Қазақстан Республикасының Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ.

Закон от 24.11.2015 № 418-V

ЗҚАИ-ның ескертпесі!

Осы Заңның қолданысқа енгізілу тәртібін 67-баптан қараңыз.

Қолданушылар назарына!

Қолданушыларға ыңғайлы болуы үшін ЗҚАИ мазмұнды жасады.

МАЗМҰНЫ

Ескерту. Заңның тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

Ескерту. Кіріспе алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

Ескерту. 1-бөлімнің тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

1-тарау. ЖАЛПЫ ЕРЕЖЕЛЕР

1-бап. Осы Заңда пайдаланылатын негізгі ұғымдар

Осы Заңда мынадай негізгі ұғымдар пайдаланылады:

1) ақпаратты қорғау құралы – ақпаратты қорғауды қамтамасыз етуге арналған және пайдаланылатын бағдарламалық қамтылым, техникалық және өзге де құралдар;

2) артықшылықты құқықтары бар пайдаланушы – цифрлық объектіге қол жеткізу құқықтары жоғары, оның жұмыс істеуінің штаттық пайдалану жағдайларын қамтамасыз ететін пайдаланушы;

3) аса маңызды цифрлық объектілер – жұмыс істеуінің бұзылуы немесе тоқтауы қолжетімділігі шектелген дербес деректерді және заңмен қорғалатын құпияны қамтитын өзге де мәліметтерді заңсыз жинауға және өңдеуге, әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайлардың туындауына немесе қорғаныс, қауіпсіздік, халықаралық қатынастар, экономика, шаруашылықтың жекелеген салалары үшін немесе тиісті аумақта тұратын халықтың тыныс-тіршілігі, оның ішінде жылумен жабдықтау, электрмен жабдықтау, газбен жабдықтау, сумен жабдықтау, өнеркәсіп, денсаулық сақтау, байланыс, банк саласы, көлік, гидротехникалық құрылысжайлар, құқық қорғау қызметі, "цифрлық үкімет" инфрақұрылымы үшін елеулі теріс салдарға алып келетін цифрлық объектілер;

4) Бастапқы кодтардың ұлттық репозиторийі – цифрлық объектілердің бастапқы кодтарын сақтау орны;

5) домендік атау – Интернетті адрестеу қағидаларына сәйкес қалыптастырылған, белгілі бір желілік мекенжайға сәйкес келетін және Интернет объектісіне атауы бойынша жүгінуге арналған символдық (әріптік-цифрлық) белгіленім;

6) зиянды бағдарлама – цифрлық деректерге санкцияланбаған қол жеткізуді, оларды жоюды, бұғаттауды, модификациялауды не көшіруді жүзеге асыруға, сондай-ақ цифрлық объектілердің жұмыс істеуін бұзуға мүмкіндік беретін жасалған немесе

қолданыстағы бағдарлама немесе енгізілген өзгерістері бар бағдарламалық өнім;

7) Интернетке қол жеткізудің бірыңғай шлюзі – Интернетке және (немесе) Интернетке шығатын байланыс желілеріне қол жеткізу кезінде цифрлық объектіні қорғауға арналған аппараттық-бағдарламалық кешен;

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

9) киберқауіпсіздік аудиті – цифрлық объектілердің қорғалу жай-күйінің киберқауіпсіздік талаптарына сәйкестігін бағалау;

10) киберқауіпсіздік зерттеушісі – киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасына қатысатын киберқауіпсіздікті қамтамасыз ету саласындағы маман;

11) киберқауіпсіздік қатері – киберқауіпсіздіктің оқыс оқиғасының туындауына алғышарттар жасайтын жағдайлар мен факторлардың жиынтығы;

12) киберқауіпсіздік оқиғаларын басқару жүйесі – цифрлық объектінің оқиғаларды тіркеу журналдарын жинау және талдау арқылы киберқауіпсіздік оқиғаларын автоматтандырылған түрде анықтауға арналған бағдарламалық қамтылым немесе аппараттық-бағдарламалық кешен;

13) киберқауіпсіздік оқиғаларының мониторингі – киберқауіпсіздік оқиғаларын басқару жүйесі арқылы киберқауіпсіздік оқиғаларын анықтау және сәйкестендіру мақсатында цифрлық объектіні тұрақты қадағалау;

14) киберқауіпсіздік оқиғасы – киберқауіпсіздіктің ықтимал бұзылуын немесе киберқауіпсіздікті қамтамасыз етуге қатысы болуы мүмкін бұрын белгісіз жағдайды көрсететін, цифрлық объектінің жай-күйінің сәйкестендірілген туындауы;

15) киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасы – киберқауіпсіздікті зерттеушілердің цифрлық объектілердегі осалдықты анықтау үшін олармен өзара іс-қимыл жасауды қамтамасыз ететін ұйымдастыру-техникалық іс-шаралар;

16) киберқауіпсіздікті қамтамасыз етуді мониторингтеу жүйесі – цифрлық технологияларды қауіпсіз пайдалану мониторингін жүргізуге бағытталған ұйымдастырушылық және техникалық іс-шаралар;

17) киберқауіпсіздікті қамтамасыз ету орталығы – шетелдік заңды және жеке тұлғалардың қатысуынсыз Қазақстан Республикасының резиденті болып табылатын, цифрлық объектілерді қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі;

18) киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) – киберқауіпсіздікті қамтамасыз ету саласындағы басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган;

19) киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институты – киберқауіпсіздік саласын дамыту мақсатында Қазақстан Республикасының Үкіметі айқындайтын заңды тұлға;

20) киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметі – шетелдік заңды және жеке тұлғалардың қатысуынсыз Қазақстан Республикасының резиденті болып табылатын, осы Заңда белгіленген құзыретке сәйкес киберқауіпсіздіктің оқыс

оқиғасына ден қоюды жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі;

21) киберқауіпсіздіктің оқыс оқиғасы – цифрлық объектінің киберқауіпсіздігіне теріс әсер ететін оқиға немесе оқиғалар жиынтығы;

22) киберқауіпсіздіктің оқыс оқиғасына ден қою – цифрлық объектілердің және олардағы цифрлық деректердің штаттық жұмыс істеуін қорғау және қалпына келтіру үшін қабылданған іс-қимылдарды қоса алғанда, киберқауіпсіздіктің оқыс оқиғасын барынша азайту немесе жою үшін қабылданған іс-әрекеттер;

23) киберқауіпсіздіктің салалық орталығы – ведомстволық бағынысты ұйымдарға және (немесе) реттелетін басқару саласына қатысты киберқауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды ұйымдастыруды және үйлестіруді жүзеге асыратын заңды тұлға немесе мемлекеттік органның құрылымдық бөлімшесі;

24) киберқауіпсіздіктің ішкі аудиті – ұйым өз мүддесі үшін жүзеге асыратын, ұйымдағы цифрлық объектілердің киберқауіпсіздігінің ағымдағы жай-күйінің сапалық және сандық сипаттамаларын бақылаудың объективті, құжатталған процесі;

25) кибермәдениет – цифрлық ортада қауіпсіз және жауапты мінез-құлық нормалары мен құндылықтарының жиынтығы;

26) қорғау бейіні – цифрлық объектілердің құрауыштары болып табылатын бағдарламалық және техникалық құралдардың қауіпсіздігіне қойылатын ең төмен талаптардың тізбесі;

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

28) осалдық – цифрлық объектінің киберқауіпсіздікке қатер төндіретін кемшілігі;

29) техникалық құралдар – цифрлық деректерді жинау, өңдеу, сақтау, коммутациялау және беру үшін пайдаланылатын құрылғылар;

30) технологиялық процестерді басқарудың автоматтандырылған жүйесі – нақты уақыт режимінде өндірістік процестерді автоматтандыруға, басқаруға, бақылауға және мониторингтеуге арналған цифрлық инфрақұрылым объектісі;

30-1) хостинг-провайдер – деректерді беру желісіндегі өз мекенжайларын пайдалана отырып, өзінің цифрлық инфрақұрылымында орналастырылған үшінші тұлғалардың интернет-ресурстарына орналастыру, сақтау және (немесе) оларға қол жеткізуді қамтамасыз ету жөніндегі көрсетілетін қызметтерді ұсыну жөніндегі қызметті жүзеге асыратын жеке немесе заңды тұлға;

31) цифрлық объектілер сыныптауышы (бұдан әрі – сыныптауыш) – цифрлық объектілерді сәйкестендіруге, санатқа бөлуге, сипаттауға және есепке алуға бағытталған санаттардың жүйеленген тізбесі;

32) цифрлық оқиғаларды журналға енгізу – кейіннен талдау, ауытқуларды анықтау және киберқауіпсіздіктің оқыс оқиғаларын зерттеу мақсатында цифрлық объектілерде болып жатқан оқиғалар туралы цифрлық жазбаларды жүйелі түрде жазу, жинау және сақтау процесі;

33) "цифрлық үкіметтің" электрондық поштасының бірыңғай шлюзі – киберқауіпсіздік талаптарына сәйкес "цифрлық үкіметтің" электрондық поштасын қорғауды қамтамасыз ететін аппараттық-бағдарламалық кешен.

Ескерту. 1-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

2-бап. Қазақстан Республикасының киберқауіпсіздік туралы заңнамасы

1. Қазақстан Республикасының киберқауіпсіздік туралы заңнамасы Қазақстан Республикасының Конституциясына негізделеді, осы Заңнан және Қазақстан Республикасының өзге де нормативтік құқықтық актілерінен тұрады.

2. Қазақстан Республикасы ратификациялаған халықаралық шарттардың осы Заң алдында басымдығы болады. Қазақстан Республикасы қатысушысы болып табылатын халықаралық шарттардың Қазақстан Республикасының аумағында қолданылу тәртібі мен талаптары Қазақстан Республикасының заңнамасында айқындалады.

Ескерту. 2-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

3-бап. Осы Заңның қолданылу аясы

Осы Заңның қолданылу аясы Қазақстан Республикасының аумағында цифрлық объектілердің өмірлік циклінің барлық кезеңінде мемлекеттік органдар, жеке және заңды тұлғалар арасында туындайтын киберқауіпсіздік саласындағы қоғамдық қатынастар болып табылады.

Ескерту. 3-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

4-бап. Киберқауіпсіздік саласындағы қоғамдық қатынастарды мемлекеттік реттеудің мақсаты мен қағидаттары

1. Қазақстан Республикасының орнықты дамуын қамтамасыз ететін цифрлық объектілердің қорғалуына қол жеткізу және қорғалуын қолдау киберқауіпсіздікті қамтамасыз ету саласындағы қоғамдық қатынастарды мемлекеттік реттеудің мақсаты болып табылады.

2. Киберқауіпсіздік саласындағы мемлекеттік реттеу мынадай негізгі қағидаттарға негізделеді:

1) заңдылық;

2) цифрлық технологияларды қолдану кезінде жеке адамның, қоғамның және мемлекеттің қауіпсіздігін қамтамасыз ету;

3) жеке адам, қоғам мен мемлекет құқықтарының, бостандықтары мен заңды мүдделерінің теңгерімі және олардың цифрлық ортадағы өзара жауапкершілігі;

4) жеке тұлғалардың құқықтарын, бостандықтары мен заңды мүдделерін, сондай-ақ заңды тұлғалардың құқықтары мен заңды мүдделерін сақтау;

5) жеке және заңды тұлғалардың киберқауіпсіздікті қамтамасыз ету саласындағы қызметке қатысу және оның нәтижелерін пайдалану құқықтарының, бостандықтары мен заңды мүдделерінің теңдігі.

Ескерту. 4-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

2-тарау. Киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік реттеу

Ескерту. 2-тараудың тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

5-бап. Киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік реттеудің міндеттері

Мыналар киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік реттеудің міндеттері болып табылады:

1) цифрлық объектілерді және аса маңызды цифрлық объектілерді олардың өмірлік циклінің барлық кезеңінде қорғау;

2) киберқауіпсіздік саласын қалыптастыруға және дамытуға жәрдемдесу;

3) киберқауіпсіздіктің заманауи шешімдерін дамыту және өндірістік процестерге ендіру үшін жағдайларды қамтамасыз ету;

4) кибермәдениетті арттыру;

5) киберқауіпсіздік саласындағы бірыңғай ғылыми, техникалық, мемлекеттік технологиялық саясатты қалыптастыру және іске асыру;

6) мемлекеттік органдардың, жеке және заңды тұлғалардың цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуді мониторингтеу;

7) киберқауіпсіздіктің оқыс оқиғаларының, оның ішінде әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше жағдай немесе соғыс жағдайы енгізілген жағдайларда алдын алу және оларға жедел ден қою;

8) киберқауіпсіздік саласындағы шешімдер мен кадр әлеуетін дамыту;

9) халықаралық ынтымақтастыққа қатысу;

10) Қазақстан Республикасының киберқауіпсіздік туралы заңнамасын жетілдіру.

Ескерту. 5-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

6-бап. Қазақстан Республикасы Үкіметінің киберқауіпсіздікті қамтамасыз ету саласындағы құзыреті

Қазақстан Республикасының Үкіметі:

1) киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік саясаттың негізгі бағыттарын әзірлейді және олардың жүзеге асырылуын ұйымдастырады;

2) киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институтын айқындайды;

2-1) Ұлттық бейнемониторинг жүйесінің операторын айқындайды;

3) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарды бекітеді;

4) киберқауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспарын бекітеді;

5) Қазақстан Республикасының Конституциясында, осы Заңда, Қазақстан Республикасының өзге де заңдарында және Қазақстан Республикасы Президентінің

актілерінде өзіне жүктелген өзге де функцияларды орындайды.

Ескерту. 6-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

7-бап. Уәкілетті органның құзыреті

Ескерту. 7-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

7-1-бап. Уәкілетті органның құзыреті

Уәкілетті орган:

1) мемлекеттің ішкі және сыртқы саясатының Қазақстан Республикасының Президенті айқындаған негізгі бағыттары мен мемлекеттің әлеуметтік-экономикалық саясатының, оның қорғаныс қабілетінің, қауіпсіздігінің, қоғамдық тәртіпті қамтамасыз етудің Қазақстан Республикасының Үкіметі әзірлеген негізгі бағыттары негізінде және оларды орындау үшін Қазақстан Республикасының заңнамасына сәйкес киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік саясатты қалыптастырады;

2) стратегиялық, реттеушілік, іске асыру және бақылау функцияларын жүзеге асырады;

3) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарды әзірлейді;

4) аса маңызды цифрлық объектілердің тізбесін, сондай-ақ цифрлық объектілерді аса маңызды объектілерге жатқызу қағидалары мен өлшемшарттарын, аса маңызды цифрлық объектілерді санаттарға бөлу әдістемесін бекітеді;

5) "цифрлық үкіметтің" цифрлық объектілері мен аса маңызды цифрлық объектілердің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекітеді;

6) Қазақстан Республикасының Ұлттық қауіпсіздік комитетімен келісу бойынша цифрлық үкіметтің цифрлық объектілерінің киберқауіпсіздігі оқиғаларына мониторингті жүзеге асыру қағидаларын бекітеді;

7) Қазақстан Республикасының Ұлттық қауіпсіздік комитетімен келісу бойынша "цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларын бекітеді;

8) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың орындалуын мониторингтеуді жүргізу қағидаларын бекітеді;

9) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың орындалуын мониторингтеуді жүзеге асырады;

10) аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету бөлігінде цифрландыру саласындағы мемлекеттік бақылауды қоспағанда, цифрландыру саласында, сондай-ақ электрондық құжатқа және электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуына мемлекеттік бақылауды жүзеге асырады;

11) аса маңызды цифрлық объектілерге жататын объектілерді қоспағанда, киберқауіпсіздікті қамтамасыз ету бөлігінде Қазақстан Республикасының цифрландыру саласындағы заңнамасының талаптарын бұзушылықтар анықталған кезде орындау үшін нұсқамалар жібереді;

12) әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше жағдай немесе соғыс жағдайы енгізілген кезде цифрлық объектілерді басқару жөніндегі қызметті үйлестіруді жүзеге асырады;

13) "цифрлық үкіметтің" цифрлық объектілерін өнеркәсіптік пайдалануға беруге қатысады;

14) цифрлық ресурстарды алу, көшіру, тарату, модификациялау, жою немесе бұғаттау жөніндегі құқыққа сыйымсыз әрекеттердің алдын алуды қоса алғанда, цифрлық объектілердің меншік иелеріне, иегерлеріне және пайдаланушыларына цифрлық технологияларды қауіпсіз пайдалану мәселелерінде жәрдемдесуді ұйымдастырады;

15) киберқауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспарын әзірлейді;

16) домендік атаулардың әкімшісін және тіркеу орнын айқындайды, Интернеттің қазақстандық сегментінің кеңістігінде домендік атауларды тіркеу, пайдалану және бөлу қағидаларын бекітеді;

17) цифрлық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасының жұмыс істеу қағидаларын, аса маңызды цифрлық объектілердің цифрлық ресурстарын резервтік көшірудің кезеңділігін бекітеді;

18) Қазақстан Республикасының Ұлттық қауіпсіздік комитетімен келісу бойынша Интернетке қол жеткізудің бірыңғай шлюзінің және "цифрлық үкіметтің" электрондық поштасы бірыңғай шлюзінің жұмыс істеу қағидаларын бекітеді;

19) Бастапқы кодтардың ұлттық репозиторийінің жұмыс істеу қағидаларын бекітеді;

20) қорғау бейіндерін және қорғау бейіндерін әзірлеу әдістемесін бекітеді;

21) киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларын бекітеді;

22) мемлекеттік техникалық қызметтің сараптамалары негізінде инвестициялық ұсыныстарға және бюджеттік инвестициялардың қаржы-экономикалық негіздемелеріне киберқауіпсіздікті қамтамасыз ету саласында қорытындылар береді;

23) Қазақстан Республикасы арнаулы мемлекеттік органдарының цифрлық объектілерін қоспағанда, мемлекеттік техникалық қызметтің сараптамалары негізінде "цифрлық үкіметтің" цифрлық объектілерін құруға немесе дамытуға арналған техникалық құжаттаманы, оның ішінде техникалық тапсырманы киберқауіпсіздік талаптарына сәйкестігі тұрғысынан келіседі;

24) киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасының жұмыс істеу қағидаларын бекітеді;

25) киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институтының

қызметін үйлестіруді жүзеге асырады;

26) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы талаптарды сақтау бөлігінде бұзушылықтарды жою туралы нұсқама немесе акт белгіленген мерзімде орындалмаған жағдайда, субъектіні нұсқамада немесе актіде көрсетілген әрекеттерді жасауға мәжбүрлеу туралы талап қоюды сотқа береді;

27) "цифрлық үкіметтің" веб-порталында дербес деректер субъектілерін жеке кабинеті арқылы хабардар ету мақсатында қауіпсіздігі бұзылған дербес деректерді өңдейді;

27-1) цифрлық оқиғаларды журналға енгізу қағидаларын бекітеді;

27-2) цифрлық оқиғаларды журналға енгізудің бірыңғай платформасының жұмыс істеу қағидаларын бекітеді;

28) осы Заңда, Қазақстан Республикасының өзге де заңдарында, Қазақстан Республикасы Президентінің және Қазақстан Республикасы Үкіметінің актілерінде көзделген өзге де өкілеттіктерді жүзеге асырады.

