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 қағидаларын бекіту туралы

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2022 жылғы 12 қыркүйектегі № 67 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2022 жылғы 16 қыркүйекте № 29639 болып тіркелді

"Ақпараттандыру туралы" Қазақстан Республикасының Заңы 7-5-бабының 4-тармағына сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Қоса беріліп отырған 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 қағидалары 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 алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

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

Қазақстан Республикасының
Қаржы нарығын
реттеу және дамыту
Агенттігінің Басқармасының

2022 жылғы 12 қыркүйектегі
№ 67 қаулысы
қосымша

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 қағидалары

1-тарау. Жалпы ережелер

1. Осы 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 қағидалары (бұдан әрі – Қағидалар) " Ақпараттандыру туралы" Қазақстан Республикасының Заңы (бұдан әрі – Ақпараттандыру туралы заң) 7-5-бабының 4-тармағына сәйкес әзірленді және қаржы нарығы мен қаржы ұйымдарының ақпараттық қауіпсіздіктің салалық орталығы пайдаланатын ақпараттық қауіпсіздіктің (бұдан әрі - АҚ) оқиғалары мен оқыс оқиғалары бойынша ақпарат жинау, өңдеу және алмасу жөніндегі ақпараттандыру объектісін қосу және пайдалану тәртібін айқындайды.

2. Қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті органның ақпараттық қауіпсіздіктің оқиғалары мен оқыс оқиғалары бойынша ақпаратты өңдеудің автоматтандырылған жүйесі (бұдан әрі - ААӨЖ) қаржы нарығы мен қаржы ұйымдарының ақпараттық қауіпсіздіктің салалық орталығы пайдаланатын ақпараттық қауіпсіздіктің оқиғалары мен оқыс оқиғалары бойынша ақпарат жинау, өңдеу және алмасу жөніндегі ақпараттандыру объектісі болып табылады.

3. Қағидаларда Ақпараттандыру туралы заңды көзделген, сондай-ақ мынадай ұғымдар пайдаланылады:

1) жауапты қызметкер – қаржы ұйымының лауазымдық міндеттерінде ААӨЖ-де ақпарат өңдеу бекітілген қызметкері;

2) қаржы ұйымының бейіні – ААӨЖ-дегі қаржы ұйымы туралы құрылымдалған ақпарат;

3) қауіп-қатер туралы ескерту – барлық қаржы ұйымдары үшін АҚ өзекті оқиғалары бойынша хабарлама;

4) оқыс оқиға картасы – уәкілетті органға Қағидаларға сәйкес ұсынылатын қаржы ұйымындағы АҚ оқыс оқиғасы туралы құрылымдалған ақпарат;

5) осалдық туралы ескерту – бағдарламалық қамтылымды және қаржы нарығы субъектілерінің инфрақұрылымында пайдаланылатын жабдықты өндірушілерде осалдықтың анықталғаны туралы хабарлама;

6) сигнал – қаржы ұйымының ақпараттық инфрақұрылымындағы АҚ жүйелерінен немесе нақты уақытта АҚ оқиғалары туралы ақпарат жинау мен талдауды жүзеге асыратын жүйелерден алынатын АҚ оқиғасы туралы құрылымдалған ақпарат;

7) сұрату – ақпаратты қорғауды қамтамасыз ететін ААӨЖ құралдары арқылы іске асырылған, АҚ қамтамасыз ету мәселелері бойынша қаржы ұйымдарының бір-біріне немесе қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті (бұдан әрі – уәкілетті орган) органға ресми түрде жүгінуі;

8) ықпалдастыру модулі – қаржы ұйымының ААӨЖ-дегі инфрақұрылымында АҚ оқиғалары бойынша ақпарат беруді автоматтандыру үшін қаржы ұйымының инфрақұрылымына орнатылатын бағдарламалық қамтылым.

4. ААӨЖ-ні пайдаланған уақытта Ақпараттандыру туралы заңның, "Дербес деректер және оларды қорғау туралы", "Қазақстан Республикасындағы банктер және банк қызметі туралы" заңдардың қорғалатын ақпараттың қауіпсіздігін қамтамасыз ету жөніндегі талаптары сақталады.

2-тарау. ААӨЖ-ге қосу

5. ААӨЖ-ге қаржы ұйымының ақпараттық қауіпсіздік бөлімшесі қосылады. ААӨЖ-де қаржы ұйымының бейінін құру үшін жауапты қызметкер АҚ салалық орталығына қаржы ұйымының мынадай есепке алу деректерін ұсынады:

1) қаржы ұйымының атауы;

2) заңды тұлғаның бизнес-сәйкестендіру нөмірі;

3) электрондық поштаның мекенжайы.

6. Қаржы ұйымы пайдаланушысының есепке алу жазбасын құру үшін ААӨЖ-де жауапты қызметкер АҚ салалық орталығына пайдаланушының мынадай есепке алу деректерін ұсынады:

1) тегі, аты, әкесінің аты (ол бар болса);

2) лауазымы;

3) ұйымның атауы;

4) байланыс телефондары;

5) электрондық поштаның мекенжайы.

