Қазақстан Республикасы
Үкіметінің
2026 жылғы « 14 » тамыздағы
№ 725 қаулысына
қосымша

Қазақстан Республикасы
Үкіметінің
2018 жылғы 9 тамыздағы
№ 488 қаулысымен
бекітілген

Киберқауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспары

1-тарау. Жалпы ережелер

1. Киберқауіпсіздіктің оқыс оқиғаларына ден қоюдың дағдарысқа қарсы ұлттық жоспары (бұдан әрі – жоспар) мемлекеттік құпияларға жатқызылған, қорғалып жасалған цифрлық жүйелерге, мемлекеттік құпияларды құрайтын мәліметтерді қамтитын цифрлық объектілерге, сондай-ақ арнаулы мақсаттағы телекоммуникация желісіне және (немесе) президенттік, үкіметтік және қорғалған байланыс желілеріне қолданылмайды.

2. Осы жоспарда мынадай ұғымдар пайдаланылады:

1) цифрлық инфрақұрылым объектілері – цифрлық объектілерді орналастыруды және олардың жұмыс істеу ортасын қамтамасыз ететін материалдық, техникалық және технологиялық құралдардың жиынтығы;

2) аса маңызды цифрлық объектілер – 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 салдарға әкелетін цифрлық объектілер;

3) киберқауіпсіздіктің оқыс оқиғаларына ден қою жүйесі (бұдан әрі – жүйе) – цифрлық ресурстарды, цифрлық жүйелер мен цифрлық инфрақұрылымды компьютерлік шабуыл мен олардың салдарын жоюдан болатын технологиялық істен шығудан немесе рұқсатсыз ықпал етуден қорғау бойынша жалпы

мемлекеттік іс-шаралар кешенін іске асыруға арналған киберқауіпсіздікті қамтамасыз ету күштері мен құралдарының жиынтығы;

4) киберқауіпсіздіктің оқыс оқиғасы – цифрлық объектінің киберқауіпсіздігіне теріс әсерін тигізетін оқиға немесе оқиғалар жиынтығы;

5) киберқауіпсіздік саласындағы дағдарысты жағдай – мемлекеттік қызметтері көрсетудің мүмкін болмауына немесе шектелуіне, тиісті аумақта тұрып жатқан халықтың тыныс-тіршілігі немесе Қазақстан Республикасының қорғанысы, қауіпсіздігі, халықаралық қатынастары, экономикасы, жекелеген шаруашылық салалары, инфрақұрылымы үшін әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайларға немесе жағымсыз салдарға әкеп соққан немесе соғуы мүмкін киберқауіпсіздік оқиғасы;

6) киберқауіпсіздіктің ұлттық үйлестіру орталығы (бұдан әрі – КҚҰҮО) – «Мемлекеттік техникалық қызмет» акционерлік қоғамының құрылымдық бөлімшесі»;

7) жүйе субъектілері – киберқауіпсіздік мәселелерін шешуге немесе киберқауіпсіздіктің оқыс оқиғаларына ден қоюға уәкілетті мемлекеттік органдар, КҚҰҮО, жедел штаб, «цифрлық үкімет» цифрлық объектілерінің иелері, аса маңызды цифрлық объектілердің иелері, киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметтері;

8) компьютерлік шабуыл – ақпаратқа, цифрлық ресурсқа, цифрлық жүйеге рұқсатсыз ықпал ету немесе оларға бағдарламалық немесе бағдарламалық-аппараттық құралдарды (немесе желіаралық өзара іс-қимылдардың хаттамаларын) қолданып қолжетімділік алу арқылы қатер төндіру мақсатындағы әрекет.

2-тарау. Профилактикалық іс-шаралар

3. Профилактика және цифрландыру мен байланыс салаларындағы оқыс оқиғаларды болғызбау мақсатында КҚҰҮО киберқауіпсіздіктің оқыс оқиғалары бойынша жоспарлы негізде түсіндіру жұмыстарын жүргізеді, киберқауіпсіздіктің салалық орталықтары мен киберқауіпсіздікті қамтамасыз ету орталықтарының «цифрлық үкімет» цифрлық объектілеріндегі және аса маңызды цифрлық объектілердегі киберқауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, талдауды және қорытуды жүзеге асырады.

4. Киберқауіпсіздікті қамтамасыз ету орталықтары киберқауіпсіздік қатерлерін анықтау және жою мақсатында «цифрлық үкімет» цифрлық объектілеріне жатпайтын аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүзеге асырады.

