Банк және микроқаржы активтерін сататын электрондық сауда алаңының ақпараттық қауіпсіздігін қамтамасыз ету қағидаларын бекіту туралы

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2024 жылғы 16 тамыздағы № 57 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2024 жылғы 19 тамызда № 34951 болып тіркелді

ЗҚАИ-ның ескертпесі!

Осы қаулы 20.08.2024 бастап қолданысқа енгізіледі

"Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" Қазақстан Республикасы Заңының 15-18-бабы 4-тармағының екінші бөлігіне сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Осы қаулыға қосымшаға сәйкес Банк және микроқаржы активтерін сататын электрондық сауда алаңының ақпараттық қауіпсіздігін қамтамасыз ету қағидалары 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 Республикасының 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 2024 жылғы 20 тамыздан 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
2024 жылғы 16 тамыздағы
№ 57 қаулысы
қосымша

Банк және микроқаржы активтерін сататын электрондық сауда алаңының ақпараттық қауіпсіздігін қамтамасыз ету қағидалары

1-тарау. Жалпы ережелер

1. Осы Банк және микроқаржы активтерін сату жөніндегі электрондық сауда алаңының ақпараттық қауіпсіздігін қамтамасыз ету қағидалары (бұдан әрі-қағидалар) " Қаржы нарығын және қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" Қазақстан Республикасы Заңының 15-18-бабы 4-тармағының екінші бөлігіне сәйкес әзірленді (бұдан әрі – Мемлекеттік реттеу туралы заң) сәйкес әзірленген және қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті органның (бұдан әрі – уәкілетті орган) банк және микроқаржы активтерін сататын электрондық сауда алаңының (бұдан әрі – электрондық сауда алаңы) ақпараттық қауіпсіздігін қамтамасыз ету тәртібін айқындайды.

2. Қағидаларда "Ақпараттандыру туралы", "Электрондық құжат және электрондық цифрлық қолтаңба туралы" Қазақстан Республикасының заңдарында және Мемлекеттік реттеу туралы заңда көзделген ұғымдар пайдаланылады.

2-тарау. Электрондық сауда алаңының ақпараттық қауіпсіздігін қамтамасыз ету

3. Электрондық сауда алаңының ақпараттық қауіпсіздігін электрондық сауда алаңының операторы (бұдан әрі-оператор):

1) оператордың қызметкерлеріне және электрондық сауда алаңында өткізілетін сауда-саттыққа қатысушыларға (бұдан әрі –қатысушылар) электрондық сауда алаңына қолжетімділікті ұйымдастыру;

2) электрондық сауда алаңындағы ақпаратты өңдеу, сақтау және беру кезінде оны қорғау;

3) электрондық сауда алаңындағы ақпарат қолжетімділігінің талап етілетін деңгейін резервтеу және қамтамасыз ету;

4) жабдықтың және бағдарламалық қамтылымның іркілісі және істен шығуынан кейін электрондық сауда алаңының ақпараттық жүйесін қалпына келтіру рәсімдері;

5) оператор мен қатысушы арасындағы электрондық сауда алаңында берілетін ақпаратты шифрлауды қамтамасыз ету жолымен қамтамасыз етеді.

4. Оператор өзінің қызметкерлерін және қатысушыларды идентификаттау және аутентификаттау арқылы оператордың қызметкерлері мен қатысушыларына электрондық сауда алаңына қолжетімділікті қамтамасыз етеді.

5. Электрондық сауда алаңына қолжетімділік оператордың қызметкерлеріне олардың функционалдық міндеттерінде айқындалатын көлемде беріледі.

6. Электрондық сауда алаңында оператор қызметкерлерінің дербестендірілген есептік жазбалары пайдаланылады.

7. Электрондық сауда алаңында есептік жазбаларды басқару, құпиясөздерді қорғау, сондай-ақ электрондық сауда алаңының ақпараттық жүйесінде оператор қызметкерлерінің есептік жазбаларын бұғаттау және бұғаттан босату жөніндегі функциялар қолданылады.

