

Кейбір бұйрықтарға өзгерістер мен толықтыру енгізу туралы

Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2022 жылғы 27 қазандағы № 399/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2022 жылғы 31 қазанда № 30354 болып тіркелді

БҰЙЫРАМЫН:

1. Қоса беріліп отырған өзгерістер мен толықтыру енгізілетін кейбір бұйрықтардың тізбесі бекітілсін:

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

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

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

3) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін күнтізбелік он жұмыс күні ішінде Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Заң департаментіне осы тармақтың 1) және 2) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер 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 жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Цифрлық даму, инновациялар және
аэроғарыш өнеркәсібі министрі

Б. Мусин

"КЕЛІСІЛДІ"

Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасының
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрі
2022 жылғы 27 қазандағы
№ 399/НҚ Бұйрықпен
бекітілген

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің өзгерістер мен толықтыру енгізілетін кейбір бұйрықтарының тізбесі

"Электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды резервтік сақтаудың бірыңғай платформасына беру қағидаларын бекіту туралы" Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 16 наурыздағы № 45/НҚ бұйрығына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16883 болып тіркелген) мынадай өзгерістер енгізілсін:

тақырып мынадай редакцияда жазылсын:

"Электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беру қағидаларын бекіту туралы";

кіріспе мынадай редакцияда жазылсын:

"Ақпараттандыру туралы" Қазақстан Республикасы Заңының 17-бабы 2-1-тармағының 4) тармақшасына сәйкес **БҰЙЫРАМЫН**";

1-тармақ мынадай редакцияда жазылсын:

"1. Электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беру қағидалары бекітілсін.";

көрсетілген бұйрықпен бекітілген Электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды резервтік сақтаудың бірыңғай платформасына беру қағидаларында:

тақырып мынадай редакцияда жазылсын:

"Электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беру қағидалары";

1-тармақ мынадай редакцияда жазылсын:

"1. Осы электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беру қағидалары (бұдан әрі – Қағидалар) "Ақпараттандыру туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 17-бабы 2-1-тармағының 4) тармақшасының негізінде әзірленді және электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына берудің тәртібі мен мерзімдерін.";

2-тармақ жаңа редакцияда жазылсын:

"2. Осы Қағидаларда мынадай негізгі ұғымдар пайдаланылады:

1) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) – ақпараттық қауіпсіздікті қамтамасыз ету саласындағы басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган;

2) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері (бұдан әрі - АКИАМО) - жұмыс істеуінің бұзылуы немесе тоқтауы қолжетімділігі шектеулі дербес деректерді және заңмен қорғалатын құпия қамтылған өзге де мәліметтерді заңсыз жинауға және өңдеуге, әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайға 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 құрылыстар, құқық қорғау қызметі, "электрондық үкімет" инфрақұрылымы үшін елеулі теріс салдарларға алып келетін ақпараттық-коммуникациялық инфрақұрылым объектілері;

3) жедел резервтеу – қосымша бағдарламалық және техникалық құралдарды пайдалану және оларды белсенді режимде ұстау және (немесе) нақты уақыт режимінде (немесе 1 сағатқа кідірумен нақты уақытқа жақын) өзгерістерді беруді және ақпараттың сақталуын қамтамасыз ету;

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

5) резервтік көшірме – резервтік көшірме – жоғалту, зақымдау, бұзу, немесе заңсыз өзгерту, жою жағдайында деректердің бастапқы және қажет болған жағдайда олардың орналасқан жаңа орнын қалпына келтіру үшін жобаланған электрондық тасымалдағышта мәліметтер базасы көшірмесін және қажет болған жағдайда қолданбалы бағдарламалық қамтылым жасау процесін сәтті аяқтаудың нәтижесі;

6) ұзақ мерзімді сақтау – электрондық ақпараттық ресурстардың резервтік көшірмелерін екі жылдан арттық сақтау мерзімімен электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына бір реттік беру;

7) іске қосусыз резервтеу – деректерді қалпына келтіру мүмкіндігін қамтамасыз ету мақсатында жұмыс істеп тұрған немесе сөндірілген электрондық ақпараттық ресурстар операциялық жүйе құралдарымен резервтік көшірме жасау;

8) электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасы (бұдан әрі – БҰРП) – электрондық ақпараттық ресурстардың сақталуын қамтамасыз ету және қажет болған жағдайда деректерді қалпына келтіру мақсатында, олардың резервтік көшірмелерін сақтауға арналған аппараттық-бағдарламалық кешен."

