"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 бұйрығына өзгерістер енгізу туралы"

Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрінің м.а. 2026 жылғы 8 шілдедегі № 394/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 14 шілдеде № 39299 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 Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ бұйрығына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 17019 болып тіркелген) мынадай өзгерістер енгізілсін:

тақырып мынадай редакцияда жазылсын:

"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларын бекіту туралы";

кіріспе мынадай редакцияда жазылсын:

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

1-тармақ мынадай редакцияда жазылсын:

"1. Қоса беріліп отырған "Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидалары бекітілсін.".

Көрсетілген бұйрықпен бекітілген "Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидалары осы бұйрыққа қосымшаға сәйкес жаңа редакцияда жазылсын.

2. Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Ақпараттық қауіпсіздік комитеті заңнамада белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық ресми жарияланғаннан кейін Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің интернет-ресурсында орналастыруды;

3) осы бұйрық мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Заң департаментіне осы тармақтың 1) және 2) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер ұсынуды қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Жасанды интеллект және цифрлық даму вице-министріне жүктелсін.

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

Қазақстан Республикасының
Жасанды интеллект және цифрлық даму министрінің
міндетін атқарушы *Р. Коняшкин*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасының
Жасанды интеллект
және цифрлық даму министрінің
міндетін атқарушы
2026 жылғы 8 шілдедегі
№ 394/НҚ бұйрығына
қосымша

"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидалары

1-тарау. Жалпы қағидалар

1. Осы "Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидалары (бұдан әрі – Қағидалар) "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 7) тармақшасына сәйкес әзірленді және "цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар пайдаланылады:

1) аса маңызды цифрлық объектілер (бұдан әрі – АМЦО) – бұзылуы немесе жұмыс істеуін тоқтатуы қолжетімділігі шектеулі дербес деректерді және заңмен қорғалатын құпияны қамтитын 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 үшін, оның ішінде жылумен

жабдықтау, электрмен жабдықтау, газбен жабдықтау, сумен жабдықтау инфрақұрылымы, өнеркәсіп, денсаулық сақтау, байланыс, банк саласы, көлік, гидротехникалық құрылыстар, құқық қорғау қызметі, "цифрлық үкімет" үшін елеулі теріс салдарларға алып келетін цифрлық объектілер;

2) киберқауіпсіздіктің жедел орталығы (бұдан әрі – КҚЖО) – цифрлық ресурстарды , цифрлық жүйелерді, телекоммуникация желілері мен цифрландырудың басқа да объектілерін қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі;

3) киберқауіпсіздік жөніндегі нормативтік-техникалық құжаттама – цифрлық объектілерінің және (немесе) ұйымның киберқауіпсіздікті (бұдан әрі – КҚ) қамтамасыз ету процестеріне қатысты саясатты, қорғау шараларын белгілейтін құжаттама;

4) КҚ қамтамасыз етуді мониторингтеу жүйесі – цифрлық технологияларды қауіпсіз пайдалану мониторингін жүргізуге бағытталған ұйымдастырушылық және техникалық іс-шаралар;

5) КҚ қамтамасыз ету саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) – КҚ қамтамасыз ету саласындағы басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган;

6) КҚ оқиғаларын басқару жүйесінің агенті – оқиғаларын басқару жүйесінің агенті – оқиғаларды тіркеу журналын жинау үшін цифрлық объектісінің серверлік жабдығына орнатылған бағдарламалық қамтылым;

7) КҚ оқиғаларын басқару жүйесі – цифрлық объектінің оқиғаларды тіркеу журналдарын жинау және талдау арқылы КҚ оқиғаларын автоматтандырылған түрде анықтауға арналған бағдарламалық қамтылым немесе аппараттық-бағдарламалық кешен;

8) КҚ оқиғасы – КҚ ықтимал бұзылуын немесе КҚ қамтамасыз етуге қатысы болуы мүмкін бұрын белгісіз жағдайды көрсететін, цифрлық объектінің жай-күйінің сәйкестендірілген туындауы;

9) КҚ оқыс оқиғасы – цифрлық объектінің КҚ теріс әсер ететін оқиға немесе оқиғалар жиынтығы;

10) мемлекеттік техникалық қызмет (бұдан әрі – "МТҚ" АҚ) – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған мемлекеттік заңды тұлға;

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

12) осалдық – цифрлық объектінің КҚ қатер төндіретін кемшілігі;

