"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы

Қазақстан Республикасының Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2019 жылғы 5 маусымда № 18795 болып тіркелді.

Ескерту. Тақырыбы жаңа редакцияда – ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 22.06.2026 № 345/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

"Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 7-1-бабының 5) тармақшасына және Қазақстан Республикасы Үкіметінің 2025 жылғы 9 қазандағы № 846 қаулысымен бекітілген Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі туралы ереженің 15-тармағының 52) тармақшасына сәйкес БҰЙЫРАМЫН:

Ескерту. Кіріспе жаңа редакцияда – ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 22.06.2026 № 345/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

1. Мыналар:

1) осы бұйрыққа 1-қосымшаға сәйкес "Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі";

2) осы бұйрыққа 2-қосымшаға сәйкес "Цифрлық үкіметтің" цифрлық объектілері мен аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары бекітілсін.

Ескерту. 1-тармақ жаңа редакцияда – ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 22.06.2026 № 345/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

2. "Сервистік бағдарламалық өнімнің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының мемлекеттік органның интернет-ресурсының және ақпараттық жүйенің олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы" Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 14 наурыздағы № 40/НҚ бұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16694 болып тіркелген, Қазақстан Республикасы

Нормативтік құқықтық актілерінің эталондық бақылау банкінде 2018 жылғы 12 сәуірде жарияланған) күші жойылды деп танылсын.

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

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

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

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

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

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

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

Қазақстан Республикасының
Цифрлық даму, қорғаныс және
аэроғарыш өнеркәсібі министрі *А. Жұмағалиев*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті
2019 жылғы "___" _____

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

"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі

Ескерту. Әдістеме жаңа редакцияда – ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 22.06.2026 № 345/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы "Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі (бұдан әрі – Әдістеме) "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 7-1 -бабының 5) тармақшасына және Қазақстан Республикасы Үкіметінің 2025 жылғы 9 қазандағы № 846 қаулысымен бекітілген Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі туралы ереженің 15-тармағының 52) тармақшасына сәйкес әзірленді.

2. Осы Әдістемеде мынадай ұғымдар және қысқартулар пайдаланылады:

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

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

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

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

5) қолданбалы бағдарламалық құрал – белгілі бір салалық мәселелер класын шешуге арналған бағдарламалық құралдар жиынтығы;

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

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

8) осалдық – ифрлық объектінің киберқауіпсіздікке қатер төндіретін кемшілігі;

9) өтініш беруші – сынақ объектісінің меншік иесі немесе иеленушісі, сондай-ақ сынақ объектісінің меншік иесі немесе иеленушісі өкілеттік берген цифрлық объектінің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізуге өтініш берген жеке немесе заңды тұлға;

10) сенімді арна – сынақ объектілерінің қауіпсіздік функциялары (бұдан әрі – ОҚФ) мен цифрлық технологиялардың қашықтан орналасқан сенімді өнімі арасындағы өзара әрекеттесу құралы, сынақ объектілерінің қауіпсіздік саясатын сақтауға қажетті деңгейде сенімділікті қамтамасыз етеді;

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

12) SYNAQ интернет-порталы – цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақ бойынша қызмет көрсету процесін автоматтандыруға арналған мемлекеттік техникалық қызметтің интернет-порталы;

13) сынақ объектісі – киберқауіпсіздік талаптарына сәйкестікке сынақтан өткізу жөніндегі жұмыстар жүргізілетін цифрлық объект;

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

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

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

17) штаттық пайдалану ортасы – цифрлық объектінің өндірістік пайдалану кезеңінде қолдануға арналған, тәжірибелік пайдалану (пилоттық жоба) кезеңінде қолданылатын серверлік жабдықтардың, желілік инфрақұрылымның, жүйелік бағдарламалық қамтамасының мақсатты жиынтығы.

3. Сынақтар жүргізу мыналарды қамтиды:

1) бастапқы кодтарды талдау;

2) киберқауіпсіздік функцияларын сынақ;

3) жүктемелік сынақ;

4) желілік инфрақұрылымды зерттеп-қарау;

5) киберқауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау.

2-тарау. Бастапқы кодтарды талдау

4. Сынақ объектілерінің бастапқы кодтарын талдау БҚ осалдықтарын анықтау мақсатында халықаралық осалдықтар жіктеуіштеріне (Common Weakness Enumeration, Open Web Application Security Project Top 10, Open Web Application Security Project Mobile Top 10, Open Web Application Security Project Application Programming Interface Top 10), осалдықтардың халықаралық деректер базаларына (Common Vulnerabilities and Exposures, National Institute of Standards and Technology) және Қазақстан Республикасының 15408-3 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету

әдістері және құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемшарттары. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар" стандартына сәйкес жүргізіледі.

"Цифрлық үкіметтің" цифрлық объектілерінің бастапқы кодтарын талдау ДМ және БҚ осалдықтарын анықтау мақсатында халықаралық осалдықтар жіктеуіштеріне (Common Weakness Enumeration, Open Web Application Security Project Top 10, Open Web Application Security Project Mobile Top 10, Open Web Application Security Project Application Programming Interface Top 10), осалдықтардың халықаралық деректер базаларына (Common Vulnerabilities and Exposures, National Institute of Standards and Technology) және Қазақстан Республикасының 15408-3 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері және құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемшарттары. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптары" стандартына сәйкес жүргізіледі.

5. Бастапқы кодтарды талдау "Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілеріне жатқызылған цифрлық жүйелердің олардың киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидаларына (бұдан әрі – Қағидалар) 2-қосымшаға сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнаманы 5-тармағы 11) тармақшасының және 12) тармақшасының кестелерінде аталған БҚ үшін жүргізіледі.

6. Бастапқы кодтарды сынақ мерзімі аяқталуына дейін қайта талдау қажеттігі анықталған жағдайда, өтініш беруші жеткізушіге сұраумен жүгінеді және Қағиданың 21-тармағына сәйкес бастапқы кодтарды қайта талдау жүргізу туралы қосымша келісім жасалады.

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

Сынақ объектілерінің БҚ осалдықтарды анықтау, "цифрлық үкімет" цифрлық объектілеріне жататын объектілер үшін бастапқы кодты қолмен талдау әдісімен және бастапқы кодты талдауға арналған бағдарламалық құралды пайдалану арқылы, өтініш беруші ұсынған бастапқы кодтар негізінде жүзеге асырылады.

"Цифрлық үкіметтің" цифрлық объектілерінің БҚ осалдықтарын анықтау бастапқы кодты талдаудың қолмен әдісімен және өтініш беруші ұсынған бастапқы кодтардың негізінде бастапқы кодты талдауға арналған бағдарламалық құралды пайдалана отырып жүргізіледі.

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

9. Бастапқы кодты талдау мыналарды қамтиды:

1) БҚ осалдықтарын анықтау;

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

3) бастапқы кодты талдау нәтижелерін бекіту.

10. БҚ осалдықтарын анықтау мынадай тәртіппен жүзеге асырылады:

1) бастапқы деректерді дайындау ("цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің бастапқы кодтарын жүктеу, сканерлеу режимін таңдау (динамикалық және/немесе статикалық), сканерлеу режимдерінің сипаттамаларын баптау) жүргізіледі;

2) бастапқы кодты талдаудың қолмен әдісі және бастапқы деректерді дайындау (" Цифрлық үкіметтің" цифрлық объектілерінің бастапқы кодтарын жүктеу), сканерлеу режимін таңдау (статикалық, тәуелділіктерді талдау және/немесе динамикалық), сканерлеу режимдерінің сипаттамаларын реттеу) жүргізіледі;

3) БҚ осалдықтарын анықтауға арналған БҚ іске қосылады;

4) жалған позитивтердің болуына бағдарламалық есептерге талдау жүргізіледі;

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

11. ДМ анықтау мынадай тәртіппен жүзеге асырылады:

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

2) сынақ объектісінің бастапқы кодын қолмен талдау жүргізу:

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

функционалдық объектілерді орындау бағытын зерделеу және өңдеу деректерін тексеру;

функционалдық объектілер деңгейінде бастапқы кодтардың толықтығын және артық болмауын бақылау;

есепте ДМ анықтау нәтижелерін кейіннен ұсыну үшін экран түсірімінің көмегімен ДМ-ны тіркеу.

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

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

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

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

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

Қосымшаларымен және есеппен берілетін бастапқы кодтарды талдаудың:

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

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

14. Бастапқы кодтарды талдау жүргізу аяқталғаннан кейін:

1) сынақ объектісінің ("цифрлық үкіметтің" цифрлық объектілерін қоспағанда) бастапқы кодтары таңбаланады және мөр басылған түрінде аккредиттелген сынақ зертханасының мұрағатына жауапты сақтауға тапсырылады.

2) сынақ объектісінің ("цифрлық үкіметтің" цифрлық объектісі) бастапқы кодтары бірегей сәйкестендіру нөмірін алады және SYNAQ интернет-порталында сақталады.

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

3-тарау. Киберқауіпсіздік функцияларын сынақ

16. Цифрлық объектілерінің функцияларын киберқауіпсіздік талаптарына сәйкестігіне бағалау (бұдан әрі – киберқауіпсіздік функцияларын сынақ) олардың нормативтік-техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында қолданыстағы киберқауіпсіздік бойынша стандарттардың талаптарына сәйкестігін бағалау мақсатында жүзеге асырылады.

17. Киберқауіпсіздік функцияларын сынақ мыналарды қамтиды:

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

2) "Цифрлық үкіметтің" цифрлық объектілеріне жататын сынақ объектілерін енуді қолмен тестілеу;

3) бағдарламалық қамтылымның жаңартуларға сканерлеуі және конфигурацияны талдау;

4) сынақ қорытындыларын бақылау нәтижелерін, сәйкестік немесе сәйкессіздік туралы бағалауды және анықталған сәйкессіздіктерді жою жөніндегі ұсынымдарды (қажет болған жағдайда) көрсете отырып, сынақ туралы есепте тіркеу.

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

19. Киберқауіпсіздік функцияларының сынағы іске асылу деңгейлері бойынша жүргізіледі:

операциялық жүйелердің виртуализация ортасы – гипервизорлар;

операциялық жүйелер;

деректерді басқару жүйелері (ДБЖ);

"Цифрлық үкіметтің" цифрлық объектілерінің құрамындағы қолданбалы бағдарламалық қамтамасыз ету және олардың жиынтығы, Қағиданың 2-қосымшаға қосылған сынақ нысанының сипаттамаларына арналған сауалнама-анкетаның 5-тармағының 1) және 4) тармақшаларында тізілген.

20. "Цифрлық үкіметтің" цифрлық объектілерінің енуіне қолмен тестілеуді қамтиды :

1) сынақ объектісінде осалдықтарды анықтау;

2) Анықталған осалдықтарды жою бойынша ұсынымдар қалыптастыру.

21. Киберқауіпсіздік функцияларын сынақ нәтижелерін қызмет берушінің осы жұмыс түрінің жауапты орындаушысы сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнаманың көшірмесін қоса бере отырып, киберқауіпсіздік функцияларын сынақ хаттамасында тіркейді (еркін нысанда).

Қосымшаларымен және есеппен берілетін киберқауіпсіздік функцияларын сынақтың:

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

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

4-тарау. Жүктемелік сынақ

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

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

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

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

25. Жүктемелік сынақ мынадай тәртіппен жүзеге асырылады:

1) сынаққа дайындық жүргізіледі;

2) сынақ жүргізіледі;

3) сынақ нәтижелері тіркеледі.

