"Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптарды бекіту туралы" Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 30 шілдедегі № 164 қаулысына өзгерістер мен толықтыру енгізу туралы

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2024 жылғы 29 тамыздағы № 73 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2024 жылғы 3 қыркүйекте № 35024 болып тіркелді

ЗҚАИ-ның ескертпесі!

Осы қаулының қолданысқа енгізілу тәртібін 4 т. қараңыз

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. "Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптарды бекіту туралы" Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 30 шілдедегі № 164 қаулысына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 17289 болып тіркелген) мынадай өзгерістер мен толықтыру енгізілсін:

кіріспесі мынадай редакцияда жазылсын:

"Сақтандыру қызметі туралы" Қазақстан Республикасының Заңына сәйкес Қазақстан Республикасы Ұлттық Банкінің Басқармасы **ҚАУЛЫ ЕТЕДІ:**";

көрсетілген қаулымен бекітілген Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптарда:

1-тармақ мынадай редакцияда жазылсын:

"1. Осы Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптар (бұдан әрі – Талаптар) " Сақтандыру қызметі туралы" Қазақстан Республикасының Заңына сәйкес әзірленді және сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз

ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптарды белгілейді.";

52-тармақ мынадай редакцияда жазылсын:

"52. Талаптардың 50-тармағында көрсетілген ақпарат уәкілетті органға ақпараттық қауіпсіздіктің оқиғалары мен оқыс оқиғалары туралы ақпаратты өңдеуге арналған ақпаратты өңдеудің автоматтандырылған жүйесі арқылы немесе берілетін деректердің құпиялылығы мен түзетілмейтіндігін қамтамасыз ететін криптографиялық қорғау құралдарымен ақпаратты кепілдікті тасымалдау жүйесін қолдана отырып, электрондық форматта ұсынылады.";

мынадай мазмұндағы 3-тараумен толықтырылсын:

"3-тарау. Сақтандыру (қайта сақтандыру) ұйымы қызметтерін қашықтан көрсетуді бағдарламалық қамтамасыз етудің ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптар

54. Сақтандыру (қайта сақтандыру) ұйымы қызметтерін қашықтан көрсетуді бағдарламалық қамтамасыз ету:

1) веб-қосымшалардың (бұдан әрі – веб-қосымша) серверлерін бағдарламалық қамтамасыз етуді;

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

3) бағдарламалық интерфейстердің серверлерін бағдарламалық қамтамасыз етуді (бұдан әрі – серверлік ББҚ) қамтиды.

55. Сақтандыру (қайта сақтандыру) ұйымы қашықтан қызметтер көрсетуді бағдарламалық қамтамасыз етуді әзірлеу және (немесе) пысықтауды сақтандыру (қайта сақтандыру) ұйымының бағдарламалық қамтамасыз етуді әзірлеу және (немесе) пысықтау тәртібін, әзірлеу кезеңдерін және олардың қатысушыларын регламенттейтін ішкі құжаттарына сәйкес жүзеге асырады.

56. Егер сақтандыру (қайта сақтандыру) ұйымы қызметтерін қашықтан көрсетуді бағдарламалық қамтамасыз етуді әзірлеу және (немесе) пысықтау бөгде ұйымға және (немесе) үшінші тұлғаға берілсе, сақтандыру (қайта сақтандыру) ұйымы бөгде ұйымның және (немесе) үшінші тұлғаның осы тараудың талаптарын және ішкі құжаттардың орындалуын қамтамасыз етеді, қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етудің қауіпсіздік жай-күйіне жауап береді.

57. Сақтандыру (қайта сақтандыру) ұйымында әзірленетін қызметтерді қашықтықтан көрсетуді бағдарламалық қамтамасыз етудің бастапқы кодтарын сақтау резервтік көшірмені қамтамасыз ете отырып, сақтандыру (қайта сақтандыру) ұйымының қорғау ауқымында орналастырылатын код репозиторийлерін басқарудың мамандандырылған жүйелерінде жүзеге асырылады.

58. Қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етуді әзірлеуге және (немесе) пысықтауға сақтандыру (қайта сақтандыру) ұйымында қабылданған

тәсілге қарамастан, пайдаланушыларды тіркеу, хабар алмасу және басқа да негізгі операциялар сияқты жүйенің негізгі функцияларын тестілеу, рұқсатсыз кіру, фишинг, бұзу және деректердің жария болуы сияқты қауіптерден қорғау үшін жүйенің қауіпсіздігін тексеру міндетті болып табылады.

59. Сақтандыру (қайта сақтандыру) ұйымы атқарушы орган бекіткен ішкі құжатта айқындалған тәртіппен анықталған осалдықтарды жою жөніндегі түзету шараларының іске асырылуын қамтамасыз етеді. Бұл ретте күрделі осалдықтар қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етуді және (немесе) оның жаңа нұсқаларын пайдалануға бергенге дейін жойылады.

60. Сақтандыру (қайта сақтандыру) ұйымы ақпараттық қауіпсіздік жөніндегі жауапты тұлғамен келісілгеннен кейін қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етуді және (немесе) оның жаңа нұсқаларын пайдалануға беруді жүзеге асырады.

