"Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларын бекіту туралы" Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығына өзгерістер енгізу туралы

Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрінің м.а. 2026 жылғы 25 маусымдағы № 354/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 26 маусымда № 39105 болып тіркелді

ЗҚАИ-ның ескертпесі!

Осы бұйрық 12.07.2026 бастап қолданысқа енгізіледі.

БҰЙЫРАМЫН:

1. "Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларын бекіту туралы" Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16886 болып тіркелген) бұйрығына мынадай өзгерістер енгізілсін:

тақырып мынадай редакцияда жазылсын:

"Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларын бекіту туралы";

кіріспе мынадай редакцияда жазылсын:

"Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 7-1-бабының 21) тармақшасына және Қазақстан Республикасы Үкіметінің 2025 жылғы 9 қазандағы № 846 қаулысымен бекітілген Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі туралы ереженің 15-тармағының 292) тармақшасына сәйкес **БҰЙЫРАМЫН**:";

1-тармақ мынадай редакцияда жазылсын:

"1. Қоса беріліп отырған Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары бекітілсін.";

көрсетілген бұйрықпен бекітілген Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру

орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу 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 Республикасы Әділет министрлігінде мемлекеттік тіркеуді;

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

3) осы бұйрық Қазақстан Республикасы Әділет министрлігінде 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 мәліметтерді ұсынуды қамтамасыз етсін.

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

4. Осы бұйрық 2026 жылғы 12 шілдеден бастап қолданысқа енгізіледі және ресми жариялануға жатады.

Қазақстан Республикасының
Жасанды интеллект және цифрлық даму
министрінің міндетін атқарушы *Д. Мусалиев*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасының
Жасанды интеллект және
цифрлық даму министрінің
міндетін атқарушы
2026 жылғы 25 маусымдағы
№ 354/НҚ бұйрығына
қосымша
Қазақстан Республикасы
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2018 жылғы 19 наурыздағы
№ 48/НҚ бұйрығымен
бекітілген

Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары

1-тарау. Жалпы ережелер

1. Осы Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары (бұдан әрі – Қағидалар) "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 21) тармақшасына және Қазақстан Республикасы Үкіметінің 2025 жылғы 9 қазандағы № 846 қаулысымен бекітілген Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі туралы ереженің 15-тармағының 292) тармақшасына сәйкес әзірленді және киберқауіпсіздікті қамтамасыз ету және киберқауіпсіздіктің оқыс оқиғаларына ден қою үшін қажетті ақпаратпен алмасу кезінде Киберқауіпсіздіктің ұлттық үйлестіру орталығының киберқауіпсіздікті қамтамасыз ету орталықтарымен және киберқауіпсіздіктің салалық орталықтарымен өзара іс-қимыл жасау тәртібін айқындайды.

2. Осы Қағидаларда мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) аса маңызды цифрлық объектілер (бұдан әрі – АМЦО) – жұмыс істеуінің бұзылуы немесе тоқтауы қолжетімділігі шектелген дербес деректерді және заңмен қорғалатын құпияны қамтитын өзге де мәліметтерді заңсыз жинауға және өңдеуге, әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайлардың туындауына 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 құрылысжайлар, құқық қорғау қызметі, "цифрлық үкімет" инфрақұрылымы үшін елеулі теріс салдарға алып келетін цифрлық объектілер;

2) киберқауіпсіздіктің оқыс оқиғасы – цифрлық объектінің киберқауіпсіздігіне теріс әсер ететін оқиға немесе оқиғалар жиынтығы;

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

4) киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) – киберқауіпсіздікті қамтамасыз ету саласында басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган;

5) Киберқауіпсіздіктің ұлттық үйлестіру орталығы (бұдан әрі – КҰҮО) – " Мемлекеттік техникалық қызмет" акционерлік қоғамының құрылымдық бөлімшесі;

6) Киберқауіпсіздіктің ұлттық үйлестіру орталығының ақпараттық өзара іс-қимыл платформасы (бұдан әрі – КҰҮО платформасы) – КҰҮО-мен киберқауіпсіздіктің қатерлері мен оқыс оқиғалары туралы деректермен және ақпаратпен алмасуға арналған бағдарламалық қамтылым;

7) Киберқауіпсіздікті қамтамасыз ету орталығы (бұдан әрі – ККҚО) – цифрлық ресурстарды, цифрлық жүйелерді, телекоммуникация желілері мен цифрлық басқа да

объектілерді қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі;