26. Сынаққа дайындық мыналарды қамтиды:

1) сынақ сценарийін анықтау;

2) сынақтың уақытша және сандық сипаттамаларын анықтау;

3) сынақ жүргізу уақытын тапсырыс берушімен келісу.

27. Сынақ жүргізу:

1) мамандандырылған бағдарламалық құралға сынақ сценарийі мен конфигурациясын баптауды;

2) мамандандырылған бағдарламалық құралды іске қосуды;

3) сынақ объектісіне жүктеуді тіркеуді;

4) сынақ объектісінің нақты өткізу қабілетін жоғарылату немесе төмендету жөнінде ұсынымдар көрсете отырып, жүктемелік сынақтың есебін қалыптастыруды және беруді қамтиды.

28. Жүктемелік тестілеу жүргізу жөніндегі жұмыстар Қағидаларға 2-қосымшаның сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнаманың 5-тармағының 9) тармақшасы мен 10) тармақшасының кестелерінде көрсетілген бір сынақ объектісіне пайдаланушыларды қосу нүктелерінің нұсқалары мен сынақ объектісінің интеграциялық өзара іс-қимылын іске қосу нүктелерінің нұсқалар саны бойынша жүргізіледі.

29. Жүктеме сынағының нәтижелері осы жұмыс түрін орындайтын қызмет берушінің жауапты орындаушысы сынақ объектілерінің сипаттамалары туралы сауалнаманың көшірмесі қоса бере отырып, жүктеме сынағының хаттамасында (еркін нысан) тіркеледі.

Қосымшаларымен және есеппен берілетін жүктемелік сынақтың:

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

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

5-тарау. Желілік инфрақұрылымды зерттеп-қарау

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

31. Желілік инфрақұрылымды зерттеу мыналарды қамтиды:

1) желілік инфрақұрылымды қорғау функцияларының нормативтік-техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілерінің және Қазақстан Республикасының аумағында қолданылатын киберқауіпсіздік бойынша стандарттардың талаптарына сәйкестігін бағалау;

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

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

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

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

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

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

Қосымшаларымен және есеппен берілетін желілік инфрақұрылымды зерттеп-қараудың:

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

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

6-тарау. Киберқауіпсіздікті қамтамасыз ету процестерін зерттеп-қарау

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

36. Киберқауіпсіздікті қамтамасыз ету процестерін зерттеу мыналарды қамтиды:

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

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

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

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

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

Қосымшаларымен және есебімен киберқауіпсіздікті қамтамасыз ету процестерін тексеру хаттамасы:

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

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

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

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды
цифрлық объектілердің
киберқауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу әдістемесіне
1-қосымша

Киберқауіпсіздік функцияларының тізбесі

р/с №	Функциялардың атауы	Функциялардың мазмұны
1	2	3
Аудит безопасности		
1	Қауіпсіздік аудитінің автоматты әрекет етуі	Киберқауіпсіздік оқиғаларын жинау және талдау құралдарымен киберқауіпсіздік мониторингін қамтамасыз ету. Тіркеу журналына жазба енгізуді, қауіпсіздікті бұзушылықты айқындау туралы әкімшіге локалдық немесе қашықтықтан сигнал беруді жүзеге асыру.

2	Қауіпсіздік аудитінің деректерін генерациялау	Хаттамалаудың, ең болмаса, тіркеу функцияларын іске қосу мен аяқтаудың, сондай-ақ аудиттің базалық деңгейіндегі барлық оқиғалардың болуы, яғни, әрбір тіркеу жазбасында оқиғаның мерзімі мен уақытының, оқиға түрінің, субъектіні сәйкестендіргіш пен оқиға нәтижесінің (сәттілігі немесе сәтсіздігі) болуы.
3	Қауіпсіздік аудитін талдау	Сәйкестендіру тетіктерін пайдаланудың ең болмаса, сәтсіз нәтижелерін, сондай-ақ криптографиялық операцияларды орындаудың сәтсіз нәтижелерін жинақтау және/немесе біріктіру арқылы (ықтимал кемшіліктерді айқындау мақсатында) жүзеге асыру.
4	Қауіпсіздік аудитін қарау	Барлық тіркеу ақпаратын қарау (оқу) мүмкіндігін қамтамасыз ету және әкімшіге беру. Өзге пайдаланушыларға тіркеу ақпаратына қолжетімділік айқын ерекше оқиғаларды қоспағанда, жабық болады.
5	Қауіпсіздік аудитінің оқиғаларын таңдау	Оқиғаларды тіркеудің, ең болмаса, мынадай атрибуттарға негізделетін іріктеудің болуы: объектіні сәйкестендіргіш; субъектіні сәйкестендіргіш; желі торабының мекенжайы; оқиға түрі ; оқиға мерзімі мен уақыты.
6	Қауіпсіздік аудитінің деректерін сақтау	Рұқсатсыз түрлендіруден сенімді қорғау туралы тіркеу ақпаратының болуы.
Криптографиялық қолдау		
7	Криптографиялық кілттерді басқару	Мыналарды қолдаудың болуы: 1) криптографиялық кілттерді құру; 2) криптографиялық кілттерді бөлу; 3) криптографиялық кілттерге қолжетімділікті басқару; 4) криптографиялық кілттерді жою.
		1. Нормативтік-техникалық құжаттаманың, Қазақстан Республикасының нормативтік құқықтық актілері мен Қазақстан Республикасы аумағында

8	Криптографиялық операциялар	қолданыстағы киберқауіпсіздік саласындағы стандарттардың талаптарына сәйкес сенімді арна арқылы жіберілетін барлық ақпарат үшін тұтастығын шифрлаудың және бақылаудың болуы. 2. Құпия деректерді, қолжетімділігі шектеулі дербес деректерді немесе таратылуы шектеулі қызметтік ақпаратты қамтитын сынақ объектілері (бұдан әрі – СО) үшін ақпаратты криптографиялық қорғау құралдарын қолдану.
Пайдаланушының деректерін қорғау		
9	Қолжетімділікті басқару саясаты	Қауіпсіздік сервисімен тікелей немесе жанама операцияларды орындайтын пайдаланушылар үшін қолжетімділікті бөлуді жүзеге асыру.
10	Қолжетімділікті басқару функциялары	Қолжетімділікті бөлу функцияларын пайдалану, ең болмаса, мынадай қауіпсіздік атрибуттарына негізделуі тиіс: қол жеткізу субъектілерін сәйкестендіргіштер; қол жеткізу объектілерін сәйкестендіргіштер; қол жеткізу субъектілерінің мекенжайлары; қол жеткізу объектілерінің мекенжайлары; субъектілердің қол жеткізу құқықтары.
11	Деректерді аутентификациялау	Ақпараттың мазмұны айлакерлік жолымен ұқсастырылмағанын немесе түрлендірілмегенін кейін тексеру үшін пайдаланылатын өзіндік деректер жинағының дұрыстығы кепілдігін қолдау.
12	Деректерді СО қауіпсіздік функцияларының (бұдан әрі – ОҚФ) әрекетінен тыс экспорттау	Пайдаланушының деректерін СО экспорттау кезінде оларды қорғау мен сақталуын немесе қауіпсіздік атрибуттарын ескермеуді қамтамасыз ету.
13	Ақпараттық ағындарды басқару саясаты	Пайдаланушының деректерін қауіпсіздік сервисінің физикалық бөлінген бөліктері арасында жіберген кезде оларды ашуға, түрлендіруге және/немесе қолжетімді болуына жол бермеуді қамтамасыз ету.

14	Ақпараттық ағындарды басқару функциялары	Деректер қоймасында қамтылған ақпаратты бақылаусыз таратуға жол бермеу мақсатында оған қолжетімділікті ұйымдастыру және қамтамасыз ету (бағдарламалық қамтылым (бұдан әрі – БҚ) сенімсіз болған жағдайда жариялаудан немесе түрлендіруден сенімді қорғауды іске асыру үшін ақпараттық ағындарды басқару).
15	Деректерді ОҚФ әрекетінен тыс жерден импорттау	Пайдаланушының деректерін олардың талап етілетін қауіпсіздік және қорғау атрибуттары болатындай етіп СО жіберуге арналған тетіктердің болуы.
16	СО шегінде жіберу	Пайдаланушының деректерін ішкі арна бойынша СО түрлі бөліктері арасында жіберген кезде қорғаудың болуы.
17	Қалған ақпаратты қорғау	Қалған ақпаратты толық қорғауды қамтамасыз ету, яғни ресурс босаған кезде алдыңғы жай-күйінің қолжетімсіздігін қамтамасыз ету.
18	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.
19	Сақталатын деректердің тұтастығы	Пайдаланушының деректерін ОҚФ шегінде сақтаған кезде олардың қорғалуын қамтамасыз ету.
20	ОҚФ арасында жіберген кезде пайдаланушы деректерінің құпиялылығын қорғау	Пайдаланушының деректерін ОҚФ арасында сыртқы арна немесе АТ басқа сенімді өнімі бойынша жіберген кезде олардың құпиялылығын қамтамасыз ету. Құпиялылық деректерді екі соңғы нүкте арасында жіберген кезде оларға рұқсатсыз қол жеткізуді болдырмау жолымен жүзеге асырылады. Соңғы нүктелер ОҚФ немесе пайдаланушы бола алады.
		Пайдаланушының деректерін ОҚФ және АТ басқа сенімді өнімі

21	ОҚФ арасында жіберген кезде пайдаланушы деректерінің тұтастығын қорғау	арасында жіберген кезде олардың тұтастығы, сондай-ақ айқындалған қателер кезінде оларды қалпына келтіру мүмкіндігі қамтамасыз етілуі тиіс.
Сәйкестендіру және теңестіру		
22	Теңестіруден бас тарту	Сәтсіз теңестіру талаптарының белгілі санына келгенде әкімшінің субъектіге қол жеткізуге рұқсат бермеу, тіркеу журналына жазба енгізуді генерациялау мен әкімшіге қауіпсіздіктің ықтимал бұзушылық туралы сигнал беру мүмкіндігінің болуы.
23	Пайдаланушының атрибуттарын айқындау	Әрбір пайдаланушы үшін, ең болмаса, келесі қауіпсіздік атрибуттарын қолдау қажет: сәйкестендіргіш; авторизациялық мәліметтер (мысалы, құпия сөз); кіру құқықтары (рөл).
24	Құпиялардың ерекшелігі	1) Құпия сөздің мерзімі өткен жағдайда тіркелгішті автоматты түрде құлыптау мүмкіндігінің болуы; 2) Қолданушының құпия сөзін өзгерту процедурасының болуы; 3) Құпия сөз өзгертілген кезде оның минималды ұзындығы мен күрделілігіне шектеулер қойылуы тиіс. Жүйе компоненттері мен қызметтік тіркелгіштер қолданатын аутентификациялық ақпаратты және басқа да құпияларды сақтау үшін арнайы механизмдерді немесе құпияларды басқару құралдарын пайдаланып, олардың құпиялылығын және рұқсатсыз қол жеткізуден қорғалуын қамтамасыз ететін шаралар іске асырылуы тиіс.
25	Пайдаланушыны теңестіру	ОҚФ ұсынатын пайдаланушы теңестіру тетіктерінің болуы.
		1) Қауіпсіздік сервисі осы пайдаланушының атынан орындайтын кез келген іс-қимыл аяқталғанға дейін әрбір пайдаланушы сәтті сәйкестендірілуге және теңестіруді; 2) Басқа пайдаланушыдан көшіріп алынған немесе ұқсастырып