8. Оператордың қызметкерлерін электрондық сауда алаңының ақпараттық жүйесінде идентификаттау және аутентификаттау қауіпсіздік рәсімдеріне сәйкес екі факторлы аутентификаттауды (үш фактордың екеуін: білімін, иеленуін, ажырамастығын) пайдалана отырып жүзеге асырылады.

9. Қатысушыны электрондық сауда алаңында бастапқы тіркеу Қазақстан Республикасының аккредиттелген куәландырушы орталығы берген электрондық цифрлық қолтаңбаның көмегімен немесе Сәйкестендіру деректерімен алмасу орталығы (бұдан әрі – СДАО) арқылы қатысушыны биометриялық идентификаттау қызметін қолдана отырып немесе электрондық сауда алаңының құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып жүзеге асырылады.

10. Қатысушыны идентификаттау және аутентификаттау мына тәсілдердің кем дегенде біреуі міндетті түрде қолданыла отырып, электрондық екі факторлы аутентификаттау тәсілдерін (үш фактордың екеуін: білімін, иеленуін, ажырамастығын) пайдалана отырып жүзеге асырылады:

1) Қазақстан Республикасының аккредиттелген куәландырушы орталығы берген электрондық цифрлық қолтаңба;

2) СДАО қызметтерін пайдалану арқылы немесе электрондық сауда алаңының құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып биометриялық идентификаттау.

11. Электрондық сауда алаңына қол жеткізу кодын (құпиясөзін) өзгерту СДАО растаған немесе электрондық сауда алаңының құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып, клиентті биометриялық идентификаттауды пайдалану арқылы жүзеге асырылады.

12. Оператор электрондық сауда алаңының ақпараттық жүйесінің барлық құрауыштарын вирусқа қарсы қорғауды қамтамасыз етеді.

13. Электрондық сауда алаңы ақпараттық жүйесінің күрделі осалдықтарды жоятын құрауыштарының қауіпсіздігін жаңарту өндіруші оларды жариялаған және таратқан күннен бастап бір айдан кешіктірмей белгіленеді.

14. Электрондық сауда алаңының ақпараттық жүйесінің бағдарламалық және аппараттық құрауыштарын өнеркәсіптік ортаға орнатылғанға дейін сынақтан өткізу отасында жаңартылады.

15. Электрондық сауда алаңының оның жұмыс істейтін көшірмесін қалпына келтіру үшін қажетті ақпараттық жүйесінің барлық құрауыштарының деректерін, файлдары мен конфигурацияларын резервтік сақтауды қамтамасыз етеді.

16. Ақпаратты резервтік көшірудің, сақтаудың, қалпына келтірудің тәртібі мен кезеңділігі, электрондық сауда алаңы ақпараттық жүйесінің резервтік көшірмелерден жұмысқа қабілеттілігін қалпына келтіруді тестілеудің кезеңділігі оператор айқындалады.

17. Оператор электрондық сауда алаңының ақпараттық жүйесінде ұйымдастырушылық және техникалық деңгейде процестер мен рәсімдердің, оқиғалар журналдарындағы жазбалардың, экран суреттерін, аудио-, фото - және бейнетіркеу нәтижелерінің орындалуын растайтын құжаттардың өзгермейтіндігін қамтамасыз етеді.

Осы тармақтың бірінше бөлігінде көзделген деректерді сақтау мерзімі жедел қолжетімділікте кемінде 3 (үш) айды және архивтегі қолжетімділікте кемінде 5 (бес) жылды құрайды.

18. Электрондық сауда алаңының бағдарламалық қамтылымына:

1) веб-қосымшалар серверлерінің (бұдан әрі – веб-қосымшалар) бағдарламалық қамтылымы;

2) мобильді құрылғыларға (бұдан әрі – мобильді қосымша) арналған бағдарламалық қамтылым;

3) бағдарламалық интерфейс серверлерінің бағдарламалық қамтылымы кіреді.

19. Электрондық сауда алаңының ақпараттық жүйесінің бағдарламалық қамтылымын әзірлеу және (немесе) пысықтау оператордың бағдарламалық қамтылымды әзірлеу және (немесе) пысықтау тәртібіне, әзірлеу кезеңдеріне және олардың қатысушыларына сәйкес жүзеге асырылады.

