Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспарын бекіту туралы

Қазақстан Республикасы Үкіметінің 2018 жылғы 9 тамыздағы № 488 қаулысы.

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 6-бабының 6-1) тармақшасына сәйкес Қазақстан Республикасының Үкіметі **ҚАУЛЫ ЕТЕДІ**:

1. Қоса беріліп отырған Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспары бекітілсін.

2. Осы қаулы алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Премьер-Министрі *Б. Сағынтаев*

Қазақстан Республикасы
Үкіметінің
2018 жылғы9 тамыздағы
№ 488 қаулысымен
бекітілген

Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспары

1-тарау. Жалпы ережелер

1. Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспары (бұдан әрі – жоспар) ақпараттық қауіпсіздіктің жай-күйіне олардың жұмысының бұзылуын бір мерзімде барынша азайта отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларының әсерін азайту бойынша жүйе субъектілерінің іс-қимыл тәртібін айқындайды.

2. Осы жоспар Қазақстан Республикасының мемлекеттік құпиялар туралы заңнамасына сәйкес мемлекеттік құпияларға жатқызылған, қорғалып орындалатын ақпараттық жүйелерге, сондай-ақ арнайы мақсаттағы телекоммуникациялар және/немесе үкіметтік, президенттік, құпияландырылған, шифрланған және кодталған байланыс желілеріне қолданылмайды.

3. Осы жоспарда мынадай ұғымдар пайдаланылады:

1) ақпараттық-коммуникациялық инфрақұрылым объектілері (бұдан әрі – АКИ объектілері) – ақпараттық жүйелер, технологиялық платформалар,

ақпараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдардың үздіксіз жұмыс істеуін және ақпараттық қауіпсіздікті қамтамасыз ету жүйелері;

2) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері (бұдан әрі – АКИАМО) – жұмыс істеуінің бұзылуы немесе тоқтауы 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, 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 АКИ объектілері;

3) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою жүйесі (бұдан әрі – жүйе) – электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымдарды компьютерлік шабуылдар мен олардың зардаптарын жою салдарынан болатын технологиялық істен шығудан немесе рұқсатсыз ықпал етуден қорғау бойынша жалпы мемлекеттік іс-шаралар кешенін іске асыруға арналған ақпараттық қауіпсіздікті қамтамасыз етудегі күштер мен құралдардың жиынтығы;

4) ақпараттық қауіпсіздіктің оқыс оқиғасы (бұдан әрі – АҚ оқыс оқиғасы) – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында олардың тиісінше жұмыс істеуіне қатер төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшіру, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын жеке немесе сериялы түрде туындайтын іркілістер;

5) ақпараттық қауіпсіздік саласындағы дағдарысты жағдай – мемлекеттік қызметтерді ұсынуды тоқтатуға немесе шектеуге, тиісті аумақтарда тұрып жатқан халықтың тіршілігі немесе Қазақстан Республикасының қорғаныс, қауіпсіздік, халықаралық қатынастар, экономика, шаруашылықтың жеке салалары, инфрақұрылымы үшін әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайларға немесе жағымсыз салдарға әкеп соғуы мүмкін АҚ оқиғасы немесе АКИ объектілерінде олардың пайда болуының нақты алғышарттары;

6) ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы (бұдан әрі – АҚҰҮО) – " Мемлекеттік техникалық қызмет" акционерлік қоғамының құрылымдық бөлімшесі";

7) жүйе субъектілері – ақпараттық қауіпсіздік мәселелерін шешуге немесе АҚ оқыс оқиғаларына ден қоюға уәкілетті мемлекеттік органдар, АҚҰҮО, Жедел штаб, "

электрондық үкімет" ақпараттандыру объектілерінің иелері, АКИАМО иелері, ақпараттық қауіпсіздіктің жедел орталықтары (бұдан әрі – АҚЖО), ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтері;

8) компьютерлік шабуыл – ақпаратқа, электрондық ресурсқа, ақпараттық жүйеге рұқсатсыз ықпал ету немесе оларға бағдарламалық немесе бағдарламалық-аппараттық құралдарды (немесе желіаралық өзара іс-қимылдардың хаттамаларын) қолдана отырып, қолжетімділік алу арқылы қатерлер төндіруді іске асырудың мақсатты әрекеті.

