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 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 9 тамызда № 17289 болып тіркелді.

РҚАО-ның ескертпесі!

Осы қаулы 01.01.2019 ж. бастап қолданысқа енгізіледі

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

Ескерту. Кіріспе жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.08.2024 № 73 (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) қаулысымен.

1. Қоса беріліп отырған 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 бекітілсін.

2. Банктік емес қаржы ұйымдарын реттеу департаменті (Көшербаева А.М.) Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) Заң департаментімен (Сәрсенова Н.В.) бірлесіп осы қаулыны Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы қаулы мемлекеттік тіркелген күннен бастап күнтізбелік он күн ішінде оның қазақ және орыс тілдеріндегі қағаз және электрондық түрдегі көшірмесін " Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына ресми жариялау және Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу үшін жіберуді;

3) осы қаулыны ресми жарияланғаннан кейін Қазақстан Республикасы Ұлттық Банкінің ресми интернет-ресурсына орналастыруды;

4) осы қаулы мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Заң департаментіне осы қаулының осы тармағының 2), 3) тармақшаларында және 3-тармағында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Қаржылық қызметтерді тұтынушылардың құқықтарын қорғау және сыртқы коммуникациялар басқармасы (Терентьев А.Л.) осы қаулы мемлекеттік тіркелгеннен кейін күнтізбелік он күн ішінде оның көшірмесін мерзімді баспасөз басылымдарында ресми жариялауға жіберуді қамтамасыз етсін.

4. Осы қаулының орындалуын бақылау Қазақстан Республикасының Ұлттық Банкі Төрағасының орынбасары Ж.Б. Құрмановқа жүктелсін.

5. Осы қаулы 2019 жылғы 1 қаңтардан бастап қолданысқа енгізіледі және ресми жариялануға тиіс.

Ұлттық Банк Төрағасы *Д. Ақышев*

Қазақстан Республикасы
Ұлттық Банкі Басқармасының
2018 жылғы 30 шілдедегі
№ 164 қаулысымен
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 талаптар

1-тарау. Жалпы ережелер

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.

Ескерту. 1-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.08.2024 № 73 (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) қаулысымен.

2. Талаптарда мынадай ұғымдар пайдаланылады:

1) ақпараттық актив - ақпараттың және оны сақтауға және (немесе) өңдеуге пайдаланылатын ақпараттық-коммуникациялық инфрақұрылым объектісінің жиынтығы;

2) ақпараттық-коммуникациялық инфрақұрылым объектілері – сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелері, технологиялық платформалар,

аппараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдардың үздіксіз жұмыс істеуін қамтамасыз ету және ақпараттық қауіпсіздік жүйесі;

3) ақпараттық-коммуникациялық инфрақұрылым (бұдан әрі - ақпараттық инфрақұрылым) - электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділік беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

4) ақпараттық қауіпсіздік - электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық инфрақұрылымның сыртқы және ішкі қауіптерден қорғалу жай-күйі;

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

6) ақпараттық қауіпсіздікті қамтамасыз ету – сақтандыру (қайта сақтандыру) ұйымының ақпараттық активтерінің конфиденциалдылық, тұтастық және қолжетімділік күйін ұстап тұруға бағытталған процесс;

7) ақпараттық қауіпсіздіктің оқыс оқиғасы - ақпараттық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялық туындайтын, олардың тиісінше жұмыс істеуіне қауіп келтіретін іркілістер және (немесе) сақтандыру (қайта сақтандыру) ұйымының электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, модификациялау, жою немесе бұғаттауға арналған талаптар;

8) деректерді өңдеу орталығы – сақтандыру (қайта сақтандыру) ұйымының ақпараттық инфрақұрылымының серверлік және коммуникациялық жабдығы орналасатын арнайы бөлінген үй-жай;

9) кіру - ақпараттық активтерді пайдалану мүмкіндігі;

10) резервтік көшірме – қажет болған жағдайда оларды түпнұсқада немесе жаңадан орналастырылған орнында қалпына келтіруге арналған ақпарат тасымалдағыштағы деректер көшірмесі;

11) сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйесі – сақтандыру (қайта сақтандыру) ұйымының және оның клиенттерінің деректері сақталатын және өңделетін ақпараттық жүйе;

12) технологиялық есептік жазба - ақпарат жүйесіндегі ақпараттық жүйелердің арасында бірегейлендіру жүргізуге арналған есептік жазба;

13) уәкілетті орган - қаржы нарығын және қаржы ұйымдарын реттеу, бақылау мен қадағалау жөніндегі уәкілетті орган;

14) шабуыл – кіруді жою, ашу, өзгерту, шектеу, рұқсатсыз кіруді алу, ұрлау немесе ақпараттық активті рұқсатсыз пайдалану әрекеті.

2-тарау. 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

3. Сақтандыру (қайта сақтандыру) ұйымы ақпараттық қауіпсіздікті қамтамасыз ету барысын басқаруға арналған сақтандыру (қайта сақтандыру) ұйымын жалпы басқару жүйесінің бөлігі болып табылатын ақпараттық қауіпсіздікті басқару жүйесін (бұдан әрі - ақпараттық қауіпсіздікті басқару жүйесі) құру арқылы сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігін ұйымдастырады.

4. Ақпараттық қауіпсіздікті басқару жүйесі сақтандыру (қайта сақтандыру) ұйымының ақпараттық активтерінің қорғалуын қамтамасыз етеді.

5. Сақтандыру (қайта сақтандыру) ұйымы ақпараттық қауіпсіздікті басқару жүйесінің жұмыс істеуін, оның дамуы мен жақсартылуын қамтамасыз етеді.

6. Сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті басқару жүйесінің қатысушылары:

1) басқару органы;

2) атқарушы орган;

3) ақпараттық қауіпсіздік бөлімшесі;

4) ақпараттық технологиялар бөлімшесі;

5) қауіпсіздік бөлімшесі;

6) қызметкерлермен жұмыс жүргізу бөлімшесі;

7) заң бөлімшесі;

8) комплаенс-бақылау бөлімшесі;

9) ішкі аудит бөлімшесі.

Осы тармақтың 3), 4), 5), 6), 7), 8) және 9) тармақшаларында көрсетілген бөлімшелердің функцияларын жауапты қызметкерлердің жүзеге асыруына рұқсат етіледі.

7. Сақтандыру (қайта сақтандыру) ұйымы ақпараттық қауіпсіздікті басқару жүйесін құру және оның жұмыс істеуі кезінде ақпараттық қауіпсіздік және ақпараттық технологиялар бөлімшелерінің тәуелсіздігін оларды сақтандыру (қайта сақтандыру) ұйымының атқарушы органының әртүрлі мүшелеріне немесе сақтандыру (қайта сақтандыру) ұйымының атқарушы органының тікелей басшысына бағыну арқылы қамтамасыз етеді.

8. Сақтандыру (қайта сақтандыру) ұйымының басқару органы ақпараттық қауіпсіздік саясатын бекітеді, онда мыналар:

1) ақпараттық қауіпсіздікті басқару жүйесін құрудың мақсаттары, міндеттері және негізгі қағидаттары;

2) сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерінде жасалатын, сақталатын және өңделетін ақпаратқа кіруді және ақпараттың және оған кірудің мониторингін ұйымдастыруға қойылатын талаптар;

3) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды және сақтауды жүзеге асыруға қойылатын талаптар;

4) ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке мониторинг жүзеге асыруға қойылатын талаптар;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратқа талдау жүргізуге қойылатын талаптар;

6) сақтандыру (қайта сақтандыру) ұйымы қызметкерлерінің өздеріне жүктелген функционалдық міндеттерді атқару кезінде ақпараттық қауіпсіздікті қамтамасыз етуге жауапкершілігі айқындалады.

