# АҚПАРАТТЫҚ ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІНЕ ЖӘНЕ ШТАТТАН ТЫС (ДАҒДАРЫСТЫҚ) ЖАҒДАЙЛАРҒА ДЕН ҚОЮ БОЙЫНША ПАЙДАЛАНУШЫЛАРДЫҢ ІС-ҚИМЫЛ ТӘРТІБІ ТУРАЛЫ НҰСҚАУЛЫҚ

**Астана**
**2023 жыл**

## Терминдер мен қысқартулар

**Ұйым**– «Qazaq Green» ЖЭК қауымдастығы ЗТБ;

**Нұсқаулық** – пайдаланушылардың ақпараттық қауіпсіздік инциденттеріне және ұйымның штаттан тыс (дағдарыстық) жағдайларына ден қою жөніндегі іс-қимыл тәртібі туралы нұсқаулық.

**Құпия сөздің бұзылуы** – құпия сөздің таралуы немесе жария етілуі.

**Ақпаратқа рұқсатсыз қол жеткізу** (бұдан әрі – РҚЖ) – есептеу техникасы құралдарымен немесе автоматтандырылған жүйелермен берілетін штаттық құралдарды пайдалана отырып, қол жеткізуді шектеу қағидаларын бұзатын ақпаратқа қол жеткізу.

**Бірінші басшы** – директор немесе оның міндетін атқарушы тұлға;

**П ровайдер –** мамандандырылған ақпараттық жүйелердің жабдықтарын орналастыру, интернет желісіне қосу және жүйелерді сүйемелдеуге байланысты өзге де қызметтер көрсететін заңды тұлға (тұлғалар).

**Ақпараттық қауіпсіздік (бұдан әрі – АҚ) жөніндегі маман** – ұйымның АТ-инфрақұрылымын қолдауды және дамытуды қамтамасыз ететін ұйым қызметкері.

**Қатер** – бұл жүйеге немесе ұйымға зиян келтіруі мүмкін жағымсыз инциденттің ықтимал себебі.

**БҚ** – бағдарламалық қамтамасыз ету.

**ЛЕЖ** – ұйымның жергілікті есептеу желісі.

**Жүйелік әкімші** (бұдан әрі – ЖӘ) – ұйымның жүйелік әкімшісінің лауазымдық нұсқаулықтарына сәйкес корпоративтік ақпараттық желінің серверлері мен қолданбалы белсенді жабдықтарын әкімшілендіру функцияларын орындайтын қызметкер.

## 1. Жалпы ережелер

1. Осы нұсқаулық ұйымда штаттан тыс (дағдарыстық) жағдайлар туындаған кезде корпоративтік есептеу желісін пайдаланушылардың, жүйелік әкімшінің, ақпараттық қауіпсіздік жөніндегі маманның және кеңсені пайдаланудың әкімшілік-шаруашылық қызметтерінің іс-қимыл тәртібін айқындайды.

2. Бұл нұсқаулықта штаттан тыс жағдай ретінде мыналар қарастырылады:

1) сервермен ұзақ уақыт байланыстың болмауы;

2) ақпаратты одан әрі өңдеу мүмкін еместігіне әкелетін бағдарламалық қамтамасыз етудің істен шығуы;

3) құпия сөзді бұзу;

4) сервердің немесе желілік жабдықтың істен шығуы;

5) серверде немесе дербес компьютерде ақпараттың жоғалуы немесе таралуы;

6) тіркеу құралдарымен тіркелген РҚЖ әрекеті;

7) АЖ-ға РҚЖ немесе БҚ-да зиянды кодты анықтау;

8) байланыс арналарының істен шығуы;

9) АЖ жұмыс қабілеттілігінің толық немесе ішінара жоғалуына, ұйымның есептеу техникасы құралдарымен ақпаратты өңдеу мүмкін еместігіне әкеп соққан электр энергиясын берудің бұзылуы;

10) табиғи-климаттық әсерлер (жер сілкінісі, су тасқыны, дауыл, өрт және т.б.);

11) АЖ жұмыс қабілеттілігінің ішінара жоғалуына (жүйенің жекелеген компоненттерінің істен шығуына, өнімділіктің жоғалуына, бағдарламалар мен ақпараттың тұтастығы мен құпиялылығының бұзылуына) немесе АЖ толық істен шығуына (бұдан әрі өз функцияларын орындай алмауына, ақпаратты жоюға, бұғаттауға, заңсыз өзгертуге немесе компаға келуге) әкеп соғатын ақпараттық ресурстарға өзге де әсер ету.