;

3-тармақ алып тасталсын;

2-тараудың тақырыбы мынадай редакцияда жазылсын:

"2-тарау Электрондық ақпараттық ресурстардың резервтік көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беру тәртібі";

5-тармақ мынадай редакцияда жазылсын:

"5. "МТҚ" АҚ АКИАМО иелеріне ЭАР резервтік көшірмелерін БҰРП-ға беру қажеттілігі туралы ақпаратты жібереді.";

6-тармақтың бірінші абзацы мынадай редакцияда жазылсын:

"6. АКИАМО иелері "МТҚ" АҚ-дан ақпаратты алған сәттен бастап 15 (он бес) жұмыс күннен кешіктірмей "МТҚ" АҚ-ға әрбір ЭАР бойынша:";

7-тармақ мынадай редакцияда жазылсын:

"7. Занның 6-бабының 4) тармақшасына сәйкес бекітілетін АКИАМО тізбесіне (бұдан әрі – Тізбе) және әрбір АКИАМО иелерінен алынған ақпарат негізінде "МТҚ" АҚ уәкілетті органмен келісім бойынша БҰРП-ға беру үшін ЭАР резервтік көшірудің мерзімділігін белгілейді.";

8-тармақтың бірінші абзацы мынадай редакцияда жазылсын:

"8. "МТҚ" АҚ АКИАМО иелеріне 20 (жиырма) жұмыс күн ішінде танысу мен орындау үшін жазбаша ресми түрде мынадай мәліметтер жолдайды:";

9-тармақ мынадай редакцияда жазылсын:

"9. "МТҚ" АҚ резервтік көшірмелерін беру үшін АҚҰҰО АКИАМО иелеріне АҚҰҰО-ға қолжетімділік береді.";

10-тармақ мынадай редакцияда жазылсын:

"10. АКИАМО иелері өз қаражаты есебінен, АКИАМО иелерінің барлық инфрақұрылымының толық жоғалту (жойылу) жағдайларын есепке ала отырып, БҰРП-да сақталатын резервтік көшірмелерді АКИАМО-ның қалпына келтіруі үшін жеткілікті көлемде, БҰРП-ға ("МТҚ" АҚ) ЭАР резервтік көшірмелерін (сондай-ақ ЭАР-ға құжаттама, нұсқаулық көшірмелерін, конфигурация файлдарын және тағы басқа) дербес беруді ұйымдастырады. АКИАМО-ның резервтік көшірмелерінің берілуі, БҰРП-ға резервтік көшірмелерді қабылдау уақытша кейінге шегеру жағдайларынан басқа, "МТҚ" АҚ-дан ресми хабарлама алған күннен бастап 20 (жиырма) жұмыс күн ішінде іске асырылады.";

11-тармақ мынадай редакцияда жазылсын:

"11. Резервтік көшірме шифрланған түрде берілген жағдайда, шифрлау кілттері мен құралды шифрлау жүргізілген құралдар шифрді ашу үшін ЭАР иелері жағында барлық инфрақұрылым жоғалған жағдайда қалпына келтіру мүмкіндігі үшін электрондық түрде "МТҚ" АҚ-ға беруге жатады.

