"Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларын бекіту туралы

Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 7 маусымда № 17019 болып тіркелді.

"Ақпараттандыру туралы" Қазақстан Республикасы Заңының 7-1-бабының 7) 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 "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидалары бекітілсін.

2. "Электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін , қорғалуын және қауіпсіз жұмыс істеуін қамтамасыз етудің мониторингін жүргізу қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушысының 2016 жылғы 26 қаңтардағы № 66 бұйрығының (Қазақстан Республикасының нормативтік құқықтық актілерін мемлекеттік тіркеу тізілімінде № 13178 болып тіркелген, "Әділет" Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық құқықтық жүйесінде 2016 жылғы 10 наурызда жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелген күнінен бастап күнтізбелік он күн ішінде оның көшірмелерін баспа және электрондық түрде қазақ және орыс тілдерінде Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу және ресми жариялау үшін " Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

3) осы бұйрық мемлекеттік тіркелгеннен кейін күнтізбелік он күн ішінде оның көшірмелерін мерзімді баспа басылымдарында ресми жариялауға жіберуді;

4) осы бұйрық ресми жариялағаннан кейін оны Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің интернет-ресурсында орналастыруды;

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

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

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

Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрі *Б. Атамқұлов*

"КЕЛІСІЛГЕН"
Қазақстан Республикасы
Ұлттық қауіпсіздік
комитетінің төрағасы
_____ К. Мәсімов
2018 жылғы 21 мамыр

Қазақстан Республикасы
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2018 жылғы "28" наурыздағы
№ 52/НҚ бұйрығымен
бекітілген

"Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидалары

Ескерту. Қағида жаңа редакцияда – ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 13.08.2019 № 195/НҚ (20.09.2019 бастап қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы қағидалар

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.

Ескерту. 1-тармақ 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.

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) осалдық – пайдаланылуы ақпараттандыру объектісі тұтастығының және (немесе) құпиялылығының және (немесе) қолжетімділігінің бұзылуына алып келуі мүмкін ақпараттандыру объектісінің кемшілігі;

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, көшірмесін 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 (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;

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.

Ескерту. 2-тармақ 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); өзгеріс енгізілді - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрықтарымен.

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

АҚ оқыс оқиғаларына ден қою мониторингі;

қорғауды қамтамасыз ету мониторингі;

қауіпсіз жұмыс істеуін қамтамасыз ету мониторингі.

Ескерту. 3-тармаққа өзгеріс енгізілді - 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.

4. АҚҚМ объектілеріне:

мемлекеттік құпияларды құрайтын мәліметтерді қамтитын электрондық ақпараттық ресурстардан;

мемлекеттік құпияларға жататын, орындалуы қорғалған ақпараттық жүйелерден;

Қазақстан Республикасы Ұлттық Банкінің ЭҮ АО-мен интеграцияланбайтын ақпараттандыру объектілерінен басқа өнеркәсіптік пайдалануға енгізілген, оның ішінде АКИАМО-ға жатқызылған ЭҮ АО жатады.

Ескерту. 4-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

5. АҚҚМ мынадай нұсқалардың бірі бойынша жүргізіледі:

1) бір жұмыс түрі бойынша;

2) бірнеше жұмыс түрлері бойынша;

3) жұмыс түрлерінің толық құрамында.

Ескерту. 5-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

Ескерту. 6-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

2-тарау. "Электрондық үкімет" ақпараттандыру объектілерінің ақпараттық қауіпсіздікті қамтамасыз ету мониторингін жүргізу тәртібі

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:

1) бағдарламалық және техникалық құралдар тізбесі;

2) телекоммуникация желілерінің сызбалары;

3) бастапқы кодтардың және/немесе бағдарламалық құралдар файлдарының бақылау жиынтықтары;

4) деректер базасының құрылымы қоса қолданылады.

Ескерту. 7-тармаққа өзгеріс енгізілді - 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.

8. АҚҚМ объектісінің меншік иесі немесе иеленушісі АҚҚМ объектісінің өнеркәсіптік пайдалануға енгізілгені немесе пайдалану тоқтатылғаны туралы өнеркәсіптік пайдалануға енгізілген немесе пайдалану тоқтатылған күннен бастап 10 жұмыс күні ішінде ресми хатпен "МТҚ" АҚ-ны хабардар етеді және осы Қағидаларға 1 -қосымшаға сәйкес нысан бойынша ЭҮ АО туралы мәліметтерді қағаз және электронды түрде жолдайды (бұдан әрі – Мәліметтер).