26	Пайдаланушыны сәйкестендіру	жасалған теңестірілген деректерді пайдалануға жол бермеу мүмкіндіктерін; 3) Пайдаланушының ұсынылған кез келген сәйкестендіргішін теңестіруді; 4) Әкімші белгілеген уақыт интервалы аяқталғаннан кейін пайдаланушыны қайтадан теңестіруді; 5) Теңестіруді орындаған кезде қауіпсіздік функциялары пайдаланушыға тек қана жасырын кері байланысқа рұқсат беруді қамтамасыз ету.
27	Пайдаланушы-субъект байланыстырушы	Пайдаланушының тиісті қауіпсіздік атрибуттарын осы пайдаланушы атынан әрекет ететін субъектілермен байланыстыру керек.
Қауіпсіздікті басқару		
28	ОҚФ жеке функцияларын басқару	Жұмыс істеу, ажырату, қосу, сәйкестендіру мен теңестіру режимдерін түрлендіру, қолжетімділік, хаттамалау және аудит құқығын басқару режимдерін анықтауға әкімшінің жеке құқығының болуы.
29	Қауіпсіздік атрибуттарын басқару	Қауіпсіздіктің түсіндірілетін мәндерін өзгертуге, сұрастыруға, атрибуттарын өзгертуге, жоюға, құруға әкімшінің жеке құқығының болуы. Бұл ретте қауіпсіздік атрибуттарына тек қана қауіпсіздік мәндер беруді қамтамасыз ету қажет.
30	ОҚФ деректерін басқару	Тіркелетін оқиғалардың түсіндірілетін мәндерін өзгертуге, сұрастыруға, өзгертуге, жоюға, тазалауға, түрлерін анықтауға, тіркеу журналдарының өлшемін, субъектілердің қол жеткізу құқықтарын, қол жеткізу субъектілерінің есептік жазбаларының, парольдерінің, криптографиялық кілттерінің жарамдылық мерзімдерін өзгертуге әкімшінің жеке құқығының болуы.
		Уақыттың кейбір сәттерінде қауіпсіздік атрибуттарын бұзуды жүзеге асырудың болуы.

31	Қауіпсіздік атрибуттарын жою	Пайдаланушылармен байланыстырылған қауіпсіздік атрибуттарын бұзу мүмкіндігі тек қана уәкілетті әкімшілерде болуы тиіс. Қауіпсіздік үшін маңызды өкілеттіктер дереу жойылуы тиіс.
32	Қауіпсіздік атрибутының қолданыс мерзімі	Қауіпсіздік атрибуттарының қолданыс мерзімін белгілеу мүмкіндігін қамтамасыз ету.
33	Қауіпсіздікті басқару рөлдері	1) Ең болмаса, мынадай рөлдерді қолдауды қамтамасыз ету: уәкілетті пайдаланушы, қашықтықтан пайдаланушы, әкімші; 2) Қашықтықтан пайдаланушы мен әкімші рөлдерін тек қана сұрау бойынша алуды қамтамасыз ету.
ОҚФ қорғау		
34	Іркіліс кезіндегі қауіпсіздік	Сервиспен аппараттық ақаулар кезінде (мысалы, электр қуатының іркілісінен орын алған) қауіпсіз жай-күйді сақтау.
35	ОҚФ экспортталатын деректерінің қолжетімділігі	Қызмет деректерді оған және қашықтан сенімді цифрлық технологиялар өнімі арасында берілу кезінде олардың қолжетімділігін тексеруді, сондай-ақ өзгерістер анықталған жағдайда ақпаратты қайта беруді және тіркеу журналының жазбасын жасауды қамтамасыз етеді.
36	ОҚФ экспортталатын деректерінің құпиялылығы	Сервис деректерді оның және қашықтан орналасқан сенімді цифрлық технологиялар өнімі арасында жіберілген кезде олардың құпиялылығын тексеруге мүмкіндік беруі, сондай-ақ ақпаратты қайта жіберуі және өзгерістер анықталған жағдайда тіркеу журналын жасауы тиіс.
37	ОҚФ экспортталатын деректерінің тұтастығы	Сервис деректерді оның және қашықтан орналасқан сенімді цифрлық технология өнімі арасында жіберген кезде сервис барлық деректердің тұтастығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер

		анықталса, тіркеу журналына жазба енгізуді генерациялауға мүмкіндік беру.
38	ОҚФ деректерін СО шегінде жіберу	Сервис деректерді оның және қашықтан орналасқан сенімді цифрлық технология өнімі арасында жіберген кезде сервис барлық деректердің қолжетімділігін, құпиялылығы мен тұтастығын тексеруге және ақпаратты қайтадан жіберуді орындауға, сондай-ақ түрлендірулер анықталса, тіркеу журналына жазба енгізуді генерациялауға мүмкіндік береді.
39	Сенімді қалыпқа келтіру	Ақаулар немесе қызмет көрсету тоқтатылғаннан кейін автоматты түрде қалпына келтіру мүмкін болмаса, сервис қауіпсіз жай-күйге қайтаруға мүмкіндік беретін авариялық қолдау режиміне ауысады. Аппараттық ақаулардан кейін автоматты рәсімдерді қолданумен қауіпсіз жай-күйге кері қайту қамтамасыз етіледі.
40	Екінші рет пайдалануды анықтау	Сервистің теңестірілген деректердің қайтадан пайдаланылуын айқындауын, қол жеткізуге жол бермеуге, тіркеу журналына жазба енгізуін және әкімшіге қауіпсіздіктің ықтимал бұзылуы туралы сигнал беруін қамтамасыз ету.
41	Өтініштер беру кезіндегі делдалдық	Сервистің қауіпсіздік саясатын жүзеге асыратын функциялар сервистің кез келген басқа функциясын орындауға рұқсат етілгенге дейін шақырылып, сәтті орындалуын қамтамасыз ету.
42	Доменді бөлу	Қауіпсіздік функциялары оларды сенімсіз субъектілердің араласуы мен бұрмалауынан қорғайтын меншікті орындауға арналған жеке доменді қолдап отыру.
43	Жай-күйлерді синхрондау хаттамасы	Серверлерде ұқсас функцияларды орындаған кезде жай-күйлерді синхрондауды қамтамасыз ету.
44	Уақыт белгілері	Қауіпсіздік функцияларының пайдалануына сенімді уақыт белгілерін ұсыну.

45	ОҚФ арасындағы деректердің келісілушілігі	Тіркелетін ақпаратты, сондай-ақ қолданылатын криптографиялық операциялар параметрлерін келісімді түсіндіруді қамтамасыз ету.
46	СО шегінде қайталау кезінде ОҚФ деректерінің келісілушілігі	СО түрлі бөліктерінде қайталаған кезде қауіпсіздік функциялары деректерінің үйлесмілігін қамтамасыз ету. Қайталанатын деректерді қамтитын бөліктер ажыратылғанда, үйлесімділік көрсетілген қауіпсіздік функцияларына кез келген сұрауларды өңдеу алдындағы қосылуды қалпына келтіргеннен кейін қамтамасыз етіледі.
47	Сценарийлерді (скриптерді) пайдалану	СО-да киберқауіпсіздікке қатысты оқиғаларға әкеп соқтыратын өзгерту құқықтары бар сценарийлердің (скрипттердің) болмауы.
Ресурстарды қолдану		
48	Істен шығуға қарсы тұрушылық	Ақаулар кезінде де сынақ объектісінің функционалдық мүмкіндіктерінің қолжетімділігін қамтамасыз ету. Осындай ақаулар үлгілері: қуат көзін ажырату, аппаратураның жұмыс істемей қалуы, БҚ іркілісі.
49	Ресурстарды бөлу	1. Басқа пайдаланушылардың немесе субъектілердің ресурстарды монополиялауы себепті қызмет көрсетуден рұқсатсыз бас тартуға жол бермеу үшін пайдаланушылардың және субъектілердің ресурстарды пайдалануын басқаруды қамтамасыз ету. 2. Цифрлық объектісі шеңберінде оның жұмыс істеуін қамтамасыз ететін бағдарламалық өнімдерді ғана пайдалану.
СО-ға қолжетімділік		
50	Таңдалатын атрибуттардың аясын шектеу	Қолжетімділік әдісі немесе орны және/немесе уақыты негізінде (мысалы, тәулік уақыты, апта күні) қол жеткізу жүзеге асырылып отырылған порттан пайдаланушы таңдай алатын қауіпсіздік атрибуттарымен қатар

		пайдаланушы байланыста болуы мүмкін субъектілердің атрибуттарын да шектеу.
51	Қатарлас сеанстарды шектеу	Бір пайдаланушыға ұсынылатын қатарлас сеанстардың барынша көп санын шектеу. Бұл шаманың ұйғарынды мәнін әкімші белгілейді.
52	Сеансты бұғаттау	Пайдаланушы әрекетсіздігі ұзақтығының әкімші белгілеген мәні аяқталғаннан кейін жұмыс сеансы мәжбүрлі аяқтау.
53	СО-ға қол жеткізуге рұқсат беру алдында алдын алу	Сәйкестендіруге және теңестіруге дейін әлеуетті пайдаланушылар үшін сынақ объектісінің пайдаланудың сипатына қатысты ескерту хабарламасын көрсету мүмкіндігін қамтамасыз ету.
54	СО-ға қолжетімділік тарихы	Сеансты сәтті ашқан кезде пайдаланушы үшін осы пайдаланушы атынан қолжетімділікті алудың сәтсіз әрекеттерінің тарихын алу мүмкіндігін қамтамасыз ету. Бұл тарих қол жеткізу мерзімін, уақытын, қолданыс тікелей қосылымнан басталатын IP-адрес, құралдарын және СО соңғы рет сәтті қолжетімділік портын, сондай-ақ сәйкестендірілген пайдаланушының соңғы сәтті қол жеткізуінен кейінгі СО сәтсіз қол жеткізу әрекеттерінің санын қамтуы мүмкін.
55	СО-мен сеансты ашу	Субъектіні сәйкестендіргішке, субъектінің паролiне, субъектінің қолжетімділік құқықтарына негізделе отырып, сервистің сеансты ашуға жол бермеуге қабілеттігін қамтамасыз ету.
Зиянды кодтан қорғау функциялары		
56	Вирустарға қарсы қорғау құралдарының болуы	Зиянды кодтан қорғану үшін серверлерден, қажеттілік туындаған жағдайда сынақ объектісінің жұмыс станцияларынан зиянды кодты анықтау және бұғаттау немесе жою, мониторинг құралдарын қолдану.
		Серверлерге және жұмыс станцияларына вирустарға қарсы қорғау құралдарының

