажет;

"-" – сынақ жүргізудің қажеті жоқ.