Ескерту. 8-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

Ескерту. 9-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

10. "МТҚ" АҚ АҚҚМ жүргізу кезінде келесілерді жүзеге асырады:

1) АҚ оқыс оқиғаларына ден қою мониторингі шеңберінде:

АҚҰҰО-ның АҚ оқиғаларын басқару жүйесіне жіберілуі қажет оқиғаларды тіркеу журналдарының тізбесін анықтау үшін АҚҚМ объектісін талдау;

АҚ оқиғаларын басқару жүйесінің агенттерін АҚҚМ объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне және, қажет болған жағдайда, АҚҚМ объектісінің меншік иесі немесе иеленушісінің өзге ақпараттық-коммуникациялық инфрақұрылым объектілеріне орнату;

АҚҰҰО-ның АҚ оқиғаларын басқару жүйесіне АҚҚМ объектісінің және оған жататын ақпаратты қорғау құралдарының оқиғаларды тіркеу журналдарын жинау, оларды АҚ оқиғалары мен АҚ оқыс оқиғаларын анықтау мақсатында өңдеу және талдау;

АҚҚМ объектілерінде анықталған АҚ оқиғалары немесе АҚ оқыс оқиғаларын бастапқы талдау;

АҚҚМ объектісінің АҚ қамтамасыз етуге жауапты тұлғаларын АҚ оқиғасы немесе АҚ оқыс оқиғасы анықталған сәттен бастап 30 минут ішінде анықталған АҚ оқиғасы немесе АҚ оқыс оқиғасы туралы деректер тізбесін осы Қағидаларға 7-қосымшаға сәйкес ұсына отырып хабардар ету;

АҚҚМ объектісінің меншік иесі мен иеленушісіне АҚ оқыс оқиғасының таралуын тоқтата тұру бойынша бастапқы ұсыныстар беру;

АҚ оқыс оқиғаларына ден қою шеңберінде қажет болған жағдайда, "МТҚ" АҚ қызметкерін АҚҚМ объектісі орналасқан жерге бағыттау (қажеттілікті ҚР ҰҚК немесе "МТҚ" АҚ дербес айқындайды);

АҚҚМ объектісінің меншік иесі немесе иеленушісі немесе оның уәкілетті тұлғасы АҚ оқыс оқиғасының себептері мен салдарын АҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде жоймаған жағдайда ҚР ҰҚК-ні хабардар ету;

2) қорғауды қамтамасыз ету мониторингі шеңберінде:

АҚҚМ бойынша жұмыстарды жүргізу кестесіне сәйкес АҚҚМ объектілерін 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);

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

енуге қолмен тестілеу кезінде АҚҚМ объектісі орналасқан жергілікті есептеу желісімен түйісетін жергілікті есептеу желісін (бар болған жағдайда) зерттеп-қарау;

АҚҚМ объектілерінің меншік иелері немесе иеленушілеріне осалдықтарға зерттеп-қарау бойынша жұмыстар аяқталғаннан кейін 10 жұмыс күні ішінде АҚҚМ объектілерін осалдықтарға зерттеп-қарау нәтижелерін және осалдықтарды жою бойынша ұсынымдар беру;

АҚҚМ объектілерінің меншік иесінің немесе иеленушісінің сұрау салуы бойынша осалдықтарға зерттеп-қарау шеңберінде анықталған АҚҚМ объектілерінің осалдықтарын жою мәселелері бойынша консультация беру;

3) қауіпсіз жұмыс істеуді қамтамасыз ету мониторингі шеңберінде:

АҚҚМ объектісін осы Қағидаларға 3-қосымшада келтірілген ақпараттық қауіпсіздік жөніндегі техникалық құжаттама (бұдан әрі – АҚ жөніндегі ТҚ) талаптарының орындалуына АҚҚМ бойынша жұмыс жүргізу кестесіне сәйкес зерттеп-қарау;

АҚҚМ объектілерінің меншік иелеріне немесе иеленушілеріне АҚҚМ объектісін АҚ жөніндегі ТҚ талаптарының орындалуына зерттеп-қарау нәтижелерін және анықталған бұзушылықтарды жою бойынша ұсынымдарды зерттеп-қарау аяқталған күннен бастап 10 жұмыс күні ішінде ұсыну.

Ескерту. 10-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

"МТҚ" АҚ қызметкерлеріне АҚҚМ объектісіне, АҚҚМ объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне АҚҚМ объектісінің меншік иесі немесе иеленушісі қызметкерлері немесе уәкілетті тұлғаның сүйемелдеуімен физикалық қолжетімділік:

"МТҚ" АҚ қызметкерлері үшін АҚҚМ объектісіне тәулік бойы желілік қолжетімділікті қамтамасыз ете отырып тегін негізде екі жұмыс орны;

АҚҚМ объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне шектеусіз барлық операцияларды орындай алатындай "МТҚ" АҚ үшін желілік қолжетімділік;

АҚҚМ объектісінің меншік иесі немесе иеленушісі бекіткен, оның қолымен және мөрімен (бар болған жағдайда) расталған АҚ жөніндегі ТҚ-ға қолжетімділік;

фото және бейнетіркеу жүргізе отырып, АҚҚМ объектісінің серверлік және желілік жабдығына, телекоммуникация желісіне және АҚҚМ объектісіне арналған құжаттама мен ілеспе құжаттамаға, оның ішінде АҚҚМ объектісін сүйемелдеу және техникалық қолдау шарттарына физикалық қолжетімділік.