57	Вирустарға қарсы қорғау құралдарына арналған лицензия	лицензиялары (сатып алынған, шектелген, еркін таратылатын) болуы тиіс.
58	Вирустарға қарсы қорғау сигнатуралары базасын және бағдарламалық қамтылымды жаңарту	Вирустарға қарсы қорғау құралдарының ұдайы жаңартылып, өзекті күйде болуын қамтамасыз ету.
59	Вирустарға қарсы қорғау құралдарына қолжетімділікті басқару	Вирустарға қарсы қорғау құралдарын орталықтандырылған басқару мен конфигурациялауды жүзеге асыру.
60	Сыртқы электрондық тасығыштардағы ақпаратты зиянды кодтан вирустарға қарсы құралдарымен қорғауды басқару	Сыртқы электрондық тасығыштардағы ақпаратты зиянды кодтан қорғау файлдардың, қажет болса ақпарат тасығыштардың тексерісін және бұғатталуын қамтамасыз ету.
БҚ жаңартылуы кезіндегі қауіпсіздік		
61	БҚ-ның ұдайы жаңартылуы	Серверлер мен жұмыс станцияларының жалпыжүйелік және қолданбалы БҚ ұдайы жаңартылуын қамтамасыз ету.
62	Интернеттегі жаңарту серверлеріне рұқсатсыз желілік ортадағы БҚ жаңартылуы	Интернеттегі жаңарту серверлеріне рұқсатсыз желілік ортадағы БҚ мамандандырылған арнайы жаңарту серверінен жаңартылуын қамтамасыз ету.
Қолданбалы БҚ-ға өзгеріс енгізу кезіндегі қауіпсіздік		
63	Қолданбалы БҚ әзірлеу және тестілеу ортасы	Қолданбалы БҚ-ны өнеркәсіптік пайдалану ортасынан оқшауландырылған қолданбалы БҚ әзірлеу және тестілеу үшін ортаның болуын қамтамасыз ету.
64	Қолданбалы БҚ әзірлеу және тестілеу ортасына қол жеткізудің аражігін ажырату	Бағдарламашылар мен әкімшілер үшін қолданбалы БҚ әзірлеу және тестілеу орталарына қол жеткізуді басқаруын қамтамасыз ету.
65	Қолданбалы БҚ өрістету жүйесі	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ өрістету (тарату) жүйесінің болуы.
66	Қолданбалы БҚ өрістету жүйесіне қол жеткізудің аражігін ажырату	Өнеркәсіптік пайдалану ортасындағы серверлер мен жұмыс станцияларындағы қолданбалы БҚ ажырату (тарату) жүйесіне қол жеткізуді басқаруды қамтамасыз ету.
Мемлекеттік органдардың цифрлық объектілерде, жергілікті атқарушы органдарда және аса маңызды цифрлық объектілерінде "құпия ақпараттың таралып кетуінен қорғау"		

67	Қол жеткізуді басқару саясаты	Құпия ақпараттың таралып кетуінен қорғау жүйесін басқару
68	Жүйе компоненттерін жаңарту	Ақпараттың таралып кетуінен қорғау жүйесін үнемі жаңартып отыруды және жаңартып отыруды қамтамасыз ету.
69	Бөлім қауіпсіздігі атрибуты	Қазақстан Республикасы " Киберқауіпсіздік туралы" Заңына 6-бабы 3) тармақшасына сәйкес Қазақстан Республикасы Үкіметі бекіткен, Цифрландыру және киберқауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға сәйкес (әрі қарай – БТ) құпия сөз саясатының қолданылуын қамтамасыз ету.
70	Деректерді сақтау	Құпия ақпараттың таралып кетуінен қорғау жүйесінің оқиғалар журналдарын кемінде үш жыл және жедел қолжетімділікте кемінде екі ай сақтау.

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды
цифрлық объектілердің
киберқауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу әдістемесіне
2-қосымша

Қолмен тестілеу функцияларының тізбесі

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

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

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

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды
цифрлық объектілердің
киберқауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу әдістемесіне
3-қосымша

Желілік инфрақұрылымды қорғау функцияларының тізбесі

№ п/п	Функциялардың атауы	Функциялардың мазмұны
1	2	3
1	Сәйкестендіру және аутентификация	1. Пайдаланушының жүзеге асырылған әрекеттермен байланысын орнату үшін есептік жазбалардың бірегей сәйкестендіргіштерін пайдалану. 2. Артықшылықты қол жеткізу құқықтары оларды пайдалану қажеттілігі негізінде есептік жазбаларға арналады. 3. Сәтсіз және сәтті аутентификация әрекеттерін тіркеу. 4. Сеанс уақытын шектеу.

		5. Аутентификациядан бас тарту (аутентификацияның сәтсіз әрекеттерінің белгілі бір санына қол жеткізу кезінде субъектіге кіруден бас тарту мүмкіндігінің болуы). 6. Күшті құпия сөздерді пайдалану және таңдау. 7. Парольді тұрақты ауыстыруды жүргізу, сондай-ақ – қажетіне қарай.
2	Аудиттерді белгілеу (желілік қосылулардың қауіпсіздігіне байланысты оқиғалар туралы есептер қалыптастыру және олардың бар болуы)	1. Киберқауіпсіздік жағдайына байланысты оқиғаларды тіркеу, бұл ретте оқиғалар журналдары мыналарды қамтиды: пайдаланушылардың идентификаторлары; жүйелік әрекеттер; кіру және шығу сияқты негізгі оқиғалардың күні, уақыты және мәліметтері; сәтті және қабылданбаған қол жеткізу әрекеттері туралы есептер ; жүйе конфигурациясының өзгерістері; артықшылықтарды пайдалану; желілік мекенжайлар мен хаттамалар. 2. Киберқауіпсіздікті бұзумен байланысты оқиғаларға мониторинг жүргізу және мониторинг нәтижелерін талдау. 3. Оқиғаларды тіркеу журналдарын киберқауіпсіздік жөніндегі нормативтік-техникалық құжаттамада көрсетілген мерзім бойы, бірақ үш жылдан кем емес мерзімге сақтау және олардың екі айдан кем емес мерзімге оперативтік сақтауда болуы. 4. Оқиғаларды тіркеу журналдарын қол сұғу және рұқсатсыз қол жеткізуден қорғауды қамтамасыз ету, соның ішінде: жүйелік әкімшілерде журналдарды өзгерту, жою және өшіру құқықтары болмауы тиіс; құпия цифрлық объектілер үшін журналдардың қосымша

		сақтағышын құру және жүргізу қажет. 5. Киберқауіпсіздік оқиғаларының сыни түрлері туралы хабарландырудың болуы. 6. Оқиға тіркелгісінің журналдарындағы уақыттың әмбебап координацияланған уақыт UTC (kz) ұлттық шкаласын қайта жасайтын уақыт және жиілік стандартымен синхронизациялануын қамтамасыз ету.
3	Басып кіруді анықтау	1. Басып кірулерді (желілік инфрақұрылымға ықтимал басып кірулерді) болжауға, оларды нақты уақыт ауқымында анықтауға және тиісті дабылды көтеруге мүмкіндік беретін қаражаттың болуын қамтамасыз ету. 2. Қағидалар базасын автоматтандырылған жаңарту мүмкіндігі.
4	Желілік қауіпсіздікті басқару	1. Жергілікті желінің кабельдік жүйесінің пайдаланылмаған интерфейстері белсенді жабдықтан физикалық түрде ажыратылады. 2. Мемлекеттік органдар мен жергілікті атқарушы органдардың ішкі контурының жергілікті желісін Интернетке қосуды болдырмау, сондай-ақ ішкі контурдың жергілікті желісін және мемлекеттік органдар мен жергілікті атқарушы органдардың сыртқы контурының жергілікті желісін өзара ұштастыруды болдырмау. 3. Мемлекеттік органдар мен жергілікті атқарушы органдардың цифрлық объектілерінің желілері арқылы берілетін деректердің құпиялылығы мен сақтығын қорғау цифрлық объектінің иесінің ішкі локальдық желісінен жүзеге асырылады. 4. Жергілікті желіні логикалық және/немесе физикалық сегменттеу құралдарын қолдану. 5. Цифрлық объектінің компоненттері арасындағы,

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

10	Сенімді бағдар	ашудан қорғауды қамтамасыз ететін маршрутты ұсыну. Пайдаланушының сенімді маршрут арқылы байланыс орнатуға мүмкіндік беруін қамтамасыз ету. Қашықтағы пайдаланушының бастапқы аутентификациясы және қашықтан басқару үшін сенімді маршрутты пайдалану міндетті болып табылады.

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды
цифрлық объектілердің
киберқауіпсіздік талаптарына
сәйкестігіне сынақтар
жүргізу әдістемесіне
4-қосымша

Киберқауіпсіздікті қамтамасыз ету процестерінің тізбесі мен олардың мазмұны

№ п/п	Процестердің атауы	АҚ қамтамасыз ету процестерінің мазмұнына қойылатын талап
1	2	3
1	Цифрлық технологиялармен байланысты активтерді басқару	1. БТ-ға сәйкес активтерді идентификациялау. 2. БТ сәйкес ақпаратты жіктеу. 3. Тестілеу объектісі үшін анықталған сыныптың цифрлық объектілерді жіктеу қағидаларының талаптарына сәйкестігін тексеру. 4. БТ-ға сәйкес активтерді таңбалау. 5. Сәйкестендірілген активтерге жауапты тұлғаларды бекіту. 6. Қабылданған тізілім нысанына сәйкес активтер тізілімін жүргізу және өзектендіру. 7. БТ-ға сәйкес активтермен жұмыс істеу рәсімдерін айқындау, құжаттау және іске асыру (беру, пайдалану, сақтау, енгізу/шығару және қайтару). 8. Есептеу техникасы, телекоммуникациялық жабдық және бағдарламалық қамтамасыз ету құралдарын паспорттау. 9. Цифрлық технологиялармен байланысты активтерді қабылдау / жөнелту кезінде жұмыстарды қауіпсіз ұйымдастыру.

		10. Серверлік және телекоммуникациялық жабдықтарды, деректерді сақтау жүйелерін, жұмыс станцияларын, ақпарат тасығыштарды қауіпсіз кәдеге жарату (қайта пайдалану).
2	Киберқауіпсіздікті ұйымдастыру	1. Киберқауіпсіздік бөлімшесінің немесе киберқауіпсіздікке жауапты, цифрлық технологиялар бөлімшесінен оқшауланған, тікелей жоғары басшылыққа бағынатын қызметкердің болуы. 2. Жұмыс топтарының жұмыс істеуі және жұмыстарды үйлестіру және киберқауіпсіздікті қамтамасыз ету мәселелері бойынша кеңестер өткізу. 3. Киберқауіпсіздік жөніндегі нормативтік-техникалық құжаттаманы әзірлеу (өзектендіру), бекіту, басшылықтың мақұлдауы, олардың мазмұнын қызметкерлер мен орындаушылар тарапынан тартылатын қызметкерлерге жеткізу. 4. Киберқауіпсіздік мамандарының өкілетті органдарымен, кәсіби қауымдастықтарымен, кәсіби қауымдастықтарымен немесе форумдарымен байланыста болу. 5. Киберқауіпсіздікті қамтамасыз ету рәсімдерін, оның ішінде бөгде ұйымдарды тарту кезінде айқындау және құжаттау. 6. Ақпаратты қорғау қажеттіліктерін көрсететін құпиялылық немесе жарияламау туралы келісімді әзірлеу (қайта қарау). 7. Киберқауіпсіздік және қызмет көрсету деңгейі жөніндегі талаптарды айқындау және үшінші тарап ұйымдарымен келісімдерге енгізу. Келісім ережелерінің іске асырылуын бақылау.
		1. Жұмысқа қабылдау кезінде кандидаттарды алдын ала тексеру. 2. Қызметкерлердің лауазымдық нұсқаулықтарында және (немесе) еңбек шартының талаптарында және орындаушылар тарапынан