61. Сақтандыру (қайта сақтандыру) ұйымы соңғы 3 (үш) жыл ішінде пайдалануға берілген қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етудің бастапқы кодтарының барлық нұсқаларына жедел режимде сақтауды және оларға қол жеткізуді және қауіпсіздікті тестілеу нәтижелерін қамтамасыз етеді.

62. қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етудің клиенттік және серверлік тараптары арасында деректер алмасу Transport Layer Security (Көлік Лейер Секьюрити) шифрлау хаттамасының 1.2-ден төмен емес нұсқасын пайдалана отырып шифрланады.

63. Клиентті мобильді қосымшада бастапқы тіркеу кезінде сақтандыру (қайта сақтандыру) ұйымы Сәйкестендіру деректерімен алмасу орталығы (бұдан әрі – СДАО) және SMS-хабарламамен алынған біржолғы дербес сәйкестендіргіш (пароль) арқылы клиентті биометриялық сәйкестендіруді жүзеге асырады.

64. Мобильді қосымшаға кіру кодын (паролін) өзгерту СДАО растаған биометриялық деректерді және SMS-хабарламамен алынған біржолғы дербес сәйкестендіргішті (парольді) пайдалана отырып, клиенттің биометриялық сәйкестендіруін қолдану арқылы жүзеге асырылады.

65. Қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етуде клиентті сәйкестендіру және бірдейлендіру сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарында белгіленген қауіпсіздік рәсімдеріне сәйкес екі факторлы бірдейлендіру тәсілдерін (үш фактордың екеуін: білімін, иеленуін, ажырамастығын) пайдалана отырып жүзеге асырылады.

66. Қызметтерді қашықтан көрсетуді бағдарламалық қамтамасыз етуді кроссдомендік бірдейлендіру тетігі ақпараттық қауіпсіздік жөніндегі бөлімшемен келісіледі.

67. Веб-қосымша:

1) веб-қосымшаның сақтандыру (қайта сақтандыру) ұйымына тиесілілігін идентификаттаудың бірегейлігін (домендік атауы, логотиптері, корпоративтік түстері);

2) браузердің жадында авторизациялық деректерді сақтауға тыйым салуды;

3) енгізілген құпияларды жасыруды;

4) веб-қосымшаны пайдалану кезінде сақтауға ұсынылатын кибергигиенаны қамтамасыз ету шаралары туралы клиенттің авторизация бетінде хабардар етілуін;

5) клиенттің интерфейсінде құпия деректердің көрсетілуіне жол бермей, қате туралы барынша жеткілікті ақпарат бере отырып, қателер мен ерекшеліктердің қауіпсіз тәсілмен өңделуін қамтамасыз етеді.

68. Мобильдік қосымша:

1) мобильдік қосымшаның сақтандыру (қайта сақтандыру) ұйымына тиесілілігін идентификаттаудың бірегейлігін (қосымшалардың ресми дүкеніндегі деректер, логотиптер, корпоративтік түстер);

2) операциялық жүйенің тұтастығын бұзу және (немесе) қорғау тетіктерін айналып өту белгілері анықталған, қашықтан басқару процестері анықталған жағдайда сақтандыру (қайта сақтандыру) ұйымының қашықтықтан қызмет көрсету жөніндегі функционалын бұғаттауды;

3) клиентке мобильдік қосымшаның жаңартулары бар екендігі туралы хабарлауды;

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

5) құпия деректерді мобильдік қосымшаның қорғалған контейнерінде немесе жүйелік есептік деректер қоймасында сақтауды;

6) құпия деректердің кэштелуін болдырмауды;

7) мобильдік қосымшаның резервтік көшірмелерінен ашық түрдегі құпия деректерін алып тастауды;

8) клиентті мобильдік қосымшаны пайдалану кезінде сақтауға ұсынылатын кибергигиенаны қамтамасыз ету әдістері туралы хабардар етуді;

9) клиентті оның есептік жазбасындағы авторландыру оқиғалары, парольді өзгерту және (немесе) қалпына келтіру, сақтандыру ұйым тіркеген ұялы телефон нөмірін өзгерту туралы хабардар ету;

10) ақшалай қаражатпен операцияларды жүзеге асыру барысында – клиенттің рұқсаты болған жағдайда мобильдік құрылғының геолокациялық деректерін сақтандыру (қайта сақтандыру) ұйымының серверлік ББҚ-ға жіберуді не мұндай рұқсаттың жоқ екендігі туралы ақпаратты жіберуді қамтамасыз етеді.

69. Сақтандыру (қайта сақтандыру) ұйымы өз тарапынан:

1) жауапта құпия деректердің жария болуына жол бермей, проблеманы диагностикалау үшін барынша аз жеткілікті ақпарат бере отырып, қателер мен ерекшеліктерді қауіпсіз тәсілмен өңдеуді;

2) мобильдік қосымшаларды және олармен байланысты құрылғыларды сәйкестендіруді және бірдейлендіруді;

3) жалған сұратулар мен зиянды кодтың инъекцияларымен шабуылдардың алдын алу үшін деректердің жарамдылығын тексеруді қамтамасыз етеді.".

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 Республикасы Қаржы нарығын реттеу және дамыту агенттігі Төрағасының жетекшілік ететін орынбасарына жүктелсін.

4. Осы қаулы алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі.

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

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