13-тармақтың бірінші абзацы мынадай редакцияда жазылсын:

"13. "МТҚ" АҚ ЭАР резервтік көшірмелерін қабылдауды:";

14-тармақ мынадай редакцияда жазылсын:

"14. ЭАР резервтік көшірмелерін қабылдауды уақытша тоқтату үшін негіз "МТҚ" АҚ уәкілетті орган мен АКИАМО иесіне себебін көрсете отырып ЭАР резервтік көшірмелерін беру процесін тоқтата тұру қажеттілігі туралы жіберген ақпарат болып табылады. ЭАР резервтік көшірмелерін қабылдауды уақытша тоқтату мерзімі уәкілетті органмен келісім бойынша осы Қағидалардың 13-тармағында көрсетілген жағдайлар жойылғанға дейін белгіленеді.";

3-тараудың тақырыбы мынадай редакцияда жазылсын:

"3-тарау. Электронды ақпараттық ресурстардың резервті көшірмелерін электрондық ақпараттық ресурстарды сақтаудың бірыңғай ұлттық резервтік платформасына беру мерзімдері";

16-тармақ мынадай редакцияда жазылсын:

"16. ЭАР Тізбеден алынған жағдайда АКИАМО иесі "МТҚ" АҚ-дан ақпарат алған күннен бастап 24 сағат ішінде АҚҰҰО-ға ЭАР резервтік көшірмелерін беруді тоқтатады.";

осы Қағидаларға қосымша осы Тізбеге 1-қосымшаға сәйкес жаңа редакцияда жазылсын.

2. "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларын бекіту туралы" Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ бұйрығына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 17019 болып тіркелген) мынадай өзгерістер мен толықтыру енгізілсін:

кіріспе мынадай редакцияда жазылсын:

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

көрсетілген бұйрықпен бекітілген "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларында:

1-тармақ мынадай редакцияда жазылсын:

"1. Осы "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидалары (бұдан әрі – Қағидалар) "Ақпараттандыру туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 7) тармақшасына сәйкес әзірленді және "электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу тәртібін айқындайды.";

2-тармақ жаңа редакцияда жазылсын:

2. Осы Қағидаларда мынадай терминдер мен аббревиатуралар пайдаланылады:

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

2) ақпараттандыру объектілерінің иеленушісі – ақпараттандыру объектілерінің меншік иесі заңда немесе келісімде айқындалған шектерде және тәртіппен ақпараттандыру объектілерін иелену және пайдалану құқықтарын берген субъект;

3) ақпараттандыру объектісінің осалдығы – бағдарламалық немесе аппараттық қамтылымда жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын заңсыз іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық немесе аппараттық қамтылымдағы кемшілік;

4) ақпараттық қауіпсіздік жөніндегі техникалық құжаттама – ақпараттандыру объектілерінің және (немесе) ұйымның ақпараттық қауіпсіздікті (бұдан әрі – АҚ) қамтамасыз ету процестеріне қатысты саясатты, қағидаларды, қорғау шараларын белгілейтін құжаттама;

5) ақпараттық қауіпсіздік оқиғаларын басқару жүйесі – ақпараттандыру объектілері оқиғаларын тіркеу журналын талдау және жинау жолымен ақпараттық қауіпсіздік оқыс оқиғаларын және ақпараттық қауіпсіздік оқиғаларын анықтауды автоматтандыруға арналған бағдарламалық қамтылым немесе аппараттық-бағдарламалық кешен;

6) ақпараттық қауіпсіздік оқиғаларын басқару жүйесінің агенті – оқиғаларды тіркеу журналын жинау үшін ақпараттандыру объектісінің серверлік жабдығына орнатылған бағдарламалық қамтылым;

7) ақпараттық қауіпсіздік 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;

8) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) – ақпараттық қауіпсіздікті қамтамасыз ету саласындағы басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган;

9) ақпараттық қауіпсіздікті қамтамасыз ету мониторингінің жүйесі – ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалану мониторингін жүргізуге бағытталған ұйымдастырушылық және технологиялық іс-шаралар;

10) ақпараттық қауіпсіздіктің жедел орталығы (бұдан әрі – АҚЖО) – электрондық ақпараттық ресурстарды, ақпараттық жүйелерді, телекоммуникация желілері мен ақпараттандырудың басқа да объектілерін қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі;

11) ақпараттық қауіпсіздіктің 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, көшімесін түсіріп алу, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын іркілістер;

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

13) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері – жұмыс істеуінің бұзылуы немесе тоқтауы қолжетімділігі шектеулі дербес деректерді және заңмен қорғалатын құпия қамтылған өзге де мәліметтерді заңсыз жинауға және өңдеуге, әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайға 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 құрылыстар, құқық қорғау қызметі, "электрондық үкімет" инфрақұрылымы үшін елеулі теріс салдарларға алып келетін ақпараттық-коммуникациялық инфрақұрылым объектілері;

