

"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 министрінің 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) 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, 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 – 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) бұйрығымен.

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:

- 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. Өнеркәсіптік пайдалануға енгізілген ЭҰ АО АҚҚМ объектілері болып табылады, оның ішінде АКИАМО-ға:

мемлекеттік құпияларды құрайтын мәліметтерді қамтитын электрондық ақпараттық ресурстар;

мемлекеттік құпияларға жататын, орындалуы қорғалған ақпараттық жүйелер;

ЭҰ АО-мен интеграцияланбайтын Қазақстан Республикасы Ұлттық Банкінің ақпараттандыру объектілерінен басқалар жатады.

5. ЭҰ ақпараттандыру объектілерінің АҚҚМ мынадай нұсқалардың бірі бойынша өткізіледі:

- 1) бір жұмыс түрі бойынша;
- 2) бірнеше жұмыс түрлері бойынша;
- 3) жұмыс түрлерінің толық құрамында жүргізіледі.

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.

Ескерту. 6-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-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 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 ЭҮ АО туралы мәліметті қағаз және электронды түрде ұсынады (бұдан әрі – Мәліметтер).

Ескерту. 8-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.

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

Ескерту. 9-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.

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.

Ескерту. 10-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.

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.

Ескерту. 11-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.

12. "МТҚ" АҚ АҚ оқыс оқиғаларына ден қою мониторингін жүргізген кезде АҚҚМ 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.

Ескерту. 12-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.

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 ЭҰ 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.

Ескерту. 13-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.

14. АҚҰҰО 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.

Ескерту. 14-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.

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.

Ескерту. 15-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.

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.

Ескерту. 16-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.

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.

Ескерту. 17-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.

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 АҚОМ 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. 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.

Ескерту. 19-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.

20. АКИАМО меншік иесі немесе иеленушісі Заңның 6-бабы 4) тармақшасына сәйкес бекітілетін, АКИАМО тізіліміне енгізілу күнінен бастап тоқсан күнтізбелік күн ішінде АКИАМО АҚ қамтамасыз ету мониторинг жүйесін (бұдан әрі – АҚ ҚМЖ)

АҚЖО техникалық құралдарына қосылуды қамтамасыз етеді, сондай-ақ АКИАМО АҚ бойынша жауапты тұлғаны анықтайды.

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 АҚЖО техникалық құралдарына қосылғаннан кейін АҚЖО АҚ ҚМЖ АҚ оқыс оқиғасын анықтаған жағдайда, АҚЖО АҚ оқыс оқиғаны анықтаған сәттен бастап 24 сағаттан аспайтын мерзімде, АКИАМО АҚ бойынша жауапты тұлғаға хабарлау жолымен, АҚ анықталған оқыс оқиғасы туралы АКИАМО меншік иесін немесе иеленушісін хабардар етеді.

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

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.

Ескерту. 24-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.

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
I-қосымша
Нысан

"Электрондық үкіметтің" ақпараттандыру объектісі туралы мәліметтер

1. "Электрондық үкіметтің" ақпараттандыру объектісінің ресми атауы.
2. "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі.

3. "Электрондық үкіметтің" ақпараттандыру объектісінің иеленуші (бар болған жағдайда).

4. "Электрондық үкіметтің" ақпараттандыру объектісінің нақты орналасқан жері (облысы, қаласы).

5. Мемлекеттік органдардың бірыңғай көлік ортасына қосылу нүктесінің болуы және байланыс арнасының өткізу қабілеті туралы ақпарат.

6. Мемлекеттік органдардың Интернет қосылу нүктесінің болуы: IP-мекенжайы (немесе IP-мекенжайлары), домендік атауы (бар болған жағдайда).

7. Меншік иесі немесе иеленуші бекіткен және оның қолымен және мөрімен (бар болған жағдайда) куәландырылған түсіндірме жазбасы бар "электрондық үкіметтің" ақпараттандыру объектісінің жалпы функционалдық сызбасы.

8. "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісі бекіткен және оның қолымен және мөрімен (бар болған жағдайда) куәландырылған "электрондық үкіметтің" ақпараттандыру объектісінің логикалық және физикалық архитектуралық кестелері.

9. Осы нысанның 1-қосымшасына сәйкес нысан бойынша "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісімен бекітілген және оның мөрімен (бар болған жағдайда) және мөртабанымен куәландырылған "электрондық үкіметтің" ақпараттандыру объектісінің техникалық құралдары тізбесі.

10. Осы нысанның 2-қосымшасына сәйкес нысан бойынша "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі және иеленушісімен бекітілген және оның мөрімен (бар болған жағдайда) және қолымен куәландырылған "электрондық үкіметтің" ақпараттандыру объектісінің бағдарламалық құралдары тізбесі.

11. Жүйенің, әзірлеушінің, үлгілердің атауын көрсете отырып және оқиғаларды тіркеу журналдарының түрлерін қоса беріп, оқиғаларды тіркеу журналдарын жинау жүйесі туралы ақпарат.

12. АҚҚМ объектісінің меншік иесі немесе иеленушісі бекіткен және оның қолымен және мөрімен (бар болған жағдайда) куәландырылған ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманың көшірмесі.