Ескерту. 2-тарау 7-1-баппен толықтырылды - ҚР 28.12.2017 № 128-VI; жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

7-2-бап. Орталық атқарушы органдар мен Қазақстан Республикасының Президентіне тікелей бағынатын және есеп беретін мемлекеттік органдардың киберқауіпсіздікті қамтамасыз ету саласындағы құзыреті

Орталық атқарушы органдар мен Қазақстан Республикасының Президентіне тікелей бағынатын және есеп беретін мемлекеттік органдар:

1) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың сақталуын қамтамасыз етеді;

2) уәкілетті орган ұсынған кибермәдениеттің базалық қағидаттарының сақталуын қамтамасыз етеді;

2-1) өзінің қызметшілері үшін киберқауіпсіздік және кибермәдениет бойынша жыл сайын профилактикалық іс-шаралар жүргізеді;

3) құзыреті шегінде аса маңызды цифрлық объектілерді реттеу мәселелерін айқындайды, сондай-ақ оларды санаттарға бөлуді жүргізеді;

4) қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті органды, арнаулы мемлекеттік органдарды және Қазақстан Республикасының Қарулы Күштерін қоспағанда, Киберқауіпсіздікті қамтамасыз ету жөніндегі ұлттық үйлестіру орталығының жұмыскерлерін цифрлық объектілерге қол жеткізетін жұмыс орындарымен қамтамасыз етеді;

5) осы Заңда, Қазақстан Республикасының өзге де заңдарында және Қазақстан Республикасы Президентінің актілерінде көзделген өзге де өкілеттіктерді жүзеге асырады.

Орталық атқарушы органдардың құзыреті де Қазақстан Республикасы Үкіметінің актілерінде айқындалады.

Ескерту. 2-тарау 7-2-баппен толықтырылды - ҚР 28.12.2017 № 128-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

7-3-бап. Жергілікті атқарушы органдардың киберқауіпсіздікті қамтамасыз ету саласындағы құзыреті

1. Жергілікті атқарушы органдар:

1) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың, деректерді басқару жөніндегі талаптардың сақталуын қамтамасыз етеді;

2) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың орындалуын мониторингтеуді жүзеге асырады;

3) кибермәдениетті арттыру үшін жағдайлар жасайды;

4) алып тасталды – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

5) аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету бөлігінде цифрландыру саласындағы мемлекеттік бақылауды қоспағанда, тиісті әкімшілік-аумақтық бірлік шегінде жеке кәсіпкерлік субъектілеріне қатысты цифрландыру саласында мемлекеттік бақылауды жүзеге асырады;

6) киберқауіпсіздік саласын дамытуға, оның ішінде инвестициялар тарту арқылы жәрдемдеседі;

7) Қазақстан Республикасының заңнамасында жергілікті атқарушы органдарға жүктелетін өзге де өкілеттіктерді жергілікті мемлекеттік басқару мүддесінде жүзеге асырады.

2. Қазақстан Республикасының Ұлттық архивін және орталық мемлекеттік архивтерді жасақтау көздерін қоспағанда, облыстың, республикалық маңызы бар қаланың және астананың жергілікті атқарушы органдары электрондық құжатқа және электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуына мемлекеттік бақылауды жүзеге асырады.

Ескерту. 2-тарау 7-3-баппен толықтырылды - ҚР 28.12.2017 № 128-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

7-4-бап. Киберқауіпсіздіктің мемлекеттік жедел орталығы

1. Киберқауіпсіздіктің мемлекеттік жедел орталығы:

1) Киберқауіпсіздіктің ұлттық үйлестіру орталығының киберқауіпсіздікті қамтамасыз етуді мониторингтеу жүйесі арқылы "цифрлық үкіметтің" цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүзеге асырады;

2) цифрлық үкіметтің цифрлық объектілерінің киберқауіпсіздік оқиғаларының

мониторингін жүзеге асырады;

3) "цифрлық үкіметтің" цифрлық объектілерінде киберқауіпсіздіктің қатерлері мен оқыс оқиғаларын анықтау, жолын кесу және зерттеу жөніндегі іс-шараларды жүзеге асырады және оларды жою және (немесе) болғызбау жөніндегі ұсынымдарды береді;

4) "цифрлық үкіметтің" цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету, сондай-ақ киберқауіпсіздіктің оқыс оқиғаларына ден қою жөніндегі іс-шараларды үйлестіруді жүзеге асырады;

5) Қазақстан Республикасының Ұлттық қауіпсіздік комитетімен келісу бойынша уәкілетті орган айқындаған тәртіппен "цифрлық үкіметтің" цифрлық объектілері үшін киберқауіпсіздік зерттеушілерімен өзара іс-қимыл жасау бағдарламасын іске асырады;

6) "цифрлық үкімет" операторымен бірлесіп, Қазақстан Республикасының Ұлттық қауіпсіздік комитетімен келісу бойынша уәкілетті орган бекіткен "цифрлық үкімет" платформасының киберқауіпсіздігін қамтамасыз ету регламентіне сәйкес "цифрлық үкімет" платформасының киберқауіпсіздігін қамтамасыз ету жөніндегі іс-шараларды жүзеге асырады;

7) дербес деректерді қорғау саласындағы уәкілетті органды дербес деректер қауіпсіздігінің бұзылғаны туралы ол анықталған кезден бастап үш сағат ішінде хабардар етеді.

2. Киберқауіпсіздіктің мемлекеттік жедел орталығының жұмыскерлері өз қызметінің нәтижесінде алған коммерциялық немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

Ескерту. 2-тарау 7-4-баппен толықтырылды - ҚР 28.12.2017 № 128-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

7-5-бап. Киберқауіпсіздікті қамтамасыз ету орталығы

1. Киберқауіпсіздікті қамтамасыз ету орталығы:

1) киберқауіпсіздікті қамтамасыз ету орталығына қосылған цифрлық объектілердің киберқауіпсіздік қатерлерін анықтау, бағалау, болжау, оқшаулау, бейтараптандыру және олардың алдын алу жөніндегі қызметті жүзеге асырады;

2) киберқауіпсіздік қатерлерін барынша азайту жөнінде шаралар қабылдайды, цифрлық объектінің меншік иесін және (немесе) иегерін, сондай-ақ Киберқауіпсіздіктің ұлттық үйлестіру орталығын киберқауіпсіздіктің оқыс оқиғалары мен қатерлерінің анықталу фактілері туралы дереу хабардар етеді;

3) "цифрлық үкіметтің" цифрлық объектілеріне жатпайтын аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүзеге асырады;

4) киберқауіпсіздіктің салалық орталығымен, Киберқауіпсіздіктің ұлттық үйлестіру орталығымен және киберқауіпсіздікті қамтамасыз етудің басқа да орталықтарымен киберқауіпсіздікті қамтамасыз ету орталығына қосылған цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету үшін қажетті ақпарат алмасуды жүзеге асырады;

5) киберқауіпсіздік оқиғалары мен оның оқыс оқиғалары туралы мәліметтерді жинауды, шоғырландыруды, талдауды және сақтауды жүзеге асырады;

6) аса маңызды цифрлық объектілердің иелеріне және (немесе) иегерлеріне цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету үшін қажетті ақпаратты, оның ішінде киберқауіпсіздік қатерлері, бағдарламалық қамтылымның, құрылғылар мен технологиялардың осалдығы, киберқауіпсіздік қатерлерін іске асыру тәсілдері, киберқауіпсіздіктің оқыс оқиғаларының туындау алғышарттары, сондай-ақ олардың алдын алу және зардаптарын жою әдістері туралы ақпаратты береді;

7) киберқауіпсіздікті қамтамасыз ету орталығына өз қызметін жүзеге асыру шеңберінде белгілі болған, таралуы шектелген мәліметтердің сақталуын қамтамасыз етеді;

8) Киберқауіпсіздіктің ұлттық үйлестіру орталығы үшін киберқауіпсіздікті қамтамасыз ету орталығына қосылған "цифрлық үкіметтің" цифрлық объектілерінің оқиғаларын тіркеу журналдарына қолжетімділікті қамтамасыз етеді;

9) киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасаудың меншікті бағдарламасын жасауға немесе киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасын пайдалану қызметін Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардан сатып алуға құқылы;

10) технологиялық процестерді басқарудың автоматтандырылған жүйелерінің киберқауіпсіздігін қамтамасыз етеді;

11) дербес деректерді қорғау саласындағы уәкілетті органды дербес деректер қауіпсіздігінің бұзылғаны туралы ол анықталған кезден бастап үш сағат ішінде хабардар етеді;

12) дербес деректерді қорғау саласындағы уәкілетті органның келісімімен "цифрлық үкіметтің" веб-порталында дербес деректер субъектілерін жеке кабинет арқылы хабардар ету мақсатында қауіпсіздігі бұзылған дербес деректерді өңдеуге құқылы;

13) деректерді өңдеу орталықтарына ұлттық техникалық аудит жүргізеді;

14) өзінің цифрлық объектілерінде цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың сақталуын қамтамасыз етеді;

15) киберқауіпсіздік аудитін жүргізеді;

16) цифрлық объектілердің, оның ішінде дербес деректерді жинауды және өңдеуді жүзеге асыратын цифрлық объектілердің цифрлық оқиғаларына мониторинг пен журналға енгізуді жүргізеді.

2. Киберқауіпсіздікті қамтамасыз ету орталығы өз қызметін ақпарат таралып кететін техникалық арналарды және жедел-іздестіру іс-шараларын жүргізуге арналған арнаулы техникалық құралдарды анықтау жөніндегі қызметтер көрсетуге арналған лицензия негізінде жүзеге асырады.

3. Киберқауіпсіздікті қамтамасыз ету орталығының жұмыскерлері өз қызметінің нәтижесінде алған коммерциялық немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

4. Осы баптың 2-тармағының талабы киберқауіпсіздікті қамтамасыз ету орталығының функцияларын олардың құрылымдық бөлімшелері жүзеге асыратын Қазақстан Республикасының құқық қорғау және арнаулы мемлекеттік органдарына,

Қазақстан Республикасының екінші деңгейдегі банктеріне қолданылмайды.

Ескерту. 2-тарау 7-5-баппен толықтырылды - ҚР 03.07.2019 № 262-VI (қолданысқа енгізілу тәртібін 2-баптан қараңыз); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

7-6-бап. Электрондық өнеркәсіп саласындағы уәкілетті органның құзыреті

Ескерту. 7-6-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

7-7-бап. Киберқауіпсіздіктің компьютерлік оқыс оқиғаларына ден қою жөніндегі ұлттық қызмет

1. Киберқауіпсіздіктің компьютерлік оқыс оқиғаларына ден қою жөніндегі ұлттық қызмет:

1) Қазақстан Республикасының заңнамасында белгіленген тәртіппен киберқауіпсіздікті қамтамасыз ету жөніндегі бірлескен іс-шараларды жүргізе отырып, "цифрлық үкіметтің" цифрлық объектілерінің, Интернеттің қазақстандық сегментінің, сондай-ақ аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету, қорғау және олардың қауіпсіз жұмыс істеуін мониторингтеу, киберқауіпсіздіктің оқыс оқиғаларына ден қою мәселелері бойынша салааралық үйлестіруді жүзеге асырады;

2) киберқауіпсіздікті қамтамасыз ету мәселелері бойынша цифрлық объектілердің меншік иелеріне, иегерлеріне және пайдаланушыларына жәрдемдеседі;

3) дербес деректерді қорғау саласындағы уәкілетті органды дербес деректер қауіпсіздігінің бұзылғаны туралы ол анықталған кезден бастап үш сағат ішінде хабардар етеді.

2. Киберқауіпсіздіктің компьютерлік оқыс оқиғаларына ден қою жөніндегі ұлттық қызметтің жұмыскерлері өз қызметінің нәтижесінде алған коммерциялық немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

Ескерту. 7-7-баппен толықтырылды - ҚР 14.07.2022 № 141-VII (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңдарымен.

7-8-бап. Киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметі

1. Киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметі:

1) киберқауіпсіздіктің оқыс оқиғалары және киберқауіпсіздіктің өзекті қатерлері туралы ақпаратты жинауды және талдауды жүзеге асырады, сондай-ақ оларды жою жөнінде ұсынымдар береді;

2) киберқауіпсіздік қатерлеріне қарсы іс-қимылға бағытталған ұсынымдар әзірлейді;

3) цифрлық объектілердің меншік иелері мен иегерлерін, сондай-ақ Киберқауіпсіздіктің ұлттық үйлестіру орталығын белгілі болған киберқауіпсіздіктің оқыс оқиғалары мен қатерлері туралы хабардар етеді;

4) киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасаудың меншікті

бағдарламасын жасауға немесе киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасын пайдалану қызметін Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардан сатып алуға құқылы;

5) дербес деректерді қорғау саласындағы уәкілетті органды дербес деректер қауіпсіздігінің бұзылғаны туралы ол анықталған кезден бастап үш сағат ішінде хабардар етеді;

6) өзінің цифрлық объектілерінде цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың сақталуын қамтамасыз етеді.

2. Киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметі өз қызметін ақпарат таралып кететін техникалық арналарды және жедел-іздестіру іс-шараларын жүргізуге арналған арнаулы техникалық құралдарды анықтау жөніндегі қызметтер көрсетуге арналған лицензия негізінде жүзеге асырады.

3. Киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметінің жұмыскерлері өз қызметінің нәтижесінде алған коммерциялық немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

4. Осы баптың 2-тармағының талабы киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметінің функцияларын олардың құрылымдық бөлімшелері жүзеге асыратын Қазақстан Республикасының екінші деңгейдегі банктеріне қолданылмайды.

Ескерту. 7-8-баппен толықтырылды - ҚР 14.07.2022 № 141-VII (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңдарымен.

8-бап. Сарапшылық кеңес

Ескерту. 8-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

9-бап. Киберқауіпсіздіктің ұлттық үйлестіру орталығы

1. Киберқауіпсіздіктің ұлттық үйлестіру орталығы:

1) киберқауіпсіздіктің салалық орталықтары мен киберқауіпсіздікті қамтамасыз ету орталықтарының "цифрлық үкіметтің" цифрлық объектілеріндегі және аса маңызды цифрлық объектілердегі киберқауіпсіздіктің оқыс оқиғалары туралы ақпаратын жинауды, талдауды және қорытуды жүзеге асырады;

2) Киберқауіпсіздіктің компьютерлік оқыс оқиғаларына ден қою жөніндегі ұлттық қызметтің міндеттері мен функцияларын іске асырады;

3) Киберқауіпсіздіктің мемлекеттік жедел орталығының міндеттері мен функцияларын іске асырады;

4) дербес деректерді қорғау саласындағы уәкілетті органды дербес деректер қауіпсіздігінің бұзылғаны туралы ол анықталған кезден бастап үш сағат ішінде хабардар етеді.

