Қаржы нарығында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ең төмен талаптарды бекіту туралы

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2026 жылғы 20 сәуірдегі № 81 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 22 сәуірде № 38505 болып тіркелді

ЗҚАИ-ның ескертпесі!

Осы қаулы 12.07.2026 ж. бастап қолданысқа енгізіледі.

"Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" Қазақстан Республикасының Заңы 13-6-бабының 1-1) тармақшасына және Қазақстан Республикасы Президентінің 2019 жылғы 11 қарашадағы № 203 Жарлығымен бекітілген Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі туралы ереженің 14-тармағының 86-1) тармақшасына сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Қоса беріліп отырған Қаржы нарығында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ең төмен талаптар бекітілсін.

2. Ақпараттық және киберқауіпсіздік департаменті 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 2026 жылғы 12 шілдеден 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

2026 жылғы 20 сәуірдегі
№ 81 қаулысымен бекітілген

Қаржы нарығында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ең төмен талаптар

1-тарау. Жалпы ережелер

1. Осы қаржы нарығында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ең төмен талаптар (бұдан әрі – Талаптар) "Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" Қазақстан Республикасының Заңы 13-6-бабының 1-1) тармақшасына және Қазақстан Республикасы Президентінің 2019 жылғы 11 қарашадағы № 203 Жарлығымен бекітілген Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі туралы ереженің 14-тармағының 86-1) тармақшасына сәйкес әзірленді.

Талаптардың мақсаты өз жұмысында цифрлық жүйелерді және цифрлық инфрақұрылымды пайдаланатын қаржы ұйымдарының ақпараттық қауіпсіздігін қамтамасыз етудің негізгі процестерін регламенттеу болып табылады.

2. Талаптарда мынадай терминдер мен анықтамалар пайдаланылады:

1) ақпараттық қауіпсіздік (бұдан әрі – ақпараттық қауіпсіздік) – ақпараттың құпиялылығы, тұтастығы және қолжетімділігі қамтамасыз етілген, ақпараттың сыртқы және ішкі қатерлерден қорғалу жағдайы;

2) ақпараттық қауіпсіздікті қамтамасыз ету – қаржы ұйымында ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтауға бағытталған процесс;

3) ақпаратты өңдеу құралдары – цифрлық ресурстарды өңдеу, сақтау және резервтік көшіру құралдары;

4) бейнелердің мемлекеттік дерекқоры – жеке тұлғалардың сәйкестендіру деректерін, сондай-ақ оларға сәйкес келетін адам бетінің эталондық бейнелерін қамтитын, мемлекетке тиесілі дерекқор;

5) цифрлық инфрақұрылым – цифрлық ресурстарды және оларға қол жеткізуді ұсыну мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған цифрлық инфрақұрылым объектілерінің жиынтығы;

6) цифрлық инфрақұрылымды қорғау аясы (бұдан әрі – қорғау аясы) – қаржы ұйымының цифрлық инфрақұрылымын сыртқы телекоммуникациялық желілерден бөлетін және оларды ақпараттық қауіпсіздік қатерлерінен қорғауды іске асыратын бағдарламалық-аппараттық құралдар жиынтығы.

2-тарау. Ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын ұйымдастырушылық талаптар

3. Қаржы ұйымының басшылығы қаржы ұйымында ақпараттық қауіпсіздікті қамтамасыз етудің тәсілдерін белгілейтін ақпараттық қауіпсіздік саясатын бекітеді.

4. Қаржы ұйымының бірінші басшысы қаржы ұйымының ақпараттық қауіпсіздігін қамтамасыз етуге дербес жауаптылық атқарады.

5. Қаржы ұйымы жаңа қызметкерді жұмысқа қабылданған сәттен бастап 5 (бес) жұмыс күнінен кешіктірмей негізгі ішкі құжаттармен және ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптармен қол қойғыза отырып таныстыруды қамтамасыз етеді. Танысу нәтижесі тиісті нұсқама журналында немесе нұсқамадан өткендігін растайтын жеке құжатта тіркеледі, ол қызметкердің жеке ісіне қоса тіркеледі .

6. Қаржы ұйымы өзінің цифрлық инфрақұрылымына қаржы ұйымының қызметкерлеріне, клиенттеріне, сондай-ақ қаржы ұйымының қызметкерлері, клиенттері болып табылмайтын тұлғаларға (бұдан әрі – үшінші тұлғалар) қол жеткізу кезінде ақпараттық қауіпсіздікті қамтамасыз етеді.

7. Үшінші тұлғалар қаржы ұйымының ақпаратына және (немесе) цифрлық инфрақұрылымына қол жеткізе алатын үшінші тұлғалармен жасалатын келісімдерде, шарттарда үшінші тұлғалардың қаржы ұйымының ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды сақтауы туралы ережелер қамтылады.

