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

Күшін жойған

Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 14 наурыздағы № 40/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 30 наурызда № 16694 болып тіркелді. Күші жойылды - Қазақстан Республикасының Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НҚ бұйрығымен

Ескерту. Күші жойылды – ҚР Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 03.06.2019 № 111/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 7-1 бабының 5) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Мыналар:

1) осы бұйрыққа 1-қосымшаға сәйкес Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі;

2) осы бұйрыққа 2-қосымшаға сәйкес Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары бекітілсін.

2. "Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің м.а. 2016 жылғы 26 қаңтардағы № 63 бұйрығының (Нормативтік құқықтық актілерді

мемлекеттік тіркеу тізілімінде № 13207 болып тіркелген, "Әділет" ақпараттық-құқықтық жүйесінде 2016 жылғы 1 наурызда жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы 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 күнінен бастап күнтізбелік он күн ішінде оның көшірмелерін қазақ және орыс тілдерінде баспа және электрондық түрде Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу және ресми жариялау үшін "Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

3) осы бұйрық мемлекеттік тіркелген күнінен кейін күнтізбелік он күн ішінде оның көшірмесін мерзімді баспа басылымдарына ресми жариялау үшін жіберуді;

4) осы бұйрықты ресми жариялағаннан кейін Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің ресми интернет-ресурсында орналастыруды;

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

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

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

Қазақстан Республикасының
Қорғаныс және аэроғарыш өнеркәсібі министрі *Б. Атамқұлов*

Қазақстан Республикасы
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2018 жылғы 14 наурыздағы
№ 40/НҚ бұйрығына
1-қосымша

Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық

қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі 1-тарау. Жалпы ережелер

1. Осы Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйені олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтан өткізуді жүргізу әдістемесі (бұдан әрі – Әдістеме) "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы 7-1-бабының 5) тармақшасына сәйкес әзірленді.

2. Осы Әдістемеде мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) осалдық – бағдарламалық қамтылымда жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын заңсыз іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық қамтылымдағы кемшілік;

2) сараптамалық әдіс – сарапшының жеке пікірін немесе сарапшылар тобының ұжымдық пікірін пайдалану негізінде алынған іздестіру әдісі мен оны қолдану нәтижесі;

3) 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 өнім арасындағы өзара іс-қимыл құралы;

4) сенімді бағыт – сынақ объектілерінің қауіпсіздік саясатын қолдауда қажетті сенімді деңгейді қамтамасыз ететін пайдаланушы мен ОҚФ арасындағы өзара іс-қимыл құралы.

3. Сынақтар жүргізу мыналарды қамтиды:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) жүктемелік сынау;

4) желілік инфрақұрылымды тексеріп қарау.

2-тарау. Бастапқы кодтарды талдау

4. Сынақ объектілерінің бастапқы кодтарын талдау бағдарламалық қамтылымның (бұдан әрі – БҚ) кемшіліктерін (бағдарламалық белгілер мен осалдықтарды) айқындау мақсатында жүргізіледі.

5. Бастапқы кодтарды талдау Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидаларына (бұдан әрі-Қағидалар)

сәйкес сынақ объектілерінің бастапқы кодтарын қабылдау-беру актісінде тізімделген БҚ үшін жүргізіледі.

6. Сынақтар жүргізу кезінде сынақ мерзімі аяқталғанға дейін бастапқы кодтарды қайта талдау жүргізу қажеттілігі айқындалған жағдайда, өтініш беруші МТҚ-ға сұрау салумен жүгінеді және Қағидалардың 25-тармағына сәйкес бастапқы кодтарға қайтадан талдау жүргізу туралы қосымша келісім жасалады.

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

8. Бастапқы кодтарды талдау:

1) БҚ кемшіліктерін айқындауды;

2) бастапқы кодты талдау нәтижелерін белгілеуді қамтиды.

9. БҚ кемшіліктерін айқындау мынадай тәртіппен жүзеге асырылады:

1) бастапқы деректерді дайындау жүргізіледі (сервистік бағдарламалық өнімнің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсы мен ақпараттық жүйенің (бұдан әрі-АО) бастапқы кодтарын жүктеу, сканерлеу режимін (қарқынды және/немесе статикалық) таңдау, сканерлеу режимдерінің сипаттамаларын баптау);

2) БҚ кемшіліктерін айқындауға арналған бағдарламалық құрал іске қосылады;

3) жалған іске қосылулардың болуына бағдарламалық есептерді талдау жүргізіледі;

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

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

11. Бастапқы кодтарды талдау нәтижелері осы жұмыс түрлерінің жауапты орындаушысымен бастапқы кодтарды талдау хаттамасында тіркеледі (Еркін нысанда).

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

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

3-тарау. Ақпараттық қауіпсіздік функцияларын сынау

14. Сервистік бағдарламалық өнімнің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсының және ақпараттық жүйенің 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 ақпараттандыру саласындағы стандарттардың талаптарына сәйкестігін бағалау мақсатында жүзеге асырылады.

15. Ақпараттық қауіпсіздік функцияларын сынау мыналарды қамтиды:

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

2) бағалау нәтижелерін тіркеу.

16. Ақпараттық қауіпсіздік функцияларының тізбесі осы Әдістеменің 1-қосымшасында беріледі.

17. Ақпараттық қауіпсіздік функцияларын сынау серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі.

18. Ақпараттық қауіпсіздік функцияларын сынау нәтижелерін осы жұмыс түрлерінің жауапты орындаушысы Ақпараттық қауіпсіздік функцияларын сынау хаттамасында тіркейді (еркін нысанда).

4-тарау. Жүктемелік сынау

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

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

21. Өтініш беруші жүктемелік сынау параметрлерін Қағидалардың 2-қосымшасына сәйкес сынақ объектісінің сипаттамалары туралы Сауалнама-сұраулықта ұсынады.

22. Жүктемелік сынау мынадай тәртіппен жүзеге асырылады:

1) сынауға дайындық жүргізіледі;

2) сынақ жүргізіледі;

3) сынақ нәтижелері тіркеледі.

23. Сынауға дайындық мыналарды қамтиды:

1) сынау сценарийін анықтау;

2) сынаудың уақытша және сандық сипаттамаларын анықтау;

3) сынау жүргізу уақытын тапсырыс берушімен келісу.

24. Сынау жүргізу:

1) мамандандырылған бағдарламалық құралға сынау сценарийі мен конфигурациясын баптауды;

2) мамандандырылған бағдарламалық құралды іске қосуды;

3) сынақ объектісіне жүктеуді тіркеуді;

4) жүктемелік сынаудың есебін қалыптастыру және беруді қамтиды.

25. Жүктемелік тестілеу жүргізу жөніндегі жұмыстар бір сынақ объектісіне пайдаланушыларды қосу нұсқалары мен сынақ объектісінің интеграциялық өзара іс-қимылының нұсқалар саны бойынша жүргізіледі.

