"Электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларын бекіту туралы" Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ бұйрығына өзгерістер мен толықтыру енгізу туралы

Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 2025 жылғы 23 сәуірдегі № 175/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2025 жылғы 24 сәуірде № 36014 болып тіркелді

БҰЙЫРАМЫН:

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

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

2-тармақта:

3) тармақша мынадай редакцияда жазылсын:

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

13) тармақша мынадай редакцияда жазылсын:

"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;";

4-тармақ мынадай редакцияда жазылсын:

"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.";

5 және 6-тармақтар мынадай редакцияда жазылсын:

"5. АҚҚМ мынадай нұсқалардың бірі бойынша жүргізіледі:

1) бір жұмыс түрі бойынша;

2) бірнеше жұмыс түрлері бойынша;

3) жұмыс түрлерінің толық құрамында.

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

8-тармақ мынадай редакцияда жазылсын:

"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).";

9, 10, 11, 12, 13, 14, 15, 16 және 17-тармақтар мынадай редакцияда жазылсын:

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

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

1) АҚ оқыс оқиғаларына ден қою мониторингі шеңберінде:

АҚҰҮО-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.

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.

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.

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.

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.

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.

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.

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.";

19 және 20-тармақтар мынадай редакцияда жазылсын:

"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.

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.";

22-тармақ мынадай редакцияда жазылсын:

"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.";

24-тармақ мынадай редакцияда жазылсын:

"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".

көрсетілген бұйрыққа 1-қосымша осы бұйрыққа 1-қосымшаға сәйкес жаңа редакцияда жазылсын;

"Электрондық үкіметтің" ақпараттандыру объектілері туралы мәліметтерге 1 және 2 -қосымшалар алып тасталсын;

көрсетілген бұйрыққа 2-қосымша осы бұйрыққа 2-қосымшаға сәйкес жаңа редакцияда жазылсын;

осы бұйрыққа 3-қосымшаға сәйкес 7-қосымшамен толықтырылсын.

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

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

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

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

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

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

Қазақстан Республикасының
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрінің міндетін атқарушы

К. Тулеушин

Қазақстан Республикасының
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрінің міндетін атқарушы
2025 жылғы 23 сәуірдегі
№ 175/НҚ бұйрығына
1 қосымша

"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

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.

Қазақстан Республикасының
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрінің міндетін атқарушы
2025 жылғы 23 сәуірдегі
№ 175/НҚ бұйрығына
2 қосымша
"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

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 мүмкінсіздігіне 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.

Қазақстан Республикасының
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрінің міндетін атқарушы
2025 жылғы 23 сәуірдегі
№ 175/НҚ Бұйрыққа
3- қосымша
"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

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	