		тартылатын жұмыспен қамту, еңбек қатынастарын өзгерту немесе тоқтату кезеңіндегі киберқауіпсіздікке байланысты рөлдерді, міндеттер мен жауапкершіліктерді және сынақ объектісі иесінің міндеттемелерін айқындау, тағайындау және көрсету. 3. Киберқауіпсіздікті қамтамасыз ету саласында міндеттемелері бар қызметкерлерді жұмыстан шығару рәсімдерін айқындау және құжаттау. 4. Киберқауіпсіздік ережелерін бұзушыларға жасалатын іс-қимылдарды айқындау және регламенттеу. 5. Қызметкерлерге олардың қызметтік міндеттерін орындауды қозғайтын киберқауіпсіздікті қамтамасыз ету саясаттарындағы, қағидаларындағы және рәсімдеріндегі өзгерістер туралы хабарлау. 6. Қызметкерлердің және тараптан тартылатын орындаушылардың жұмыспен қамту, еңбек қатынастарын өзгерту немесе тоқтату кезеңінде киберқауіпсіздікті қамтамасыз етуге байланысты міндеттер мен жауапкершіліктер туралы хабардар болуы және орындауы. 7. Киберқауіпсіздік саласындағы қызметкерлерді оқыту және даярлау. 8. Қызметкерлердің және орындаушылар тарапынан тартылатын киберқауіпсіздікке қатысты міндеттемелерді орындау мүмкіндігін қамтамасыз ету үшін басшылықтың жауапкершілігі.
3	Қызметкерлермен байланысты қауіпсіздік	
		1. Пайдаланушы, оператор, әкімші және операциялық жүйелердің оқиғаларын, дерекқорды басқару жүйелерін, антивирустық бағдарламаларды, қолданбалы бағдарламаларды, телекоммуникациялық жабдықтарды, шабуылдарды

		анықтау және алдын алу жүйелерін, мазмұнды басқару жүйелерін тіркеу.
4	КҚ оқиғаларының мониторингі және КҚ инциденттерін басқару	2. Оқиғаларды тіркеу журналдарын жүргізу, сақтау және қорғау. 3. Оқиғаларды тіркеу журналдарын талдауды жүзеге асыру. 4. Тіркелген оқиғаларды бақылау және киберқауіпсіздік үшін маңыздылығы жоғары және маңызды оқиғалар туралы ескерту . 5. Киберқауіпсіздік оқиғасын бағалау және шешім қабылдау. 6. Қызметкерлерді және тараптан тартылатын орындаушыларды әзірлеу, құжаттау, олардың назарына жеткізу, киберқауіпсіздік инциденттеріне ден қою рәсімдерін орындау. 7. Киберқауіпсіздік инциденттеріне талдау жүргізу.
5	КҚ үздіксіздігін басқару	1. Киберқауіпсіздіктің үздіксіздігін жоспарлау. 2. Киберқауіпсіздікті немесе бизнес-процестерді қамтамасыз ету процесінің үздіксіздігінің бұзылуының ықтимал себебі болып табылатын оқиғаларды идентификациялау. 3. Штаттан тыс (дағдарыстық) жағдайларда киберқауіпсіздіктің үздіксіздігінің қажетті деңгейін ұстап тұру процестері мен рәсімдерін әзірлеу (өзектендіру), енгізу. 4. Қызметкерлерді және орындаушылар тарапынан тартылатын қызметкерлерді анықтау, құжаттау, олардың назарына жеткізу, штаттан тыс (дағдарыстық жағдайларда) рәсімдерді орындау. 5. Киберқауіпсіздіктің үздіксіздігін қамтамасыз ету процестері мен рәсімдерін тексеру (тестілеу), талдау және бағалау. 6. Заңнаманың талаптарын ескере отырып, ақпаратты өңдеу құралдарын, цифрлық объектіні резервтеу.

		1. Қызметкерлерді және орындаушылар тарапынан тартылатын қызметкерлерді анықтау, құжаттау және олардың назарына жеткізу, желілік жабдықты басқару рәсімдерін орындау. 2. Желілерге қызмет көрсету және ақпарат беру жөніндегі келісімдерге қауіпсіздікті қамтамасыз ету тетіктерін, барлық желілік қызметтер мен сервистер үшін қолжетімділік деңгейлерін айқындау және енгізу.
6	Желілік қауіпсіздікті басқару	3. Қызметкерлерді және орындаушылар тарапынан тартылатын қызметкерлерді анықтау, құжаттау, олардың назарына жеткізу, желілер мен Желілік қызметтерді пайдалану, ақпарат беру, Интернетке, телекоммуникация және байланыс желілеріне қосылу және желілік ресурстарға сымсыз қол жеткізуді пайдалану саясаттары мен рәсімдерін орындау. 4. Желі және электрондық хабарламалар арқылы берілетін ақпаратты қорғау құралдарын қолдану жөніндегі рәсімдерді айқындау, құжаттау және орындау . 5. Заңнама талаптарын ескеретін желілерді қосу және өзара іс-қимыл жасау тәсілдері.
7	Криптографиялық қорғау әдістері	1. Заңнаманың талаптарын ескеретін криптографиялық кілттерді дайындау, есепке алу, сақтау, беру, пайдалану, қайтару (жою), қорғау мәселелерін қамтитын криптографиялық кілттерді басқаруды регламенттеу. 2. Аутентификациялық деректерді қоса алғанда, ақпаратты сақтау және беру кезінде криптографиялық құралдарды қолдану.
		1. Тәуекелдерді бағалау әдістемесін таңдау; 2. Сәйкестендірілген және жіктелген активтер үшін қатерлерді (тәуекелдерді) сәйкестендіру және

8	Киберқауіпсіздік тәуекелдерін басқару	киберқауіпсіздік қатерлерінің (тәуекелдерінің) каталогын қалыптастыру (өзектендіру). Киберқауіпсіздікті қамтамасыз ету процестерімен байланысты қатерлерді (тәуекелдерді), тәуекелдерді каталогта көрсету. 3. Анықталған тәуекелдерді бағалау (қайта бағалау). 4. Тәуекелдерді өңдеу, тәуекелдерді өңдеу жоспарын қалыптастыру және бекіту (өзектендіру). 5. Тәуекелдерді бақылау және қайта қарау.
9	Қол жеткізуді басқару	1. БТ-ға сәйкес ақпаратқа, қолданбалы жүйелердің функцияларына, қызметтерге, жүйелік бағдарламалық қамтамасыз етуге, желілерге және желілік қызметтерге қол жеткізу құқықтарын шектеу ережелерін әзірлеу (өзектендіру), құжаттау, пайдаланушыларды таныстыру. 2. Пайдаланушыларды сәйкестендіру, аутентификациялау және авторизациялаудың қолданылатын әдістері мен рәсімдері. 3. БТ-ға сәйкес қол жеткізу құқықтарын шектеу ережелерін жүзеге асыру. 4. Пайдаланушыларды тіркеу және тіркеуден шығару (бұғаттау) рәсімдері. 5. Артықшылықты кіру құқығымен есептік жазбаларды басқару. 6. Пайдаланушының аутентификация процедураларында криптографиялық әдістерді қолдану және басқару. 7. Қол жеткізу құқықтарының өзгеруін басқару. 8. Құпия сөздерді басқару. 9. Артықшылықты утилиталарды пайдалану. 10. Сынақ объектісінің бастапқы кодына қол жеткізуді басқару.
		1. Заңнама талаптарын ескере отырып, серверлік, телекоммуникациялық

		жабдықтарды, деректерді сақтау жүйелерін орналастыру. 2. Цифрлық технологиялармен байланысты активтер орналастырылған үй-жайлардың қауіпсіздік периметрін физикалық қорғау. 3. Заңнаманың талаптарын ескеретін негізгі және резервтік серверлік үй-жайларды ұйымдастыру. 4. Негізгі және резервтік серверлік үй-жайларды заңнаманың талаптарын ескеретін қамтамасыз ету жүйелерімен жарақтандыру. 5. Серверлік үй-жайларға бақыланатын қол жеткізуді ұйымдастыру. 6. Серверлік үй-жайда жұмыстарды ұйымдастыру. 7. Серверлік және телекоммуникациялық жабдықтарды, деректерді сақтау жүйелерін және қамтамасыз ету жүйелерін техникалық сүйемелдеу және оларға қызмет көрсету жөніндегі жұмыстарды ұйымдастыру. 8. Жабдықты электрмен жабдықтау жүйесіндегі ақаулардан және коммуналдық қызметтердің жұмысындағы ақаулардан туындаған басқа да бұзылулардан қорғау тәсілдері. 9. Кабельдік жүйенің қауіпсіздігін қамтамасыз ету. 10. Кросс үй-жайларының қауіпсіздігін қамтамасыз ету.
10	Физикалық қауіпсіздік және табиғи қауіптерден қорғау	
		1. Киберқауіпсіздікті қамтамасыз етудің пайдалану рәсімдерін регламенттейтін нұсқаулықтарды әзірлеу (өзектендіру), құжаттау, пайдаланушыларды таныстыру. 2. Киберқауіпсіздікті қамтамасыз ету құралдары мен жүйелерін қолдану. 3. Ақпараттың сақтық көшірмесін жасау процедуралары және көшіру нәтижелерін тексеру. Сақтық көшірмелерді сақтау орындарының қауіпсіздігі.

11	АҚ қамтамасыз етудің пайдалану рәсімдері	4. Оқиғаларды тіркеу журналдарының уақытын бір уақыт көзімен синхрондау. 5. Қолданыстағы жүйелерде қолданбалы және жүйелік бағдарламалық қамтылымның жаңа нұсқаларын орнату кезіндегі өзгерістерді басқару процедуралары. 6. Осалдықтарды бақылау және басқару. 7. БТ-ға сәйкес ережелерді жүзеге асыру және қызметкерлерді таныстыру. 8. Қашықтан жұмысты ұйымдастыру жөніндегі нұсқаулықтың ережелерін әзірлеу (өзектендіру), қызметкерлерді таныстыру, іске асыру. 9. Сынақ объектісінің жұмыс қабілеттілігінің мониторингі. 10. Әзірлеу, тестілеу және пайдалану орталарын бөлу. 11. Электрондық пошта хабарламалары мен ақпараттарды Интернет арқылы беру кезінде құпиялылықты қамтамасыз ету. 12. Заңнаманың талаптарына сәйкес интернетті ұсыну және сыртқы электрондық пошта жүйелерімен өзара іс-қимыл жасау тәсілдері. 13. Интернет ресурстарына қол жеткізу кезіндегі шектеулер мен сүзу тәртібі.
12	Заңнамалық және шарттық талаптарға сәйкестігі	1. Сынақ объектісі үшін заңнамалық, нормативтік, өзге де міндетті, шарттық талаптарды айқындау (өзектендіру), құжаттау. 2. Зияткерлік меншік құқықтарына байланысты заңнамалық, нормативтік және шарттық талаптарға сәйкестікті іске асыратын рәсімдерді енгізу. 3. Заңнаманың нормаларына сәйкес келетін құпия және дербес деректерді қорғау саясатын әзірлеу және іске асыру. 4. Қолданылатын криптографиялық әдістер мен құралдардың заңнама талаптарына және келісімдерге (шарттарға) сәйкестігі.

		5. Киберқауіпсіздік аудитін жүргізу. 6. Киберқауіпсіздік жөніндегі заңнаманың, стандарттардың және техникалық құжаттаманың талаптарына сәйкестігі тұрғысынан сынақ объектісіне талдау жүргізу. 7. Жазбаларды жоғалтудан, бүлінуден, бұрмалануда, рұқсатсыз кіруден және заңнамалық, нормативтік, шарттық талаптарға сәйкес рұқсатсыз шығарудан қорғау.
13	Жүйелерді сатып алу, әзірлеу және қызмет көрсету	1. Киберқауіпсіздікке байланысты және қолданыстағы заңнамаға және стандарттарға сәйкес келетін талаптарды сынақ объектісіне нормативтік-техникалық құжаттаманың құрамына енгізу (өзектендіру). 2. Пайдаланылатын жүйелер үшін БҚ (жүйелік және қолданбалы) өзгерістерін басқарудың қауіпсіз рәсімдерін айқындау және қолдану. 3. Сынақ объектісі бойынша, оның ішінде бөгде ұйым жүзеге асыратын әзірлеу процесін бақылау. 4. Бөгде ұйым жүзеге асыратын жүйені техникалық сүйемелдеу процесін бақылау. 5. Жүйенің қауіпсіздік мүмкіндіктерін тексеру.

