"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" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 7-1-бабының 7) тармақшасына сәйкес БҰЙЫРАМЫН:

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

1-тарау. Жалпы ережелер

1. Осы "Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидалары (бұдан әрі – Қағида) " Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 7) тармақшасына сәйкес әзірленді және "электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар мен қысқартулар пайдаланылады:

1) ақпараттандыру объектілері – электрондық ақпараттық ресурстар, бағдарламалық қамтылым 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 қамтылымда жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын заңсыз іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық қамтылымдағы кемшілік;

4) ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын және мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестікке аттестаттау (бұдан әрі – аттестаттау) – аттестаттау объектілерінің қорғалуының жай-күйін, сондай-ақ олардың ақпараттық қауіпсіздік талаптарына сәйкестігін айқындау жөніндегі ұйымдастырушылық-техникалық іс-шаралар;

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

6) ақпараттық қауіпсіздік оқиғаларды жүйесін басқару агенті – оқиғаларды жинау үшін белсенді серверлік, желілік және (немесе) мамандандырылған жабдыққа орнатылатын бағдарламалық қамтылым;

7) 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;

8) 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;

9) 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;

10) 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;

11) Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы (бұдан әрі – АҚҰҮО) – Қазақстан Республикасы Ұлттық қауіпсіздік комитетінің "Мемлекеттік техникалық қызмет" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнының құрылымдық бөлімшесі;

12) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері (бұдан әрі – АКИАМО) – жұмыс істеуінің бұзылуы немесе тоқтауы әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайға немесе Қазақстан Республикасының қорғанысы, қауіпсіздігі, халықаралық қатынастары, экономикасы, жекелеген шаруашылық салалары, инфрақұрылымы үшін немесе тиісті аумақта тұратын халықтың тыныс-тіршілігі үшін айтарлықтай теріс салдарларға әкеп соғатын ақпараттық-коммуникациялық инфрақұрылымның, оның ішінде "электрондық үкіметтің" ақпараттық-коммуникациялық инфрақұрылымының объектілері;

13) мемлекеттік техникалық қызмет (бұдан әрі – "МТҚ" РМК) – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған, шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорын;

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

15) оқиғалардың тіркеу журналдарын жинаудың бірыңғай 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 электрондық ақпараттық ресурстар, мемлекеттік органдардың бағдарламалық қамтылымы және "электрондық үкіметтің" ақпараттық-коммуникациялық инфрақұрылымы, оның ішінде мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйелер;

17) "электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингі (бұдан әрі – АҚҚМ) – ақпараттық қауіпсіздіктің оқыс оқиғалары мен қауіптерін анықтау мақсатында "электрондық үкіметтің" ақпараттандыру объектілеріне бақылау жүргізу, сондай-ақ оларды жою мен алдын алу бойынша шаралар қолдану;

18) "электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздікті қамтамасыз етуді мониторингілеу жүйесі – ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды бақылайтын, соның ішінде ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу және ақпараттық қауіпсіздікті бұзу оқиғаларына жауап беретін ұйымдастырушылық және техникалық шаралар;

19) "электрондық үкіметтің" архитектуралық порталы – сыныптауышқа сәйкес "электрондық үкіметтің" ақпараттандыру объектілері туралы мәліметтерді тіркеуді жүзеге асыруға, есепке алуға, сақтауға және бір жүйеге келтіруге және ақпараттандыру саласында мониторингілеу, талдау және жоспарлау үшін мемлекеттік органдардың одан әрі пайдалануына арналған ақпараттық жүйе.

Осы Қағидаларда пайдаланылатын өзге де ұғымдар Заңға сәйкес қолданылады.

3. АҚҚМ-ды "электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуді мониторингілеу жүйесі арқылы "МТҚ" РМК жүргізеді.

4. Өнеркәсіптік пайдалануға берілген "электрондық үкіметтің" ақпараттандыру объектілері АҚҚМ объектілеріне жатады, мыналардан басқа:

- мемлекеттік құпияларды құрайтын мәліметтерді қамтитын электрондық ақпараттық ресурстар;

- АҚҚМ объектілерімен интеграцияланбаған Қазақстан Республикасы Ұлттық Банкінің " электрондық үкіметтің" ақпараттандыру объектілері.