26. Жүктемелік сынау нәтижелерін осы жұмыс түрлерінің жауапты орындаушысы Жүктемелік сынау хаттамасында тіркейді (еркін нысанда).

5-тарау. Желілік инфрақұрылымды тексеріп қарау

27. Желілік инфрақұрылымды тексеріп қарау желілік инфрақұрылымның қауіпсіздігін бағалау мақсатында жүргізіледі.

28. Желілік инфрақұрылымды тексеріп қарау мыналарды қамтиды:

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

2) өтініш берушінің желілік инфрақұрлымын тексеріп қарау;

3) алынған нәтижелерді тіркеу.

29. Желілік инфрақұрылымның қорғалу функцияларының тізбесі осы Әдістеменің 2-қосымшасында беріледі.

30. Желілік инфрақұрылымды зерттеп қарау бойынша жұмыстар сынақ объектісінің әрбір кіші желісіне (желі сегментіне) жүргізіледі.

31. Желілік инфрақұрылымды зерттеп қарау нәтижелерін осы жұмыс түрлерінің жауапты орындаушысы Желілік инфрақұрылымды зерттеп қарау хаттамасында тіркейді (еркін нысанда).

Сервистік бағдарламалық
өнімге, "электрондық үкіметтің"
ақпараттық-коммуникациялық
платформасына, мемлекеттік
органның интернет-ресурсына
және ақпараттық жүйеге
олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне
сынақтар жүргізу әдістемесіне
1-қосымша

Ақпараттық қауіпсіздік функцияларының тізбесі

р / с №	Функциялардың атауы	Функциялардың мазмұны
1	2	3
Қауіпсіздік аудиті		
1	Қауіпсіздік аудитінің автоматты әрекет етуі	Тіркеу журналына жазба енгізуді, қауіпсіздікті бұзушылықты айқындау туралы әкімшіге локалдық немесе қашықтықтан сигнал беруді жүзеге асыру
2	Қауіпсіздік аудитінің деректерін өндіру	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.
Байланысты ұйымдастыру		
7	Жіберуден бас тартпаушылық	Жіберуші куәлігі жіберуші мен жіберілген ақпарат арасындағы байланысты (мысалы, цифрлық қолтаңба) дәлелдейтін, ақпаратты жіберу фактісінен бас тартпауы үшін пайдаланушыларға/ жіберушінің ұқсастығын куәландыру субъектілеріне кейбір ақпаратты беру
8	Алудан бас тартпаушылық	Алушының ақпаратты алу фактісінен бас тарту мүмкінсіздігін қамтамасыз ету
Криптографиялық қолдау		
9	Криптографиялық кілттерді басқару	Мыналарды қолдаудың болуы: 1) криптографиялық кілттерді құру; 2) криптографиялық кілттерді бөлу; 3) криптографиялық кілттерге қолжетімділікті басқару; 4) криптографиялық кілттерді жою
		Техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы

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

22	ОҚФ арасында жіберген кезде пайдаланушы деректерінің құпиялылығын қорғау	Пайдаланушының деректерін ОҚФ арасында сыртқы арна немесе АТ басқа сенімді өнімі бойынша жіберген кезде олардың құпиялылығын қамтамасыз ету. Құпиялылық деректерді екі соңғы нүкте арасында жіберген кезде оларға рұқсатсыз қол жеткізуді болдырмау жолымен жүзеге асырылады. Соңғы нүктелер ОҚФ немесе пайдаланушы бола алады.
23	ОҚФ арасында жіберген кезде пайдаланушы деректерінің тұтастығын қорғау	Пайдаланушының деректерін ОҚФ және АТ басқа сенімді өнімі арасында жіберген кезде олардың тұтастығы, сондай-ақ айқындалған қателер кезінде оларды қалпына келтіру мүмкіндігі қамтамасыз етілуі тиіс.
Сәйкестендіру және теңестіру		
24	Теңестіруден бас тарту	Сәтсіз теңестіру талаптарының белгілі санына келгенде әкімшінің субъектіге қол жеткізуге рұқсат бермеу, тіркеу журналына жазба енгізу мен әкімшіге қауіпсіздіктің ықтимал бұзушылық туралы сигнал беру мүмкіндігінің болуы
25	Пайдаланушының атрибуттарын анықтау	Әрбір пайдаланушы үшін, ең болмаса, келесі қауіпсіздік атрибуттарын қолдау қажет: - сәйкестендіргіш; - теңестірілген ақпарат (мысалы, пароль); - қол жеткізу құқығы (рөлі).
26	Құпиялардың ерекшелігі	Егер теңестірілген ақпарат криптографиялық операциялармен қамтамасыз етілсе, сондай-ақ ашық және құпия кілттеріне қолдау көрсетілуі қажет.
27	Пайдаланушыны теңестіру	ОҚФ ұсынатын пайдаланушы теңестіру тетіктерінің болуы
28	Пайдаланушыны сәйкестендіру	1) Қауіпсіздік сервисі осы пайдаланушының атынан орындайтын кез келген іс-қимыл аяқталғанға дейін әрбір пайдаланушы сәтті сәйкестендірілуге және теңестіруді; 2) Басқа пайдаланушыдан көшіріп алынған немесе ұқсастырып жасалған теңестірілген деректерді пайдалануға жол бермеу мүмкіндіктерін; 3) Пайдаланушының ұсынылған кез келген сәйкестендіргішін теңестіру қажет; 4) Әкімші белгілеген уақыт интервалы аяқталғаннан кейін пайдаланушыны қайтадан теңестіруіді; 5) Теңестіруді орындаған кезде қауіпсіздік функциялары пайдаланушыға тек қана жасырын кері байланысқа рұқсат беруді Қамтамасыз ету
29	Пайдаланушы-субъект байланыстырушы	Пайдаланушының тиісті қауіпсіздік атрибуттарын осы пайдаланушы атынан әрекет ететін субъектілермен байланыстыру керек
Қауіпсіздікті басқару		
30	ОҚФ жеке функцияларын басқару	Жұмыс істеу, ажырату, қосу, сәйкестендіру мен теңестіру режимдерін түрлендіру, қолжетімділік, хаттамалау және аудит құқығын басқару режимдерін анықтауға әкімшінің жеке құқығының болуы.
31	Қауіпсіздік атрибуттарын басқару	Қауіпсіздіктің түсіндірілетін мәндерін өзгертуге, сұрастыруға, атрибуттарын өзгертуге, жоюға, құруға әкімшінің жеке құқығының болуы. Бұл ретте, қауіпсіздік атрибуттарына тек қана қауіпсіздік мәндер беруді қамтамасыз ету қажет
		Тіркелетін оқиғалардың түсіндірілетін мәндерін өзгертуге, сұрастыруға, өзгертуге, жоюға, тазалауға, түрлерін анықтауға,