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

15) оқиғаларды тіркеу журналдарын жинау жүйесі – ақпараттандыру объектілері оқиғаларын тіркеу журналдарының орталықтандырылған жинағын, олардың сақталуын және одан әрі ақпараттық қауіпсіздік оқиғаларын басқару жүйесіне беруді қамтамасыз ететін аппараттық-бағдарламалық кешен;

16) "электрондық үкіметтің" ақпараттандыру объектілері (бұдан әрі – ЭҮ АО) – мемлекеттік функцияларды жүзеге асыру және мемлекеттік қызметтерді көрсету, мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік электрондық ақпараттық ресурстар, мемлекеттік органдардың бағдарламалық қамтамасыз етуі, мемлекеттік органның интернет-ресурстары, "электрондық үкіметтің" ақпараттық-коммуникациялық инфрақұрылым объектілері, оның ішінде өзге тұлғалардың ақпараттандыру объектілері;

17) "электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингі (бұдан әрі – АҚҚМ) – АҚ қауіп-қатерлері мен оқыс оқиғаларын анықтау арқылы ЭҮ АО АҚ қамтамасыз ету бойынша техникалық және ұйымдастыру іс-шараларын "электрондық үкіметтің" ақпараттандыру объектілерінің иелері және (немесе) меншік иелерімен іске асырудың толықтығы мен сапасын қадағалау.

18) "электрондық үкіметтің" архитектуралық порталы – мемлекеттік органдардың ақпараттандыру саласында мониторингтеу, талдау және жоспарлау үшін одан әрі

пайдалануы мақсатында "электрондық үкіметтің" ақпараттандыру объектілері туралы мәліметтерді, "электрондық үкіметтің" архитектурасын есепке алуды, сақтауды және жүйелеуді жүзеге асыруға арналған ақпараттандыру объектісі.

3-тармақтың бірінші абзацы мынадай редакцияда жазылсын:

3. АҚҚМ-ны Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығының (бұдан әрі – АҚҰҰО) міндеттері мен функцияларын іске асыратын "МТҚ" АҚ Заңның 14-бабының 1-тармағының 15) тармақшасына сәйкес, АҚҰҰО АҚҚМ жүйесі арқылы жүргізеді және мынадай жұмыс түрлерін қамтиды:

6-тармақ мынадай редакцияда жазылсын:

6. АКИАМО-ға жатқызылған ЭҰ АО АҚҚМ Қазақстан Республикасының Ұлттық қауіпсіздік комитеті (бұдан әрі – ҚР ҰҚК) мен "МТҚ" АҚ арасындағы шарттық қатынастар негізінде жүзеге асырылады.

7-тармақтың бірінші абзацы мынадай редакцияда жазылсын:

7. "МТҚ" АҚ АҚҚМ жүргізу үшін бастапқы ақпарат ретінде "электрондық үкімет" архитектуралық порталынан АҚҚМ объектісі туралы мәліметтерді, сондай-ақ сервистік бағдарламалық өнімнің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсының және ақпараттық жүйенің ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақ жүргізу кезеңдерінен алынған мәліметтерді қолданады, оның ішінде:

8-тармақ мынадай редакцияда жазылсын:

8. АҚҚМ объектісінің меншік иесі немесе иеленушісі АҚҚМ объектісінің өнеркәсіптік пайдалануға енгізілгені немесе пайдаланудың тоқтатылғаны туралы өнеркәсіптік пайдалануға енгізілген күннен бастап 10 жұмыс күні ішінде немесе пайдаланудың тоқтатылуы туралы ресми хатпен "МТҚ" АҚ-ға хабарлайды және осы Қағидалардың 1-қосымшасына сәйкес нысан бойынша ЭҰ АО туралы мәліметті қағаз және электронды түрде ұсынады (бұдан әрі – Мәліметтер).

9-тармақ мынадай редакцияда жазылсын:

9. "МТҚ" АҚ АҚОМ бойынша жұмыстар жүргізу кестесін әзірлейді және оны ҚР ҰҚК-пен келіседі.