2. Киберқауіпсіздіктің ұлттық үйлестіру орталығының жұмыскерлері өз қызметінің нәтижесінде алған коммерциялық немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

Ескерту. 9-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

9-1-бап. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы лицензиялау

Ескерту. 9-1-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

10-бап. Киберқауіпсіздіктің салалық орталығы

1. Киберқауіпсіздіктің салалық орталығы мемлекеттік реттеудің тиісті саласының (аясының) цифрлық объектілері меншік иелерінің немесе иегерлерінің киберқауіпсіздікті қамтамасыз етуін ұйымдастырады және үйлестіреді, оның ішінде:

1) ұйымдардың киберқауіпсіздігі қатерлерін талдау, бағалау, болжау және олардың алдын алу жөніндегі қызметті жүзеге асырады;

2) Киберқауіпсіздіктің ұлттық үйлестіру орталығымен киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасуды жүзеге асырады;

3) тиісті саланың (аяның) цифрлық объектілерінің меншік иелерінен немесе иегерлерінен келіп түскен киберқауіпсіздіктің оқиғалары мен оқыс оқиғалары туралы мәліметтерді жинауды, шоғырландыруды, талдауды және сақтауды жүзеге асырады;

4) тиісті саланың (аяның) цифрлық объектілерінің меншік иелеріне немесе иегерлеріне киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпаратты, оның ішінде киберқауіпсіздік қатерлері, тиісті саланың (аяның) цифрлық объектілеріндегі осалдық, киберқауіпсіздіктің оқыс оқиғаларының туындау алғышарттары, сондай-ақ олардың алдын алу және зардаптарын жою әдістері туралы ақпаратты береді;

5) киберқауіпсіздіктің салалық орталығына өз қызметін жүзеге асыру шеңберінде белгілі болған таралуы шектелген мәліметтердің сақталуын қамтамасыз етеді;

6) дербес деректерді қорғау саласындағы уәкілетті органды дербес деректер қауіпсіздігінің бұзылғаны туралы ол анықталған кезден бастап үш сағат ішінде хабардар етеді;

7) технологиялық процестерді басқарудың автоматтандырылған жүйелерінің және аса маңызды цифрлық объектілердің құрамына кіретін технологиялық процестерді басқару жүйелерінің киберқауіпсіздігін қамтамасыз етуді киберқауіпсіздіктің салалық орталығы қызметінің ішкі регламенттерінде белгіленген тәртіппен және мерзімдерде үйлестіреді;

8) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптар негізінде мемлекеттік реттеудің тиісті саласында (аясында) киберқауіпсіздікті қамтамасыз ету жөніндегі қосымша талаптарды әзірлейді.

2. Киберқауіпсіздіктің салалық орталығының жұмыскерлері өз қызметінің нәтижесінде алған коммерциялық құпияны, банк құпиясын немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

3. Киберқауіпсіздіктің салалық орталығы өз функцияларын жүзеге асыру үшін киберқауіпсіздіктің оқиғалары мен оқыс оқиғалары бойынша ақпаратты жинау, өңдеу және алмасу жөніндегі цифрлық объектіні пайдаланады, оны салалық ұйымдардың қосу және пайдалану тәртібін мемлекеттік реттеудің тиісті саласының

(аясының) уәкілетті органы айқындайды.

Ескерту. 10-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

11-бап. Ақпараттық-коммуникациялық технологиялар саласындағы ұлттық даму институты

Ескерту. 11-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

12-бап. "Электрондық үкіметтің" сервистік интеграторы

Ескерту. 12-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

13-бап. Оператор

Ескерту. 13-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

13-1-бап. "Астана Хаб" халықаралық технологиялық паркі

Ескерту. 13-1-бап алып тасталды – ҚР 27.09.2025 № 220-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) Заңымен.

13-2-бап. Ұлттық жасанды интеллект платформасы операторының құзыреті

Ескерту. 13-2-бап алып тасталды – ҚР 17.11.2025 № 231-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

13-3-бап. Деректерді өңдеу орталығы

Ескерту. 13-3-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

13-4-бап. Бұлттық есептеулер

Ескерту. 13-4-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

13-5-бап. Хостинг-провайдер

1. Хостинг-провайдер Киберқауіпсіздіктің ұлттық үйлестіру орталығымен ақпараттық өзара іс-қимыл жасауды қамтамасыз етеді.

Хостинг-провайдер Киберқауіпсіздіктің ұлттық үйлестіру орталығынан өзінің цифрлық инфрақұрылымында орналастырылған интернет-ресурстағы киберқауіпсіздіктің анықталған оқыс оқиғасы және (немесе) осалдық туралы хабарлама алған кезде бұл туралы ақпаратты осы интернет-ресурстың меншік иесіне немесе иеленушісіне дереу жіберуге міндетті.

2. Хостинг-провайдер Қазақстан Республикасының телекоммуникация желілерін орталықтандырылған басқару жүйесінің жұмыс істеу қағидаларын сақтауды ескере отырып, өзінің цифрлық инфрақұрылымында орналастырылған үшінші тұлғалардың интернет-ресурстарына Қазақстан Республикасының телекоммуникация желілері арқылы қолжетімділік береді.

3. Хостинг-провайдерлер өздерінің цифрлық инфрақұрылымын киберқауіпсіздік қатерлері мен тәуекелдерінен қорғауды қамтамасыз етеді.

Ескерту. 13-5-баппен толықтырылды – ҚР 24.06.2026 № 326-VIII (алғашқы ресми

жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

14-бап. Мемлекеттік техникалық қызмет

1. Мемлекеттік техникалық қызмет цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларында мемлекеттік монополияға жатқызылған мынадай қызмет түрлерін жүзеге асырады:

1) Интернетке қол жеткізудің бірыңғай шлюзінің және "цифрлық үкіметтің" электрондық поштасы бірыңғай шлюзінің жұмыс істеуін қамтамасыз етеді;

2) "цифрлық үкіметтің" цифрлық объектілерінің киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізеді;

3) инвестициялық ұсынысқа және бюджеттік инвестициялардың қаржы-экономикалық негіздемесіне және "цифрлық үкіметтің" цифрлық объектісін құруға немесе дамытуға арналған техникалық тапсырмаға киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сараптама жүргізеді;

4) интернет-ресурстардың мониторингін, сондай-ақ Интернеттің қазақстандық сегменті кеңістігінде домендік атаулар жүйесінің жұмыс істеуіне мониторингті жүзеге асырады;

5) Киберқауіпсіздіктің ұлттық үйлестіру орталығының міндеттері мен функцияларын іске асырады;

6) Ұлттық бейнемониторинг жүйесіне қол жеткізу құқықтарын әкімшілендіруді, оның жұмыс істеуін мониторингтеуді және киберқауіпсіздігін қамтамасыз ету мониторингін жүзеге асырады;

7) цифрлық объектілерде қамтылған дербес деректерді сақтау, өңдеу және тарату процестерінің қорғалуын қамтамасыз етуді зерттеп-қарауды жүзеге асырады;

8) Киберқауіпсіздіктің ұлттық үйлестіру орталығының цифрлық объектілерінің жұмыс істеуін қамтамасыз етеді;

9) цифрлық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасының жұмыс істеуін қамтамасыз етеді, уәкілетті орган айқындайтын тәртіппен аса маңызды цифрлық объектілердің цифрлық ресурстарын резервтік көшірудің кезеңділігін белгілейді;

10) цифрландыру саласында киберқауіпсіздікті қамтамасыз ету бөлігінде мемлекеттік бақылауды жүзеге асыруға қатысады;

11) Бастапқы кодтардың ұлттық репозиторийін пайдалану қызметтерін ұсынады;

12) "цифрлық үкіметтің" цифрлық объектілерінде және аса маңызды цифрлық объектілерде пайдаланылатын ақпаратты криптографиялық қорғау құралдарының киберқауіпсіздік талаптарына сәйкестігін техникалық куәландыруды жүргізеді;

13) цифрлық оқиғаларды журналға енгізудің бірыңғай платформасын пайдалану қызметін ұсынады.

1-1. Мемлекеттік мүлік жөніндегі уәкілетті орган ұлттық қауіпсіздік органдарымен келісу бойынша киберқауіпсіздікті қамтамасыз етуге арналған, мемлекеттің меншігі болып саналатын және Қазақстан Республикасының ұлттық қауіпсіздік органдарының басқаруындағы цифрлық объектілерді "Мемлекеттік мүлік туралы" Қазақстан Республикасының Заңына сәйкес мемлекеттік техникалық қызметке

өтеусіз пайдалануға беруге құқылы.

2. Осы баптың 1-тармағында көрсетілген, мемлекеттік техникалық қызмет өндіретін және (немесе) өткізетін тауарлардың (орындалатын жұмыстардың, көрсетілетін қызметтердің) бағаларын монополияға қарсы органмен келісу бойынша Қазақстан Республикасының Ұлттық қауіпсіздік комитеті белгілейді.

Ескерту. 14-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

14-1-бап. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институты

Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институты:

1) киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік саясатты іске асыруға қатысады;

2) киберқауіпсіздікті қамтамасыз ету саласындағы стандарттау жөніндегі құжаттарды әзірлейді;

3) киберқауіпсіздікті қамтамасыз ету саласындағы ғылыми-техникалық қызметті жүзеге асырады;

4) киберқауіпсіздікті қамтамасыз ету саласындағы жобалардың ғылыми-техникалық сараптамасын жүргізеді;

5) киберқауіпсіздікті қамтамасыз ету саласында даярлауды, қайта даярлауды және біліктілікті арттыруды жүзеге асырады.

Ескерту. 2-тарау 14-1-баппен толықтырылды - ҚР 28.12.2017 № 128-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңдарымен.

15-бап. Бірыңғай байланыс орталығы

Ескерту. 15-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

3-тарау. Киберқауіпсіздікті қамтамасыз ету саласындағы цифрлық объектілердің меншік иелерінің және иегерлерінің құқықтары мен міндеттері, аса маңызды цифрлық объектілердің меншік иесінің және (немесе) иегерінің міндеттері

Ескерту. 3-тараудың тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

16-бап. Цифрлық объектілердің меншік иелерінің құқықтары мен міндеттері

1. Цифрлық объектілердің меншік иесі:

1) цифрлық объектілерді жалға, сенімгерлік басқаруға, шаруашылық жүргізуге немесе жедел басқаруға беруге және оларға өзге де түрде билік етуге;

2) өз құзыреті шегінде цифрлық объектілерді өңдеу, қорғау және оларға қол жеткізу режимі мен қағидаларын белгілеуге;

3) цифрлық объектілерді сақтау, көшіру және тарату кезінде оларға билік ету

шарттарын айқындауға;

4) цифрлық объектілерді иелену және пайдалану шарттарын айқындауға;

5) осы Заңда және Қазақстан Республикасының заңдарында белгіленген өзге де құқықтарды пайдалануға құқылы.

2. Цифрлық объектілердің меншік иесі:

1) цифрлық объектілердің киберқауіпсіздігін қамтамасыз етуге;

2) осы Заңға және Қазақстан Республикасының өзге де заңдарына сәйкес цифрлық ресурстар мен цифрлық инфрақұрылым объектілеріне қолжетімділікті таратуға, беруге, шектеуге немесе оған тыйым салуға;

3) осы Заңға және Қазақстан Республикасының өзге де заңдарына сәйкес өзге де міндеттерді орындауға міндетті.

3. Дербес деректерді қамтитын цифрлық объектінің меншік иесі Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасында көзделген шараларды қабылдауға міндетті.

4. Цифрлық объектінің меншік иесі өзіне тиесілі цифрлық объектілерде орналастырылған цифрлық ресурстардың сақталу қауіпсіздігі және қорғалуы үшін цифрлық ресурстардың меншік иесінің және (немесе) иегерінің алдында жауапты болады.

Ескерту. 16-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

17-бап. Цифрлық объектілердің иегерінің құқықтары мен міндеттері

1. Цифрлық объектінің иегері:

1) цифрлық объектілерді меншік иесі айқындаған шарттарда иеленуге және пайдалануға;

2) осы тармақтың 1) тармақшасына сәйкес цифрлық объектілерге қол жеткізу және пайдалану шарттарын айқындауға;

3) цифрлық жүйеде цифрлық ресурстарды өңдеу шарттарын айқындауға;

4) осы Заңда және Қазақстан Республикасының заңдарында белгіленген өзге де құқықтарды пайдалануға құқылы.

2. Цифрлық объектілердің иегері:

1) цифрлық объектілердің киберқауіпсіздігін қамтамасыз етуге;

2) цифрлық объектілердің меншік иесінің және үшінші тұлғалардың құқықтарын, бостандықтары мен заңды мүдделерін сақтауға;

3) осы Заңға және Қазақстан Республикасының өзге де заңдарына сәйкес өзге де міндеттерді орындауға міндетті.

3. Дербес деректер қамтылған цифрлық объектінің иегері Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасында көзделген шараларды қабылдауға міндетті.

4. Цифрлық объектінің иегері өзіне тиесілі объектілерде орналастырылған цифрлық ресурстардың, цифрлық объектілердің сақталу қауіпсіздігі және қорғалуы үшін

цифрлық ресурстардың, цифрлық объектілердің меншік иесінің және (немесе) иегерінің алдында жауапты болады.

Ескерту. 17-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

18-бап. Аса маңызды цифрлық объектілердің меншік иесінің және (немесе) иегерінің міндеттері

1. Аса маңызды цифрлық объектілердің меншік иесі немесе иегері:

1) өзінің киберқауіпсіздікті қамтамасыз етудің меншікті орталығын құруға және оның жұмыс істеуін қамтамасыз етуге немесе киберқауіпсіздікті қамтамасыз ету орталығы көрсететін қызметтерді Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардан киберқауіпсіздікті қамтамасыз ету орталығының көрсетілетін қызметтерінің сатып алуға міндетті көлемдерінің (жиынтықтарының) және олардың сипаттамаларының тізбесінде белгіленген көлемде (жиынтықта) сатып алуға;

2) "цифрлық үкіметтің" цифрлық объектілері болып табылатын аса маңызды цифрлық объектілер үшін цифрлық оқиғаларды журналға енгізу жүйелерін Киберқауіпсіздіктің ұлттық үйлестіру орталығының және цифрлық оқиғаларды журналға енгізудің бірыңғай платформасының киберқауіпсіздікті қамтамасыз етуді мониторингтеу жүйесінің техникалық құралдарына дербес немесе Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардың көрсететін қызметтерін сатып алу арқылы қосуды қамтамасыз етуге;

3) егер Қазақстан Республикасының заңдарында өзгеше белгіленбесе, "цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларында айқындалған тәртіппен және мерзімдерде, аса маңызды цифрлық объектілер қосылған Киберқауіпсіздікті ұлттық үйлестіру орталығы мен киберқауіпсіздікті қамтамасыз ету орталығын дербес анықталған киберқауіпсіздіктің оқыс оқиғалары туралы хабардар етуге;

4) егер Қазақстан Республикасының заңдарында өзгеше белгіленбесе, уәкілетті орган айқындаған тәртіппен және мерзімдерде цифрлық ресурстардың резервтік көшірмелерін цифрлық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беруді жүзеге асыруға;

5) жыл сайын өзінің барлық жұмыскері үшін киберқауіпсіздік және кибермәдениет бойынша оқытуды жүргізуге міндетті.

Цифрлық ресурстың меншік иесін немесе иегерін қоспағанда, цифрлық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасында сақталатын цифрлық ресурстардың көшірмесіне қол жеткізуге тыйым салынады.

2. Заңмен қорғалатын құпияны қамтитын деректерді өңдейтін аса маңызды цифрлық объектілердің меншік иесі және (немесе) иегері жылына бір реттен сиретпей киберқауіпсіздік аудитін жүргізеді. Екінші деңгейдегі банктердің киберқауіпсіздік аудиті Қазақстан Республикасының банк заңнамасының талаптарына сәйкес жүргізіледі.

Ескерту. 18-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 №

326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

18-1-бап. Зияткерлік робот меншік иесінің және иеленушісінің құқықтары мен міндеттері

Ескерту. 18-1-бап алып тасталды – ҚР 17.11.2025 № 231-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

18-2-бап. Қазақстан Республикасының аумағында шетелдік онлайн-платформаның және лездік хабарлар алмасу сервисінің қызметі

Ескерту. 3-тарау 18-2-баппен толықтырылды – ҚР 03.05.2022 № 118-VII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен; алып тасталды - ҚР 10.07.2023 № 19-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

19-бап. Электрондық нысанда көрсетілетін қызметтердің түрлері

Ескерту. 19-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

20-бап. Электрондық нысанда қызметтер көрсету кезінде мәліметтер ұсыну

Ескерту. 20-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

20-1-бап. Жай электрондық қолтаңбаны пайдалану

1. Жай электрондық қолтаңба кодтарды, парольдерді немесе өзге де сәйкестендіру құралдарын пайдалану арқылы адамның қолтаңбасын растаудың электрондық-цифрлық түрі болып табылады.

2. Жеке кәсіпкерлік субъектілері шетелдіктермен, шетелдік заңды тұлғалармен, шетелдік қатысуы бар заңды тұлғалармен өзара іс-қимыл жасау кезінде жай электрондық қолтаңбаны пайдалануға құқылы.

3. Қазақстан Республикасының заңнамасына сәйкес нотариаттық куәландыруға немесе міндетті мемлекеттік тіркеуге жататын мәмілелерді және тізбесін уәкілетті орган бекітетін мәмілелерді қоспағанда, мынадай жағдайлар орындалған кезде:

1) мәміле тараптары арасында өзара мәмілелер жасау кезінде жай электрондық қолтаңбаны пайдалану туралы жазбаша нысанда келісімге қол жеткізілсе;

2) мәміле тараптары жазбаша нысандағы өзара келісіммен жай электрондық қолтаңба арқылы өзара жасалған мәмілелердің түпнұсқалығы мен жарамдылығын таныса, мәмілелерге қол қоюға өкілеттігі бар тұлғаның жай электрондық қолтаңбасы арқылы куәландырылған мәмілелердің қол қойылған қағаз жеткізгіштердегі құжаттармен мәні бірдей болады.