32	ОҚФ деректерін басқару	тіркеу журналдарының өлшемін, субъектілердің қол жеткізу құқықтарын, қол жеткізу субъектілерінің есептік жазбаларының, парольдерінің, криптографиялық кілттерінің жарамдылық мерзімдерін өзгертуге әкімшінің жеке құқығының болуы.
33	Қауіпсіздік атрибуттарын жою	Уақыттың кейбір сәттерінде қауіпсіздік атрибуттарын бұзуды жүзеге асырудың болуы. Пайдаланушылармен байланыстырылған қауіпсіздік атрибуттарын бұзу мүмкіндігі тек қана уәкілетті әкімшілерде болуы тиіс. Қауіпсіздік үшін маңызды өкілеттіктер дереу жойылуы тиіс.
34	Қауіпсіздік атрибутының қолданыс мерзімі	Қауіпсіздік атрибуттарының қолданыс мерзімін белгілеу мүмкіндігін қамтамасыз ету
35	Қауіпсіздікті басқару рөлдері	1) Ең болмаса, мынадай рөлдерді қолдауды қамтамасыз ету: уәкілетті пайдаланушы, қашықтықтан пайдаланушы, әкімші. 2) Қашықтықтан пайдаланушы мен әкімші рөлдерін тек қана сұрау бойынша алуды қамтамасыз ету
ОҚФ қорғау		
36	Кідіру кезіндегі қауіпсіздік	Сервиспен аппараттық кідірістер кезінде (мысалы, электр қуатының іркілісінен орын алған) қауіпсіз жай-күйді сақтау
37	ОҚФ экспортталатын деректерінің қолжетімділігі	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің қолжетімділігін тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер айқындалса, тіркеу журналына жазба енгізуге мүмкіндік беруге тиіс
38	ОҚФ экспортталатын деректерінің құпиялылығы	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің құпиялылығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер айқындалса, тіркеу журналына жазба енгізуге мүмкіндік беру
39	ОҚФ экспортталатын деректерінің тұтастығы	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің тұтастығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер айқындалса, тіркеу журналына жазба енгізуге мүмкіндік беру
40	ОҚФ деректерін СО шегінде жіберу	Деректерді олардың және АТ қашықтықтағы сенімді өнімі арасында жіберген кезде сервис барлық деректердің қолжетімділігін, құпиялылығы мен тұтастығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер айқындалса, тіркеу журналына жазба енгізуге мүмкіндік береді
41	ОҚФ физикалық қорғау	ОҚФ физикалық қорғауды жүзеге асыру
42	Сенімді қалыпқа келтіру	Кідірулер немесе қызмет көрсету тоқтатылғаннан кейін автоматты түрде қалпына келтіру мүмкін болмаса, сервис қауіпсіз жай-күйге қайтаруға мүмкіндік беретін авариялық қолдау режиміне ауысады. Аппараттық кідірістерден кейін автоматты рәсімдерді қолданумен қауіпсіз жай-күйге кері қайту қамтамасыз етіледі
43	Екінші рет пайдалануды айқындау	Сервистің теңестірілген деректердің қайтадан пайдаланылуын айқындауын, қол жеткізуге жол бермеуге, тіркеу журналына жазба енгізуін және әкімшіге қауіпсіздіктің ықтимал бұзылуы туралы сигнал беруін қамтамасыз ету

44	Өтініштер беру кезіндегі делдалдық	Сервистің қауіпсіздік саясатын жүзеге асыратын функциялар сервистің кез келген басқа функциясын орындауға рұқсат етілгенге дейін шақырылып, сәтті орындалуын қамтамасыз ету
45	Доменді бөлу	Қауіпсіздік функциялары оларды сенімсіз субъектілердің араласуы мен бұрмалауынан қорғайтын меншікті орындауға арналған жеке доменді қолдап отыру
46	Жай-күйлерді синхрондау хаттамасы	Серверлерде ұқсас функцияларды орындаған кезде жай-күйлерді синхрондауды қамтамасыз ету
47	Уақыт белгілері	Қауіпсіздік функцияларының пайдалануына сенімді уақыт белгілерін ұсыну
48	ОҚФ арасындағы деректердің келісілушілігі	Тіркелетін ақпаратты, сондай-ақ қолданылатын криптографиялық операциялар параметрлерін келісімді түсіндіруді қамтамасыз ету
49	СО шегінде қайталау кезінде ОҚФ деректерінің келісілушілігі	СО түрлі бөліктерінде қайталаған кезде қауіпсіздік функциялары деректерінің үйлесмілігін қамтамасыз ету. Қайталанатын деректерді қамтитын бөліктер ажыратылғанда, үйлесімділік көрсетілген қауіпсіздік функцияларына кез келген сұрауларды өңдеу алдындағы қосылуды қалпына келтіргеннен кейін қамтамасыз етіледі
50	ОҚФ өзін-өзі тестілеу	Іске қосу кезінде қауіпсіздік функциялары жұмысының дұрыстығын көрсету үшін қылыпты жұмыс процесінде және/немесе әкімшінің сұрауы бойынша мерзімді түрде өзін-өзі тестілеу пакетін орындау. Әкімшінің қауіпсіздік функциялары деректері мен орындалатын кодтың тұтастығын тексеру мүмкіндігі болуы тиіс
Ресурстарды қолдану		
51	Істен шығуға қарсы тұрушылық	Кідірулер кезінде де сынақ объектісінің функционалдық мүмкіндіктерінің қолжетімділігін қамтамасыз ету. Осындай кідірістердің үлгілері: қуат көзін ажырату, аппаратураның жұмыс істемей қалуы, БҚ іркілісі
52	Қызмет көрсетудің басымдылығы	Пайдаланушылардың немесе субъектілердің өздерінің әрекет ету аясында ресурстарды пайдалануын сынақ объектісі шегіндегі басымдылығы жоғары операциялар басымдылығы төмен операциялар жағынан кедергісіз және кідіріссіз орындалатын етіп басқаруды қамтамасыз ету
53	Ресурстарды бөлу	Басқа пайдаланушылардың немесе субъектілердің ресурстарды монополиялауы себепті қызмет көрсетуден рұқсатсыз бас тартуға жол бермеу үшін пайдаланушылардың және субъектілердің ресурстарды пайдалануын басқаруды қамтамасыз ету
СО-ға қолжетімділік		
54	Таңдалатын атрибуттардың аясын шектеу	Қолжетімділік әдісі немесе орны және/немесе уақыты негізінде (мысалы, тәулік уақыты, апта күні) қол жеткізу жүзеге асырылып отырылған порттан пайдаланушы таңдай алатын қауіпсіздік атрибуттарымен қатар пайдаланушы байланыста болуы мүмкін субъектілердің атрибуттарын да шектеу
55	Қатарлас сеанстарды шектеу	Бір пайдаланушыға ұсынылатын қатарлас сеанстардың барынша көп санын шектеу. Бұл шаманың ұйғарынды мәнін әкімші белгілейді.
56	Сеансты бұғаттау	Пайдаланушы әрекетсіздігі ұзақтығының әкімші белгілеген мәні аяқталғаннан кейін жұмыс сеансы мәжбүрлі аяқтау.