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

"Цифрлық үкіметтің" цифрлық объектілері және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары

Ескерту. Қағидалар жаңа редакцияда – ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 22.06.2026 № 345/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы "Цифрлық үкіметтің" цифрлық объектілері мен аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидалары (бұдан әрі – Қағидалар) "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 5) тармақшасына, Қазақстан Республикасы Үкіметінің 2025 жылғы 9 қазандағы № 846 қаулысымен бекітілген Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі туралы ереженің 15-тармағының 52) тармақшасына сәйкес әзірленді және "цифрлық үкіметтің" цифрлық объектілері мен аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар мен қысқартулар пайдаланылады:

1) бағдарламалық қамтылым – белгілі бір функциялардың орындалуын, цифрлық деректерді өңдеуді, сақтауды, қайта көшіруді және (немесе) беруді қамтамасыз ететін алгоритмдерді іске асыратын, пайдалану үшін дайындалған кодтардың жиынтығы болып табылатын цифрлық объект;

2) бастапқы код – бағдарламалық құралды жасау, өзгерту және қолдау үшін бағдарламалау тілінде жазылған бағдарлама мәтіндері;

3) киберқауіпсіздік – цифрлық объектілердің құпиялылығын, тұтастығын немесе қолжетімділігін бұзудан қорғалу жай-күйі;

4) киберқауіпсіздік жөніндегі нормативтік-техникалық құжаттама – цифрлық объектілердің және (немесе) ұйымның киберқауіпсіздікті қамтамасыз ету процестеріне қатысты саясатты, қағидаларды, қорғау шараларын белгілейтін құжаттама;

5) киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның интернет-порталы – цифрлық объектілердің киберқауіпсіздік жағдайының мониторингін жүргізуге арналған интернет-портал;

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

7) мемлекеттік техникалық қызмет – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған мемлекеттік заңды тұлға;

8) өтініш беруші – сынақ объектісінің меншік иесі немесе иеленушісі, сондай-ақ сынақ объектісінің меншік иесі немесе иеленушісі өкілеттік берген цифрлық объектінің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізуге өтініш берген жеке немесе заңды тұлға;

9) сынақ зертханасы – киберқауіпсіздік талаптарына сәйкестігін сынаққа уәкілеттік берілген және техникалық регламент туралы заңнамаға сәйкес аккредиттелген заңды тұлға немесе оның атынан әрекет ететін заңды тұлғаның құрамындағы бөлімше;

10) SYNAQ интернет-порталы – цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақ бойынша қызмет көрсету процесін автоматтандыруға арналған мемлекеттік техникалық қызметтің интернет-порталы;

11) сынақ объектісі – киберқауіпсіздік талаптарына сәйкестікке сынақтан өткізу жөніндегі жұмыстар жүргізілетін цифрлық объект;

12) цифрлық жүйе – цифрлық деректерді құруды, жинауды, өңдеуді, сақтауды және таратуды қамтамасыз ету мақсатында цифрлық инфрақұрылым объектілерін пайдаланатын, сондай-ақ цифрлық орта субъектілерінің өзара іс-қимылын автоматтандыратын және (немесе) цифрлық ортада қызметтер көрсетуді қамтамасыз ететін функционалдық байланысты цифрлық ресурстар кешені;

13) цифрлық жүйенің кіші жүйесі – цифрлық жүйенің белгілі бір функцияларын іске асыратын, цифрлық жүйенің мақсатына жетуі үшін қажетті жиынтық бөлігі (компоненті немесе модулі);

14) "Цифрлық үкімет" платформасы – оператордың платформалық бағдарламалық өнімдерді әзірлеуге, дамытуға, орналастыруға, интеграциялауға және (немесе) цифрлық объектілерді орналастыруға арналған цифрлық платформасы;

15) "Цифрлық үкімет" платформасының бағдарламалық өнімі (әрі қарай – платформалық бағдарламалық өнім) – "Цифрлық үкімет" платформасында әзірленген және орналастырылған бағдарламалық қамтама;

16) штаттық пайдалану ортасы – цифрлық объектінің өндірістік пайдалану кезеңінде қолдануға арналған, тәжірибелік пайдалану (пилоттық жоба) кезеңінде қолданылатын серверлік жабдықтардың, желілік инфрақұрылымның, жүйелік бағдарламалық қамтамасының мақсатты жиынтығы.

2-тарау. "Цифрлық үкіметтің" цифрлық объектілері және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігі бойынша сынақ тәртібі

3. Киберқауіпсіздік талаптарына сәйкестік бойынша объектілерді сынақтан (бұдан әрі – сынақтар) өткізу сынақталатын объектілердің нормативтік-техникалық құжаттамаға, Қазақстан Республикасының нормативтік құқықтық актілеріне және Қазақстан Республикасы аумағында қолданылатын киберқауіпсіздік стандарттарына сәйкестігін бағалау жұмыстарын қамтиды және сынақталатын объектінің штаттық пайдалану ортасында жүргізіледі.

4. "Цифрлық үкіметтің" цифрлық платформасында және "Цифрлық үкіметтің" цифрлық платформасында құрылған және (немесе) орналастырылған бағдарламалық қамтылымды (бағдарламалық өнімді) қоспағанда, сынақ объектісінің сынақтарының құрамына мынадай жұмыс түрлері кіреді:

1) бастапқы кодтарды талдау;

2) киберқауіпсіздік функцияларын сынақ;

3) жүктеме сынағы;

4) желілік инфрақұрылымды зерттеу;

5) КҚ қамтамасыз ету процестерін тексеру.

5. Сынақ объектісінің бастапқы коды болмаған немесе сынақтардың басқа түрін (түрлерін) жүргізу мүмкін болмаған жағдайда ("цифрлық үкімет" цифрлық объектілерді қоспағанда), сынақ объектісінің бастапқы кодына немесе сынақтарының басқа түріне (түрлеріне) талдау жүргізудің міндетті еместігі туралы киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның шешімімен өтініш берушінің сұрау салуы бойынша белгіленеді.

Киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган осы Қағидалардың 4-тармағына сәйкес басқа түрлері бойынша сынақтар жүргізу кезеңінде бастапқы кодты немесе сынақ объектісінің сынақтарының басқа түрін (түрлерін) талдауды алып тастау туралы өтінім берушінің сұрау салуының негізділігін тексеру туралы қызмет берушіге сұрау салуды жібереді.

6. "Цифрлық үкіметтің" цифрлық платформасында және (немесе) орналастырылған бағдарламалық қамтылымды (платформалық бағдарламалық өнімді) сынаққа мыналар кіреді:

1) бастапқы кодтарды талдау, соның ішінде статикалық және динамикалық талдау, тәуелділіктерді талдау;

2) киберқауіпсіздік функцияларын сынақ;

3) жүктеме сынағы.

7. "Цифрлық үкіметтің" цифрлық платформасының сынақтарына мыналар кіреді:

1) бастапқы кодтарды талдау;

2) киберқауіпсіздік функцияларын сынақ;

3) жүктемелік сынақ;

4) желілік инфрақұрылымды зерттеу;

5) киберқауіпсіздікті қамтамасыз ету процестерін тексеру.

8. Объектіні сынақ кезінде, егер сыналып жатқан объекті басқа да цифрлық объектімен интеграцияланса (қазіргі кезде немесе жоспарланған), сынақ интеграцияны қамтамасыз ететін компоненттерді (интеграция модулі, интеграциялық кіші жүйе, интеграциялық шина немесе басқа да) қоса алғанда жүргізіледі.

9. "Цифрлық үкіметтің" цифрлық объектілері және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігін сынақ әдістемеге сәйкес жүргізіледі.

10. Объектілерді сынақтың меншік иелері және (немесе) иеленушілері Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш индустриясы министрінің 2024 жылғы 29 ақпан № 110/НҚ бұйрығымен бекітілген Ұлттық бастапқы кодтар репозиторийінің жұмыс істеу қағидаларына сәйкес оң нәтижелерді көрсеткен цифрлық объектілердің бастапқы кодтарын тапсырады (Нормативтік құқықтық актілердің мемлекеттік тіркеу тізімінде № 34101 болып тіркелген).

3-тарау. "Цифрлық үкіметтің" цифрлық объектілері және аса маңызды цифрлық объектілердің мемлекеттік техникалық қызметтегі киберқауіпсіздік талаптарына сәйкестігі бойынша сынақ тәртібі

11. Интернет-порталында SYNAQ арқылы өтініш беруші сынақтан өту үшін өтініш (бұдан әрі – өтініш) толтырылады, электрондық цифрлық қолтаңбамен (бұдан әрі – ЭЦҚ) қол қойылады және осы Ережедегі 1-қосымшаға сәйкес нысан бойынша мемлекеттік техникалық қызметке келесі құжаттармен бірге жіберіледі:

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

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

3) цифрландыру саласындағы уәкілетті органмен және киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органмен келісілген цифрлық объектіге техникалық тапсырманың электрондық көшірмесі;

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

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

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

12. Мемлекеттік сатып алулардың веб-порталы арқылы жүзеге асырылатын сатып алу кезінде сынақтарды жүргізу туралы өтініш ағымдағы жылдың 1 (бірінші) қарашасына дейін қабылданады.

13. Мемлекеттік техникалық қызмет өтінімді алған күннен бастап 3 (үш) жұмыс күні ішінде осы Қағидалардың 11-тармағында көрсетілген құжаттардың толықтығын тексеруді жүзеге асырады.

14. Өтінім мен қоса берілген құжаттар осы Қағидалардың 11-тармағында көрсетілген талаптарға сәйкес келмеген жағдайда, өтінім қайтару себептері көрсетіле отырып, 10 (он) жұмыс күні ішінде өтініш берушіге қайтарылады.

15. Мемлекеттік техникалық қызмет осы Қағидалардың 11-тармағына сәйкес құжаттардың толық топтамасының болуына өтінімді тексергеннен кейін 3 (үш) жұмыс күні ішінде өтініш берушіге жібереді:

1) мемлекеттік сатып алу веб-порталы арқылы сатып алуды жүзеге асыру кезінде сынақтар жүргізуге арналған шартқа техникалық ерекшеліктің жобасы. Өтініш беруші техникалық ерекшелік жобасын алған күннен бастап 3 (үш) жұмыс күні ішінде мемлекеттік сатып алу туралы шартты тікелей жасасу арқылы бір көзден алу тәсілімен

мемлекеттік сатып алу туралы шарттың жобасын мемлекеттік сатып алу веб-порталында орналастырады;

2) мемлекеттік сатып алу веб-порталын қолданбай сатып алуды жүзеге асыру кезінде сынақтар жүргізуге арналған шарттың екі данасы.

Өтініш беруші жоғарыда көрсетілген шарттың екі данасын алған күннен бастап 5 (бес) жұмыс күні ішінде оларға қол қояды және шарттың бір данасын мемлекеттік техникалық қызметке қайтарады.

16. Мемлекеттік сатып алу туралы шарт веб-портал арқылы мемлекеттік техникалық қызметке осы жылдың 15 қарашасына дейін жіберілмеген жағдайда, өтініш күшін жойып, өтініш берушіге қайтарылады.

