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 Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 11 мамырда № 16886 болып тіркелді

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 7-1-бабының 19) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары бекітілсін.

2. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелген күнінен бастап күнтізбелік он күн ішінде оның қазақ және орыс тілдеріндегі қағаз және электрондық түрдегі көшірмелерін Қазақстан Республикасы Нормативтік құқықтық актілерінің эталондық бақылау банкіне ресми жариялау және енгізу үшін "Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

3) осы бұйрық мемлекеттік тіркелгеннен кейін күнтізбелік он күн ішінде оның көшірмесін мерзімді баспа басылымдарына ресми жариялауға жіберуді;

4) осы бұйрық ресми жарияланғаннан кейін оны Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің ресми интернет-ресурсында орналастыруды;

5) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Заң департаментіне осы тармақтың 1), 2), 3) және 4) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер беруді қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

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

Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрі	*Б. Атамқұлов*

	Қазақстан Республикасы Қорғаныс және аэроғарыш

	өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығымен бекітілген

Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпараталмасу қағидалары 1-тарау. Жалпы ережелер

1. Осы Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидалары (бұдан әрі – Қағидалар) "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 7-1-бабының 19) тармақшасына сәйкес әзірленді және Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығының ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтарымен ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу мен ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою кезіндегі өзара іс-қимыл тәртібін айқындайды.

2. Осы Қағидаларда мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы (бұдан әрі – АҚҰҮО) – Қазақстан Республикасы Ұлттық қауіпсіздік комитетінің "Мемлекеттік техникалық қызмет" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнының құрылымдық бөлімшесі;

2) ақпараттық қауіпсіздіктің жедел орталығы (бұдан әрі – АҚЖО) – электрондық ақпараттық ресурстарды, ақпараттық жүйелерді, телекоммуникация желілері мен ақпараттандырудың басқа да объектілерін қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі;

3) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – ақпараттық қауіпсіздік) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі ;

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

5) ақпараттық қауіпсіздік оқиғасы – ақпараттандыру объектілерінің қазіргі бар қауіпсіздік саясатын ықтимал бұзу туралы не ақпараттандыру объектілерінің қауіпсіздігіне қатысы болуы мүмкін, бұрын белгісіз болған жағдай туралы куәландыратын жай-күйі;

6) ақпараттық қауіпсіздіктің оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жекелей немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қатер төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшірмесін түсіріп алу, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын іркілістер;

7) ақпараттық қауіпсіздіктің қатері – ақпараттандыру объектісінің құпиялығына, тұтастығына және қолжетімділігіне жағымсыз әсер ете алатын іс-қимылдар;

8) 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;

9) осалдық – бағдарламалық қамтылымда жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын заңсыз іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық қамтылымдағы кемшілік.

2-тарау. Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қаупсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу тәртібі

3. Ақпараттық қауіпсіздікті қамтамасыз етуге қажетті ақпараттық алмасудың қатысушылары :

1) ұлттық қауіпсіздік органдары;

2) уәкілетті орган;

3) АҚҰҰО;

4) АҚЖО болып табылады.

4. АҚЖО және АҚҰҰО ақпараттық қауіпсіздік саласындағы өздеріне жүктелген міндеттер мен функцияларды жүзеге асыруға қажетті ақпарат алмасады.

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

6. АҚЖО және АҚҰҰО алмасатын ақпарат және алмасу тәртібі өкілеттіліктерді жүзере асыруға, сондай-ақ олардың құрылымдық бөлімшелерінің қызметін үйлестіруді қамтамасыз етуге жәрдемдеседі.

7. АҚЖО және АҚҰҰО:

1) ақпараттық қауіпсіздікті бұзудың алдын алу механизмдерін жетілдіруге;

2) АҚЖО қызметін жақсартуға;

3) АҚЖО мен АҚҰҰО арасындағы іс-әрекеттің келісімділігі мен жеделдігін арттыруға;

4) ақпараттандыру объектілерінің ақпараттық қауіпсіздік деңгейін арттыру бойынша бірлескен шешімдер әзірлеуге бағытталған міндеттерді шешу мүддесінде өзара іс-қимылды жүзеге асыруы қажет.

8. Ақпараттық қауіпсіздікті қамтамасыз етуге қажетті ақпарат құпия электрондық ақпраттық деректер санатына жатады, оларды алу, өңдеу және қолдану олар жиналатын мақсаттармен шектелген. АҚҰҰО-дан АҚЖО-ға және АҚЖО-дан АҚҰҰО-ға ақпараттық қауіпсіздік оқыс оқиғалары туралы мәлімет жолдау осы Қағидалар шеңберінде жүзеге асырылады.

9. АҚЖО АҚҰҰО-ға ақпараттық қауіпсіздік оқыс оқиғалары туралы ақпаратты анықталған сәттен бастап 15 минут аралығында жолдайды.

10. Деректерді жинау мынадай жағдайларда жүзеге асырылады:

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

2) ақпараттық қауіпсіздіктің оқыс оқиғасы электрондық ақпараттық ресурстардың, ақпараттық жүйелердің, телекоммуникация желілерінің және өзге ақпараттандыру объектілерінің жұмыс істеу қабілетіне әсер ете алады деп ойлауға негіз болған кезде;

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

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

5) ақпараттық қауіпсіздік оқыс оқиғаларының әсерін жою кезіндегі көмек көрсету кезінде .

11. АҚҰҰО-ның сұратуы бойынша АҚЖО АҚҰҰО-ға қолда бар ақпараттық қауіпсіздікті қамтамасыз етудің мониторингі жүйелеріне қолжетімділікті қамтамасыз етеді.

