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 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2019 жылғы 23 тамызда № 19286 болып тіркелді.

ЗҚАИ-ның ескертпесі!

Бұйрықтың тақырыбы жаңа редакцияда көзделген – ҚР Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 30.04.2026 № 229/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

ЗҚАИ-ның ескертпесі!

Кіріспе жаңа редакцияда көзделген – ҚР Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 30.04.2026 № 229/НҚ (12.07.2026 бастап қолданысқа енгізіледі) бұйрығымен.

"Ақпараттандыру туралы" Қазақстан Республикасы Заңының 7-1-бабының 5-1) тармақшасына сәйкес **БҰЙЫРАМЫН:**

Ескерту. Кіріспе жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 27.10.2022 № 399/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1. Қоса беріліп отырған Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу қағидалары бекітілсін.

2. Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрықты мемлекеттік тіркелген күнінен бастап күнтізбелік он күн ішінде оны қазақ және орыс тілдерінде Қазақстан Республикасының Нормативтік құқықтық актілерінің эталондық бақылау банкіне ресми жариялау және енгізу үшін "Қазақстан Республикасының Заңнама және құқықтық ақпарат институты" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

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

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

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

4. Осы бұйрық алғашқы ресми жарияланғаннан кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Цифрлық даму, инновациялар және
аэроғарыш өнеркәсібі министрінің м.а.

"КЕЛІСІЛГЕН"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасы
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрінің
2019 жылғы 16 тамыздағы
№ 199/НҚ бұйрығымен
бекітілген

Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу қағидалары

Ескерту. Қағида жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 27.10.2022 № 399/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу қағидалары (бұдан әрі – Қағидалар) " Ақпараттандыру туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 5-1) тармақшасына сәйкес әзірленді және мемлекеттік органдардың ақпараттандыру объектілері оқиғаларына мониторинг жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар мен анықтамалар пайдаланылады:

1) ақпараттандыру объектілері – электрондық ақпараттық ресурстар, бағдарламалық қамтылым, интернет-ресурс және ақпараттық-коммуникациялық инфрақұрылым;

2) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – ақпараттық қауіпсіздік) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және

ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі;

3) ақпараттық қауіпсіздік оқиғаларын мониторингтеу – ақпараттық қауіпсіздік оқиғаларын анықтау және сәйкестендіру мақсатында ақпараттандыру объектісін тұрақты байқау;

4) ақпараттық қауіпсіздік оқиғасы (бұдан әрі – АҚ оқиғасы) – ақпараттандыру объектілерінің қазіргі бар қауіпсіздік саясатын ықтимал бұзу туралы не ақпараттандыру объектілерінің қауіпсіздігіне қатысы болуы мүмкін, бұрын белгісіз болған жағдай туралы куәландыратын жай-күйі;

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

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

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

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

9) ақпараттық қауіпсіздік үйлестірушісі – тұрақты негізде мемлекеттік органда болатын және мемлекеттік органдардың ақпараттандыру объектілері қорғалуының жай-күйін ұстауға бағытталған іс-шараларды үйлестіруді жүзеге асыратын "МТҚ" АҚ қызметкері;

Осы Қағидаларда пайдаланылатын өзге де ұғымдар Заңға сәйкес қолданылады.

3. Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларының мониторингін (бұдан әрі – АҚОМ) Ақпараттық қауіпсіздіктің ұлттық үйлестіруші орталығының (бұдан әрі – АҚҰҮО) міндеттері мен функцияларын іске асыратын "МТҚ" АҚ жүргізеді.

4. АҚОМ объектілері мемлекеттік органның (бұдан әрі – МО) ақпараттандыру объектілері болып табылады.

5. Мыналар:

1) мемлекеттік құпияларды құрайтын мәліметтерді қамтитын электрондық ақпараттық ресурстар;

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

3) "электрондық үкіметтің" ақпараттық-коммуникациялық инфрақұрылымы объектілерімен интеграцияланбаған Қазақстан Республикасы Ұлттық Банкінің ақпараттандыру объектілері АҚОМ объектілеріне жатпайды.

