

Ақпараттық қауіпсіздікті қамтамасыз ету бөлігінде ақпараттандыру саласындағы тәуекел дәрежесін бағалау өлшемшарттарын және тексеру парақтарын бекіту туралы

Қазақстан Республикасы Премьер-Министрінің орынбасары – Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 29 қаңтардағы № 13/НҚ және Қазақстан Республикасы Ұлттық экономика министрінің 2019 жылғы 29 қаңтардағы № 12 бірлескен бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2019 жылғы 6 ақпанда № 18269 болып тіркелді.

Қазақстан Республикасының 2015 жылғы 29 қазандағы Кәсіпкерлік кодексі 141-бабының 3-тармағына және 143-бабының 1-тармағына сәйкес БҰЙЫРАМЫЗ:

1. Мыналар:

1) алып тасталды - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 20.01.2023 № 21/НҚ және ҚР Ұлттық экономика министрінің 23.01.2023 № 8 (01.01.2023 бастап қолданысқа енгізіледі) бірлескен бұйрығымен.

2) алып тасталды - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 20.01.2023 № 21/НҚ және ҚР Ұлттық экономика министрінің 23.01.2023 № 8 (01.01.2023 бастап қолданысқа енгізіледі) бірлескен бұйрығымен.

3) Киберқауіпсіздік бөлігінде цифрландыру саласындағы тәуекел дәрежесін бағалау өлшемшарттары, осы бірлескен бұйрыққа 3-қосымшаға сәйкес;

4) мемлекеттік заңды тұлғаларға, квазимемлекеттік сектор субъектілеріне, мемлекеттік органдардың цифрлық жүйелерімен интеграцияланатын немесе мемлекеттік цифрлық ресурстарды қалыптастыруға арналған мемлекеттік емес цифрлық жүйелердің иелері мен иеленушілеріне, киберқауіпсіздікті қамтамасыз ету орталықтарына, сондай-ақ аса маңызды цифрлық объектілерінің иелері мен иеленушілеріне қатысты киберқауіпсіздік бөлігінде ақпараттандыру саласындағы тексеру парағы, осы бірлескен бұйрыққа 4-қосымшаға сәйкес.

Ескерту. 1-тармаққа өзгеріс енгізілді - ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 10.09.2026 № 550/НҚ және ҚР Премьер-Министрінің орынбасары – Ұлттық экономика министрінің 11.09.2026 № 145 (алғаш ресми жарияланған күнінен кейін он күнтізбелік күн өткен соң қолданысқа енгізіледі) бірлескен бұйрығымен.

2. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бірлескен бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бірлескен бұйрық мемлекеттік тіркелген күннен бастап күнтізбелік он күн ішінде оны қазақ және орыс тілдерінде ресми жариялау және Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкінде орналастыру үшін "Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

3) осы бірлескен бұйрықтың көшірмесін Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің интернет-ресурсында орналастыруды қамтамасыз етсін.

3. Осы бірлескен бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

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

Қазақстан Республикасы
Премьер-Министрінің орынбасары –
Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрі

А. Жұмағалиев

Қазақстан Республикасының
Ұлттық экономика министрі

Т. Сүлейменов

"КЕЛІСІЛДІ"

Қазақстан Республикасы
Бас прокуратурасының
Құқықтық статистика және
арнайы есепке алу жөніндегі
комитеті

Қазақстан Республикасы
Премьер-Министрінің
орынбасары –
Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2019 жылғы 29 қаңтардағы
№ 13/НҚ және
Қазақстан Республикасы
Ұлттық экономика
министрінің
2019 жылғы 29 қаңтардағы
№ 12 бірлескен бұйрығына
1-қосымша

Ақпараттың қауіпсіздікті қамтамасыз ету бөлігінде ақпараттандыру саласындағы тәуекел дәрежесін бағалау өлшемшарттары

Ескерту. 1-қосымша алып тасталды - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 20.01.2023 № 21/НҚ және ҚР Ұлттық экономика

министрінің 23.01.2023 № 8 (01.01.2023 бастап қолданысқа енгізіледі) бірлескен бұйрығымен.

Қазақстан Республикасы
Премьер-Министрінің
орынбасары –
Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2019 жылғы 29 қаңтардағы
№ 13/НҚ және
Қазақстан Республикасы
Ұлттық экономика министрінің
2019 жылғы 29 қаңтардағы
№ 12 бірлескен бұйрығына
2-қосымша

Мемлекеттік және жергілікті атқарушы органдарға қатысты ақпараттық қауіпсіздікті қамтамасыз ету бөлігінде ақпараттандыру саласындағы тексеру

Ескерту. 2-қосымша алып тасталды - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 20.01.2023 № 21/НҚ және ҚР Ұлттық экономика министрінің 23.01.2023 № 8 (01.01.2023 бастап қолданысқа енгізіледі) бірлескен бұйрығымен.

Қазақстан Республикасы
Премьер-Министрінің
орынбасары –
Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2019 жылғы 29 қаңтардағы
№ 13/НҚ және
Қазақстан Республикасы
Ұлттық экономика министрінің
2019 жылғы 29 қаңтардағы
№ 12 бірлескен бұйрығына
3-қосымша

Киберқауіпсіздік бөлігінде цифрландыру саласындағы тәуекел дәрежесін бағалау өлшемшарттары

Ескерту. 3-қосымша жаңа редакцияда - ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 10.09.2026 № 550/НҚ және ҚР Премьер-Министрінің орынбасары – Ұлттық экономика министрінің 11.09.2026 № 145 (алғаш ресми жарияланған күнінен кейін он күнтізбелік күн өткен соң қолданысқа енгізіледі) бірлескен бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы Киберқауіпсіздік бөлігінде ету цифрландыру саласындағы тәуекел дәрежесін бағалау өлшемшарттары (бұдан әрі – Өлшемшарттар) Қазақстан Республикасының

Кәсіпкерлік кодексінің 143-бабы, 141-бабының 5 және 6 тармақтарына (бұдан әрі – Кодекс), "Реттеуші мемлекеттік органдардың тәуекелдерді бағалау және басқару жүйесін қалыптастыру қағидаларын бекіту және "Мемлекеттік органдардың тәуекелдерді бағалау жүйесін қалыптастыру қағидаларын және тексеру парақтарының нысанын бекіту туралы" Қазақстан Республикасы Ұлттық экономика министрінің міндетін атқарушының 2018 жылғы 31 шілдедегі № 3 бұйрығына өзгерістер енгізу туралы" Қазақстан Республикасы Ұлттық экономика министрінің міндетін атқарушының 2022 жылғы 22 маусымдағы № 48 бұйрығына өзгеріс енгізу туралы бұйрығына (Нормативтік құқықтық актілердің мемлекеттік тіркеу тізілімінде № 31148 болып тіркелген) және Қазақстан Республикасы Ұлттық экономика министрінің міндетін атқарушысының 2018 жылғы 31 шілдедегі № 3 бұйрығымен (Нормативтік құқықтық актілердің мемлекеттік тіркеу тізілімінде № 17371 болып тіркелген) бекітілген тексеру парағының нысанына сәйкес әзірленген.

2. Осы Өлшемшарттарда мынадай ұғымдар пайдаланылады:

1) елеулі бұзушылық – цифрлық ресурстарда, цифрлық жүйелерде және басқа да цифрландыру объектілері үшін қызмет көрсетуді елеулі шектеуге, жағдайдың елеулі нашарлауына немесе елеулі теріс салдарға әкеп соқтырған немесе әкеп соғуы мүмкін киберқауіпсіздік бөлігінде цифрландыру саласындағы, қызмет көрсету саласында екі немесе одан да көп расталған шағымдардың немесе өтініштердің болуы, цифрландыру саласында киберқауіпсіздік бөлігінде Қазақстан Республикасы нормативтік құқықтық актілерінің талаптарын сақтамау;

2) елеусіз бұзушылық – электрондық цифрлық ресурстарға, цифрлық жүйелерге және басқа да цифрландыру объектілеріне әсер етпейтін елеусіз оқиғаларға әкеп соққан немесе әкелуі мүмкін киберқауіпсіздік бөлігінде цифрландыру саласындағы Қазақстан Республикасы нормативтік құқықтық актілерінің талаптарын сақтамау, киберқауіпсіздік бөлігінде цифрландыру саласында бір расталған шағымның немесе өтініштің болуы;

3) Киберқауіпсіздік бөлігінде цифрландыру саласындағы бақылау субъектілері (бұдан әрі – бақылау субъектілері – квазимемлекеттік сектор субъектілері, мемлекеттік органдардың цифрлық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық цифрлық ресурстарды қалыптастыруға арналған мемлекеттік емес цифрлық жүйелердің иелері мен иеленушілері, киберқауіпсіздікті қамтамасыз ету орталықтары, сондай-ақ аса маңызды цифрлық объектілерінің иелері мен иеленушілері;

4) өрескел бұзушылық – цифрлық ресурстар, цифрлық жүйелер және басқа да цифрлық объектілер үшін елеулі теріс салдарға әкеп соққан немесе қызмет көрсету мүмкін болмауына әкеп соғуы мүмкін киберқауіпсіздік бөлігінде цифрландыру саласындағы Қазақстан Республикасы нормативтік құқықтық актілерінің талаптарын сақтамау, уәкілетті органның нұсқамаларын орындамау;

5) тәуекел – бақылау субъектісінің қызметі нәтижесінде жеке және заңды тұлғалардың заңды мүдделеріне, мемлекеттің мүліктік мүдделеріне салдарларының ауырлық дәрежесін ескере отырып зиян келтіру ықтималдығы;

