"Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу қағидаларын бекіту туралы" Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 2019 жылғы 16 тамыздағы № 199/НҚ бұйрығына өзгерістер енгізу туралы"

Қазақстан Республикасы Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 2026 жылғы 30 сәуірдегі № 229/НҚ бұйрығы

ЗҚАИ-ның ескертпесі!

Осы бұйрық 12.07.2026 ж. бастап қолданысқа енгізіледі

БҰЙЫРАМЫН:

1. "Меншік иесінің және (немесе) оператордың өздері жүзеге асыратын міндеттерді орындау үшін қажетті және жеткілікті дербес деректердің тізбесін айқындау қағидаларын бекіту туралы" Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2023 жылғы 21 маусымдағы № 199/НҚ бұйрығына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 19286 болып тіркелген) мынадай өзгеріс енгізілсін:

тақырып мынадай редакцияда жазылсын:

"Мемлекеттік органдардың ақпараттандыру объектілерінің киберқауіпсіздік оқиғаларына мониторинг жүргізу қағидаларын бекіту туралы";

преамбула мынадай редакцияда жазылсын:

""Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 7-1-бабының 6) тармақшасына сәйкес БҰЙЫРАМЫН:";

2. Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Ақпараттық қауіпсіздік комитеті заңнамада белгіленген тәртіппен:

1) осы бұйрықты қол қойылған күннен бастап бес жұмыс күн ішінде қазақ және орыс тілдерінде электрондық түрде Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу үшін Қазақстан Республикасы Әділет министрлігінің "Қазақстан Республикасының Заңнама және құқықтық ақпарат институты" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

2) осы бұйрықты Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігінің интернет-ресурсында орналастыруды қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Жасанды интеллект және цифрлық даму вице-министріне жүктелсін.

4. Осы бұйрық 2026 жылғы 12 шілдеден бастап қолданысқа енгізіледі және ресми жариялануға жатады.

Қазақстан Республикасы
Премьер-Министрінің орынбасары –
Жасанды интеллект және цифрлық даму министрі *Ж. Мәдиев*

"КЕЛІСІЛДІ"
Қазақстан Республикасы
Ұлттық қауіпсіздік комитеті

Бұйрығына қосымша

Мемлекеттік органдардың цифрлық объектілерінің киберқауіпсіздік оқиғаларына мониторинг жүргізу қағидалары

1-тарау. Жалпы ережелер

1. Осы Мемлекеттік органдардың цифрлық объектілерінің киберқауіпсіздік оқиғаларына мониторинг жүргізу қағидалары (бұдан әрі – Қағидалар) " Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 6) тармақшасына сәйкес әзірленді және мемлекеттік органдардың цифрлық объектілері оқиғаларына мониторинг жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар мен анықтамалар пайдаланылады:

1) киберқауіпсіздік оқиғаларын мониторингтеу – киберқауіпсіздік оқиғаларын анықтау және сәйкестендіру мақсатында цифрлық объектісін тұрақты байқау;

2) киберқауіпсіздік оқиғасы (бұдан әрі – КҚ оқиғасы) – цифрлық объектілерінің қазіргі бар қауіпсіздік саясатын ықтимал бұзу туралы не цифрлық объектілерінің қауіпсіздігіне қатысы болуы мүмкін, бұрын белгісіз болған жағдай туралы куәландыратын жай-күйі;

3) киберқауіпсіздіктің оқыс оқиғасы (бұдан әрі – АҚ оқыс оқиғасы) – цифрлық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жекелей немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қатер төндіретін және (немесе) цифрлық ресурстарды заңсыз алу, көшірмесін түсіріп алу, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын іркілістер;

4) киберқауіпсіздік үйлестірушісі – тұрақты негізде мемлекеттік органда болатын және мемлекеттік органдардың цифрлық объектілері қорғалуының жай-күйін ұстауға бағытталған іс-шараларды үйлестіруді жүзеге асыратын "МТҚ" АҚ қызметкері;

5) мемлекеттік техникалық қызмет (бұдан әрі – "МТҚ" АҚ) – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған акционерлік қоғам;

6) оқиғаларды журналдау – цифрлық объектісімен болып жатқан бағдарламалық немесе аппараттық оқиғалар туралы ақпаратты оқиғаларды тіркеу журналына жазу процесі;

7) оқиғаларды тіркеу журналдарын жинау жүйесі – цифрлық объектілерінің оқиғаларын тіркеу журналдарын орталықтандырылған жинауды, оларды сақтауды және КҚ оқиғаларын басқару жүйесіне одан әрі беруді қамтамасыз ететін аппараттық-бағдарламалық кешен;

8) цифрландыру саласындағы киберқауіпсіздік (бұдан әрі – киберқауіпсіздік) – цифрлық ресурстардың, цифрлық жүйелердің және цифрлық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі;

9) цифрлық объектілері – цифрлық ресурстар, бағдарламалық қамтылым, интернет-ресурс және цифрлық инфрақұрылым.