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

5. "МТҚ" РМК 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 және АҚ бойынша аттестаттау талаптарына сәйкестігін сынау кезеңдерінен алынған мәліметтерді қолданады, оның ішінде:

1) бағдарламалық және техникалық құралдар тізбесін;

2) телекоммуникация желілерінің схемаларын;

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

4) деректер базасының құрылымын қоса алғанда АҚ бойынша аттестаттау және АҚ бойынша сынақ жүргізу кезеңінде алынған мәліметтерді қолданады.

6. АҚҚМ объектісінің меншік иесі немесе иеленушісі оны өнеркәсіптік пайдалануға енгізген немесе одан шығарған күннен бастап 10 жұмыс күні ішінде "МТҚ" РМК-ні АҚҚМ объектісін өнеркәсіптік пайдалануға енгізу туралы немесе одан шығару туралы хабарлайды және "электрондық үкіметтің" ақпараттандырудың осы объектісі туралы мәліметті осы Қағидаларға 1-қосымшаға сәйкес нысан бойынша ақпарат жолдайды (бұдан әрі – Мәліметтер).

7. "МТҚ" РМК АҚҚМ жүргізу бойынша кесте әзірлейді және оны Қазақстан Республикасының Ұлттық қауіпсіздік комитеті (бұдан әрі – ҚР ҰҚК) және АҚҚМ объектісінің меншік иесі немесе иеленушісімен келіседі.

8. "МТҚ" РМК АҚҚМ жүргізу шеңберінде мыналарды іске асырады:

1) АҚ-ның оқыс оқиғаларының пайда болуына мемлекеттік органдардың АҚҚМ объектілері жағдайын қадағалау мыналарды қамтиды:

"МТҚ" РМК АҚ оқиғаларын басқару жүйесіне беру үшін оқиғаларды тіркеу журналының тізбесін анықтау мақсатында мемлекеттік органдардың (бұдан әрі – МО) ақпараттандыру объектілерін талдау;

МО ақпараттандыру объектісінің меншік иесі мен иеленушісінің оқиғаларды тіркеу журналын жинаудың бірыңғай жүйесіне және қажеттілік туындаса МО ақпараттандыру объектісінің меншік иесі немесе иеленушісінің өзге ақпараттық-коммуникациялық инфрақұрылым объектілеріне АҚ оқиғаларын басқару жүйелерінің агентін орнату;

"МТҚ" РМК АҚ оқиғаларын басқару жүйесінде МО ақпараттандыру объектілерінің оқиғаларды тіркеу журналын жинау, оларды өңдеу және АҚ оқиғалары мен АҚ оқыс оқиғаларын анықтау мақсатында талдау;

МО ақпаратандыру объектілерінде анықталған АҚ оқыс оқиғалары мен АҚ оқиғаларын бастапқы талдау;

Анықталған АҚ оқиғалары мен АҚ оқыс оқиғалары жайлы МО ақпараттандыру объектісінің меншік иесі мен иеленушісін АҚ оқиғасы, АҚ оқыс оқиғаны анықталған сәттен бастап 30 минут ішінде, ҚР ҰҚК – 24 сағат ішінде хабардар ету.

МО ақпараттандыру объектісінің меншік иесі мен иеленушісіне АҚ оқыс оқиғаларының таралуын тоқтата тұру бойынша бастапқы ұсыныстар беру;

АҚ оқыс оқиғаларына ден қою шеңберінде қажет болған жағдайда, МО ақпараттандыру объектілері орналасқан жерге "МТҚ" РМК қызметкерін жіберу (қажеттілік ҚР ҰҚК немесе "МТҚ" РМК-мен өз бетінше анықталады);

МО ақпараттандыру объектілерінде анықталған АҚ оқыс оқиғаларын талдау;

"МТҚ" РМК оқыс оқиға талдауын аяқтаған сәттен бастап 48 сағат ішінде МО ақпараттандыру объектісінің меншік иесі немесе иеленушісіне АҚ оқыс оқиғаларын жою және оларды одан әрі алдын алу бойынша ұсынымдар беру;

АҚ оқыс оқиғаларын жою одан әрі алдын алу бойынша ұсынымдар берілген сәттен бастап МО ақпараттандыру объектісінің меншік иесі немесе иеленушісінің 48 сағат ішінде АҚ оқыс оқиғаларын жоймауы туралы ҚР ҰҚК-ні және Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрлігін (бұдан әрі – ҚР ҚАӨМ) хабардар ету.