6) тексеру парағы – бақылау субъектілерінің (объектілерінің) қызметіне қойылатын, олардың сақталмауы жеке және заңды тұлғалардың, мемлекеттің заңды мүдделеріне қатер төндіруге алып келетін талаптар тізбесі;

7) тәуекелдерді бағалау және басқару жүйесі – тиісті қызмет салаларында тәуекелдің жол берілетін деңгейін қамтамасыз ете отырып, кәсіпкерлік еркіндігін шектеудің ең төменгі ықтимал дәрежесі мақсатында бақылау субъектісіне бару арқылы профилактикалық бақылауды кейіннен жүзеге асыру үшін бақылау субъектілерін тәуекел дәрежелері бойынша бөлу арқылы қолайсыз факторлардың туындау ықтималдығын азайтуға бағытталған, сондай-ақ нақты бақылау субъектісі (объектісі) үшін тәуекел деңгейін өзгертуге бағытталған басқарушылық шешімдерді қабылдау және (немесе) осындай бақылау субъектісін, бақылау субъектісіне бару арқылы профилактикалық бақылаудан босату процесі;

8) тәуекел дәрежесін бағалаудың объективті өлшемшарттары (бұдан әрі – объективті өлшемшарттар) – белгілі бір қызмет саласында тәуекел дәрежесіне байланысты, субъектіден (объектіден) тікелей байланыссыз, бақылау субъектісін (объектісін) іріктеу үшін пайдаланылатын тәуекел дәрежесін бағалау өлшемшарттары;

9) тәуекел дәрежесін бағалаудың субъективті өлшемшарттары (бұдан әрі – субъективті өлшемшарттар) – нақты бақылау субъектісінің (объектісінің) қызмет нәтижелеріне байланысты бақылау субъектілерін (объектілерін) іріктеу үшін пайдаланылатын тәуекел дәрежесін бағалау өлшемшарттары.

3. Бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау үшін тәуекел дәрежесін бағалау өлшемшарттары объективті және субъективті өлшемшарттар арқылы қалыптастырылады.

2-тарау. Объективті өлшемшарттар

4. Бірінші кезеңде объективті өлшемшарттар бойынша бақылау субъектілері тәуекелдің үш дәрежесі бойынша бөлінеді: осы өлшемшарттарға 1-қосымшаға сәйкес жоғары, орташа, төмен.

5. Тәуекел дәрежесі жоғары субъектілерге аса маңызды цифрлық объектілерінің иелері мен иеленушілері жатады.

Тәуекел дәрежесі орташа субъектілерге квазимемлекеттік сектор субъектілері және мемлекеттік органдардың цифрлық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық цифрлық ресурстарды қалыптастыруға арналған мемлекеттік емес цифрлық жүйелердің иелері мен иеленушілері жатады.

Тәуекел дәрежесі төмен субъектілерге киберқауіпсіздікті қамтамасыз ету орталықтары жатады.

3-тарау. Субъективті өлшемшарттар

6. Субъективті өлшемшарттар тексеру парақтарында санамаланған талаптардың (бұдан әрі – талаптар) негізінде әзірленеді, онда талаптардың сақталмауы бағалау өлшемшарттарына сәйкес бұзушылықтың белгілі бір дәрежесіне сәйкес келеді. Тексеру парақтарының әрбір талаптарына қатысты бұзушылық дәрежесі – осы өлшемшарттардың қосымшасына сәйкес айқындалады.

7. Субъективті өлшемшарттарды анықтау мынадай:

- 1) деректер базасын қалыптастыру және ақпарат жинау;
- 2) ақпаратты талдау және тәуекелдерді бағалау кезеңдерін пайдалана отырып жүзеге асырылады.

8. Деректер базасын қалыптастыру және ақпарат жинау Қазақстан Республикасының киберқауіпсіздік бөлігінде цифрландыру саласындағы заңнамасын бұзатын бақылау субъектілерін (объектілерін) анықтау үшін қажет.

9. Тәуекелдер дәрежесін субъективті өлшемшарттар бойынша бағалау үшін ақпараттың мынадай дереккөздері пайдаланылады:

- 1) бақылау субъектілеріне (объектілеріне) бару арқылы алдыңғы профилактикалық бақылау және тексеру нәтижелері.

10. Әрбір ақпараттық дереккөз бойынша тәуекел дәрежесі мынадай жолмен айқындалады.

Өрескел дәреженің бір орындалмаған талабы 100 көрсеткішіне теңестіріледі және бұл ішінара тәртіппен тексеру жүргізу үшін негіздеме болып табылады.

Егер талаптардың өрескел дәрежесінің бұзушылығы анықталмаған жағдайда, онда тәуекел дәрежесінің көрсеткішін анықтау үшін елеулі және болмашы дәрежелері талаптарының бұзушылығы бойынша жиынтық көрсеткіш есептеледі.

Елеулі дәреженің бұзушылық көрсеткішін айқындау кезінде 0,7 коэффициенті қолданылады және осы көрсеткіш мынадай формуламен есептеледі:

$SP3 = (SP2 \times 100 / SP1) \times 0,7$, мұндағы:

SP3 - елеусіз бұзушылықтар көрсеткіші;

SP1 - елеулі бұзушылықтардың талап етілетін саны;

SP2 - анықталған елеулі бұзушылықтар саны.

Болмашы бұзушылықтардың көрсеткішін айқындау кезінде 0,3 коэффициенті қолданылады. Бұл көрсеткіш мына формула бойынша есептеледі:

$SPH = (SP2 \times 100 / SP1) \times 0,3$, мұндағы:

SPH - елеусіз бұзушылықтар көрсеткіші;

SP1 - елеусіз бұзушылықтардың талап етілетін саны;

SP2 - анықталған елеусіз бұзушылықтардың саны.

Бұзушылықтар бойынша тәуекел дәрежесінің көрсеткіші (SP) 0-ден 100-ге дейінгі шәкіл бойынша есептеледі және мына формула бойынша елеулі және болмашы бұзушылықтардың көрсеткіштерін қосу арқылы айқындалады:

- $SP = SP3 + SPH$ мұндағы:
- SP - тәуекел дәрежесінің ортақ көрсеткіші;
 - SP3 - елеулі бұзушылықтар көрсеткіші;
 - SPH - елеусіз бұзушылықтар көрсеткіші.

Тәуекел дәрежесінің көрсеткіштері бойынша бақылау субъектісі (объектісі) жатқызылады:

жоғары тәуекел дәрежесіне – тәуекел дәрежесі 71-ден 100-ге дейінгі көрсеткіш кезінде және оған қатысты бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау жүргізіледі;

жоғары тәуекел дәрежесіне жатқызылмаған – тәуекел дәрежесі 0-ден 71-ге дейінгі көрсеткіш кезінде және оған қатысты бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау жүргізілмейді.

11. Бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау жүргізудің жиілігі жарты жылда бір реттен артық болмау керек.

12. Субъектіге (объектіге) бару арқылы профилактикалық бақылау субъектіге (объектіге) бару арқылы профилактикалық бақылаудың жартыжылдық тізімдері негізінде жүзеге асырылады.

13. Субъектіге (объектіге) бару арқылы профилактикалық бақылаудың тізімдері субъективті өлшемшарттар бойынша тәуекел дәрежесінің ең жоғары көрсеткіштерімен бақылау субъектісінің (объектісінің) басымдылығын есепке ала отырып жасалады.

Киберқауіпсіздік бөлігінде
цифрландыру саласындағы
тәуекел дәрежесін
бағалау өлшемшарттарына
қосымша

Субъективті өлшемшарттар бойынша тәуекел дәрежесін айқындауға арналған субъективті өлшемшарттар тізбесі

№	Өлшемшарттар	Бұзушылық дәрежесі
Бақылау субъектілеріне (объектілеріне) бару арқылы алдыңғы тексерулер мен профилактикалық бақылау нәтижелері (ауырлық дәрежесі келесі талаптарды орындамау кезінде анықталады)		
	Спутниктік (ғарыштық) байланыс арналарын пайдаланатын ауылдық елді мекендердің орта білім беру объектілерін және екінші деңгейдегі банктерді қоспағанда, мемлекеттік органдардың жергілікті, ведомстволық және корпоративтік телекоммуникация желілерін, жергілікті атқарушы	

1.	органның (бұдан әрі-ЖАО), мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, сондай-ақ аса маңызды цифрлық объектілерінің иелерін байланыс операторларының Интернетке қол жеткізудің бірыңғай шлюзі арқылы Интернетке қосуын жүзеге асыру жөніндегі талаптарды сақтау	Елеулі
2.	Аса маңызды цифрлық объектілері иеленушілерінің Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығын киберқауіпсіздіктің оқыс оқиғалары туралы хабардар етуі бойынша талаптарды сақтау	Өрескел
3.	Қаражатты қолдану жөніндегі талаптарды сақтау: пайдаланушыларды сәйкестендіру , аутентификациялау және қол жеткізуді басқару; жабдықты сәйкестендіру; диагностикалық және конфигурациялық порттарды қорғау; жергілікті желіні физикалық сегменттеу; жергілікті желіні логикалық сегменттеу; желілік қосылымдарды басқару; брандмауэр; жергілікті желінің ішкі мекенжай кеңістігін жасыру; деректердің, хабарламалардың және конфигурациялардың тұтастығын бақылау; ақпаратты криптографиялық қорғау.	Елеулі
4.	Сыныптауышқа сәйкес "цифрлық үкіметтің" бірінші және екінші сыныптағы цифрлық объектілерін пайдалану кезінде Киберқауіпсіздікті қамтамасыз ету , қорғау және цифрлық объектілерді қауіпсіз жұмыс істеуін қамтамасыз ету мониторингі жүйесіне қосылу бойынша талаптарды сақтау	Елеулі
	Сыртқы контурдың жергілікті желілерінен интернетке қол	