57	СО-ға қол жеткізуге рұқсат беру алдында алдын алу	Сәйкестендіруге және теңестіруге дейін әлеуетті пайдаланушылар үшін сынақ объектісінің пайдаланудың сипатына қатысты ескерту хабарламасын көрсету мүмкіндігін қамтамасыз ету
58	СО-ға қолжетімділік тарихы	Сеансты сәтті ашқан кезде пайдаланушы үшін осы пайдаланушы атынан қолжетімділікті алудың сәтсіз әрекеттерінің тарихын алу мүмкіндігін қамтамасыз ету. Бұл тарих қол жеткізу мерзімін, уақытын, құралдарын және СО соңғы рет сәтті қолжетімділік портын, сондай-ақ сәйкестендірілген пайдаланушының соңғы сәтті қол жеткізуінен кейінгі СО сәтсіз қол жеткізу әрекеттерінің санын қамтуы мүмкін.
59	СО-мен сеансты ашу	Субъектіні сәйкестендіргішке, субъектінің пароліне, субъектінің қолжетімділік құқықтарына негізделе отырып, сервистің сеансты ашуға жол бермеуге қабілеттігін қамтамасыз ету.
Зиянды кодтан қорғау функциялары		
60	Вирустарға қарсы қорғау құралдарының болуы	Зиянды кодтан қорғану үшін серверлерден, қажеттілік туындаған жағдайда сынақ объектісінің жұмыс станцияларынан зиянды кодты анықтау және бұғаттау немесе жою, мониторинг құралдарын қолдану
61	Вирустарға қарсы қорғау құралдарына арналған лицензия	Серверлерге және жұмыс станцияларына вирустарға қарсы қорғау құралдарының лицензиялары (сатып алынған, шектелген, еркін таратылатын) болуы тиіс
62	Вирустарға қарсы қорғау сигнатуралары базасын және бағдарламалық қамтылымды жаңарту	Вирустарға қарсы қорғау құралдарының ұдайы жаңартылып, өзекті күйде болуын қамтамасыз ету
63	Вирустарға қарсы қорғау құралдарына қолжетімділікті басқару	Вирустарға қарсы қорғау құралдарын орталықтандырылған басқару мен конфигурациялауды жүзеге асыру
64	Сыртқы электрондық тасығыштардағы ақпаратты зиянды кодтан вирустарға қарсы құралдарымен қорғауды басқару	Сыртқы электрондық тасығыштардағы ақпаратты зиянды кодтан қорғау файлдардың, қажет болса ақпарат тасығыштардың тексерісін және бұғатталуын қамтамасыз ету
БҚ жаңартылуы кезіндегі қауіпсіздік		
65	БҚ ұдайы жаңартылуы	Серверлер мен жұмыс станцияларының жалпыжүйелік және қолданбалы БҚ ұдайы жаңартылуын қамтамасыз ету
66	Интернеттегі жаңарту серверлеріне рұқсатсыз желілік ортадағы БҚ жаңартылуы	Интернеттегі жаңарту серверлеріне рұқсатсыз желілік ортадағы БҚ мамандандырылған арнайы жаңарту серверінен жаңартылуын қамтамасыз ету
Қолданбалы БҚ-ға өзгеріс енгізу кезіндегі қауіпсіздік		
67	Қолданбалы БҚ әзірлеу және тестілеу ортасы	Қолданбалы БҚ әзірлеу және тестілеу үшін өнеркәсіптік пайдалану ортасынан изоляцияланған ортамен қамтамасыз ету
68	Қолданбалы БҚ әзірлеу және тестілеу ортасына қол жеткізудің аражігін ажырату	Бағдарламашылар мен әкімшілер үшін қолданбалы БҚ әзірлеу және тестілеу орталарына қол жеткізуді басқаруын қамтамасыз ету
69	Қолданбалы БҚ өрістету жүйесі	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ өрістету (тарату) жүйесінің болуы

70	Қолданбалы БҚ өрістету жүйесіне қол жеткізудің аражігін ажырату	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ ажырату жүйесіне қол жеткізу құқығын қамтамасыз ету.

Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне 2-қосымша

Желілік инфрақұрылымды қорғау функцияларының тізбесі

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

7	Ақпарат алмасу бойынша жасалған іс-қимылдардан бас тартпаушылық	тексеруді талап ететін қосымшалардың хатамалары;3) жіберуші мен алушы мекенжайларының форматтары синтаксистің дұрыстығына және тиісті директорийлердегі ақпаратпен үйлесімділікке қатысты тексерілетін желіаралық экрандар;4) желіаралық өзара іс-қимыл шеңберінде ақпаратты жеткізу фактілерін растайтын хаттамалар; 5) ақпараттың реттілігін белгілеуге рұқсат беретін тетіктерді қамтитын хаттамалар
8	Үздіксіз жұмыс және қалыпқа келуді қамтамасыз ету	Әрбір іскерлік операцияның үзілуден кейінгі керекті уақыт итервалында қалыпқа келу қабілетін қамтамасыз ету жолымен төтенше жағдайлар кезіндегі үзілген бизнес функцияларының жалғасуын қамтамасыз ететін қорғаныс шараларының болуы
9	Сенімді арна	1) Қашықтықтағы сенімді АТ-өнімімен байланыс үшін қауіпсіздік функциялары басқалардан логикалық ерекшеленетін және оның тараптарының сенімді теңестірудің, сондай-ақ деректерді түрлендіру мен ашудан қорғауды қамтамасыз ететін арна ұсыну;2) сенімді арна арқылы екі тараптарда байланыстарды бастамалауға мүмкіндікті қамтамасыз ету
10	Сенімді бағдар	1) Қашықтықтағы пайдаланушымен байланыс үшін қауіпсіздік функциялары басқалардан логикалық ерекшеленетін және оның тараптарының сенімді теңестіретін, сондай-ақ деректерді түрлендіру мен ашудан қорғауды қамтамасыз ететін арна ұсыну; 2) Пайдаланушының байланыстарды сенімді арна арқылы бастамалауға мүмкіндікті қамтамасыз ету; 3) Қашықтықтағы пайдаланушы мен қашықтықтан басқаруды бастапқы аутентификациялау үшін сенімді бағдарды пайдалану міндетті болып табылады .