2) АҚҚМ объектілерінің қорғалу жағдайын қадағалау мыналарды қамтиды:

АҚҚМ бойынша жұмыс жүргізу кестесіне сәйкес осалдықтар табуға АҚҚМ объектілерін зерттеп-қарау (бұдан әрі – осалдықтарға зерттеп-қарау);

АҚҚМ объектілерінің меншік иесі немесе иеленушісіне осалдықтарға зерттеп-қарау бойынша жұмыстар аяқталғаннан кейін 10 жұмыс күн ішінде АҚҚМ объектілерін осалдықтарға зерттеп-қарау нәтижелерін және осалдықтарды жою бойынша ұсынымдар беру;

осалдықтарға зерттеп-қарау шеңберінде анықталған АҚҚМ объектілерінің осалдықтарын жою мәселесі бойынша АҚҚМ объектілерінің осалдықтарын жою мәселесі бойынша АҚҚМ объектілерінің меншік иесі немесе иеленушісіне консультация беру;

3) АҚҚМ объектілерін АҚ-ны қамтамасыз ету бойынша техникалық және ұйымдастыру іс-шараларын толық және сапалы іске асырылуын қадағалау мыналарды қамтиды:

АҚҚМ объектісін осы Қағидаларға 2-қосымшада келтірген АҚҚМ бойынша жұмыс жүргізу кестесіне сәйкес ақпараттық қауіпсіздік жөніндегі техникалық құжаттама (бұдан әрі – АҚ жөніндегі ТҚ) талаптарын орындау бөлігінде зерттеп-қарау;

АҚҚМ меншік иесі мен иеленушісіне аталған зерттеп-қарау аяқтанған күннен баспат 10 жұмыс күні ішінде АҚ жөніндегі ТҚ талаптарын орындау бөлігінде АҚҚМ объектісін зерттеп-қарау нәтижелерін және анықтылған АҚ жөніндегі ТҚ бұзушылықтарын жою бойынша ұсыным ұсыну.

4) АҚҚМ объектілерінің функционалдығы және жұмыс істеу шарттарының өзгермеушілігін қадағалау мыналарды қамтиды:

АҚҚМ бойынша жұмыс жүргізу кестесіне сәйкес АҚҚМ объектісінің фунционалдығы және жұмыс істеу шарттарының өзгеруін (бұдан әрі – АҚҚМ объектілерінің өзгеруі) анықтау бойынша ұйымдастырушылық және техникалық іс-шараларды жүргізу;

АҚҚМ объектілерінің анықталған өзгерістерін есептеу;

АҚҚМ объектілерінің анықталған өзгерістерін талдау;

ҚР ҰҚК-не және АҚҚМ объектісінің меншік иесі мен иеленушісіне АҚҚМ объектісінің өзгерісі анықталған сәттен бастап 10 жұмыс күні ішінде АҚҚМ объектісінің өзгерісін талдау нәтижесін ұсынады.

9. АҚҚМ объектісінің меншік иесі мен иеленушісі "МТҚ" РМК-ға АҚҚМ бойынша жұмыстар жүргізу үшін, жағдайлар жасайды, оған мыналар кіреді:

АҚҚМ объектілеріне, АҚҚМ объектісі меншік иесінің немесе иеленушісінің оқиғаларды тіркеу журналдарын жинаудың бірыңғай жүйесіне АҚҚМ объектісінің меншік иесі немесе иеленушісі қызметкерлерінің сүйемелдерімен "МТҚ" РМК қызметкерлеріне тәулік бойы физикалық қолжетімділік;

"МТҚ" РМК қызметкерлеріне АҚҚМ объектісіне тәулік бойы желілік қолжетімділік болатындай тегін негізде екі жұмыс орын;

АҚҚМ объектісі меншік иесі немесе иеленушісінің оқиғаларды тіркеу журналдарын жинаудың бірыңғай жүйесіне шектеусіз барлық операцияларды орындай алатындай "МТҚ" РМК-ға желілік қолжетімділік.