5. Киберқауіпсіздікті қамтамасыз ету және киберқауіпсіздіктің оқыс оқиғаларына ден қою үшін қажетті ақпарат алмасу кезінде КҚҰҮО-ның киберқауіпсіздікті қамтамасыз ету орталықтарымен өзара іс-қимыл жасауы

Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығымен бекітілген (нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16886 болып тіркелген) Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасындағы киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларымен айқындалады.

6. Цифрлық ресурстардың, бағдарламалық қамтылымның, цифрлық жүйелер мен оларды қолдайтын цифрлық инфрақұрылымның қорғалу деңгейін арттыру үшін жүйе субъектілері Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарды, сондай-ақ киберқауіпсіздік саласын регламенттейтін өзге де нормативтік құқықтық актілерді басшылыққа алады.

3-тарау. Аса маңызды цифрлық объектілердің және «цифрлық үкіметтің» цифрлық объектілерінің меншік иелері мен иеленушілерінің әрекеті

7. Маңыздылық деңгейі 1-ден 4-ке дейінгі оқыс оқиғаларға ден қоюды қамтамасыз ету мақсатында «цифрлық үкімет» цифрлық объектілерінің иелері, аса маңызды цифрлық объектілердің иелері, киберқауіпсіздікті қамтамасыз ету орталықтары ден қою жоспарларын әзірлейді және бекітеді, оларда киберқауіпсіздік қатерін (қауіпін) өңдеу, үздіксіз жұмысты қамтамасыз ету және ақпарат өңдеу құралдарына байланысты активтердің жұмыс істеу қабілетін қалпына келтіру бойынша шаралар және мынадай:

1) киберқауіпсіздіктің дағдарысты жағдайының туындауына жол бермеу бойынша іс-шараларды ұйымдастыру және өткізу;

2) цифрлық инфрақұрылымдағы киберқауіпсіздіктің жай-күйі туралы деректерді жинақтау және талдау;

3) киберқауіпсіздікті қамтамасыз ету орталықтарымен және ҚҚҰҰО-мен өзара іс-қимылды жүзеге асыру;

4) іркіліссіз жұмысты қамтамасыз етуді және сыртқы өзгерістерге төзімділікті қолдау шаралары;

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

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

7) киберқауіпсіздіктің оқыс оқиғаларының цифрлық ізін сақтау шаралары (журналдар, есептер және нысандар);

8) киберқауіпсіздіктің оқыс оқиғаларының себебін белгілеу;

9) киберқауіпсіздіктің оқыс оқиғаларынан кейін жасалуға тиіс әрекет;

10) киберқауіпсіздіктің оқыс оқиғаларының себептерін жою;

11) қалпына келтіру рәсімдері бойынша міндетті іс-шаралар көзделеді.

8. «Цифрлық үкімет» цифрлық объектілері мен аса маңызды цифрлық объектілердің иегерлері киберқауіпсіздікті қамтамасыз ету жөніндегі уәкілетті органға және КҚҰҰО-ға киберқауіпсіздіктің оқыс оқиғаларына ден қоюдың бекітілген жоспарларының көшірмесін жолдайды.

9. Киберқауіпсіздіктің оқыс оқиғаларының мәселелері бойынша аса маңызды цифрлық объектілердің және «цифрлық үкімет» цифрлық объектілерінің меншік иелері мен иегерлері КҚҰҰО-мен тәулік бойы 1400 call-орталығы, КҚҰҰО платформасы, incident@cert.gov.kz электрондық поштасы немесе www.cert.gov.kz ресми сайты арқылы өзара іс-қимыл жасайды.

10. «Цифрлық үкімет» цифрлық объектілерінің, аса маңызды цифрлық объектілердің иегерлерінің шешімі бойынша киберқауіпсіздіктің оқыс оқиғаларына ден қоюға киберқауіпсіздіктің оқыс оқиғаларына ден қою қызметтері және (немесе) киберқауіпсіздікті қамтамасыз ету орталықтары жұмылдырылады.

11. «Цифрлық үкімет» цифрлық объектілерінің, аса маңызды цифрлық объектілердің иегерлері ден қою аяқталғаннан кейін жүйені қалпына келтіру бойынша жоспарда көзделген шараларды, оның ішінде киберқауіпсіздік жөніндегі уәкілетті органның және КҚҰҰО ұсыныстарын пайдалана отырып іске асыруға кіріседі.

