

**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**

### *Күшін жойған*

Қазақстан Республикасы Инвестициялар және даму министрінің м.а. 2016 жылғы 26 қаңтардағы № 63 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2016 жылы 24 ақпанда № 13207 болып тіркелді. Күші жойылды - Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 14 наурыздағы № 40/НҚ бұйрығымен

**Ескерту. Күші жойылды – ҚР Қорғаныс және аэроғарыш өнеркәсібі министрінің 14.03.2018 № 40/НҚ (алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.**

"Ақпараттандыру туралы" 2015 жылғы 24 қарашдағы Қазақстан Республикасының Заңы 7-бабының 16) 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. "Бағдарламалық өнімдерді, бағдарламалық кодтарды сынақтан өткізу, оларды және нормативтік құжаттаманы тіркеу, беру, сақтау, депозитке берудің толықтығын қамтамасыз ету және оларды тіркеу, депозитарийге беру мен сақтау туралы мәліметтерді ұсыну ережесін бекіту туралы" Қазақстан Республикасы Ақпараттандыру және байланыс агенттігі Төрағасының 2009 жылғы 1 желтоқсандағы № 480 бұйрығының (Қазақстан Республикасының нормативтік құқықтық актілерін мемлекеттік тіркеу тізілімінде № 5981 болып тіркелген және

Қазақстан Республикасы орталық атқарушы және өзге де орталық мемлекеттік органдарының актілер жинағында 2010 жылғы 20 сәуірде жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы Инвестициялар және даму министрлігінің Байланыс, ақпараттандыру және ақпарат комитеті (Т.Б. Қазанғап):

1) осы бұйрықты Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін оның көшірмелерін баспа және электрондық түрде күнтізбелік он күн ішінде мерзімді баспа басылымдарында және "Әділет" ақпараттық-құқықтық жүйесінде ресми жариялауға, сондай-ақ тіркелген бұйрықты алған күннен бастап күнтізбелік он күн ішінде Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу үшін Республикалық құқықтық ақпарат орталығына жіберуді;

3) осы бұйрықты Қазақстан Республикасы Инвестициялар және даму министрлігінің интернет-ресурсында және мемлекеттік органдардың интранет-порталында орналастыруды;

4) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Инвестициялар және даму министрлігінің Заң департаментіне осы бұйрықтың 3-тармағының 1), 2) және 3) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Инвестициялар және даму вице-министріне жүктелсін.

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

Қазақстан Республикасының  
Инвестициялар және даму  
министрінің міндетін атқарушы

Ж. Қасымбек

Қазақстан Республикасы  
Инвестициялар және даму  
министрінің міндетін атқарушының  
2016 жылғы 26 қаңтардағы  
№ 63 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. 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 25 қарашадағы Қазақстан Республикасы заңының 7-бабы 16) тармақшасына сәйкес әзірленді.

2. Осы Әдістемеді мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) ақпараттық қауіпсіздік функцияларын сынау – сервистік бағдарламалық өнімді, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын және ақпараттық жүйені ақпараттық қауіпсіздік талаптарына сәйкестігіне бағалау;

2) жүктемелік сынау – жоспарлы, көтеріңкі және өте жоғары жүктемелер кезінде сынау объектілерінің қол жетімділігін, тұтастығын және құпиялықты сақтауды бағалау;

3) мемлекеттік техникалық қызмет – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған, шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорн;

4) осалдық – бағдарламалық қамтамасыз етуде жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын заңсыз іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық қамтамасыз етудегі кемшілік;

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

6) 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;

7) сенімді бағдар – функцияларды өзара іс-қимыл қауіпсіздігін қамтамасыз ету арқылы орындауға арналған пайдаланушылардың сынақ объектілерінің қауіпсіздік саясатын қолдауда сенімдікті қамтамасыз ететін пайдаланушылар мен ОҚФ арасындағы өзара іс-қимыл құралы;

8) сервистік бағдарламалық өнімді, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын және ақпараттық жүйені қауіпсіздік талаптарына сәйкестігіне

сынау (бұдан әрі – сынау) – ақпараттық қауіпсіздік талаптарына сынақ объектілерін бағалау жөніндегі техникалық іс-шаралар;

9) сынау объектілері (бұдан әрі – СО) - сервистік бағдарламалық өнім, " электрондық үкіметтің" ақпараттық-коммуникациялық платформасы, мемлекеттік органның интернет-ресурсы, ақпараттық жүйе.

3. Сынақтан өткізуді жүргізу мыналарды қамтиды:

- 1) бастапқы кодтарды талдау;
- 2) ақпараттық қауіпсіздік функцияларын сынау;
- 3) жүктемелік сынау;
- 4) телекоммуникация желілерін және серверлік жабдықты тексеріп қарау.

## **2. Бастапқы кодтарды талдау**

4. СО бастапқы кодтарын талдау бағдарламалық қамтамасыз етудің (бұдан әрі – БҚ) кемшіліктерін (бағдарламалық белгілер мен осалдықтарды) айқындау мақсатында жүргізіледі.