10. МО ақпараттандыру объектілерінің меншік иесі немесе иеленушісі МО ақпараттандыру объектілерінің жағдайына "МТҚ" РМК АҚ-ның оқыс оқиғаларының пайда болуына қадағалау жүргізу кезінде:

осы Қағидаларға 3-қосымшада келтірілген "электрондық үкімет" ақпараттандыру объектілерінің оқиғаларын тіркеу журналдары жазбаларының типтері және форматтарына сәйкес МО ақпараттандыру объектісінің оқиғаларының журналдануын ұйымдастырады;

МО ақпараттандыру объектілерінің меншік иесі немесе иеленушісінің оқиғаларды тіркеу журналдарын жинаудың біріңғай жүйесіне МО ақпараттандыру объектісінің оқиғаларын тіркеу журналын беруді ұйымдастырады;

МО ақпараттандыру объектісінің оқиғаларының журналдануына өзгерістер енгізу бойынша жоспарланған жұмыстар бойынша өзгерістер енгізгенге дейін 5 жұмыс күн бұрын "МТҚ" РМК-ны хабардар етеді;

"МТҚ" РМК АҚ оқиғаларын басқару жүйесіне ақпараттандыру объектісінің меншік иесі немесе иеленушісінің оқиғаларды тіркеу журналдарын жинаудың бірынғай жүйесінен МО

ақпараттандыру объектісінің оқиғаларды тіркеу журналын беру үшін "МТҚ" РМК-мен келісілген жағдайлар жасайды;

"МТҚ" РМК-ні МО ақпараттандыру объектісінде өзі анықталған АҚ оқиғаны туралы ол анықталған сәттен бастап 15 минут ішінде хабардар етеді;

"МТҚ" РМК-ға осы Қағидаларға 4-қосымшаға сәйкес нысан бойынша МО (бұдан әрі – Деректер тізбесі) ақпараттандыру объектісінде анықталған АҚ-ның оқыс оқиғасы туралы деректер тізбесін АҚ-ның оқыс оқиғасы анықталған сәттен бастап 24 сағат ішінде ұсынады.

11. "МТҚ" РМК АҚҚМ объектілері қорғалуы жағдайда қадағалау жүргізген кезде АҚҚМ объектілерінің меншік иесі немесе иеленушісі:

осалдықтарды табуға зерттеп-қарау нәтижелерін алған күннен бастап 1 айдың ішінде АҚҚМ объектісінің осалдықтарын жою үшін қабылданған шаралар туралы ақпаратты "МТҚ" РМК-ға жолдайды;

АҚҚМ объектісінің осалдығы жойылмаған жағдайда осы Қағидаларға 5-Қосымшаға сәйкес осалдықпен санаттардың біреуіне жатқызады (өндірістік қажеттілік, нолдік күннің осалдығы, алдамшы іске қосылу) және қажетті қимылтарды жүргізеді.

"МТҚ" РМК-ға осы Қағидаларға 6-қосымшаға сәйкес нысан бойынша "электрондық үкіметтің" ақпараттандыру объектісінің осалдығы туралы деректер тізбесін АҚҚМ объектісінің осалдығы анықталған сәттен бастап 24 сағат ішінде 6-қосымшаға сәйкес ұсынады.

12. "МТҚ" РМК АҚҚМ объектілерін АҚ қамтамасыз ету бойынша техникалық және ұйымдастыру іс-шараларының толығымен және сапалы іске асырылуына қадағалау жүргізген кезде АҚҚМ объектісінің меншік иесі мен иеленушісі АҚҚМ объектілерінің АҚ жөніндегі ТҚ талаптарын орындауға зерттеп-қарау нәтижесін алған күннен бастап, бір ай ішінде "МТҚ" РМК-ға анықталған АҚ жөніндегі ТҚ бұзушылықтарына қатысты қабылданған шаралар туралы ақпарат ұсынады.