Осы баптың талаптары пилоттық жоба шеңберінде 2026 жылғы 1 шілдеге дейін қолданылады.

Ескерту. 3-тарау 20-1-баппен толықтырылды – ҚР 21.05.2024 № 86-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

Ескерту. 2-бөлімнің тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

4-тарау. Киберқауіпсіздікті қамтамасыз ету субъектілері мен объектілері

Ескерту. 4-тараудың тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

21-бап. "Электрондық үкіметтің" жұмыс істеуі

Ескерту. 21-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

22-бап. "Электрондық үкімет" архитектурасы

Ескерту. 22-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

23-бап. Мемлекеттік органның архитектурасы

Ескерту. 23-бап алып тасталды – ҚР 14.07.2022 № 141-VII (01.01.2023 бастап қолданысқа енгізіледі) Заңымен.

24-бап. "Электрондық әкімдіктің" үлгілік архитектурасы

Ескерту. 24-бап алып тасталды – ҚР 14.07.2022 № 141-VII (01.01.2023 бастап қолданысқа енгізіледі) Заңымен.

25-бап. Мемлекеттік функцияларды автоматтандыру және олардан туындайтын мемлекеттік қызметтерді көрсету

Ескерту. 25-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

26-бап. "Электрондық үкіметтің" ақпараттық-коммуникациялық платформасы

Ескерту. 26-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

27-бап. "Электрондық үкіметтің" веб-порталы

Ескерту. 27-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

28-бап. "Электрондық үкіметтің" төлем шлюзі

Ескерту. 28-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

28-1-бап. Киберқауіпсіздікті зерттеуші

1. Киберқауіпсіздікті зерттеуші:

1) цифрлық объектінің меншік иесі және (немесе) иегері белгілеген шекараларда осалдықты іздеуді жүзеге асырады;

2) анықталған осалдық сипатталған есепті ұсынады;

3) цифрлық объектілердің меншік иелерін және (немесе) иегерлерін анықталған осалдық туралы хабардар етеді;

4) анықталған осалдық туралы мәліметтерді ол толық жойылғанға дейін және цифрлық объектінің меншік иесі және (немесе) иегері тарапынан ресми рұқсат берілгенге дейін ашпайды;

5) анықталған осалдықты жеке немесе заңсыз мақсаттарда пайдаланбайды;

6) осалдықты іздеу кезінде цифрлық объектінің штаттық жұмыс істеуін бұзбайды.

2. Киберқауіпсіздікті зерттеуші өз қызметінің нәтижесінде алған коммерциялық

немесе заңмен қорғалатын өзге де құпияны жария еткені үшін Қазақстан Республикасының заңдарына сәйкес жауапты болады.

Ескерту. 28-1-баппен толықтырылды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

28-2-бап. Киберқауіпсіздікті қамтамасыз ету саласындағы лицензиялау

1. Киберқауіпсіздікті қамтамасыз ету саласындағы қызмет Қазақстан Республикасының рұқсаттар және хабарламалар туралы заңнамасында белгіленген тәртіппен лицензиялауға жатады.

2. Киберқауіпсіздікті қамтамасыз ету саласындағы лицензиаттар лицензиарға есептерді, хабарламаларды, тізбені ұсынады, олардың нысандары мен кезеңділігін біліктілік талаптары шеңберінде лицензиар айқындайды.

Ескерту. 28-2-баппен толықтырылды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

29-бап. Мемлекеттік органдардың бірыңғай көліктік ортасы

1. Мемлекеттік органдардың бірыңғай көліктік ортасы – "цифрлық үкіметтің" инфрақұрылымына кіретін және мемлекеттік органдардың, олардың ведомстволық бағынысты ұйымдары мен жергілікті өзін-өзі басқару органдарының, сондай-ақ уәкілетті орган айқындаған өзге де цифрлық орта субъектілерінің оқшау (Интернетке қолжетімділігі бар оқшау желілерді қоспағанда), ведомстволық және корпоративтік телекоммуникация желілерінің өзара іс-қимыл жасауын киберқауіпсіздіктің қажетті деңгейін сақтай отырып қамтамасыз етуге арналған телекоммуникациялар желісі.

2. Мемлекеттік органдар, олардың ведомстволық бағынысты ұйымдары және жергілікті өзін-өзі басқару органдары, сондай-ақ уәкілетті орган айқындаған цифрлық ортаның өзге де субъектілері оқшау (Интернетке қолжетімділігі бар оқшау желілерді қоспағанда), ведомстволық және корпоративтік желілердің өзара іс-қимыл жасауы үшін тек қана мемлекеттік органдардың бірыңғай көліктік ортасын пайдалануға міндетті.

3. Киберқауіпсіздікті қамтамасыз ету мақсатында мемлекеттік органдардың бірыңғай көліктік ортасына, жалпыға ортақ пайдаланылатын телекоммуникация желілеріне және басқа да телекоммуникация желілеріне қосылған оқшау, ведомстволық және корпоративтік желілерді қосу цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарға сәйкес жүзеге асырылады.

Ескерту. 29-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

30-бап. Интернетке қол жеткізудің бірыңғай шлюзі және "цифрлық үкіметтің" электрондық поштасының бірыңғай шлюзі

1. Мемлекеттік органдардың, жергілікті өзін-өзі басқару органдарының, мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, сондай-ақ аса маңызды цифрлық объектілердің меншік иелерінің немесе иегерлерінің цифрлық объектілерін Интернетке қосуды байланыс операторлары Интернетке қол жеткізудің бірыңғай шлюзі арқылы жүзеге асырады.

1-1. Байланыс операторларының уәкілетті орган айқындайтын тәртіппен Интернет

желісіне қол жеткізудің бірыңғай шлюзіне қосылу үшін өздерінің техникалық құралдарын (аппараттық-бағдарламалық кешендерін) пайдалануға құқығы бар.

Мұндай техникалық құралдарды басқару мемлекеттік техникалық қызметке беріледі.

2. Мемлекеттік органдар мен жергілікті өзін-өзі басқару органдарының цифрлық объектілерін Интернетке қосу цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарға сәйкес жүзеге асырылады.

3. Қазақстан Республикасының арнаулы мемлекеттік, құқық қорғау органдары және Қазақстан Республикасы Қорғаныс министрлігінің әскери барлау органдары жедел мақсаттарда, Қазақстан Республикасының Ұлттық Банкі Интернетке қол жеткізудің бірыңғай шлюзін пайдаланбай Интернетке қосуды ұйымдастыруы мүмкін.

Қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті орган киберқауіпсіздіктің салалық орталығының функцияларын іске асыруды ескере отырып, Интернетке қол жеткізудің бірыңғай шлюзін пайдаланбай Интернетке қосылуды ұйымдастыруы мүмкін.

4. Мемлекеттік органдар мен аса маңызды цифрлық объектілердің меншік иелері және (немесе) иегерлері электрондық поштасының өзге тұлғалардың сыртқы электрондық поштасымен электрондық өзара іс-қимыл жасауы электрондық хабарларды "цифрлық үкіметтің" электрондық поштасының бірыңғай шлюзі арқылы қайта бағыттау арқылы жүзеге асырылады.

Ескерту. 30-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

30-1-бап. Ұлттық бейнемониторинг жүйесі

1. Ұлттық бейнемониторинг жүйесі – ұлттық қауіпсіздік пен қоғамдық тәртіпті қамтамасыз ету міндеттерін шешу үшін бейнекескіндерді жинауды, өңдеуді және сақтауды жүзеге асыратын бағдарламалық және техникалық құралдардың жиынтығын білдіретін цифрлық жүйе.

2. Осы баптың 1-тармағында көзделмеген міндеттерді шешу үшін Ұлттық бейнемониторинг жүйесі арқылы алынған мәліметтерді пайдалануға жол берілмейді.

3. Мыналар Ұлттық бейнемониторинг жүйесіне міндетті түрде қосылуға жататын объектілердің санаттары болып табылады:

1) орталық мемлекеттік және жергілікті атқарушы органдардың бейнебақылау жүйелері;

2) террористік тұрғыдан осал объектілерді бейнебақылау жүйелері;

3) қоғамдық және жол қауіпсіздігін бейнебақылау жүйелері;

4) объектінің меншік нысанына қарамастан, қоғамдық орындарда, азаматтар көп болатын орындарда және халықтың еркін баруына қолжетімді объектілерде орнатылған бейнебақылау жүйелері.

3-1. Ұлттық бейнемониторинг жүйесінің қатысушылары – оның үйлестірушісі, операторы, әкімшісі, пайдаланушылары мен абоненттері.

4. Қазақстан Республикасының арнаулы мемлекеттік органдары, құқық қорғау органдары, Қазақстан Республикасының Төтенше жағдайлар министрлігі және жергілікті атқарушы органдар Ұлттық бейнемониторинг жүйесін пайдаланушылар болып табылады.

Ұлттық бейнемониторинг жүйесінің жұмыс істеуі нәтижесінде алынған мәліметтер Қазақстан Республикасының заңдарында белгіленген жағдайларда өзге де мемлекеттік органдарға берілуі мүмкін.

5. Ұлттық бейнемониторинг жүйесінің жұмыс істеу қағидаларын Қазақстан Республикасының Ұлттық қауіпсіздік комитеті бекітеді.

6. Қазақстан Республикасының Үкіметі айқындайтын мемлекеттік орган немесе дауыс беретін акцияларының (жарғылық капиталға қатысу үлестерінің) елу пайызынан астамы мемлекетке тиесілі заңды тұлға Ұлттық бейнемониторинг жүйесінің операторы болып саналады.

7. Ұлттық бейнемониторинг жүйесінің операторы Ұлттық бейнемониторинг жүйесін жасайды әрі дамытады және оның жұмыс істеуін қамтамасыз етеді, сондай-ақ Ұлттық бейнемониторинг жүйесін пайдалану қызметін ұсынады.

Ұлттық бейнемониторинг жүйесін пайдалану Қазақстан Республикасының арнаулы мемлекеттік органдарына, құқық қорғау органдарына және Төтенше жағдайлар министрлігіне өтеусіз негізде беріледі.

8. Ұлттық бейнемониторинг жүйесінің жұмыс істеуін қамтамасыз ету мыналарды қамтиды:

Ұлттық бейнемониторинг жүйесінің бағдарламалық қамтылымына, байланыс арналары мен техникалық құралдарына жүйелік-техникалық қызмет көрсету мен сүйемелдеу;

Ұлттық бейнемониторинг жүйесінде деректердің сақталуын қамтамасыз ету;

Ұлттық бейнемониторинг жүйесінің тоқтаусыз және үздіксіз жұмысын қамтамасыз ету үшін кезекші қызметтің тәулік бойы жұмыс істеуін қамтамасыз ету.

Ескерту. 4-тарау 30-1-баппен толықтырылды - ҚР 25.06.2020 № 347-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

30-2-бап. Цифрлық оқиғаларды журналға енгізу

1. Цифрлық оқиғаларды журналға енгізу цифрлық оқиғалар журналдарын жинау, есепке алу мен сақтау және олардың өзгермеуі арқылы қамтамасыз етіледі.

2. Цифрлық оқиғаларды журналға енгізу мемлекеттік органдардың цифрлық объектілерінде және мемлекеттік органдар өз қызметін цифрландыру үшін пайдаланатын өзге де тұлғалардың цифрлық объектілерінде артықшылықты құқықтары бар пайдаланушылардың іс-әрекеттері нәтижесінде туындайтын цифрлық оқиғалар журналдарын мониторингтеуді, талдауды және сақтауды қамтамасыз ету үшін пайдаланылады.

3. Цифрлық оқиғаларды журналға енгізуді жүзеге асыру тәртібін уәкілетті орган

айқындайды.

Ескерту. 30-2-баппен толықтырылды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

31-бап. "Электрондық үкіметтің" архитектуралық порталы

Ескерту. 31-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

Ескерту. 5-тараудың тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

32-бап. Электрондық ақпараттық ресурстардың түрлері

Ескерту. 32-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

33-бап. Электрондық ақпараттық ресурстардың құқықтық режимі

Ескерту. 33-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

33-1-бап. Цифрлық активтер айналымының құқықтық режимі

Ескерту. 33-1-бап алып тасталды – ҚР 06.02.2023 № 194-VII (01.04.2023 бастап қолданысқа енгізіледі) Заңымен.

34-бап. Электрондық ақпараттық ресурстарды қалыптастыру және пайдалану

Ескерту. 34-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

35-бап. Электрондық ақпараттық ресурстарға қолжетімділік

Ескерту. 35-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

36-бап. Дербес деректерді қамтитын электрондық ақпараттық ресурстар

Ескерту. 36-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

6-тараудың тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

37-бап. Ақпараттық жүйелердің түрлері

Ескерту. 37-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

38-бап. "Цифрлық үкіметтің" цифрлық объектісіне қойылатын киберқауіпсіздік талаптары

1. "Цифрлық үкіметтің" цифрлық объектісі Қазақстан Республикасының заңнамасына, Қазақстан Республикасының аумағында қолданылатын стандарттарға, "цифрлық үкіметтің" цифрлық объектісінің өмірлік циклiне сәйкес және мыналарды:

1) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарды;

2) "цифрлық үкімет" архитектурасын, сондай-ақ деректерді басқару жөніндегі талаптарды;

3) "цифрлық үкіметтің" басқа да цифрлық объектілерімен интеграциялануын (қажет болған жағдайда);

4) "цифрлық үкіметтің" цифрлық объектісінің Киберқауіпсіздіктің ұлттық үйлестіру орталығының киберқауіпсіздік оқиғаларын мониторингтеу жүйесімен және цифрлық оқиғаларды журналға енгізудің бірыңғай платформасымен цифрлық өзара іс-қимыл жасауын;

5) киберқауіпсіздікті қамтамасыз етудің меншікті орталығын құруды және оның жұмыс істеуін қамтамасыз етуді немесе киберқауіпсіздікті қамтамасыз ету орталығының көрсетілетін қызметтерінің сатып алуға міндетті көлемдерінің (жиынтықтарының) және олардың сипаттамаларының тізбесінде белгіленген көлемде (жиынтықта) киберқауіпсіздікті қамтамасыз ету орталығы көрсететін қызметтерді Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардан сатып алуды;

6) еркін бағдарламалық қамтылымның басымдығын;

7) сыныптауышқа сәйкес сынып беруді;

8) мүмкіндігі шектеулі пайдаланушыларға қолжетімділікті қамтамасыз етуді ескере отырып құрылады, пайдаланылады және дамытылады.

2. Мемлекеттік цифрлық ресурстарды қалыптастыруға арналған мемлекеттік заңды тұлғаның цифрлық жүйесі және мемлекеттік емес цифрлық жүйе Қазақстан Республикасының заңнамасына, Қазақстан Республикасының аумағында қолданылатын стандарттарға, цифрлық жүйенің өмірлік цикліне сәйкес және мынадай талаптар:

1) уәкілетті органмен және цифрландыру саласындағы уәкілетті органмен келісілген техникалық тапсырманың;

2) киберқауіпсіздік талаптарына сәйкестігіне сынаудың оң нәтижелері бар хаттамалары алынған;

3) мемлекеттік органның цифрлық жүйесі өнеркәсіптік пайдалануға енгізілген "цифрлық үкіметтің" сыртқы шлюзі арқылы ғана мемлекеттік емес цифрлық жүйемен интеграциясының талаптары;

4) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптар орындалған жағдайда құрылады, пайдаланылады және дамытылады.

3. Цифрлық ресурста қамтылған ақпарат, нормативтік-техникалық құжаттама, сондай-ақ мемлекеттік органдардың цифрлық жүйесінің басқа да ілеспе құжаттары қазақ және орыс тілдерінде жасалады және сақталады.

4. Мемлекеттік органның цифрлық жүйесінің меншік иесі немесе иегері немесе ол уәкілеттік берген тұлға киберқауіпсіздікті қамтамасыз ету мониторингін жүргізу үшін оның орналасқан жері бойынша мемлекеттік органның цифрлық жүйесіне Киберқауіпсіздіктің ұлттық үйлестіру орталығына қолжетімділікті қамтамасыз етеді.

Ескерту. 38-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

39-бап. "Электрондық үкіметтің" ақпараттандыру объектілерін құру және дамыту

Ескерту. 39-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

39-1-бап. Қазақстан Республикасы арнаулы мемлекеттік органдарының ақпараттық жүйесін құру және дамыту тәртібі

Ескерту. 39-1-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

40-бап. "Электрондық үкіметтің" ақпараттандыру объектісін өнеркәсіптік пайдалану

Ескерту. 40-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

41-бап. "Электрондық үкіметтің" ақпараттандыру объектісін өнеркәсіптік пайдалануды тоқтату

Ескерту. 41-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

41-1-бап. "Электрондық үкіметтің" ақпараттандыру объектілерін есептен шығару

Ескерту. 41-1-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

42-бап. "Цифрлық үкіметтің" цифрлық инфрақұрылымының цифрлық ресурстарын өңдеу, сақтау және резервтік көшіру құралдарына қойылатын міндетті талаптар

1. "Цифрлық үкіметтің" цифрлық инфрақұрылымы объектілерінің жұмыс істеу сенімділігі мен қауіпсіздігін қамтамасыз ету үшін цифрлық ресурстарды сақтау, өңдеу және беру үшін пайдаланылатын техникалық құралдар Қазақстан Республикасының техникалық реттеу саласындағы заңнамасының талаптарына сәйкес келуге міндетті.