5. БҚ кемшіліктерін айқындау тапсырыс беруші ұсынған бастапқы кодтардың негізінде бағдарламалық құралдың талдауға арналған бастапқы кодын пайдалана отырып жүргізіледі.

6. Бастапқы кодтарды талдау:

- 1) БҚ кемшіліктерін айқындауды;
- 2) бастапқы кодты талдау нәтижелерін белгілеуді қамтиды.

7. БҚ кемшіліктерін айқындау мынадай тәртіппен жүзеге асырылады:

1) бастапқы деректерді дайындау жүргізіледі (СО бастапқы кодтарын жүктеу, сканерлеу режимін (қарқынды және/немесе статикалық) таңдау, сканерлеу режимдерінің сипаттамаларын күйге келтіру);

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.

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

9. Бастапқы кодтарды талдау нәтижелері Бастапқы кодтарды талдау хаттамасында белгіленеді.

10. СО бастапқы кодтарын талдауды жүргізу аяқталғаннан кейін оның нәтижелері оң болған кезде СО бастапқы кодтары таңбаланады және мөр

басылған түрінде мемлекеттік техникалық қызметтің мұрағатына жауапты сақтауға тапсырылады.

### **3. Ақпараттық қауіпсіздік функцияларын сынау**

11. Ақпараттық қауіпсіздік функцияларын сынау олардың стандарттардың талаптарына сәйкестігін бағалау мақсатында жүзеге асырылады.

12. Ақпараттық қауіпсіздік функцияларын сынау мыналарды қамтиды:

1) қауіпсіздік функцияларының өтініш берушімен келісілген стандарттың талаптарына сәйкестігін бағалау;

2) бағалау нәтижелерін белгілеу.

13. Қауіпсіздік функцияларының мазмұны осы Әдістемеге 1-қосымшаға сәйкес ақпараттық қауіпсіздік функцияларының тізбесінде келтірілген.

14. Ақпараттық қауіпсіздік функцияларын сынау нәтижелері Ақпараттық қауіпсіздік функцияларын сынау хаттамасында тіркеледі.

### **4. Жүктемелік сынау**

16. Жүктемелік сынау нақты пайдаланушылардың жұмысына сәйкес келетін жүктемемен СО қол жетімділігін, тұтастығын және құпиялығын сақтауды бағалау мақсатында жүргізіледі.

17. Жүктемелік сынау СО пайдаланушыларының жұмысын тапсырыс беруші ұсынған мындай орталардың бірінде қамтитын автоматты сценарийлер негізінде арнайы бағдарламалық құралды (бұдан әрі - БҚ) пайдалана отырып жүргізіледі:

СО штаттық пайдалану ортасына ұқсас тестілік орта;

дербес деректер жоқ СО штаттық пайдалану ортасы;

дербес деректер жалған деректерге ауыстырылған СО штаттық пайдалану ортасы.

18. Өтініш беруші жүктемелік сынау параметрлерін СО сипаттамалары туралы сауалнама-сұраулықта ұсынады және мыналарды қамтиды:

1) пайдаланушы рөлдерінің тізбесі;

2) пайдаланушының типтік іс-қимыл тізбесі;

3) пайдаланушылардың ең көп саны;

4) секундына өңделетін сұраулардың ең көп саны және сұраулар арасындағы күту уақыты.

19. Жүктемелік сынау мынадай тәртіппен жүзеге асырылады:

1) сынауға дайындық жүргізіледі;

2) сынақ жүргізіледі;

3) сынақ нәтижелері тіркеледі.

20. Сынауға дайындық мыналарды қамтиды:

1) виртуалды пайдаланушылардың операцияларын, сондай-ақ оқиғалар мен олардың іс-қимылының ерекшеліктерін сипаттай отырып сынақ сценарийінің сараптамалық әдісін әзірлеу;

2) әрбір операцияның уақытша сипаттамалары мен сынаққа қатысатын виртуалды пайдаланушылардың санын анықтау;

3) виртуалды пайдаланушылардың скриптерін қалыптастыру және: әрбір виртуалды пайдаланушы;

бірнеше виртуалды пайдаланушы бір мезгілде орындайтын міндеттерді анықтау;

4) сынақтар жүргізу уақытын тапсырыс берушімен келісу.

21. Сынақ жүргізу:

1) СО-ға жиынтық жүктемені бөлуді, оның процесінде бірнеше виртуалды пайдаланушыға белгілі міндеттерді бір мезгілде орындау жөніндегі нұсқаулықтар беріледі;

2) конфигурацияны күйге келтіру мен сынақ сценарийін мамандандырылған БҚ жазуды;

3) мамандандырылған бағдарламалық құралды іске қосуды;

4) виртуалды пайдаланушының әрбір скриптінде белгіленген барлық транзакциялардың жазбалары (өңделген СО-ға сұрау салулар) қамтитын бағдарламалық есепті қалыптастыруды және беруді қамтиды.

22. Жүктемелік тестілеуді жүргізу жұмыстары СО пайдалану нұсқаларының саны бойынша бір СО үшін жүргізіледі.

23. Жүктемелік сынақ нәтижелері Жүктемелік сынақ хаттамасында тіркеледі.