7. ААӨЖ-ге сигналдарды беру үшін банктер, Қазақстан Республикасы бейрезидент-банктерінің филиалдары (бұдан әрі – банктер) және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдар (бұдан әрі – ұйымдар) АҚ-ның салалық орталығы ұсынған ықпалдасу модулін банктің, ұйымның АҚ жүйелеріне немесе банктің, ұйымның ақпараттық инфрақұрылымында АҚ оқиғалары туралы ақпаратты нақты уақытта жинауды және талдауды жүзеге асыратын жүйелерге қоса отырып, банктің, ұйымның ақпараттық инфрақұрылымына орнатуды жүзеге асырады.

8. Банктер, ұйымдар мынадай АҚ оқиғалары анықталған жағдайда сигналдарды ААӨЖ-ге береді:

1) IPS/IDS зиянды белсенділігін анықтау (басып кіруді анықтау және алдын алу жүйесі);

2) WAF зиянды белсенділігін анықтау (веб-қосымшалардың желілік сүзгісі);

3) соңғы нүктелерді қорғау жүйесінің зиянды белсенділігін анықтау;

4) зиянды кодты алу;

5) фишингтік хабарлама алу;

6) белсенді желілік қызметтерді анықтау үшін IP-мекенжайларды желілік сканерлеу ;

7) есептік жазбаның құпиясөзін мөлшерден артық теру (сыртқы аяда);

8) құпиясөзге есептік жазбаларды мөлшерден артық теру (сыртқы аяда).

9. Банк, ұйым ААӨЖ-мен ықпалдасу модулін байланыстыру үшін интернет-арнаны қамтамасыз етеді.

3-тарау. ААӨЖ-ні пайдалану

10. Қазақстан Республикасының қаржы нарығы үшін АҚ қауіп-қатері анықталған кезде қаржы ұйымының жауапты қызметкері АҚ бөлімшесі басшылығының келісімі бойынша мынадай деректерді енгізу арқылы ААӨЖ-ге қауіп-қатер туралы ескерту жасайды:

1) пайда болу көзі;

2) қауіп-қатердің түрі;

3) қауіп-қатердің дәрежесі;

4) конфиденциалдылық дәрежесі;

5) қауіп-қатердің сипаттамасы;

6) ұсынымдар.

11. Қаржы ұйымының АҚ басқару жүйесінің жұмыс істеуін қамтамасыз ету үшін қосымша ақпарат алу қажет болған кезде қаржы ұйымының жауапты қызметкері АҚ бөлімшесі басшылығының келісімі бойынша уәкілетті органға немесе қаржы ұйымдарына ААӨЖ-ге сұрату жібереді.

12. Банктің, ұйымның жауапты қызметкері АҚ бөлімшесі басшылығының келісімі бойынша АҚ-ның мынадай оқыс оқиғалары анықталған жағдайда ААӨЖ-де дереу оқыс оқиға картасын жасайды:

1) қолданбалы және жүйелік бағдарламалық қамтылымдағы осалдықтарды пайдалану;

2) ақпараттық жүйеге рұқсатсыз кіру;

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

4) серверді зиянды бағдарламамен немесе кодпен зақымдау;

5) АҚ бақылауларын бұзу салдарынан ақша қаражатын санкциясыз аудару;

6) ақпараттық жүйелердің бір сағаттан астам тұрып қалуына әкеп соққан өзге де АҚ оқыс оқиғалары.

13. Қауіп-қатер немесе осалдық туралы ескерту алған кезде қаржы ұйымының жауапты қызметкері АҚ бөлімшесі басшылығының келісімі бойынша 1 (бір) жұмыс күні ішінде ескертуден ұсынымдарды қабылдайды немесе қолданудан бас тартады және оны ААӨЖ-де көрсетеді.

Ұсынымдарды қолдану аяқталғаннан кейін қаржы ұйымының жауапты қызметкері ААӨЖ-де ескерту мәртебесін өңделген күйге өзгертеді.

14. ААӨЖ-ге сұрату алған кезде қаржы ұйымының жауапты қызметкері АҚ бөлімшесі басшылығының келісімі бойынша 1 (бір) жұмыс күні ішінде оны жұмысқа қабылдайды немесе қабылдамайды және мұны сұратуға түсініктемелерде көрсетеді. Жұмыс аяқталғаннан кейін 10 (он) жұмыс күнінен кешіктірмей сұрату бойынша қаржы ұйымының жауапты қызметкері АҚ бөлімшесі басшылығының келісімі бойынша ААӨЖ-де жауап құрастырады.

15. Қаржы ұйымының жауапты қызметкері АҚ салалық орталығы ААӨЖ-де қауіп-қатер туралы ескертуді, оқыс оқиға картасын немесе ұсынылған деректердің толық болмауына байланысты сұратуға жауапты қайтарған жағдайда 3 (үш) жұмыс күні ішінде кемшіліктерді жояды.