Ескерту. 11-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

12. "МТҚ" АҚ АҚ оқыс оқиғаларына ден қою мониторингін жүргізген кезде АҚҚМ объектінің меншік иесі немесе иеленушісі немесе оған АҚЖО қызметтерін көрсететін тұлға:

АҚҚМ объектісі оқиғаларының және оған қатысты ақпаратты қорғау құралдарының журналдануын осы Қағидаларға 4-қосымшада келтірілген ЭҮ АО оқиғаларын тіркеу журналдары жазбаларының үлгілері мен түрлеріне сәйкес ұйымдастырады;

АҚҚМ объектісі жұмыс істейтін телекоммуникация желісінің шеңберінде оқиғаларды тіркеу журналдарын жинау жүйесін ұйымдастырады;

АҚҚМ объектісінің және оған қатысты ақпаратты қорғау құралдарының оқиғаларды тіркеу журналдарын АҚҚМ объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне беруді ұйымдастырады;

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

оқиғаларды тіркеу журналдарын АҚҚМ объектісінің оқиғаларды тіркеу журналдарын жинау жүйесінен АҚҰҮО АҚ оқиғаларын басқару жүйесіне жіберу үшін, "МТҚ" АҚ-мен келісілген жағдайларды қамтамасыз етеді;

АҚҚМ объектісінде АҚ оқыс оқиғасы өз бетінше анықталған кезде, АҚ оқыс оқиғасы расталған сәттен бастап 15 минут ішінде "МТҚ" АҚ-ны хабардар етеді және АҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде "МТҚ" АҚ-ға АҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы ақпаратты осы Қағидаларға 2-қосымшаға сәйкес жібереді;

"МТҚ" АҚ АҚ оқиғасы немесе АҚ оқыс оқиғасы туралы хабардар еткен кезде, "МТҚ" АҚ-ға хабарлама сәтітен бастап 72 сағат ішінде:

АҚ оқиғасы расталған кезде - АҚ оқиғасын талдау нәтижелері туралы ақпаратты;

АҚ оқыс оқиғасы расталған кезде - АҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы ақпаратты осы Қағидаларға 2-қосымшаға сәйкес жолдайды.

Ескерту. 12-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

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

АҚҚМ объектісінде осалдықды өз бетінше анықтаған жағдайда, осалдық анықталған сәттен бастап 24 сағат ішінде ЭҮ АО осалдығы туралы деректер тізбесін осы Қағидаларға 5-қосымша нысаны бойынша "МТҚ" АҚ-ға жолдайды;

АҚҚМ объектісінің осалдығын жоймаған кезде осалдыққа санаттардың бірін (өндірістік қажеттілік, нөлдік күннің осалдығы, жалған іске қосу) бере алады және осы Қағидаларға 6-қосымшаға сәйкес осалдықты жоймау себептерінің санаттарын және жоймау себебінің негіздемесін "МТҚ" АҚ-ға ұсынады.

Ескерту. 13-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

14. АҚҚМ объектісінің меншік иесі немесе иеленушісі "МТҚ" АҚ қауіпсіз жұмыс істеуді қамтамасыз ету мониторингін жүргізген кезде:

АҚҚМ объектісін АҚ жөніндегі ТҚ талаптарының орындалуына зерттеп-қарау бойынша жұмыстарды жүргізу туралы хабарламаны алған күннен бастап 10 жұмыс күні ішінде "МТҚ" АҚ-ға АҚҚМ объектісінің меншік иесі немесе иеленушісі бекіткен, оның қолымен және мөрімен (бар болған жағдайда) куәландырылған осы Қағидаларға 3 -қосымшада келтірілген АҚ жөніндегі ТҚ көшірмелерін ұсынады;

АҚҚМ объектісін АҚ жөніндегі ТҚ талаптарының орындалуына зерттеп-қарау нәтижелерін алған күннен бастап бір ай ішінде "МТҚ" АҚ-ға АҚ жөніндегі ТҚ талаптарының анықталған бұзушылықтары бойынша қабылданған шаралар туралы ақпаратты ұсынады.

Ескерту. 14-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

Ескерту. 15-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

Ескерту. 16-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

17. "МТҚ" АҚ тоқсан сайын ҚР ҰҚК-ға анықталған АҚ оқиғалары, АҚ оқыс оқиғалары, ЭҮ АО-ның осалдықтары, ЭҮ АО өзгерістері және АҚ жөніндегі ТҚ талаптарының анықталған бұзушылықтары бойынша жиынтық ақпаратты, сондай-ақ АҚҚМ меншік иелері мен иеленушілері қабылдаған шаралар туралы деректерді жолдайды.

Ескерту. 17-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

18. ҚР ҰҚК тоқсан сайын уәкілетті органға анықталған АҚ оқыс оқиғалары, ЭҮ АО осалдықтары, ЭҮ АО өзгерістері және АҚ жөніндегі ТҚ талаптарының анықталған бұзушылықтары бойынша жиынтық ақпарат, сондай-ақ АҚҚМ меншік иелері мен иеленушілері қабылдаған шаралар туралы деректер жолдайды.