## **5. Телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау**

24. Телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау телекоммуникациялар желісі мен серверлік жабдықтың қауіпсіздігін бағалау, сондай-ақ оның компоненттері (сервер, жұмыс станциялары, желілік жабдық) пайдаланатын БҚ осалдықтарын айқындау мақсатында жүргізіледі.

25. Телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау мыналарды қамтиды:

1) телекоммуникациялар желісін және серверлік жабдықты қорғау функцияларының ҚР СТ ИСО/МЭК 13335-5-2008 "Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық және коммуникациялық технологияларды қорғауды басқару. 5-бөлік. Желіні қорғауды басқару жөніндегі нұсқау" талаптарына сәйкестігін бағалау;

2) БҚ осалдықтарын айқындау;

3) алынған нәтижелерді белгілеу.

26. Телекоммуникациялар желісін және серверлік жабдықты қорғау функцияларының мазмұны осы Әдістемеге 2-қосымшада сәйкес телекоммуникациялар желісін және серверлік жабдықты қорғау функцияларының тізбесінде келтірілген.

27. БҚ осалдықтарын айқындау өтініш беруші ұсынған СО компоненттеріне қол жеткізуге арналған есептік жазбалардың негізінде бағдарламалық-аппараттық кешенді (бұдан әрі – БАК) пайдалана отырып жүргізіледі.

28. БҚ осалдықтарын айқындау мыналарды қамтиды:

1) БАК күйге келтіру (локальдық және қашықтықтан тексерулерді жүргізуге арналған есептік жазбаларды жазу, аспаптық тексеріп қарау режимін таңдау);

2) БАК іске қосу;

3) айқындалған осалдықтардың сипаттамасын, саны мен деңгейін көрсете отырып олардың тізбесін қамтитын бағдарламалық есепті қалыптастыру және беру.

29. Телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау бойынша жұмыстар, сондай-ақ СО компоненттерін аспаптық тексеріп қарау әр ішкі желі (желі сегменті) үшін бөлек жүргізіледі.

30. Телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау нәтижелері Телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау хаттамасында тіркеледі.

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 (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
1	Қауіпсіздік аудитінің автоматты әрекет етуі	Тіркеу журналына жазба енгізуді жүзеге асыру, қауіпсіздікті бұзушылықты айқындау туралы әкімшіге локальдық немесе қашықтықтан сигнал беру

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 уақыты, оқиға түрі, субъектіні сәйкестендіргіш және оқиға нәтижесі (сәттілігі немесе сәтсіздігі) көрсетілуі тиіс
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	Тіркеу ақпараты рұқсатсыз түрлендіруден сенімді қорғалған болуы тиіс.
Байланысты ұйымдастыру (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
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
9	Киптографиялық қолдау (тексеру СО ақпаратты криптографиялық қорғау құралдары бөлінісінде жүргізіледі)	
10	Киптографиялық кілттерді басқару	Мыналарды қолдаудың болуы: 1) киптографиялық кілттерді құру; 2) киптографиялық кілттерді бөлу; 3) киптографиялық кілттерге қолжетімділікті басқару; 4) киптографиялық кілттерді жою
11	Криптографиялық операциялар	Сенімді арна арқылы жіберілетін барлық ақпарат үшін стандарттардың талаптарына сәйкес тұтастығын шифрлаудың және бақылаудың болуы
Пайдаланушының деректерін қорғау (тексеру серверлер (виртуалды ресурстар) бөлінісінде жүргізіледі)		
12	Қолжетімділікті басқару саясаты	Қауіпсіздік сервисімен тікелей немесе жанама операцияларды орындайтын пайдаланушылар үшін қолжетімділікті бөлуді жүзеге асыру
13	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.



14	Деректерді тексеру	Ақпараттың мазмұны айлакерлік жолымен ұқсастырылмағанын немесе түрлендірілмегенін кейін тексеру үшін пайдаланылуы мүмкін өзіндік деректер жинағының дұрыстығы кепілдігін қолдау.
15	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
16	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
17	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)
18	Деректерді ОҚФ әрекетінен тыс жерден импорттау	Пайдаланушының деректерін олардың талап етілетін қауіпсіздік және қорғау атрибуттары болатындай етіп СО жіберуге арналған тетіктердің болуы
19	СО шегінде жіберу	Пайдаланушының деректерін ішкі арна бойынша СО түрлі бөліктері арасында жіберген кезде қорғаудың болуы
20	Қалған ақпаратты қорғау	Қалған ақпаратты толық қорғауды қамтамасыз ету, яғни ресурс босаған кезде алдыңғы жай-күйінің қолжетімсіздігін қамтамасыз ету
21	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.
22	Сақталатын деректердің тұтастығы	Пайдаланушының деректерін ОҚФ шегінде сақтаған кезде олардың қорғалуын қамтамасыз ету
23	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.
24	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 (тексеру сәйкестендіру мен аутентификацияны орындайтын серверлердің және виртуалды есурстар бөлінісінде жүргізіледі)		

