Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтеріне, ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексерулер жүргізуге қойылатын талаптарды бекіту туралы

Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2020 жылғы 21 қыркүйектегі № 90 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2020 жылғы 25 қыркүйекте № 21274 болып тіркелді.

ЗҚАИ-ның ескертпесі!

Осы қаулы 01.01.2021 бастап қолданысқа енгізіледі

"Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" 2003 жылғы 4 шілдедегі Қазақстан Республикасы Заңының 13-6-бабы бірінші бөлігінің 4) тармақшасына сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Қоса беріліп отырған Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтеріне, ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексерулер жүргізуге қойылатын талаптар бекітілсін.

2. Киберқауіпсіздік басқармасы Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) Заң департаментімен бірлесіп осы қаулыны Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы қаулыны ресми жарияланғаннан кейін Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің ресми интернет-ресурсына орналастыруды;

3) осы қаулы мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Заң департаментіне осы тармақтың 2) тармақшасында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Осы қаулының орындалуын бақылау Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Төрағасының жетекшілік ететін орынбасарына жүктелсін.

4. Осы қаулы 2021 жылғы 1 қаңтардан бастап қолданысқа енгізіледі және ресми жариялануға тиіс.

Қазақстан Республикасының
Қаржы нарығын реттеу және
дамыту Агенттігінің Төрағасы *М. Абылкасымова*

Қазақстан Республикасының
Қаржы нарығын реттеу және
дамыту агенттігі
Басқармасының

2020 жылғы 21 қыркүйегі
№ 90 қаулысымен
бекітілген

Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтеріне, ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексерулер жүргізуге қойылатын талаптар

1-тарау. Жалпы ережелер

1. Осы Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтеріне, ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексерулер жүргізуге қойылатын талаптар (бұдан әрі – Талаптар) "Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" 2003 жылғы 4 шілдедегі Қазақстан Республикасының Заңына тармақшасына сәйкес әзірленді және екінші деңгейдегі банктер және Қазақстан Республикасы бейрезидент-банктерінің филиалдары (бұдан әрі – банк) мен банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың (бұдан әрі – ұйым) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметтеріне, ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексерулер жүргізуге қойылатын талаптарды белгілейді.

Ескерту. 1-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 17.02.2021 № 34 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

2. Талаптарда "Ақпараттандыру туралы" Қазақстан Республикасының Заңында және Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16772 болып тіркелген "Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы" Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысында көзделген ұғымдар, сондай-ақ мынадай ұғымдар пайдаланылады:

1) ақпараттық қауіпсіздік оқиғаларын ретроспективтік талдау – ақпараттық қауіпсіздіктің бұрын байқалған оқыс оқиғаларын және (немесе) онымен байланысты ақпараттық қауіпсіздіктің қауіп-қатерлерін анықтау мақсатында компрометацияның жаңартылған индикаторлары және ақпараттық қауіпсіздіктің маңызды қауіп-қатерлері жөнінде өзге де мәліметтердің негізінде кемінде үш ай уақыт аралығы үшін ақпараттық қауіпсіздік оқиғаларын мониторингтеу барысында алынған деректер жиынтығын талдау;

2) ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексеру – ақпараттық қауіпсіздіктің оқыс оқиғасының туындау, ақпараттық қауіпсіздіктің оқыс оқиғасының

іске асырылу тәртібінің себептері мен алғышарттарын белгілеу, ақпараттық қауіпсіздіктің оқыс оқиғасының іске асырылуының әсер ету ауқымын және одан болған шығынды бағалау, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою үшін қабылданған шаралардың тиімділігін талдау мақсатында банктің, ұйымның қызметкерлері және үшінші тұлғалар жүзеге асыратын процесс;

3) ден қоюдың стандартты рәсімі – ақпараттық қауіпсіздіктің оқыс-оқиғасын оқшаулау бойынша шұғыл шаралар қолдану тәртібі, оның туындау ықтималдылығы қысқа мерзімде ақпараттық қауіпсіздіктің оқыс оқиғасының туындау тәуекелін төмендету мүмкіндігінсіз жоғары;

4) компрометация индикаторы – объектінің электрондық тасымалдағыштардағы немесе желілік трафиктегі энергияға тәуелді жадыда байқалатын, құрылғының компрометациясына үлкен ықтималдылық үлесіпен көрсететін бірегей сипаттамасы;

5) осалдық – ақпараттық жүйенің немесе оның жекелеген элементтерінің жетіспеушілігі, оны пайдалану ақпараттық жүйенің тұтастығын және (немесе) конфиденциалдылығы және (немесе) қолжетімділігін бұзуға әкеледі.