10-тармақ мынадай редакцияда жазылсын:

10. "МТҚ" АҚ АҚҚМ жүргізу кезінде:

1) АҚ оқыс оқиғаларына ден қою мониторингі шеңберінде:

АҚҰҰО АҚ оқиғаларын басқару жүйесіне жіберу үшін қажетті оқиғаларды тіркеу журналының тізбесін анықтауға АҚҚМ объектілерін талдауды;

АҚҚМ объектісінің оқиғаларды тіркеу журналын жинаудың жүйесіне және қажет болған жағдайда АҚҚМ объектісінің меншік иесі немесе иеленушісінің өзге ақпараттық-коммуникациялық инфрақұрылым объектілеріне АҚ оқиғаларын басқару жүйелерінің агентін орнатуды;

АҚҚМ объектісінің оқиғаларын және АҚҰҰО АҚ оқиғаларын басқару жүйесіндегі оған жататын ақпаратты қорғау құралдарын тіркеу журналдарын жинауды, АҚ оқиғаларын мен АҚ оқыс оқиғаларын анықтау мақсатында оларды өңдеуді және талдауды;

АҚОМ объектілерінде анықталған АҚ оқиғаларын немесе АҚ оқыс оқиғаларын бастапқы талдауды;

АҚ оқыс оқиғалары туралы деректер тізбесін (бұдан әрі – Деректер тізбесі) ұсынумен АҚ оқиғасы немесе АҚ оқыс оқиғасы анықталған сәттен бастап 30 минут ішінде осы Қағидалардың 2-қосымшасына сәйкес АҚОМ объектісінің АҚ қамтамасыз етуге жауапты тұлғаларын хабардар етуді;

АҚОМ объектісінің меншік иесі мен иеленушісіне АҚ оқыс оқиғаларының таралуын тоқтата тұру бойынша бастапқы ұсыныстар беруді;

АҚ оқыс оқиғаларына ден қою шеңберінде қажет болған жағдайда, "МТҚ" АҚ қызметкерін АҚОМ ақпараттандыру объектілері орналасқан жерге бағыттауды (қажеттілікті ҚР ҰҚК немесе "МТҚ" АҚ дербес айқындайды);

АҚОМ объектісінің меншік иесі немесе иеленушісінің АҚ оқыс оқиғасын немесе уәкілетті тұлғаның себептер мен салдарларды жоймауы туралы АҚ оқыс оқиғасы анықталған сәттен бастап 75 сағат өткеннен кейін ҚР ҰҚК-ны хабардар етуді;

2) қорғауды қамтамасыз ету мониторингі шеңберінде:

АҚОМ бойынша жұмыстар жүргізу кестесіне сәйкес АҚОМ объектілерін, оның ішінде АҚОМ объектісі орналасқан локалды есептеуіш желімен түйіндесетін локалды есептеу желісін (бар болса) осалдықтардың бар-жоғы мәніне зерттеп-қарау (бұдан әрі – осалдықтарға зерттеп-қарау):

"енуге тестілеу" режимінде – жылына 8 рет (4 негізгі, 4 бақылау);

"жаңартуларды бақылау және конфигурацияларды талдау" режимінде – жылына 2 рет (негізгі, бақылау);

бастапқы кодты талдау – жылына 4 рет (2 негізгі, 2 бақылау);

"қолмен" енуге тестілеу – жылына 2 рет (негізгі, бақылау);

АҚОМ объектілерінің меншік иесі немесе иеленушісіне осалдықтарға зерттеп-қарау бойынша жұмыстар аяқталғаннан кейін 10 жұмыс күні ішінде АҚОМ объектілерін осалдықтарға зерттеп-қарау нәтижелерін және осалдықтарды жою бойынша ұсынымдар беруді;

осалдықтарға зерттеп-қарау шеңберінде анықталған АҚОМ объектілерінің осалдықтарын жою мәселелері бойынша АҚОМ объектілерінің меншік иесі немесе иеленушісіне консультация беруді;

3) қауіпсіз жұмыс істеуді қамтамасыз ету мониторингі шеңберінде:

АҚОМ объектісін АҚОМ бойынша жұмыс жүргізу кестесіне сәйкес, осы Қағидалардың 3-қосымшасында келтірген, ақпараттық қауіпсіздік жөніндегі

техникалық құжаттама (бұдан әрі – АҚ жөніндегі ТҚ) талаптарының орындалуын зерттеп-қарауды;

АҚОМ меншік иесі мен иеленушісіне АҚ жөніндегі ТҚ талаптарын орындауға АҚОМ объектісін зерттеп-қарау нәтижелерін және анықталған АҚ жөніндегі ТҚ бұзушылықтарын жою бойынша ұсынымдарды аталған зерттеп-қарау аяқталған күннен бастап 10 жұмыс күні ішінде ұсынуды жүзеге асырады.

11-тармақ мынадай редакцияда жазылсын:

11. АҚОМ объектісінің меншік иесі немесе иеленушісі "МТҚ" АҚ АҚОМ бойынша жұмыстар жүргізу үшін жағдайлар жасайды, оның ішінде:

АҚОМ объектілеріне, АҚОМ объектісі оқиғаларды тіркеу журналдарын жинаудың жүйесіне АҚОМ объектісінің меншік иесі немесе иеленушісі қызметкерлері немесе уәкілетті тұлғаның сүйемелдерімен "МТҚ" АҚ қызметкерлеріне физикалық қолжетімділік;

"МТҚ" АҚ қызметкерлері үшін АҚОМ объектісіне тәулік бойы желілік қолжетімділік болатындай тегін негізде екі жұмыс орны;

АҚОМ объектісі оқиғаларды тіркеу журналдарын жинаудың жүйесіне шектеусіз барлық операцияларды орындай алатындай "МТҚ" АҚ үшін желілік қолжетімділік;

АҚОМ объектісінің меншік иесі немесе иеленушісімен бекітілген, оның қолымен және мөрімен (бар болған жағдайда) расталған, ақпараттық қауіпсіздік жөніндегі техникалық құжаттамаға қолжетімділік.

12-тармақ мынадай редакцияда жазылсын:

12. "МТҚ" АҚ АҚ оқыс оқиғаларына ден қою мониторингін жүргізген кезде АҚОМ объектісінің меншік иесі немесе иеленушісі:

осы Қағидалардың 4-қосымшасында келтірілген ЭҮ АО оқиғаларын тіркеу журналдары жазбаларының үлгілері мен түрлеріне сәйкес, АҚОМ объектісінің оқиғаларын және оған қатысты ақпаратты қорғау құралдарын журналдануын ұйымдастырады;

АҚОМ объектісі жұмыс істейтін телекоммуникациялық желінің контурында оқиғаларды тіркеу журналдарын жинау жүйесін ұйымдастырады;

АҚОМ объектісінің оқиғаларын тіркеу журналдарын және оған жататын ақпаратты қорғау құралдарын, оқиғаларын тіркеу журналдарын жинау жүйесіне беруді ұйымдастырады;

АҚОМ объектісінің оқиғаларының журналдануына өзгерістер енгізу бойынша жоспарланған жұмыстар туралы өзгерістер енгізгенге дейін 5 жұмыс күн бұрын "МТҚ" АҚ-ны хабардар етеді. Хабарламаға өзгертілетін оқиғаларды тіркеу журналдарының үлгілері және олардың сипаттамасы қоса беріледі:

АҚҰҰО АҚ оқиғаларын басқару жүйесіне оқиғаларды тіркеу журналдарын жинаудың жүйесінен АҚОМ объектісінің оқиғаларды тіркеу журналын жіберу үшін "МТҚ" АҚ-мен келісілген жағдайларды қамтамасыз етеді;

АҚОМ объектісінде өзі анықтаған АҚ оқыс оқиға туралы анықталған сәттен бастап 15 минут ішінде "МТҚ" АҚ-ны хабардар етеді;

АҚ оқыс оқиғасы анықталған сәттен бастап 24 сағат ішінде Деректер тізбесін "МТҚ" АҚ-ға ұсынады.