25	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
26	Пайдаланушының атрибуттарын анықтау	Әрбір пайдаланушы үшін, ең болмаса, келесі қауіпсіздік атрибуттарын қолдау қажет: - сәйкестендіргіш; - теңестірілген ақпарат (мысалы, пароль); - қол жеткізу құқығы (рөлі).
27	Құпиялардың ерекшелігі	Егер теңестірілген ақпарат криптографиялық операциялармен қамтамасыз етілсе, сондай-ақ ашық және құпия кілттеріне қолдау көрсетілуі қажет.
28	Пайдаланушыны теңестіру	ОҚФ ұсынатын пайдаланушы теңестіру тетіктерінің болуы
29	Пайдаланушыны сәйкестендіру	1) Қауіпсіздік сервисі осы пайдаланушының атынан орындайтын кез келген іс-қимыл аяқталғанға дейін әрбір пайдаланушы сәтті сәйкестендірілуіне және теңестіруге тиіс; 2) Басқа пайдаланушыдан көшіріп алынған немесе ұқсастырып жасалған теңестірілген деректерді пайдалануға жол бермеу мүмкіндіктері болуы тиіс; 3) Пайдаланушының ұсынылған кез келген сәйкестендіргішін теңестіру қажет; 4) Әкімші белгілеген уақыт интервалы аяқталғаннан кейін пайдаланушыны қайтадан теңестіруі тиіс; 5) Теңестіруді орындаған кезде қауіпсіздік функциялары пайдаланушыға тек қана жасырын кері байланысқа рұқсат беруі тиіс
30	Пайдаланушы-субъект байланыстырушы	Пайдаланушының тиісті қауіпсіздік атрибуттарын осы пайдаланушы атынан әрекет ететін субъектілермен байланыстыру керек
Қауіпсіздікті басқару (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
31	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.
32	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
33	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.
34	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.
35	Қауіпсіздік атрибутының қолданыс мерзімі	Қауіпсіздік атрибуттарының қолданыс мерзімін белгілеу мүмкіндігін қамтамасыз ету
36		1) Ең болмаса, мынадай рөлдерді қолдауды қамтамасыз ету: уәкілетті пайдаланушы, қашықтықтан пайдаланушы, әкімші.

	Қауіпсіздікті басқару рөлдері	2) Қашықтықтан пайдаланушы мен әкімші рөлдерін тек қана сұрау бойынша алуды қамтамасыз ету
Биресмилікті қамтамасыз ету (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
37	Құпиялық	Пайдаланушының ресурсты немесе СО қызметін өзінің сәйкестендіргішін ашпай пайдалану мүмкіндігін қамтамасыз ету
38	Бүркеншек атау	Пайдаланушының ресурсты немесе қызметті өзінің сәйкестендіргішін ашпай, сонымен қатар осы пайдалану үшін жауапты болып пайдалану мүмкіндігін қамтамасыз ету
39	Бейәлуметтік мүмкінсіздігі	Пайдаланушының ресурстарды немесе қызметтерді, олардың пайдаланылғанын байланыстыруға ешкімге мүмкіндік бермей, бірнеше рет пайдалану мүмкіндігін қамтамасыз ету
40	Жасырындық	1) Ресурсты немесе қызметті пайдалану туралы ақпаратты кімге болсын, әсіресе үшінші тарапқа ұсынбай, пайдаланушының ресурстарды немесе қызметті пайдалану мүмкіндігін қамтамасыз ету; 2) Әкімшінің қауіпсіздік сервисінің ресурстарын пайдалануды бақылау мүмкіндігі болуы тиіс
ОҚФ қорғау (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
41	Кідіру кезіндегі қауіпсіздік	Сервис аппараттық кідірістер кезінде (мысалы, электр қуатының іркілісінен орын алған) қауіпсіз жай-күйді сақтауға тиіс
42	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
43	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 беруге тиіс
44	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 беруге тиіс
45	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 беруге тиіс
46	ОҚФ физикалық қорғау	ОҚФ физикалық қорғау жүзеге асырылуы тиіс
47	Сенімді қалпына келтіру	Кідірулер немесе қызмет көрсету тоқтатылғаннан кейін автоматты түрде қалпына келтіру мүмкін болмаса, сервис қауіпсіз жай-күйге қайтаруға мүмкіндік беретін авариялық қолдау режиміне ауысу керек. Аппараттық кідірістерден кейін автоматты рәсімдерді қолданумен қауіпсіз жай-күйге кері қайту қамтамасыз етілуі тиіс
48	Екінші рет пайдалануды айқындау	Сервис теңестірілген деректердің қайтадан пайдаланылуын айқындауға, қолжеткізуге жол бермеуге, тіркеу журналына жазба енгізуге және әкімшіге қауіпсіздіктің ықтимал бұзылуы туралы сигнал беруге тиіс