13) цифрлық объект – цифрлық технологиялар арқылы құрылған, пайдаланылатын немесе берілетін, бірегей цифрлық сипаттамаларға ие және цифрлық орта субъектілеріне Қазақстан Республикасының заңнамасында белгіленген көлемде иелену,

пайдалану не билік ету құқықтарын жүзеге асыруға мүмкіндік беретін цифрлық ортаның ерекшеленген элементі;

14) цифрлық объектілерінің иегері – цифрлық объектілерінің меншік иесі заңда немесе келісімде айқындалған шектерде және тәртіппен цифрлық объектілерін иелену және пайдалану құқықтарын берген субъект;

15) цифрлық оқиғаларды журналға енгізу – кейіннен талдау, ауытқуларды анықтау және ҚҚ оқыс оқиғаларын зерттеу мақсатында цифрлық объектілерде болып жатқан оқиғалар туралы цифрлық жазбаларды жүйелі түрде жазу, жинау және сақтау процесі;

16) Мемлекеттің цифрлық объектілерінің архитектуралық порталы – цифрландыру саласындағы мониторинг, талдау және жоспарлау үшін мемлекеттік органдардың одан әрі пайдалануы мақсатында мемлекеттің цифрлық объектілері, мемлекеттің цифрлық архитектурасы, платформалық бағдарламалық өнімдер туралы мәліметтерді есепке алуды, сақтауды және жүйелеуді жүзеге асыруға арналған цифрлық объект;

17) "Цифрлық үкіметтің" цифрлық объектілері (бұдан әрі – ЦҮ ЦО) – мемлекеттік органдардың және өзге де адамдардың мемлекеттік органдардың қызметін жүзеге асыруға, мемлекеттік функцияларды орындауға және мемлекеттік қызметтер көрсетуге арналған цифрлық объектілері жатады;

18) "Цифрлық үкіметтің" цифрлық объектілерінің Киберқауіпсіздігін қамтамасыз ету мониторингі (бұдан әрі – КҚҚМ) – ҚҚ қауіп-қатерлері мен оқыс оқиғаларын анықтау арқылы ЦҮ ЦО ҚҚ қамтамасыз ету бойынша техникалық және ұйымдастыру іс-шараларын ЦҮ ЦО иелері және (немесе) меншік иелерімен іске асырудың толықтығы мен сапасын қадағалау.

3. КҚҚМ-ны Киберқауіпсіздіктің ұлттық үйлестіру орталығының (бұдан әрі – КҰҮО) міндеттері мен функцияларын іске асыратын "МТҚ" АҚ Заңның 14-бабының 1-тармағының 5) тармақшасына сәйкес, КҰҮО КҚҚМ жүйесі арқылы жүргізеді және мынадай жұмыс түрлерін қамтиды:

ҚҚ оқыс оқиғаларына ден қою мониторингі;

қорғауды қамтамасыз ету мониторингі;

қауіпсіз жұмыс істеуін қамтамасыз ету мониторингі.

4. КҚҚМ объектілері: Мемлекеттік құпияларды құрайтын мәліметтерді қамтитын цифрлық ресурстарды; мемлекеттік құпияларға жатқызылған, қорғалған орындаудағы цифрлық жүйелерді; Қазақстан Республикасы Ұлттық Банкінің ЦҮ ЦО-мен интеграцияланбайтын цифрлық объектілерді қоспағанда өнеркәсіптік пайдалануға енгізілген ЦҮ ЦО, оның ішінде АМЦО-ға жатқызылған ЦҮ ЦО болып табылады.

5. КҚҚМ мынадай нұсқалардың бірі бойынша жүргізіледі:

1) бір жұмыс түрі бойынша;

2) бірнеше жұмыс түрлері бойынша;

3) жұмыс түрлерінің толық құрамында.

6. АМЦО-ға жатқызылған КҚҚМ-ы Қазақстан Республикасының Ұлттық қауіпсіздік комитеті (бұдан әрі – ҚР ҰҚК) мен "МТҚ" АҚ арасында жасалған шарт негізінде жүзеге асырылады.