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

Ескерту. 3-тараудың тақырыбы 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.

19. ЭҮ АО-ға жатпайтын АКИАМО-ның ақпараттық қауіпсіздігін қамтамасыз ету мониторингі АКИАМО иесінің АҚ бойынша өз бөлімшесімен немесе Қазақстан Республикасы Азаматтық кодексінің 683-бабына сәйкес үшінші тұлғалардың қызметтерін сатып алу жолымен жүзеге асырылады.

Ескерту. 19-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

20. АКИАМО меншік иесі немесе иеленушісі Заңның 7-1-бабы 3) тармақшасына сәйкес ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органмен бекітілетін АКИАМО тізбесіне енгізілу күнінен бастап тоқсан күнтізбелік күн ішінде АКИАМО-ның АҚ-ны қамтамасыз ету мониторингі жүйесін (бұдан әрі – АҚ ҚМЖ)

АҚЖО-ның техникалық құралдарына қосуды қамтамасыз етеді, сондай-ақ АКИАМО-ның АҚ бойынша жауапты тұлғасын анықтайды.

Ескерту. 20-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

21. Алып тасталды - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 31.03.2023 № 128/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

22. АКИАМО АҚ ҚМЖ-сы АҚЖО-ның техникалық құралдарына қосылғаннан кейін, АҚЖО-ның АҚ ҚМЖ-сы АҚ оқыс оқиғасын анықтаған жағдайда, АҚЖО АҚ оқыс оқиғасы расталған сәттен бастап 15 минут ішінде, "МТҚ" АҚ-ны және АКИАМО-ның АҚ бойынша жауапты тұлғасына хабарлау арқылы АКИАМО меншік иесін немесе иеленушісін хабардар етеді. АҚЖО "МТҚ" АҚ-ға АҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде АҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы ақпаратты осы Қағидаларға 2-қосымшаға сәйкес жолдайды.

Ескерту. 22-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

23. АКИАМО меншік иесі немесе иеленушісі хабарландыру алғаннан кейін отыз күнтізбелік күн ішінде анықталған осалдықтарды түзетеді.

24. АКИАМО-ның АҚ бөлімшесі АҚ оқыс оқиғасын өзі дербес анықтаған жағдайда, АКИАМО-ның АҚ бойынша жауапты тұлғасы АҚ оқыс оқиғасы расталған сәттен бастап 15 минут ішінде "МТҚ" АҚ мен АҚЖО-ны хабардар етеді. АҚЖО "МТҚ" АҚ-ға АҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде АҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы ақпаратты осы Қағидаларға 2-қосымшаға сәйкес жолдайды.

АҚЖО қызметтерін көрсететін тұлға болмаған жағдайда, "МТҚ" АҚ-ға АҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы ақпаратты АКИАМО-ның АҚ бойынша бөлімшесі жолдайды.

Ескерту. 24-тармақ жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

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

Ескерту. Қағида 25-тармақпен толықтырылды - 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.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз
етуге мониторинг
жүргізу қағидаларына
1-қосымша
Нысан

"Электрондық үкіметтің" ақпараттандыру объектісі туралы мәліметтер

Ескерту. 1-қосымша жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1. "Электрондық үкіметтің" ақпараттандыру объектісінің (бұдан әрі - ЭҮ АО) ресми атауы.

2. ЭҮ АО меншік иесі.

3. ЭҮ АО иеленушісі (бар болған жағдайда).

4. ЭҮ АО нақты орналасқан жері (көше, қала, облыс).

5. ЭҮ АО-ны қолдап отыруды және (немесе) жүйелік-техникалық қызмет көрсетуді жүзеге асыратын ұйым (толық байланыс деректерін көрсете отырып).

6. Ақпараттандыру объектілерінің сыныптауышына сәйкес маңыздылық деңгей: жоғары, орташа, төмен.

7. ЭҮ АО-ның мемлекеттік органдардың бірыңғай көліктік ортасына қосылуының болуы және байланыс арнасының өткізу қабілеті туралы ақпарат.

8. ЭҮ АО-ның Интернетке қосылуының болуы және байланыс арнасының өткізу қабілеті туралы ақпарат.

9. ЭҮ АО меншік иесі немесе иеленушісі бекіткен және оның қолымен және мөрімен (бар болған жағдайда) куәландырылған ЭҮ АО-ның логикалық және физикалық архитектуралық схемалары.

10. Жүйенің атауын және жүйе жұмыс істейтін жергілікті желінің шеңберін көрсете отырып, оқиғаларды тіркеу журналдарын жинау жүйесінің болуы туралы ақпарат.

11. АҚЖО немесе ЭҮ АО-ның ақпараттық қауіпсіздігін қамтамасыз етуге жауапты тұлғаның байланыс деректері.