Қазақстан Республикасы
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2018 жылғы 14 наурыздағы
№ 40/НҚ бұйрығына
2-қосымша

Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары 1-тарау. Жалпы ережелер

1. Осы Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары (бұдан әрі – Қағидалар) " Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы (бұдан әрі – Заң) 7-1-бабының 5) тармақшасына сәйкес әзірленді және сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге (бұдан әрі – сынақ объектілері)

олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібін айқындайды.

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

3. Осы Қағидаларда мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – АҚ) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің, ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қауіптерден қорғалу жай-күйі;

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

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

4) интернет-ресурс – аппараттық-бағдарламалық кешенде орналастырылатын, мәтіндік, графикалық, аудиовизуалды немесе өзге де түрде бейнеленетін, бірегей желілік мекенжайы және (немесе) домендік атауы бар және (немесе) Интернет желісінде жұмыс істейтін, электрондық ақпараттық ресурс;

5) мемлекеттік техникалық қызмет (бұдан әрі – МТҚ) – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған, шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорны;

6) өтініш беруші – сервистік бағдарламалық өнімнің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, интернет-ресурстың, ақпараттық жүйенің иесі (иеленуші), сондай-ақ сервистік бағдарламалық өнімнің , "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, интернет-ресурстың, ақпараттық жүйенің иесі (иеленуші) өкілеттік берген сервистік бағдарламалық өнімді, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, интернет-ресурсты, ақпараттық жүйені ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізуге өтініш берген жеке немесе заңды тұлға;

7) сервистік бағдарламалық өнім – ақпараттық-коммуникациялық қызметті іске асыруға арналған бағдарламалық өнім;

8) "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы – ақпараттандырудың сервистік моделін іске асыруға арналған технологиялық платформа.

4. Ақпараттық қауіпсіздік талаптарына сәйкестікке міндетті сынақ жүргізілетін сынақ объектілеріне мыналар жатады:

1) сервистік бағдарламалық өнім;

2) "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы;

3) мемлекеттік органның интернет-ресурсы;

4) мемлекеттік органның ақпараттық жүйесі;

5) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйе;

6) мемлекеттік органның ақпараттық жүйесімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйе.

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

6. Объектілерді АҚ талаптарына сәйкестігіне сынау (бұдан әрі – сынақ) сынақ өткізу объектілерінің техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы ақпараттандыру саласындағы стандарттардың талаптарына сәйкестігін бағалау бойынша жұмыстарды қамтиды.

7. Сервистік бағдарламалық өнімді және "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын қоспағанда, сынақ объектілерін сынақтан өткізудің құрамына мынадай жұмыс түрлері кіреді:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) жүктемелік сынау;

4) желілік инфрақұрылымды тексеріп қарау.

8. Сынақ объектісінің бастапқы коды болмаған жағдайда сынақ объектісінің бастапқы кодына талдау жүргізудің міндетті еместігі туралы шешім өтінім берушінің сұрау салуы бойынша ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның (бұдан әрі – уәкілетті орган) шешімімен белгіленеді.

9. Сервистік бағдарламалық өнімді сынауға:

1) бастапқы кодтарын талдау;

2) ақпараттық қауіпсіздік функцияларын сынау кіреді.

10. "Электрондық үкіметтің" ақпараттық-коммуникациялық платформасын сынақтан өткізуге:

1) ақпараттық қауіпсіздік функцияларын сынау;

2) жүктемелік сынау;

3) желілік инфрақұрылымын тексеріп қарау кіреді.

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

12. Сынақтар:

1) бір жұмыс түрі бойынша;

2) бірнеше жұмыс түрлері бойынша;

3) жұмыс түрлерінің толық құрамында жүргізіледі.

13. Сынақ жүргізуге кіретін жұмыстардың әрбір түрін жүргізу бағалары " Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 14-бабының 2-тармақшасына сәйкес белгіленеді.

14. Сынақ жүргізу құнының есебі осы Қағидалардың 12-тармағы бойынша бекітілген тәртіпке сәйкес белгіленген сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық деректерінің, сынақ объектісінің компакт-дискіде кітапханаларымен берілген компоненттері мен модульдерінің бастапқы кодтары мен бағалардың негізінде жүзеге асырылады.

2-тарау. Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібі

15. Сынақтар жүргізу үшін өтініш беруші мынадай құжаттарды ұсына отырып, МТҚ-ға қағаз түрінде осы Қағидаларға 1-қосымшаға сәйкес сынақтар жүргізуге өтінім (бұдан әрі – өтінім) береді:

1) жеке басты куәландыратын құжаттың көшірмесі (жеке тұлғалар үшін);

2) құрылтайшы құжаттардың және заңды тұлғаны мемлекеттік тіркеу туралы анықтаманың немесе куәліктің өтініш берушінің қолымен және мөрімен куәландырылған көшірмелері (заңды тұлғалар үшін);

3) осы Қағидаларға 2-қосымшаға сәйкес нысан бойынша СО сипаттамалары туралы сауалнама-сұраулық;

4) осы Қағидаларға 3-қосымшаға сәйкес сынақтар жүргізуге қажетті техникалық құжаттаманың тізбесі;

5) сәтті компиляция үшін қажетті сынақ объектілері компоненттерінің және қажетті кітапханалары мен файлдары бар модульдерінің бастапқы кодтары,

сынақ объектісінің компакт-дискідегі дерекқорларының схемасы (мәліметтерді сипаттау тілінде);

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

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

17. МТҚ өтінімді алған күнінен бастап бес жұмыс күні ішінде осы Қағидалардың 15-тармағында көрсетілген талаптарға сәйкес өтінімді тексеруді жүзеге асырады.

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

19. Осы Қағидалардың 15-тармағында көрсетілген пакеттер топтамасы толық болған кезде МТҚ бес күн ішінде өтінім берушіге:

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

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

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

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

21. Сынақтар жүргізу үшін өтініш беруші МТҚ-ға мыналарды қамтамасыз етеді:

1) пайдаланушының жұмыс орнына, серверлік және желілік жабдыққа, сынақ объектісінің телекоммуникациялық желісіне және сынақ уақытына өндірістікке ұқсас құрылған ортаға нақты қолжетімділік;

2) сынақ объектісінің функцияларын техникалық құжаттама талаптарына сәйкес көрсету.

22. Өтініш берушінің осы Қағидалардың 21-тармағының талаптарын қамтамасыз ету мүмкінсіздігі жағдайында, шартқа оны орындау мерзімін ұзарту туралы қосымша келісімге қол қоюды ескере отырып, сынақтар Өтініш берушіге оларды қамтамасыз ету үшін қажетті уақытқа тоқтатылады.

23. Сынақтар Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесіне сәйкес жүргізіледі.