8. Қаржы ұйымы уәкілетті органға анықталған ақпараттық қауіпсіздіктің мынадай оқыс-оқиғалары туралы ақпарат ұсынады:

1) қолданбалы және жүйелік бағдарламалық қамтылымдағы осалдықтарды пайдалану;

2) цифрлық жүйеге рұқсатсыз кіру;

3) цифрлық жүйеге немесе деректерді беру желісіне "қызмет көрсетуден бас тарту" шабуылы;

4) серверге зиянды бағдарлама немесе код кіргізу;

5) ақпараттық қауіпсіздікті бақылауды бұзу салдарынан рұқсатсыз ақша қаражатын аударуды жүргізу;

6) клиентті сәйкестендіру және аутентификациялау жүйелерінің жұмысын бұзу;

7) цифрлық жүйелердің бір сағаттан артық тоқтап қалуына әкеп соққан ақпараттық қауіпсіздіктің өзге де оқыс-оқиғалары.

Осы тармақта көрсетілген ақпараттық қауіпсіздіктің оқыс-оқиғалары туралы ақпаратты қаржы ұйымы ақпараттық қауіпсіздік оқиғалары мен оқыс-оқиғалары туралы уәкілетті органның ақпаратты өңдеуге арналған автоматтандырылған жүйесі (бұдан әрі – ААӨЖ) арқылы немесе ұсынылатын деректердің конфиденциалдығын және түзетілмейтіндігін қамтамасыз ететін криптографиялық қорғау құралдарымен ақпаратты кепілді жеткізудің көлік жүйесін пайдалана отырып, электрондық форматта дереу ұсынады.

Жоғарыда көрсетілген жүйелер қолжетімсіз болған жағдайда, оқыс-оқиға туралы ақпаратты беру қаржы ұйымын ААӨЖ-да тіркеу кезінде көрсетілген қаржы ұйымының телефон нөмірінен уәкілетті органның "Ақпараттық қауіпсіздік" бөліміндегі

интернет-ресурсында байланыс үшін көрсетілген уәкілетті органның телефон нөміріне қаржы ұйымының ресми хатымен қағаз тасымалдағышта қайталана отырып жүзеге асырылады.

Қаржы ұйымы ААӨЖ-ға қосылмаған кезде ақпараттық қауіпсіздік оқыс-оқиғалары туралы ақпарат уәкілетті органның интернет-ресурсында "Ақпараттық қауіпсіздік" бөлімінде көрсетілген Агенттіктің электрондық поштасының мекенжайына беріледі.

Дауыс беретін акцияларының елу және одан да көп пайызы Қазақстан Республикасының Ұлттық Банкіне тиесілі немесе оның сенімгерлік басқаруындағы заңды тұлғалар үшін ақпараттық қауіпсіздік оқыс-оқиғалары туралы мәліметтерді Қазақстан Республикасы Ұлттық Банкінің ААӨЖ-мен ықпалдастырылған цифрлық инфрақұрылым объектілері арқылы беруге жол беріледі.

9. Қаржы ұйымы үй-жайларда дене қауіпсіздігі шараларын іске асырады, оның ішінде өткізу және объектішілік режимді ұйымдастырады.

3-тарау. Ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын техникалық талаптар

10. Қаржы ұйымы қаржы ұйымын қорғау аясының жұмыс істеуін қамтамасыз етеді.

11. Қаржы ұйымының қорғау аясының шегінен шығатын телекоммуникациялық біріктіру шифрлауға жатады.

12. Қаржы ұйымдарының, оның ішінде Қазақстан Республикасының мемлекеттік органдарымен және азаматтарымен өзара іс-қимыл жасау үшін пайдаланылатын пошта сервистері тек Қазақстан Республикасының аумағында нақты орналастырылған цифрлық инфрақұрылымда (бұдан әрі – қазақстандық электрондық пошта мекенжайлары) жұмыс істейді.

13. Қаржы ұйымы өзінің қазақстандық электрондық почта мекенжайлары туралы ақпаратты Қазақстан Республикасының азаматтары қаржы ұйымымен өзара іс-қимыл жасау үшін пайдалануы тиіс екенін түсіндіре отырып, жалпыға қолжетімді ақпарат көздерінде жариялайды.

14. Қаржы ұйымы электрондық почта хабарламаларын жіберу және алу кезінде электрондық почтаның мынадай қорғау тетіктерін қолдануды қамтамасыз ететін пошта сервистерін пайдаланады: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting & Conformance (DMARC).

15. Қаржы ұйымы қорғау аясының бағдарламалық-аппараттық құралдарының жүйелік және конфигурациялық файлдарының іске қосылуы мен тұтастығының өзгеруін бақылауды қамтамасыз етеді.