2-тарау. "Цифрлық үкімет" цифрлық объектілерінің киберқауіпсіздікті қамтамасыз ету мониторингін жүргізу тәртібі

7. "МТҚ" АҚ КҚҚМ жүргізу үшін бастапқы ақпарат ретінде "цифрлық үкімет" архитектуралық порталынан КҚҚМ объектісі туралы мәліметтерді, сондай-ақ сервистік бағдарламалық өнімнің, "цифрлық үкіметтің" цифрлық платформасының, мемлекеттік органның интернет-ресурсының және цифрлық жүйенің КҚ 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 сомалары;

4) деректер базаларының құрылымдары бар.

8. КҚҚМ объектісінің меншік иесі немесе иеленушісі КҚҚМ объектісінің өнеркәсіптік пайдалануға енгізу немесе пайдалануды тоқтату 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 ЦҮ ЦО туралы мәліметтерді қағаз және электрондық түрде ұсынады (бұдан әрі – Мәліметтер).

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

10. "МТҚ" АҚ КҚҚМ жүргізу кезінде:

1) КҚ оқыс оқиғаларына ден қою мониторингі шеңберінде:

КҰҮО-ның КҚ оқиғаларын басқару жүйесіне жіберілуі қажет оқиғаларды тіркеу журналдарының тізбесін анықтау үшін КҚҚМ объектісін талдау;

КҚ оқиғаларын басқару жүйесінің агенттерін КҚҚМ объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне және қажет болған жағдайда, КҚҚМ объектісінің меншік иесінің немесе иеленушісінің цифрлық инфрақұрылымының өзге объектілеріне орнату;

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

КҚҚМ объектісінде анықталған КҚ оқиғаларын немесе КҚ оқыс оқиғаларын бастапқы талдау;

КҚ оқиғасы немесе КҚ оқыс оқиғасы анықталған сәттен бастап 30 минут ішінде КҚҚМ объектісінің КҚ-сын қамтамасыз етуге жауапты тұлғалардың хабарламаларын

қарайды, осы Қағидаларға 2-қосымшаға сәйкес анықталған КҚ оқиғасы немесе КҚ оқыс оқиғасы туралы деректер тізбесін ұсыну;

КҚ оқыс оқиғасының таралуын тоқтата тұру бойынша КҚҚМ объектісінің меншік иесіне мен иеленушісіне бастапқы ұсынымдар беру;

КҚ оқыс оқиғасына ден қою шеңберінде "МТҚ" АҚ қызметкерін КҚҚМ объектісі орналасқан жерге жіберу (ҚР ҰҚК және "МТҚ" АҚ келісімі бойынша);

КҚҚМ объектісінің меншік иесі немесе иеленушісі не ол уәкілетті тұлға КҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде КҚ оқыс оқиғасының себептері мен салдарын жоймаған жағдайда ҚР ҰҚК-ні хабардар ету;

2) қорғауды қамтамасыз ету мониторингі шеңберінде:

КҚҚМ бойынша жұмыстарды жүргізу кестесіне сәйкес КҚҚМ объектілерін осалдықтардың болуына зерттеп-қарау (бұдан әрі – осалдықтарға зерттеп-қарау):

енуге қолмен тестілеу жүргізу кезінде КҚҚМ объектісі орналастырылған жергілікті есептеу желісімен түйіскен жергілікті есептеу желісін (бар болған жағдайда) зерттеп-қарау;

осалдықтарға зерттеп-қарау жөніндегі жұмыстар аяқталғаннан кейін 10 жұмыс күні ішінде КҚҚМ объектілерінің меншік иелеріне немесе иеленушілеріне КҚҚМ объектілерін осалдықтарға зерттеп-қарау нәтижелерін және осалдықтарды жою бойынша ұсынымдарды ұсыну;

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

3) қауіпсіз жұмыс істеуді қамтамасыз ету мониторингі шеңберінде:

КҚҚМ бойынша жұмыстар жүргізу кестесіне сәйкес осы Қағидаларға 3-қосымшада келтірілген КҚ бойынша НТҚ ережелерінің орындалуы тұрғысынан(бұдан әрі – КҚ жөніндегі ТҚ) талаптарының орындалуына КҚҚМ объектісін зерттеп-қарау;

КҚҚМ объектісін зерттеп-қарау аяқталған күннен бастап "қ жұмыс күні ішінде КҚҚМ объектілерінің меншік иелеріне немесе иеленушілеріне КҚ бойынша НТҚ ережелерінің орындалуы және анықталған бұзушылықтарды жою бойынша КҚҚМ объектісін зерттеп-қарау нәтижелерін ұсынуды жүзеге асырады.