12. АҚҰҰО мүдделі тараптарды хабарландырады:

1) өздеріне қатысты ақпарат бөлігінде АҚЖО-ны – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің, телекоммуникация желілерінің және өзге ақпараттандыру объектілерінің жұмыс істеу қабілетіне әсер ете алатын ақпараттық қауіпсіздік оқыс оқиғасы жағдайында;

2) ұлттық қауіпсіздік органдарын – электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және өзге ақпараттандыру объектілері мен байланысты ақпараттық қауіпсіздік оқыс оқиғасы жағдайында;

3) уәкілетті органды – ақпараттық қауіпсіздік саласындағы заңнама бұзылған жағдайда;

4) Қазақстан Республикасының ақпараттандыру саласындағы уәкілетті органын – ақпараттандыру саласындағы заңнама бұзылған жағдайда;

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

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

13. Ақпараттық алмасу мынадай тәсілдермен жүзеге асырылады:

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

2) деректерді ақпарат алмасуға арналған бағдарламалық қамтылымды қолдана отырып XML немесе JSON пішіндерін дежіберу;

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

Ақпараттық қауіпсіздік оқыс оқиғасының карточкасы осы Қағидалардың 1-қосымшасына сәйкес нысан бойынша беріледі.

Осалдықтар туралы деректер карточкасы осы Қағидалардың 2-қосымшасына сәйкес нысан бойынша беріледі.

14. Электрондық хабарламаларда Қазақстан Республикасының заңнамасына сәйкес рұқсаты шектелген ақпарттың қамтылуына жол берілмейді.

15. Ақпараттық алмасу барысында алынған ақпарат тек қана ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюды үйлестіру мақсатында қолданылады.

16. АҚҰҰО мен АҚЖО арасындағы электрондық хабарламалармен тікелей алмасу электрондық хабарламалардың жеткізілу кепілдігін қамтамасыз ететін және берілетін деректерді көліктік деңгейде қорғайтын жүйелерді қолдану мен жүзеге асырылады.

17. АҚЖО АҚҰҰО-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 АҚҰҰО-ны дереу хабардар етеді.

	Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларына 1-қосымша Нысан

Ақпараттық қауіпсіздік оқыс оқиғасының карточкасы

Оқыс оқиғаны тіркеу күні	
Маңыздылық деңгейі*	Деңгей 5 Деңгей 4 Деңгей 3 Деңгей 2 Деңгей 1 Деңгей 0
Оқыс оқиға типі	Қызмет көрсетуден бас тарту (DoS, DDoS) Заңсыз қолжетімділік және құрамын модификациялау Ботнет Вирустық шабуыл Осалдықтарды пайдалану Құралдарды бұрмалау Аутентификация/авторландыру құралдарын компрометациялау Фишинг Басқа
Ауқымы	Жеке Жаппай
Детальдар	Туындау күні мен уақыты Анықтау күні мен уақыты Хабарлау күні мен уақыты Оқиғааяқталдыма? "иә" болса, күн/сағат/минут өлшемінде қанша ұзақ созылғанын дәлдеу Қайтадан/жаңадан Компрометация индикаторы (IOC)
Белгілер	Нақты Әрекет Күдік
Көз	Ішкі контур Сыртқы контур
Оқыс оқиға сипаттамасы	
Зардабы	Зардапсыз Жұмыс қабілеттілігінің бұзылуы Тұтастықтың бұзылуы Ақпараттың құпиялық режимінің бұзылуы
Залал тиген объект	
Оқыс оқиғаны шешу үшін қолданылған іс-қимылдар	
Ескертпе	

* Ескертпе: Ақпараттық қауіпсіздік оқыс оқиғасының маңыздылық деңгейі

Маңыздылық деңгейі		Анықтама
Маңызды	Деңгей 5	Қызмет көрсету мүмкіндігін жоятын, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпаратандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын, айналып өту мүмкін емес оқыс оқиғалар

Елеулі	Деңгей 4	Қызмет көрсету мүмкіндігін жоятын, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын ықтимал оқыс оқиғалар.
Жоғары	Деңгей 3	Қызмет көрсету мүмкіндігін айтарлықтай шектейтін, жағдайдың айтарлықтай нашарлауына, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын ықтимал оқыс оқиғалар.
Орташа	Деңгей 2	Қызмет көрсету мүмкіндігін шектейтін, жағдайдың айтарлықтай нашарлауына, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкеп соғатын, болуы мүмкін оқыс оқиғалар.
Төмен	Деңгей 1	Қызмет көрсету мүмкіндігін шектейтін, жағдайдың нашарлауына, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері және басқа ақпараттандыру объектілері үшін елеусіз теріс салдарға әкеп соғатын, болуы екіталай оқыс оқиғалар.
Маңызды емес	Деңгей 0	Электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және басқа ақпараттандыру объектілеріне әсер етпейтін елеусіз оқыс оқиғалар.

	Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпарат алмасу қағидаларына 2-қосымша Нысан

Осалдықтар туралы деректер карточкасы

Осалдықты анықтау күні мен уақыты	Контур	Осалдықтың маңыз дылық деңгейі	Ресурс атауы/ IP мекенжай	Инфрақұрылым объектісі (атауы, ip, hostname және т.б.)	Порт	Осалдық сипаттамасы	Ұсыныс сипаттамасы	Қосымша ақпарат
	Сыртқы /Ішкі контур							