16. Жергілікті әкімшінің қол жеткізу құқықтары немесе жергілікті әкімшінің қол жеткізу құқықтарына ұқсас құқықтар қызметкер өзінің функционалдық міндеттерін орындау үшін пайдаланатын бағдарламалық қамтылымның жұмыс істеуі үшін талап етілетін жағдайларды қоспағанда, қаржы ұйымының қызметкерлеріне жергілікті әкімшінің қол жеткізу құқықтары немесе ұқсас қол жеткізу құқықтары берілмейді.

17. Қаржы ұйымы серверлерде, сол сияқты қаржы ұйымының жұмыс станцияларында, ноутбуктерде, мобильді құрылғыларында (техникалық мүмкіндігі болған жағдайда) вирусқа қарсы жүйелерді немесе бағдарламалық ортаның тұтастығы мен өзгермейтіндігін бақылайтын жүйелерді пайдаланады. Бұл ретте:

1) лицензиялардың, жаңартулардың және техникалық қолдаудың болуы;

2) соңғы пайдаланушы үшін осы жүйенің жұмыс істеуін тоқтатудың мүмкін еместігі қамтамасыз етіледі.

18. Қаржы ұйымы деректерді өңдеудің, деректерді өңдеу және (немесе) сақтаудың сыртқы сервистерін пайдаланудың бөгде орталықтарында серверлік қуаттарды орналастырған жағдайларда үшінші тұлғалардың ақпаратқа қол жеткізу мүмкіндігі алып тасталады, оны азаматтық, банктік туралы Қазақстан Республикасының заңнамасына, Дербес деректер және оларды қорғау туралы Қазақстан Республикасының заңнамасына сәйкес үшінші тұлғаларға беруге жол берілмейді.

19. Цифрлық жүйелердің және оларда өңделетін деректердің резервтік көшірмесін қаржы ұйымы цифрлық жүйелердің жұмысындағы іркілістерден кейін қалпына келтіру қажеттіліктерін негізге ала отырып қамтамасыз етеді. Деректердің резервтік көшірмесін жасау, сақтау, қалпына келтіру тәртібі мен кезеңділігі, резервтік көшірмелерден цифрлық жүйелердің жұмыс істеу қабілеттін қалпына келтіруді тестілеудің өткізу кезеңділігі қаржы ұйымының ішкі құжаттарында бизнеске әсер етуді талдау негізінде айқындалады.

4-тарау. Цифрлық жүйелерге қолжетімділікті ұйымдастыру кезінде қауіпсіздікті қамтамасыз ету

20. Осы тараудың талаптары Қазақстан Республикасының заңнамасына сәйкес қорғалуға жататын не уәкілетті органның талаптарына сәйкес жүргізілген ақпараттық қауіпсіздік тәуекелдерін бағалау нәтижелері бойынша маңызды санатына жатқызылған ақпаратты өңдеу, сақтау немесе беру үшін қаржы ұйымы пайдаланатын цирфлық жүйелерге қолданылады.

Қаржы ұйымы осы тараудың талаптарын қолдану саласына жатқызылған цифрлық жүйелердің тізбесін (бұдан әрі – Тізбе) жасайды.

21. Қаржы ұйымы қызметкерлерінің, қаржы ұйымында шарттық қатынастар жасалған үшінші тұлғалардың (бұдан әрі – пайдаланушы) немесе қаржы ұйымы клиенттерінің (бұдан әрі – клиент) қаржы ұйымының цифрлық жүйелеріне қолжетімділігі ақпараттық жүйелерді қоспағанда, сәйкестендіру және аутентификациялау рәсімінің нәтижелері бойынша жүзеге асырылады, олар бойынша қаржы ұйымының ішкі құжатымен оның орындылығы мен қауіпсіздігін негіздей отырып, қолжетімділіктің өзге тәртібі бекітіледі.

22. Қаржы ұйымының цифрлық жүйелерінде аудиторлық із жүргізу функциясы пайдаланылады, ол кем дегенде мыналарды көрсетеді:

1) қосылғыштарды орнату, сәйкестендіру, аутентификациялау және авторизациялау (сәтті және сәтсіз) оқиғалары;

2) қауіпсіздік теңшеулерін түрлендіру оқиғалары;

3) пайдаланушылардың топтарын және олардың өкілеттіктерін түрлендіру оқиғасы;

4) пайдаланушылардың есептік жазбаларын және олардың өкілеттіктерін түрлендіру оқиғасы;

5) жаңартуларды және (немесе) өзгерістерді орнатуды көрсететін оқиға;

6) аудиторлық із жүргізу өлшемдерінің өзгеру оқиғасы.

23. Аудиторлық ізді сақтау кезінде оның өзгермейтіндігін бақылау қамтамасыз етіледі. Аудиторлық іздің сақталу мерзімі жедел қолжетімділікте кемінде 3 (үш) айды және архивтік қолжетімділікте кемінде 1 (бір) жылды не жедел қолжетімділікте кемінде 1 (бір) жылды құрайды.