2. "Цифрлық үкіметтің" цифрлық инфрақұрылымы объектісінің меншік иесі немесе иегері, сондай-ақ "цифрлық үкімет" операторы "цифрлық үкіметтің" цифрлық инфрақұрылымы объектілерінде қамтылған мемлекеттік цифрлық ресурстарды сақтауды жүзеге асырады және қажет болған жағдайда қалпына келтіруді қамтамасыз етеді және Қазақстан Республикасының заңдарында және тараптардың келісімімен белгіленген тәртіппен мемлекеттік цифрлық ресурстардың жоғалуына, модификациялануына немесе сақталуын өзге де қамтамасыз етпеуге жауапты болады.

3. Мемлекеттік цифрлық ресурстардың резервтік көшірмесін дайындауды қамтамасыз ету "цифрлық үкіметтің" цифрлық инфрақұрылым объектісінің меншік иесі мен иегері немесе "цифрлық үкімет" операторы үшін міндетті болып табылады.

Мемлекеттік цифрлық ресурстарды қамтитын резервтік көшірмені жасау және сақтау тәсілі келесі резервтік көшірме жасалғанға дейін цифрлық ресурстардың сақталуын қамтамасыз етуге тиіс.

Мемлекеттік цифрлық ресурстарды резервтік көшірудің мерзімділігі "цифрлық үкіметтің" цифрлық объектісіне арналған техникалық құжаттамада белгіленеді.

Ескерту. 42-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

43-бап. "Электрондық үкіметтің" ақпараттандыру объектілерінің интеграциясы

Ескерту. 43-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған

күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

44-бап. Мемлекеттік органның ақпараттық жүйесімен интеграцияланатын мемлекеттік емес ақпараттық жүйелерге қойылатын талаптар

Ескерту. 44-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

7-тарау. АҚПАРАТТАНДЫРУДЫҢ СЕРВИСТІК МОДЕЛІ

Ескерту. 7-тарау алып тасталды – ҚР 14.07.2022 № 141-VII (01.01.2023 бастап қолданысқа енгізіледі) Заңымен.

8-тарау. Киберқауіпсіздік талаптарына сәйкестікке сынақтар жүргізу, киберқауіпсіздік аудиті

Ескерту. 8-тараудың тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

48-бап. Электрондық ақпараттық ресурстарды және ақпараттық жүйелер туралы мәліметтерді (ақпаратты)құжаттандыру

Ескерту. 48-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

49-бап. Киберқауіпсіздік талаптарына сәйкестікке сынақтар жүргізу

1. Цифрлық объектілерге киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу міндетті түрде және (немесе) меншік иесінің немесе иегердің бастамасы бойынша жүргізіледі.

2. Киберқауіпсіздік талаптарына сәйкестігіне міндетті сынақтар жүргізуге жататын сынақ объектілеріне мыналар жатады:

1) платформалық бағдарламалық өнім;

2) "цифрлық үкіметтің" платформасы;

3) мемлекеттік органның, мемлекеттік заңды тұлғаның, квазимемлекеттік сектор субъектісінің интернет-ресурсы;

4) мемлекеттік органның, мемлекеттік заңды тұлғаның, квазимемлекеттік сектор субъектісінің цифрлық жүйесі;

5) аса маңызды цифрлық объектілер;

6) мемлекеттік цифрлық ресурстарды қалыптастыруға, мемлекеттік функцияларды жүзеге асыруға және мемлекеттік қызметтер көрсетуге арналған мемлекеттік емес цифрлық жүйе.

3. Қазақстан Республикасының ұлттық куәландырушы орталығының электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру жөніндегі сервистерін пайдалану үшін мемлекеттік органның цифрлық жүйесі мен мемлекеттік емес цифрлық жүйеге киберқауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу талап етілмейді.

4. Цифрлық объектілерге (меншік иесі (иегері) және (немесе) тапсырыс беруші мемлекеттік орган болып табылатын цифрлық объектілерді қоспағанда) киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сынақты осы Заңға және Қазақстан Республикасының техникалық реттеу саласындағы заңнамасына сәйкес

аккредиттелген сынақ зертханалары жүргізеді.

5. Цифрлық объектілердің сапасын бағалау мақсатында оларға сынақ жүргізу Қазақстан Республикасының техникалық реттеу саласындағы заңнамасына сәйкес жүргізіледі.

Ескерту. 49-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

50-бап. Киберқауіпсіздік аудиті

1. Цифрлық объектілердің киберқауіпсіздік аудиті олардың меншік иесінің және (немесе) иегерінің бастамасы бойынша жүргізіледі.

2. Цифрлық объектілердің меншік иесі және (немесе) иегері ішкі аудит жүргізуге немесе киберқауіпсіздікті қамтамасыз ету саласында лицензиясы бар заңды тұлғалардан Қазақстан Республикасының Азаматтық кодексіне сәйкес көрсетілетін қызметті сатып алуға құқылы.

3. Аса маңызды цифрлық объектілердің, заңмен қорғалатын құпиясы бар цифрлық деректерді өңдейтін цифрлық объектілердің иегері жылына бір реттен сиретпей киберқауіпсіздік аудитін жүргізеді. Аудит нәтижелері уәкілетті органға және Киберқауіпсіздіктің ұлттық үйлестіру орталығына жіберіледі.

Ескерту. 50-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

51-бап. Аттестаттау

Ескерту. 51-бап алып тасталды - ҚР 18.03.2019 № 237-VI Заңымен (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі).

52-бап. Цифрлық орта саласындағы сәйкестікті растау

Цифрлық орта саласындағы сәйкестікті растау Қазақстан Республикасының техникалық реттеу саласындағы заңнамасына сәйкес жүзеге асырылады.

Ескерту. 52-бапқа өзгеріс енгізілді – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

9-тарау. Цифрлық объектілерді қорғау

Ескерту. 9-тараудың тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

53-бап. Цифрлық объектілерді қорғау мақсаттары

1. Цифрлық объектілерді сақтауға, оларға құқыққа сыйымсыз және (немесе) абайсызда қол жеткізуге және (немесе) әсер етуге жол бермеуге бағытталған құқықтық, ұйымдастырушылық және техникалық іс-шаралар кешенін іске асыру цифрлық объектілерді қорғау болып табылады.

2. Цифрлық объектілерді қорғау Қазақстан Республикасының заңнамасына және Қазақстан Республикасының аумағында қолданылатын стандарттарға сәйкес:

1) цифрлық ресурстардың қызметін қамтамасыз ету;

2) қолжетімділігі шектелген цифрлық ресурстардың құпиялылық режимін қамтамасыз ету;

3) киберқауіпсіздік субъектілерінің цифрлық ресурстарға қол жеткізу құқығын іске асыру;

4) цифрлық ресурстарға қатысты санкцияланбаған және (немесе) абайсызда қол жеткізуге, таралып кетуге және өзге де әрекеттерге, сондай-ақ цифрлық инфрақұрылым объектілеріне санкцияланбаған және (немесе) абайсызда әсер етуге жол бермеу;

5) цифрлық объектілер мен аса маңызды цифрлық объектілердің жұмыс істеуінің бұзылуына жол бермеу;

6) телекоммуникация желілерінің абоненттері туралы қызметтік ақпаратқа және телекоммуникация хабарларына санкцияланбаған және (немесе) абайсызда қол жеткізуге жол бермеу;

7) телекоммуникация желілерінің абоненттік құрылғыларының жұмысын санкцияланбаған және (немесе) абайсызда бұғаттауға жол бермеу мақсатында жүзеге асырылады.

3. Мыналар цифрлық объектілерге қатысты өзге де санкцияланбаған және (немесе) абайсызда болған әрекеттер болып табылады:

1) цифрлық ресурстар мен цифрлық инфрақұрылым объектілеріне қол жеткізуді шектеуге немесе жабуға алып келетін әрекеттер түрінде жасалған цифрлық ресурстар мен цифрлық инфрақұрылым объектілерін бұғаттау;

2) цифрлық объектілерді санкцияланбаған және (немесе) абайсызда модификациялау;

3) цифрлық ресурстарды санкцияланбаған және (немесе) абайсызда көшіру;

4) цифрлық ресурстарды санкцияланбаған және (немесе) абайсызда жою, жоғалту;

5) цифрлық объектілердің жұмысын бұзу;

6) зиянды бағдарламаларды пайдалану.

4. Цифрлық объектілерді қорғау сыныптауышқа сәйкес берілген сыныпқа сай жүзеге асырылады.

Ескерту. 53-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

54-бап. Цифрлық объектілерді қорғауды ұйымдастыру

1. Цифрлық объектілерді қорғауды:

1) цифрлық ресурстарға қатысты – олардың меншік иелері, иегерлері және пайдаланушылары;

2) цифрлық инфрақұрылым объектілеріне және аса маңызды цифрлық объектілерге қатысты – олардың меншік иелері немесе иегерлері жүзеге асырады.

2. "Цифрлық үкіметтің" цифрлық инфрақұрылым объектілерінің және аса маңызды цифрлық объектілердің меншік иелері немесе иегерлері мыналарды:

1) санкцияланбаған қол жеткізуге жол бермеуді;

2) егер санкцияланбаған қол жеткізудің алдын алу мүмкін болмаса, мұндай санкцияланбаған қол жеткізу фактілерін уақтылы анықтауды;

3) қол жеткізу тәртібін бұзудың қолайсыз салдарын барынша азайтуды;

4) цифрлық ресурстарды өңдеу және беру құралдарына санкцияланбаған әсер етуге жол бермеуді;

5) киберқауіпсіздіктің оқыс оқиғаларын, осалдықты жоюды;

6) санкцияланбаған қол жеткізу салдарынан модификацияланған не жойылған цифрлық ресурстарды жедел қалпына келтіруді;

7) мемлекеттік құпияларды құрайтын мәліметтерді қамтитын цифрлық ресурстардың меншік иелерін және (немесе) иегерлерін қоспағанда, цифрлық деректерді кейіннен жібере отырып, орын алған киберқауіпсіздіктің оқыс оқиғасы туралы, киберқауіпсіздіктің оқыс оқиғасын жою жөнінде қабылданған шаралар туралы Киберқауіпсіздіктің ұлттық үйлестіру орталығын дереу хабардар етуді;

8) "цифрлық үкіметтің" цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингі мәселелері бойынша Киберқауіпсіздіктің ұлттық үйлестіру орталығымен ақпараттық өзара іс-қимыл жасауды;

9) Киберқауіпсіздікті ұлттық үйлестіру орталығына "цифрлық үкіметтің" цифрлық объектілеріне және киберқауіпсіздікті қамтамасыз ету орталықтарына "цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларына сәйкес киберқауіпсіздікті қамтамасыз ету мониторингін іске асыруға бағытталған ұйымдастырушылық-техникалық іс-шараларды жүргізу үшін аса маңызды цифрлық объектілерге қол жеткізуді беруді қамтамасыз ететін шараларды қабылдауға міндетті.

3. Мемлекеттік органдардың цифрлық объектілерінің меншік иелері немесе иегерлері мыналарды:

1) Интернетке қолжетімділігі бар цифрлық объектілердің "цифрлық үкіметтің" цифрлық объектілері үшін киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасына қатысуын;

2) "цифрлық үкіметтің" цифрлық объектілері үшін киберқауіпсіздікті зерттеушілермен өзара іс-қимыл жасау бағдарламасы шеңберінде анықталған осалдықты жоюды;

3) осы Заңға және Қазақстан Республикасының өзге де заңдарына сәйкес өзге де міндеттерді орындауды қамтамасыз ететін шараларды қабылдауға міндетті.

4. Мемлекеттік органдардың қызметін цифрландыруға арналған мемлекеттік емес цифрлық объектілердің меншік иелері немесе иегерлері мемлекеттік органдардың цифрлық объектілерімен интеграцияланғанға дейін:

1) цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарға сәйкестікті қамтамасыз ету жөнінде шаралар қабылдайды;

2) киберқауіпсіздікті қамтамасыз етудің меншікті орталығын құрады және оның жұмыс істеуін қамтамасыз етеді немесе киберқауіпсіздікті қамтамасыз ету орталығы көрсететін қызметтерді Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардан киберқауіпсіздікті қамтамасыз ету орталығының көрсетілетін қызметтерінің сатып алуға міндетті көлемдерінің (жиынтықтарының) және олардың сипаттамаларының тізбесінде белгіленген көлемде (жиынтықта) сатып алады.

5. Мемлекеттік органдарды, жергілікті өзін-өзі басқару органдарын, мемлекеттік заңды тұлғаларды, квазимемлекеттік сектор субъектілерін қоспағанда, аса маңызды цифрлық объектілердің меншік иелері немесе иегерлері аса маңызды цифрлық объектілер тізбесіне енгізілген күннен бастап алты ай ішінде:

1) киберқауіпсіздік саласына жататын, цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарға сәйкестік жөнінде шаралар қабылдайды;

2) киберқауіпсіздікті қамтамасыз етудің меншікті орталығын құрады және оның жұмыс істеуін қамтамасыз етеді немесе киберқауіпсіздікті қамтамасыз ету орталығы көрсететін қызметтерді Қазақстан Республикасының Азаматтық кодексіне сәйкес үшінші тұлғалардан киберқауіпсіздікті қамтамасыз ету орталығының көрсетілетін қызметтерінің сатып алуға міндетті көлемдерінің (жиынтықтарының) және олардың сипаттамаларының тізбесінде белгіленген көлемде (жиынтықта) сатып алады;

3) киберқауіпсіздік талаптарына сәйкестікке сынақтар рәсімінен өтеді;

4) жүргізілген киберқауіпсіздік аудиті жөніндегі ақпаратты киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға береді.

6. Әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше жағдай немесе соғыс жағдайы енгізілген кезде интернет-ресурстар мен цифрлық инфрақұрылым объектілерін басқаруды Қазақстан Республикасының заңнамасына сәйкес уәкілетті орган жүзеге асырады.

Ескерту. 54-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі); өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңдарымен.

54-1-бап. Цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптар

1. Цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптар Қазақстан Республикасы Үкіметінің қаулысымен бекітіледі.

2. Киберқауіпсіздікті қамтамасыз ету саласына жататын, цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың ережелері мемлекеттік органдардың, жергілікті өзін-өзі басқару органдарының, мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, мемлекеттік органдардың цифрлық объектілерімен интеграцияланатын немесе мемлекеттік цифрлық ресурстарды қалыптастыруға арналған мемлекеттік емес цифрлық объектілердің меншік иелері мен иегерлерінің, сондай-ақ аса маңызды цифрлық объектілердің меншік иелері мен иегерлерінің қолдануы үшін міндетті.

3. Цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптардың ережелері мемлекеттік құпияларға жатқызылған қорғалған түрде орындалған цифрлық жүйелерге, мемлекеттік құпияларды құрайтын мәліметтерді қамтитын цифрлық объектілерге, сондай-ақ арнаулы мақсаттағы телекоммуникациялар желісіне және (немесе) президенттік, үкіметтік және қорғалған байланыс желілеріне қолданылмайды.

Ескерту. 54-1-баппен толықтырылды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

55-бап. Цифрлық объектілерді қорғау шаралары

1. Цифрлық объектілерді қорғаудың құқықтық шараларына мыналар жатады:

1) Қазақстан Республикасы заңнамасының талаптары және Қазақстан Республикасының аумағында қолданылатын цифрландыру саласындағы стандарттар;

2) Қазақстан Республикасының цифрландыру заңнамасын бұзғаны үшін жауаптылық;

3) цифрлық объектілердің меншік иесі немесе иегері жасасатын, оларда осы объектілердің жұмыс істеу, оларға қол жеткізу немесе оларды пайдалану шарттары, сондай-ақ оларды бұзғаны үшін жауаптылық белгіленетін келісімдер.

2. Цифрлық объектілерді қорғаудың ұйымдастырушылық шараларына цифрлық объектілерге қол жеткізу жүзеге асырылуы мүмкін аумаққа (ғимараттарға, үй-жайларға) кіру режимін белгілеу және қамтамасыз ету, сондай-ақ оларға қол жеткізуді шектеу жатады.

3. Цифрлық объектілерді қорғаудың техникалық (бағдарламалық-техникалық) шараларына мыналар жатады:

1) ақпаратты қорғау құралдарын пайдалану, ал мемлекеттік құпияларды құрайтын мәліметтерге қатысты – Қазақстан Республикасының заңнамасына сәйкес әзірленген, дайындалған және (немесе) пайдалануға қабылданып алынған, мемлекеттік құпияларды құрайтын ақпаратты қорғау құралдарын қолдана отырып қана пайдалану;

2) цифрлық объектілерге қол жеткізуді бақылау және қол жеткізу фактілерін тіркеу жүйесін пайдалану;

3) цифрлық объектілердің меншік иелерінің немесе иегерлерінің қорғау шараларын айқындауы үшін бекітілген қорғау бейіндерінің негізінде қауіпсіздік жөніндегі тапсырманы әзірлеу.