24. Сынақтар жүргізу кезінде осы Қағидалардың 15-тармағының

3) тармақшасына сәйкес ұсынылған сынақ объектісінің сипаттамалары туралы сауалнама-сұраулықтың деректері мен сынақ объектісінің нақты жай-күйі арасында айырмашылық айқындалған жағдайда, өтініш беруші МТҚ-ға сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сұраулықты жібереді. Сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сұраулық (қажет болған кезде) сынақ мерзімін ұзартуға және сынақтар жүргізу құнын өзгеруге қосымша келісім жасаудың негіздемесі болып табылады.

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

26. Сынаққа кіретін әрбір жұмыс түрінің нәтижелері және анықталған сәйкессіздіктерді жою жөніндегі ұсынымдар екі данада ресімделетін жеке хаттамаға енгізіліп, біреуі өтініш берушіге беріледі.

27. Хаттамалар жинағының негізінде МТҚ екі данада (МТҚ мен өтініш беруші үшін бір-бірден) осы Қағидаларға 4-қосымшаға сәйкес нысан бойынша Сынақтар актісін ресімдейді.

28. Сынақтарға кіретін барлық жұмыс түрлерін өткізгеннен берілетін оң қорытындысы бар Сынақтар актісі болған кезде және олар бойынша оң нәтиже бар хаттамалар болған кезде сынақтар оң болып танылады.

29. Егер өтініш беруші сынақ кезінде анықталған сәйкессіздіктерді Сынақтар актісін немесе атқарылған жұмыстар бойынша хаттамаларды алған сәттен бастап бір ай ішінде жойса және айқындалған сәйкессіздіктерді түзету нәтижелерімен салыстыру кестесін және осы Қағидаларға 5-қосымшаға сәйкес сынақ объектісінің бастапқы кодтарын қабылдау-тапсыру актісін қоса бере отырып, МТҚ-ға қайтадан сынақтар жүргізуге сұрау салу жіберсе, МТҚ өтініш берушіден

хабарламаны алған күннен бастап он жұмыс күні ішінде аталған жұмыс түрлері бойынша тиісті құжаттарды ресімдей отырып, ақысыз негізде қайтадан сынақтар жүргізеді.

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

30. Сынақ объектісінің бағдарламалық қамтылымына өзгерістер енгізуге байланысты сәйкессіздіктерді жойғаннан кейін қайтадан сынақ жүргізген кезде бастапқы кодты талдау бұрын сәйкессіздіктер айқындалмай орындалғанына қарамасатан, міндетті тәртіппен жүргізіледі. Бұл ретте өтініш беруші қайтадан сынақтар жүргізу туралы сұрау салуға сынақ объектісінің компакт-дискіге сәтті компиляциясы үшін қажетті кітапханалары мен файлдары бар сынақ объектісі компоненттерінің және модульдерінің бастапқы кодтарын қоса береді.

31. Қайтадан сынақтар жүргізген кезде сәйкессіздіктер анықталған жағдайда, МТҚ Сынақтар актісін немесе теріс қорытынды бар хаттаманы ресімдейді, одан кейін сынақтар осы Қағидалардың 2-тарауында белгіленген тәртіппен жүргізіледі
.

32. Ақпараттандыру объектісінің жұмыс істеу жағдайлары мен функционалдығына өзгерістер енгізген кезде ақпараттандыру объектісінің иесі немесе иеленушісі өзгерістерге әкелген жұмыстарды аяқтағаннан кейін МТҚ-ға барлық жүргізілген өзгерістердің сипаттамасын қоса беріп, осы Қағидалардың 2-тарауында белгіленген тәртіппен сынақтар жүргізу қажеттілігі туралы өтінім жібереді.

33. Сынақтар хаттамалары және (немесе) Актісі жоғалған, бүлінген немесе зақымдалған кезде сынақ объектісін иеленуші себептерін көрсете отырып, МТҚ-ға хабарлама жібереді.

34. МТҚ хабарламаны алған күнінен бастап бес жұмыс күні ішінде сынақтар хаттамаларының және (немесе) Актісінің телнұсқасын береді.

35. Оң нәтижесімен Сынақтар актісінің жарамдылық мерзімі сынақ объектісін өнеркәсіптік пайдалану мерзімімен немесе сынақ объектісін жаңғыртуды бастау сәтіне дейін шектеледі.

36. Осы Қағидалардың 27-тармағы бойынша Сынақтар актісіне енгізілмеген сынақтың жеке түрі бойынша хаттаманың жарамдылық мерзімі 1 жылдан аспайды.

Сервистік бағдарламалық
өнімге, "электрондық үкіметтің"
ақпараттық-коммуникациялық
платформасына, мемлекеттік
органның интернет-ресурсына
және ақпараттық жүйеге
олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне

сынақтар жүргізу қағидаларына
1-қосымша
Нысан

_____
__
(сынақтар жүргізу объектісінің атауы)
ақпараттық қауіпсіздік талаптарына сәйкестігіне (бұдан әрі –сынақтар)

Сынақтар жүргізуге өтінім

1._____
_
(өтініш беруші ұйымның атауы, өтініш берушінің Т.А.Ә.)

_____
__
(өтініш берушінің пошталық мекенжайы, e-mail және телефоны, облыс, қала, аудан)
мынадай жұмыстар құрамымен:
1) _____
_
2) _____
_
3) _____
_
4) _____
_
(осы Қағидалардың 7/8/9/10 тармағына сәйкес жұмыс түрлерінің тізбесі (қажетті тармақты көрсету))
_____ сынақтар жүргізуді сұрайды.
(сынақ объектісінің атауы, нұсқасының нөмірі, әзірлеу күні)
2. Сыналатын сынақ объектісінің иесі (иеленушісі) туралы мәліметтер

_____
_
(атауы немесе Т.А.Ә.)

_____
_
(облыс, қала, аудан, пошталық мекенжайы, телефоны)
3. Сыналатын сынақ объектісінің әзірлеушісі туралы мәліметтер

_____
_

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

_____
_

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

4. Сынақ объектісіне қысқаша аңдатпа немесе оның мақсаты

_____
_

(мақсаты, пайдаланылуы, жаңалығы, аналогтары және т.б., қолданылатын әзірлеу құралдары)

5. Қосымша мәліметтер:_____
___

Өтініш беруші ұйымның басшысы/ өтініш берушінің Т.А.Ә. _____
(қолы, күні) (мөрдің орны) болған кезде

Сервистік бағдарламалық
өнімге, "электрондық үкіметтің"
ақпараттық-коммуникациялық
платформасына, мемлекеттік
органның интернет-ресурсына
және ақпараттық жүйеге
олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне
сынақтар жүргізу
қағидаларына 1-қосымша
Нысан

Сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық

1. Сынақ объектісінің атауы: _____
_____

_____
_____

2. Сынақ объектісі әзірлеушісінің деректері:

1) әзірлеушінің атауы: _____
_____;

2) мекенжайы: _____ қ., _____ к.;

3) телефоны: _____, факс: _____;

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

3. Осы сауалнаманы толтыру және мемлекеттік техникалық қызметпенбайланысу үшін

жауапты тұлғаның деректері:

1) тегі, аты, әкесінің аты: _____ _____ _____ _____;

2) лауазымы: _____ _____;

3) жұмыс телефоны:_____, ұялы телефоны: _____;

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

4. Сынақ объектісінің сыныптауы:

1) электрондың ақпараттық ресурстардың сыныбы _____;

2) бағдарламалық қамтамасыз етуің сыныбы _____/_____.