3. Штаттан тыс жағдайдың пайда болуы туралы ақпарат көздері:

1) АЖ аппараттық-бағдарламалық кешендерінің жұмысында штаттан тыс жағдай анықталған кезде пайдаланушыларды ақпараттық технологиялар бөлімінің қызметкеріне хабарлау;

2) жүйенің жұмысында немесе конфигурациясында күдікті өзгерістерді анықтаған АЖ-ны пайдалануды жүзеге асыратын қызметкерлерді жүйелік әкімшіге және ақпараттық қауіпсіздік жөніндегі маманға хабарлау;

3) корпоративтік ақпараттық желінің, серверлердің, пайдаланушы жұмыс станцияларының, БҚ және т.б. жай-күйіне мониторинг жүргізу жүйелері;

4) штаттан тыс жағдайдың туындағанын немесе туындау мүмкіндігін куәландыратын жазбалары бар жүйелік журналдар.

## 2. Штаттан тыс жағдай туындаған кездегі әрекеттердің жалпы тәртібі

4. Пайдаланушы нұсқаулықтың 2-тармағының 2, 3,5,6, 7, 10, 11-тармақшаларында санамаланған штаттан тыс жағдай туындаған жағдайда:

1) жұмысын уақытша тоқтатады;

2) ақпараттық технологиялар бөлімінің қызметкерін дереу хабардар етеді;

3) басшылықты хабардар етеді;

4) нұсқаулықтың 2-тармағының 2, 9-тармақшаларында санамаланған штаттан тыс жағдайлар бойынша ақпараттық технологиялар бөлімі қызметкерінің рұқсатынан кейін және нұсқаулықтың 2-тармағының 3,5,6,7,10, 11-тармақшалары бойынша ақпараттық қауіпсіздік жөніндегі маманның рұқсатынан кейін ғана жұмысты қайта бастайды.

5. Жүйелік әкімші жағдайға алдын ала талдау жүргізеді, егер мүмкін болса, жедел түрде жояды және басшыны хабардар етеді және штаттан тыс жағдайларды тіркеу журналында штаттан тыс жағдайдың туындау фактісін тіркейді (оның нысаны осы нұсқаулықтың **1-қосымшасында** келтірілген).

6. Ұйымның бизнес-процестерін жүзеге асыруға елеулі ықпал ете алатын штаттан тыс жағдай туындаған жағдайда ақпараттық технологиялар бөлімінің қызметкері:

1) штаттан тыс жағдайлардың туындағаны туралы бірінші басшыға, ал 3,5, 6,7,10,11-тармақшаларда аталған штаттан тыс жағдайлар бойынша – ақпараттық қауіпсіздік жөніндегі маманға хабарлайды;

2) штаттан тыс жағдайдың ауқымын, ықтимал зақымдану көлемін және аймағын анықтайды;

3) зардап шеккен компоненттерді өшіреді немесе резервтік ресурстарды пайдалануға ауысады;

4) зақымдалған маңызды аппараттық құралдар мен басқа да жабдықтардың жұмысқа қабілеттілігін қалпына келтіреді, қажет болған жағдайда істен шыққан тораптар мен блоктарды резервтік қондырғылармен ауыстырады;

5) эталондық көшірмелерді қолдана отырып, бүлінген бағдарламалық қамтамасыз етуді қалпына келтіреді;

6) резервтік көшірмелерді пайдаланып қажетті ақпаратты қалпына келтіреді;

7) қалпына келтірілген жүйенің жұмыс қабілеттілігін тексереді, штаттан тыс жағдайдың салдары жүйенің одан әрі жұмысына әсер етпейтіндігіне көз жеткізеді;

8) штаттан тыс жағдайды жою туралы бірінші басшыны хабардар етеді;

9) штаттан тыс жағдайды штаттан тыс жағдайларды тіркеу журналына тіркейді.

10) жүйелік әкімшіге штаттан тыс жағдай туралы есеп береді.

7. Бағдарламалық қамтамасыз етуді орнату және баптау немесе желілік жабдықты ауыстыру үшін есептеу құралдарына функционалдық міндеттерге

сәйкес ақпараттық технологиялар бөлімінің қызметкері ғана қол жеткізе алады.