13. "Электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге жауапты тұлғаның байланыс деректері.

14. "Электрондық үкіметтің" ақпараттандыру объектісінің желілік IP-мекенжайларының, оның ішінде ақпаратты қорғау құралдарының тізбесі.

"Электрондық үкіметтің"
ақпараттандыру объектісі
туралы мәліметтерге
1-қосымша
Нысан

"Электрондық үкіметтің" ақпараттандыру объектісінің техникалық құралдарының тізбесі

P/c №	Өндіруші, үлгісі	Сериялық /түгендеу нөмірі	Желілік мекенжай	Нақты орналасқан жері	Түрі (техникалық құжаттамаға сәйкес)	Негізгі функциялық мақсаты ("электрондық үкіметтің" ақпараттандыру объектісіне бағдарламалық құжаттамаға сәйкес)	Ақпаратты қорғаудың пайдаланылатын әдістері	Әзірлеуші, атауы, нұсқасы (кіріктірілген бағдарламалық қамтылымның)
1	2	3	4	5	6	7	8	9

"Электрондық үкіметтің" ақпараттандыру объектісі туралы мәліметтерге
2-қосымша
Нысан

"Электрондық үкіметтің" ақпараттандыру объектісінің бағдарламалық құралдарының тізбесі

P/c №	Әзірлеуші	Атауы	Нұсқасы	Орналасқан жері (техникалық құралдардың тізбесінен)	Түрі (бағдарламалық құжаттамаға сәйкес)	Негізгі функционалдық мақсаты (бағдарламалық құжаттамаға сәйкес)	Ақпаратты қорғаудың пайдаланылатын әдістері
1	2	3	4	5	6	7	8

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

Ақпараттық қауіпсіздіктің оқыс оқиға туралы деректер тізімі

Оқыс оқиғаны тіркеу күні	
Ақпараттық қауіпсіздік оқыс оқиғасының маңыздылық деңгейі*	5-деңгей (қара); 4-деңгей (қызыл); 3-деңгей (қызғылт сары); 2-деңгей (сары);

	1-деңгей (жасыл); 0-деңгей (ак);
Оқыс оқиға түрі	Қызмет көрсетуден бас тарту (DoS, DDoS); Заңсыз қолжетімділік және қамтылымды модификациялау; Ботнет; Вирустық шабуыл; Осалдықтарды пайдалану; Құралдарды бұрмалау; Аутентификация/авторландыру құралдарын компрометациялау; Фишинг; Басқа.
Ауқымы	Жеке; жаппай.
Детальдар	Туындау күні мен уақыты; Анықтау күні мен уақыты; Хабарлау күні мен уақыты; Оқиға аяқталды ма? (егер "иә" болса, күн/сағат/минут, өлшемінде қанша ұзақ созылғанын дәлдеу); Қайтадан/жаңадан; компрометация индикаторы (ИОС).
Белгілер	Нақты; Әрекет; Күдік.
Көз	Ішкі контур; Сыртқы контур.
Оқыс оқиға сипаттамасы	
Зардабы	Зардапсыз; Жұмыс қабілеттілігінің бұзылуы; Тұтастықтың бұзылуы; Ақпарат құпиялық режимінің бұзылуы.
Залал тиген объект	
Оқыс оқиғаны шешу үшін қолданылған іс-қимылдар	
Ескертпе	

Ақпараттық қауіпсіздіктің оқыс оқиғасының маңыздылық деңгейлері

	Маңыздылық деңгейі	Анықтама
Маңызды	5-деңгей (қара)	Қызмет көрсету мүмкіндігін жоятын, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын, айналып өту мүмкін емес оқыс оқиғалар.
		Қызмет көрсету мүмкіндігін жоятын, электрондық ақпараттық ресурстар, ақпараттық жүйелер,

Елеулі	4-деңгей (қызыл)	телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын ықтимал оқыс оқиғалар.
Жоғары	3-деңгей (қызғылт сары)	Қызмет көрсету мүмкіндігін айтарлықтай шектейтін, жағдайдың айтарлықтай нашарлауына, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын ықтимал оқыс оқиғалар.
Орташа	2-деңгей (сары)	Қызмет көрсету мүмкіндігін шектейтін, жағдайдың айтарлықтай нашарлауына, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын болуы мүмкін оқыс оқиғалар.
Төмен	1-деңгей (жасыл)	Қызмет көрсету мүмкіндігін шектейтін, жағдайдың нашарлауына, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін елеусіз теріс салдарға әкеп соғатын болуы екіталай оқыс оқиғалар.
Маңызды емес	0-деңгей (ақ)	Электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және басқа ақпараттандыру объектілеріне әсер етпейтін елеусіз оқыс оқиғалар.

"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 активациялау/деактивациялау;
- 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, HP-UX 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, psexec * .exe, ps.exe * .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 таймауына 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 жазбалардын 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.

"Электрондық үкіметтің"
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.
Жалған іске қосылу	Осалдық ретінде анықталған "электрондық үкіметті" ақпараттандыру объектісінің сипаттамасын немесе жай-күйін сипаттау.