13-тармақ мынадай редакцияда жазылсын:

13. "МТҚ" АҚ қорғауды қамтамасыз ету мониторингін жүргізу кезінде АҚҚМ объектілерінің меншік иесі немесе иеленушісі:

АҚОМ объектісінің осалдықтарын жою үшін қабылданған шаралар туралы ақпаратты осалдықтарды табуға зерттеп-қарау нәтижелерін алған күннен бастап жиырма күнтізбелік күн ішінде "МТҚ" АҚ-ға жолдайды;

АҚОМ объектісінің осалдығын өз бетінше анықтаған жағдайда, осы Қағидалардың 5-қосымшасына сәйкес нысан бойынша ЭҮ АО осалдығы туралы деректер тізбесін АҚОМ объектісінің осалдығы анықталған сәттен бастап 24 сағат ішінде "МТҚ" АҚ-ға-ға ұсынады;

АҚОМ объектілерінің осалдығын жоймаған кезде, осалдықты санаттардың бірін (өндірістік қажеттілік, нөлдік күннің осалдығы, жалған іске қосылу) бере алады және осы Қағиданың 6-қосымшасына сәйкес "МТҚ" АҚ-ға осалдықтарды жоймау себептерінің санаттарын және жоймау себептерінің негіздемесін ұсынады.";

14-тармақ мынадай редакцияда жазылсын:

14. АҚҰҮО қауіпсіз жұмыс істеуін қамтамасыз ету мониторингін жүргізу кезінде АҚОМ объектісінің меншік иесі немесе иеленушісі АҚ жөніндегі ТҚ талаптарының орындауға АҚОМ объектісін зерттеп-қарау нәтижелерін алған күннен бастап бір ай ішінде АҚ жөніндегі ТҚ талаптарының анықталған бұзушылықтары бойынша қабылданған шаралар туралы "МТҚ" АҚ-ға ақпарат ұсынады.

15-тармақ мынадай редакцияда жазылсын:

15. АҚОМ объектілер тізбесін қалыптастыру мақсатында, "МТҚ" АҚ АҚОМ объектілерінің меншік иелеріне немесе иеленушілеріне Мәліметтерді ұсыну туралы сұраныс жолдайды. АҚОМ объектісінің меншік иесі немесе иеленушісі "МТҚ" АҚ-дан сұраныс алған сәттен бастап 10 жұмыс күні ішінде Мәліметтерді электрондық формада "МТҚ" АҚ-ға ұсынады.

16-тармақ мынадай редакцияда жазылсын:

16. АҚОМ объектісінің АҚ қамтамасыз етуге жауапты тұлғасының байланыс деректері өзгерген жағдайда, АҚОМ меншік иесі немесе иеленушісі аталған өзгеріс сәтінен бастап 48 сағат ішінде "МТҚ" АҚ-ға өзекті байланыс деректерін жолдайды";

17-тармақ мынадай редакцияда жазылсын:

17. "МТҚ" АҚ тоқсан сайын ҚР ҰҚК-ға анықталған АҚ оқиғалары, АҚ оқыс оқиғалары, ЭҮ АО осалдықтары, ЭҮ АО өзгерістері және АҚ жөніндегі ТҚ

талаптарының анықталған бұзушылықтары бойынша жиынтық ақпарат, сондай-ақ АҚОМ меншік иелері мен иеленушілері қабылдаған шаралар туралы деректер жолдайды.

3-тараудың тақырыбы мынадай редакцияда жазылсын:

"3-тарау. Ақпараттық коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу тәртібі";

19-тармақ мынадай редакцияда жазылсын:

"19. АКИАМО ақпараттандыру АҚОМ-ны АКИАМО иесінің АҚ жөніндегі өз бөлімшесі немесе Қазақстан Республикасы Азаматтық кодексінің 683-бабына сәйкес үшінші тұлғалардан қызметтер сатып алу арқылы жүзеге асырылады.";

21-тармақ мынадай редакцияда жазылсын:

АКИАМО АҚ ҚМЖ АҚЖО техникалық құралдарына қосу АКИАМО меншік иесінің немесе иеленушісінің АҚ бойынша бөлімшесімен немесе Қазақстан Республикасының Азаматтық кодексінің 683-бабына сәйкес үшінші тұлғалардың қызметін сатып алу арқылы жүзеге асырылады.