8) киберқауіпсіздіктің қатері – киберқауіпсіздіктің оқыс оқиғасының туындауына алғышарттар жасайтын жағдайлар мен факторлардың жиынтығы;

9) Қазақстан Республикасының ұлттық қауіпсіздік органдары (бұдан әрі – ұлттық қауіпсіздік органдары) – Қазақстан Республикасының қауіпсіздігін қамтамасыз ету жүйесінің құрамдас бөлігі болып табылатын және өздеріне берілген өкілеттіктер шегінде жеке адамның және қоғамның қауіпсіздігін, елдің конституциялық құрылысын, мемлекеттік егемендігін, аумақтық тұтастығын, экономикалық, ғылыми-техникалық және қорғаныс әлеуетін қорғауды қамтамасыз етуге арналған Қазақстан Республикасының Президентіне тікелей бағынатын және есеп беретін арнаулы мемлекеттік органдар;

10) цифрлық объектінің осалдығы – бағдарламалық немесе аппараттық қамтылымда жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын санкцияланбаған іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық немесе аппараттық қамтылымдағы кемшілік;

11) цифрландыру саласындағы киберқауіпсіздік (бұдан әрі –киберқауіпсіздік) – цифрлық ресурстардың, цифрлық жүйелердің және цифрлық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі;

12) "цифрлық үкіметтің" цифрлық объектілері (бұдан әрі – ЦҮ ЦО) – мемлекеттік цирфлық ресурстар, мемлекеттік органдардың бағдарламалық қамтылымы, мемлекеттік органның интернет-ресурсы, "цифрлық үкіметтің" цифрлық инфрақұрылым объектілері , оның ішінде өзге де тұлғалардың мемлекеттік цифрлық ресурстарды қалыптастыруға, мемлекеттік функцияларды жүзеге асыруға және мемлекеттік қызметтер көрсетуге арналған цифрлық объектілері.

2-тарау. Киберқауіпсіздікті қамтамасыз ету орталықтары, киберқауіпсіздіктің салалық орталықтары мен Киберқауіпсіздіктің ұлттық үйлестіру орталығы арасында киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу тәртібі

3. Киберқауіпсіздікті қамтамасыз етуге қажетті ақпараттық алмасудың қатысушылары:

1) ұлттық қауіпсіздік органдары;

2) уәкілетті орган;

3) КҰҮО;

4) ККҚО болып табылады.

4. ККҚО және КҰҮО киберқауіпсіздік саласындағы өздеріне жүктелген міндеттер мен функцияларды жүзеге асыруға ақпарат алмасады.

5. КҚО КҰҰО-дан алынған ақпаратты өздері қызмет көрсететін ұйымдарға және инфрақұрылымды сүйемелдеуді қамтамасыз ететін өзінің құрылымдық бөлімшелеріне, оларға қатысы бар бөлімінде, ақпарат жеткізуді қамтамасыз етеді.

6. КҚО және КҰҰО:

1) киберқауіпсіздікті бұзудың алдын алу тетіктерін жетілдіруге;

2) КҚО қызметін жақсартуға;

3) КҚО мен КҰҰО арасындағы іс-әрекеттің келісімділігі мен жеделдігін арттыруға;

4) цифрлық объектілердің киберқауіпсіздік деңгейін арттыру бойынша бірлескен шешімдер әзірлеуге бағытталған міндеттерді шешу мүддесінде өзара іс-қимылды жүзеге асыруы қажет.

7. Киберқауіпсіздікті қамтамасыз етуге қажетті ақпарат құпия цифрлық деректер санатына жатады, оларды алу, өңдеу және қолдану олар жиналатын мақсаттармен шектелген. КҰҰО-дан КҚО-ға және КҚО-дан КҰҰО-ға киберқауіпсіздік оқыс оқиғалары туралы мәлімет жолдау осы Қағидалар шеңберінде жүзеге асырылады.

8. КҚО киберқауіпсіздіктің оқыс оқиғасы анықталған кезде:

киберқауіпсіздіктің оқыс оқиғасы расталған сәттен бастап 15 (он бес) минут ішінде КҰҰО-ны және ҰҮ ҰО немесе ҰИАМО меншік иесін немесе иеленушісін хабардар етеді;

КҰҰО-ға киберқауіпсіздіктің оқыс оқиғасы расталған сәттен бастап 72 (жетпіс екі) сағат ішінде осы Қағидалардың қосымшасына сәйкес нысан бойынша киберқауіпсіздіктің оқыс оқиғасының карточкасын жібереді.