12. «Цифрлық үкімет» цифрлық объектілерінің, аса маңызды цифрлық объектілердің иегерлері өзара тиімді іс-қимыл жасау мақсатында киберқауіпсіздікті қамтамасыз ету үшін жауапты лауазымды тұлғаларды анықтайды.

Лауазымды тұлғалардың байланыс деректері КҚҰҰО-ға жіберіледі. Жауапты лауазымды тұлғалар немесе оның байланыс деректері ауысқан барлық жағдайлар туралы 48 сағат ішінде КҚҰҰО-ға хабарланады.

4-тарау. Киберқауіпсіздіктің оқыс оқиғаларына ден қою

1-параграф. Уәкілетті органдардың киберқауіпсіздіктің оқыс оқиғаларына ден қою жөніндегі әрекеті

13. КҚҰҰО цифрлық объектілерде киберқауіпсіздіктің оқыс оқиғалары маңыздылығының 4-деңгейіне сәйкес киберқауіпсіздіктің оқыс оқиғалары туралы ақпарат алған жағдайларда Қазақстан Республикасының ұлттық қауіпсіздік органдарына хабарлайды.

14. Кейінге қалдыруға болмайтын және 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 тұлғалар кейіннен байланыс, масс-медиа салаларындағы уәкілетті органдарды және Қазақстан Республикасының Бас прокуратурасын жиырма төрт 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.

15. Әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайларда, төтенше немесе әскери жағдайлар енгізілгенде киберқауіпсіздікті қамтамасыз ету жөніндегі уәкілетті орган интернет-ресурстарды және инфрақұрылымның цифрлық объектілерін басқару қызметін үйлестіруді жүзеге асырады.

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

2-параграф. Жедел штабтың әрекеті

17. Киберқауіпсіздік саласындағы дағдарысты жағдайларға ден қою қызметін үйлестіру мақсатында ҚҚҰҰО базасында киберқауіпсіздіктің дағдарысты жағдайларына ден қою жөніндегі жедел штаб (бұдан әрі – жедел штаб) құрылады.

18. Жедел штаб шақырылғанға дейін «Киберқауіпсіздік туралы» Қазақстан Республикасының Заңы 7-7-бабының 1-тармағының 1) тармақшасына сәйкес ҚҚҰҰО аса маңызды цифрлық объектілердің және «цифрлық үкімет» цифрлық объектілерінің меншік иелері мен иегерлері жүзеге асыратын киберқауіпсіздік саласындағы дағдарысты жағдайға ден қою жөніндегі жұмыстарды үйлестіреді.

19. Ұлттық қауіпсіздік комитеті Төрағасының киберқауіпсіздік саласына жетекшілік ететін немесе оның міндеттерін атқарушы орынбасары жедел штаб жетекшісі болады. Киберқауіпсіздік саласындағы уәкілетті органның киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік саясатты іске асыруды қамтамасыз ететін ведомствосының басшысы немесе оның міндетін атқарушы жедел штаб жетекшісінің орынбасары болады.

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

21. Киберқауіпсіздіктің дағдарысты жағдайын бастапқы талдау негізінде киберқауіпсіздіктің оқыс оқиғасы салдарын жою және оқшаулау бойынша шаралар кешенін ұйымдастыру және іске асыру үшін ҚҚҰҰО басшысы жедел штаб жетекшісіне жедел штабты шақыру туралы шешім қабылдауды ұсынады.

22. Жедел штабтың дағдарысты жағдайлардағы негізгі міндеттері:

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

мемлекеттік органдар мен ұйымдардың уәкілетті бөлімшелерінің күштері мен құралдарының киберқауіпсіздіктің дағдарысты жағдайларын оқшаулау және жою жөніндегі іс-қимылына түзетулер енгізу;

киберқауіпсіздік саласындағы дағдарысты жағдайларға ұйымдастырушылық және техникалық ден қоюды үйлестіру;

киберқауіпсіздіктің дағдарысты жағдайы кезеңінде жұмысы зардап шеккен цифрлық инфрақұрылымның жұмысын қалпына келтіру бойынша іс-шараларды әзірлеу және ұйымдастыру;

киберқауіпсіздіктің дағдарысты жағдайының туындау себептері мен шарттарын анықтау бойынша қызметтік және техникалық тергеп-тексеруді және талқылауды ұйымдастыру;

цифрлық объектілердің меншік иелері мен иегерлерін киберқауіпсіздіктің оқыс оқиғалары туралы бұқаралық ақпарат құралдары арқылы құлақтандыру.