Қазақстан Республикасының Қаржы нарығын реттеу мен дамыту агенттігі

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2020 жылғы 23 қарашадағы № 111 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2020 жылғы 27 қарашада № 21686 болып тіркелді

Агентство Республики Казахстан по регулированию и развитию финансового рынка

Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесін бекіту туралы

Ескерту. 01.01.2021 бастап қолданысқа енгізіледі – осы қаулының 4-тармағымен.

«Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы» 2003 жылғы 4 шілдедегі Қазақстан Республикасының Заңының 13-6-бабы бірінші бөлігінің 2) тармақшасына сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы **ҚАУЛЫ ЕТЕДІ**:

1. Қоса беріліп отырған Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі 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-шараның орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Осы қаулының орындалуын бақылау Қазақстан Республикасының 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 Агенттігінің Басқармасының
2020 жылғы 23 қарашасы № 111
Қаулысымен бекітілді

Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі

1-тарау. Жалпы ережелер

1. Осы Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі (бұдан әрі – Әдістеме) «Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы» 2003 жылғы 4 шілдедегі Қазақстан Республикасының Заңына сәйкес әзірленді және ақпараттық қауіпсіздік тәуекелдерін бағалау жөніндегі талаптар қойылатын қаржы ұйымдарында және Қазақстан Республикасының бейрезидент-банктерінің филиалдарында, Қазақстан Республикасының бейрезидент-сақтандыру (қайта сақтандыру) ұйымдарының филиалдарында, Қазақстан Республикасының бейрезидент-сақтандыру брокерлерінің филиалдарында (бұдан әрі – қаржы ұйымдары) ақпараттық қауіпсіздік тәуекелдерін бағалау процесін ұйымдастыру мақсатында, қаржы ұйымдарында ақпараттық қауіпсіздік тәуекелдерін өңдеу кезінде іске қосылған ресурстардың басымдықтарын айқындау және оңтайландыру үшін қолданылады.

2. Әдістемеде мынадай ұғымдар пайдаланылады:

1) ақпараттық активтің бизнес-иесі – жұмыс істеу циклін қамтамасыз ету үшін ақпараттық актив пайдаланылатын негізі бизнес-процестің иесі;

2) ақпараттық қауіпсіздік қатері – ақпараттық қауіпсіздіктің оқыс оқиғаларының пайда болуының алғышарттарын туындататын жағдайлардың және факторлардың жиынтығы;

3) ақпараттық қауіпсіздік тәуекелі – конфиденциалдылықты бұзу, активтердің тұтастығын немесе қолжетімділігін қасақана бұзу салдарынан зиянның пайда болу ықтималдығы;

4) ақпараттық қауіпсіздік тәуекелінің деңгейі – оқиғаның және оның салдарының ықтималдылығының комбинациясы;

5) ақпараттық қауіпсіздіктің бұзылуынан болған залалдың маңыздылық деңгейі – қаржы ұйымында ақпараттық қауіпсіздіктің бұзылуынан болған залалдың артып кетуі жекелеген ақпараттық актив бойынша қаржы ұйымы үшін қолайлы болмайтын деңгейі;

6) маңызды ақпараттық актив – 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 қаулысына сәйкес айқындалатын ақпараттық актив.

Ескерту. 2-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.04.2022 № 30 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

3. Ақпараттық қауіпсіздік тәуекелдерін бағалау үшін қаржы ұйымы мынадай іс-шаралар жүргізіледі:

1) маңызды ақпараттық активтердің тізбесін қалыптастыру;

2) маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелдерін бағалау.

2-тарау. Маңызды ақпараттық активтер тізбесін қалыптастыру

4. Маңызды ақпараттық активтердің тізбесін қалыптастыру және одан әрі маңызын арттыру мақсатында қаржы ұйымдары мынадай процестерді іске асыруды қамтамасыз етеді:

1) қаржы ұйымының ақпараттық қауіпсіздігін басқару жүйесінің қолдану аясына кіретін бизнес-процестерді талдау;

2) ақпараттық активтердің ақпараттық қауіпсіздігінің қасиеттерін (конфиденциалдылығы, тұтастығы және қолжетімділігі) бұзудан болған әлеуетті зиянды анықтау;

3) маңызды ақпараттық активтердің тізбесін қалыптастыру және одан әрі маңызын арттыру.

5. Қаржы ұйымының ақпараттық қауіпсіздігінің басқару жүйесінің қолдану аясына кіретін бизнес-процестерді талдауды қаржы ұйымының бизнес-процестерінің иелері-бөлімшелері бизнес-процестердің жұмыс істеуі үшін қажетті ақпараттық активтерді идентификаттау мақсатында қаржы ұйымының тәуекелдерді басқару бөлімшесінің басшылығымен жүзеге асырады. Идентификатталатын ақпараттық активтердің түрлері Әдістемеге 1-қосымшаға сәйкес ақпараттық активтер түрлерінің тізбесі бойынша айқындалады.