12. ЭҮ АО техникалық және бағдарламалық құралдары, оның ішінде IP-мекенжайларын, домендік аттарды (бар болған жағдайда), техникалық және

бағдарламалық құралдың мақсатын және IP-мекенжай жататын нұсқасын (бар болған жағдайда) көрсете отырып, ЭҮ АО-ға жататын резервтік техникалық және бағдарламалық құралдар мен ақпаратты қорғау құралдары туралы мәліметтер.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз
етуге мониторинг
жүргізу қағидаларына
2-қосымша
нысан

Ақпараттық қауіпсіздіктің оқыс оқиғасы туралы деректер тізбесі

Ескерту. 2-қосымша жаңа редакцияда - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

АҚ оқыс оқиғасы тіркелген күні	
АҚ оқыс оқиғасының маңыздылық деңгейі*	Жоғары (4); Орташа (3); Төмен (2); Анықталмаған (1).
АҚ оқыс оқиғасының түрі	Қызмет көрсетуден бас тарту (DoS, DDoS); Рұқсатсыз қол жеткізу және қамтылымды түрлендіру; Ботнет; Вирустық шабуыл; Шифрлаушы; Осалдықты пайдалану; Аутентификация/авторизация құралдарының жария етілуі; Фишинг; Спам; Басқа.
Ауқымы	Жеке; Жаппай.
Егжей-тегжейліліктер	Туындау күні мен уақыты; Растау күні мен уақыты; Қайта / жаңа; Жария ету индикаторы (IOC).
Белгісі	Жарамды; Әрекет; Күдік;

Шеңбер	Ішкі шеңбердің жергілікті желісі; Сыртқы шеңбердің жергілікті желісі.
АҚ оқыс оқиғасының сипаты	
Салдары	Салдары жоқ; Жұмысқа қабілеттілігінің бұзылуы; Тұтастығының бұзылуы; Ақпараттың құпиялылық режимінің бұзылуы
Зиян келтірілген объект	
АҚ оқыс оқиғасын жою үшін қолданылған әрекеттер	
Ескертпе	

Ақпараттық қауіпсіздіктің оқыс оқиғасының маңыздылық деңгейлері

Маңыздылық деңгей	Белгілері	АҚ оқыс оқиғаларының үлгілері
Жоғары (4)	Қызметтерді ұсыну/жұмыстарды орындау мүмкіндігіне және (немесе) маңызды* деректердің жоғалуына/түрлендіруге және (немесе) маңызды* деректерді өңдейтін ақпараттандыру объектісінің құпиялылығының бұзылуына әкеп соғатын АҚ оқыс оқиғалары.	- Рұқсатсыз қол жеткізу - Осалдықты пайдалану - Шифрлаушы - Зиянды БҚ - Қызмет көрсетуден бас тарту (DoS/ DDoS шабуылы) Және т. б.
Орташа (3)	Қызметтер көрсетуді/жұмыстарды орындауды елеулі шектеуге және (немесе) маңызды болып табылмайтын деректерді жоғалтуға/түрлендіруге және (немесе) маңызды болып табылмайтын деректерді өңдейтін ақпараттандыру объектісінің құпиялылығын бұзуға әкелетін АҚ оқыс оқиғалары*.	- Рұқсатсыз қол жеткізу - Шифрлаушы - Зиянды БҚ - Қызмет көрсетуден бас тарту (DoS/DDoS шабуылы) - Осалдықты пайдалану - Және т. б.
Төмен (2)	Қызмет көрсетуге/жұмыстарды орындауға әсер етпейтін АҚ оқыс оқиғалары.	- Зиянды БҚ - Қызмет көрсетуден бас тарту (DoS /DdoS шабуылы) - Осалдықты пайдалану - Спам - Фишингтік шабуыл - Және т. б.
Анықталмаған (1)**	АҚ оқыс оқиғасының қызмет көрсетуге әсері анықталмаған	Сипатқа ие емес / күдікті белсенділік

Ескертпе:

* Маңызды деректерге Қазақстан Республикасының заңнамасымен қорғалатын және/немесе ақпараттандыру объектісінің меншік иесі/иеленушісі маңыздыларға жатқызған деректер жатады.

** АҚ оқыс оқиғасы расталған сәттен бастап 48 сағат ішінде деңгейді қайта қарау қажет.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз етуге
мониторинг жүргізу
қағидаларына
3-қосымша
Нысан

Ақпараттық қауіпсіздік жөніндегі техникалық құжаттама

1. Бірінші деңгейлі құжаттар:

1) ақпараттық қауіпсіздік саясаты.

2. Екінші деңгейлі құжаттар:

1) ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;

2) ақпаратты өңдеу құралдарымен байланысты активтерді сыныптау және маркалау, сәйкестендіру қағидалары;

3) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз қамтамасыз ету бойынша қағидалар;

4) есептеу техникасы құралдарын, телекоммуникациялық жабдықты және бағдарламалық қамтылымды түгендеу және паспорттандыру қағидалары;

5) ішкі АҚ аудитін жүргізу қағидалары;

6) ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;

7) электрондық ақпараттық ресурстарға қол жеткізу құқықтарын бөлу қағидалары;

8) Интернетті және электронды поштаны пайдалану қағидалары;

9) аутентификация рәсімін ұйымдастыру қағидалары;

10) вирусқа қарсы бақылауды ұйымдастыру қағидалары;

11) мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану қағидалары;

12) ақпаратты өңдеу құралдарын физикалық қорғауды және ақпараттық ресурстардың қауіпсіз жұмыс істеу ортасын ұйымдастыру қағидалары.