6. АҚОМ шеңберінде АҚ оқиғаларының көздері:

МО иелігіндегі ақпараттық-коммуникациялық инфрақұрылымдағы ақпаратты қорғау құралдары (бұдан әрі – МО АКИ), оның ішінде "МТҚ" АҚ орнататын және қолдап отыратын (бұдан әрі – АҚ оқиғаларының көздері);

ҰАҚҰО АҚ оқиғаларын басқару жүйесі болып табылады.

7. АҚОМ мынадай жұмыс түрлерін:

1) МО АКИ-де АҚ оқиғалар көздерін орнатуды;

2) АҚ оқиғалар көздерін МО АКИ-де техникалық сүйемелдеуді;

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

8. АҚОМ мынадай нұсқалардың бірі бойынша:

1) бір жұмыс түрі бойынша;

2) бірнеше жұмыс түрлері бойынша;

3) жұмыс түрлерінің толық құрамында жүргізіледі.

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

2-тарау. Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу тәртібі

10. АҚОМ жүргізу кезінде "МТҚ" АҚ:

1) АҚ орнату шеңберінде:

МО АКИ-ды зерделеуді;

АҚ аппараттық-бағдарламалық кешенін МО АКИ-ға өрістетуді;

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

2) АҚ оқиғаларының көздерін техникалық сүйемелдеу шеңберінде:

АҚ жаңартуларын өндірушінің шығаруына қарай орнатуды;

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

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

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

ҰАҚҰО АҚ оқиғаларын басқару жүйесіне беру үшін қажетті оқиғаларды тіркеу журналдарының тізбесін айқындауды;

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

АҚОМ объектісі жұмыс істейтін МО телекоммуникациялық желісінің контурында ҰАҚҰО оқиғаларын тіркеу журналдарын жинау жүйесін ұйымдастыруды;

ҰАҚҰО оқиғаларын тіркеу журналдарын жинау жүйесіне АҚ және АҚОМ объектілерінің оқиғаларын тіркеу журналдарын жинауды ұйымдастыруды;

ҰАҚҰО АҚ оқиғаларын басқару жүйесіне АҚОМ және АҚ объектілерінің оқиғаларын тіркеу журналдарын беруді ұйымдастыруды және АҚ оқиғалары мен АҚ оқыс оқиғаларын анықтау мақсатында оларды өңдеуді және талдауды;

АҚОМ объектісінде анықталған, АҚ оқиғаларын немесе АҚ оқыс оқиғаларын бастапқы талдауды;

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

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

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

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

АҚ оқыс оқиғасы анықталған сәттен бастап 48 сағат өткеннен кейін МО немесе ол уәкілеттік берген тұлғаның АҚ 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. Ақпараттық қауіпсіздік үйлестірушісі:

МО АО қорғалғандық деңгейін арттыру бойынша ұсынымдар қалыпастыру мақсатында МО-ның ақпараттық-коммуникациялық инфрақұрылымын зерделеуді;

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

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

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

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

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

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

"МТҚ" АҚ-ға АҚОМ объектілерінің оқиғаларын тіркеу журналдарын және АҚ оқиғаларының көздерін АҚҰҰО АҚ 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 АҚ оқиғасының немесе сәйкесінше АҚ оқыс оқиғасының анықталғаны туралы хабарлама алған сәттен бастап 48 сағат ішінде АҚ оқиғасын талдау нәтижелері және (немесе) АҚ оқыс оқиғасын жою бойынаш қабылданған шаралар туралы "МТҚ" АҚ-ны хабардар етеді.

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

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

Мемлекеттік органдардың
ақпараттандыру объектілерінің
ақпараттық қауіпсіздігі
оқиғаларына мониторинг
жүргізу қағидаларына
қосымша

АҚОМ объектісі туралы мәліметтер

№	Мемлекеттік органның атауы	Құрылымдық бөлімше (департамент)	Физикалық орналасуы (этаж, 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 локалды желісі							
Сыртқы контурдың локалды желісі							