9. Сақтандыру (қайта сақтандыру) ұйымының басқару органы қорғалатын ақпараттың тізбесін, оның ішінде сақтандыру құпиясы, қызметтік, коммерциялық немесе өзге де заңмен қорғалатын құпия болып табылатын мәліметтер туралы ақпаратты (бұдан әрі - қорғалатын ақпарат) қамтитын тізбені және қорғалатын ақпаратпен жұмыс тәртібін бекітеді.

10. Сақтандыру (қайта сақтандыру) ұйымының басқару органы сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті басқару жүйесінің жай-күйін бақылауды жүзеге асырады.

11. Сақтандыру (қайта сақтандыру) ұйымының атқарушы органы ақпараттық қауіпсіздікті қамтамасыз ету процесін регламенттейтін сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарын, қарау сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарында айқындалатын тәртібі мен кезеңділігін бекітеді.

12. Ақпараттық қауіпсіздік бөлімшесі сақтандыру (қайта сақтандыру) ұйымы ақпаратының конфиденциалдылығын, тұтастығын және қолжетімділігін қамтамасыз ету мақсатында мынадай функцияларды жүзеге асырады:

1) ақпараттық қауіпсіздікті басқару жүйесін құрады, сақтандыру (қайта сақтандыру) ұйымы бөлімшелерінің ақпараттық қауіпсіздікті және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл жасау және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу жөніндегі іс-шараларды қамтамасыз ету бойынша қызметін үйлестіруді және бақылауды жүзеге асырады;

2) сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздік саясатын әзірлейді;

3) сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті қамтамасыз ету процесін әдіснамалық қолдауын қамтамасыз етеді;

4) өз құзыреті шегінде сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздігін басқарудың, қамтамасыз етудің және бақылаудың әдістерін, құралдарын және тетіктерін таңдауды, енгізуді және қолдануды жүзеге асырады;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды, сақтауды және өңдеуді жүзеге асырады;

6) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдауды жүзеге асырады;

7) сақтандыру (қайта сақтандыру) ұйымы қызметкерлерінің ақпараттық қауіпсіздік мәселелері жөнінде хабардар болуын қамтамасыз ету бойынша іс-шараларды ұйымдастырады және жүргізеді;

8) сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті басқару жүйесінің жай-күйінің мониторингін жүзеге асырады;

9) сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті басқару жүйесінің жай-күйі туралы сақтандыру (қайта сақтандыру) ұйымының басшылығын хабардар етуді жүзеге асырады.

13. Ақпараттық технологиялар бөлімшесі мынадай функцияларды жүзеге асырады:

1) сақтандыру (қайта сақтандыру) ұйымының ақпараттық инфрақұрылымының схемаларын әзірлейді;

2) сақтандыру (қайта сақтандыру) ұйымының пайдаланушыларға ақпараттық активтеріне кіру рұқсатын беруді қамтамасыз етеді;

3) сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарына сәйкес ақпараттық инфрақұрылымның үзіліссіз жұмыс істеуі, сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелері деректерінің конфиденциалдылығы, тұтастығы және қолжетімділігі (ақпаратты резервтеуді және (немесе) мұрағаттауды және резервтік көшіруді қоса алғанда) бойынша белгіленген талаптардың орындалуын қамтамасыз етеді;

4) ақпараттық жүйелерді таңдау, ендіру, әзірлеу және тестілеуден өткізу кезінде ақпараттық қауіпсіздікке қойылатын талаптарды қамтитын сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарын сақталуын қамтамасыз етеді.

14. Қауіпсіздік бөлімшесі мынадай функцияларды жүзеге асырады:

1) сақтандыру (қайта сақтандыру) ұйымында жеке басының қауіпсіздігі және техникалық қауіпсіздік шараларын іске асырады, оның ішінде кіру және объектішілік режимін ұйымдастырады;

2) сақтандыру (қайта сақтандыру) ұйымының қызметкерлерін жұмысқа қабылдаған және жұмыстан босатқан кезде ақпараттық қауіпсіздік қауіптерінің туындауы тәуекелдерін барынша азайтуға бағытталған алдын алу іс-шараларын жүргізеді.