4. Цифрлық объектілерді қорғаудың техникалық (бағдарламалық-техникалық) шараларын пайдалану жеке тұлғалардың өміріне, денсаулығына және мүлкіне, сондай-ақ заңды тұлғалардың мүлкіне және мемлекеттік мүлікке зиян келтірмеуге немесе зиян келтіру қатерін туғызбауға тиіс.

Ескерту. 55-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

56-бап. Дербес деректерді қамтитын цифрлық ресурстарды қорғау

Ескерту. 56-баптың тақырыбына өзгеріс енгізілді – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

Дербес деректерді қамтитын цифрлық жүйелердің меншік иелері және иеленушілері, дербес деректерді қамтитын базаның меншік иесі және (немесе) операторы, сондай-ақ үшінші тұлғалар осы Заңға және Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасына сәйкес оларды қорғау бойынша шараларды қолдануға міндетті.

Бұл міндет дербес деректерді қамтитын цифрлық ресурстар алынған немесе дербес деректер жиналған кезден бастап және олар жойылғанға не иесіздендірілгенге дейін туындайды.

Ескерту. 56-бапқа өзгеріс енгізілді - ҚР 25.06.2020 № 347-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); 06.04.2024 № 71-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі); 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңдарымен.

56-1-бап. Интернеттің қазақстандық сегментінің кеңістігінде домендік аттарды қорғау

1. .KZ және (немесе) .ҚАЗ домендік аттармен тіркелген интернет-ресурс Интернеттің қазақстандық сегментінің кеңістігінде орналастырылады.

2. Интернет-ресурстармен деректерді беру кезінде Интернеттің қазақстандық сегментінің кеңістігінде .KZ және (немесе) .ҚАЗ домендік аттарды пайдалану қауіпсіздік сертификаттарын қолдану арқылы жүзеге асырылады.

Ескерту. 9-тарау 56-1-баппен толықтырылды - ҚР 25.06.2020 № 347-VI Заңымен (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі).

Ескерту. 3-бөлімнің тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

10-тараудың тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

57-бап. Ақпараттандыру және ақпараттық қауіпсіздікті қамтамасыз ету салаларындағы қорытындылар

Ескерту. 57-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

58-бап. Бюджеттік инвестициялардың техникалық-экономикалық негіздемесіне немесе қаржылық-экономикалық негіздемесіне ақпараттандыру саласындағы сараптаманың қорытындысы

Ескерту. 58-бап алып тасталды - ҚР 18.03.2019 № 237-VI Заңымен (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі).

59-бап. Цифрлық орта және киберқауіпсіздікті қамтамасыз ету салаларындағы техникалық құжаттаманы және мемлекеттік-жекешелік әріптестік жобалары бойынша құжаттаманы келісу

Ескерту. 59-баптың тақырыбына өзгеріс енгізілді – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

1. "Цифрлық үкіметтің" цифрлық объектісін құруға және дамытуға арналған техникалық тапсырманы келісуді киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган цифрландыру саласындағы уәкілетті орган бекіткен "цифрлық үкіметтің" цифрлық объектілерін құруға және дамытуға арналған техникалық тапсырмаларды жасау және қарау қағидаларында айқындалған тәртіппен және мерзімдерде жүзеге асырады.

2. Алып тасталды – ҚР 14.07.2022 № 141-VII (01.01.2023 бастап қолданысқа енгізіледі) Заңымен.

3. Қазақстан Республикасының мемлекеттік-жекешелік әріптестік саласындағы заңнамасына сәйкес цифрландыру саласындағы мемлекеттік-жекешелік әріптестіктің республикалық және жергілікті жобалары шеңберінде "цифрлық үкіметтің" цифрлық объектілерін құру және дамыту кезінде киберқауіпсіздікті

қамтамасыз ету саласындағы уәкілетті орган жекеше әріптесті айқындау жөніндегі тікелей келіссөздер кезінде мемлекеттік-жекешелік әріптестік жобасының конкурстық құжаттамасын, мемлекеттік-жекешелік әріптестік жобасына бизнес-жоспарды келіседі.

Ескерту. 59-бап жаңа редакцияда - ҚР 18.03.2019 № 237-VI Заңымен (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); өзгеріс енгізілді - ҚР 25.06.2020 № 347-VI (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі); 14.07.2022 № 141-VII (01.01.2023 бастап қолданысқа енгізіледі); 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңдарымен.

60-бап. Ақпараттандыру саласындағы тауарларды, жұмыстар мен көрсетілетін қызметтерді мемлекеттік сатып алуға арналған шығыстардың есеп-қисаптарына уәкілетті органның қорытындысы

Ескерту. 60-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

10-1-тарау. Цифрландыру саласындағы, сондай-ақ электрондық құжат пен электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуын мемлекеттік бақылау

Ескерту. 10-1-тараумен толықтырылды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

60-1-бап. Цифрландыру саласындағы мемлекеттік бақылау

1. Цифрландыру саласындағы мемлекеттік бақылау тексерулер, бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау және бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау нысанында жүзеге асырылады.

2. Тексеру және бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау Қазақстан Республикасының Кәсіпкерлік кодексіне сәйкес жүзеге асырылады.

3. Бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау осы Заңға және Қазақстан Республикасының Кәсіпкерлік кодексіне сәйкес жүзеге асырылады.

4. Мемлекеттік органдарға қатысты цифрландыру саласындағы мемлекеттік бақылау осы Заңның 60-3-бабына сәйкес жүзеге асырылады.

5. Егер Қазақстан Республикасының заңдарында өзгеше көзделмесе, осы баптың талаптары Қазақстан Республикасының Ұлттық Банкіне және оның құрылымына кіретін ұйымдарға, сондай-ақ Қазақстан Республикасының арнаулы мемлекеттік органдарына қолданылмайды.

60-2-бап. Цифрландыру саласында бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау жүргізу тәртібі

1. Бақылау субъектісіне (объектісіне) бармай профилактикалық бақылауды уәкілетті орган және Қазақстан Республикасының Ұлттық қауіпсіздік органдары бақылау субъектілеріне (объектілеріне) бармай, цифрлық жүйелерді, ашық дереккөздерді, бұқаралық ақпарат құралдарын талдаудың және олардың деректерінің, сондай-ақ бақылау субъектісінің (объектісінің) қызметі туралы басқа да мәліметтердің негізінде жүзеге асырады.

2. Бұзушылықтардың уақтылы жолын кесу және оларға жол бермеу, бақылау субъектісіне (объектісіне) бармай профилактикалық бақылаудың нәтижелері бойынша анықталған бұзушылықтарды дербес жою құқығын бақылау субъектісіне беру және бақылау субъектісіне әкімшілік жүктемені азайту бақылау субъектісіне (объектісіне) бармай профилактикалық бақылаудың мақсаттары болып табылады.

3. Бақылау субъектілеріне бұзушылықтарды дербес жою құқығын беру үшін бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау Қазақстан Республикасының заңнамасына сәйкес салдарын жоюға болатын бұзушылықтар бойынша ғана жүргізіледі.

4. Бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау қорытындысы бойынша бақылау субъектісіне анықталған бұзушылықтарды жою тәртібі міндетті түрде түсіндіріле отырып, әкімшілік құқық бұзушылық туралы іс қозғалмай, оларды жою туралы ұсыным жасалады.

5. Анықталған бұзушылықтарды жою туралы ұсыным бақылау субъектісіне жеке қолын қойғызып немесе жөнелту және алу фактісін растайтын өзге тәсілмен табыс етілуге тиіс.

6. Төменде санамаланған тәсілдердің бірімен жіберілген, анықталған бұзушылықтарды жою туралы ұсыным мынадай жағдайларда:

1) қолма-қол – ұсынымда алғаны туралы белгі жасалған күннен бастап;

2) поштамен – хабарламасы бар тапсырысты хатпен;

3) электрондық тәсілмен – уәкілетті органның және Қазақстан Республикасы ұлттық қауіпсіздік органдарының сұрау салуы кезінде бақылау субъектісінің хатта көрсетілген электрондық мекенжайына уәкілетті орган жөнелткен күннен бастап табыс етілді деп есептеледі.

7. Анықталған бұзушылықтарды жою туралы ұсыным табыс етілген күнінен кейінгі күннен бастап отыз жұмыс күні ішінде орындалуға тиіс.

8. Бақылау субъектісі анықталған бұзушылықтарды жою туралы ұсынымда көрсетілген бұзушылықтармен келіспеген жағдайда анықталған бұзушылықтарды жою туралы ұсынымды жіберген уәкілетті органға, Қазақстан Республикасының ұлттық қауіпсіздік органдарына ұсыным табыс етілген күннен кейінгі күннен бастап бес жұмыс күні ішінде қарсылық жіберуге құқылы.

9. Анықталған бұзушылықтарды жою туралы ұсынымды белгіленген мерзімде орындамау бақылау субъектісін (объектісін) бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылаудың жартыжылдық тізіміне енгізуге алып келеді.

10. Бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау тоқсанына бір реттен жиілетпей жүргізіледі.

Ескерту. 60-2-бапқа өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

60-3-бап. Мемлекеттік органдарға қатысты цифрландыру саласында мемлекеттік бақылау жүргізу тәртібі

1. Мемлекеттік органдарға (бұдан әрі – тексерілетін мемлекеттік органдар) қатысты цифрландыру саласында мемлекеттік бақылауды уәкілетті орган және Қазақстан Республикасының ұлттық қауіпсіздік органдары тексерулер нысанында жүргізеді.

Тексерулер мерзімдік және жоспардан тыс болып бөлінеді.

Тексерілетін мемлекеттік органдарға қатысты мерзімдік тексерулер мынадай ақпарат көздеріне:

1) алдыңғы тексерулердің нәтижелеріне;

2) есептілік пен мәліметтер мониторингінің нәтижелеріне;

3) мемлекеттік органдардың интернет-ресурстарын талдау нәтижелеріне;

4) мемлекеттік техникалық қызмет мәліметтеріне сәйкес жүзеге асырылады.

2. Мерзімдік тексерулер Қазақстан Республикасының киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органы мен ұлттық қауіпсіздік органдарының бірінші басшылары бекіткен мерзімдік тексерулер жүргізу жоспарларына сәйкес жылына бір реттен жиі болмайтын кезеңділікпен жүргізіледі.

Уәкілетті орган және Қазақстан Республикасының ұлттық қауіпсіздік органдары мерзімдік тексерулер жүргізу жоспарын тексерулер жүргізу жылының алдындағы жылдың 1 желтоқсанынан кешіктірмей бекітеді.

Мерзімдік тексерулер жүргізу жоспары уәкілетті органның және Қазақстан Республикасының ұлттық қауіпсіздік органдарының интернет-ресурсында тексерулер жүргізу жылының алдындағы жылдың 20 желтоқсанынан кешіктірілмей орналастырылады.

Мерзімдік тексерулер жүргізу жоспарында мыналар қамтылады:

1) жоспардың бекітілген күні мен нөмірі;

2) мемлекеттік органның атауы;

3) тексерілетін мемлекеттік органның атауы;

4) тексерілетін мемлекеттік органның тұрған жері;

5) тексеру жүргізу мерзімдері;

6) тексерудің нысанасы;

7) жоспарға қол қоюға уәкілеттік берілген адамның қолтаңбасы.

Мерзімдік тексерулер жүргізу жоспарына өзгерістер мен толықтырулар енгізу тексерілетін мемлекеттік орган таратылған, қайта ұйымдастырылған, оның атауы өзгерген немесе өкілеттіктері тексерілетін мемлекеттік органдар арасында қайта бөлінген жағдайларда жүзеге асырылады.

3. Уәкілетті орган, Қазақстан Республикасының ұлттық қауіпсіздік органдары мынадай:

1) тексерілетін мемлекеттік органға қатысты жеке және заңды тұлғалардан келіп түскен, Қазақстан Республикасының киберқауіпсіздік туралы заңнамасы талаптарының бұзылуы туралы расталған жолданымдар болған;

2) құқықтары мен заңды мүдделері бұзылған жеке және заңды тұлғалар жүгінген;

3) жеке және заңды тұлғалардың, мемлекеттің құқықтары мен заңды мүдделеріне зиян келтірудің нақты фактілері бойынша не зиян келтіру қатері туралы прокурор талап еткен;

4) жеке және заңды тұлғалардың, мемлекеттің құқықтары мен заңды мүдделеріне зиян келтірудің нақты фактілері бойынша, сондай-ақ жойылмауы жеке және заңды тұлғалардың құқықтары мен заңды мүдделеріне зиян келтіруге алып келетін Қазақстан Республикасы заңнамасы талаптарының бұзылуының нақты фактілері бойынша мемлекеттік органдар жүгінген;

4-1) аса маңызды цифрлық объектілер меншік иелерінің, иеленушілерінің Қазақстан Республикасының киберқауіпсіздікті қамтамасыз ету саласындағы заңнамасының талаптарын бұзушылықтары анықталғаны туралы Қазақстан Республикасы Ұлттық қауіпсіздік органдары лауазымды адамының баянаты болған;

5) қылмыстық қудалау органының Қазақстан Республикасының Қылмыстық-процестік кодексінде көзделген негіздер бойынша тапсырмасы болған;

6) тексеру нәтижелері туралы актінің орындалуына бақылау жүргізу қажет болған жағдайларда тағайындайтын тексеру жоспардан тыс тексеру болып табылады.

4. Уәкілетті органның лауазымды адамдарының тексеру жүргізу кезінде:

1) осы баптың 8-тармағында көрсетілген құжаттарды көрсеткен кезде тексерудің нысанасына сәйкес тексерілетін мемлекеттік органның аумағына және үй-жайларына кедергісіз кіруге;

2) тексеру нәтижелері туралы актіге қоса тіркеу үшін тексерудің нысанасына сәйкес қағаз және цифрлық жеткізгіштердегі құжаттарды (мәліметтерді) не олардың көшірмелерін, сондай-ақ автоматтандырылған дерекқорларға (цифрлық жүйелерге) рұқсат алуға;

3) аудио-, фото- және бейнетүсірілімді жүзеге асыруға;

4) мемлекеттік органдардың, ведомстволық бағыныстағы және өзге де ұйымдардың мамандарын, консультанттары мен сарапшыларын тартуға құқығы бар.

5. Тексерілетін мемлекеттік орган не оның уәкілетті өкілі тексеру жүргізілген кезде:

1) уәкілетті органның және Қазақстан Республикасы ұлттық қауіпсіздік органдарының тексеру жүргізуге келген лауазымды адамдарын:

осы бапта белгіленген мерзімдерге сәйкес келмейтін, тексеруді тағайындау туралы актіде (ұзарту туралы қосымша акт болған кезде онда) көрсетілген мерзімдер асып кеткен не өтіп кеткен;

осы баптың 8-тармағында көзделген құжаттар болмаған жағдайларда тексеруге жібермеуге;

2) тексеру нәтижелері туралы актіге Қазақстан Республикасының заңнамасында белгіленген тәртіппен шағым жасауға құқылы.

6. Тексерілетін мемлекеттік орган не оның уәкілетті өкілі тексеру жүргізілген кезде:

1) уәкілетті органның және Қазақстан Республикасы ұлттық қауіпсіздік органдарының лауазымды адамдарының аумаққа және үй-жайларға кедергісіз кіруін қамтамасыз етуге;

2) уәкілетті органның және Қазақстан Республикасы ұлттық қауіпсіздік органдарының лауазымды адамдарына тексеру нәтижелері туралы актіге қоса тіркеу үшін тексерудің нысанасына сәйкес қағаз және цифрлық жеткізгіштердегі құжаттарды (мәліметтерді) не олардың көшірмелерін ұсынуға, сондай-ақ

автоматтандырылған дерекқорларға (цифрлық жүйелерге) рұқсат беруге;

3) тексеруді тағайындау туралы актінің және тексеру нәтижелері туралы актінің екінші данасына тексеру аяқталған күні белгі жасауға міндетті.

7. Тексеру тексеруді тағайындау туралы акт негізінде жүргізіледі.

Тексеруді тағайындау туралы актіде мыналар көрсетіледі:

1) актінің күні мен нөмірі;

2) мемлекеттік органның атауы;

3) тексеру жүргізуге уәкілеттік берілген адамның (адамдардың) тегі, аты, әкесінің аты (егер ол жеке басты куәландыратын құжатта көрсетілсе) және лауазымы;

4) мемлекеттік органдардың, ведомстволық бағынысты және өзге де ұйымдардың тексеру жүргізуге тартылатын мамандары, консультанттары мен сарапшылары туралы мәліметтер;

5) тексерілетін мемлекеттік органның атауы, оның тұрған жері.

Мемлекеттік органның құрылымдық бөлімшесі тексерілген жағдайда тексеруді тағайындау туралы актіде оның атауы мен тұрған жері көрсетіледі;

6) тексерудің нысанасы;

7) тексеру түрі;

8) тексеру жүргізу мерзімі;

9) тексеру жүргізу негіздері;

10) тексерілетін кезең;

11) тексерілетін мемлекеттік органның құқықтары мен міндеттері;

12) тексерілетін мемлекеттік орган басшысының не оның уәкілетті адамының актіні алғаны немесе алудан бас тартқаны туралы қолтаңбасы;

13) актіге қол қоюға уәкілеттік берілген адамның қолтаңбасы.