Жоспардағы басқа да пайдаланылатын ұғымдар Қазақстан Республикасының ақпарат және байланыс саласындағы заңнамаларда қолданылатын ұғымдарға сәйкес келеді.

Ескерту. 3-тармаққа өзгерістер енгізілді - ҚР Үкіметінің 01.10.2020 № 630; 26.10.2022 № 849 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулыларымен.

2-тарау. Профилактикалық іс-шаралар

4. Профилактика және ақпараттандыру мен байланыс саласындағы оқыс оқиғаларды болдырмау мақсатында АҚҰҰО жоспарлы негізде АҚ оқыс оқиғалары бойынша түсіндіру жұмыстарын өткізеді, бұл үшін тұрақты негізде ақпараттық қауіпсіздік саласындағы шетелдік және халықаралық ұйымдарды қоса алғанда жүйе субъектілерінен және өзге көздерден ақпаратты жинауды, талдауды және қорытындылауды жүзеге асырады.

5. АҚЖО АҚ қатерлерін анықтау мен болдырмау мақсатында оған қосылған ақпараттық-коммуникациялық инфрақұрылымға және ақпараттандырудың объектілеріне мониторингілеуді жүзеге асырады.

6. Ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингі мәселелері бойынша АҚЖО-ның өзара іс-қимылын АҚҰҰО қамтамасыз етеді.

7. Электрондық ақпараттық ресурстардың, бағдарламалық қамтылымның, ақпараттық жүйелер мен оларды қолдайтын ақпараттық-коммуникациялық инфрақұрылымның қорғалу деңгейін арттыруға арналған жүйе субъектілері Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды, сондай-ақ ақпараттық қауіпсіздік саласын регламенттейтін өзге де нормативтік құқықтық актілерді басшылыққа алады.

3-тарау. Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің және "электрондық үкімет" ақпараттандыру объектілерінің иелері мен меншік иелерінің іс-шаралары

8. АҚ-ның 0-ден 5-ке дейінгі маңыздылық деңгейіндегі оқыс оқиғаларына ден қоюды қамтамасыз ету мақсатында "электрондық үкімет" ақпараттандыру обьектілерінің иелері, АКИАМО иелері, АҚЖО ақпараттық қауіпсіздік қатерлерін (қауіптерін) өңдеу, үздіксіз жұмысты қамтамасыз ету және ақпараттарды өңдеу құралдарына байланысты активтердің жұмыс істеу қабілетін қалпына келтіру бойынша шаралар және мынадай міндетті іс-шаралар көзделген ден қою жоспарларын әзірлейді және бекітеді:

1) ақпараттық қауіпсіздіктің дағдарыстық жағдайын болдырмау бойынша іс-шаралар ұйымдастыру және өткізу;

2) ақпараттық-коммуникациялық инфрақұрылымдағы ақпараттық қауіпсіздіктің жай-күйі туралы деректерді жинақтау және талдау;

3) АҚЖО және АҚҰҰО-мен өзара іс-қимылды жүзеге асыру;

4) үздіксіз жұмысты қамтамасыз етуді қолдайтын шаралар және сыртқы өзгерістерге төзімділік;

5) анықталған ақпараттық қауіпсіздіктің оқыс оқиғалары және оларды жою мәселелері бойынша жүйенің мүдделі субъектілерін ақпараттандыру;

6) ақпараттық қауіпсіздіктің оқыс оқиғаларын және олардың салдарын жою кезіндегі іс-қимыл тәртібі, жүйе субъектісінің ақпараттық-коммуникациялық инфрақұрылымына әсерін барынша азайту;

7) ақпараттық қауіпсіздіктің оқыс оқиғаларының (журналдардың, баяндамалардың және нысандардың) цифрлық ізін сақтау шаралары;

8) ақпараттық қауіпсіздіктің оқыс оқиғаларының себебін белгілеу;

9) ақпараттық қауіпсіздіктің оқыс оқиғаларынан кейін жасалуы тиіс әрекеттер;

10) АҚ оқыс оқиғаларының себептерін жою;

11) қалпына келтіру рәсімдері.