15. Қызметкерлермен жұмыс жүргізу бөлімшесі мынадай функцияларды жүзеге асырады:

1) сақтандыру (қайта сақтандыру) ұйымы қызметкерлерінің, сондай-ақ қызмет көрсету туралы шарт бойынша жұмысқа тартылған адамдардың, стажерлардың, практиканттардың ақпаратты жария етпеу туралы міндеттемелерге қол қоюын қамтамасыз етеді;

2) сақтандыру (қайта сақтандыру) ұйымы қызметкерлерінің ақпараттық қауіпсіздік саласында хабардар болуын арттыру процесін ұйымдастыруға қатысады.

16. Заң бөлімшесі сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша ішкі құжаттарының құқықтық сараптамасын жүргізеді.

17. Комплаенс-бақылау бөлімшесі сақтандыру (қайта сақтандыру) ұйымының заң бөлімшесімен бірлесе отырып Талаптардың 9-тармағында көзделген қорғалатын ақпараттың тізбесіне енгізуге жататын ақпараттың барлық түрін айқындайды.

18. Ішкі аудит бөлімшесі сақтандыру (қайта сақтандыру) ұйымының ішкі аудит жүйесін ұйымдастыруды реттейтін сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарына сәйкес сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті басқару жүйесінің жай-күйін бағалауды жүргізеді.

19. Сақтандыру (қайта сақтандыру) ұйымы бөлімшелерінің басшылары:

1) қызметкерлердің ақпараттық қауіпсіздікке қойылатын талаптармен танысуын қамтамасыз етеді;

2) олар басқаратын бөлімшелерде ақпараттық қауіпсіздікті қамтамасыз ету үшін дербес жауапкершілік атқарады.

20. Сақтандыру (қайта сақтандыру) ұйымы бөлімшелерінің қызметкерлері:

1) сақтандыру (қайта сақтандыру) ұйымында қабылданған ақпараттық қауіпсіздікке қойылатын талаптардың орындалуы үшін жауап береді;

2) өзінің тікелей басшысына және ақпараттық қауіпсіздік бөлімшесіне ақпараттық активтермен жұмыс істеу кезіндегі барлық күдікті жағдайлар мен бұзушылықтар туралы хабарлайды.

21.Сақтандыру (қайта сақтандыру) ұйымының ақпараттық активтеріне нақты кіруді ұсыну сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарына сәйкес жүзеге асырылады.

22. Қызметкерлерге ақпаратқа кіру олардың функционалдық міндеттерін орындау үшін қажетті көлемде беріледі.

23. Сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелеріне кіру сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерін пайдаланушыларды сәйкестендіру және бірегейлендіру арқылы жүзеге асырылады.

24. Сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерінде пайдаланушылардың дербестендірілген есептік жазбалары ғана пайдаланылады.

25. Технологиялық есептік жазбаларды пайдалануға және жаңартылуына дербес жауапкершілік атқаратын адамдарды көрсете отырып, әрбір ақпараттық жүйе үшін

ақпараттық қауіпсіздік бөлімшесі басшысының келісімімен ақпараттық технологиялар бөлімшесінің басшысы бекітетін осындай есептік жазбалардың тізбесіне сәйкес технологиялық есептік жазбаларды пайдалануға жол беріледі.

26. Сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерінде сақтандыру (қайта сақтандыру) ұйымының ішкі құжатында айқындалатын есептік жазбаларды және парольдерді басқару, сондай-ақ есептік жазбаларды оқшаулау бойынша функциялар немесе құралдар пайдаланылады.

27. Сақтандыру (қайта сақтандыру) ұйымы жұмыс істеуге қабілетті ақпараттық жүйелерінің көшірмелерін қалпына келтіруді қамтамасыз ететін сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелер деректерінің, олардың файлдарының және теңшеулерінің резервтік сақталуын қамтамасыз етеді.

28. Ақпаратты резервтік көшіру, сақтау, қалпына келтіру тәртібі мен кезеңділігі сақтандыру (қайта сақтандыру) ұйымының ішкі құжатында айқындалады.