3. Мемлекеттік органдардың цифрлық объектілерінің киберқауіпсіздік оқиғаларының мониторингін (бұдан әрі – КҚОМ) Киберқауіпсіздіктің ұлттық үйлестіруші орталығының (бұдан әрі – КҰҮО) міндеттері мен функцияларын іске асыратын "МТҚ" АҚ жүргізеді.

4. КҚОМ объектілері мемлекеттік органның (бұдан әрі – МО) цифрлық объектілері болып табылады.

5. Мыналар:

1) мемлекеттік құпияларды құрайтын мәліметтерді қамтитын цифрлық ресурстар;

2) Қазақстан Республикасының Мемлекеттік құпиялар туралы заңнамасына сәйкес мемлекеттік құпияларға жатқызылған қорғалған орындаудағы цифрлық жүйелер, сондай-ақ арнайы мақсаттағы және/немесе үкімет, құпия, шифрланған және кодталған телекоммуникация желілері;

3) "цифрлық үкіметтің" цифрлық инфрақұрылымы объектілерімен интеграцияланбаған Қазақстан Республикасы Ұлттық Банкінің цифрлық объектілері КОМ объектілеріне жатпайды.

6. КҚОМ шеңберінде АҚ оқиғаларының көздері:

МО иелігіндегі цифрлық инфрақұрылымдағы ақпаратты қорғау құралдары (бұдан әрі – МО ЦИ), оның ішінде "МТҚ" АҚ орнататын және қолдап отыратын (бұдан әрі – КҚ оқиғаларының көздері);

КҚҰҮО АҚ оқиғаларын басқару жүйесі болып табылады.

7. КҚОМ мынадай жұмыс түрлерін:

1) МО ЦИ-де КҚ оқиғалар көздерін орнатуды;

2) КҚ оқиғалар көздерін МО ЦИ-де техникалық сүйемелдеуді;

3) КҚ оқыс оқиғаларын анықтауды және оларға кейіннен ден қою мақсатында КҚОМ объектілерінің КҚ оқиғасын қадағалауды қамтиды.

8. КҚОМ мынадай нұсқалардың бірі бойынша:

бір жұмыс түрі бойынша;

бірнеше жұмыс түрлері бойынша жүргізіледі.

9. КҚОМ-ны "МТҚ" АҚ Қазақстан Республикасының Ұлттық қауіпсіздік комитеті (бұдан әрі – ҚР ҰҚК) мен "МТҚ" АҚ арасындағы шарттық қатынастар негізінде, Қазастан Республикасының аумағында орналасқан КҚОМ-ге қатысты жүргізеді.

2-тарау. Мемлекеттік органдардың цифрлық объектілерінің киберқауіпсіздік оқиғаларына мониторинг жүргізу тәртібі

10. КҚОМ жүргізу кезінде "МТҚ" АҚ:

АҚ орнату шеңберінде:

МО ЦИ-ды зерделеуді;

КҚ аппараттық-бағдарламалық кешенін МО ЦИ-ға өрістетуді;

КҚ-тың жекелеген қорғау механизмдерін және қауіпсіздік саясатын баптауды және олардың жұмысының дұрыстығын тексеруді жүзеге асырады;

2) КҚ оқиғаларының көздерін техникалық сүйемелдеу шеңберінде:

КҚ жаңартуларын өндірушінің шығаруына қарай орнатуды;

КҚ -ның жай-күйін, олардың параметрлері мен қорғау режимдерін бақылауды, оның ішінде олардың жұмыс істеуіндегі қателер мен кемшіліктерді жоюды;

КҚ -тың жұмыс істеу мәселелері бойынша өтінімдерді өңдеуді жүзеге асырады.

3) КҚ оқыс оқиғаларын анықтау және оларға кейіннен ден қою мақсатында КҚОМ объектілерінің жай-күйін қадағалау шеңберінде:

КҚҰҰО КҚ оқиғаларын басқару жүйесіне беру үшін қажетті оқиғаларды тіркеу журналдарының тізбесін айқындауды;

"МТҚ" АҚ қолдап отыратын, КҚ оқиғаларын журналдауды ұйымдастыруды;

КҚОМ объектісі жұмыс істейтін МО телекоммуникациялық желісінің контурында КҚҰҰО оқиғаларын тіркеу журналдарын жинау жүйесін ұйымдастыруды;

КҚҰҰО оқиғаларын тіркеу журналдарын жинау жүйесіне КҚ және КОМ объектілерінің оқиғаларын тіркеу журналдарын жинауды ұйымдастыруды;

КҚҰҰО КҚ оқиғаларын басқару жүйесіне КҚОМ және КҚ объектілерінің оқиғаларын тіркеу журналдарын беруді ұйымдастыруды және КҚ оқиғалары мен КҚ оқыс оқиғаларын анықтау мақсатында оларды өңдеуді және талдауды;

КҚОМ объектісінде анықталған, КҚ оқиғаларын немесе КҚ оқыс оқиғаларын бастапқы талдауды;