5.	жеткізуді ұйымдастыру кезінде интернет желісіне қосылған жұмыс станцияларында вирусқа қарсы құралдардың, операциялық жүйелердің жаңартуларының болуы бойынша талаптарды сақтау	Елеулі
6.	Цифрлық объектілерді құру, сүйемелдеу және дамыту мәселелерімен айналысатын басқа құрылымдық бөлімшелерден оқшауланған құрылымдық бөлімше болып табылатын киберқауіпсіздік бөлімшесінің болуы немесе сертификат бере отырып, киберқауіпсіздікті қамтамасыз етуге және киберқауіпсіздікті қамтамасыз ету саласында кемінде үш жылда бір рет сертификат бере отырып мамандандырылған курстардан өтуге жауапты лауазымды адамды айқындау бойынша талаптарды сақтау.	Өрескел
	Мемлекеттік органдар (бұдан әрі – МО), ЖАО немесе ұйым өз қызметінде басшылыққа алатын құжатталған қағидалардың, рәсімдердің, практикалық тәсілдердің немесе басшылық қағидаттардың төрт деңгейлі жүйесі түрінде киберқауіпсіздікті қамтамасыз ету жөніндегі нормативтік-техникалық құжаттаманың (бұдан әрі – ТҚ) болуы және оған сәйкестігі бойынша талаптарды сақтау киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ қазақ және орыс тілдерінде әзірленеді, МО-ның, ЖАО-ның немесе ұйымның құқықтық актісімен бекітіледі және МО, ЖАО барлық қызметшілерінің немесе ұйым қызметкерлерінің назарына жеткізіледі. Киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ ондағы ақпаратты талдау және жаңарту мақсатында кемінде екі жылда бір рет қайта қаралады. 1. МО-ның, ЖАО-ның немесе ұйымның киберқауіпсіздік	

саясаты бірінші деңгейдегі құжат болып табылады және МО немесе ұйым күнделікті қызметінде басшылыққа алатын киберқауіпсіздікті қамтамасыз ету саласындағы мақсаттарды, міндеттерді, басшылық қағидаттары мен практикалық тәсілдерді айқындайды.

2. Екінші деңгейдегі құжаттар тізбесіне МО-ның, ЖАО-ның немесе ұйымның киберқауіпсіздік саясатының талаптарын нақтылайтын құжаттар кіреді, оның ішінде:

- 1) киберқауіпсіздіктің тәуекелдерін бағалау әдістемесі;
- 2) ақпаратты өңдеу және оларды түгендеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау, паспорттау қағидалары;
- 3) ішкі киберқауіпсіздік аудитін жүргізу қағидалары;
- 4) ақпаратты криптографиялық қорғау құралдарын (бұдан әрі - АҚКҚ) пайдалану тәртібі;
- 5) аутентификациялау рәсімін ұйымдастыру, цифрлық ресурстарға қол жеткізу құқығының аражігін ажырату қағидалары;
- 6) вирусқа қарсы бақылауды ұйымдастыру, мобильдік қондырғыларды және ақпаратты тасығыштарды пайдалану, интернет желісі мен электрондық поштаны пайдалану қағидалары;
- 7) ақпараттық ресурстардың жұмыс істеуінің физикалық қорғалуын және қауіпсіз ортасын ұйымдастыру, ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар;

3. Үшінші деңгейдегі құжаттар киберқауіпсіздікті қамтамасыз ету процестері мен рәсімдерінің сипаттамаларын қамтиды, оның ішінде:

- 1) киберқауіпсіздік қатерлері (тәуекелдері) каталогы;

	2) киберқауіпсіздік қатерлерін (тәуекелдерін) өңдеу жоспары; 3) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын және жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету бойынша іс-шаралар жоспары; 4) әкімшінің цифрлық объектісін сүйемелдеу, ақпаратты резервтік көшіру және қалпына келтіру жөніндегі басшылығы; 5) пайдаланушылардың киберқауіпсіздіктің оқыс оқиғаларына ден қою және штаттан тыс (дағдарысты) жағдайларда әрекет ету бойынша іс-қимыл тәртібі туралы нұсқаулық. 4. Төртінші деңгейдегі құжаттар тізбесі орындалған рәсімдер мен жұмыстарды тіркеу және растау үшін пайдаланылатын жұмыс нысандарын, журналдарды, өтінімдерді, хаттамаларды және басқа да құжаттарды, сонымен бірге электрондық құжаттарды қамтиды, оның ішінде: 1) киберқауіпсіздік оқыс оқиғаларын тіркеу және штаттан тыс оқиғаларды есепке алу журналы; 2) серверлік үй-жайларға кіру журналы; 3) желілік ресурстардың осалдықтарын бағалауды жүргізу туралы есеп; 4) кабельдік қосылуларды есепке алу журналы; 5) резервтік көшірмелерді (резервтік көшірме, қайта қалпына келтіру), резервтік көшірмелерді тестілеуді есепке алу журналы;	
8.	Көп факторлы аутентификацияны қолдану бойынша сыныптауышқа сәйкес, оның ішінде цифрлық сертификаттар пайдалана отырып, бірінші және екінші сыныптардың цифрлық объектілерге қол жеткізу кезінде талаптарды сақтау	Елеулі
	Лауазымдық нұсқаулықтарға киберқауіпсіздікті қамтамасыз ету бойынша функционалдық	

9.	міндеттерді енгізу жөніндегі талаптарды және МО, ЖАО немесе ұйым қызметшілерінің киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ талаптарын орындау бойынша міндеттемелерін сақтау	Елеулі
10.	АКҚҚ пайдалану бойынша талаптарды сақтау: бірінші сыныптағы цифрландыру объектілері үшін сыныптауышқа сәйкес – үшінші қауіпсіздік деңгейінің; екінші сыныптағы цифрландыру объектілері үшін сыныптауышқа сәйкес – екінші қауіпсіздік деңгейінің; үшінші сыныптағы цифрландыру объектілері үшін сыныптауышқа сәйкес – бірінші қауіпсіздік деңгейінің АКҚҚ (бағдарламалық және аппараттық) қолданылады.	Өрескел
11.	"Цифрлық үкіметтің" цифрлық инфрақұрылымы объектісінің меншік иесі немесе иегері, сондай-ақ "цифрлық үкімет" операторы "цифрлық үкіметтің" цифрлық инфрақұрылымы объектілерінде қамтылған мемлекеттік цифрлық ресурстарды (бұдан әрі-ЦР) сақтау бойынша талаптарды сақтау	Өрескел
12.	Мазмұнды (контентті) басқару жүйелерін қолдану бойынша ЦР киберқауіпсіздікті қамтамасыз ету үшін талаптарды сақтау: ЦР-ды орналастыру, өзгерту және жою операцияларына санкция беру; ЦР-ды орналастыру, өзгерту және жою кезінде авторлықты тіркеу; жүктелетін ЦР-ды зиянды кодқа тексеру; орындалатын код пен сценарийлердің қауіпсіздік аудиті; орналастырылған ЦР тұтастығын бақылау; ЦР өзгерістер журналын жүргізу; пайдаланушылардың және бағдарламалық роботтардың қалыптан тыс белсенділігін мониторингтеу	Өрескел

13.	Домендік аттың төлнұсқалылығын тексеру және ЦР киберқауіпсіздікті қамтамасыз ету кезінде ақпаратты криптографиялық қорғау құралдарын пайдалана отырып, байланыс сеансындағы ақпаратты криптографиялық қорғау үшін тіркеу куәліктерін қолдану бойынша талапты сақтау	Елеулі
14.	Виртуалдау технологиясын пайдалану кезінде сәйкестендіруді басқару бойынша талаптарды сақтау: Көрсетілетін цифрлық қызметтерінің клиенттерін және ерекшеленген пайдаланушыларды аутентификациялауды; пайдаланушыларды бір технологиялық платформа шегінде федеративтік сәйкестендіруді; пайдаланушыны сәйкестендіргішті жойғаннан кейін аутентификация туралы ақпаратты сақтауды; пайдаланушы өкілеттерінің бейіндерін тағайындау рәсімдерін бақылау құралдарын қолдануды талап ететін сәйкестендіруді басқару	Елеулі
15.	Виртуалдау технологиясын пайдалану кезінде киберқауіпсіздіктің оқиғаларына аудит жүргізу бойынша талаптарды сақтау: киберқауіпсіздік ТҚ-да айқындалатын рәсімдердің міндеттілігі мен тұрақтылығын; барлық операциялық жүйелерге, клиенттік виртуалды машиналарға, желілік компоненттердің инфрақұрылымына арналған аудит рәсімдерін жүргізуді; оқиғаларды тіркеу журналын жүргізуді және әкімшіге қолжетімсіз сақтау жүйесінде сақтауды; оқиғаларды тіркеу журналын жүргізу жүйесі жұмысының дұрыстығын тексеруді; оқиғаларды тіркеу журналдарын киберқауіпсіздікті қамтамасыз ету	Елеулі