49	Өтініштер беру кезіндегі делдалдық	Сервистің қауіпсіздік саясатын жүзеге асыратын функциялар сервистің кез келген басқа функциясын орындауға рұқсат етілгенге дейін шақырылып, сәтті орындалуы керек
50	Доменді бөлу	Қауіпсіздік функциялары оларды сенімсіз субъектілердің араласуы мен бұрмалауынан қорғайтын меншікті орындауға арналған жеке доменді қолдауға тиіс
51	Жай-күйді синхрондау хаттамасы	Жай-күйлерді синхрондау қамтамасыз етілуі тиіс
52	Уақыт белгілері	Қауіпсіздік функцияларының пайдалануына сенімді уақыт белгілері ұсынылуы тиіс
53	ОҚФ арасындағы деректердің келісілушілігі	Тіркелетін ақпаратты, сондай-ақ қолданылатын криптографиялық операциялар параметрлерін келісімді түсіндіру қамтамасыз етілуі тиіс
54	СО шегінде қайталау кезінде ОҚФ деректерінің келісілушілігі	СО түрлі бөліктерінде қайталаған кезде қауіпсіздік функциялары деректерінің келісу қамтамасыз етілуі тиіс. Қайталанатын деректерді қамтитын бөліктер ажыратылғанда, үйлесімділік көрсетілген қауіпсіздік функцияларына кез келген сұрауларды өңдеу алдындағы қосылуды қалпына келтіргеннен кейін қамтамасыз етілуі тиіс
55	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 пакеті орындалу керек. Әкімшінің қауіпсіздік функциялары деректері мен орындалатын кодтың тұтастығын тексеру мүмкіндігі болуы тиіс
Ресурстарды пайдалану (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
56	Істеп шығуға қарсы тұрушылық	Кідірулер кезінде де СО функционалдық мүмкіндіктеріне қолжетімділік қамтамасыз етілуі тиіс. Осындай кідірістердің үлгілері: қуат көзін ажырату, аппаратураның жұмыс істемей қалуы, бағдарламалық қамтамасыз етудің іркілісі
57	Қызмет көрсетудің басымдылығы	Пайдаланушылардың немесе субъектілердің өздерінің әрекет ету аясында ресурстарды пайдалануын СО шегіндегі басымдылығы жоғары операциялар басымдылығы төмен операциялар жағынан кедергісіз және кідіріссіз орындалатын етіп басқаруды қамтамасыз ету
58	Ресурстарды бөлу	Басқа пайдаланушылардың немесе субъектілердің ресурстарды монополиялауы себепті қызмет көрсетуден рұқсатсыз бас тартуға жол бермеу үшін пайдаланушылардың және субъектілердің ресурстарды пайдалануын басқару қамтамасыз етілуге тиіс
СО-ға қолжетімділік (тексеру жалпы СО үшін жүргізіледі)		
59	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 атрибуттары да шектелуге тиіс
60	Қатарлас сеанстарды шектеу	Бір пайдаланушыға ұсынылатын қатарлас сеанстардың барынша көп саны шектелуі тиіс. Бұл шаманың әкімші белгілейтін ұйғарынды мәні болуы тиіс.
61	Сеансты бұғаттау	Пайдаланушы әрекетсіздігі ұзақтығының әкімші белгілеген мәні аяқталғаннан кейін жұмыс сеансы мәжбүрлі аяқталуы тиіс.

62	СО-ға қол жеткізуге рұқсат беру алдында алдын алу	Сәйкестендіруге және теңестіруге дейін әлеуетті пайдаланушылар үшін СО пайдаланудың сипатына қатысты ескерту хабарламасын көрсету мүмкіндігі қамтамасыз етілуі тиіс
63	СО-ға қолжетімділік тарихы	Сеансты сәтті ашқан кезде пайдаланушы үшін осы пайдаланушы атынан қолжетімділікті алудың сәтсіз әрекеттерінің тарихын алу мүмкіндігі қамтамасыз етілуі тиіс. 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.
64	СО-мен сеансты ашу	Субъектіні сәйкестендіргішке, субъектінің пароліне, субъектінің қолжетімділік құқықтарына негізделе отырып, сервис сеансты ашуға жол бермеуге қабілетті болуы тиіс.
Сенімді бағдарды/арнаны қамтамасыз ету (тексеру серверлер мен виртуалды ресурстар бөлінісінде жүргізіледі)		
65	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 ұсынуға тиіс; 2) Екі тараптың байланыстарды сенімді арна арқылы бастамалауға мүмкіндігі болуы тиіс.
66	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 ұсынуға тиіс; 2) Пайдаланушының байланыстарды сенімді арна арқылы бастамалауға мүмкіндігі болуы тиіс; 3) Қашықтықтағы пайдаланушы мен қашықтықтан басқаруды бастапқы аутентификациялау үшін сенімді бағдарды пайдалану міндетті болып табылады.