КҚ оқиғасы немесе КҚ оқыс оқиғасы анықталған сәттен бастап 30 минут ішінде, ҚР ҰҚК – 3 сағат ішінде КҚ оқиғалары мен КҚ оқыс оқиғалар туралы МО немесе ол уәкілеттік берген тұлғаны хабардар етуді;

МО КҚ немесе ол уәкілеттік берген тұлғаға оқыс оқиғасының таралуын тоқтата тұру бойынша бастапқы ұсынымдар беруді;

техникалық мүмкіндік болған жағдайда КҚ оқыс оқиғасының таралуын КҚ арқылы тоқтата тұру бойынша шаралар қабылдауды;

қажет болған жағдайда КҚ оқыс оқиғаға ден қою шеңберінде "МТҚ" АҚ қызметкерінің КҚОМ объектісін орналастыру орнына жіберуді (қажеттілігіне қарай ҚР ҰҚК немесе "МТҚ" АҚ дербес айқындайды);

КҚ оқыс оқиғасы анықталған сәттен бастап 48 сағат өткеннен кейін МО немесе ол уәкілеттік берген тұлғаның КҚ оқыс оқиғасының себептері мен салдарын жоймағаны туралы ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органды (бұдан әрі – уәкілетті орган) және ҚР ҰҚК хабардар етуді жүзеге асырады.

11. Киберқауіпсіздік үйлестірушісі:

МО ЦО қорғалғандық деңгейін арттыру бойынша ұсынымдар қалыпастыру мақсатында МО-ның цифрлық инфрақұрылымын зерделеуді;

МО КҚ жөніндегі техникалық құжаттамасын өзектендіру бойынша ұсынымдар қалыптастыру және техникалық құжаттама талаптарын қайта қарау мақсатында оны зерделеуді;

МО ақпараттық-коммуникациялық инфрақұрылымында анықталған КҚ оқыс оқиғаларына ден қою жөніндегі іс-шараларды үйлестіруді;

"МТҚ" АҚ қызметкерлері орнатқан ақпаратты қорғау құралдары арқылы КҚ оқыс оқиғаларына ден қоюға жәрдемдесуді (техникалық мүмкіндік болған кезде);

МО қызметкерлерінде КҚ саласындағы хабардарлықты арттыру жөнінде іс-шаралар жүргізуге жәрдемдесуді жүзеге асырады.

12. МО немесе ол уәкілеттілік берген тұлға КОМ жүргізу кезінде:

"МТҚ" АҚ қызметкерлеріне МО цифрлық инврақұрылымына физиклық және желілік қолжетімділік және ақпаратты қорғау құралдарын орнату және қолдап отыру үшін қажетті құқықтармен есептік жазбалар ұсынады;

"МТҚ" АҚ-ға КҚОМ объектілерінің оқиғаларын тіркеу журналдарын және КҚ оқиғаларының көздерін КҚҰҰО КҚ оқиғаларды басқару жүйесіне беруді ұйымдастыру үшін телекоммуникациялар желілері контурларында IP-мекенжайлар береді;

тоқсан сайынғы негізде "МТҚ" АҚ-ға осы Қағидаларға қосымшаға сәйкес өзекті мәліметтер ұсынады;

қолданушылық және серверлік операциялық жүйелердің өзекті нұсқаларына дейін жаңартуды жүзеге асырады;

"МТҚ" АҚ-дын КҚ оқиғасының немесе сәйкесінше КҚ оқыс оқиғасының анықталғаны туралы хабарлама алған сәттен бастап 48 сағат ішінде КҚ оқиғасын талдау нәтижелері және (немесе) КҚ оқыс оқиғасын жою бойынаш қабылданған шаралар туралы "МТҚ" АҚ-ны хабардар етеді.

13. "МТҚ" АҚ КҚОМ қызметтерін көрсетуге шарттарға сәйкес, тоқсан сайын ҚР ҰҚК-ға анықталған КҚ қатерлері, КҚ оқиғалары және КҚ оқыс оқиғалары жөнінде жиынтық ақпарат, сондай-ақ олар бойынша МО қабылдаған шаралар туралы мәліметтер жолдайды.

14. ҚР ҰҚК тоқсан сайын уәкілетті органға анықталған КҚ оқыс оқиғалары жөнінде жиынтық ақпарат, сондай-ақ олар бойынша МО қабылдаған шаралар туралы мәліметтер жолдайды.

Мемлекеттік органдардың
цифрлық объектілерінің
киберқауіпсіздігі оқиғаларына
мониторинг жүргізу
қағидаларына қосымша

ККОМ объектісі туралы мәліметтер

№	Мемлекеттік органның атауы	Құрылымдық бөлімше (департамент)	Физикалық орналасқан жері (қабат, кабинет)	Пайдаланушының/ жауапты тұлғаның ТАӘ	Жұмыс станциясының / серверлік жабдықтың желілік атауы	IP-мекенжай	Операциялық жүйенің атауы
1	2	3	4	5	6	7	8
Ішкі контурдың жергілікті желісі							
Сыртқы контурдың жергілікті желісі							