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

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

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

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

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

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

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

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

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

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

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

ККҚМ объектісінде КҚ оқыс оқиғасы өз бетінше анықталған кезде, КҚ оқыс оқиғасы расталған сәттен бастап 15 минут ішінде "МТҚ" АҚ-ны хабардар етеді және КҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде осы Қағидаларға 5-қосымшаға сәйкес КҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы деректерді "МТҚ" АҚ-ға;

"МТҚ" АҚ КҚ оқиғасы немесе КҚ оқыс оқиғасы туралы хабардар еткен кезде, хабардар етілген сәттен бастап 72 сағат ішінде "МТҚ" АҚ-ға:

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

КҚ оқыс оқиғасы расталған кезде - КҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы деректерді осы Қағидаларға 5-қосымшаға сәйкес жолдайды.

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

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

ККҚМ объектісінде осалдықды өз бетінше анықтаған жағдайда, осалдық анықталған сәттен бастап 24 сағат ішінде ЦҮ ЦО осалдығы туралы деректер тізбесін осы Қағидаларға 6-қосымша нысаны бойынша "МТҚ" АҚ-ға жолдайды;

ККҚМ объектісінің осалдығын жоймаған кезде осалдыққа санаттардың бірін (өндірістік қажеттілік, нөлдік күннің осалдығы, жалған іске қосу) бере алады және осы Қағидаларға 7-қосымшаға сәйкес осалдықтарды жоймау себептерінің санаттарын және жоймау себептерінің негіздемесін "МТҚ" АҚ-ға ұсынады.

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

ҚҚ бойынша НТҚ ережелерінің орындалуы тұрғысының ККҚМ объектісін зерттеп-қарау бойынша жұмыстар жүргізу туралы хабарламаны алған күннен бастап 10 жұмыс күні ішінде "МТҚ" АҚ-ға ККҚМ объектісінің меншік иесі немесе иеленушісі бекіткен , оның қолымен және мөрімен (бар болған жағдайда) куәландырылған ҚҚ бойынша НТҚ көшірмелерін ұсынады;

ККҚМ объектісін ҚҚ жөніндегі НТҚ ережелерінің орындалуына зерттеп-қарау нәтижелерін алған күннен бастап бір ай ішінде "МТҚ" АҚ-ға ҚҚ жөніндегі НТҚ ережелерінің анықталған бұзушылықтары бойынша қабылданған шаралар туралы ақпаратты ұсынады.

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

16. ККҚМ объектісінің АҚ-ны қамтамасыз етуге жауапты тұлғасының байланыс деректері өзгерген жағдайда, ККҚМ 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 ҚҚ оқиғалары, ҚҚ оқыс оқиғалары, ЦҮ ЦО-ның осалдықтары, ЦҮ ЦО өзгерістері және ҚҚ жөніндегі ТҚ талаптарының анықталған бұзушылықтары бойынша жиынтық ақпаратты, сондай-ақ ККҚМ меншік иелері мен иеленушілері қабылдаған шаралар туралы деректерді жолдайды.

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

3-тарау. Аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуге мониторинг жүргізу тәртібі

19. ЦҮ ЦО-ға жатпайтын АМЦО-ның КҚ қамтамасыз ету мониторингі АМЦО иесінің КҚ бойынша өз бөлімшесімен немесе Қазақстан Республикасы Азаматтық кодексінің 683-бабына сәйкес үшінші тұлғалардың қызметтерін сатып алу жолымен жүзеге асырылады.

20. АМЦО меншік иесі және (немесе) иеленушісі Қазақстан Республикасы Үкіметінің 2025 жылғы 9 қазандағы № 846 қаулысымен бекітілген Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі туралы ереженің 15-тармағының 385) тармақшасына сәйкес бекітілетін АМЦО тізбесіне енгізілген күннен бастап тоқсан күнтізбелік күн ішінде АМЦО КҚ-сын қамтамасыз ету монитронгі жүйесін (бұдан әрі – КҚ МҚЖ) КҚЖО техникалық құралдарына қосуды қамтамасыз етеді, сондай-ақ АМЦО КҚ бойынша жауапты тұлғасын айқындайды.

21. АМЦО КҚ МҚЖ КҚЖО техникалық құралдарына қосылғаннан кейін, АМЦО КҚ МҚЖ КҚ оқыс оқиғасын анықтаған кезде, КҚЖО КҚ оқыс оқиғасы расталған сәттен бастап 15 минут ішінде жазбаша (электрондық) хабарлама арқылы "МТҚ" АҚ-ны және АМЦО меншік иесін және (немесе) иеленушісін хабардар етеді, АМЦО КҚ бойынша жауапты тұлғасын жазбаша (электрондық) хабарлама арқылы құлақтандырады. КҚЖО КҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде КҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы деректерді "МТҚ" АҚ-ға жолдайды.

22. АМЦО КҚ бойынша бөлімшесі КҚ оқыс оқиғасын өз бетінше анықтаған кезде, АМЦО КҚ бойынша жауапты тұлғасы КҚ оқыс оқиғасы расталған сәттен бастап 15 минут ішінде "МТҚ" АҚ-ны және КҚЖО-ны хабардар етеді. КҚЖО КҚ оқыс оқиғасы расталған сәттен бастап 72 сағат ішінде КҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы деректерді "МТҚ" АҚ-ға жолдайды. КҚЖО қызметтерін көрсететін тұлға болмаған кезде КҚ оқыс оқиғасын жою бойынша қабылданған шаралар туралы ақпаратты "МТҚ" АҚ-ға АМЦО КҚ бойынша бөлімшесі жолдайды.

"Цифрлық үкіметтің"
Цифрлық объектілерінің
және аса маңызды
цифрлық объектілерінің
киберқауіпсіздігін қамтамасыз
ету мониторингін
жүргізу қағидаларына
1-қосымша
Нысан

"Цифрлық үкіметтің" цифрлық объектісі туралы мәліметтер

1. ЦҮ ЦО ресми атауы.
2. ЦҮ ЦО меншік иесі.

3. ЦҮ ЦО иеленушісі (бар болған жағдайда).

4. ЦҮ ЦО нақты орналасқан жері (көше, қала, облыс).

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

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

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

8. ЦҮ ЦО-ның Интернетке қосылуының болуы және байланыс арнасының өткізу қабілеті туралы ақпарат.

9. ЦҮ ЦО меншік иесі немесе иеленушісі бекіткен және оның қолымен және мөрімен (бар болған жағдайда) куәландырылған ЦҮ ЦО-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. КЖО немесе ЦҮ ЦО-ның КҚ қамтамасыз етуге жауапты тұлғаның байланыс деректері.

12. ЦҮ ЦО 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, ЦҮ ЦО-ға жататын резервтік техникалық және бағдарламалық құралдар мен ақпаратты қорғау құралдары туралы мәліметтер.

"Цифрлық үкіметтің" цифрлық
объектілерінің және аса
маңызды цифрлық
объектілерінің
киберқауіпсіздігін қамтамасыз
ету мониторингін жүргізу
қағидаларына
2-қосымша
Нысан

Анықталған киберқауіпсіздік оқиғасы немесе киберқауіпсіздік оқыс оқиғасы туралы деректер тізбесі

КҚ оқиғасы/КҚ оқыс оқиғасы тіркелген күні	
Егжей-тегжейлер	Анықтау күні мен уақыты; Дереккөздің IP-мекенжайы; Тағайындалған IP-мекенжайы (оқиғаларды тіркеу журналдарында ақпарат болған жағдайда); Құрылғының атауы/Компьютердің аты; КҚ оқиғасының/КҚ оқыс оқиғасының атауы; Файл жолы/Сұрау салу (ОТЖ-да ақпарат болған жағдайда);

	Серверден жауап коды (ОТЖ-да ақпарат болған жағдайда); Ақпаратты қорғау құралындағы іске қосылулар саны (ОТЖ-да ақпарат болған жағдайда); Дереккөз-ұйым (ОТЖ-да ақпарат болған жағдайда); Алғашқы тіркеу/қайта тіркеу;
КҚ оқиғасының/КҚ оқыс оқиғасының түрі	ОТЖ-да қосымша ақпарат болған жағдайда
ЦҮ ЦО меншік иесі немесе иеленушісі	
КҚ оқиғасы/КҚ оқыс оқиғасы анықталған объект	
Ескертпе	

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды цифрлық
объектілерінің
киберқауіпсіздігін
қамтамасыз ету
мониторингін жүргізу
қағидаларына
3-қосымша
Нысан

Киберқауіпсіздік бойынша нормативтік-техникалық құжаттама

1. Бірінші деңгейлі құжаттар:

1) КҚ саясаты.

2. Екінші деңгейлі құжаттар:

1) КҚ тәуекелдерін бағалау әдістемесі;

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

3) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету қағидалары;

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

5) ішкі КҚ аудитін жүргізу қағидалары;

6) ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;

7) цифрлық 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 жеткізгіштепрді пайдалану қағидалары;

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

3. Үшінші деңгейлі құжаттар:

1) КҚ қауіптерінің (тәуекелдерінің) каталогы;

2) КҚ 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 цифрлық объектісін сүйемелдеу жөніндегі басшылығы;

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

4. Төртінші деңгейлі құжаттар:

1) КҚ 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, цифрлық 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.

"Цифрлық үкіметтің"
цифрлық объектілерінің және
аса маңызды цифрлық
объектілерінің ақпараттық
қауіпсіздігін қамтамасыз ету
мониторингін жүргізу
қағидаларына
4-қосымша
Нысан

"Цифрлық үкімет" цифрлық объектілерінің оқиғаларды тіркеу журналдары жазбаларының үлгілері мен түрлері

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

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

1) жүйені іске қосу/тоқтату;

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

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

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

5) жүйелік конфигурациясының өзгеруі;

6) есептік жазбаларды құру, жою және түрлендіру;

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

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

9) артықшылықты есептік жазбаларды пайдалану;

10) кіріс/шығыс құрылғысын қосу/ажырату;

11) қолданушының сәтсіз немесе қабылданбаған әрекеттері;

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

13) ОЖ-да процестерді іске қосу, тоқтату.

2. ОЖ оқиғаларын тіркеу журналы мынадай өрістерді қамтиды:

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

2) хост атауы;

3) оқиғаның сипаттамасы.

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

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

2) жүйеде жаңа порттар ашу;

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

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

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

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

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

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

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

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

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

8) қызмет таймаутына қол жеткізілді – Windows EID 7009;

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

10) тізілімнің мәні өзгерген – Windows EID 4657;

11) WMI аттар кеңістігіндегі жазба – Windows EID 4662.

5. Оқиғаларды тіркеу журналындағы жазбалар мәтіндік үлгіде сақталады.

6. Оқиғаларды тіркеу журналдары өрістерінің мәндері ажыратқыш символдармен бөлінеді, егер өріс ұзын форматта болып, оның мазмұнында ажыратқыш символ болса, өрістерді шектеуші символдар қолданылады .

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. Журналға енгізуге 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 мәндері ажыратқыш символдармен бөлінеді, егер өріс ұзын форматта болып, оның мазмұнында ажыратқыш символ болса, өрістерді шектеуші символдар қолданылады .

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 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 үлгіде сақталады.

19. Оқиғаларды тіркеу журналдары өрістерінің мәндері ажыратқыш символдармен бөлінеді, егер өріс ұзын форматта болып, оның мазмұнында ажыратқыш символ болса, өрістерді шектеуші символдар қолданылады .

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. Журналға енгізуге 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 мәндері ажыратқыш символдармен бөлінеді, егер өріс ұзын форматта болып, оның мазмұнында ажыратқыш символ болса, өрістерді шектеуші символдар қолданылады .

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. Журналға енгізуге 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 мәндері ажыратқыш символдармен бөлінеді, егер өріс ұзын форматта болып, оның мазмұнында ажыратқыш символ болса, өрістерді шектеуші символдар қолданылады .

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

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

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды
цифрлық объектілерінің
киберқауіпсіздігін қамтамасыз
ету мониторингін
жүргізу қағидаларына
5-қосымша
Нысан

Киберқауіпсіздік оқыс оқиғасы туралы деректер тізбесі

КҚ оқыс оқиғасы тіркелген күні	
КҚ оқыс оқиғасының маңыздылық деңгейі	Жоғары(4); Орташа(3); Төмен(2); Анықталмаған(1).
КҚ оқыс оқиғасының түрі	Қызмет көрсетуден бас тарту(DoS, DDoS) Рұқсатсыз қол жеткізу және мазмұнды өзгерту; Ботнет; Вирустық шабуыл; Шифрлаушы; Осалдықты пайдалану; Аутентификация/авторизация құралдарының компрометациясы; Фишинг; Спам; Басқа.
Ауқымдылығы	Жеке; Жаппай.
Егжей-тегжейлер	Туындау күні мен уақыты; Растау күні мен уақыты; Қайталанған жаңа; Компрометация индикаторы(IOC).
Белгісі	Расталған; Әрекеттену; Күдік.
Контур	Ішкі контурдың жергілікті желісі; Сыртқы контурдың жергілікті желісі.
КҚ оқыс оқиғасының сипаттамасы	
Салдары	Салдарсыз; Жұмысқа қабілеттілігінің бұзылуы; Тұтастығының бұзылуы; Ақпараттың құпиялық режимінің бұзылуы.
Зиян келтірілген объект	

КҚ оқыс оқиғасын жою үшін қабылданған әрекеттер	
Ескертпе	

Киберқауіпсіздік оқыс оқиғасының маңыздылық деңгейлері

Маңыздылық деңгейі	Белгілері	КҚ оқыс оқиғаларының мысалдары
Жоғары (4)	Қызметтер көрсету/жұмыстарды орындау мүмкін болмауына және (немесе) маңызды* деректердің жоғалуына/ өзгертілуіне және (немесе) маңызды деректерді өңдейтін объект құпиялығының бұзылуына алып келетін КҚ оқыс оқиғалары.	- Рұқсатсыз қол жеткізу - Осалдықты пайдалану - Шифрлаушы - Зиянды БҚ - Қызмет көрсетуден бас тарту (DoS /DDoS-шабуыл) және тағы басқа.
Орташа (3)	Қызметтер көрсетуді/жұмыстарды орындауды елеулі шектеуге және (немесе) маңызды болып табылмайтын деректердің жоғалуына/ өзгертілуіне және (немесе) маңызды болып табылмайтын деректерді өңдейтін цифрлық объект құпиялығының бұзылуына алып келетін КҚ оқыс оқиғалары*.	- Рұқсатсыз қол жеткізу - Шифрлаушы - Зиянды БҚ - Қызмет көрсетуден бас тарту (DoS /DDoS-шабуыл) - Осалдықты пайдалану және тағы басқа.
Төмен (2)	Қызмет көрсетуге/жұмыстарды орындауға әсер етпейтін КҚ оқыс оқиғалары.	- Зиянды БҚ - Қызмет көрсетуден бас тарту (DoS/DDoS-шабуыл) - Осалдықты пайдалану - Спам - Фишингтік шабуыл және тағы басқа
Анықталмаған (1)**	КҚ оқыс оқиғасының көрсетуге әсері анықталмаған	Сипатқа тән емес/күдікті белсенділік

Ескертпе:

* Маңызды деректерге Қазақстан Республикасының заңнамасымен қорғалатын және/немесе цифрлық объектінің иеленушісі/меншік иесі маңыздыларға жатқызған деректер жатады. **КҚ оқыс оқиғасы расталған сәттен бастап нү сағат ішінде деңгейді қайта қарау қажет.

"Цифрлық үкіметтің"
цифрлық объектілерінің
және аса маңызды цифрлық
объектілерінің
киберқауіпсіздігін
қамтамасыз ету
мониторингін жүргізу
қағидаларына
6-қосымша
Нысан

"Цифрлық үкіметтің" цифрлық объектілерінің осалдығы туралы деректер тізбесі

Осалдық анықталған күн/уақыт	Контур	Цифрлық объект атауы	Компоненті (атауы, IP, hostname және т.б)	Порт	Осалдық сипаттамасы	Қосымша ақпарат
1	2	3	4	5	6	7
	Сыртқы/ішкі контур					

"Цифрлық үкіметтің" цифрлық объектілерінің және аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларына 7-қосымша Нысан

Осалдықтарды жоймау себептерінің санаттары және жоймау себептерінің негіздемесі

Осалдықтарды жоймау себептерінің санаттары	Осалдықты жоймау себептерін негіздемесі
Өндірістік қажеттілік	Осалдықтың және ЦҮ ЦО жай-күйінің сипаттамасы; осалдықты жою бойынша қабылданған шаралар; цифрлық объектісіндегі қажетті өзгерістердің себептері мен сипаты; осалдық бірінші рет анықталған сәттен бастап алты айдан аспайтын осалдықты жою мерзімдері.
Нөлдік күн осалдығы	ЦҮ ЦО осалдығы мен жай-күйінің сипаттамасы; сондай-ақ осалдықты пайдалану ықтималдылығын төмендету бойынша жүргізілген іс-шаралар;
Жалған іске қосылу	Осалдық ретінде айқындалған ЦҮ ЦО сипаттамасының немесе жай-күйінің сипаттамасы.