	жөніндегі ТҚ-да сақтау ұзақтығын айқындауды талап ететін киберқауіпсіздік оқиғалары аудитін жүргізу	
16.	Виртуалдау технологиясын пайдалану кезінде киберқауіпсіздік оқиғаларын тіркеу талаптарын сақтау: әкімшілердің іс-қимылын журналға енгізуді; киберқауіпсіздік оқыс оқиғалары мен оқиғалар мониторингі жүйесін қолдануды; сыни оқиғаны немесе киберқауіпсіздік оқыс оқиғаларын автоматты тану негізінде хабарландыруды талап ететін киберқауіпсіздік оқиғаларын тіркеу	Елеулі
17.	Желілік және жүйелік әкімшілендіру рәсімдерін орындау бойынша талаптарды сақтау: виртуалды машиналар кескіндерінің сақталуын, операциялық жүйенің, қосымшалардың, желілік конфигурацияның, МО немесе ұйымның бағдарламалық қамтылымдарын (бұдан әрі -БҚ) және деректерінің зиянды қолтаңбалардың болуын бақылауды қамтамасыз ету; сыртқы пайдаланушылардың аппараттық бөлікке кіруін болдырмау мақсатында аппараттық платформаны виртуалды машинаның операциялық жүйесінен бөлу	Елеулі
18.	Резервтік көшіру жүйесімен деректерді сақтау жүйесін қамтамасыз ету бойынша талаптарды сақтау	Елеулі
19.	Жергілікті желілерді біріктіретін бөлінген байланыс арнасын ұйымдастыру кезінде ақпаратты қ о р ғ а у д ы ң бағдарламалық-техникалық құралдарын, оның ішінде криптографиялық шифрлауды АҚКҚ пайдалана отырып қолдану жөніндегі талаптарды сақтау	Елеулі

20.	Шетелде орналасқан немесе экрандалған ішкі желіні қолдана отырып ұйымдастырылған Қазақстан Республикасының мекемелері үшін АКҚҚ пайдалана отырып ұйымдастырылған байланыс арналарын қоспағанда, ішкі контурдың жергілікті желісі (бұдан әрі- ЖЖ) және сыртқы контурдың ЖЖ бір-бірімен ұштасуын болдырмау жөніндегі талаптарды сақтау	Өрескел
21.	Ведомстволық электрондық поштаны, жедел хабарламалар қызметін және өзге де сервистерді МО, ЖАО қызметшілерінің және мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, сондай-ақ аса маңызды цифрлық объектілер иелерінің: олар қызметтік міндеттерін атқарған кезде электрондық нысандағы жедел ақпарат алмасуды (қызметтік хат алмасуды) жүзеге асыру үшін, егер уәкілетті орган өзгеше белгілемесе, Қазақстан Республикасының аумағында нақты орналасқан электрондық поштаны, жедел хабар алмасу қызметін және өзге де сервистерді, басқару орталықтары мен серверлерді пайдалану жөніндегі талаптарды сақтауы	Елеулі
22.	Жергілікті желілердің белсенді жабдықтары үшін үздіксіз электрмен жабдықтаудың болуы бойынша талаптарды сақтау	Елеулі
23.	Жергілікті желінің кабельдік жүйесінің пайдаланылмайтын порттарын белсенді жабдыктан физикалық ажырату бойынша талапты сақтау	Елеусіз
24.	Желіаралық экрандауды пайдалану бойынша талаптарды сақтау	Елеулі
	Серверлік үй-жай бойынша келісі талаптарды сақтау: 1) Серверлік үй-жайда орнатылған жабдықты техникалық сүйемелдеу кезіне құжаттаманың болуы; жабдыққа қызмет көрсету; аппараттық-бағдарламалық	

қамтылымның жұмысында пайда болатын проблемаларды жою; кідірулер мен істен шығу фактілері, сондай-ақ қалпына келтіру жұмыстарының нәтижелері; өте маңызды жабдыққа кепілдікті қызмет көрсету мерзімі аяқталған соң кепілдікті мерзімнен кейінгі қызмет көрсету құжатталады.

2) Санкцияланған кіруді және санкцияланған шығуды қамтамасыз ететін кіруді бақылау және басқару жүйесінің болуы;

3) Цифрлық инфрақұрылым объектілерін сүйемелдеуді жүзеге асыру үшін уәкілетті тұлғалар тізімінің өзекті күйінде болуы;

4) Жабдықты техникалық сүйемелдеу кезінде құжаттаудың болуы;

5) Күзет дабылы жүйесінің болуы;

6) Бейнебақылау жүйесінің болуы;

7) Өрт дабылы жүйесінің болуы;

8) Өрт сөндіру жүйесінің болуы;

9) Кепілдендірілген электрмен жабдықтау жүйесінің болуы;

10) Жерге тұйықтау жүйесінің болуы;

11) Серверлік жабдықтың конфигурациясын тексере отырып, оны тұрақты негізде түгендеу жүргізу жөніндегі талаптарды сақтау;

12) Серверлік үй-жайда аппараттық-бағдарламалық кешен серверлік жабдығын және деректерді сақтау жүйесін орналастыру жөніндегі талаптарды сақтау;

13) Серверлік үй-жай өте алмайтын, терезе ойықтары жоқ бөлек үй-жайларда орналастыру. Терезе ойықтары болған жағдайда, олар жабылады немесе жанбайтын материалдармен бекітіледі. Қабырға, төбе мен еден сырттары үшін шаң шығармайтын және жинамайтын материалдар пайдаланылу. Еден жабыны үшін антистатикалық қасиеті бар материалдар пайдаланылады;

	14) Серверлік үй-жай кабельдік жүйелер мен инженерлік коммуникацияларды орналастыруға арналған фальшеденмен және (немесе) фальштөбемен жабдықталудың болуы; 15) Кез келген транзиттік коммуникациялардан өту бойынша алып тастау жөніндегі талаптарды сақтау; 16) Негізгі және резервтік серверлік үй-жайлардың бір-бірінен шалғайдағы ғимараттарда қауіпсіз қашықтықта орналасуы бойынша талаптарды сақтау. Резервтік серверлік үй жайларға қойылатын талаптар негізгі серверлік үй жайларға қойылатын талаптармен бірдей.	
26.	Кростық үй-жай бойынша келесі талаптарды сақтау: 1) Электромагниттік кедергілердің қуатты көздерінің болмауы; 2) Сумен жабдықтау жүйесінің бұрандалары мен құбырларының болмауы; 3) Өрт қауіпсіздігі жүйесінің болуы; 4) Жеңіл жанатын материалдардың болмауы; 5) Жоба бойынша шкафты қосу үшін автоматтан бөлек жеке электр қуатталу желісінің болуы; 6) Сигнализациялық күзет жүйесінің, кіруді бақылау жүйесінің болуы; 7) Ауа баптау жүйесінің болуы.	Өрескел
27.	Цифрлық объектілерді тәжірибелік және өнеркәсіптік пайдалану кезеңінде құралдар мен жүйелерді пайдалану талаптарын сақтау: оқиғаларды және киберқауіпсіздіктің оқыс оқиғаларын мониторингілеу және басқару; цифрлық инфрақұрылым; басып кірудің алдын алу және анықтау.	Елеулі
	Киберқауіпсіздік жеке жедел орталығын құру және оның жұмыс істеуін қамтамасыз ету немесе үшінші тұлғалардан киберқауіпсіздіктің жедел	

28.	орталығының қызметтерін сатып алу жөніндегі талаптарды сақтау, сондай-ақ оның Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығымен өзара іс-қимылы.	Өрескел
29.	Тіркелген. KZ және (немесе). ҚАЗ домендік атауы бар интернет-ресурсты Қазақстан Республикасының аумағында орналасқан аппараттық-бағдарламалық кешенде орналастыру жөніндегі талапты сақтау. Интернеттің қазақстандық сегментінің кеңістігінде. KZ және (немесе). ҚАЗ домендік аттарын пайдалану қауіпсіздік сертификаттарын қолдану арқылы жүзеге асырылу талаптарын сақтау	Елеулі
30.	МО, ЖАО және ұйымдар сенім білдірілген бағдарламалық қамтылым және электрондық өнеркәсіп өнімдерінің тізілімінен елдің қорғанысы мен мемлекеттің қауіпсіздігі үшін киберқауіпсіздікті қамтамасыз ету талаптарын іске асыру мақсатында тауарларды сатып алу жөніндегі талаптарды сақтау.	Елеусіз
	МО-да, ЖАО-да немесе ұйымда киберқауіпсіздіктің бұзылу оқиғаларын бақылау мақсатында талаптарды сақтау: 1) Киберқауіпсіздікті бұзуға байланысты оқиғалар мониторингі мен мониторинг нәтижелерін талдау жүргізіледі; 2) Киберқауіпсіздіктің жай-күйіне байланысты оқиғалар тіркеліп, оқиғалар журналдарын, оның ішінде: операциялық жүйелердің оқиғалар журналдарын; дерекқорларды басқару жүйелерінің оқиғалар журналдарын; вирусқа қарсы қорғау оқиғаларының журналдарын; қолданбалы БҚ оқиғалар журналдарын;	