8. Штаттан тыс жағдайды жойған ақпараттық технологиялар бөлімінің қызметкері жағдайды сипаттайтын акт жасайды.

9. Әрбір штаттан тыс жағдайды ақпараттық қауіпсіздік жөніндегі маман талдайды. Осы талдау нәтижелері бойынша басшылыққа болашақта штаттан тыс жағдайлардың алдын алуға бағытталған ықтимал ұйымдастырушылық және техникалық іс-шаралар бойынша ұсыныстар әзірленеді және ұсынылады.

10.Қажет болған жағдайда ұйымның бірінші басшысының шешімі бойынша оның себептерін анықтау, келтірілген залалды бағалау, кінәлі адамдарды анықтау және тиісті ықпал ету шараларын қабылдау мақсатында штаттан тыс жағдайдың туындау фактісі бойынша қызметтік тергеп-тексеру жүргізілуі мүмкін.

## 3. Штаттан тыс (дағдарыстық) жағдайлардың туындауын және олар бойынша түзету іс-қимылдарын бақылау

11.Лауазымды адамдарды хабардар ету тәртібі және штаттан тыс жағдайларда іс-шараларды орындау мерзімдері ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету және жұмысқа қабілеттілігін қалпына келтіру жөніндегі іс-шаралар жоспарында айқындалған.

12.Алдын алу шараларын орындау үшін штаттан тыс немесе дағдарыстық жағдайлардың туындауын болдырмау мақсатында мынадай іс-шаралар жүргізілуі тиіс:

1) Жүйелік әкімші мамандандырылған бағдарламалық қамтамасыз етудің көмегімен АҚБЖ, ОЖ және ҚБҚ жай-күйін сұрауды қамтитын ұйымның ақпараттық жүйелеріне күн сайын мониторинг жүргізуі тиіс, ақпараттық жүйелердің қолжетімділік жай-күйі өзгерген жағдайда «онлайн» режимінде әкімшіні хабардар етеді;

2) Жүйелік әкімші күн сайын АҚ бұзылуына байланысты оқиғаларға мониторинг жүргізіп, мониторинг нәтижелеріне талдау жүргізуі тиіс;

3) Жүйелік әкімші ақпараттың резервтік көшірмесін жасау және қалпына келтіру регламентіне сәйкес ақпараттың резервтік көшірмесін жасауы керек;

4) Алдағы мүмкін болатын штаттан тыс жағдайлар туралы ақпарат алған жағдайда барлық қатысушы тұлғалар мен құрылымдарды жедел хабардар ету қамтамасыз етілуі тиіс.

5) Жүйелік әкімші ақпараттық қауіпсіздік саласындағы кез келген оқиғалар туралы ақпараттық қауіпсіздік жөніндегі маманға мүмкіндігінше тез хабарлауға және 1-қосымшада көрсетілген «Штаттан тыс жағдайларды есепке алу журналы» құжатында штаттан тыс жағдайлардың туындауының тиісті жазбасын жүргізуге міндетті;

6) әрбір штаттан тыс жағдайды ақпараттық қауіпсіздік маманы жүйелік әкімшімен бірлесіп талдауы керек.

13.Штаттан тыс немесе дағдарыстық жағдайлардың туындауын болдырмау үшін профилактикалық іс-қимылдардың орындалуын бақылауды жүзеге асыру жүйелік әкімшіге жүктеледі.

14. АҚБЖ басшылығының өкілі штаттан тыс (дағдарыстық) жағдайлар мен ақпараттық қауіпсіздік инциденттері туындаған жағдайда ұйым қызметкерлерін хабардар етуге жауапты тұлға болып табылады.

15.Штаттан тыс жағдайларда әрекет ету жөніндегі іс-шараларды тиімді іске асыру үшін әр түрлі штаттан тыс жағдайлар бойынша тұрақты жаттығулар өткізілуі тиіс. Жаттығу нәтижелері бойынша қажет болған жағдайда осы нұсқаулықты нақтылау жүргізіледі.

16.Егер ақпараттық қауіпсіздік инциденті ҚР СТ ИСО МЭК 27002-2009 стандартының 13.2.3-бөліміне сәйкес сот талқылауына әкелуі мүмкін болса, ақпараттық қауіпсіздік инциденттері туралы ақпаратты жинау, сақтау және ұсыну.

17.Ақпараттық қауіпсіздік жағдайына байланысты оқиғаларды тіркеу және Қазақстан Республикасының бірыңғай талаптарына сәйкес оқиғалар журналдарын талдау арқылы бұзушылықтарды анықтау.