3. Үшінші деңгейлі құжаттар:

1) АҚ қауіптерінің (тәуекелдерінің) каталогы;

2) АҚ қауіптерінің (тәуекелдерінің) өңдеу жоспары;

3) ақпараттық резервті көшіру және қалпына келтіру регламенті;

4) ақпаратты өңдеу құралдарымен байланысты активтер жұмысының үздіксіздігін қамтамасыз етуі және жұмысқа жарамдылығын қалпына келтіру бойынша іс-шаралар жоспары;

5) әкімшінің ақпараттандыру объектісін сүйемелдеу жөніндегі басшылығы;

6) пайдаланушылардың АҚ оқыс оқиғаларына және штаттан тыс (дағдарысты) жағдайларда әрекет етуі бойынша іс-қимыл тәртібі туралы нұсқаулық.

4. Төртінші деңгейлі құжаттар:

1) АҚ оқыс оқиғаларын тіркеу және штаттан тыс жағдайларды есеп журналы;

2) серверлік үй-жайларға бару журналы;

3) желілік ресурстар осалдығын бағалауды жүргізу туралы есеп;

4) кабельді қосылысты есептеу журналы;

5) резервті көшірудің (резервті көшірудің, қалпына келтірудің), резервті көшіруді тестілеудің есепке алу журналы;

6) жабдық конфигурациясының өзгеруін есепке алу, ақпараттық жүйенің еркін бағдарламалық қамтылымды және қолданбалы бағдарламалық қамтылымды тестілеу және өзгерістерді есепке алу, бағдарламалық қамтылым осалдықтарын тіркеу және жою журналы;

7) серверлік үй-жайларға арналған дизель-генераторлық қондырғыларды және үздіксіз қуат беру көздерін тестілеу журналы;

8) серверлік үй-жайлардың микроклиматын, бейнебақылауды, өрт сөндіруді қамтамасыз ету жүйелерін тестілеу журналы.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз етуге
мониторинг жүргізу
қағидаларына
4-қосымша
Нысан

"Электрондық үкімет" ақпараттандыру объектілерінің оқиғаларын тіркеу журналдары жазбаларының үлгілері мен түрлері

1-тарау. Операциялық жүйенің оқиғаларын тіркеу журналдары жазбаларының үлгілері мен түрлері

1. Журналдауға жататын операциялық жүйенің (бұдан әрі – ОЖ) оқиғаларының түрлері:

1) жүйені іске қосу/тоқтату;

2) ОЖ объектілерімен жұмыс (ашу, сақтау, атын өзгерту, жою, құру, көшіру);

3) бағдарламалық қамтылымды (бұдан әрі – БҚ) орнату және жою;

4) ОЖ-де қолданушылардың авторландыру (енгізу және шығару), сәтті және сәтсіз авторландыру әрекеттері;

5) жүйелік конфигурациясының өзгеруі;

6) есептік жазбаларды құру, жою және түрлендіру;

7) антивирустық жүйелер және басып кіруді табу жүйелері және оқиғаларды тіркеу журналын жүргізу құралы секілді қорғау жүйелерін активициялау/дезактивациялау;

8) баптау және жүйені қорғауды басқару құралдарын өзгерту әрекеті және өзгерту;

9) артықшылықты есептік жазбаларды пайдалану;

10) кіріс/шығыс құрылғысын қосу/ажырату;

11) қолданушының сәтсіз немесе қабылданбаған әрекеттері;

12) деректерді және басқа ресурстарды қозғайтын сәтсіз немесе қабылданбаған әрекеттер;

13) ОЖ-да процестерді іске қосу, тоқтату.

2. ОЖ оқиғаларын тіркеу журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) хост атауы;

3) оқиғаның сипаттамасы.

3. Unix-ұқсас жүйелердің серверлік ОЖ үшін (Unix, Linux, AIX, HPUX және т.б.) 1-тармақтағы оқиғаларға қосымша мынадай оқиғаларды тіркеу қажет:

1) әртүрлі IP-мекенжайлардан бірдей есептік жазбаны бір серверге қосу;

2) жүйеде жаңа порттар ашу;

3) негізгі логтардағы барлық оқиғаларды тіркеу: /var/log/secure, /var/log/messages, /var/log/audit.