31.	телекоммуникациялық жабдықтың оқиғалар журналдарын; шабуылдарды анықтау және алдын алу жүйелерінің оқиғалар журналдарын; контентті басқару жүйесі оқиғаларының журналын талдау арқылы бұзушылықтар анықталады; 3) оқиғаларды тіркеу журналдарындағы уақытты уақыт көзінің инфрақұрылымымен үйлесімді қамтамасыз ету; 4) оқиғаларды тіркеу журналдарын киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ-да көрсетілген мерзім ішінде сақтау, бірақ үш жылдан кем емес және екі айдан кем емес жедел қолжетімділікте болу; 5) оқиғаларды тіркеу журналдарын жүргізу; 6) оқиғаларды тіркеу журналдарын араласудан және рұқсатсыз кіруден қорғауды қамтамасыз ету. Жүйелік әкімшілерде журналдарды өзгертуге, жоюға және өшіруге өкілеттіктердің болуына жол бермеу. Құпия ЦЖ журналдардың резервтік қоймасын құруды және жүргізуді талап етеді; 7) Киберқауіпсіздік оқыс оқиғалары туралы хабардар етудің және киберқауіпсіздік оқыс оқиғаларына әрекет етудің формальді рәсімін енгізу қамтамасыз етіледі.	Елеулі
32.	ЦР, ЦЖ, цифрлық инфрақұрылымның киберқауіпсіздігін қамтамасыз етуге бөгде ұйымдарды тартқан жағдайда олардың иесі немесе иеленушісі аталған объектілермен жұмыс істеу, оларға қол жеткізу немесе пайдалану шарттары, сондай-ақ оларды бұзғаны үшін жауапкершілігі белгіленетін келісімдерінің болуы жөніндегі талапты сақтау	Өрескел
	Ұйым қызметкерінің еңбек шартының талаптарына өзгерістер	

33.	енгізу, МО, ЖАО қызметшісін ротациялау немесе Мемлекеттік қызмет бойынша ілгерілету, оларды жұмыстан шығару кезінде физикалық және логикалық қолжетімділікті, қол жеткізу, жазылу сәйкестендіргіштерін, оны МО, ЖАО жұмыс істейтін қызметшісі немесе ұйым жұмыскері ретінде сәйкестендіретін құжаттаманы қамтитын ақпаратқа және ақпаратты өңдеу құралдарына қол жеткізу құқықтарын сақтау, жойылады.	Өрескел
34.	Кадр қызметімен МО, ЖАО қызметшілерін немесе ұйым жұмыскерлерін цифрландыру және киберқауіпсіздікті қамтамасыз ету саласында оқытуын ұйымдастыру және электрондық сертификат беріле отырып, жеке іс материалдарында сақталу есебін жүргізу талаптарын сақтау	Елеусіз
35.	Киберқауіпсіздік оқиғалары мониторингін және оқиғалар журналын талдау нәтижелері бойынша құпиялылығы, қолжетімділігі мен тұтастығы үшін өте қатерлі болып сәйкестендірілген киберқауіпсіздік оқиғаларын мемлекеттік техникалық қызметтің компьютерлік инциденттерге әрекет ету қызметінде тіркеу талаптарын сақтау	Елеулі
36.	Екінші деңгейдегі банктерді қоспағанда, заңмен қорғалатын құпияны қамтитын деректерді өңдейтін аса маңызды цифрлық объектілерінің иелеріне жылына кемінде бір рет киберқауіпсіздік аудитін жүргізу жөніндегі талаптарды сақтау.	Елеулі
37.	Сервистік бағдарламалық өнімді өнеркәсіптік пайдалану кезінде киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сынақтардың оң нәтижелері бар актінің болуы жөніндегі талаптарды сақтау.	Елеулі

38.	Өзірленетін немесе сатып алынатын дайын қолданбалы БҚ пайдаланушы интерфейсін пайдаланушының тіл интерфейсін таңдау мүмкіндігімен, деректерді қазақ, орыс және қажет болған жағдайда басқа тілдерде енгізуді, өңдеу мен шығаруды қамтамасыз ету талаптарын сақтау	Елеусіз
39.	МО, ЖАО немесе ұйым: пайдаланушылар мен персоналдың іс-қимылы; ақпаратты өңдеу құралдарын қолдану мониторингін жүзеге асырады.	Елеусіз
40.	Өзірленетін немесе сатып алынатын дайын қолданбалы БҚ қазақ және орыс тілдерінде пайдалану жөніндегі техникалық құжаттамамен қамтамасыз ету талаптарын сақтау	Елеусіз
41.	Ендірілген жүйелер серверінің жоғары қолжетімділігін қамтамасыз ету жөніндегі талаптарды сақтау: 1) резервтік желдеткіштерді, қуат көздерін, дискілерді және енгізу-шығару адаптерлерін қызу ауыстыру; 2) сыни оқиғалар туралы ескертулер; 3) сыни компоненттердің жай-күйін үздіксіз бақылауды қолдау және бақыланатын көрсеткіштерді өлшеу	Елеулі
42.	Құпия ЦЖ-да, құпия ЦР-да және қолжетімділігі шектелген дербес деректерді қамтитын ЦР-да пайдаланылатын ақпаратты тасығыштарды пайдаланудан шығарған кезде ақпаратты кепілдікті жоюдың бағдарламалық және аппараттық қамтылымы қолдану жөніндегі талапты сақтау	Елеулі
43.	Жергілікті желінің құжат жүзіндегі схемасы болуы және оны пайдаланған кезде өзектілендірілген күйде ұсталу талабының сақталуы	Елеусіз
	МО, ЖАО цифрлық объектілерін және аса маңызды цифрлық объектілерін қорғау үшін деректердің тарап кетуін болғызбау жүйелері (DLP)	

44.	қолдану жөніндегі талаптарды сақтау. Бұл ретте: іс-қимылға жүргізілетін бақылау туралы пайдаланушыны визуалды түрде хабардар ету; жергілікті желі шегінде деректердің тарап кетуін болғызбау жүйесінің басқару орталығы мен серверлерін орналастыру қамтамасыз етіледі.	Елеусіз
45.	МО-ның және ЖАО-ның ЦЖ-сын, оның ішінде МО-ның немесе ЖАО-ның тәжірибелік пайдалануға енгізілген ЦЖ-сымен интеграциялау талаптарын сақтау.	Елеулі
46.	"Цифрлық үкіметтің" операторы ұйымдастырған АКҚҚ пайдаланылатын мемлекеттік органдардың бірыңғай көліктік ортасының (бұдан әрі - МО БКО) сымсыз байланыс арналарын қоспағанда, МО БКО-ға, ЦС-нің жергілікті желісіне, сондай-ақ МО БКО, ЦС-нің жергілікті желісінің құрамына кіретін техникалық құралдарға сымсыз желілер арқылы қашықтан қол жеткізуді, сымсыз қолжетімділікті ұйымдастыруға арналған құралдарды, модемдерді, радиомодемдерді, ұялы байланыс операторларының желілік модемдерін, ұялы байланыстың абоненттік құрылғыларын және басқа да сымсыз желілік құрылғыларды қосуға жол берілмеу бойынша талаптарды сақтау	Өрескел
47.	"Цифрлық үкіметтің" цифрлық объектісін өнеркәсіптік пайдалануға беруді оның меншік иесі немесе иеленушісі мемлекеттік техникалық қызмет берген "цифрлық үкіметтің" цифрлық объектілерінің бастапқы кодтарынан құрастырылған орындалатын кодтарды пайдалана отырып қана жүзеге асыру бойынша талаптарды сақтау.	Елеулі
48.	Цифрлық субъектінің ішкі шеңберінің ЖЖ Интернетке	Өрескел

	қосуға жол берілмеу бойынша талаптарды сақтау	
49.	Интернет-ресурс иесі және (немесе) иеленушісі пайдаланушының кескін тілін таңдау мүмкіндігімен қазақ, орыс және қажет болған жағдайда басқа тілдерде көпшілікке қолжетімді Интернет-ресурстарды құруды қамтамасыз ету бойынша талаптарды сақтау	Елеусіз
50.	Тәжірибелік пайдалану оң аяқталған, киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сынақтардың оң нәтижелері бар сынақ хаттамалары болған, цифрландыру және киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органдардың, мүдделі МО-ның, ЖАО-ның және ұйымдардың өкілдері қатысатын қабылдау комиссиясы ЦЖ-ны өнеркәсіптік пайдалануға беру туралы актіге қол қойған жағдайда МО-ның, ЖАО-ның және ұйымдардың ЦЖ-ны өнеркәсіптік пайдалануға беру жөніндегі талаптарды сақтау	Елеулі

Қазақстан Республикасы
Премьер-Министрінің
орынбасары-
Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2019 жылғы 29 қаңтардағы
№13/НҚ және
Қазақстан Республикасы
Ұлттық экономика
министрінің
2019 жылғы 29 қаңтардағы
№ 12 бірлескен
бұйрығына
4-қосымша

Қазақстан Республикасы Кәсіпкерлік кодексінің 138 бабына сәйкес квазимемлекеттік сектор субъектілеріне, мемлекеттік органдардың цифрлық жүйелерімен интеграцияланатын немесе мемлекеттік цифрлық ресурстарды қалыптастыруға арналған мемлекеттік емес цифрлық жүйелердің иелері мен иеленушілеріне, киберқауіпсіздікті қамтамасыз ету орталықтарына, сонымен қатар аса маңызды цифрлық объектілерінің иелері мен иеленушілеріне қатысты киберқауіпсіздік бөлігінде цифрландыру саласындағы тексеру парағы

Ескерту. Бұйрық 4-қосымшамен толықтырылды - ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 10.09.2026 № 550/НҚ және ҚР Премьер-Министрінің орынбасары – Ұлттық экономика министрінің 11.09.2026 № 145 (алғаш ресми жарияланған күнінен кейін он күнтізбелік күн өткен соң қолданысқа енгізіледі) бірлескен бұйрығымен.