Тексеру жүргізу кезінде уәкілетті орган және Қазақстан Республикасының ұлттық қауіпсіздік органдары тексеру жүргізу нысанасын көрсете отырып, ол басталғанға дейін кемінде бір тәулік бұрын тексерілетін мемлекеттік органды тексеру жүргізудің басталатыны туралы хабардар етуге міндетті.

Тексерілетін мемлекеттік органға тексеруді тағайындау туралы акт табыс етілген күн тексеру жүргізудің басталуы деп есептеледі.

8. Уәкілетті органның және Қазақстан Республикасы ұлттық қауіпсіздік органдарының объектіге тексеруге келген лауазымды адамдары тексерілетін мемлекеттік органға:

1) тексеруді тағайындау туралы актіні;

2) қызметтік куәлігін не сәйкестендіру картасын;

3) қажет болған кезде құзыретті органның режимдік объектілерге баруға рұқсатын көрсетуге міндетті.

9. Тексеру жүргізу мерзімі тексерудің нысанасы, сондай-ақ алдағы жұмыстардың

көлемі ескеріле отырып белгіленеді және он жұмыс күнінен аспауға тиіс.

Тексеру жүргізу мерзімі он бес жұмыс күнінен аспайтын мерзімге бір рет қана ұзартылуы мүмкін. Ұзарту уәкілетті орган мен Қазақстан Республикасы ұлттық қауіпсіздік органдары басшыларының шешімімен жүзеге асырылады.

Тексеру жүргізу мерзімдерін ұзарту тексерілетін мемлекеттік орган хабардар етіле отырып, тексеру мерзімдерін ұзарту туралы қосымша актімен ресімделеді, онда тексеруді тағайындау туралы алдыңғы акт бұйрығының күні мен нөмірі және ұзарту себептері көрсетіледі.

Тексеру мерзімдерін ұзарту туралы хабарламаны уәкілетті орган мен Қазақстан Республикасының ұлттық қауіпсіздік органдары табыс етілгені туралы хабарламамен тексерілетін мемлекеттік органға ұзартылғанға дейін бір жұмыс күні бұрын табыс етеді.

10. Тексеру нәтижелері бойынша уәкілетті органның, Қазақстан Республикасының ұлттық қауіпсіздік органдарының тексеруді жүзеге асыратын лауазымды адамдары тексеру нәтижелері туралы акт жасайды.

Тексеру нәтижелері туралы актінің бірінші данасы электрондық нысанда өз құзыреті шегінде мемлекеттік құқықтық статистика және арнайы есепке алу саласында қызметті жүзеге асыратын мемлекеттік органға, екінші данасы тексерілетін мемлекеттік органда түпнұсқасы бар құжаттардың көшірмелерін қоспағанда, қосымшалардың көшірмелерімен бірге танысу және анықталған бұзушылықтарды жою бойынша шаралар мен басқа да әрекеттер қабылдау үшін қағаз жеткізгіште қол қойғызып немесе электрондық нысанда тексерілетін мемлекеттік органға (басшысына не оның уәкілетті адамына) табыс етіледі, үшінші данасы уәкілетті органда қалады.

11. Тексеру нәтижелері туралы актіде мыналар көрсетіледі:

1) актінің жасалған күні, уақыты және орны;

2) мемлекеттік органның атауы;

3) тексеруді тағайындау туралы актінің (мерзімді ұзарту туралы қосымша акт болған кезде оның) күні мен нөмірі;

4) тексеру жүргізген адамның (адамдардың) тегі, аты, әкесінің аты (егер ол жеке басты куәландыратын құжатта көрсетілсе) және лауазымы;

5) мемлекеттік органдардың, ведомстволық бағыныстағы және өзге де ұйымдардың тексеру жүргізуге тартылатын мамандары, консультанттары мен сарапшылары туралы мәліметтер;

6) тексерілетін мемлекеттік органның атауы, оның тұрған жері;

7) тексерудің нысанасы;

8) тексеру түрі;

9) тексеру жүргізу мерзімі мен кезеңі;

10) тексеру нәтижелері туралы, оның ішінде анықталған бұзушылықтар және олардың сипаты туралы мәліметтер;

11) орындалу мерзімі көрсетілген, Қазақстан Республикасының киберқауіпсіздік

туралы заңнамасы талаптарының анықталған бұзушылықтарын жою туралы талаптар;

12) тексерілетін мемлекеттік орган басшысының не оның уәкілетті адамының, сондай-ақ тексеру жүргізу кезінде қатысқан адамдардың актімен танысқаны немесе танысудан бас тартқаны туралы мәліметтер, олардың қолтаңбалары немесе қол қоюдан бас тарту туралы жазба;

13) тексеру жүргізген лауазымды адамдардың қолтаңбасы.

Тексеру нәтижелері туралы актіге тексеру нәтижелеріне байланысты құжаттар (олар болған кезде) және олардың көшірмелері қоса беріледі.

12. Тексеру нәтижелері бойынша ескертулер және (немесе) қарсылықтар болған жағдайда тексерілетін мемлекеттік орган оларды жазбаша түрде жазады. Ескертулер және (немесе) қарсылықтар тексеру нәтижелері туралы актіге қоса беріледі, бұл туралы тиісті белгі жасалады.

Уәкілетті орган, Қазақстан Республикасының ұлттық қауіпсіздік органдары тексерілетін мемлекеттік органның тексеру нәтижелері туралы актіге ескертулерін және (немесе) қарсылықтарын қарауға және он бес жұмыс күні ішінде уәжді жауап беруге тиіс.

Тексеру нәтижелері туралы актіні қабылдаудан бас тартылған жағдайда акт жасалады, оған тексеруді жүзеге асыратын лауазымды адамдар және тексерілетін мемлекеттік органның басшысы не оның уәкілетті өкілі қол қояды.

Тексерілетін мемлекеттік орган бас тарту себебі туралы жазбаша түсіндірме бере отырып, актіге қол қоюдан бас тартуға құқылы.

13. Тексеру нәтижелері туралы акт тексерілетін мемлекеттік органға тексеруді тағайындау туралы актіде немесе тексеру мерзімдерін ұзарту туралы қосымша актіде көрсетілген тексерудің аяқталу мерзімінен кешіктірілмей табыс етілген күн тексеру мерзімінің аяқталуы деп есептеледі.

14. Тексеру нәтижелері туралы актінің орындалу мерзімдері оны орындаудың нақты мүмкіндігіне әсер ететін мән-жайлар ескеріле отырып, бірақ тексеру нәтижелері туралы акт табыс етілген күннен бастап кемінде күнтізбелік он күн болып айқындалады.

15. Тексеру нәтижелері туралы актінің орындалу мерзімдерін айқындау кезінде:

1) тексерілетін мемлекеттік органда бұзушылықтарды жою бойынша ұйымдастырушылық, техникалық мүмкіндіктердің болуы;

2) мемлекеттік органдарда Қазақстан Республикасының заңдарында белгіленген міндетті қорытындыларды, келісулерді және басқа да құжаттарды алу мерзімдері ескеріледі.

16. Тексеру нәтижелері туралы актіде белгіленген анықталған бұзушылықтарды жою мерзімі өткеннен кейін тексерілетін мемлекеттік орган тексеру нәтижелері туралы актіде белгіленген мерзім ішінде уәкілетті органға, Қазақстан Республикасының ұлттық қауіпсіздік органдарына растайтын құжаттармен бірге анықталған бұзушылықтардың жойылғаны туралы ақпарат беруге міндетті.

Анықталған бұзушылықтардың жойылғаны туралы ақпарат берілмеген жағдайда уәкілетті орган, Қазақстан Республикасының ұлттық қауіпсіздік органдары осы

баптың 3-тармағының 6) тармақшасына сәйкес жоспардан тыс тексеру тағайындауға құқылы.

17. Тексеруді жүзеге асыру кезінде тексерілетін мемлекеттік органның құқықтары мен заңды мүдделері бұзылған жағдайда тексерілетін мемлекеттік орган уәкілетті органның және Қазақстан Республикасы ұлттық қауіпсіздік органдарының лауазымды адамдарының шешімдеріне, әрекеттеріне (әрекетсіздігіне) жоғары тұрған лауазымды адамға не Қазақстан Республикасының заңнамасында белгіленген тәртіппен сотқа шағым жасауға құқылы.

Ескерту. 60-3-бапқа өзгеріс енгізілді – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

60-4-бап. Электрондық құжат пен электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуын мемлекеттік бақылау

1. Электрондық құжат пен электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуын мемлекеттік бақылау, егер осы тармақтың екінші бөлігінде өзгеше белгіленбесе, Қазақстан Республикасының Кәсіпкерлік кодексіне сәйкес жоспардан тыс тексеру және бақылау субъектісіне (объектісіне) бару арқылы профилактикалық бақылау нысанында жүзеге асырылады.

Мемлекеттік органдарға қатысты электрондық құжат пен электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуын мемлекеттік бақылау осы Заңға сәйкес жүзеге асырылады.

Осы тармақтың талабы Қазақстан Республикасының Ұлттық Банкіне және оның құрылымына кіретін ұйымдарға және дауыс беретін акцияларының (жарғылық капиталға қатысу үлестерінің) елу және одан да көп пайызы Қазақстан Республикасының Ұлттық Банкіне тиесілі немесе оның сенімгерлік басқаруындағы заңды тұлғаларға, сондай-ақ Қазақстан Республикасының арнаулы мемлекеттік органдарына қолданылмайды.

60-5-бап. Мемлекеттік органдарға қатысты электрондық құжат пен электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуына мемлекеттік бақылау жүргізу тәртібі

1. Мемлекеттік органдарға (бұдан әрі – бақылау субъектілері) қатысты электрондық құжат пен электрондық цифрлық қолтаңбаға қойылатын талаптардың сақталуына мемлекеттік бақылауды уәкілетті орган тексерулер нысанында жүргізеді.

Тексерулер мерзімдік және жоспардан тыс болып бөлінеді.

Бақылау субъектілеріне қатысты мерзімдік тексерулер мынадай ақпарат көздеріне:

1) алдыңғы тексерулердің нәтижелеріне;

2) есептілік пен мәліметтер мониторингінің нәтижелеріне;

3) мемлекеттік органдардың интернет-ресурстарын талдау нәтижелеріне;

4) "цифрлық үкімет" операторының мәліметтеріне сәйкес жүзеге асырылады.

2. Мерзімдік тексерулер уәкілетті органның бірінші басшысы бекіткен мерзімдік тексерулер жүргізу жоспарына сәйкес жылына бір реттен жиі болмайтын кезеңділікпен жүргізіледі.

Уәкілетті орган мерзімдік тексерулер жүргізу жоспарын тексерулер жылының

алдындағы жылдың 1 желтоқсанынан кешіктірмей бекітеді.

Мерзімдік тексерулер жүргізу жоспары уәкілетті органның интернет-ресурсында тексерулер жылының алдындағы жылдың 20 желтоқсанынан кешіктірілмей орналастырылады.

Мерзімдік тексерулер жүргізу жоспарында мыналар қамтылады:

1) жоспардың бекітілген күні мен нөмірі;

2) мемлекеттік органның атауы;

3) бақылау субъектісінің атауы;

4) бақылау субъектісінің (объектісінің) тұрған жері;

5) тексеру жүргізу мерзімдері;

6) тексерудің нысанасы;

7) жоспарға қол қоюға уәкілеттік берілген адамның қолтаңбасы.

Мерзімдік тексерулер жүргізу жоспарына өзгерістер мен толықтырулар енгізу бақылау субъектісі таратылған, қайта ұйымдастырылған, оның атауы өзгерген немесе өкілеттіктері бақылау субъектілері арасында қайта бөлінген жағдайларда жүзеге асырылады.

3. Уәкілетті орган мынадай:

1) бақылау субъектісіне қатысты жеке және заңды тұлғалардан келіп түскен, Қазақстан Республикасының цифрлық заңнамасы талаптарының бұзылуы туралы расталған жолданымдар болған;

2) құқықтары мен заңды мүдделері бұзылған жеке және заңды тұлғалар жүгінген;

3) жеке және заңды тұлғалардың, мемлекеттің құқықтары мен заңды мүдделеріне зиян келтірудің нақты фактілері бойынша не зиян келтіру қатері туралы прокурор талап еткен;

4) жеке және заңды тұлғалардың, мемлекеттің құқықтары мен заңды мүдделеріне зиян келтірудің нақты фактілері бойынша, сондай-ақ жойылмауы жеке және заңды тұлғалардың құқықтары мен заңды мүдделеріне зиян келтіруге алып келетін Қазақстан Республикасы заңнамасы талаптарының бұзылуының нақты фактілері бойынша мемлекеттік органдар жүгінген;

5) қылмыстық қудалау органының Қазақстан Республикасының Қылмыстық-процестік кодексінде көзделген негіздер бойынша тапсырмасы болған;

6) тексеру нәтижелері туралы актінің орындалуына бақылау жүргізу қажет болған жағдайларда тағайындайтын тексеру жоспардан тыс тексеру болып табылады.

4. Уәкілетті органның лауазымды адамдарының тексеру жүргізу кезінде:

1) осы баптың 8-тармағында көрсетілген құжаттарды көрсеткен кезде тексерудің нысанасына сәйкес бақылау субъектісінің (объектісінің) аумағына және үй-жайларына кедергісіз кіруге;

2) тексеру нәтижелері туралы актіге қоса тіркеу үшін тексерудің нысанасына сәйкес қағаз және электрондық жеткізгіштердегі құжаттарды (мәліметтерді) не олардың көшірмелерін, сондай-ақ автоматтандырылған дерекқорларға (цифрлық жүйелерге)

рұқсат алуға;

3) аудио-, фото- және бейнетүсірілімді жүзеге асыруға;

4) мемлекеттік органдардың, ведомстволық бағынысты және өзге де ұйымдардың мамандарын, консультанттары мен сарапшыларын тартуға құқығы бар.

5. Бақылау субъектілері не олардың уәкілетті өкілдері тексеру жүргізілген кезде:

1) уәкілетті органның тексеру жүргізуге келген лауазымды адамдарын:

осы бапта белгіленген мерзімдерге сәйкес келмейтін, тексеруді тағайындау туралы актіде (мерзімді ұзарту туралы қосымша акт болған кезде онда) көрсетілген мерзімдер асып кеткен не өтіп кеткен;

осы баптың 8-тармағында көзделген құжаттар болмаған жағдайларда тексеруге жібермеуге;

2) тексеру нәтижелері туралы актіге Қазақстан Республикасының заңнамасында белгіленген тәртіппен шағым жасауға құқылы.

6. Бақылау субъектілері не олардың уәкілетті өкілдері тексеру жүргізілген кезде:

1) уәкілетті органның лауазымды адамдарының бақылау субъектісінің (объектісінің) аумағына және үй-жайларына кедергісіз кіруін қамтамасыз етуге;

2) уәкілетті органның лауазымды адамдарына тексеру нәтижелері туралы актіге қоса тіркеу үшін тексерудің нысанасына сәйкес қағаз және электрондық жеткізгіштердегі құжаттарды (мәліметтерді) не олардың көшірмелерін ұсынуға, сондай-ақ автоматтандырылған дерекқорларға (цифрлық жүйелерге) рұқсат беруге;

3) тексеруді тағайындау туралы актінің және тексеру нәтижелері туралы актінің екінші данасына тексеру аяқталған күні белгі жасауға міндетті.

7. Тексеру тексеруді тағайындау туралы акт негізінде жүргізіледі.

Тексеруді тағайындау туралы актіде мыналар көрсетіледі:

1) актінің күні мен нөмірі;

2) мемлекеттік органның атауы;

3) тексеру жүргізуге уәкілеттік берілген адамның (адамдардың) тегі, аты, әкесінің аты (егер ол жеке басты куәландыратын құжатта көрсетілсе) және лауазымы;

4) мемлекеттік органдардың, ведомстволық бағынысты және өзге де ұйымдардың тексеру жүргізуге тартылатын мамандары, консультанттары мен сарапшылары туралы мәліметтер;

5) бақылау субъектісінің атауы, оның тұрған жері.

Мемлекеттік органның құрылымдық бөлімшесі тексерілген жағдайда тексеруді тағайындау туралы актіде оның атауы мен тұрған жері көрсетіледі;

6) тексерудің нысанасы;

7) тексеру түрі;

8) тексеру жүргізу мерзімі;

9) тексеру жүргізу негіздері;

10) тексерілетін кезең;

11) бақылау субъектісінің құқықтары мен міндеттері;

12) бақылау субъектісі басшысының не оның уәкілетті адамының актіні алғаны немесе алудан бас тартқаны туралы қолтаңбасы;

13) актіге қол қоюға уәкілеттік берілген адамның қолтаңбасы.

Тексеру жүргізу кезінде уәкілетті орган тексеру жүргізу нысанасын көрсете отырып, ол басталғанға дейін кемінде бір тәулік бұрын бақылау субъектісін тексеру жүргізудің басталатыны туралы хабардар етуге міндетті.

Бақылау субъектісіне тексеруді тағайындау туралы акт табыс етілген күн тексеру жүргізудің басталуы деп есептеледі.