КҰҰО-дан киберқауіпсіздіктің қатері, киберқауіпсіздіктің оқиғасы немесе киберқауіпсіздіктің оқыс оқиғасы туралы хабарлама түскен кезде КҚО хабарландырылған сәттен бастап 72 (жетпіс екі) сағат ішінде КҰҰО-ға:

киберқауіпсіздік қатерін талдау нәтижелерін;

киберқауіпсіздік оқиғасы расталған кезде киберқауіпсіздік оқиғасын талдау нәтижелерін;

киберқауіпсіздіктің оқыс оқиғасы расталған кезде осы Қағидалардың қосымшасына сәйкес нысан бойынша киберқауіпсіздіктің оқыс оқиғасын карточкасын жолдайды.

9. Деректерді жинау мынадай жағдайларда:

1) киберқауіпсіздіктің туындаған қатерлері, осалдықтары, оқыс оқиғалары бойынша деректерге талдау жүргізу кезінде;

2) киберқауіпсіздіктің оқыс оқиғасы цифрлық ресурстардың, цифрлық жүйелердің, телекоммуникация желілерінің және өзге цифрлық объектілерінің жұмыс істеу қабілетіне әсер ете алады деп пайымдауға негіз болған кезде;

3) киберқауіпсіздік қатері, осалдығы және оқыс оқиғасының таралып кету кезінде;

4) ұлттық қауіпсіздік органының, уәкілетті органның, және КҰҰО-ның киберқауіпсіздік қатерлері, осалдықтары, оқиғалары мен оқыс оқиғалары туралы сұратуы бойынша;

5) киберқауіпсіздік оқыс оқиғаларының әсерін жою кезіндегі көмек көрсету кезінде жүзеге асырылады.

10. КҰҰО-ның сұратуы бойынша ККҚО КҰҰО-ға қолда бар ақпараттық қауіпсіздікті қамтамасыз етудің мониторингі жүйелеріне қолжетімділікті қамтамасыз етеді.

11. КҰҰО мүдделі тараптарды:

1) цифрлық ресурстардың, цифрлық жүйелердің, телекоммуникация желілерінің және цифрлық объектілерінің тұтастығына, қолжетімділігіне, құпиялылығына әсер ете алатын киберқауіпсіздік қатерлері, киберқауіпсіздік оқиғалары немесе киберқауіпсіздік оқыс оқиғалары анықталған жағдайда өздеріне қатысты ақпарат бөлігінде ККҚО-ны;

2) цифрлық ресурстар, цифрлық жүйелер, телекоммуникация желілері және өзге цифрлық объектілері мен байланысты киберқауіпсіздіктің оқыс оқиғасы жағдайында ұлттық қауіпсіздік органдарын;

3) киберқауіпсіздік саласындағы заңнама бұзылған жағдайда уәкілетті органды;

4) киберқауіпсіздік саласындағы заңнама бұзылған жағдайда Қазақстан Республикасының киберқауіпсіздік саласындағы уәкілетті органын;

5) олардың құзыреті шегінде тиісті заңнама бұзылған жағдайда Қазақстан Республикасының прокуратура органдарын;

6) олардың құзыреті шегінде тиісті заңнама бұзылған жағдайда Қазақстан Республикасының ішкі істер органдарын хабарландырады.

12. Ақпараттық алмасу мынадай тәсілдермен жүзеге асырылады:

1) деректерді шифрлауды қолданып, электрондық хабарлама көмегімен белгілеудің кеңейтілген тілі (eXtensible Markup Language – XML) немесе деректер алмасудың мәтіндік пішіні (JavaScript Object Notation – JSON) пішіндерінде жіберу;

2) деректерді ақпарат алмасуға арналған бағдарламалық қамтылымды қолдана отырып XML немесе JSON форматтарында жіберу;

3) шифрланған деректерді HTTPS (HyperText Transfer Protocol Secure) хаттамасын қолдана отырып жіберу;

4) деректерді қолданылуы уәкілетті органмен келісілген хаттамаларды қолдана отырып жіберу.

13. Ақпараттық алмасу барысында алынған ақпарат тек қана киберқауіпсіздіктің оқыс оқиғаларына ден қоюды үйлестіру мақсатында қолданылады.

14. Хабарламалар КҰҰО мен ККҚО арасында КҰҰО платформасын және отандық шифрлау сертификатын пайдалана отырып жүзеге асырылады.