бақылау субъектілерінің (объектілерінің) біртекті тобының атауы
Тексеруді/ бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылауды тағайындаған мемлекеттік орган

Тексеруді/ бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылауды тағайындау туралы акт

№, күні
Бақылау субъектісінің (объектісінің) атауы

Бақылау субъектісінің (объектісінің) (жеке сәйкестендіру нөмірі), бизнес-сәйкестендіру нөмірі

Орналасқан жерінің мекенжайы

№	Талаптар тізбесі	Талаптарға сәйкес келеді	Талаптарға сәйкес келмейді
1	2	3	4
1	Спутниктік (ғарыштық) байланыс арналарын пайдаланатын ауылдық елді мекендердің орта білім беру объектілерін және екінші деңгейдегі банктерді қоспағанда, мемлекеттік органдардың жергілікті, ведомстволық және корпоративтік телекоммуникация желілерін, жергілікті атқарушы органның (бұдан әрі-ЖАО), мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, сондай-ақ аса маңызды цифрлық объектілерінің		

	иелерін байланыс операторларының Интернетке қол жеткізудің бірыңғай шлюзі арқылы Интернетке қосуын жүзеге асыру жөніндегі талаптарды сақтау		
2	Аса маңызды цифрлық объектілері иеленушілерінің Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығын киберқауіпсіздіктің оқыс оқиғалары туралы хабардар етуі бойынша талаптарды сақтау		
3	Қаражатты қолдану жөніндегі талаптарды сақтау: пайдаланушыларды сәйкестендіру, аутентификациялау және қол жеткізуді басқару; жабдықты сәйкестендіру; диагностикалық және конфигурациялық порттарды қорғау; жергілікті желіні физикалық сегменттеу; жергілікті желіні логикалық сегменттеу; желілік қосылымдарды басқару; брандмауэр; жергілікті желінің ішкі мекенжай кеңістігін жасыру; деректердің, хабарламалардың және конфигурациялардың тұтастығын бақылау; ақпаратты криптографиялық қорғау.		
	Сыныптауышқа сәйкес "цифрлық үкіметтің" бірінші және екінші сыныптағы цифрлық объектілерін пайдалану кезінде Киберқауіпсіздікті қамтамасыз ету, қорғау		

4	және цифрлық объектілерді қауіпсіз жұмыс істеуін қамтамасыз ету мониторингі жүйесіне қосылу бойынша талаптарды сақтау		
5	Сыртқы контурдың жергілікті желілерінен интернетке қол жеткізуді ұйымдастыру кезінде интернет желісіне қосылған жұмыс станцияларында вирусқа қарсы құралдардың, операциялық жүйелердің жаңартуларының болуы бойынша талаптарды сақтау		
6	Цифрлық объектілерді құру, сүйемелдеу және дамыту мәселелерімен айналысатын басқа құрылымдық бөлімшелерден оқшауланған құрылымдық бөлімше болып табылатын киберқауіпсіздік бөлімшесінің болуы немесе сертификат бере отырып, киберқауіпсіздікті қамтамасыз етуге және киберқауіпсіздікті қамтамасыз ету саласында кемінде үш жылда бір рет сертификат бере отырып мамандандырылған курстардан өтуге жауапты лауазымды адамды айқындау бойынша талаптарды сақтау.		
	Мемлекеттік органдар (бұдан әрі – МО), ЖАО немесе ұйым өз қызметінде басшылыққа алатын құжатталған қағидалардың, рәсімдердің, практикалық тәсілдердің немесе		

басшылық қағидаттардың төрт деңгейлі жүйесі түрінде киберқауіпсіздікті қамтамасыз ету жөніндегі нормативтік-техникалық құжаттаманың (бұдан әрі – ТҚ) болуы және оған сәйкестігі бойынша талаптарды сақтау киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ қазақ және орыс тілдерінде әзірленеді, МО-ның, ЖАО-ның немесе ұйымның құқықтық актісімен бекітіледі және МО, ЖАО барлық қызметшілерінің немесе ұйым қызметкерлерінің назарына жеткізіледі. Киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ ондағы ақпаратты талдау және жаңарту мақсатында кемінде екі жылда бір рет қайта қаралады.

1. МО-ның, ЖАО-ның немесе ұйымның киберқауіпсіздік саясаты бірінші деңгейдегі құжат болып табылады және МО немесе ұйым күнделікті қызметінде басшылыққа алатын киберқауіпсіздікті қамтамасыз ету саласындағы мақсаттарды, міндеттерді, басшылық қағидаттары мен практикалық тәсілдерді айқындайды.

2. Екінші деңгейдегі құжаттар тізбесіне МО-ның, ЖАО-ның немесе ұйымның киберқауіпсіздік саясатының талаптарын нақтылайтын құжаттар кіреді, оның ішінде:

- 1) киберқауіпсіздіктің тәуекелдерін бағалау әдістемесі;
 - 2) ақпаратты өңдеу және оларды түгендеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау, паспорттау қағидалары;
 - 3) ішкі киберқауіпсіздік аудитін жүргізу қағидалары;
 - 4) ақпаратты криптографиялық қорғау құралдарын (бұдан әрі - АҚКҚ) пайдалану тәртібі ;
 - 5) аутентификациялау рәсімін ұйымдастыру, цифрлық ресурстарға қол жеткізу құқығының аражігін ажырату қағидалары;
 - 6) вирусқа қарсы бақылауды ұйымдастыру , мобильдік қондырғыларды және ақпаратты тасығыштарды пайдалану, интернет желісі мен электрондық поштаны пайдалану қағидалары;
 - 7) ақпараттық ресурстардың жұмыс істеуінің физикалық қорғалуын және қауіпсіз ортасын ұйымдастыру, ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар;
3. Үшінші деңгейдегі құжаттар киберқауіпсіздікті қамтамасыз ету процестері мен рәсімдерінің сипаттамаларын қамтиды , оның ішінде:

- 1) киберқауіпсіздік қатерлері (тәуекелдері) каталогы;
 - 2) киберқауіпсіздік қатерлерін (тәуекелдерін) өңдеу жоспары;
 - 3) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын және жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету бойынша іс-шаралар жоспары;
 - 4) әкімшінің цифрлық объектісін сүйемелдеу, ақпаратты резервтік көшіру және қалпына келтіру жөніндегі басшылығы;
 - 5) пайдаланушылардың киберқауіпсіздіктің оқыс оқиғаларына ден қою және штаттан тыс (дағдарысты) жағдайларда әрекет ету бойынша іс-қимыл тәртібі туралы нұсқаулық.
4. Төртінші деңгейдегі құжаттар тізбесі орындалған рәсімдер мен жұмыстарды тіркеу және растау үшін пайдаланылатын жұмыс нысандарын, журналдарды, өтінімдерді, хаттамаларды және басқа да құжаттарды, сонымен бірге электрондық құжаттарды қамтиды, оның ішінде:
- 1) киберқауіпсіздік оқыс оқиғаларын тіркеу және штаттан тыс оқиғаларды есепке алу журналы;
 - 2) серверлік үй-жайларға кіру журналы;
 - 3) желілік ресурстардың осалдықтарын бағалауды жүргізу туралы есеп;

	4) кабельдік қосылуларды есепке алу журналы; 5) резервтік көшірмелерді (резервтік көшірме, қайта қалпына келтіру), резервтік көшірмелерді тестілеуді есепке алу журналы;		
8	Көп факторлы аутентификацияны қолдану бойынша сыныптауышқа сәйкес, оның ішінде цифрлық сертификаттар пайдалана отырып, бірінші және екінші сыныптардың цифрлық объектілерге қол жеткізу кезінде талаптарды сақтау		
9	Лауазымдық нұсқаулықтарға киберқауіпсіздікті қамтамасыз ету бойынша функционалдық міндеттерді енгізу жөніндегі талаптарды және МО, ЖАО немесе ұйым қызметшілерінің киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ талаптарын орындау бойынша міндеттемелерін сақтау		
10	АКҚҚ пайдалану бойынша талаптарды сақтау: бірінші сыныптағы цифрландыру объектілері үшін сыныптауышқа сәйкес – үшінші қауіпсіздік деңгейінің; екінші сыныптағы цифрландыру объектілері үшін сыныптауышқа сәйкес – екінші қауіпсіздік деңгейінің; үшінші сыныптағы цифрландыру объектілері үшін сыныптауышқа сәйкес – бірінші қауіпсіздік деңгейінің АКҚҚ (бағдарламалық		

	және аппараттық) қолданылады.		
11	"Цифрлық үкіметтің" цифрлық инфрақұрылымы объектісінің меншік иесі немесе иегері, сондай-ақ "цифрлық үкімет" операторы "цифрлық үкіметтің" цифрлық инфрақұрылымы объектілерінде қамтылған мемлекеттік цифрлық ресурстарды (бұдан әрі-ЦР) сақтау бойынша талаптарды сақтау		
12	Мазмұнды (контентті) басқару жүйелерін қолдану бойынша ЦР киберқауіпсіздікті қамтамасыз ету үшін талаптарды сақтау; ЦР-ды орналастыру, өзгерту және жою операцияларына санкция беру; ЦР-ды орналастыру, өзгерту және жою кезінде авторлықты тіркеу; жүктелетін ЦР-ды зиянды кодқа тексеру; орындалатын код пен сценарийлердің қауіпсіздік аудиті; орналастырылған ЦР тұтастығын бақылау; ЦР өзгерістер журналын жүргізу; пайдаланушылардың және бағдарламалық роботтардың қалыптан тыс белсенділігін мониторингтеу		
13	Домендік аттың төлнұсқалылығын тексеру және ЦР киберқауіпсіздікті қамтамасыз ету кезінде аппаратты криптографиялық қорғау құралдарын пайдалана отырып, байланыс		