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

## Телекоммуникациялар желісін және серверлік жабдықты 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	Зиянды кодтан сақтап қалу	Зиянды кодтан сақтап қалу үшін мыналарды қамтитын қорғау шараларының болуы: 1) нұсқаларын, кем дегенде, апта сайын жаңарту арқылы сканерлеуші бағдарламалық қамтамасыз етуді қазіргі уақыт деңгейінде қолдау; 2) зиянды кодтың жүйеге басып кіру мүмкіндігін азайтуға бағытталған рәсімдер мен практикалық іс-қимылдарды жалпы реттейтін басшылық нұсқаулардың бар болуы.
5	Желіні қорғауды басқару	Қашықтықтан диагностикалаудың барлық порттарына ( виртуалды немесе физикалық) рұқсатсыз қол жеткізуден сақтандыруды қамтамасыз ететін қорғау шараларының болуы.
6	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
7	Желілер арқылы деректермен алмасудың құпиялылығы	Құпиялылықты сақтау маңызды болған жағдайларда желілік қосылулар арқылы өтетін ақпаратты шифрлау үшін криптографиялық қорғау шаралары қарастырылуы тиіс
8	Желілер бойынша жіберілетін деректердің тұтастығы	Деректердің тұтастығын сақтау маңызды болған жағдайларда желілік қосылулар арқылы өтетін ақпаратты қорғау үшін цифрлық қолтаңба мен хабарламаның тұтастығын қорғау шаралары қарастырылуы тиіс
9	Ақпарат алмасу бойынша жасалған іс-қимылдардан бас тартпаушылық	Ақпаратты желі бойынша жіберудің растауын ұсыну талап етілетін жағдайда, мынадай қорғау шараларын пайдалану керек: 1) құжатты жіберу фактісін растайтын байланыс хаттамалары; 2) бастапқы адресі немесе сәйкестендіргішті ұсынуды және аталған ақпараттың бар болуын 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
10	Үздіксіз жұмысты және қалпына келтіруді қамтамасыз ету	Табиғи апат жағдайында әрбір іскери операцияның үзілістен кейін үйлесімді уақыт аралығында қалпына келу қабілетін қамтамасыз ету арқылы бизнес функцияларын жалғастыруды қамтамасыз ететін қорғау шараларының болуы.

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

**1. 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-бабының 16) 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 сынақта жүргізу тәртібін айқынтайды.

2. Осы Қағидаларда мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – АҚ) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің, ақпараттық-коммуникациялық инфроқұрылымның 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) 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;

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

5) 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;

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

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

3. Сынақ объектілері:

1) сервистік бағдарламалық өнім;

2) "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы;

3) мемлекеттік органның интернет-ресурсы;

4) ақпараттық жүйе болып табылады.

4. Объектілерді АҚ талаптарына сәйкестігіне сынау (бұдан әрі – сынақ) сынақ өткізу объектілерінің Қазақстан Республикасының аумағында қабылданған, стандарттармен белгіленген АҚ талаптарына сәйкестігін бағалау бойынша жұмыстарды қамтиды.

5. Сынаққа:

1) бастапқы кодтарын талдау;

2) ақпараттық қауіпсіздік функцияларын сынау;

3) жүктемелік сынау;

4) телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау кіреді.

6. Мемлекеттік органның немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған ақпараттық жүйенің мемлекеттік емес ақпараттық жүйемен интеграциялануы жағдайында, оның бастапқы кодын талдауға қосымша интеграция компоненттерінің (интеграциялау модулі, ішкі интеграциялау жүйесі, интеграциялық шина) бастапқы кодтарын талдау жүргізіледі.

7. Сынақтар:



- 1) бір жұмыс түрі бойынша;
- 2) бірнеше жұмыс түрлері бойынша;
- 3) жұмыс түрлерінің толық құрамында жүргізіледі мүмкін.

8. Сынаққа өткізулерге кіретін жұмыстың әрбір түрін жүргізудің құнын монополияға қарсы органмен келісім бойынша ақпараттандыру саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) белгілейді.

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

9. Сынвақтан өткізулер жүргізу үшін Өтініш беруші мынадай құжаттарды ұсына отырып, МТҚ-ға осы Қағидаларға 1-қосымшаға сәйкес нысан бойынша сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның, интернет-ресурсына олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне 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 мөрмен куәландырылған көшірмелері (заңды тұлғалар үшін);
- 3) осы Қағидаларға 2-қосымшаға сәйкес нысан бойынша СО сипаттамалары туралы сауалнама-сұраулық;
- 4) осы Қағидаларға 3-қосымшаға сәйкес Техникалық құжаттама тізбесіне сәйкес техникалық құжаттама;
- 5) сынақ объектілері компоненттерінің және компакт-дискіге сәтті орнату үшін қажетті кітапханалары мен файлдары бар модульдерінің бастапқы кодтары.

10. МТҚ өтінімді алған сәттен бастап бес жұмыс күні ішінде осы Қағидалардың 9-тармағында көрсетілген талаптарға сәйкес өтінімді тексеруді жүзеге асырады.

11. Осы Қағидалардың 9-тармағында көрсетілген талаптарға сәйкес өтінім және қоса берілген құжаттар сәйкес келмеген жағдайда, өтінім қайтару себептерін көрсете отырып, кері қайтарылады.

12. Осы Қағидалардың 9-тармағында көрсетілген талаптарға сәйкес өтінім және қоса берілген құжаттар сәйкес болған кезде МТҚ бес жұмыс күні ішінде өтініш берушіге 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.

13. Сынақтар мерзімі өтініш берушімен келісіледі және СО сынақтары өткізу бойынша жұмысатрдың көлемі мен сыныптау сипаттамаларына байланысты болады.

14. Сынақтар жүргізу үшін өтініш беруші МТҚ-ны мыналармен 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.

15. Сынақтар Заңның 14-бабының 7) тармақшасына сәйкес 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.