29. Сақтандыру (қайта сақтандыру) ұйымы ақпараттық инфрақұрылымды вирусқа қарсы қорғауды сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарына сәйкес қамтамасыз етеді.

30. Сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерінде аудиторлық із жүргізу функциясы пайдаланылады, ол мынадай оқиғаларды (ойдағыдай және ойдағыдай емес) көрсетеді:

1) сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйесіндегі қосылғыштарды орнату, сәйкестендіру және бірегейлендіру;

2) есептік жазбаларды және олардың өкілеттіктерін түрлендіру оқиғасы;

3) сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйесіндегі жаңартуларды және (немесе) өзгерістерді орнатуды көрсететін оқиға;

4) аудиттің өлшемдерінің өзгеру оқиғасы;

5) жүйелік өлшемдердің өзгерістер оқиғасы.

31. Аудиторлық ізді сақтау мерзімі сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйесіндегі кемінде 3 (үш) айды және аудиторлық іздің резервтік көшірмелері түрінде кемінде 1 (бір) жылды құрайды.

32. Ақпараттық технологиялар бөлімшесі сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерін жаңартуларды қадағалап отырады және ақпараттық қауіпсіздік бөлімшесімен бірлесіп сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерін жаңартуларды басқару тәртібін айқындайды.

33. Сақтандыру (қайта сақтандыру) ұйымының ақпараттық жүйелерін жаңартулар өнеркәсіптік ортаға орнатылғанға дейін тестілеу ортасында сынақтан өтеді.

34. Деректерді өңдеу орталықтарының нақты қауіпсіздігін қамтамасыз ету тәртібі сақтандыру (қайта сақтандыру) ұйымының ішкі құжаттарында айқындалады.

35. Сақтандыру (қайта сақтандыру) ұйымы сақтандыру (қайта сақтандыру) ұйымында пайдалануға рұқсат етілетін бағдарламалық қамтамасыз етудің тізбесін айқындайды.

36. Сақтандыру (қайта сақтандыру) ұйымының деректерді өңдеу орталығы техникалық қауіпсіздіктің мынадай жүйелерімен жарақтандырылады:

1) кіруді бақылау және басқару жүйесі;

2) күзет сигнализациясы;

3) өрт сигнализациясы;

4) өртті автоматты сөндіру жүйесі;

5) микроклиматтың белгіленген өлшемдерін ұстап тұру жүйесі;

6) бейнебақылау жүйесі;

7) үздіксіз электр қуат беру жүйесі.

37. Деректерді өңдеу орталығына кіру рұқсаты тізбесін ақпараттық қауіпсіздік бөлімшесінің келісімі бойынша ақпараттық технологиялар бөлімшесінің басшысы бекітетін адамдарға беріледі.

38. Деректерді өңдеу орталығының бейнебақылау жүйесі оқиғалардың жазбасы үздіксіз немесе қозғалыс детекторын пайдалана отырып жүргізіледі.

39. Деректерді өңдеу орталығының бейнебақылау жүйесінің мұрағаты кемінде 3 (үш) ай сақталады.

40. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті мониторингтеу барысында алынған ақпараттық қауіпсіздік оқиғалары туралы ақпарат кемінде 5 (бес) жыл шоғырландырылуға, жүйелендірілуге және сақталуға тиіс.

41. Сақтандыру (қайта сақтандыру) ұйымы сақтандыру (қайта сақтандыру) ұйымының басшы қызметкерлеріне және бөлімшелеріне ақпараттық қауіпсіздіктің орын алған оқыс оқиғалары туралы хабарлау тәртібін айқындайды.

42. Сақтандыру (қайта сақтандыру) ұйымы ақпараттық қауіпсіздіктің оқыс оқиғаларын, оның себептері мен салдарын жою үшін кезек күттірмес шаралар қабылдау тәртібін айқындайды.