	сеансындағы ақпаратты криптографиялық қорғау үшін тіркеу куәліктерін қолдану бойынша талапты сақтау		
14	Виртуалдау технологиясын пайдалану кезінде сәйкестендіруді басқару бойынша талаптарды сақтау; Көрсетілетін цифрлық қызметтерінің клиенттерін және ерекшеленген пайдаланушыларды аутентификациялауды; пайдаланушыларды бір технологиялық платформа шегінде федеративтік сәйкестендіруді; пайдаланушыны сәйкестендіргішті жойғаннан кейін аутентификация туралы ақпаратты сақтауды; пайдаланушы өкілеттерінің бейіндерін тағайындау рәсімдерін бақылау құралдарын қолдануды талап ететін сәйкестендіруді басқару		
15	Виртуалдау технологиясын пайдалану кезінде киберқауіпсіздіктің оқиғаларына аудит жүргізу бойынша талаптарды сақтау; киберқауіпсіздік ТҚ-да айқындалатын рәсімдердің міндеттілігі мен тұрақтылығын; барлық операциялық жүйелерге, клиенттік виртуалды машиналарға, желілік компоненттердің инфрақұрылымына арналған аудит рәсімдерін жүргізуді; оқиғаларды тіркеу журналын жүргізуді және		

	әкімшіге қолжетімсіз сақтау жүйесінде сақтауды; оқиғаларды тіркеу журналын жүргізу жүйесі жұмысының дұрыстығын тексеруді; оқиғаларды тіркеу журналдарын киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ-да сақтау ұзақтығын айқындауды талап ететін киберқауіпсіздік оқиғалары аудитін жүргізу		
16	Виртуалдау технологиясын пайдалану кезінде киберқауіпсіздік оқиғаларын тіркеу талаптарын сақтау: әкімшілердің іс-қимылын журналға енгізуді; киберқауіпсіздік оқыс оқиғалары мен оқиғалар мониторингі жүйесін қолдануды; сыни оқиғаны немесе киберқауіпсіздік оқыс оқиғаларын автоматты тану негізінде хабарландыруды талап ететін киберқауіпсіздік оқиғаларын тіркеу		
17	Желілік және жүйелік әкімшілендіру рәсімдерін орындау бойынша талаптарды сақтау: виртуалды машиналар кескіндерінің сақталуын, операциялық жүйенің, қосымшалардың, желілік конфигурацияның, МО немесе ұйымның бағдарламалық қамтылымдарын (бұдан әрі -БҚ) және деректерінің зиянды қолтаңбалардың болуын бақылауды қамтамасыз ету;		

	с ы р т қ ы пайдаланушылардың аппараттық бөлікке кіруін болдырмау мақсатында аппараттық платформаны виртуалды машинаның операциялық жүйесінен бөлу		
18	Резервтік көшіру жүйесімен деректерді сақтау жүйесін қамтамасыз ету бойынша талаптарды сақтау		
19	Жергілікті желілерді біріктіретін бөлінген байланыс арнасын ұйымдастыру кезінде ақпаратты қорғаудың бағдарламалық-техникал ық құралдарын, оның ішінде криптографиялық шифрлауды АҚҚҚ пайдалана отырып қолдану жөніндегі талаптарды сақтау		
20	Шетелде орналасқан немесе экрандалған ішкі желіні қолдана отырып ұйымдастырылған Қ а з а қ с т а н Республикасының мекемелері үшін АҚҚҚ пайдалана отырып ұйымдастырылған байланыс арналарын қоспағанда, ішкі контурдың жергілікті желісі (бұдан әрі- ЖЖ) және сыртқы контурдың ЖЖ бір-бірімен ұштасуын болдырмау жөніндегі талаптарды сақтау		
	Ведомстволық электрондық поштаны, жедел хабарламалар қызметін және өзге де сервистерді МО, ЖАО қызметшілерінің және мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің,		

21	сондай-ақ аса маңызды цифрлық объектілер иелерінің: олар қызметтік міндеттерін атқарған кезде электрондық нысандағы жедел ақпарат алмасуды (қызметтік хат алмасуды) жүзеге асыру үшін, егер уәкілетті орган өзгеше белгілемесе, Қазақстан Республикасының аумағында нақты орналасқан электрондық поштаны, жедел хабар алмасу қызметін және өзге де сервистерді, басқару орталықтары мен серверлерді пайдалану жөніндегі талаптарды сақтауы		
22	Жергілікті желілердің белсенді жабдықтары үшін үздіксіз электрмен жабдықтаудың болуы бойынша талаптарды сақтау		
23	Жергілікті желінің кабельдік жүйесінің пайдаланылмайтын порттарын белсенді жабдықтан физикалық ажырату бойынша талапты сақтау		
24	Желіаралық экрандауды пайдалану бойынша талаптарды сақтау		
	Серверлік үй-жай бойынша келісі талаптарды сақтау: 1) Серверлік үй-жайда орнатылған жабдықты техникалық сүйемелдеу кезіне құжаттаманың болуы: жабдыққа қызмет көрсету; аппараттық-бағдарламалық қамтылымның жұмысында пайда болатын проблемаларды жою; кідірулер мен істен шығу фактілері, сондай-ақ қалпына		

келтіру жұмыстарының нәтижелері; өте маңызды жабдыққа кепілдікті қызмет көрсету мерзімі аяқталған соң кепілдікті мерзімнен кейінгі қызмет көрсету құжатталады.

2) Санкцияланған кіруді және санкцияланған шығуды қамтамасыз ететін кіруді бақылау және басқару жүйесінің болуы;

3) Цифрлық инфрақұрылым объектілерін сүйемелдеуді жүзеге асыру үшін уәкілетті тұлғалар тізімінің өзекті күйінде болуы;

4) Жабдықты техникалық сүйемелдеу кезінде құжаттаудың болуы;

5) Күзет дабылы жүйесінің болуы;

6) Бейнебақылау жүйесінің болуы;

7) Өрт дабылы жүйесінің болуы;

8) Өрт сөндіру жүйесінің болуы;

9) Кепілдендірілген электрмен жабдықтау жүйесінің болуы;

10) Жерге тұйықтау жүйесінің болуы;

11) Серверлік жабдықтың конфигурациясын тексере отырып, оны тұрақты негізде түгендеу жүргізу жөніндегі талаптарды сақтау;

12) Серверлік үй-жайда аппараттық-бағдарламалық кешен серверлік жабдығын және деректерді сақтау жүйесін орналастыру жөніндегі талаптарды сақтау;

13) Серверлік үй-жай өте алмайтын, терезе ойықтары жоқ бөлек

	үй-жайларда орналастыру. Терезе ойықтары болған жағдайда, олар жабылады немесе жанбайтын материалдармен бекітіледі. Қабырға, төбе мен еден сырттары үшін шаң шығармайтын және жинамайтын материалдар пайдаланылу. Еден жабыны үшін антистатикалық қасиеті бар материалдар пайдаланылады; 14) Серверлік үй-жай кабельдік жүйелер мен инженерлік коммуникацияларды орналастыруға арналған фальшеденмен және (немесе) фальштөбемен жабдықталудың болуы; 15) Кез келген транзиттік коммуникациялардан өту бойынша алып тастау жөніндегі талаптарды сақтау; 16) Негізгі және резервтік серверлік үй-жайлардың бір-бірінен шалғайдағы ғимараттарда қауіпсіз қашықтықта орналасуы бойынша талаптарды сақтау. Резервтік серверлік үй жайларға қойылатын талаптар негізгі серверлік үй жайларға қойылатын талаптармен бірдей;	
	Кростық үй-жай бойынша келесі талаптарды сақтау: 1) Электромагниттік кедергілердің қуатты көздерінің болмауы; 2) Сумен жабдықтау жүйесінің бұрандалары мен құбырларының болмауы; 3) Өрт қауіпсіздігі жүйесінің болуы;	

26	4) Жеңіл жанатын материалдардың болмауы ; 5) Жоба бойынша шкафты қосу үшін автоматтан бөлек жеке электр қуатталу желісінің болуы; 6) Сигнализациялық күзет жүйесінің, кіруді бақылау жүйесінің болуы ; 7) Ауа баптау жүйесінің болуы.		
27	Цифрлық объектілерді тәжірибелік және өнеркәсіптік пайдалану кезеңінде құралдар мен жүйелерді пайдалану талаптарын сақтау: оқиғаларды және киберқауіпсіздіктің оқыс оқиғаларын мониторингілеу және басқару; цифрлық инфрақұрылым; басып кірудің алдын алу және анықтау.		
28	Киберқауіпсіздік жеке жедел орталығын құру және оның жұмыс істеуін қамтамасыз ету немесе үшінші тұлғалардан киберқауіпсіздіктің жедел орталығының қызметтерін сатып алу жөніндегі талаптарды сақтау, сондай-ақ оның Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығымен өзара іс-қимылы.		
29	Тіркелген. KZ және (немесе). ҚАЗ домендік атауы бар интернет-ресурсты Қазақстан Республикасының аумағында орналасқан аппараттық-бағдарламалық кешенде орналастыру жөніндегі талапты сақтау .		