Электрондық сауда алаңының ақпараттық жүйесінің бағдарламалық қамтылымын әзірлеу және (немесе) пысықтау бөгде ұйымға және (немесе) үшінші тұлғаға берілсе, оператор электрондық сауда алаңының ақпараттық қауіпсіздігін қамтамасыз ету туралы талаптарды қамтитын шарт негізінде жүргізілетін жұмыстармен айқындалатын кезеңге және көлемде бөгде ұйымының және (немесе) үшінші тұлғаның электрондық алаңының ақпараттық жүйесіне қол жеткізуді ұсынады. Бөгде ұйыммен және (немесе) үшінші тұлғамен жасалатын шарттарда конфиденциалдылық туралы ережелер, ақпараттық қауіпсіздікті бұзу, сондай-ақ бөгде ұйымның және (немесе) үшінші тұлғаның әрекетінен немесе әрекетсіздігінен электрондық сауда алаңының ақпараттық жүйесінің жұмысында туындаған іркілістер салдарынан туындаған залалды өтеу туралы талаптар қамтылады.

20. Электрондық сауда алаңының ақпараттық жүйесі бағдарламалық қамтылымының бастапқы кодтарын сақтау резервтік көшіруді қамтамасыз ете отырып операторды қорғау аясында орналастырылатын код репозиторийлерін басқарудың мамандандырылған жүйелерінде жүзеге асырылады.

21. Операторда электрондық сауда алаңының ақпараттық жүйесінің бағдарламалық қамтамасыз етуін әзірлеуге және (немесе) пысықтауға қабылданған тәсілге қарамастан,

электрондық сауда алаңының ақпараттық қауіпсіздігін тестілеу міндетті кезең болып табылады, оның барысында кем дегенде мынадай іс-шаралар жүзеге асырылады:

1) бастапқы кодты статикалық талдау;

2) құрауыштар мен бөгде анықтамалықтарды талдау.

22. Электрондық сауда алаңының ақпараттық жүйесі бағдарламалық қамтылымының бастапқы кодын статикалық талдау тексеріліп отырған бағдарламалық қамтылымда қолданылатын барлық бағдарламалау тілдеріне талдауды қолдайтын бастапқы кодтарға статикалық талдаудың сканерін қолдану арқылы жүргізіледі, оның функциясына төмендегі осалдықтарды анықтау кіреді, бірақ онымен шектелмейді:

1) зиянды кодтың инъекциясына жол беретін тетіктердің болуы;

2) бағдарламалау тілдерінің осал функцияларын қолдану;

3) әлсіз және осал криптографиялық алгоритмдерді қолдану;

4) қызмет көрсетуден бас тартуды немесе электрондық сауда алаңы ақпараттық жүйесінің бағдарламалық қамтылымы жұмысының елеулі түрде баяулауын тудыратын кодты қолдану;

5) электрондық сауда алаңының ақпараттық жүйесінің бағдарламалық қамтамасыз етуді қорғау жүйелерін айналып өту тетіктерінің болуы;

6) кодта ашық түрде құпияларды қолдану;

7) электрондық сауда алаңының ақпараттық жүйесі бағдарламалық қамтылымының қауіпсіздігін қамтамасыз ету шаблондары мен практикаларын бұзу.

23. Электрондық сауда алаңының ақпараттық жүйесі бағдарламалық қамтылымының құрауыштарын және (немесе) бөгде анықтамалықтарын талдау құрауыштың және (немесе) бөгде анықтамалықтың қолданылатын нұсқасына тән белгілі осалдықтарды анықтау, сондай-ақ құрауыштардың және (немесе) бөгде анықтамалықтардың және олардың нұсқаларының арасындағы байланыстарды бақылап отыру мақсатында жүргізіледі.

24. Оператор соңғы 3 (үш) жыл ішінде пайдалануға берілген электрондық сауда алаңының ақпараттық жүйесі бағдарламалық қамтылымының бастапқы кодтарының және ақпараттық қауіпсіздікті тестілеу нәтижелерінің барлық нұсқасын сақтауды және жедел режимде қол жеткізуді қамтамасыз етеді.