Ақпараттық-коммуникациялық инфрақұрылымның жұмыс істеу ерекшелігіне және (немесе) жүйе субъектілерінің технологиялық процестеріне сүйене отырып, өзге іс-шаралар қосылуы мүмкін.

9. "Электрондық үкіметтің" ақпараттандыру объектілері мен АКИАМО иелері ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі уәкілетті органға ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюдың бекітілген жоспарларының көшірмесін жолдайды.

10. АҚ оқыс оқиғалары мәселелері бойынша АКИАМО және "Электрондық үкіметтің" ақпараттандыру объектілерінің иелері мен меншік иелері АҚҰҰО-мен тәулік бойы 1400 call-орталығы немесе www.kz-cert.kz ресми сайты арқылы өзара іс-қимыл жасайды.

11. "Электрондық үкіметтің" ақпараттандыру объектілерінің және АКИАМО иелерінің шешімі бойынша ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюға

ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтері және (немесе) АҚЖО жұмылдырылуы мүмкін.

12. "Электрондық үкіметтің" ақпараттандыру объектілері мен АКИАМО иелері ден қою аяқталғаннан кейін ақпараттық қауіпсіздік жөніндегі уәкілетті органның және АҚҰҰО ұсыныстарын пайдалана отырып, жүйені қалпына келтіру бойынша жоспарда көзделген шараларды іске асыруға кіріседі.

13. "Электрондық үкіметтің" ақпараттандыру объектілері, АКИАМО иелері өзара тиімді іс-қимыл жасау мақсатында ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапты лауазымды адамдарды анықтайды.

Адамдардың байланыс деректері АҚҰҰО-ға жіберіледі. Жауапты лауазымды адамдарды немесе оның байланыс деректерін ауыстыру бойынша барлық жағдайлар туралы 48 сағат ішінде АҚҰҰО-ға хабарланады.

4-тарау. Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою

4.1-параграф. Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою бойынша уәкілетті органның іс-қимылы

14. АҚҰҰО "электрондық үкіметтің" ақпараттандыру объектілерінің және АКИ аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларында және Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларында белгіленген, ақпараттық қауіпсіздіктің оқыс оқиғалары маңыздылығының 3, 4 және 5 деңгейлеріне сәйкес ақпараттандыру объектілерінде ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат алған жағдайларда Қазақстан Республикасының Ұлттық қауіпсіздік органдарына хабарлайды.

15. Кейінге қалдыруға болмайтын, ауыр және аса ауыр қылмыстардың, сондай-ақ қылмыстық топ дайындайтын және жасайтын қылмыстардың жасалуына әкеп соғуы мүмкін жағдайларда Қазақстан Республикасы Ұлттық қауіпсіздік комитетінің төрағасы, оның орынбасарлары немесе Қазақстан Республикасы Ұлттық қауіпсіздік комитетінің аумақтық органдарының бастықтары не оларды алмастыратын адамдар кейіннен байланыс саласындағы уәкілетті органды және Қазақстан Республикасының Бас прокуратурасын 24 сағат ішінде хабардар ете отырып, жедел-іздестіру қызметінің барлық субъектілерінің мүддесінде байланыс желілерінің және (немесе) құралдарының жұмысын, байланыс қызметтерінің көрсетілуін, интернет-ресурстарға және (немесе) оларда орналастырылған ақпаратқа қол жеткізуді тоқтата тұруға құқылы.

16. Әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайларда, төтенше немесе әскери жағдайларды енгізген кезде ақпараттық қауіпсіздікті қамтамасыз ету

жөніндегі уәкілетті орган интернет-ресурстарды және инфрақұрылымның АКИ объектілерін басқару бойынша қызметті үйлестіруді жүзеге асырады.

17. Трансшекаралық сипаттағы АҚ-ның оқыс оқиғаларына ден қою шаралары сыртқы саяси қызмет жөніндегі уәкілетті органмен келісіледі және Қазақстан Республикасы ратификациялаған халықаралық шарттарға сәйкес жүзеге асырылады.

4.2-параграф. Жедел штабтың іс-қимылы

18. Ақпараттық қауіпсіздік саласындағы дағдарысты жағдайларға ден қою бойынша қызметті үйлестіру мақсатында АҚҰҰО негізінде ақпараттық қауіпсіздіктің дағдарысты жағдайларына ден қою бойынша жедел штаб (бұдан әрі – Жедел штаб) құрылады.

19. Жедел штаб шақырылғанға дейін АҚҰҰО АКИ-дің аса маңызды объектілерінің және "Электрондық үкіметтің" ақпараттандыру объектілерінің меншік иелері мен иелерінің күштерімен және құралдарымен бірге дағдарыстық жағдайға, оның таратылуын тоқтату мен зардаптарын азайту мақсатында бастапқы ден қою шараларын өткізеді.

20. Ұлттық қауіпсіздік комитеті төрағасының ақпараттық қауіпсіздік саласына жетекшілік ететін немесе оның міндеттерін атқарушы орынбасары Жедел штаб басшысы болып табылады. Ақпараттық қауіпсіздік саласындағы уәкілетті органның ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік саясатты іске асыруды қамтамасыз ететін ведомствосының басшысы немесе оның міндетін атқарушы Жедел штаб басшысының орынбасары болып табылады.

21. Жедел штаб басшысының шешімі бойынша оның құрамына мемлекеттік органдардың және өзге де ұйымдардың өкілдері кіре алады.

22. Ақпараттық қауіпсіздіктің дағдарыстық жағдайын бастапқы талдау негізінде ақпараттық қауіпсіздіктің оқыс оқиғасы салдарын жою және оқшаулау бойынша шаралар кешенін ұйымдастыру және іске асыру үшін АҚҰҰО басшысы Жедел штаб басшысына Жедел штабты шақыру туралы шешім қабылдауды ұсынады.

23. Жедел штабтың дағдарыстық жағдайлардағы негізгі міндеттері:

ақпараттық қауіпсіздіктің дағдарысты жағдайына ден қою бойынша мемлекеттік органдар мен ұйымдардың уәкілетті бөлімшелерінің іс-қимыл тәртібін белгілеу;

ақпараттық қауіпсіздіктің дағдарыстық жағдайларын оқшаулау және жою жөніндегі мемлекеттік органдар мен ұйымдардың уәкілетті бөлімшелерінің күштері мен құралдарына түзетулер енгізу;

ақпараттық қауіпсіздік саласындағы дағдарыстық жағдайларға ұйымдастырушылық және техникалық ден қоюды үйлестіру;

ақпараттық қауіпсіздік саласындағы дағдарыстық жағдай кезеңінде жұмысы зардап шеккен ақпараттық-коммуникациялық инфрақұрылымның жұмысын қалпына келтіру іс-шараларын әзірлеу және ұйымдастыру;

ақпараттық қауіпсіздік саласындағы дағдарыстық жағдайдың туындау себептері мен жағдайларын анықтау бойынша қызметтік және техникалық тергеп-тексеруді және талқылауды ұйымдастыру;

ақпараттандыру объектілерінің иелері мен меншік иелерін ақпараттық қауіпсіздіктің оқыс оқиғалары туралы бұқаралық ақпарат құралдары арқылы құлақтандыру болып табылады.