Ескерту. 2-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 27.11.2023 № 86 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

3. Банк, ұйым ақпараттық қауіпсіздіктің оқыс-оқиғаларына ден қою жөніндегі құрылымдық бөлімшені – ақпараттық қауіпсіздіктің оқыс-оқиғаларына ден қою қызметін (бұдан әрі – ден қою қызметі) құруды қамтамасыз етеді.

4. Ден қою қызметінің тиісінше жұмыс істеуі мақсатында банк, ұйым:

1) ақпараттық қауіпсіздік оқиғаларын мониторингтеу және ақпараттық қауіпсіздіктің оқыс-оқиғаларына ден қою процестерін автоматтандыратын бағдарламалық-техникалық құралдарды енгізуді, тиісінше жұмыс істеуін;

2) қабылданған шараларды, ақпараттық қауіпсіздік оқиғаларының көздерін, ақпараттық қауіпсіздік оқиғаларын мониторингтеу кезеңділігін, тәртібі мен әдістерін белгілей отырып, оларға ден қою қызметі міндетті түрде дереу ден қоюды талап ететін ақпараттық қауіпсіздік оқиғаларының тізбесін және (немесе) оқиғалар жиынтығын (бұдан әрі – ақпараттық қауіпсіздік оқиғаларының тізбесі) айқындауды;

3) ақпараттық қауіпсіздік оқиғаларын ақпараттық қауіпсіздіктің оқыс оқиғаларына жатқызу, оларды жіктеу және басымдық беру тәртібін айқындауды;

4) ден қоюдың стандартты рәсімдерін әзірлеу, өзекті жағдайда қолдау және ден қою қызметінің қызметкерлерін ден қоюдың стандартты рәсімдерін қолдану мәселелері бойынша оқытуды;

5) банктің, ұйымның басшы қызметкерлерін, банктің, ұйымның және қаржы нарығын және қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті

органның (бұдан әрі – уәкілетті орган) бөлімшелерін, оның ішінде ақпараттық қауіпсіздіктің оқыс-оқиғасына ішкі тергеп-тексерулер жүргізу туралы шешім қабылдау үшін ақпараттандыру тәртібін айқындауды;

6) ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді, ақпараттық қауіпсіздіктің оқыс оқиғаларының ішкі тергеп-тексерулер нәтижелері туралы ақпаратты және осы тергеп-тексерулердің материалдарын қоса алғанда, ақпараттық қауіпсіздіктің оқыс-оқиғалары туралы ақпаратты есепке алу, сақтау, тұтастығы мен сақталуын қамтамасыз ету тәртібін айқындауды;

7) ақпараттық қауіпсіздіктің оқыс-оқиғаларына ден қою процесіне тартылған банктің, ұйымның жауапты қызметкерлерін және (немесе) бөлімшелерін айқындауды;

8) ақпараттық қауіпсіздіктің оқыс оқиғаларын жою бойынша шұғыл шаралар қабылдау, ақпараттық қауіпсіздіктің оқыс оқиғаларының туындау себептері мен олардың салдарларын анықтау тәртібін айқындауды;

9) ден қою қызметіне ақпараттық қауіпсіздіктің оқыс оқиғасы анықталған жағдайда банкте, ұйымда бизнес-процесті ішінара немесе толық тоқтату бойынша қосымша бақылау шараларын енгізу жөнінде өкілеттіктер беруді;

10) ақпараттық қауіпсіздік оқиғаларының тізбесін, ақпараттық қауіпсіздік оқиғаларының көздерін, ақпараттық қауіпсіздік оқиғаларының кезеңділігін, мониторингтеу тәртібі мен әдістерін жылына кемінде бір рет қайта қарауды;

11) ақпараттық қауіпсіздік тәуекелдерін бағалау, ақпараттық қауіпсіздікті қамтамасыз етудің әдістері мен құралдарын түзету, банктің, ұйымның бизнес-процестерін өзгерту мақсатында анықталған ақпараттық қауіпсіздіктің оқыс оқиғаларын және банктің, ұйымның алқалы органының қарауы үшін олар келтірген зиянды жылына кемінде бір рет талдауды;

12) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою тәртібінің іске асырылуын растайтын құжаттардың, мәліметтер мен фактілердің болуын;

13) ден қою қызметінің банктің, ұйымның маңызды ақпараттық жүйелерінде туындайтын ақпараттық қауіпсіздік оқыс оқиғаларына ден қоюдың үздіксіздігін қамтамасыз ететін жұмыс режимін;

14) ақпараттық қауіпсіздік оқыс оқиғасының іске асырылу салдарынан банкке, ұйымға және (немесе) банктің, ұйымның клиенттеріне материалдық залал келтірілген жағдайларда, уәкілетті органды тергеп-тексеруді жүргізудің басталғаны, мерзімдері және нәтижелері туралы хабардар ете отырып, ақпараттық қауіпсіздіктің оқыс оқиғасына ішкі тергеп-тексеру жүргізуді қамтамасыз етеді.

Ескерту. 4-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 23.11.2022 № 95 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

5. Ден қою қызметінің ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою тәртібі банктің, ұйымның ішкі құжаттарымен белгіленеді және олармен шектелмей, қоса алғанда, мынадай кезеңдерден тұрады:

1) ақпараттық қауіпсіздік оқиғаларының мониторингі және ақпараттық қауіпсіздіктің оқыс оқиғаларын анықтау (бұдан әрі – мониторингтеу және анықтау кезеңі);

2) ақпараттық қауіпсіздіктің оқыс оқиғасын оқшаулау және оған қарсы іс-қимыл (бұдан әрі – ден қою кезеңі);

3) ақпараттық қауіпсіздіктің оқыс оқиғасын ішкі тергеп-тексеру (бұдан әрі – ішкі тергеп-тексеру кезеңі).

6. Ден қою қызметінің жекелеген функциялары тысқары ұйымға-заңды тұлғаға берілген жағдайда банк, ұйым Талаптардың орындалуын, оның ішінде үшінші тұлғалармен жасалатын қызметтер көрсету шарттарына Талаптардың тиісті нормаларын енгізу жолымен қамтамасыз етеді.

2-тарау. Ден қою қызметтеріне қойылатын талаптар

7. Мониторинг және анықтау сатысында ден қою қызметі мыналарды:

1) ақпараттық қауіпсіздік оқиғаларының мониторингі және талдауын;

2) ақпараттық қауіпсіздік оқиғаларын ақпараттық қауіпсіздік оқыс оқиғасына ақпараттық қауіпсіздіктің оқиғаларын ақпараттық қауіпсіздік оқыс оқиғаларына жатқызудың әзірленген тәртібіне сәйкес жатқызуды;

3) ақпараттық қауіпсіздік оқыс оқиғаларын жіктеу және басымдылығын айқындауды;

4) ақпараттық қауіпсіздік оқыс оқиғасы туралы ақпаратты ден қою сатысына тапсыруды жүзеге асырады.

8. Ақпараттық қауіпсіздік оқыс оқиғаларына ден қою сатысында ден қою қызметі ден қоюдың стандартты рәсімдерін қолданады, ал ден қоюдың стандартты рәсімдерін қолданудың тиімділігі төмен болған жағдайда ақпараттық қауіпсіздік оқыс оқиғаларына ден қоюдың мынадай, бірақ олармен шектелмейтін шаралары кіретін жедел ден қою шараларын қабылдайды:

1) ақпараттық қауіпсіздік оқыс оқиғасына тиімді қарсы іс-қимыл процесін қамтамасыз ету мақсатында банктің, ұйымның қызметкерлерін, сондай-ақ үшінші тұлғаларды ақпараттандыру және тарту;

2) бизнес-процесстің иелерімен келісім бойынша банкте, ұйымда бизнес-процессті ішінара немесе толық тоқтату бойынша қосымша шаралар қабылдау;

3) ақпараттық қауіпсіздік оқыс оқиғасына тартылған бағдарламалық-техникалық құралдардан деректер жинау;

4) ақпараттық қауіпсіздік оқыс оқиғасын талдау, оны тежеу және оның салдарын жою;

5) ақпараттық қауіпсіздік оқиғаларын ретроспективті талдау;

6) ақпараттық қауіпсіздік оқыс оқиғаларына ден қою барысында анықталған ымыраға келу және осалдықтардың индикаторларын айқындау және бұдан былай ұқсас ақпараттық қауіпсіздік оқыс оқиғасына жол бермеуге бағытталған түзету шараларын іске асыру;

7) ақпараттық қауіпсіздік оқыс оқиғасына ішкі тергеу жүргізу қажеттілігі туралы шешім қабылдау.