8. Уәкілетті органның объектіге тексеруге келген лауазымды адамдары бақылау субъектісіне:

1) тексеруді тағайындау туралы актіні;

2) қызметтік куәлігін не сәйкестендіру картасын;

3) қажет болған кезде құзыретті органның режимдік объектілерге баруға рұқсатын көрсетуге міндетті.

9. Тексеру жүргізу мерзімі тексерудің нысанасы, сондай-ақ алдағы жұмыстардың көлемі ескеріле отырып белгіленеді және он жұмыс күнінен аспауға тиіс.

Тексеру жүргізу мерзімі он бес жұмыс күнінен аспайтын мерзімге бір рет қана ұзартылуы мүмкін. Ұзарту уәкілетті орган басшысының шешімімен жүзеге асырылады.

Тексеру жүргізу мерзімдерін ұзарту бақылау субъектісі хабардар етіле отырып, тексеру мерзімдерін ұзарту туралы қосымша актімен ресімделеді, онда тексеруді тағайындау туралы алдыңғы акт бұйрығының күні мен нөмірі және ұзарту себептері көрсетіледі.

Тексеру мерзімдерін ұзарту туралы хабарламаны уәкілетті орган табыс етілгені туралы хабарламамен бақылау субъектісіне ұзартылғанға дейін бір жұмыс күні бұрын табыс етеді.

10. Тексеру нәтижелері бойынша уәкілетті органның тексеруді жүзеге асыратын лауазымды адамдары тексеру нәтижелері туралы акт жасайды.

Тексеру нәтижелері туралы актінің бірінші данасы цифрлық нысанда өз құзыреті шегінде мемлекеттік құқықтық статистика және арнайы есепке алу саласында қызметті жүзеге асыратын мемлекеттік органға, екінші данасы бақылау субъектісінде түпнұсқасы бар құжаттардың көшірмелерін қоспағанда, қосымшалардың көшірмелерімен бірге танысу және анықталған бұзушылықтарды жою бойынша шаралар мен басқа да әрекеттер қабылдау үшін қағаз жеткізгіште қол қойғызып немесе цифрлық нысанда бақылау субъектісіне (басшысына не оның уәкілетті адамына) табыс етіледі, үшінші данасы уәкілетті органда қалады.

11. Тексеру нәтижелері туралы актіде мыналар көрсетіледі:

1) актінің жасалған күні, уақыты және орны;

2) мемлекеттік органның атауы;

3) тексеруді тағайындау туралы актінің (мерзімді ұзарту туралы қосымша акт болған кезде оның) күні мен нөмірі;

4) тексеру жүргізген адамның (адамдардың) тегі, аты, әкесінің аты (егер ол жеке басты куәландыратын құжатта көрсетілсе) және лауазымы;

5) мемлекеттік органдардың, ведомстволық бағыныстағы және өзге де ұйымдардың тексеру жүргізуге тартылатын мамандары, консультанттары мен сарапшылары туралы мәліметтер;

6) бақылау субъектісінің атауы, оның тұрған жері;

7) тексерудің нысанасы;

8) тексеру түрі;

9) тексеру жүргізу мерзімі мен кезеңі;

10) тексеру нәтижелері туралы, оның ішінде анықталған бұзушылықтар және олардың сипаты туралы мәліметтер;

11) орындалу мерзімі көрсетілген, Қазақстан Республикасының цифрлық заңнамасы талаптарының анықталған бұзушылықтарын жою туралы талаптар;

12) бақылау субъектісі басшысының не оның уәкілетті адамының, сондай-ақ тексеру жүргізу кезінде қатысқан адамдардың актімен танысқаны немесе танысудан бас тартқаны туралы мәліметтер, олардың қолтаңбалары немесе қол қоюдан бас тарту туралы жазба;

13) тексеру жүргізген лауазымды адамдардың қолтаңбасы.

Тексеру нәтижелері туралы актіге тексеру нәтижелеріне байланысты құжаттар (олар болған кезде) және олардың көшірмелері қоса беріледі.

12. Тексеру нәтижелері бойынша ескертулер және (немесе) қарсылықтар болған жағдайда бақылау субъектісі оларды жазбаша түрде жазады. Ескертулер және (немесе) қарсылықтар тексеру нәтижелері туралы актіге қоса беріледі, бұл туралы тиісті белгі жасалады.

Уәкілетті орган бақылау субъектісінің тексеру нәтижелері туралы актіге ескертулерін және (немесе) қарсылықтарын қарауға және он бес жұмыс күні ішінде уәжді жауап беруге тиіс.

Тексеру нәтижелері туралы актіні қабылдаудан бас тартылған жағдайда акт жасалады, оған тексеруді жүзеге асыратын лауазымды адамдар және бақылау субъектісінің басшысы не оның уәкілетті өкілі қол қояды.

Бақылау субъектісі бас тарту себебі туралы жазбаша түсіндірме бере отырып, актіге қол қоюдан бас тартуға құқылы.

13. Тексеру нәтижелері туралы акт бақылау субъектісіне тексеруді тағайындау туралы актіде немесе тексеру мерзімдерін ұзарту туралы қосымша актіде көрсетілген тексерудің аяқталу мерзімінен кешіктірілмей табыс етілген күн тексеру мерзімінің аяқталуы деп есептеледі.

14. Тексеру нәтижелері туралы актінің орындалу мерзімдері оны орындаудың нақты мүмкіндігіне әсер ететін мән-жайлар ескеріле отырып, бірақ тексеру нәтижелері туралы акт табыс етілген күннен бастап кемінде күнтізбелік он күн болып

айқындалады.

15. Тексеру нәтижелері туралы актінің орындалу мерзімдерін айқындау кезінде:

1) бақылау субъектісінде бұзушылықтарды жою бойынша ұйымдастырушылық, техникалық мүмкіндіктердің болуы;

2) мемлекеттік органдарда Қазақстан Республикасының заңдарында белгіленген міндетті қорытындыларды, келісулерді және басқа да құжаттарды алу мерзімдері ескеріледі.

16. Тексеру нәтижелері туралы актіде белгіленген анықталған бұзушылықтарды жою мерзімі өткеннен кейін бақылау субъектісі тексеру нәтижелері туралы актіде белгіленген мерзім ішінде уәкілетті органға растайтын құжаттармен бірге анықталған бұзушылықтардың жойылғаны туралы ақпарат беруге міндетті.

Анықталған бұзушылықтардың жойылғаны туралы ақпарат берілмеген жағдайда уәкілетті орган осы баптың 3-тармағының 6) тармақшасына сәйкес жоспардан тыс тексеру тағайындауға құқылы.

17. Тексеруді жүзеге асыру кезінде бақылау субъектісінің құқықтары мен заңды мүдделері бұзылған жағдайда бақылау субъектісі уәкілетті органның лауазымды адамдарының шешімдеріне, әрекеттеріне (әрекетсіздігіне) жоғары тұрған лауазымды адамға не Қазақстан Республикасының заңнамасында белгіленген тәртіппен сотқа шағым жасауға құқылы.

11-тарау. Киберқауіпсіздік саласын дамыту және осы саладағы халықаралық ынтымақтастық

Ескерту. 11-тараудың тақырыбы жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

61-бап. Киберқауіпсіздік саласын дамытуды мемлекеттік қолдау

1. Киберқауіпсіздік саласын дамытуды мемлекеттік қолдауды Қазақстан Республикасында киберқауіпсіздік саласын дамытуды ынталандыру мақсатында уәкілетті мемлекеттік органдар, киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институты және басқа да ұлттық даму институттары жүзеге асырады.

2. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық даму институты өз қызметін осы Заңға сәйкес жүзеге асырады.

3. Киберқауіпсіздік саласын дамытуды мемлекеттік қолдаудың негізгі қағидаттары:

1) киберқауіпсіздік саласын жеке кәсіпкерлік және мемлекеттік-жекешелік әріптестік базасында дамыту;

2) киберқауіпсіздікті әзірлеуге тапсырыстар алу кезінде отандық заңды тұлғаларға басымдық беру;

3) отандық бағдарламалық қамтылым, бағдарламалық өнімдер өндірісін және техникалық құралдар өндірісін дамытуды ынталандыру;

4) киберқауіпсіздік нарығының құрылымын дамыту;

5) киберқауіпсіздік нарығында адал бәсекелестікті қолдау.

4. Мемлекеттік қолдау қағидаттарына сәйкес Қазақстан Республикасының

Кәсіпкерлік кодексінде көзделген шаралардан басқа, мыналар киберқауіпсіздік саласын дамыту жөніндегі шаралар болып табылады:

1) киберқауіпсіздік саласындағы қызметтің нормативтік-әдіснамалық базасын қалыптастыру және дамыту, оның ішінде халықаралық стандарттарды ендіру;

2) киберқауіпсіздік саласындағы жобаларды қаржыландыру;

3) киберқауіпсіздік саласындағы жобаларды венчурлік және өзге де бюджеттен тыс өтеулі қаржыландыру үшін жағдайлар жасау;

4) заңды тұлғалардың жарғылық капиталдарына қатысу, заңды тұлғаларды, оның ішінде шет елдердің қатысумен және Қазақстан Республикасының заңнамасында көзделген өзге де тәсілдермен құру арқылы киберқауіпсіздік саласындағы жобаларға инвестицияларды жүзеге асыру.

Ескерту. 61-бап жаңа редакцияда – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

61-1-бап. Киберқауіпсіздікті қамтамасыз ету саласындағы офтейк-келісімшарттар

Мемлекеттік органдар, мемлекеттік заңды тұлғалар және дауыс беретін акцияларының (жарғылық капиталға қатысу үлестерінің) елу және одан көп пайызы мемлекетке тиесілі заңды тұлғалар отандық цифрлық өнімдер мен киберқауіпсіздік технологияларының бәсекеге қабілеттілігін арттыру және оларды дамыту мақсатында киберқауіпсіздікті қамтамасыз ету саласындағы цифрлық өнімдер мен технологияларды әзірлеуге және жеткізуге арналған офтейк-келісімшарттарды Қазақстан Республикасының мемлекеттік сатып алу туралы заңнамасында белгіленген тәртіппен жасасуға құқылы.

Өнім беруші офтейк-келісімшарт бойынша киберқауіпсіздікті қамтамасыз ету саласындағы технологияны немесе цифрлық өнімді құруға және ендіруге міндетті, ал тапсырыс беруші мұндай өнімді шартта көзделген бағамен, көлемде, мерзімдерде және талаптарда сатып алуды қамтамасыз етуге міндетті.

Әзірлеуші жасалған офтейк-келісімшарттарды қаржыландыруды тарту кезінде қамтамасыз ету (кепіл) ретінде пайдалануға құқылы.

Ескерту. 61-1-баппен толықтырылды – ҚР 24.06.2026 № 326-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) Заңымен.

62-бап. Цифрлық технологиялар саласын кадрлық және ғылыми қамтамасыз ету

1. Мемлекет цифрлық технологиялар саласындағы мамандықтар бойынша техникалық, кәсіптік, жоғары және жоғары оқу орнынан кейінгі білімі бар мамандарды отандық және шетелдік жоғары оқу орындарында даярлау және қайта даярлау үшін жағдайлар жасайды.

2. Ұйымдар, ұлттық компаниялар, олардың үлестес тұлғалары цифрлық технологиялар саласындағы мамандықтар бойынша кәсіптік, техникалық, жоғары және жоғары оқу орнынан кейінгі білім беру ұйымдарындағы білім алушылар үшін практика базасы ретінде әрекет етеді.

3. Цифрлық технологиялар саласын ғылыми қамтамасыз ету цифрлық технологиялар саласындағы ғылыми және ғылыми-техникалық қызметті мемлекеттік қолдау арқылы, оның ішінде технологияларды коммерцияландыру үшін жағдайлар жасау арқылы жүзеге асырылады.

Ескерту. 62-бапқа өзгеріс енгізілді – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

12-тараудың тақырыбы алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

63-бап. Киберқауіпсіздік саласындағы халықаралық ынтымақтастық

1. Қазақстан Республикасының киберқауіпсіздік саласындағы халықаралық ынтымақтастығы Қазақстан Республикасы халықаралық шарттарына және заңнамасына сәйкес жүзеге асырылады.

2. Қазақстан Республикасының цифрлық орта субъектілері халықаралық ұйымдар мен бірлестіктерге кіруге, халықаралық және шетелдік жобалар мен бағдарламаларға қатысуға құқылы.

Мемлекеттік органдар уәкілетті органмен келісу бойынша киберқауіпсіздік саласында шет мемлекеттердің мемлекеттік органдарымен, халықаралық ұйымдармен және шетелдік заңды тұлғалармен өзара іс-қимылды жүзеге асырады.

3. Киберқауіпсіздік саласындағы халықаралық ынтымақтастық:

1) шет мемлекеттердің мемлекеттік органдарымен, халықаралық ұйымдармен және шетелдік заңды тұлғалармен өзара іс-қимыл жасау, оның ішінде Қазақстан Республикасының халықаралық шарттарын орындау жөніндегі іс-шараларды іске асыруға қатысу;

2) цифрлық технологияларды қолдана отырып, оның ішінде Қазақстан Республикасының ұлттық шлюзі арқылы халықаралық (мемлекетаралық) ақпараттық өзара іс-қимылдың тұрақты және қауіпсіз жүйесін қалыптастыруға көмек көрсету;

3) цифрлық технологияларды дамытуды қамтамасыз ету бойынша шетелдік заңды тұлғалармен өзара іс-қимыл жасау, сондай-ақ кадрлық даму және ғылыми ынтымақтастық;

4) цифрлық технологиялардың дамуына шетелдік заңды тұлғалармен және халықаралық ұйымдармен бірлесіп ұдайы негізде мониторинг және болжау жүргізу;

5) цифрлық технологияларды қауіпсіз пайдалану мәселелері бойынша шет мемлекеттердің мемлекеттік органдарымен және халықаралық ұйымдармен өзара іс-қимыл жасасу, сондай-ақ мемлекеттің цифрлық инфрақұрылымына қол сұғатын және мемлекеттік қызметтің саяси, экономикалық, әлеуметтік және өзге салаларын бұзатын әрекеттерге тыйым белгілеу;

6) Қазақстан Республикасында және шетелде семинарлар, конференциялар және тренингтер өткізу;

7) цифрлық технологияларды адамға, қоғамға және мемлекетке зиян келтіру тұрғысынан пайдалануға өзара түсіністік негізінде тыйым белгілеу;

8) киберқауіпсіздік саласындағы жобаларды шет мемлекеттермен, халықаралық ұйымдармен, шетелдік заңды тұлғалармен, шетелдік қоғамдық ұйымдармен және қорлармен бірлесіп қаржыландыру және іске асыру нысанында жүзеге асырылады.

4. Цифрлық технологияларды дамыту, институттық қамтамасыз ету және тәжірибе мен білім алмасу мәселелері жөніндегі халықаралық ынтымақтастық шет

мемлекеттердің мемлекеттік органдарының, халықаралық ұйымдардың және шетелдік заңды тұлғалардың қатысуымен жүзеге асырылады.

Ескерту. 63-бапқа өзгеріс енгізілді – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

13-тарау. ҚОРЫТЫНДЫ ЖӘНЕ ӨТПЕЛІ ЕРЕЖЕЛЕР

64-бап. Ақпараттандыру саласындағы мемлекеттік бақылау

Ескерту. 64-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

64-1-бап. Бақылау субъектісіне (объектісіне) бармай профилактикалық бақылау жүргізу тәртібі

Ескерту. 64-1-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

64-2-бап. Мемлекеттік органдарға қатысты Қазақстан Республикасының ақпараттандыру туралы заңнамасының сақталуына мемлекеттік бақылау жүргізу тәртібі

Ескерту. 64-2-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

65-бап. Қазақстан Республикасының киберқауіпсіздік туралы заңнамасын бұзғаны үшін жауаптылық

Қазақстан Республикасының киберқауіпсіздік туралы заңнамасын бұзу Қазақстан Республикасының заңдарына сәйкес жауаптылыққа әкеп соғады.

Ескерту. 65-бапқа өзгеріс енгізілді – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

66-бап. Өтпелі ережелер

Ескерту. 66-бап алып тасталды – ҚР 09.01.2026 № 256-VIII (алғашқы ресми жарияланған күнінен кейін алты ай өткен соң қолданысқа енгізіледі) Заңымен.

67-бап. Осы Заңды қолданысқа енгізу тәртібі

1. Осы Заң 2016 жылғы 1 қаңтардан бастап қолданысқа енгізіледі.

2. "Ақпараттандыру туралы" 2007 жылғы 11 қаңтардағы Қазақстан Республикасы Заңының (Қазақстан Республикасы Парламентінің Жаршысы, 2007 ж., № 2, 13-құжат; 2009 ж., № 15-16, 74-құжат; № 18, 84-құжат; 2010 ж., № 5, 23-құжат; № 17-18, 111-құжат; 2011 ж., № 1, 2-құжат; № 11, 102-құжат; № 15, 118-құжат; 2012 ж., № 2, 13-құжат; № 8, 64-құжат; № 14, 95-құжат; № 15, 97-құжат; 2013 ж., № 5-6, 30-құжат; № 7, 36-құжат; № 14, 75-құжат; 2014 ж., № 1, 4-құжат; № 19-I, 19-II, 96-құжат; № 23, 143-құжат) күші жойылды деп танылсын.

Қазақстан Республикасының

Президенті Н. НАЗАРБАЕВ