	Интернеттің қазақстандық сегментінің кеңістігінде. KZ және (немесе). ҚАЗ домендік аттарын пайдалану қауіпсіздік сертификаттарын қолдану арқылы жүзеге асырылу талаптарын сақтау		
30	МО, ЖАО және ұйымдар сенім білдірілген бағдарламалық қамтылым және электрондық өнеркәсіп өнімдерінің тізілімінен елдің қорғанысы мен мемлекеттің қауіпсіздігі үшін киберқауіпсіздікті қамтамасыз ету талаптарын іске асыру мақсатында тауарларды сатып алу жөніндегі талаптарды сақтау.		
	МО-да, ЖАО-да немесе ұйымда киберқауіпсіздіктің бұзылу оқиғаларын бақылау мақсатында талаптарды сақтау: 1) Киберқауіпсіздікті бұзуға байланысты оқиғалар мониторингі мен мониторинг нәтижелерін талдау жүргізіледі; 2) Киберқауіпсіздіктің жай-күйіне байланысты оқиғалар тіркеліп, оқиғалар журналдарын, оның ішінде: операциялық жүйелердің оқиғалар журналдарын; дерекқорларды басқару жүйелерінің оқиғалар журналдарын; вирусқа қарсы қорғау оқиғаларының журналдарын; қолданбалы БҚ оқиғалар журналдарын;		

телекоммуникациялық жабдықтың оқиғалар журналдарын;
шабуылдарды анықтау және алдын алу жүйелерінің оқиғалар журналдарын;
контентті басқару жүйесі оқиғаларының журналын талдау арқылы бұзушылықтар анықталады;
3) оқиғаларды тіркеу журналдарындағы уақытты уақыт көзінің инфрақұрылымымен үйлесімді қамтамасыз ету ;
4) оқиғаларды тіркеу журналдарын киберқауіпсіздікті қамтамасыз ету жөніндегі ТҚ-да көрсетілген мерзім ішінде сақтау, бірақ үш жылдан кем емес және екі айдан кем емес жедел қолжетімділікте болу;
5) оқиғаларды тіркеу журналдарын жүргізу;
6) оқиғаларды тіркеу журналдарын араласудан және рұқсатсыз кіруден қорғауды қамтамасыз ету . Жүйелік әкімшілерде журналдарды өзгертуге, жоюға және өшіруге өкілеттіктердің болуына жол бермеу. Құпия ЦЖ журналдардың резервтік қоймасын құруды және жүргізуді талап етеді;
7) Киберқауіпсіздік оқыс оқиғалары туралы хабардар етудің және киберқауіпсіздік оқыс оқиғаларына әрекет етудің формальді рәсімін енгізу қамтамасыз етіледі .

ЦР, ЦЖ, цифрлық инфрақұрылымның киберқауіпсіздігін қамтамасыз етуге бөгде

32	ұйымдарды тартқан жағдайда олардың иесі немесе иеленушісі аталған объектілермен жұмыс істеу, оларға қол жеткізу немесе пайдалану шарттары, сондай-ақ оларды бұзғаны үшін жауапкершілігі белгіленетін келісімдерінің болуы жөніндегі талапты сақтау		
33	Ұйым қызметкерінің еңбек шартының талаптарына өзгерістер енгізу, МО, ЖАО қызметшісін ротациялау немесе Мемлекеттік қызмет бойынша ілгерілету, оларды жұмыстан шығару кезінде физикалық және логикалық қолжетімділікті, қол жеткізу, жазылу сәйкестендіргіштерін, оны МО, ЖАО жұмыс істейтін қызметшісі немесе ұйым жұмыскері ретінде сәйкестендіретін құжаттаманы қамтитын ақпаратқа және ақпаратты өңдеу құралдарына қол жеткізу құқықтарын сақтау, жойылады.		
34	Кадр қызметімен МО, ЖАО қызметшілерін немесе ұйым жұмыскерлерін цифрландыру және киберқауіпсіздікті қамтамасыз ету саласында оқытуын ұйымдастыру және электрондық сертификат беріле отырып, жеке іс материалдарында сақталу есебін жүргізу талаптарын сақтау		
	Киберқауіпсіздік оқиғалары мониторингін және оқиғалар журналын		

35	талдау нәтижелері бойынша құпиялылығы, қолжетімділігі мен тұтастығы үшін өте қатерлі болып сәйкестендірілген киберқауіпсіздік оқиғаларын мемлекеттік техникалық қызметтің компьютерлік инциденттерге әрекет ету қызметінде тіркеу талаптарын сақтау		
36	Екінші деңгейдегі банктерді қоспағанда, заңмен қорғалатын құпияны қамтитын деректерді өңдейтін аса маңызды цифрлық объектілерінің иелеріне жылына кемінде бір рет киберқауіпсіздік аудитін жүргізу жөніндегі талаптарды сақтау.		
37	Сервистік бағдарламалық өнімді өнеркәсіптік пайдалану кезінде киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сынақтардың оң нәтижелері бар актінің болуы жөніндегі талаптарды сақтау.		
38	Әзірленетін немесе сатып алынатын дайын қолданбалы БҚ пайдаланушы интерфейсін пайдаланушының тіл интерфейсін таңдау мүмкіндігімен, деректерді қазақ, орыс және қажет болған жағдайда басқа тілдерде енгізуді, өңдеу мен шығаруды қамтамасыз ету талаптарын сақтау		
39	МО, ЖАО немесе ұйым: пайдаланушылар мен персоналдың іс-қимылы; ақпаратты өңдеу құралдарын қолдану		

	мониторингін жүзеге асырады.		
40	Өзірленетін немесе сатып алынатын дайын қолданбалы БҚ қазақ және орыс тілдерінде пайдалану жөніндегі техникалық құжаттамамен қамтамасыз ету талаптарын сақтау		
41	Ендірілген жүйелер серверінің жоғары қолжетімділігін қамтамасыз ету жөніндегі талаптарды сақтау: 1) резервтік желдеткіштерді, қуат көздерін, дискілерді және енгізу-шығару адаптерлерін қызу ауыстыру; 2) сыни оқиғалар туралы ескертулер; 3) сыни компоненттердің жай-күйін үздіксіз бақылауды қолдау және бақыланатын көрсеткіштерді өлшеу		
42	Құпия ЦЖ-да, құпия ЦР-да және қолжетімділігі шектелген дербес деректерді қамтитын ЦР-да пайдаланылатын ақпаратты тасығыштарды пайдаланудан шығарған кезде ақпаратты кепілдікті жоюдың бағдарламалық және аппараттық қамтылымы қолдану жөніндегі талапты сақтау		
43	Жергілікті желінің құжат жүзіндегі схемасы болуы және оны пайдаланған кезде өзектілендірілген күйде ұсталу талабының сақталуы		
	МО, ЖАО цифрлық объектілерін және аса маңызды цифрлық объектілерін қорғау үшін		

44	деректердің тарап кетуін болғызбау жүйелері (DLP) қолдану жөніндегі талаптарды сақтау. Бұл ретте: іс-қимылға жүргізілетін бақылау туралы пайдаланушыны визуалды түрде хабардар ету; жергілікті желі шегінде деректердің тарап кетуін болғызбау жүйесінің басқару орталығы мен серверлерін орналастыру қамтамасыз етіледі.		
45	МО-ның және ЖАО-ның ЦЖ-сын, оның ішінде МО-ның немесе ЖАО-ның тәжірибелік пайдалануға енгізілген ЦЖ-сы мен интеграциялау талаптарын сақтау.		
46	"цифрлық үкіметтің" операторы ұйымдастырған АҚКҚ пайдаланылатын мемлекеттік органдардың бірыңғай көліктік ортасының (бұдан әрі - МО БКО) сымсыз байланыс арналарын қоспағанда, МО БКО-ға, ЦС-нің жергілікті желісіне, сондай-ақ МО БКО, ЦС-нің жергілікті желісінің құрамына кіретін техникалық құралдарға сымсыз желілер арқылы қашықтан қол жеткізуді, сымсыз қолжетімділікті ұйымдастыруға арналған құралдарды, модемдерді, радиомодемдерді, ұялы байланыс операторларының желілік модемдерін, ұялы байланыстың абоненттік құрылғыларын және басқа да сымсыз желілік құрылғыларды қосуға		

	жол берілмеу бойынша талаптарды сақтау		
47	"Цифрлық үкіметтің" цифрлық объектісін өнеркәсіптік пайдалануға беруді оның меншік иесі немесе иеленушісі мемлекеттік техникалық қызмет берген "цифрлық үкіметтің" цифрлық объектілерінің бастапқы кодтарынан құрастырылған орындалатын кодтарды пайдалана отырып қана жүзеге асыру бойынша талаптарды сақтау.		
48	Цифрлық субъектінің ішкі шеңберінің ЖЖ Интернетке қосуға жол берілмеу бойынша талаптарды сақтау		
49	Интернет-ресурс иесі және (немесе) иеленушісі пайдаланушының кескін тілін таңдау мүмкіндігімен қазақ, орыс және қажет болған жағдайда басқа тілдерде көпшілікке қолжетімді интернет-ресурстар құруды қамтамасыз ету бойынша талаптарды сақтау		
50	Тәжірибелік пайдалану оң аяқталған, киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сынақтардың оң нәтижелері бар сынақ хаттамалары болған, цифрландыру және киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органдардың, мүдделі МО-ның, ЖАО-ның және ұйымдардың өкілдері қатысатын қабылдау комиссиясы ЦЖ-ны өнеркәсіптік пайдалануға беру туралы актіге қол қойған жағдайда МО-ның		

	, ЖАО-ның және ұйымдардың ЦЖ-ны өнеркәсіптік пайдалануға беру жөніндегі талаптарды сақтау		
--	---	--	--

Лауазымды адам (-дар) _____

лауазымы қолы

тегі, аты, әкесінің аты (бар болған жағдайда)

Бақылау субъектісінің басшысы _____

лауазымы қолы

тегі, аты, әкесінің аты (бар болған жағдайда)