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

17. Егер өтініш беруші сынақ кезінде анықталған сәйкессіздіктерді сынақтар актісін немесе атқарылған жұмыстар бойынша хаттамаларды алған сәттен бастап бір ай ішінде жойса, 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.

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

19. Хаттамалар жинағының негізінде МТҚ екі данада (МТҚ мен өтініш беруші үшін бір-бірден) атқарылған жұмыстар туралы мәліметтерді, олардың нәтижелерін анықталған сәйкессіздіктерді жою жөнінде қорытынды мен ұсынымдарды (болған кезде) қамтитын осы Қағидаларға 4-қосымшаға сәйкес нысан бойынша Сынақтар актісін ресімдейді.

20. Сынақтар кіретін жұмыстардың барлық түрлерін өткізгеннен кейін берілетін оң қорытындысы бар сынақтар актісі болған кезде және олар бойынша оң нәтиже бар хаттамалар болған кезде оң болып танылады.

21. СО-ға өзгерістер енгізген кезде сынақтар жүргізуді оның иесі (иеленушісі) қамтамасыз еткен кезде МТҚ осы Қағидалармен белгіленген жалпы тәртіппен қайтадан сынақтар жүргізеді.

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

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

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 өткізу 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) \_\_\_\_\_

(ҚР Инвестициялар және даму министрінің 20\_\_\_\_ жылғы "\_\_\_\_" \_\_\_\_\_  
№\_\_\_\_\_ бұйрығымен бекітілген Сервистік бағдарламалық  
өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық  
платформасына, мемлекеттік органның интернет-ресурсына және  
ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына  
сәйкестігіне сынақтар жүргізу әдістемесіне сәйкес жұмыстар түрінің  
тізбесі)

\_\_\_\_\_ сынақтар жүргізуді сұрайды.  
(сынақ объектісінің атауы, нұсқасының нөмірі, әзірлеу күні)

2. Сынақ объектінің әзірлеушісі туралы мәліметтер

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

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

3. Сынақтар объектісіне қысқаша аңдатпа \_\_\_\_\_

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

4. Қосымша мәліметтер:

Өтініш беруші ұйымның басшысы/ өтініш берушінің Т.А.Ә. \_\_\_\_\_  
(қолы, мерзімі)

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

Нысан

## Сынақ объектісінің сипаттамалары туралы сауалнама-сұраулық

1. Сынақ объектісінің атауы: \_\_\_\_\_  
\_\_\_\_\_

2. Сынақтан өткізу объектісін әзірлеушінің деректері:

1) әзірлеушінің атауы: \_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_;

2) мекенжайы: \_\_\_\_\_ к., \_\_\_\_\_ к.;

3) телефоны: \_\_\_\_\_, факс: \_\_\_\_\_;

4) электрондық пошта мекенжайы: E-mail: \_\_\_\_\_@\_\_\_\_\_.

3. Осы сауалнаманы толтыру және мемлекеттік техникалық қызметпен байланысу үшін жауапты тұлғаның деректері:

1) тегі, аты, әкесінің аты: \_\_\_\_\_;

2) лауазымы: \_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_;

3) телефоны: \_\_\_\_\_, факс: \_\_\_\_\_;

4) электрондық пошта мекенжайы: E-mail: \_\_\_\_\_@\_\_\_\_\_.

4. Сынақ объектінің сәулеті (резервілеудің барлық байланыстары мен күйге келтірулер көрсетілген СО сәулетінің схемасын қоса беру):

1) серверлер туралы ақпарат (кестені толтыру):

Сервердің немесе виртуалды ресурстың атауы	Мақсаты	Саны	Сервердің немесе пайдаланылатын мәлімделген виртуалды ресурстың сипаттамалары	Серверлерде орнатылған БҚ, ОЖ, қосымшалар мен кітапханалар немесе пайдаланатын виртуалды ресурстар	IP-мекенжайы
1	2	3	4	5	6

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

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

3) пайдаланушылар туралы ақпарат (кестені толтыру):

--	--	--	--	--	--

Пайдаланушының рөлі	Пайдаланушының типтік іс-қимылдарының тізбесі	Пайдаланушының жұмыс станциясының техникалық сипаттамаларына қойылатын ең төменгі талаптар	Пайдаланушылардың барынша көп саны	Секундына өңделетін сұраулардың барынша көп саны/сұраулар арасындағы күту уақыты	Жұмыс станциясында орнатылған БҚ, ОЖ, қосымшалар мен кітапханалар
1	2	3	4	5	6

4) резервтік жабдықтың сипаттамалары (кестені толтыру):

Сервердің немесе виртуалды ресурстың атауы	Мақсаты	Саны	Сервердің немесе пайдаланатын мәлімделген виртуалды ресурстың сипаттамалары	Серверлерде орнатылған БҚ, ОЖ, қосымшалар мен кітапханалар немесе пайдаланылатын виртуалды ресурстар	IP-мекенжайы	Резервілеу әдісі
1	2	3	4	5	6	7

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

Мониторингі құралдарының атауы	Мониторингтің мақсаты	Мониторинг жүргізуге жауапты қызметкер	Мониторингі нәтижелері бойынша талдау жүргізу туралы ақпарат
1	2	3	4