Ескерту. 8-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 27.11.2023 № 86 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

9. Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 29639 болып тіркелген Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2022 жылғы 12 қыркүйектегі № 67 қаулысымен бекітілген Қаржы ұйымдарының қаржы нарығы мен қаржы ұйымдарының ақпараттық қауіпсіздіктің салалық орталығы пайдаланатын ақпараттық қауіпсіздіктің оқиғалары мен оқыс оқиғалары бойынша ақпарат жинау, өңдеу және алмасу жөніндегі ақпараттандыру объектісін қосу және пайдалану қағидаларының 12-тармағына сәйкес көрсетілген ақпаратты уәкілетті органның ақпараттық қауіпсіздік оқиғалары мен инциденттері бойынша ақпаратты өңдеудің автоматтандырылған жүйесіне енгізе отырып, ден қою қызметі ақпараттық қауіпсіздіктің оқыс оқиғасы, қабылданған шаралар және ұсынылатын түзету шаралары туралы ақпаратты көрсетумен, ақпараттық қауіпсіздіктің оқыс оқиғаларын есепке алу журналында ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты қағаз тасымалдағышта не электрондық түрде шоғырландыруды, жүйелендіруді, сақтауды, оның тұтастығын және сақталуын қамтамасыз етеді.

Ескерту. 9-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 27.11.2023 № 86 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

10. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты сақтау мерзімі кемінде 5 (бес) жыл құрайды.

3-тарау. Ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеп-тексерулер жүргізуге қойылатын талаптар

11. Банк, ұйым ақпараттық қауіпсіздіктің оқыс оқиғасын ішкі тергеп-тексеру кезеңінде мыналарды қамтамасыз етеді:

1) ақпараттық қауіпсіздіктің оқыс оқиғасын ішкі тергеп-тексеруге ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесіне тартылған банктің, ұйымның жауапты қызметкерлерін және (немесе) бөлімшелерін, сондай-ақ үшінші тұлғаларды тарту;

2) ақпараттық қауіпсіздіктің оқыс оқиғасына ішкі тексеру жүргізу үшін қажетті материалдарды жинау және талдау;

3) ақпараттық қауіпсіздіктің оқыс оқиғасының туындау себептерін және ақпараттық қауіпсіздіктің оқыс оқиғасын тарату тәртібін белгілеу;

4) ақпараттық қауіпсіздіктің оқыс оқиғасын таратудан болған әсері мен зиянның ауқымын бағалау;

5) тергеп-тексеріліп жатқан ақпараттық қауіпсіздіктің оқыс оқиғасына қабылданған ден қою шараларының тиімділігін талдау;

6) ақпараттық қауіпсіздіктің оқыс оқиғасы туралы ақпарат көрсетілетін ақпараттық қауіпсіздіктің оқыс оқиғасын тергеп-тексеру нәтижелері туралы қорытынды, сондай-ақ ақпараттық қауіпсіздіктің оқыс оқиғасын қайта таратудан зиян ықтималдығы мен болу мүмкіндігін азайту мақсатында түзету шараларын қабылдау бойынша ұсынымдар дайындау.

12. Банк, ұйым банктің, ұйымның ішкі құжаттарына сәйкес ақпараттық қауіпсіздіктің оқыс оқиғасын тергеп-тексеру нәтижелері туралы банктің, ұйымның басшы қызметкерлерін, уәкілетті органды, сондай-ақ қажет болған кезде банктің, ұйымның басқа бөлімшелерінің өкілдерін хабардар етеді.

13. Банк, ұйым ақпараттық қауіпсіздіктің оқыс оқиғасын ішкі тергеп-тексеру нәтижелері туралы ақпаратты және тергеп-тексеру материалдарын қағаз тасымалдағышта және (немесе) электрондық түрде шоғырландыруды, жүйелендіруді, оның тұтастығын және сақталуын қамтамасыз етеді.

14. Ақпараттық қауіпсіздіктің оқыс оқиғасын ішкі тергеп-тексеру нәтижелері туралы ақпаратты және тергеп-тексеру материалдарын сақтау мерзімі кемінде 5 (бес) жыл құрайды.