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

Сынақ мерзімдері келісілмесе, өтініш қанағаттандырылмай, өтініш берушіге сынақ мерзімдерін нақтылау үшін киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға жүгіну мүмкіндігі туралы хабарламамен бірге қайтарылады.

18. Сынақ жүргізу үшін өтініш беруші келесілерді қамтамасыз етеді:

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

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

19. Қағиданың 18-тармағында белгіленген талаптарды жүзеге асыру мүмкін болмаған жағдайда, сынақтар Заң беруші оларды қамтамасыз ету үшін қажетті уақытқа тоқтатылады, оның ішінде келісімшарт мерзімін ұзарту туралы қосымша келісімге қол қойылады.

20. Сынақ объектілерінің сипаттамалары туралы сауалнамадағы мәліметтер мен осы Ережелердің 11-тармағының 1-тармақшасына сәйкес ұсынылған сынақ объектісінің нақты күйі арасындағы қарама-қайшылықтар анықталған жағдайда, өтініш беруші мемлекеттік техникалық қызметке сынақ объектісінің сипаттамалары туралы жаңартылған сауалнаманы SYNAQ интернет-порталында сынақ объектісі иесінің (ұстаушысының) ЭЦҚ-мен куәландырылған күйде жібереді. Сынақ объектісінің сипаттамалары туралы жаңартылған сауалнама-сауалнама (қажет болған жағдайда) сынақ мерзімін ұзартуға және сынақ жүргізу құнын өзгертуге қосымша келісім жасасу үшін негіз болады.

21. Мерзімі аяқталғанға дейін бір немесе бірнеше сынақ түрлері бойынша қайта сынақ қажеттігі анықталған жағдайда, өтініш беруші мемлекеттік техникалық қызметке

сұраумен жүгінеді және осы жұмыс түрлері бойынша қайта сынақ жүргізу туралы қосымша келісім жасалады, бұл жұмыс ақысыз негізде жүзеге асырылады.

22. Сынақтардың нәтижелері және анықталған сәйкессіздіктерді жою бойынша ұсынымдар жеке хаттамаларға енгізіліп, барлық жұмыс түрлері аяқталғаннан кейін SYNAQ интернет-порталында өтініш берушінің жеке кабинетіне орналастырылады.

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

24. Сынақтарды өткізу құнын есептеу үшін өтініш беруші мемлекеттік техникалық қызметке SYNAQ интернет-порталында сынақ объектісінің меншік иесінің (иесінің) ЭЦҚ-мен куәландырылған сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнаманы және цифрлық объектіні құруға арналған техникалық тапсырманы (дамытуға арналған техникалық тапсырманы, бар болған жағдайда техникалық тапсырмаға толықтыруды) жібереді.

25. Өтініш беруші сынақ жүргізу нәтижесінде анықталған сәйкессіздіктерді өтініш берушінің сынақтар туралы хаттамалар интернет-порталына жарияланған күнінен бастап 60 (алпыс) жұмыс күні ішінде SYNAQ интернет-порталы арқылы жіберілген түзетулердің нәтижелерін көрсететін салыстырмалы кестемен бірге мемлекеттік техникалық қызметке қайта сынақтар өткізу туралы сұраныспен жолданған жағдайда, мемлекеттік техникалық қызмет өтініш берушіден сұраныс алған күнінен бастап 20 (жиырма) жұмыс күні ішінде аталған жұмыс түрлері бойынша тиісті құжаттарды ресімдей отырып, сынақтарды тегін өткізеді.

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

Қажет болған жағдайда, өтініш беруші сынақтар барысында анықталған сәйкессіздіктерді жою мерзімін бір рет қосымша өтініш беру арқылы ұлғайтуға болады, бірақ 20 жұмыс күнінен аспауы тиіс.

Белгіленген мерзімді өткізіп алу осы Қағидаларда белгіленген жалпы тәртіппен сынақтар жүргізуге негіз болады.

27. Объектінің БҚ өзгерістер енгізумен байланысты кемшіліктерді жойғаннан кейін қайта сынақ жүргізілген кезде бастапқы кодты талдау жүргізіледі.

Бұл ретте, өтініш беруші қайта сынақ жүргізу туралы сұранысына сынақ объектісінің компоненттері мен модульдерінің бастапқы кодтарын, сондай-ақ сынақ объектісін сәтті құрастыру үшін қажетті кітапханалар мен файлдарды қоса береді.

28. Мемлекеттік техникалық қызмет қайта сынақтар жүргізу кезінде сәйкессіздіктер анықталған жағдайда, теріс қорытындысы бар хаттама толтырып, содан кейін сынақтар осы Ережелердің 3-тарауында белгіленген тәртіппен жүргізіледі.

4-тарау. "Цифрлық үкіметтің" цифрлық объектілері және аса маңызды цифрлық объектілердің сынақ зертханаларында киберқауіпсіздік талаптарына сәйкестігі бойынша сынақ тәртібі

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

30. Сынақтар жүргізу үшін өтініш беруші мынадай құжаттарды ұсына отырып, мемлекеттік техникалық қызметке қағаз тасымалдауышта ілеспе хатпен осы Қағидаларға 1-қосымшаға сәйкес нысан бойынша сынақтар жүргізуге өтінім (бұдан әрі – өтінім) береді:

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

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

3) меншік иесі немесе иеленуші бекіткен, мемлекеттік заңды тұлғаның меншік иесі немесе иеленуші бекіткен техникалық тапсырма немесе цифрлық объектіге қатысты техникалық сипаттама, "цифрлық үкімет" цифрлық объектісінен басқа, компакт-дискіде (қажет болған жағдайда);

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

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

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

31. Өтініш беруші сынақ нәтижелері бойынша анықталған сәйкессіздіктерді жойғаннан кейін, сынақ хаттамаларын алған күнінен бастап 20 (жиырма) жұмыс күні ішінде салыстырмалы кестесін қоса отырып, қайта сынақ үшін қызмет берушіге өтініш жібереді. Қызмет беруші хабарлама алған күнінен бастап 20 (жиырма) жұмыс күні ішінде қайта сынақты тегін негізде жүргізуге және тиісті құжаттарды рәсімдеуге міндеттенеді.

32. Өтініш беруші белгіленген мерзімде екі реттен артық емес қайталама сынақтарға өткізуге өтініш бере алады.

33. Өтініш беруші сынақ жүргізу кезінде анықталған сәйкессіздіктерді жою мерзімін, осы мерзімді арттыру туралы қосымша өтініш беру арқылы, бір рет арттыруға құқылы, бірақ 20 (жиырма) жұмыс күнінен аспауы тиіс.

Қайта сынақтарды жүргізу туралы өтінішті уақтылы ұсынбау осы Қағидада белгіленген жалпы тәртіппен сынақтар жүргізуге негіз болады.

34. Қайта сынақтар барысында сәйкессіздіктер анықталған жағдайда, қызмет беруші теріс қорытындысы бар хаттама рәсімдейді, содан кейін сынақтар осы Ережелердің 3-тарауында белгіленген тәртіппен жүргізіледі.

35. Сынақ хаттамалары жоғалған, бүлінген немесе зақымданған жағдайда, сынақ объектісінің иесі немесе пайдаланушысы себептерін көрсете отырып, қызмет берушіге хабарлама жібереді.

Қызмет беруші хабарлама алған күнінен бастап 5 (бес) жұмыс күні ішінде сынақ хаттамаларының көшірмесін береді.

5-тарау. Сынақ хаттамаларын беру және кері қайтару тәртібі

36. Сынақ хаттамаларын қызмет беруші береді.

37. Сынақ хаттамаларының жарамдылық мерзімі "цифрлық үкіметтің" цифрлық платформасын қоспағанда, барлық сынақ объектілері үшін немесе сынақ объектісінің жұмыс істеуі және (немесе) функционалдық шарттары және (немесе) меншік және (немесе) иелену құқықтары өзгергеннен кейін 3 (үш) жыл мерзімге беріледі.

Бұл ретте цифрлық объектіні өнеркәсіптік пайдалануға беру үшін сынақтың жекелеген түрі бойынша хаттаманың қолданылу мерзімі хаттама берілген күннен бастап бір жылдан аспайды.

Цифрлық объектінің меншік иесі немесе иеленушісі сынақ хаттамаларының жарамдылық мерзімінің аяқталуына дейін осы Қағидалардың 3 немесе 4-тарауларында белгіленген тәртіппен 3 (үш) ай бұрын қызмет берушіге сынақ өту жөнінде өтініш береді.

"Цифрлық үкіметтің" цифрлық платформасының сынақ хаттамалары 1 (бір) жыл қолданылу мерзімімен беріледі.

38. Қызмет беруші тұрақты негізде киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға мынадай деректерді ұсынады:

1) сынақтар жүргізуге өтінімді;

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

3) сынақ объектісінің атауын;

4) сынақ объектісінің меншік иесінің және (немесе) иеленушінің атауын;

5) нәтижесін көрсете отырып, жұмыстың әрбір түрі бойынша киберқауіпсіздік талаптарына сәйкестігін сынақтың тізілімдік нөмірі, берілген күні және хаттамасын;

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

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

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

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

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

39. Цифрлық объектінің жұмыс істеу жағдайлары және (немесе) функционалдығы өзгерген және (немесе) меншік құқықтары өзгерген кезде цифрлық объектінің меншік иесі немесе иеленушісі өзгерістерге әкелген жұмыстарды аяқтағаннан кейін көрсетілетін қызмет берушіге барлық жүргізілген өзгерістердің сипаттамасын және сынақтар объектісінің меншік иесінің немесе иеленушісімен бекітілген сынақтар объектісінің сипаттамалары туралы жаңартылған сауалнама-сұрақнаманы қоса беріп, хабарлама жібереді.

Сынақ бір (бірнеше) түрін өткізу туралы шешім қабылданған кезде бұрын берілген тиісті сынақ хаттамасы (хаттамалары) немесе сынақ актісі өз қолданысын тоқтатады.

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

41. Қызмет беруші цифрлық объектіге енгізілген өзгерістерді және (немесе) анықталған сәйкессіздіктер туралы ақпаратты және (немесе) өзгермеуге талдау нәтижелері бойынша бастапқы кодтың өзгерістері туралы ақпаратты 10 (он) жұмыс күнінен аспайтын мерзімде қарайды және тестілеу хаттамаларын кері қайтарып алу және цифрлық объектінің жұмыс істеу және (немесе) функционалдығы жағдайлары өзгерген кезде функциялары бұзылған сынақтардың сол түрін жүргізу қажеттілігі туралы шешім қабылдайды.

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

42. Сынақ хаттамаларын қайтарып алу кезінде меншік иесі немесе иеленуші үш ай мерзімде осы Қағидалардың 3 немесе 4-тарауында белгіленген тәртіппен сынақтардан өту туралы қызмет берушілерге өтінім береді.

43. Қазақстан Республикасының Әкімшілік рәсімдік-процестік кодексінің 91-бабына сәйкес, өтініш беруші сынақ хаттамаларының нәтижелерімен келіспеген жағдайда, әкімшілік актіге (әрекетсіздікке) шағымдану жүзеге асырылады.