13. АҚҚМ объектісің өзгерісін талдау үшін мәліметтер жеткіліксіз болған жағдайда "МТҚ" РМК жұмыс істеу және функционалдылығы шарттарының өзгермеуі қадағалау кезінде АҚҚМ объектісі туралы қосымша мәліметтерді сұратуға құқылы. АҚҚМ объектісінің меншік иесі немесе иеленушісі "МТҚ" РМК-дан сұраныс алған күннен бастап 3 жұмыс күні ішінде АҚҚМ объектісі туралы қосымша мәліметтер сұратады.

14. АҚҚМ объектілерінің тізбесін қалып тастыру мақсатында "МТҚ" РМК "электрондық үкіметтің" ақпараттандыру объектілері туралы мәліметті осы Қағидаға 1-қосымшаға сәйкес нысан бойынша сұратады. АҚҚМ объектісінің меншік иесі немесе иеленушісі "МТҚ" РМК-дан сұраныс алған сәттен бастап 10 жұмыс күні ішінде АҚҚМ объектісі туралы сұратылатын мәліметтерді электронды формада "МТҚ" РМК-ға ұсынады.

15. АҚҚМ объектісінің АҚ бойынша жауапты тұлғасының байланыс деректері өзгерген жағдайда АҚҚМ меншік иесі немесе иеленушісі аталған өзгеріс сәтінен бастап 48 сағат ішінде " МТҚ" РМК-ға өзекті байланыс деректерін жолдайды.

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

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 ету мониторингін жүргізу тәртібі

17. АКИАМО ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингі АКИАМО иеленушісінің АҚ бойынша өз бөлімшесімен немесе Қазақстан Республикасының азаматтық заңнамасына сәйкес үшінші тұлғалардан қызмет сатып алу арқылы жүзеге асырылады.

18. АКИАМО-ның меншік иесі мен иеленушісі Заңының 6-бабының 4) тармақшасына сәйкес АКИАМО-ның ақпараттық қауіпсіздікті қамтамасыз ету мониторинг жүйесін АҚЖО техникалық құралына қосылуды қамтамасыз етеді, сонымен қатар АКИАМО тізіліміне енгізілу күнінен бастап отыз күн ішінде АКИАМО-ның ақпараттық қауіпсіздік бойынша жауаптыны анықтайды.

19. АКИАМО АҚҚМЖ-ні АҚЖО-ның техникалық құралдарына қосу АКИАМО меншік иесінің немесе иеленушісінің АҚ бойынша бөлімшесімен немесе Қазақстан Республикасының азаматтық заңнамасына сәйкес үшінші тұлғалардың қызметін сатып алу арқылы жүзеге асырылады.

20. АКИАМО АҚҚМЖ АҚЖО-ның техникалық құралдырына қосылғаннан кейін АҚ ЖО АҚ қамтамасыз ету мониторингі жүйесімен АҚ оқыс оқиғаны анықталған жағдайда АҚЖО АҚ оқыс оқиғаны анықталған сәттен бастап 24 сағаттан аспайтын мерзімде АКИАМО АҚ бойынша жауаптыға хабарлау жолымен АКИАМО меншік иесін немесе иеленушісін анықталған АҚ оқыс оқиғасы туралы хабардар етеді.

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

22. АКИАМО-ның АҚ бөлігі АҚ-ның оқыс оқиғаларын өз бетімен анықтаған жағдайда АКИАМО АҚ бойынша жауапты АҚҚМЖ мен АҚЖО-ны АҚ оқыс оқиғасы анықталған сәттен бастап 24 сағат ішінде Қағидаларға 4-қосымшаға сәйкес нысан бойынша АҚ-ның оқыс оқиғалары туралы Деректер тізбесін жолдау арқылы хабарлайды.

	"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 деректер

1. "Электрондық үкіметтің" ақпараттандыру объектісінің ресми атауы.

2. "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі.

3. "Электрондық үкіметтің" ақпараттандыру объектісінің иеленуші.

4. "Электрондық үкіметтің" ақпараттандыру объектісінің физикалық орналасқан жері.