25. Электрондық сауда алаңының ақпараттық жүйесі бағдарламалық қамтылымының клиенттік және серверлік тараптары арасында деректер алмасу Transport Layer Security (Транспорт Лэйер Секьюрити) шифрлау хаттамасының 1.2-ден төмен емес нұсқасын пайдалана отырып шифрланады.

26. Веб-қосымша мыналарды қамтамасыз етеді:

1) веб-қосымшаның электрондық сауда алаңына тиесілігін идентификаттаудың бірегейлігі (домендік атау, логотиптер, корпоративтік түстер, жария байланыс ақпараты);

2) браузердің жадында авторизациялық деректерді сақтауға тыйым салу;

3) енгізілетін құпияларды жасыру;

4) клиенттің авторизациялау парақшасында веб-қосымшаны пайдалану кезінде сақтау ұсынылатын кибергигиенаны қамтамасыз ету шаралары туралы хабарлау;

5) клиенттің интерфейсінде конфиденциалды деректердің көрсетілуіне жол бермей, проблеманы диагностикалау үшін ең аз деңгейде жеткілікті болатын ақпарат бере отырып, қателер мен ерекше жағдайларды қауіпсіз тәсілмен өңдеу.

27. Мобильді қосымша мыналарды қамтамасыз етеді:

1) мобильді қосымшаның операторға тиесілігін идентификаттаудың бірегейлігі (ресми қосымшалар дүкеніндегі деректер, логотиптер, корпоративтік түстер);

2) операциялық жүйенің тұтастығын бұзу және (немесе) қорғау тетіктерін айналып өту белгілерін анықтау, қашықтан басқару процестерін анықтау жағдайында электрондық сауда алаңының қашықтықтан қызмет көрсету жөніндегі функционалын бұғаттау;

3) қатысушыға мобильді қосымшаның жаңартулары туралы хабарлау;

4) маңызды осалдықтарды жою қажет болған жағдайда оларды орнатқанға дейін мобильді қосымшаның жаңартуларын мәжбүрлеп орнату немесе мобильді қосымшаның функционалын бұғаттау мүмкіндігі;

5) конфиденциалды деректерді мобильді қосымшаның қауіпсіз контейнерінде немесе жүйелік есепке алу деректерін сақтау қоймасында сақтау;

6) электрондық сауда алаңының авторизацияланған серверлік бағдарламалық қамтылымдарымен ғана деректер алмасу;

7) конфиденциалды деректерді кэштеуді алып тастау;

8) мобильді қосымшаның резервтік көшірмелерінен конфиденциалды деректерді алып тастау;

9) қатысушыға мобильді қосымшаны пайдалану кезінде сақтау ұсынылатын кибергигиенаны қамтамасыз етудің тиімді әдістері туралы хабарлау;

10) қатысушыға оның есептік жазбасы арқылы авторизациялау, құпиясөзді өзгерту және (немесе) қалпына келтіру, электрондық сауда алаңы тіркеген ұялы телефон нөмірін өзгерту оқиғалары туралы хабарлау;

11) клиенттің рұқсаты болған жағдайда электрондық сауда алаңының серверлік бағдарламалық қамтылымына мобильді құрылғының геолокациялық деректерін беру немесе мұндай рұқсаттың жоқ екені туралы ақпаратты беру.

28. Серверлік бағдарламалық қамтылым мыналарды қамтамасыз етеді:

1) қатысушының мобильді және веб-қосымшалары тарапынан сұратуларды қабылдау жылдамдығын бақылау;

2) жауапта қатысушының конфиденциалды ақпаратының жария етілуіне жол бермей, проблеманы диагностикалау үшін ең аз деңгейде жеткілікті болатын ақпарат бере отырып, қателер мен ерекше жағдайларды қауіпсіз тәсілмен өңдеу;

3) мобильді қосымшаларды және олармен байланысты құрылғыларды идентификаттау және аутентификаттау;

4) жалған сұратулар мен инъекцияларды жасаумен байланысты абуылдардың алдын алу үшін деректердің жарамдылығын тексеру.

© 2012. Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» ШЖҚ РМК