"Цифрлық үкіметтің" цифрлық
объектілерінің және аса
маңызды цифрлық объектілердің
киберқауіпсіздік талаптарына
сәйкестігіне сынақтар жүргізу

қағидаларына
1-қосымша
Нысан

_____

(қызмет берушінің атауы)
Сынақтарды өткізуге өтінім

_____

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

_____

_____

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

_____

(сынақ объектісінің атауы, нұсқа нөмірі, әзірленген күні)
мынадай жұмыс түрлерінің құрамында:
1) _____
2) _____
3) _____
4) _____
5) _____
(Қағидалардың 4,6,7-тармақтарына сәйкес жұмыс түрлерінің тізбесі
(қажетті тармақты көрсетіңіз)
2. Сыналатын сынақ объектісінің меншік иесі (иеленуші) туралы мәліметтер

_____

(атауы немесе аты-жөні (бар болса)

_____

_____

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

_____

(әзірлеуші туралы ақпарат, авторлардың атауы немесе аты-жөні (бар болған жағдайда))

_____

(қала, аудан, пошта мекенжайы, телефон)
4. Қызмет берушімен байланыс үшін жауапты тұлғаның деректері:
1) тегі, аты, әкесінің аты: _____;

2) лауазымы: _____;
3) жұмыс телефоны:_____, ұялы
телефон:_____;
4) электрондық пошта мекенжайы: _____@_____.
Өтініш беруші ұйымның басшысы/ аты-жөні (бар болған жағдайда),
өтініш берушінің _____ (өтініш берушінің)
(Мөр орны) болған жағдайда

"Цифрлық үкіметтің" цифрлық
объектілерінің және аса
маңызды цифрлық объектілердің
киберқауіпсіздік талаптарына
сәйкестігіне сынақтар жүргізу
қағидаларына
2-қосымша
Нысан

Сынақ объектісінің сипаттамалары туралы сауалнама-сұрақнама

1. Сынақ объектісінің атауы: _____
_____
2. Сынақ объектісіне қысқаша аннотация _____
_____
(мақсаты және қолдану саласы)
3. Сынақ объектісінің жіктелуі:
1) қолданбалы бағдарламалық қамтылым класы _____.
2) Қазақстан Республикасының Цифрлық кодексінің 20-бабы 3-тармағысына сәйкес бекітілетін Цифрлық объектілердің классификаторындағы классификация схемасы.
4. Сынақ объектісінің архитектурасы:
1) сынақ объектісінің функционалдық схемасы (қажет болған жағдайда):
сынақ объектісінің компоненттерін, модульдерін және олардың IP-мекенжайларын;
компоненттер немесе модульдер арасындағы байланыстар және ақпараттық ағындардың бағыттары;
басқа объектілермен интеграциялық өзара әрекеттесудің қосылу нүктелері цифрландыру;
пайдаланушылардың қосылу нүктелері;
деректерді сақтау орындары мен технологиялары;
қолданылатын резервтік жабдық;
қолданылатын терминдер мен аббревиатураларды түсіндіру;
2) сынақ объектісінің деректерін беру желісінің сызбасы (қажет болған жағдайда):
желінің архитектурасы мен сипаттамалары;
серверлік желілік және коммуникациялық жабдықтар;
адрестеу және қолданылатын желілік технологиялар ;

пайдаланылатын жергілікті, ведомстволық (корпоративтік) және жаһандық желілер; ақауларға төзімділікті қамтамасыз ету және резервтеу жөніндегі шешім(дер). қолданылатын терминдер мен аббревиатураларды түсіндіру;

5. Сынақ объектісі туралы ақпарат:

1) серверлік жабдық туралы ақпарат:

№ р/н	Сервердің немесе виртуалды ресурстың атауы (домендік атау, желі атауы немесе логикалық сервер атауы)	Мақсаты (орындалатын функционалдық міндеттер)	Саны	Сервердің сипаттамалары немесе қолданылатын мәлімделген виртуалды ресурстар	Операциялық жүйе (бұдан әрі – ОЖ), деректер қоры басқару жүйесі (бұдан әрі – ДҚБЖ), бағдарламалық қамтама (бұдан әрі – БҚ), қосымшалар, кітапханалар және серверлерде орнатылған немесе пайдаланылатын виртуалды сервистер қорғау құралдары (нұсқа нөмірлері көрсетілген бағдарламалық ортаның құрамы)	Қолданылатын IP мекенжайлары
1	2	3	4	5	6	7

2) желілік жабдық туралы ақпарат:

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

3) серверлік және желілік жабдықтың орналасқан жері:

№ р/н	Серверлік үй-жайдың иесі	Серверлік үй-жай иесінің заңды мекенжайы	Нақты орналасқан жері – сервер бөлмесінің мекен-жайы	Қолжетімділікті ұйымдастыруға жауапты тұлғалар (Т.А.Ә. (бар болса)	Жауапты тұлғалардың телефондары (жұмыс, ұялы)

1	2	3	4	5	6

4) резервтік серверлік жабдықтың сипаттамалары:

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

5) резервтік желілік жабдықтың сипаттамалары:

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

6) резервтік серверлік және желілік жабдықтың орналасқан жері:

№ р/н	Серверлік үй-жайдың иесі	Серверлік үй-жай иесінің заңды мекенжайы	Нақты орналасқан жері – сервер бөлмесінің мекенжайы	Қолжетімділікті ұйымдастыруға жауапты тұлғалар (тегі, аты, әкесінің аты (бар болса)	Жауапты тұлғалардың телефондары (жұмыс, ұялы телефоны)
1	2	3	4	5	6

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

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

8) әкімшілердің жұмыс станциялары бойынша ақпарат:

					Әкімші жұмыс	Нақты орналасқан

№ р/н	Әкімші рөлі	Әкімші есептік жазбаларының саны	Интернетке қол жетімділіктің болуы	Жабдыққа қашықтан қол жеткізудің болуы	станциясының IP мекенжайы	жері-жұмыс орнының мекенжайы
1	2	3	4	5	6	7

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

№ п/п	Пайдалану шының рөлі	Пайдалану шының үлгілік әрекеттерінің тізбесі	Пайдалану шылардың сынақ объектісіне қосылу нүктесінің мекенжайы мен порты	Пайдалану шыларды сынақ объектісіне қосу хаттамасы	Сынақ объектісін құруға немесе дамытуға арналған нормативтік-техникалық құжаттамаға сәйкес пайдаланушылар саны	Секундына өңделетін сұрауларды ң ( ) ең көп саны	Сұраулар арасындағы максималды күту уақыты
1	2	3	4	5	6	7	8

10) сынақ объектісінің интеграциялық өзара іс-қимылы туралы, оның ішінде жоспарланатын ақпарат:";

№ р/н	Интеграциялық байланыстың (цифрлық объектінің) атауы	Интеграцияланатын объектінің меншік иесі немесе иесі
1	2	3

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

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

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

№ р/н	Дискіні маркалау (қажет болған жағдайда)	Каталог атауы / дискідегі каталог атауы	Кітапхана / бағдарламалық платформа / файл атауы	Өлшемі, Мбайт	Бағдарламалау тілі (қажет болған жағдайда)	Кітапхана нұсқасы
1	2	3	4	5	6	7

6. Сыналатын объектіні құжаттау (қажет болған жағдайда):

					Құжат әзірленген

№ р/н	Құжаттың атауы	Болуы	Беттер саны	Бекітілген күні	Стандарт немесе нормативтік құжат
1	2	3	4	5	6
1	Киберқауіпсіздік саясаты;				
2	Киберқауіпсіздік тәуекелдерін бағалау әдістемесі;				
3	Ақпаратты өңдеу құралдарымен және оларды түгендеумен байланысты активтерді сәйкестендіру, сыныптау, таңбалау, паспорттау қағидалары;				
4	Киберқауіпсіздіктің ішкі аудитін жүргізу қағидалары;				
5	Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;				
6	Цифрлық ресурстарға қол жеткізу құқықтарын аутентификациялау және олардың аражігін ажырату рәсімін ұйымдастыру қағидалары;				
7	Антивирустық бақылауды ұйымдастыру, мобильді құрылғыларды, ақпарат жеткізгіштерді, Интернетті және электрондық				

	поштаны пайдалану қағидалары;				
8	Ақпаратты өңдеу құралдарымен байланысты активтердің физикалық қорғалуын, жұмыс істеуі мен үздіксіз жұмысын қамтамасыз етудің қауіпсіз ортасын ұйымдастыру қағидалары;				
9	Цифрлық объектіні сүйемелдеу, ақпаратты резервтік көшіру және қалпына келтіру жөніндегі әкімшінің нұсқауы;				
10	Пайдаланушылардың киберқауіпсіздікті оқыс оқиғаларына және штаттан тыс (дағдарысты) жағдайларда ден қою бойынша іс-қимыл тәртібі туралы нұсқаулық.				

"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидаларына
3-қосымша
Нысан

Сынақ объектісінің киберқауіпсіздігі жөніндегі нормативтік-техникалық құжаттаманың тізбесі

1. Киберқауіпсіздік саясаты;

2. Киберқауіпсіздік тәуекелдерін бағалау әдістемесі;

3. Ақпаратты өңдеу құралдарымен және оларды түгендеумен байланысты активтерді сәйкестендіру, жіктеу, таңбалау, паспорттау қағидалары;

4. Киберқауіпсіздіктің ішкі аудитін жүргізу қағидалары;

5. Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;

6. Цифрлық ресурстарға қол жеткізу құқықтарын аутентификациялау және олардың ара-жігін ажырату рәсімін ұйымдастыру қағидалары;

7. Антивирустық бақылауды ұйымдастыру, мобильді құрылғыларды, ақпарат жеткізгіштерді, Интернетті және электрондық поштаны пайдалану қағидалары;

8. Ақпаратты өңдеу құралдарымен байланысты активтердің физикалық қорғалуын, жұмыс істеуінің қауіпсіз ортасын ұйымдастыру және үздіксіз жұмысын қамтамасыз ету қағидалары;

9. Цифрлық объектіні сүйемелдеу, ақпаратты резервтік көшіру және қалпына келтіру жөніндегі әкімшінің нұсқауы;

10. Киберқауіпсіздіктің инциденттеріне және штаттан тыс (дағдарыстық) жағдайларға ден қою бойынша пайдаланушылардың іс-қимыл тәртібі туралы нұсқаулық.".

"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу қағидаларына
4-қосымша
Нысан

Цифрлық объектінің жұмыс істеуі және (немесе) функционалдығы өзгерістерінің тізбесі

№ р/	Жасалған өзгерістер	Бастапқы кодтарды талдау	Киберқауіпсіздік функциялары	Жүктеме сынағы	Желілік инфрақұрылымды зерттеу	Киберқауіпсіздікті қамтамасыз ету процестерін зерттеу
1	2	3	4	5	6	7
1.	Даму ортасын (бағдарламалау тілі) өзгерту	+	-	-	-	-
2.	Қолданбалы бағдарламалық қамтамасының функциясын өзгерту	+	+	+	-	-

3.	Серверлік жабдықты ауыстыру	-	+	+	+	+
4.	Желілік жабдықты ауыстыру	-	-	+	+	-
5.	Операциялық жүйе, деректер базасын басқару жүйесі түрінің өзгеруі	-	+	+	-	-
6.	Сынақ объектісінің орналасқан жерін өзгерту	-	+	-	+	+
7.	Сынақ объектісінің ішкі контурдан сыртқы контурға немесе айналымға көшуі	-	+	+	+	+
8.	Жаңа компонентті (серверді)қосу	-	+	-	+	+
9.	Басқалармен жаңа интеграция	+	+	+	+	+
10.	Цифрлық объектінің сыныбын өзгерту	-	+	-	+	+
11.	Цифрлық объектінің меншік және (немесе) иеленуші құқықтарын өзгерту (меншік иесін және/немесе иеленушісін өзгерту)	-	-	-	-	+