Ақпараттық активтерді идентификаттау үшін қаржы ұйымының бизнес-процесінің иесі бөлімшесінің шешімі бойынша қаржы ұйымының ақпараттық технологиялар бөлімшесі тартылады.

6. Әрбір идентификатталған ақпараттық актив бойынша қаржы ұйымы ақпараттық қауіпсіздікті бұзудан болған әлеуметтік зиянның мынадай түрлерін айқындайды:

1) ақпараттық активтің конфиденциалдығын бұзудан болған зиян;

2) ақпараттық активтің тұтастығын бұзудан болған зиян;

3) ақпараттық активтің қолжетімділігін бұзудан болған зиян.

Ақпараттық активтердің бизнес-иелері қаржы ұйымының тәуекелдерді басқару бөлімшесінің басшылығымен зиянды анықтайды.

7. Ақпараттық активтердің ақпараттық қауіпсіздігінің бұзылуынан болған әлеуетті зиянды бағалау үшін қаржы ұйымы зиянды бағалауға:

1) қаржы ұйымының ақпараттық активтерді пайдаланатын бизнес-процестерге сәйкес кәсіби қызметті регламенттейтін ішкі құжаттарын;

2) ақпараттық активтерді пайдаланатын бизнес-процестер, сондай-ақ ақпараттық активтермен жұмыс процестерін;

3) Әдістеменің 8-тармағында көрсетілген әлеуетті зиянның мөлшеріне ықпал ететін факторларды білетін қызметкерлердің қатысуын қамтамасыз етеді.

8. Қаржы ұйымының ақпараттық активтің құпиялылығын, тұтастығын және қолжетімділігін бұзудан болатын ықтимал зияндарды айқындауы мынадай факторларды ескере отырып жүзеге асырылады:

1) қаржы ұйымындағы бизнес - процестердің өмірлік цикліне бұзушылықтың әсер ету дәрежесі;

2) бұзушылықтың қаржы ұйымының іскерлік беделіне әсер ету дәрежесі;

3) қаржы ұйымының ықтимал қаржылық шығындарының көлемі;

4) Қазақстан Республикасы заңнамасының, оның ішінде Қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау мен қадағалау жөніндегі уәкілетті органның (бұдан әрі – уәкілетті орган) нормативтік құқықтық актілерінің талаптарын және (немесе) қаржы ұйымының шарттық міндеттемелерін ықтимал бұзудың салдарлары;

5) ақпараттық актив өңдейтін қорғалатын маңызды ақпараттың көлемі.

9. Ақпараттық активтерді жіктеуді жүзеге асыру мақсатында қаржы ұйымының тәуекелдерді басқару жөніндегі бөлімшесі ақпараттық қауіпсіздікті бұзудан болған зияндардың маңыздылығы деңгейін белгілейді. Ақпараттық қауіпсіздікті бұзудан болған зияндардың маңыздылығы деңгейі қаржы ұйымындағы операциялық тәуекелдерге арналған тәуекел-тәбетіне және ол қаржы ұйымында болған кезде ақпараттық қауіпсіздік тәуекелдеріне арналған тәуекел-тәбетіне сәйкес айқындалады.

10. Маңызды ақпараттық активтердің тізбесін қаржы ұйымының тәуекелдерді басқару бөлімшесінің басшылығымен жұмыс тобы қалыптастырады және жаңартып отырады. Маңызды ақпараттық активтердің тізбесіне олардың ерекшеліктерін бұзудан болған зияндар ақпараттық қауіпсіздікті бұзудан болған зияндардың маңыздылығының белгіленген деңгейінен асатын ақпараттық активтер кіреді. Әрбір маңызды ақпараттық актив үшін Әдістемеге 1-қосымшаға

сәйкес Ақпараттық активтер түрлерінің тізбесіне сәйкес оның түрі мен типі, ерекшеліктерін (конфиденциалдығын, тұтастығын және (немесе) қолжетімділігін) бұзудан болған зияндар, сондай-ақ ақпараттық активтің бизнес-иесі көрсетіледі.