4. Windows тобындағы серверлік ОЖ үшін, 1-тармақтағы оқиғаларға қосымша мынадай оқиғаларды тіркеу қажет:

1) жаңа сессияға (logon) арнайы артықшылықтар беру – Windows EID 4672;

2) желілік кіру (Network logon) – Windows EID 4624;

3) әкімшінің желілік папкасына қол жеткізу (administrative share access) және SMB арналарға қол жеткізу (pipes) – Windows EID 5140/5145;

4) "Деректер жазу" немесе "Файл қосу" құқықтармен "Файл" объектісіне қол жеткізу – Windows EID 4663;

5) ықтимал қауіпті процестерді іске қосу (WmiPrvSE.exe, WinrsHost.exe, wsmprovhost.exe, mmc.exe, psexe * .exe, paexe * .exe) – Sysmon EID 1;

6) қызметті (сервисті) орнату және іске қосу – Windows EID 7045/7036/4697;

7) міндеттер жоспарлағышындағы (scheduled tasks) тапсырмалардың параметрлерін жасау немесе өзгерту – Windows EID 4698/4702;

8) қызмет таймаутына қол жеткізілді – Windows EID 7009;

9) қызметті іске асыру кезіндегі қате – Windows EID 7000;

10) тізілімнің мәні өзгерген – Windows EID 4657;

11) WMI аттар кеңістігіндегі жазба – Windows EID 4662.

5. Оқиғаларды тіркеу журналындағы жазбалар мәтіндік үлгіде сақталады.

6. Оқиғаларды тіркеу журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

7. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылады.

8. Оқиғаларды тіркеу журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

2-тарау. Деректер базасын басқару жүйесіндегі оқиғаларды тіркеу журналдары жазбаларының үлгілері мен түрлері

9. Журналдауға жататын деректер базасын басқару жүйесінің оқиғаларының түрлері:

1) сессияларды бақылау (сәтті/сәтсіз авторландыру, тіркелмеген есептік жазбалардың пайдаланылуын тіркеу);

2) әкімшілік артықшылықтар бар деректер базасын (бұдан әрі – ДБ) қолданушылардың барлық іс-қимылдары (оның ішінде: select, create, alter, drop, truncate , rename, insert, update, delete, call (execute), lock);

3) басқа ДБ қолданушыларға жеңілдіктер тағайындау құқығы бар қолданушылардың барлық іс-қимылдары (grant, revoke, deny).

10. ДБ оқиғаларын тіркеу журналы мынадай өрістер болады:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) есептік жазбаның/қолданушының ID атауы;

3) хосттың IP-мекенжай немесе хост атауы;

4) оқиғаның сипаттамасы;

5) объектінің атауы (іске асыру мүмкіндігі болған жағдайда кестелер, рәсімдер, функциялар).

11. Оқиғаларды тіркеу журналындағы жазбалар мәтіндік үлгіде сақталады.

12. Оқиғаларды тіркеу журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

13. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылады.

14. Оқиғаларды тіркеу журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

3-тарау. Телекоммуникациялық жабдық оқиғаларын тіркеу журналдары жазбаларының үлгілері мен түрлері

15. Журналдауға жататын телекоммуникациялық жабдық оқиғалары:

1) жүйені іске қосу/тоқтату;

2) жүйенің конфигурациясын өзгерту;

3) локалдық есептік жазбалардың құру, жою, түрлендіру;

4) артықшылықты есептік жазбалардың пайдалану;

5) кіріс/шығыс құрылғысын қосу/ажырату;

6) қолданушының сәтсіз немесе қабылданбаған іс-қимылдары.

7) желілік линктердің (қосылыстар) іске қосылуы, төмендеуі, тоқтауы.

16. Техникалық мүмкіндік болса желіаралық экрандардан барлық трафиктің (кіріс және шығыс) логтарын жазу, сондай-ақ құрылғыдағы барлық оқиғаларды жазып алу талап етіледі.

17. Телекоммуникациялық жабдық оқиғаларын тіркеу журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) құрылғының атауы;

3) есептік жазбаның/қолданушының ID;

4) хосттың IP-мекенжайы;

5) бастапқы IP-мекенжайы;

6) тағайындалған IP-мекенжайы;

7) оқиғаның сипаттамасы.

18. Оқиғаларды тіркеу журналындағы жазбалар мәтіндік үлгіде сақталады.

19. Оқиғаларды тіркеу журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

20. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылады.

21. Оқиғаларды тіркеу журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

4-тарау. Қолданбалы бағдарламалық қамтылым оқиғаларын тіркеу журналдары жазбаларының үлгілері мен түрлері

22. Журналдауға жататын БҚ оқиғаларының түрлері:

1) қолданушыларды авторландыру (енгізу және шығару), сәтті және сәтсіз авторландыру іс-қимылдары;

2) локалдық есептік жазбалардың және конфигурациялық файлдарды құру, көшіру, ауыстыру, жою, түрлендіру;

3) қолданушының сәтсіз немесе қабылданбаған әрекеттері;

4) қолданушының қол жеткізу объектілеріне қолжетімділік алуы;

5) қолданбалы БҚ қолданушысының іс-қимылдары (объектіге (деректерге) қолжетімділік, объектінің (деректердің) өзгерістері, объектіні (деректерді) жою).