(қолданбалы / жалпыжүйелік)

Ескертпе: Қазақстан Республикасы Инвестициялар және даму министрінің 2016 жылғы 28 қаңтардағы № 135 бұйрығымен (Нормативтік құқықтық актілерді мемлекеттік тіркеу тіркелімінде № 13349 болып тіркелген, "Әділет" ақпараттық-құқықтық жүйесінде 2016 жылғы 17 наурызда жарияланған) бекітілген Ақпараттандыру объектілерін сыныптау қағидаларына 2-қосымшадан алынған ақпараттандыру объектілерін сыныптау схемасы бойынша бектілген схемасын қоса беру.

5. Сынақ объектінің архитектурасы:

1) мыналар:

сынақ объектінің компоненттері мен модульдерінің орналасуы;

компоненттері мен модульдері арасындағы байланыстары;

басқа ақпараттандыру объектілерімен интеграциялық өзара іс-қимылы;

негізгі ақпараттық ағындардың бағыттары;

пайдаланушылар қосылған орындары мен тәсілдері;

деректерді сақтау орындары мен технологиялары;

пайдаланылатын локальдық, ведомстволық (корпоративтік) және жаһандық желілері;

қолданылатын резервтік жабдық көрсетіліп бекітілген сынақ объектінің функционалдық схемасын қоса беру;

2) мыналар:

желінің архитектурасы мен сипаттамалары;

серверлік жабдығы;

желілік және коммуникациялық жабдығы;

адрестеу мен қолданылатын желілік технологиялар;

жұмыс істемей қалуы болмаушылығын қамтамасыз ету және резервтеу жөніндегі шешім(дер) көрсетіліп бекітілген сынақ объектінің деректерді беру желісінің/телекоммуникация желісінің схемасын қоса беру.

6. Сынақ объектісі туралы ақпарат:

1) серверлерлік жабдық туралы ақпарат (кестені толтыру):

р/с №	Сервердің немесе виртуалды ресурстың атауы (сервердің домендік атауы, желілік атауы немесе логикалық атауы)	Мақсаты (орындайтын функционалдық міндеттері)	Саны	Сервердің немесе мәлімденген пайдаланылатын виртуалды ресурстардың сипаттамалары	Серверлерде орнатылған БҚ, ОЖ, қосымшалар мен кітапханалар немесе пайдаланатын виртуалды сервистер (бағдарламалық ортаның құрамы)	IP-мекенжайы
1	2	3	4	5	6	7

2) серверлерлік жабдық орналасқан орны (кестені толтыру):

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

3) серверлерлік жабдықтың сипаттамалары (кестені толтыру):

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

4) резервтік серверлерлік жабдық орналасқан орны (кестені толтыру):

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

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

р/с №	Әкімшінің рөлі	Әкімшілердің есептік жазбаларының саны	Интернетке қолжетімділіктің болуы	Серверге қашықтықтан қолжетімділіктің болуы	Әкімші жұмыс станциясының IP-мекенжайы	Әкімші жұмыс станциясының сипаттамалары
1	2	3	4	5	6	7

6) пайдаланушылар туралы ақпарат (кестені толтыру):

р/с №	Пайдаланушының рөлі	Пайдаланушының типтік іс-қимылдарының тізбесі	Пайдаланушыларды қосу әдісі мен мекенжайы	Пайдаланушыларды авторизациялау әдісі (қажет кезінде)	Пайдаланушылардың ең көп саны	Секунды өңделеті сұраулар (пакеттер) барын көп саны
1	2	3	4		5	6

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

р/с №	Интеграциялық байланыстың (ақпараттандыру объектісінің) атауы	Интеграциялау объектісінің иеленушісі (иесі)	Қолданыстағы / жоспарлы	Интеграциялау модулінің болуы	Пайдаланылатын интеграциялау хаттамалары	Авторизация тәсілі (қажет болған кезде)	Секундына сұраулардың (пакеттердің) барынша көп саны	С ар ку ен уа
1	2	3	4	5	6		7	8

8) серверлік, желілік жабдықтың, жүйе қызметтері мен процессорлардың, бос дискілік кеңістіктің жұмыс қабілеттігі мониторингі үшін пайдаланылатын құралдар туралы ақпарат (кестені толтыру):

р/с №	Мониторингі құралдарының атауы	Мониторингтің мақсаты	Мониторинг жүргізуге жауапты қызметкер	Талдау жүргізудің мерзімділігі
1	2	3	4	5

9) оқиғалар журналдарын талдау туралы ақпарат (кестені толтыру):

р/с №	Сервистердің, оқиғалар журналының атауы	Талдауға арналған құралдар	Талдау жүргізудің мерзімділігі	Оқиғалар журналдарын сақтау мерзімі	Оқиғалар журналдарын сақтау орындары
1	2	3	4	5	6

10) сыналатын үлгіні әзірлеудің тілдік ортасы (кестені толтыру):

р/с №	Модульдің атауы	Қолданылатын бағдарламалау тілі	Пайдаланылатын кітапханалар, компоненттер мен файлдар	Бастапқы кодтың көлемі, Мбайт
1	2	3	4	5

11) корпоративтік желінің құрылымы (кестені толтыру):

р/с №	Желі сегментінің атауы	Желіаралық қосылулардың саны	Желіні қорғаудың аппараттық-бағдарламалық құралдары	Желілерді қорғаудың басқа құралдары
1	2	3	4	5

7. Сыналатын объектіні құжаттау (кестені толтыру):

р/с №	Құжаттың атауы	Бар болуы	Парақтар саны	Бекітілген күні	Оған сайкес құжат әзірленген стандарт
1	2	3	4	5	6
1.	Техникалық тапсырма немесе сервистік бағдарламалық өнімді жобалауға тапсырма				
2.	Пайдаланушының басшылығы				
3.	Бағдарламаның мәтіні				
4.	Бағдарламаның сипаттамасы				

8. Стандарттарда көзделген басқа құжаттаманың болуы (кестені толтыру):