43. Сақтандыру (қайта сақтандыру) ұйымында ақпараттық қауіпсіздіктің оқыс оқиғасы қағаз тасымалдағышта не электронды түрде жүргізіледі, онда Талаптардың 46-тармағына сәйкес ақпараттық қауіпсіздіктің оқыс оқиғасына жасалған талдау нәтижелері бойынша қорытындының тіркеу деректері енгізіледі.

44.Ақпараттық қауіпсіздіктің оқыс оқиғасына қатысты бағдарламалық-техникалық құралдардан техникалық деректерді жинау кезінде жинақталған деректердің сақталуы және өзгермеуі қамтамасыз етіледі.

45. Ақпараттық қауіпсіздіктің оқыс оқиғасын өңдеу нәтижесі бойынша ақпараттық қауіпсіздіктің оқыс оқиғасының туындау себептеріне, оның тетігіне және салдарына талдау жүргізіледі.

46. Ақпараттық қауіпсіздіктің оқыс оқиғасын талдау нәтижесі бойынша қорытынды еркін нысанда дайындалады, онда ақпараттық қауіпсіздіктің оқыс оқиғасы бойынша барлық ақпарат, сондай-ақ ақпараттық қауіпсіздіктің қайталанған оқыс оқиғасының болу ықтималын және ықтимал залалды төмендету мақсатында түзету шараларын қабылдау бойынша ұсыныстар көрсетіледі.

47. Сақтандыру (қайта сақтандыру) ұйымының қызметкерлеріне бағдарламалық қамтамасыз етуді өз бетінше орнатуды және теңшеуді жүргізуге тыйым салынатын сақтандыру (қайта сақтандыру) ұйымында ұйымдастырушылық және техникалық шаралар анықталады және енгізіледі.

48. Ерекше жағдайларда пайдаланушылардың жекелеген топтарына бағдарламалық қамтамасыз етуді және жабдықты өз бетінше орнату және теңшеу құқығы беріледі. Пайдаланушылардың бұл топтарына жергілікті әкімшінің құқықтары немесе ұқсас құқықтар беріледі.

49. Талаптардың 48-тармағында көрсетілген пайдаланушылардың тізбесін ақпараттық қауіпсіздік бөлімшесімен келісу бойынша ақпараттық технологиялар бөлімшесінің басшысы қалыптастырады, жаңартады және бекітеді. Пайдаланушыларға қосымша құқықтар берілген жағдайда Талаптардың 48-тармағына сәйкес ақпараттық қауіпсіздік бөлімшесі олардың пайдаланылуын бақылайды.

50. Сақтандыру (қайта сақтандыру) ұйымы жыл сайын есепті жылдан кейінгі жылдың 10 қаңтарынан кешіктірмей уәкілетті органға ақпараттық қауіпсіздікті басқару жүйесінің жай-күйі туралы ақпарат береді.

51. Талаптардың 50-тармағында көрсетілген ақпаратта мыналар:

1) ақпараттық қауіпсіздікті басқару жүйесін құруды және оның жұмыс істеуін реттейтін құжаттардың болуы;

2) ақпараттық қауіпсіздікті қамтамасыз ету үшін пайдаланылатын бағдарламалық-техникалық құралдарының болуы және сандық құрамы;

3) деректер өңдеу орталықтарының болуы, материалдық-техникалық жабдықталуы;

4) сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздікті басқару жүйесін және ақпараттық активтерін жетілдіру бойынша жүргізілген іс-шаралар не олардың болмауы туралы мәліметтер қамтылады.

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.

Ескерту. 52-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.08.2024 № 73 (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) қаулысымен.

53. Уәкілетті орган сақтандыру (қайта сақтандыру) ұйымының Талаптарға сәйкестігін тексеруді 3 (үш) жылда кемінде бір рет жүзеге асырады.

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

Ескерту. Талаптар 3-тараумен толықтырылды - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.08.2024 № 73 (алғашқы ресми жарияланған күнінен кейін күнтізбелік алпыс күн өткен соң қолданысқа енгізіледі) қаулысымен.

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.