23. БҚ оқиғаларын тіркеу журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) оқиға (сервис/қызмет) көзінің атауы;

3) есептік жазбаның атауы/қолданушының ID;

4) қолданушының IP-мекенжайы;

5) операцияның басталу уақыты;

6) операцияның аяқталу уақыты;

7) оқиғаның сипаттамасы.

24. Оқиғаларды тіркеу журналындағы жазбалар мәтіндік үлгіде сақталады.

25. Оқиғаларды тіркеу журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

26. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылады.

27. Оқиғаларды тіркеу журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

5-тарау. Ақпаратты қорғау құралдарымен анықталатын оқиғаларды тіркеу журналдары жазбаларының үлгілері мен түрлері

28. Журналдауға жататын ақпаратты қорғау құралдарымен анықталатын оқиғаларының түрлері:

1) локалдық есептік жазбалар және конфигурациялық файлдар құру, көшіру, ауыстыру, жою, өзгерту;

2) қызметтің іске қосылуы/тоқтауы;

3) жүйе конфигурациясын өзгерту;

4) локалдық есептік жазбалар құру, жою, түрлендіру.

29. Ақпаратты қорғау құралдары оқиғаларын тіркеу журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) оқиға (сервис/қызмет) көзінің атауы;

3) есептік жазбаның атауы/қолданушының ID;

4) клиенттің IP-мекенжайы;

5) операцияның басталу уақыты;

6) операцияның аяқталу уақыты;

7) оқиғаның сипаттамасы.

30. Оқиғаларды тіркеу журналындағы жазбалар мәтіндік үлгіде сақталады.

31. Оқиғаларды тіркеу журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

32. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылады.

33. Оқиғаларды тіркеу журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз етуге
мониторинг жүргізу
қағидаларына
5-қосымша
Нысан

"Электрондық үкімет" ақпараттандыру объектісінің осалдығы туралы деректердің тізбесі

Осалдығын анықтау күні мен уақыты	Контур	Ақпараттандыру объектісінің атауы	Ақпараттандыру объектісінің компоненті (атауы, IP, hostname және т.б.)	Порт	Осалдықты сипаттау	Қосымша ақпарат
1	2	3	4	5	6	7
	Сыртқы/ Ішкі контур					

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз етуге
мониторинг жүргізу
қағидаларына
6-қосымша
Нысан

Осалдықтарды жоймау себептерінің санаттары және жоймау себептерінің негіздемесі

Осалдықтарды жоймау себептерінің санаттары	Осалдықты жоймау себептерін негіздеу
Өндірістік қажеттілік	"Электрондық үкімет" ақпараттандыру объектісінің осалдығы мен жай-күйінің сипаттамасы; осалдықты жою бойынша қабылданған шаралар; ақпараттандыру объектісіндегі қажетті өзгерістердің себептері мен сипаты; бірінші рет анықталған күннен бастап алты айдан аспайтын осалдықты жою мерзімдері.
Нөлдік күн осалдығы	"Электрондық үкімет" ақпараттандыру объектісінің осалдығы мен жай-күйінің сипаттамасы, сондай-ақ осалдықты пайдалану ықтималдығын төмендету бойынша қабылданған іс-шаралар.

	Осалдық ретінде анықталған "электрондық үкіметті"
Жалған іске қосылу	

	ақпараттандыру объектісінің сипаттамасын немесе жай-күйін сипаттау.

"Электрондық үкіметтің"
ақпараттандыру объектілерінің
және ақпараттық-
коммуникациялық
инфрақұрылымның аса маңызды
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз
етуге мониторинг
жүргізу қағидаларына
7-қосымша
Нысан

Анықталған ақпараттық қауіпсіздік оқиғасы немесе ақпараттық қауіпсіздіктің оқыс оқиғасы туралы деректер тізбесі

Ескерту. Қағидалар 7-қосымшамен толықтырылды - ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 23.04.2025 № 175/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

АҚ оқиғасы/АҚ оқыс оқиғасы тіркелген күні	
Егжей-тегжейліліктер	Анықтау күні мен уақыты; Шығу орнының IP-мекенжайы; Нысананың IP-мекенжайы (ОТЖ-да ақпарат болған жағдайда); Құрылғының атауы / Компьютердің аты; АҚ оқиғасының/АҚ оқыс оқиғасының атауы; Файл жолы / Сұрау салу (ОТЖ-да ақпарат болған жағдайда); Серверден жауап коды (ОТЖ-да ақпарат болған жағдайда); АҚҚ-да әрекет ету саны (ОТЖ-да ақпарат болған жағдайда); Дереккөз-ұйым (ОТЖ-да ақпарат болған жағдайда); Алғашқы тіркеу/қайта тіркеу;
АҚ оқиғасының/АҚ оқыс оқиғасының сипаты	ОТЖ-да қосымша ақпарат болған жағдайда
ЭҮ АО иесі немесе иеленушісі	
АҚ оқиғасы/АҚ оқыс оқиғасы анықталған объект	
Ескертпе	