15. ККҚО КҰҰО-ға байланыс деректерін жолдайды (электрондық пошта мекенжайы, 24/7/365 режимінде қолжетімді телефон), сонымен қатар әр тоқсан сайын, тоқсанның бірінші айының 10-ынан кешіктірмей байланыс деректерін растайды, жаңартады және жібереді. Байланыс деректері өзгерген жағдайда КҰҰО-ны жедел хабардар етеді.

16. ККО тоқсан сайын, есепті тоқсаннан кейінгі айдың 10-на дейін КҰҰО-ға есепті тоқсанда тіркелген киберқауіпсіздіктің оқыс оқиғалары және олардың туындау себептерін жою үшін қолданылған шаралар туралы ақпаратты береді.

Киберқауіпсіздікті қамтамасыз
ету орталықтары,
киберқауіпсіздіктің салалық
орталықтары мен
Киберқауіпсіздіктің ұлттық
үйлестіру орталығы арасында
киберқауіпсіздікті қамтамасыз
ету үшін қажетті ақпарат алмасу
қағидаларының
қосымшасы
Нысан

Киберқауіпсіздік оқыс оқиғасының карточкасы

Киберқауіпсіздіктің оқыс оқиғасы тіркелген күні	
Киберқауіпсіздік оқыс оқиғасының маңыздылық деңгейі	Жоғары (4); Орташа (3); Төмен (2); Анықталмаған (1).
Киберқауіпсіздік оқыс оқиғасының түрі	Қызмет көрсетуден бас тарту (DoS, DDoS) ; Рұқсатсыз қол жеткізу және мазмұнды түрлендіру; Ботнет; Вирустық шабуыл; Шифрлаушы; Осалдықты пайдалану; Аутентификация/авторизация құралдарының жария етілуі; Фишинг; Спам; Өзге ақпараттық қауіпсіздіктің оқыс оқиғалары.
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.
Киберқауіпсіздік оқыс оқиғасының сипаты	
Салдары	Салдары жоқ; Жұмысқа қабілеттілігінің бұзылуы;

	Тұтастығының бұзылуы; Ақпараттың құпиялылық режимінің бұзылуы
Зиян келтірілген объект	
Киберқауіпсіздіктің оқыс оқиғасын жою үшін қолданылған әрекеттер	
Ескертпе	

Киберқауіпсіздік оқыс оқиғасының маңыздылық деңгейлері

Маңыздылық деңгей	Белгілері	Киберқауіпсіздік оқыс оқиғаларының үлгілері
Жоғары (4)	қызметтерді көрсету/жұмыстарды орындау мүмкіндігіне және (немесе) аса маңызды деректердің жоғалуына/түрленуіне және (немесе) аса маңызды деректерді өңдейтін цифрлық объектінің құпиялылығының бұзылуына әкеп соғатын киберқауіпсіздіктің оқыс оқиғалары.	-Рұқсатсыз қол жеткізу -Осалдықты пайдалану -Шифрлаушы -Зиянды бағдарламалық қамтылым -Қызмет көрсетуден бас тарту (DoS/ DDoS шабуылы) - Өзге ақпараттық қауіпсіздіктің оқыс оқиғалары
Орташа (3)	қызметтер көрсетуді/жұмыстарды орындауды елеулі шектеуге және (немесе) аса маңызды болып табылмайтын деректердің жоғалуына/түрленуіне және (немесе) аса маңызды болып табылмайтын деректерді өңдейтін цифрлық объектінің құпиялылығының бұзылуына әкелетін киберқауіпсіздіктің оқыс оқиғалары.	-Рұқсатсыз қол жеткізу -Шифрлаушы -Зиянды бағдарламалық қамтылым Қызмет көрсетуден бас тарту (DoS/DDoS шабуылы) -Осалдықты пайдалану - Өзге ақпараттық қауіпсіздіктің оқыс оқиғалары
Төмен (2)	қызметтерді көрсетуге/ жұмыстарды орындауға әсер етпейтін киберқауіпсіздіктің оқыс оқиғалары.	-Зиянды бағдарламалық қамтылым Қызмет көрсетуден бас тарту (DoS /DdoS шабуылы) -Осалдықты пайдалану -Спам -Фишингтік шабуыл - Өзге ақпараттық қауіпсіздіктің оқыс оқиғалары
Анықталмаған (1) *	киберқауіпсіздік оқыс оқиғасының қызметтерді көрсетуге әсері анықталмаған	Сипатқа ие емес/күдікті белсенділік

Ескертпе:

* Киберқауіпсіздіктің оқыс оқиғасы расталған сәттен бастап 48 (қырық сегіз) сағат ішінде деңгейді қайта қарау қажет.

© 2012. Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» ШЖҚ РМК