## 4. Ең көп таралған штаттан тыс жағдайлар туындаған кездегі іс-әрекеттің ерекшеліктері

18. Провайдерде орналасқан бір немесе бірнеше серверлермен байланыс болмаған кезде жүйелік әкімші байланыстың болмау себептерін дереу анықтайды және қажет болған жағдайда осы нұсқаулыққа сәйкес іс-шаралар жүргізіледі.

19.Бағдарламалық қамтамасыз ету істен шыққан кезде ақпараттық технологиялар бөлімінің қызметкері ақаулықтың себебін анықтайды. Егер қатені өз бетімен, соның ішінде бағдарламалық қамтамасыз етуді әзірлеушімен кеңескеннен кейін түзету мүмкін болмаса, ақпараттық технологиялар қызметкері актінің және ілеспе материалдардың (сондай-ақ қажет болған жағдайда файлдардың) көшірмесін бағдарламалық қамтамасыз етуді әзірлеушіге жібереді.

20. Құпия сөз бұзылған кезде ұйымның аутентификация рәсімін ұйымдастыру қағидаларын сақтау қажет.

21. Компьютерлік вирус анықталған кезде ұйымның вирусқа қарсы бақылауын ұйымдастыру қағидаларын басшылыққа алу қажет.

22. Сервер немесе желілік жабдық істен шыққан кезде жүйелік әкімші:

1) сервердің немесе желілік жабдықтың істен шыққан компоненттерін өшіруі;

2) үздіксіз жұмысты қамтамасыз ету үшін резервтік серверді немесе желілік жабдықты олар болған кезде дереу іске қосу жөнінде шаралар қабылдауы;

3) деректер мен бағдарламалық қамтамасыз ету тұтастығының жоғалуына және/немесе бұзылуына талдау жүргізуі;

4) зақымдалған жабдықтың жұмысын тексеруі;

5) серверлік немесе желілік жабдықтың бүлінген компоненттерінің немесе сервистерінің жұмысқа қабілеттілігін қалпына келтіруі (қажет болған жағдайда бағдарламалық қамтамасыз етуді және актіні жасай отырып, резервтік көшірмелерден деректерді қалпына келтіруі) тиіс.

23. Пайдаланушылардың серверлерінде немесе дербес компьютерлерінде ақпараттың жоғалуы немесе таралуы анықталған жағдайда, ақпараттық технологиялар бөлімінің қызметкері жүйелік әкімшінің қатысуымен ақпараттың жоғалу себептерін іздеу және жою бойынша іс-шаралар (БҚ мен есептеу техникасы құралдарының тұтастығы мен жұмысқа қабілеттілігін тексеру) жүргізеді, қажет болған жағдайда резервтік көшірмелерден ақпарат қалпына келтіріледі. Егер ақпараттың таралуы техникалық себептер бойынша орын алса, ақпараттың қорғалуына талдау жүргізіледі, осалдықтардың туындауын жою және алдын алу бойынша шаралар қабылданады.

24. Тіркеу құралдарымен тіркелген РҚЖ әрекеті кезінде жүйелік әкімші тіркеу журналдарындағы ақпаратқа талдау жүргізеді және талдау нәтижелері бойынша РҚЖ-ға нақты қауіп төнген жағдайда РҚЖ болдырмау бойынша мынадай шаралар қабылданады:

1) құпия сөздерді жоспардан тыс толық өзгерту жүргізіледі;

2) қауіпсіздік жүйесінің осалдығын жоятын қолда бар бағдарламалық қамтамасыз етудің жаңартуы қолданылады.

25. РҚЖ анықталған кезде келесі іс-шаралар жүргізіледі:

1) жүйелік әкімші және ақпараттық қауіпсіздік жөніндегі маман РҚЖ мән-жайларына жедел талдау жүргізеді, оның нәтижелері бойынша бірінші басшы инцидентті тергеу аяқталғанға дейін АЖ пайдалануды жалғастыру мүмкіндігі туралы шешім қабылдайды.

2) қажет болған жағдайда АЖ және БҚ-ны зиянды кодтың болуын тексеру үшін серверді желіден ажырату немесе серверді тоқтату жүргізіледі. Резервтік серверге уақытша көшу мүмкін.

3) резервтік көшірме жасау арқылы кейінгі талдау үшін жүйенің көшірмесі жасалады.