р/с №	Құжаттың атауы	Белгіленуі	Парақтар саны	Бекітілген күні	Оған сайкес құжат әзірленген стандарт
1	2	3	4	5	6

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

_____

10. Сыналатын объектіге лицензияның болуы (авторлық құқықтың болуы, бастапқы

кодты ұсынуға әзірлеуші ұйыммен келісімнің болуы)

_____

_____

11. Қосымша ақпарат: _____

_____

Ескертпе: аббервиатуралардың толық жазылуы:

БҚ – бағдарламалық қамтылым

ОЖ – операциялық қамтылым

Сервистік бағдарламалық
өнімге, "электрондық үкіметтің"
ақпараттық-коммуникациялық
платформасына, мемлекеттік
органның интернет-ресурсына
және ақпараттық жүйеге
олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне
сынақтар жүргізу қағидаларына
3-қосымша

Сынақтар жүргізуге қажетті техникалық құжаттаманың тізбесі

1) Сервистік бағдарламалық өнімді жобалауға техникалық тапсырма немесе тапсырма (сервистік бағдарламалық өнімге).

2) Пайдаланушының басшылығы.

3) Бағдарламаның мәтіні (ЭҮ АКП және бастапқы кодтары жоқ сынақ объектілерін қоспағанда).

4) Бағдарламаның сипаттамасы (ЭҮ АКП және бастапқы кодтары жоқ сынақ объектілерін қоспағанда).

Сервистік бағдарламалық
өнімге, "электрондық үкіметтің"
ақпараттық-коммуникациялық
платформасына, мемлекеттік
органның интернет-ресурсына
және ақпараттық жүйеге
олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне
сынақтар жүргізу қағидаларына
4-қосымша

"Бекітемін"
Мемлекеттік техникалық
қызмет директоры
_____ _____
(Т.А.Ә.) (қолы)
20_ жылғы "_____" _____

Нысан

_____
_____

(өтініш беруші ұйымның атауы/ өтініш берушінің Т.А.Ә.)

_____
_____

(сынақ объектісінің (бұдан әрі – СО) атауы)

20 __ жылғы "____" _____ № ____

сынақтар актісі

1. Мемлекеттік техникалық қызмет 20 __ жылғы "____" _____ ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтар жүргізу туралы (бұдан әрі – сынақтар) Өтінімге және 20 __ жылғы "____" _____ №___ шартқа сәйкес мынадай жұмыстар құрамында

_____

(СО атауы)

сынақтар жүргізді:

1) бастапқы кодтарды талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) жүктемелік сынақтан өткізу;

4) желілік инфрақұрылымды тексеріп қарау.

2. Сынақ барысында мыналар анықталды:

1) бастапқы кодты талдау бойынша:

СО бастапқы кодтарын талдау қатесіз аяқталды (БҚ кемшіліктері болмаған жағдайда);

СО бастапқы кодтарын талдау қателермен аяқталды (БҚ кемшіліктері орын алған жағдайда);

СО бастапқы кодтарын талдау (осы Қағидалардың 8,9 және 10 тармағы бойынша негіздемесін көрсету) негізінде жүргізілген жоқ;

Хаттама (СО бастапқы кодтарын талдау хаттамасының нөмірі мен күні);

2) ақпараттық қауіпсіздік функцияларын сынау бойынша:

СО ақпараттық қауіпсіздік функцияларын іске асыру АҚ талаптарына сәйкес (сәйкессіздіктер болмаған жағдайда);

СО ақпараттық қауіпсіздік функцияларын іске асыру АҚ талаптарына сәйкес емес (сәйкессіздіктер орын алған жағдайда);

Хаттама (СО ақпараттық қауіпсіздік функцияларын сынау хаттамасының нөмірі мен күні);

3) жүктемелік сынау бойынша:

жүктемелік сынау сәтті өтті (СО белгіленген параметрлер кезінде үздіксіз және тұрақты (кідірістерсіз) жұмыс істеуі);

жүктемелік сынау сәтсіз өтті (СО белгіленген параметрлер кезінде үздіксіз және тұрақты жұмыс істеуінің бұзылуы (кідірістердің орын алуы);

Хаттама (жүктемелік сынау хаттамасының нөмірі мен күні);

4) желілік инфрақұрылымды тексеріп қарау бойынша:

желілік инфрақұрылымның қауіпсіздігі АҚ талаптарына сәйкес (СО қауіпсіз жұмыс істеуіне ықпал ететін сәйкессіздіктер мен осалдықтар болмаған жағдайда);

желілік инфрақұрылымның қауіпсіздігі АҚ талаптарына сәйкес емес (СО қауіпсіз жұмыс істеуіне ықпал ететін сәйкессіздіктер мен осалдықтар орын алған жағдайда);

Хаттама (СО желілік инфрақұрылымын тексеріп қарау хаттамасының нөмірі мен күні).

Қорытынды

Жүргізілген сынақтар негізінде _____

(сынақ объектісінің атауы)

ақпараттық қауіпсіздік талаптарына сәйкес / сәйкес емес.

КЕЛІСІЛДІ: ДАЙЫНДАЛДЫ:

_____ _____

(лауазымы) (лауазымы)

_____ _____ _____ _____

(қолы) (Т.А.Ә.) болған кезде (қолы) (Т.А.Ә.) болған кезде

20__ жылғы "__" _____ 20__ жылғы "__" _____

Сервистік бағдарламалық
өнімге, "электрондық үкіметтің"
ақпараттық-коммуникациялық
платформасына, мемлекеттік
органның интернет-ресурсына
және ақпараттық жүйеге
олардың ақпараттық қауіпсіздік
талаптарына сәйкестігіне
сынақтар жүргізу қағидаларына
5-қосымша
Нысан

Сынақ объектісінің бастапқы кодтарын қабылдау – беру актісі

_____

__

(Сынақ объектісінің (бұдан әрі-СО) атауы)

_____

__

(өтініш беруші ұйымның атауы / өтініш берушінің Т.А.Ә.)

20__ жылғы "_____" _____

Берілетін БҚ нұсқасы _____.

Дискілер саны _____.

р/с №	Дискінің таңбалауы	Дискідегі каталогтың атауы	Файлдың атауы	Файлдың көлемі, Мбайт	Пайдаланылатын бағдарламалау тілі (қажет болған кезде)	Файл түрлендірілген күні
1	2	3	4	5	6	7

Табыстады: Қабылдады:

_____ _____

(лауазымы) (лауазымы)

_____ _____

(қолы) (Т.А.Ә.) болған кезде (қолы) (Т.А.Ә.) болған кезде

20____жылғы "_____" _____ 20____ жылғы "____" _____

Үлгілерді тіркеу журналында 20__ жылығы "_" _____ №_ болып тіркелді.

Тіркеген _____

(қолы) (Т.А.Ә.) болған кезде