24. Пайдаланушылар мен клиенттердің қызметін бақылауды қамтамасыз ету мақсатында қаржы ұйымының цифрлық жүйелеріндегі олардың есептік жазбалары іс-әрекеттерінің аудиторлық ізі жүргізіледі.

25. Пайдаланушыны немесе клиентті сәйкестендіру және аутентификациялау білім, иелік ету немесе ажырамастықты қоса алғанда, бір немесе бірнеше факторлардың көмегімен жүзеге асырылады. Білім факторы пайдаланушы немесе клиент білуі керек ақпаратқа негізделеді. Иелік ету факторы пайдаланушының немесе клиенттің белгілі бір физикалық құрылғыға немесе криптографиялық кілтке иелік етуіне негізделеді. Ажырамастық факторы пайдаланушының немесе клиенттің бірегей биометриялық ерекшеліктеріне негізделеді.

26. Пайдаланушылар мен клиенттердің цифрлық жүйелерге қаржы ұйымының қорғау аясынан тыс қол жеткізуі кемінде екі түрлі аутентификациялау факторларын қолдану арқылы жүзеге асырылады.

27. Қаржы ұйымы қызметкерінің цифрлық жүйелерге қол жеткізуі қызметкер міндеттерін орындауы үшін осындай қолжетімділіктің қажеттілігін растайтын қаржы ұйымының бекітілген құжаттары болған жағдайда қаржы ұйымының ішкі құжаттарына сәйкес жүзеге асырылады.

28. Үшінші тұлғалардың цифрлық жүйелерге қол жеткізуі үшінші тұлғаларға қаржы ұйымының цифрлық жүйесіне осындай қолжетімділіктің қажеттілігін растайтын қолданыстағы шарт болған жағдайда қаржы ұйымының ішкі құжаттарына сәйкес жүзеге асырылады.

29. Қаржы ұйымының клиентін сәйкестендіру және аутентификациялау қаржы ұйымының клиентін тіркеу кезінде алынған деректер негізінде қаржы ұйымының ішкі құжаттарына сәйкес жүзеге асырылады.

30. Клиентті қаржы ұйымының цифрлық жүйелерінде тіркеу клиенттің жеке басы расталғаннан кейін қаржы ұйымының ішкі құжаттарына сәйкес жүзеге асырылады.

Жеке басын қашықтан растау үшін кем дегенде төмендегі тексерулер жиынтығы қолданылады:

1) клиентті бейнелердің мемлекеттік дерекқорын пайдалану арқылы бет-әлпеті бойынша немесе клиенттің жеке қатысумен қаржы ұйымының арнайы құрылғылары арқылы алынған биометриялық деректер бойынша биометриялық тексеру;

2) азаматтардың мобильді телефондары нөмірлерінің мемлекеттік дерекқорында тіркелген телефон нөміріне иелік етуін тексеру не аккредиттелген куәландырушы орталық шығарған электрондық цифрлық қолтаңба сертификатының жабық криптографиялық кілтіне иелік етуін тексеру.

31. Клиентті алдағы уақытта сәйкестендіру және аутентификациялау мақсатында тіркеу барысында мынадай деректерді жинауға рұқсат етіледі:

1) клиент белгілейтін құпиясөз;

2) инициализация векторы, сериялық нөмірі немесе біржолғы құпиясөздердің аппараттық немесе бағдарламалық генераторын (OTP генераторы) қосуға қажетті өзге де ақпарат;

3) мобильді құрылғыға мобильді қосымшаны орнатудың бірегей сәйкестендіргіші, сондай-ақ мобильді құрылғының дербес сипаттамалары;

4) клиенттің құрылғысында сақталатын жабық криптографиялық кілтке сәйкес келетін электрондық цифрлық қолтаңба сертификаты;

5) клиенттің оған иелік етуі расталған мобильді телефонының қосымша нөмірі;

6) клиенттің бейнелердің мемлекеттік дерекқоры арқылы тексерілген немесе қаржы ұйымының құрылғылары арқылы алынған биометриялық деректері;

7) клиенттің құрылғысында сақталатын жабық криптографиялық кілтке сәйкес ашық криптографиялық кілт.

32. Телефон нөміріне иелік етуді тексеру тексерілетін мобильді телефон нөміріне алдын ала болжауға болмайтын құрастырылған кодты жіберу, кейіннен аталған кодты мобильді телефон нөмірінің иесінен аутентификациялау жүйесінің алуы арқылы жүзеге асырылады.

33. Электрондық цифрлық қолтаңба сертификатының жабық криптографиялық кілтіне иелік етуді тексеру электрондық цифрлық қолтаңбаның осы сертификатын шығарған аккредиттелген куәландырушы орталықтың қағидаларына сәйкес жүзеге асырылады.