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

6. Мемлекетік органдардың Интернет қосылу нүктесінің болуы: IP-мекенжайы (немесе IP-мекенжайлары), домендік атауы (егер болса).

7. Меншік иесі немесе иеленуші бекіткен және оның қолымен және мөрімен куәландырылған түсіндірме жазбасы бар "электрондық үкіметтің" ақпараттандыру объектісінің жалпы функционалдық схемасы.

8. "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісі бекіткен және оның қолымен және мөрімен куәландырылған "электрондық үкіметтің" ақпараттандыру объектісінің логикалық және физикалық архитектуралық схемалары.

9. Осы нысанның 1-қосымшасына сәйкес нысан бойынша "Электрондық үкіметтің" ақпараттандыру объектісінің меншік иесі немесе иеленушісімен бекітілген және оның мөрімен 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 және қолымен куәландырылған "электрондық үкіметтің" ақпараттандыру объектісінің бағдарламалық құралдары тізбесі.

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

12. АҚ бойынша ТҚ-ға сәйкес ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманың меншік иесі немесе иеленуші бекіткен және оның қолымен және мөрімен куәландырылған ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманың көшірмесі.

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

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

"Электрондық үкіметтің" ақпараттандыру объектісінің техникалық құралдарының тізбесі

						Негізгі функционалдық мақсаты ("		

Р/с №	Өндіруші, үлгісі	Сериялық / түгендеу нөмірі	Желілік мекенжай	Физикалық орналасқан жері	Типі (техникалық құжаттамаға сәйкес)	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

Р/с №	Әзірлеуші	Атауы	Нұсқасы	Орнатылған жері (техникалық құралдардың тізбесінен)	Типі (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 қауіпсіздік жөніндегі техникалық құжаттама

1. Ақпараттық қауіпсіздік саясаты.

2. Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі. Ақпараттық қауіпсіздік қатерлерінің (тәуекелдерінің) каталогы. Ақпараттық қауіпсіздік қатерлерін (тәуекелдерін) өңдеу жоспары.

3. Ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және маркалау қағидалары.

4. Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету қағидалары.

5. Есептеу техникасы құралдарын, телекоммуникация жабдығын және бағдарламалық қамтылымды түгендеу мен паспорттандыру қағидалары.

6. Ішкі ақпараттық қауіпсіздікке ішкі аудит жүргізу қағидалары.

7. Ақпаратты қорғаудың криптографиялық құралдарын пайдалану қағидалары.

8. Электрондық ақпараттық ресурстарына қол жеткізу құқықтарын шектеу қағидалары.

9. Интернет және электрондық поштаны пайдалану қағидалары.

10. Аутентификация рәсімдерін ұйымдастыру қағидалары.

11. Вирусқа қарсы бақылауды ұйымдастыру қағидалары.

12. Ақпаратты өндеу құралдарын физикалық қорғауды және электрондық ақпараттық ресурстарының қауіпсіз жұмыс істеу ортасын ұйымдастыру қағидалары.

13. Ақпаратты резервтік көшіру және қалпына келтіруді жүргізу регламенті.

14. Қолданушылардың ақпараттық қауіпсіздіктің оқыс оқиғаларына және штаттан тыс (дағдарысты) жағдайларда ден қою бойынша іс-қимыл тәртібі туралы нұсқаулық.

15. Әкімшінің ақпараттандыру объектісін сүйемелдеу жөніндегі нұсқаулығы.

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

"Электрондық үкімет" ақпараттандыру объектілерінің оқиғаларын тіркеу журналдары жазбаларының форматтары мен типтері

1-тарау. Операциялық жүйенің оқиғаларын тіркеу журналдары жазбаларының форматтары мен типтері

1. Журналдауға жататын операциялық жүйенің (бұдан әрі - ОЖ) оқиғаларының типтері:

1) жүйені іске қосу/тоқтату;

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

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

4) операциялық жүйеде қолданушылардың авторландыру (енгізу және шығару), сәтті және сәтсіз авторландыру әрекеттері;

5) жүйелік конфигурациясының өзгеруі;

6) есептік жазбаларды құру, жою және түрлердіру;

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: ҚҚ:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) хост атауы;

3) оқиғаның сипаттамасы.