3-тарау. Маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелін бағалау

11. Маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелін бағалау мақсатында қаржы ұйымдары мынадай процестерді іске асыруды қамтамасыз етеді:

1) маңызды ақпараттық активтерге ақпараттық қауіпсіздік қатерлерін идентификаттау;

2) маңызды ақпараттық активтер үшін релевантты ақпараттық қауіпсіздік қатерлерінің көздерін идентификаттау;

3) маңызды ақпараттық активтердің осалдықтарын идентификаттау;

4) ақпараттық қауіпсіздік тәуекелдерін басқарудың қолданыстағы шараларын идентификаттау;

5) маңызды ақпараттық активтерге ақпараттық қауіпсіздік қатерлері көздерінің ақпараттық қауіпсіздік қатерлеріне әкеп соғу ықтималын бағалау;

6) ақпараттық қауіпсіздік тәуекелдерінің деңгейін бағалау.

12. Маңызды ақпараттық активтерге ақпараттық қауіпсіздік қатерлерін идентификаттауды қаржы ұйымының ақпараттық қауіпсіздігі жөніндегі бөлімшесі жүзеге асырады. Әрбір маңызды ақпараттық актив үшін ақпараттық қауіпсіздік қатерлеріне, оның ішінде Әдістемеге 2-қосымшаға сәйкес Ақпараттық активтерге ақпараттық қауіпсіздік қатерлерінің тізбесінде көрсетілген ақпараттық қауіпсіздік қатерлеріне талдау жасалады.

13. Маңызды ақпараттық активтер үшін орынды ақпараттық қауіпсіздік қатерлерінің көздерін идентификаттауды қаржы ұйымының ақпараттық қауіпсіздігі жөніндегі бөлімшесі Әдістеменің 10-тармағында көрсетілген маңызды ақпараттық активтер тізбесінің және Әдістеменің 12-тармағына сәйкес идентификатталған маңызды ақпараттық активтерге ақпараттық қауіпсіздік

қатерлерінің негізінде жүзеге асырады. Маңызды ақпараттық активтерге ақпараттық қауіпсіздіктің әрбір идентификатталған қатері үшін Әдістемеге 3-қосымшаға сәйкес Ақпараттық қауіпсіздік қатерлерінің үлгі көздерінің тізбесінде көрсетілген ақпараттық қауіпсіздік қатерлерінің көздерін ескере отырып, ақпараттық қауіпсіздік қатерлерінің релевантты көздеріне талдау жасалады.

14. Маңызды ақпараттық активтердің осалдықтарын идентификаттауды қаржы ұйымының ақпараттық қауіпсіздігі жөніндегі бөлімшесі Әдістеменің 10-тармағында көрсетілген маңызды ақпараттық активтер тізбесінің негізінде, мынадай ақпаратты ескере отырып жүзеге асырады:

1) ақпараттық активтің конструкциясы туралы;

2) ақпараттық активтің нақты орналасуы туралы;

3) бағдарламалық кодтағы белгілі қателер туралы;

4) конфигурациядағы қателер туралы;

5) ақпараттық активті пайдалану процесінің кемшіліктері туралы.

15. Маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелдерін басқарудың бар шараларын идентификаттауды қаржы ұйымының ақпараттық қауіпсіздік бөлімшесі Әдістеменің 10-тармағында көрсетілген маңызды ақпараттық активтердің тізбесі негізінде маңызды ақпараттық активтердің ақпараттық қауіпсіздігін қамтамасыз ету процесіндегі орын алған кемшіліктерді не оны бұзу салдарын түзетуге бағытталған ұйымдастыру және техникалық іс-шаралар туралы ақпаратты ескере отырып жүзеге асырады.

16. Ақпараттық қауіпсіздік қаупінің маңызды ақпараттық активтерге іске асу ықтималдығын ақпараттық қауіпсіздік қаупі дереккөздерімен бағалауды қаржы ұйымының ақпараттық қауіпсіздік бөлімшесі маңызды ақпараттық актив үшін ақпараттық қауіпсіздік қаупі, ақпараттық қауіпсіздік қаупі және осалдық дереккөзінің барлық релевантты комбинациялары үшін мына ақпаратты ескере отырып жүзеге асырады:

1) тиісті маңызды ақпараттық активтерге қатысты ақпараттық қауіпсіздік қаупі дереккөзінің орналасуы (ішкі немесе сырты) туралы деректер. Ақпараттық қауіпсіздік қаупінің ішкі дереккөздері үшін активті пайдаланушылар саны, ақпараттық қауіпсіздік қаупінің сыртқы дереккөздері үшін қорғау өлшемінен тыс ықтимал кіру рұқсатының болуы;

2) ақпараттық қауіпсіздік қаупі дереккөзіне кіру рұқсатының деңгейі туралы деректер;

3) ақпараттық қауіпсіздік қаупінің бұрын маңызды ақпараттық активке іске асу жиілігі туралы статистикалық деректер;

4) ақпараттық қауіпсіздік қаупінің маңызды ақпараттық активке іске асуының күрделілігі туралы ақпарат;

5) қарастырылып отырған маңызды ақпараттық активтерде қорғау шараларының бар болуы туралы деректер.