24-тармақ мынадай редакцияда жазылсын:

24. АКИАМО-ның АҚ бөлімшесі АҚ-тың оқыс оқиғаларын өзі дербес анықтаған жағдайда АКИАМО АҚ бойынша жауапты "МТҚ" АҚ мен АҚЖО-ны АҚ оқыс оқиғасы анықталған сәттен бастап 24 сағат ішінде Деректер тізбесін жолдау арқылы хабардар етеді.

мынадай мазмұндағы 25-тармақпен толықтырылсын:

"Осы тарауда жазылған тәртіп пен талаптар ЭҮ АО-ға жатпайтын АКИАМО үшін белгіленген.".

3. "Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу қағидаларын бекіту туралы" Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 2019 жылғы 16 тамыздағы № 199/НҚ бұйрығына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 19286 болып тіркелген) мынадай өзгерістер енгізілсін:

кіріспе мынадай редакцияда жазылсын:

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

көрсетілген бұйрықпен бекітілген Мемлекеттік органдардың ақпараттандыру объектілерінің ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу қағидалары осы Тізбеге 2-қосымшаға сәйкес жаңа редакцияда жазылсын.

Өзгерістер мен толықтыру
енгізілетін кейбір
бұйрықтардың тізбесіне
1 қосымша
Электронды ақпараттық
ресурстардың
резервтік көшірмелерін

электрондық ақпараттық ресурстарды бірыңғай ұлттық резервтік сақтау платформасына беру қағидалары мен мерзімдеріне қосымша

Нысан

Электрондық ақпараттық ресурстардың техникалық сипаттамалары туралы мәліметтер

№	ЭАР толық атауы	Операциялық жүйе (нұсқа)	ДҚБЖ / БҚ / ҚБҚ (атауы / нұсқасы)	Деректер қорының өлшемі, Гб	Резервтіккөшірме (дамп) өлшемі, Гб	МҚ көлемінің жоспарлы жыл сайынғы ұлғаюы, Гб
---	-----------------	--------------------------	-----------------------------------	-----------------------------	------------------------------------	--

Кестенің жалғасы

Сервердің CPU саны	Сервердің CPU жүктемесі (%)	Сервердің ЖЖҚ көлемі, Гб	Резервтікөшірме құралдары	АКИАМО иесі	ЭАР класы	ЭАР жауапты тұлғасының тегі, аты, әкесінің аты/ телефоны
--------------------	-----------------------------	--------------------------	---------------------------	-------------	-----------	--

Қысқартуларды декодтау туралы ескертпе:
ДҚБЖ – мәліметтер қорын басқару жүйесі;
БҚ - бағдарламалық қамтылым;
ҚБҚ – қолданбалы бағдарламалық қамтылым;
CPU – компьютердің орталық процессоры;
Гб - гигабайт;
ДҚ – деректер қоры;
ЖЖҚ – жедел жады құрылғысы;
ЭАР – электрондық ақпараттық ресурс

Өзгерістер мен толықтыру енгізілетін кейбір бұйрықтардың тізбесіне 2-қосымша

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

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 – АҚҰҰО) 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, Қазақстан 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 өндеуді жүзеге асырады.

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

ҰАҚҮО 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 ҰАҚҮО оқиғаларын тіркеу журналдарын жинау жүйесін ұйымдастыруды;

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

ҰАҚҮО АҚ оқиғаларын басқару жүйесіне АҚОМ және АҚ объектілерінің оқиғаларын тіркеу журналдарын беруді ұйымдастыруды және АҚ оқиғалары мен АҚ оқыс оқиғаларын анықтау мақсатында оларды өндеуді 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 қалыптастыру 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 инфрақұрылымына 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 бойынша 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

					Жұмыс станциясын		
--	--	--	--	--	---------------------	--	--

№	Мемлекеттік органның атауы	Құрылымдық бөлімше (департамент)	Физикалық орналасуы (этаж, кабинет)	Пайдаланушының/ жауапты тұлғаның ТАӘ	ың / 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							

© 2012. Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» ШЖҚ РМК