3. Linux тектес серверлік ОЖ үшін орнатылатылу тиіс оқиғалар:

1) әртүрлі IP-мекенжайлардан сол серверге бірдей шоттың қосылуын белгілеу;

2) жүйеде жаңа порттардың іске қосылуын тіркеу;

3) негізгі логтерді тіркеу /var/log/secure, /var/log/messages, /var/log/audit:

4. Windows тектес ОЖ-ның тіркеу құралдарымен қамтамасыз етілген оқиғалар тізімі, соның ішінде штаттық ақпарат:

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 форматта сақталуы керек.

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

7. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылуы тиіс.

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

2-тарау. Деректер базасын басқару жүйесіндегі оқиғаларды тіркеу журналдары жазбаларының форматтары мен типтері

9. Журналдауға жататын деректер базасын басқару жүйесінің оқиғаларының типтері:

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 форматта сақталуы керек.

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

13. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылуы тиіс.

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

3-тарау. Телекоммуникациялық жабдық оқиғаларын тіркеу журналдары жазбаларының форматтары мен типтері

15. Журналдауға жататын телекоммуникациялық жабдық оқиғалары:

1) жүйені іске қосу/тоқтату;

2) жүйенің конфигурациясын өзгерту;

3) локалдық есептік жазбалардын құру, жою, түрлендіру;

4) артықшылықты есептік жазбалардын 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 форматта сақталуы керек.

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

20. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылуы тиіс.

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

4-тарау. Қолданбалы бағдарламалық қамтылым оқиғаларын тіркеу журналдары жазбаларының форматтары мен типтері

22. Журналдауға жататын БҚ оқиғаларының типтері:

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 қолжеткізілім 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 форматта сақталуы керек.

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

26. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылуы тиіс.

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

5-тарау. Ақпаратты қорғау құралдары оқиғаларын тіркеу журналдары жазбаларының форматтары мен типтері

28. Журналдауға жататын ақпаратты қорғау құралдары оқиғаларының типтері:

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 форматта сақталуы керек.

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

32. Оқиғалар тіркеу журналдары үшін UTF-8 кодтамасы пайдаланылуы тиіс.

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

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

	қағидаларына 4-қосымша
	Нысан

Ақпараттық қауіпсіздіктің оқыс оқиға деректерінің тізімі

Оқыс оқиғаны тіркеу күні	
Ақпараттық қауіпсіздік оқыс оқиғасының маңыздылық деңгейі*	Деңгей 5 (қара); деңгей 4 (қызыл); деңгей 3 (қызғылтсары); деңгей 2 (сары); деңгей 1 (жасыл); деңгей 0 (ақ);
Оқыс оқиға типі	Қызмет көрсетуден бас тарту (DoS, DDoS) Заңсыз қолжетімділік және құрамын 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 аяқталдыма? "иә" болса, күн/сағат/минут өлшемінде қанша ұзақ созылғанын дәлдеу Қайтадан/жаңадан Компрометация индикаторы (IOC)
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		Қызмет көрсету мүмкіндігін жоятын, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және

	Деңгей 5 (қара)	басқа ақпаратандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын, айналып өту мүмкін емес оқыс оқиғалар
Елеулі	Деңгей 4 (қызыл)	Қызмет көрсету мүмкіндігін жоятын, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпаратандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын ықтимал оқыс оқиғалар.
Жоғары	Деңгей 3 (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	Деңгей 2 (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	Деңгей 1 (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	Деңгей 0 (ақ)	Электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және басқа ақпаратандыру объектілеріне әсер етпейтін елеусіз оқыс оқиғалар.

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

Осалдықтарды жоймау себептерінің санаттары және ол жойылмаған жағдайда меншік иесінің немесе иеленушінің іс-қимылдары

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 шаралар

Жалған іске қосылу	Осалдық ретінде анықталған "электрондық үкіметті" 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 6-қосымша
	Нысан

"Электрондық үкімет" ақпараттандыру объектісінің осалдығы туралы мәліметтердің тізімі

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