4) Жүйелік әкімші серверді тіркеу журналдарына және ақпаратты қорғау құралдарын тіркеу журналдарына талдау жүргізеді.

5) серверлерге қатысты құпия сөздерді жоспардан тыс өзгерту жүргізіледі.

26. Байланыс арналары істен шыққан кезде жүйелік әкімші байланыс қызметтерін жеткізушіге хабарлайды, байланыс арнасын қалпына келтіру мәселесін пысықтайды, олар болған жағдайда қосалқы байланыс арналарына көшу жөнінде шаралар қабылдайды.

27. Электр энергиясы 10 минуттан артық ажыратылған жағдайда және үздіксіз қоректендіру көздерін пайдалану мүмкін болмаған жағдайда, ақпараттық технологиялар бөлімінің қызметкері барлық серверлер мен желілік жабдықтарды дұрыс ажыратуды жүргізуі қажет. Ұйым ғимаратында электр энергиясын беру кезінде жүйелік әкімші ақпараттық қауіпсіздік жөніндегі маманмен бірлесіп, серверде және БҚ деректерінің жоғалуына және (немесе) бұзылуына талдау жүргізеді, сондай-ақ жабдықтың жұмысқа қабілеттілігін тексереді. Қажет болған жағдайда акт жасай отырып, соңғы резервтік көшірмеден БҚ мен деректерді қалпына келтіру жүргізіледі.

28. Кеңседе немесе провайдердің аумағында орналасқан жабдықты электрмен қоректендірудің істен шығуы анықталған кезде ақпараттық технологиялар қызметкері уәкілетті қызметкерлерді дереу хабардар етеді. Егер электр қуатының істен шығуын жоюдың болжамды уақыты 30 минуттан асса, ақпараттық технологиялар қызметкері бірінші басшыға хабарлайды. Электр қуатын беруді қайта бастаған кезде жүйелік әкімші жабдықтың тұтастығын тексеру және БҚ бойынша іс-шаралар жүргізеді.

29. Табиғи-климаттық әсер (жер сілкінісі, су тасқыны, дауыл, өрт және т.б.) пайда болған кезде жүйелік әкімшілер мүмкіндігінше жүйенің соңғы толық көшірмесін сақтауды қамтамасыз етуі керек.

30.Табиғи апаттар кезінде жұмыскерлердің нақты іс-қимылдарын әзірлеу үшін ақпараттық қауіпсіздік жөніндегі маман жылына кемінде бір рет арнайы оқыту жаттығуларын ұйымдастыруы тиіс.

## 5. Үздіксіз жұмыс пен қалпына келтіруді қамтамасыз ету құралдары

31. Осы нұсқаулық шеңберінде техникалық сипаттағы штаттан тыс жағдайлардың туындау тәуекелдері қарастырылады.

**Техногендік әсер етудің және табиғи апаттардың штаттан тыс жағдайларының туындау тәуекелдері төтенше жағдайларға жатады және «Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар» құжатында қаралады.**

32. Үздіксіз жұмыс пен қалпына келтіруді қамтамасыз ету құралдары:

1) ұйымның ақпараттық ресурстарының резервтік көшірмесі;

2) серверлік машиналардағы үздіксіз қуат көздері

33. Резервтік көшірме ақпарат жоғалған жағдайда ақпаратты қалпына келтіруді қамтамасыз етеді. Резервтік көшірме Ақпараттың резервтік көшірмесін жасау және қалпына келтіру регламентінің талаптарына сәйкес орындалады.

34. Үздіксіз қуат көздері электр тогының параметрлері рұқсат етілген параметрлерден ажыратылған немесе шыққан жағдайда қосылған жабдықтың аккумуляторлардан біраз уақыт жұмыс істеуін қамтамасыз етеді.

## 6. Ақпараттық жүйелердің үздіксіз жұмысын қамтамасыз ету және қалпына келтіру жөніндегі персоналдың міндеттері мен іс-әрекеттері

35. Дағдарыс жағдайындағы қызметкерлердің әрекеттері оның ауырлығына байланысты.