17. Ақпараттық қауіпсіздік қаупінің маңызды ақпараттық активтерге іске асу ықтималдығын бағалауға ақпараттық қауіпсіздік қаупінің дереккөздері бірнеше сарапшыларды тартқан және түрлі бағалар алған кезде анағұрлым ықтималдықты айқындайтын бағаға тең жинақталған жиынтық баға қабылданады.

18. Ақпараттық қауіпсіздік тәуекелдері деңгейін бағалау ақпараттық қауіпсіздік қаупінің маңызды ақпараттық активтерге іске асу ықтималдығын ақпараттық қауіпсіздік дереккөздерімен бағалауды және маңызды ақпараттық активтердің конфиденциалдығы, тұтастығы немесе қолжетімділігі бұзылуынан тиісті әлеуетті шығындарды бағалауды салыстыру негізінде жүргізіледі.

4-тарау. Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау

19. Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралауды уәкілетті орган мынадай көрсеткіштер бойынша жүзеге асырады:

1) ықтимал залалдардың көрсеткіші, ол қаржылық ұйымның барлық маңызды ақпараттық активтерінің конфиденциалдылықты, тұтастықты және қолжетімділігін бұзудан болатын ықтимал залалдардың жалпы сомасы ретінде айқындалады;

2) маңызды ақпараттық активтер үлесінің көрсеткіші, ол барлық маңызды ақпараттық активтердің конфиденциалдылықты, тұтастықты және

қолжетімділігін бұзудан болатын шығындардың жалпы сомасының банктің меншікті капиталына немесе банктік операциялардың жекелеген түрлерін жүзеге асыратын ұйымның жарғылық капиталына қатынасы ретінде айқындалады.

20. Саралауды жүзеге асыру үшін ақпаратты қаржы ұйымдары уәкілетті органның сұратуы бойынша ұсынады.

21. Ықтимал залалдардың көрсеткіші үшін саралау жоғарыдан төменгіге дейін жүргізіледі.

22. Маңызды ақпараттық активтер үлесінің көрсеткіші үшін саралау төменнен жоғарыға жүргізіледі.

Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесіне
1-қосымша

Ақпараттық активтер түрлерінің тізбесі

Актив түрі	Типі
Ақпаратты өңдеудің жеке құрылғысы (компьютер, планшет, ноутбук, смартфон)	Аппараттық
Ақпаратты тасымалдаушы	Аппараттық
Перифериялық компьютерлік жабдық	Аппараттық
Сервер	Аппараттық
Желілік жабдық	Аппараттық
Телефония аппаратурасы	Аппараттық
Байланыстың нақты арнасы	Аппараттық
Дерекқор	Бағдарламалық
Байланыстың виртуалды арнасы	Бағдарламалық
Виртуалдандыру жүйесі	Бағдарламалық
Операциялық жүйе	Бағдарламалық
Аппараттық құралдарды бағдарламалық қамтамасыз ету	Бағдарламалық
Қолданбалы бағдарламалық қамтамасыз ету	Бағдарламалық
Телефонияны бағдарламалық қамтамасыз ету	Бағдарламалық

Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесіне 2-қосымша

Ақпараттық активтерге ақпараттық қауіпсіздік қатерлерінің тізбесі

Актив типі	Ақпараттық қауіпсіздік қатері	Әсері
Аппараттық	Нақты ұрлау	Конфиденциалдылық, қолжетімділік
Аппараттық	Рұқсат етілмеген нақты қол жеткізу	Конфиденциалдылық, тұтастылық, қолжетімділік
Аппараттық	Нақты бұзылу	Қолжетімділік
Бағдарламалық	Жою	Қолжетімділік
Бағдарламалық	Рұқсат етілмеген кодтың орындалуы	Конфиденциалдылық, тұтастылық, қолжетімділік
Бағдарламалық	Бағдарламалық қате	Конфиденциалдылық, тұтастылық, қолжетімділік
Бағдарламалық	Конфигурация қатесі	Конфиденциалдылық, тұтастылық, қолжетімділік

Қаржы ұйымдарын ақпараттық қауіпсіздік тәуекелдеріне ұшырау дәрежесі бойынша саралау тәртібін қоса алғанда, ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесіне
3-қосымша

Ақпараттық қауіпсіздік қатерлерінің үлгі көздерінің тізбесі

Ақпараттық қауіпсіздік қатерлерінің көзі	Орналасуы	Қол жеткізу деңгейі
Хакерлер	Сыртқы	Төмен
Пайдаланушы	Ішкі	Орташа
Артықшылық берілген пайдаланушы	Ішкі	Жоғары