6) журналдық оқиғаларды талдау туралы ақпарат (кестені толтыру):

Сервистердің атауы	Талдауға арналған құралдар	Талдау жиілігі
1	2	3

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

Жүйе модульдерінің атауы	Бағдарламалау тілдері	Пайдаланылатын кітапханалар	Бастапқы код және пайдаланылатын кітапханалар, файлдар көлемі, Мбайт
1	2	3	

--	--	--	--

8) корпоративтік желінің құрылымы (кестені толтыру):

Ішкі желінің (желі сегментінің) атауы	Желіаралық қосылулардың саны	Желіні қорғаудың аппараттық-бағдарламалық құралдарының саны	Желіні қорғаудың басқа құралдары	Мониторингі құралдары

5. Қосымша мәліметтер:

1) пайдаланылатын деректерді тарату желісінің/телекоммуникациялар желісінің конфигурациясы және сипаттамасы (схемасын қоса беру):

—;

2) резервтік деректерді тарату желісінің/ телекоммуникациялар желісінің конфигурациясы және сипаттамасы (схемасын қоса беру):

—

6. Сыналанын объекті құжаттамалау (кестені толтыру)

р/с №	Құжаттың атауы	Бар болуы	Парақтар саны	Бекітілген күні	Оған сәйкес құжат әзірленген стандарт
1	2	3	4	5	6
1	Техникалық тапсырма немесе сервистік бағдарламалық өнімді жобалауға тапсырма				
2	Пайдаланушының нұсқауы				
3	Бағдарламаның мәтіні				
4	Бағдарламаның сипаттамасы				
5	Функционалдық схемасы немесе "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы ресурстарының сипаттамасы				

7. Сыналанын объектінің бастапқы кодтарының әзірлеу ортасын кеңейтумен компиляцияға дайындығы (нұсқасы, атауы, дискіде ұсыну):

—

8. Стандарттарда көзделген басқа құжаттаманың болуы:

р/с №	Құжаттың атауы	Белгіленуі	Парақтар саны	Бекітілген күні	Оған сәйкес 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: аббревиатуралардың толық жазылуы:

БҚ – бағдарламалық қамтамасыз ету

ОЖ – операциялық қамтамасыз ету

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

## Техникалық құжаттама тізбесі

1) Сервистік бағдарламалық өнімді жобалауға техникалық тапсырма немесе тапсырма.

2) Пайдаланушының нұсқауы.

3) Бағдарламаның мәтіні.

4) Бағдарламаның сипаттамасы.

5) Функционалдық схемасы немесе "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы ресурстарының сипаттамасы.



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

\_\_\_\_\_  
(сынақ объектісінің (бұдан әрі – СО) атауы)

**20 \_\_ жылғы "\_\_\_\_\_" № \_\_\_\_\_**  
**сынақтар актісі**

20 \_\_ жылғы "\_\_\_\_\_" \_\_\_\_\_ дейін жарамды

1. Мемлекеттік техникалық қызмет 20 \_\_ жылғы "\_\_\_\_\_"

\_\_\_\_\_  
ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтар жүргізу туралы ( бұдан әрі – сынақтар) өтінімге сәйкес мынадай жұмыстар құрамында

\_\_\_\_\_  
(СО атауы)

сынақтар жүргізді:

- 1) бастапқы кодтарды талдау;
- 2) ақпараттық қауіпсіздік функцияларын сынау;
- 3) жүктемелік сынақтан өткізу;
- 4) телекоммуникациялар желісін және серверлік жабдықты 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 және оларды жойғаннан кейін СО бастапқы кодтарын қайтадан талдау қажет (БҚ кемшіліктері орын алған жағдайда);

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);

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);

4) телекоммуникациялар желісін және серверлік жабдықты тексеріп қарау бойынша:

телекоммуникациялар желісінің және серверлік жабдықтың қауіпсіздігі АҚ талаптарына сәйкес (СО қауіпсіз жұмыс істеуіне ықпал ететін сәйкессіздіктер мен осалдықтар болмаған жағдайда);

телекоммуникациялар желісінің және серверлік жабдықтың қауіпсіздігі АҚ талаптарына сәйкес емес (СО қауіпсіз жұмыс істеуіне ықпал ететін сәйкессіздіктер мен осалдықтар орын алған жағдайда).

Қорытынды

Жүргізілген сынақтар негізінде \_\_\_\_\_

(сынақ объектісінің атауы)

ақпараттық қауіпсіздік талаптарына сәйкес / сәйкес емес.

Анықталған сәйкессіздіктерді жою және қайтадан сынақтар жүргізу ұсынылады (Теріс қорытындысы бар акт берілген жағдайда).

КЕЛІСІЛДІ: ӘЗІРЛЕНДІ:

\_\_\_\_\_  
(лауазымы) (лауазымы)

\_\_\_\_\_  
(қолы) (Т.А.Ә.) (қолы) (Т.А.Ә.)

болған кезде болған кезде

20\_\_ жылғы " \_\_ " \_\_\_\_\_ 20\_\_ жылғы " \_\_ " \_\_\_\_\_