36. Қауіпті немесе ауыр сыни жағдай туындаған жағдайда қызметкерлердің әрекеттері келесі кезеңдерді қамтиды:

1) жауапты қызметкерлердің жедел реакциясы;

2) өнімділікті ішінара қалпына келтіру және өңдеуді қалпына келтіру;

3) жүйені толық қалпына келтіру және өңдеуді толық қалпына келтіру;

4) дағдарыс жағдайының себептерін тергеп-тексеру және кінәлілерді анықтау;

5) күндізгі уақытта штаттан тыс (дағдарыстық) жағдайды анықтаған қызметкер өзінің тікелей басшысын және жүйелік әкімшісін – ауызша, ақпараттық қауіпсіздік жөніндегі маманды – ауызша, қажет болған жағдайда жазбаша хабардар етуі тиіс;

6) мұндай бұзушылықтардың себептерін жою және кейіннен жол бермеу жөнінде шешімдер әзірлеу.

37. Ұйым ғимаратты күзететін ұйымның назарына мыналардың қажеттілігін жеткізеді: тәуліктің түнгі уақытында штаттан тыс жағдай туындаған кезде қауіпсіздікке жауапты күзетші төлдейтін ақпараттық технологиялардың жауапты қызметкерін хабардар етуі тиіс.

38. АЖ пайдалануды жүзеге асыратын қызметкерлер ақпараттық қауіпсіздік жөніндегі маманға штаттан тыс жағдайлардың туындауының барлық байқалған алғышарттары туралы хабарлауға міндетті.

39. Дағдарыс жағдайында жұмысты ұйымдастыруды жүйелік әкімші және ақпараттық қауіпсіздік жөніндегі маман оларға жүктелген міндеттерге сәйкес жүзеге асырады.

40. Дағдарыс жағдайында жұмыстың ұйымдастырылуын бақылауды ұйым басшысы жүзеге асырады.

## 7. Штаттан тыс немесе дағдарыстық жағдайлардың туындауын және олар бойынша түзету әрекеттерін бақылау

41. Штаттан тыс жағдайлардың пайда болуын бақылау келесі функциялардың көмегімен жүзеге асырылады:

1) штаттан тыс жағдайлардың туындауын штаттан тыс жағдайларды тіркеу журналында тіркеу;

2) штаттан тыс жағдайды және түзету әрекеттерін сипаттай отырып, олардың түпнұсқалығын растайтын құжатпен жазылған түсіндірме материалдарды (скриншоттар, оқиғалар журналының басып шығарулары және т.б.) қоса бере отырып, актілер жасау.

## 8. Жауапкершілік

42. АЖ жұмысына жауапты басшылық пен қызмет көрсетуші персонал мыналар үшін жауапкершілік алады:

1) өзінің функционалдық міндеттерін тиісінше орындамау;

2) өз құзыреті шеңберінде өңделетін ақпараттың сақталуына, қолжетімділігіне, құпиялылығына тиісті жағдайларды қамтамасыз етпеу.

43. Жүйелік әкімші кемінде жарты жылда бір рет штаттан тыс жағдайлардың қайталану тәуекелдерін төмендету бойынша алдын алу шараларын әзірлеу үшін штаттан тыс жағдайларды тіркеу журналында тіркелген оқиғаларға талдау жүргізеді.

44. Осы нұсқаулықтың талаптарын бұзған адамдар Қазақстан Республикасының қолданыстағы заңнамасына сәйкес тәртіптік немесе өзге де жауапкершілікке тартылады.

## 9. Нұсқаулықтың сақталуын бақылау

45. Осы нұсқаулықтың сақталуын бақылауды жүйелік әкімші және ақпараттық қауіпсіздік жөніндегі маман жүзеге асырады.

46. Осы нұсқаулықта көзделген нормаларды бұзғаны үшін қызметтік тергеп-тексеру материалдары негізінде ақпараттық қауіпсіздік жөніндегі

маманның ұсынуы бойынша ұйым қызметкерлеріне тәртіптік жаза шаралары қолданылуы мүмкін.

**Ақпараттық қауіпсіздік инциденттеріне және штаттан тыс (дағдарыстық) жағдайларда ден қою бойынша пайдаланушылардың іс-қимыл тәртібі туралы нұсқаулыққа 1-қосымша**

202_ жылғы «__» _____ № __

## Штаттан тыс жағдайларды тіркеу журналы

| р/т № | Күні | Штаттан тыс қағдайдың қысқаша сипаттамасы | Басталу уақыты | Аяқталу уақыты | Тоқтау | Себебі | Жою әдісі | Жауапты |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## ТАНЫСУ ПАРАҒЫ

| № | Тегі, аты, әкесінің аты | Лауазымы | Жеке қолы | Күні |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |