Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау қағидаларын бекіту туралы

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2020 жылғы 23 қарашадағы № 110 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2020 жылғы 27 қарашада № 21685 болып тіркелді.

ЗҚАИ-ның ескертпесі!

Осы қаулы 01.01.2021 бастап қолданысқа енгізіледі

"Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" 2003 жылғы 4 шілдедегі Қазақстан Республикасының Заңының 13-6-бабы бірінші бөлігінің 1) тармақшасына сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Қоса беріліп отырған Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау 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 2021 жылғы 1 қаңтардан 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
2020 жылғы 23 қарашасы
№ 110 Қаулымен
бекітілді

Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау қағидалары

1-тарау. Жалпы ережелер

1. Осы Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау қағидалары (бұдан әрі - Қағидалар) "Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" 2003 жылғы 4 шілдедегі Қазақстан Республикасының Заңына сәйкес әзірленді және қаржы ұйымдарының және Қазақстан Республикасының бейрезидент-банктері филиалдарының, Қазақстан Республикасының бейрезидент-сақтандыру (қайта сақтандыру) ұйымдары филиалдарының, Қазақстан Республикасының бейрезидент-сақтандыру брокерлері филиалдарының (бұдан әрі – қаржы ұйымдары) ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау тәртібін айқындайды.

2. Қағидаларда мынадай ұғымдар пайдаланылады:

1) қаржы ұйымының негізгі ақпараттық жүйелері – қаржы ұйымы қызметінің негізгі бағыттарын іске асыратын бизнес – процестердің жұмыс істеуі үшін қажетті қаржы ұйымының ақпараттық жүйелері;

2) уәкілетті орган – қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеуді, бақылауды және қадағалауды жүзеге асыратын мемлекеттік орган.

2-тарау. Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау тәртібі

3. Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалауды қаржы ұйымдары уәкілетті органның сұрау салуы бойынша жүзеге асырады.

4. Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалауды Қағидалардың қосымшасына сәйкес ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау өлшемдеріне сәйкес қаржы ұйымы жүзеге асырады.

Қағидаларға қосымшаның 2-бағанында көрсетілген әрбір өлшем бойынша қаржы ұйымы Қағидаларға қосымшаның 3, 4, 5-бағандарында көрсетілген қорғалу деңгейлерінің бірін айқындайды.

5. Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалауды қаржы ұйымы Қағидаларға қосымшаның 2-бағанында санамаланған ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау параметрлерін, қорғалу деңгейін және олардың орындалуының қысқаша сипаттамасын көрсете отырып, кесте түрінде ресімдейді.

6. Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау нәтижесін қаржы ұйымының басшысы бекітеді және қаржы ұйымы осындай бағалауды жүргізуге уәкілетті органның сұрау салуы алынған күннен бастап үш айдан аспайтын мерзімде уәкілетті органға ілеспе хатпен ұсынады.

7. Қаржы ұйымы ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау нәтижелеріне Қағидаларға қосымшаға сәйкес 2 және 3 қорғалу деңгейлерін растайтын құжаттарды қоса береді.

8. Уәкілетті орган қаржы ұйымы ұсынған ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау нәтижелерінің қоса берілген құжаттарға сәйкестігін тексереді және Қағидаларға қосымшаға сәйкес ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау өлшемдерінің әрқайсысы бойынша қаржы ұйымы қорғалуының қорытынды деңгейін айқындайды.

9. Қаржы ұйымының ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалаудың қорытынды нәтижелерін уәкілетті орган қаржы ұйымының назарына жеткізеді.

Ақпараттық қауіпсіздік
қатерлерінен қорғалу деңгейін
бағалау қағидаларына
қосымша

Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау өлшемдері

№	Ақпараттық қауіпсіздік қатерлерінен қорғалу деңгейін бағалау өлшемі	Қорғалу деңгейі 1	Қорғалу деңгейі 2	Қорғалу деңгейі 3
1	2	3	4	5
1.	Қаржы ұйымы ақпараттық қауіпсіздік саясатының сипаттамасын қамтитын құжатты бекіткен және қаржы ұйымының, сондай-ақ сыртқы ұйымдардың барлық қызметкерлеріне назарына жеткізген.	Ақпараттық қауіпсіздік саясатының сипаттамасы бар құжат жоқ.	Ақпараттық қауіпсіздік саясатының сипаттамасын қамтитын бекітілген құжат бар.	Ақпараттық қауіпсіздік саясатының сипаттамасын қамтитын және барлық қызметкерлердің, сондай-ақ сыртқы ұйымдардың назарына жеткізілген, бекітілген құжат бар.
2.	Қаржы ұйымы ақпараттық қауіпсіздік саясатының сипаттамасын қамтитын құжатты талдауды және қайта қарауды берілген уақыт аралығынан кейін немесе елеулі өзгерістер туындаған кезде жүзеге асырады.	Ақпараттық қауіпсіздік саясатының сипаттамасы бар құжатты қайта қарау кезеңділігі бекітілмеген.	Ақпараттық қауіпсіздік саясатының сипатын қамтитын құжатты қайта қарау кезеңділігі бекітілген, бекітілген мерзімде құжаттамалық қайта қарау куәліктері жоқ.	Ақпараттық қауіпсіздік саясатының сипатын қамтитын құжатты қайта қарау кезеңділігі бекітілген, бекітілген мерзімде құжаттамалық қайта қарау куәліктері бар.
3.	Қаржы ұйымы қызметкерлерінің және қаржы ұйымы басшылығының ақпараттық қауіпсіздікті	Басшылар мен қызметкерлердің ақпараттық қауіпсіздікті қамтамасыз ету	Қызметкерлердің ақпараттық қауіпсіздікті қамтамасыз ету	Басшылар мен қызметкерлердің ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі міндеттерін

	қамтамасыз ету жөніндегі міндеттерін айқындаған.	жөніндегі міндеттерін айқындайтын құжат жоқ.	жөніндегі міндеттерін айқындайтын бекітілген құжат бар.	айқындайтын бекітілген құжат бар.
4.	Қаржы ұйымы құпия ақпаратқа қол жеткізе алатын қаржы ұйымының барлық қызметкерлері қол қойған ақпаратты жария етпеу туралы келісімді айқындаған.	Ақпаратты жария етпеу туралы келісім жоқ.	Ақпаратты жария етпеу туралы бекітілген келісім бар, бірақ оған конфиденциалды ақпаратқа рұқсаты бар барлық қызметкерлер қол қоймаған.	Конфиденциалды ақпаратқа рұқсаты бар барлық қызметкерлер қол қойған ақпаратты жария етпеу туралы бекітілген келісім бар.
5.	Қаржы ұйымы адамдардың тізбесін және олардың құзыретті органдармен (мысалы, құқық қорғау органдары, өрт қызметтері, уәкілетті орган) өзара іс-қимыл тәртібін айқындайтын рәсімдерді айқындаған.	Қызметкерлердің құзыретті органдармен өзара іс-қимылын айқындайтын рәсімдер жоқ.	-	Қызметкерлердің құзыретті органдармен өзара іс-қимылын айқындайтын құжатталған және бекітілген рәсімдер бар.
6.	Қаржы ұйымының ақпараттық қауіпсіздік жөніндегі қызметкерлерінің кәсіби топтармен, қауымдастықтармен өзара іс-қимылы және ақпараттық қауіпсіздік бойынша конференцияларға (форумдарға) қатысуы қолдау табады.	Қаржы ұйымының ақпараттық қауіпсіздік жөніндегі қызметкерлерінің кәсіби топтармен, қауымдастықтармен өзара іс-қимылы және ақпараттық қауіпсіздік бойынша конференцияларға (форумдарға) қатысуы жоқ.	Қаржы ұйымының ақпараттық қауіпсіздік жөніндегі қызметкерлерінің кәсіби топтармен, қауымдастықтармен өзара іс-қимыл тәртібін және ақпараттық қауіпсіздік жөніндегі конференцияларға (форумдарға) қатысуды айқындайтын бекітілген құжат жоқ, Ақпараттық қауіпсіздік жөніндегі қызметкерлер өзара іс-қимылды өз бастамасы бойынша жүзеге асырады.	Қаржы ұйымының ақпараттық қауіпсіздік жөніндегі қызметкерлерінің кәсіби топтармен, қауымдастықтармен өзара іс-қимыл жасау және ақпараттық қауіпсіздік жөніндегі конференцияларға (форумдарға) қатысу тәртібін айқындайтын бекітілген құжат бар, ақпараттық қауіпсіздік жөніндегі қызметкерлер кәсіби топтарда, қауымдастықтарда тұрады және жыл сайын ақпараттық қауіпсіздік жөніндегі конференцияларға (форумдарға) қатысады.
7.	Қаржы ұйымы белгілі бір уақыт аралығында негізгі ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету процестерін сыртқы аудитке шығарады.	Соңғы үш жылдың ішінде барлық негізгі ақпараттық жүйелердің ақпараттық қауіпсіздігіне сыртқы аудит жүргізілген жоқ.	Соңғы үш жылдың ішінде барлық негізгі ақпараттық жүйелердің жартысынан астамында ақпараттық қауіпсіздікті қамтамасыз етуге сыртқы аудит жүргізілді.	Соңғы үш жылдың ішінде барлық негізгі ақпараттық жүйелерде ақпараттық қауіпсіздікті қамтамасыз етуге сыртқы аудит жүргізілді.
	Қаржы ұйымы негізгі ақпараттық жүйелердің			

8.	ақпараттық қауіпсіздігін қамтамасыз етудің сыртқы аудитінің нәтижелерін ақпараттық қауіпсіздікті қамтамасыз етуді жақсарту үшін пайдаланады.	Негізгі ақпараттық жүйелердің ақпараттық қауіпсіздігінің сыртқы аудиті жүргізілмейді.	-	Негізгі ақпараттық жүйелердің ақпараттық қауіпсіздіктіқамтамасыз етудің соңғы сыртқы аудитінің нәтижелері бойынша ақпараттық қауіпсіздікті қамтамасыз етуді жақсарту жөніндегі іс-шаралар іске асырылды.
9.	Қаржы ұйымы үшінші тұлғалардың өзінің ақпаратты өңдеу құралдарына қол жеткізуін бақылайды.	Қаржы ұйымының ақпаратты өңдеу құралдарына үшінші тараптардың қол жеткізуі бақыланбайды.	Үшінші тұлғаларға ақпаратты өңдеу құралдарына рұқсат беру кезінде ақпараттық қауіпсіздікті қамтамасыз етуді айқындайтын бекітілген құжат бар	Үшінші тараптарға қолжетімділік берілген кезде ақпараттық қауіпсіздік тәуекелдерін талдау жүзеге асырылады және анықталған тәуекелдерді төмендету бойынша іс-шаралар әзірленеді.
10.	Қаржы ұйымы клиенттерге қаржы ұйымының ақпараттық жүйелеріне қол жеткізуді ұсыну кезіндегі ақпараттық қауіпсіздік шараларын айқындаған.	Клиенттерге қаржы ұйымының ақпараттық жүйелеріне қол жеткізуді ұсыну кезіндегі ақпараттық қауіпсіздік шаралары айқындалмаған.	Клиенттерге қаржы ұйымының ақпараттық жүйелеріне қол жеткізуді ұсыну кезіндегі ақпараттық қауіпсіздік шараларын айқындайтын бекітілген құжат бар.	-
11.	Қаржы ұйымының ақпаратқа немесе қаржы ұйымының ақпараттық активтеріне қолжетімділігі бар сыртқы ұйымдармен жасасқан келісімдерінде ақпараттық қауіпсіздік жөніндегі талаптар қамтылады.	Ақпаратқа немесе қаржы ұйымының ақпараттық активтеріне қол жеткізе алатын сыртқы ұйымдармен жасалған келісімдерде ақпараттық қауіпсіздік жөніндегі талаптар қамтылмайды.	Қаржы ұйымының ақпаратына немесе ақпараттық активтеріне қол жеткізе алатын сыртқы ұйымдармен жасалған жекелеген келісімдерде ақпараттық қауіпсіздік жөніндегі талаптар қамтылады.	Қаржы ұйымының ақпаратына немесе ақпараттық активтеріне қол жеткізе алатын сыртқы ұйымдармен жасалған барлық қолданыстағы келісімдерде ішкі құжатпен айқындалған ақпараттық қауіпсіздік стандартталған талаптары қамтылған.
12.	Қаржы ұйымы иелерін көрсете отырып, қаржы ұйымының негізгі ақпараттық жүйелерінің тізбесін қамтитын құжатты бекіткен.	Қаржы ұйымының негізгі ақпараттық жүйелерінің тізбесі көрсетілген құжат жоқ.	-	Иелерін көрсете отырып, қаржы ұйымының негізгі ақпараттық жүйелерінің тізбесін қамтитын соңғы жыл ішінде бекітілген немесе өзектендірілген құжат бар.
13.	Қаржы ұйымы электрондық поштаны пайдалану қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Электрондық поштаны пайдалану қағидалары бар құжат жоқ.	-	Қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, электрондық поштаны пайдалану қағидаларын қамтитын бекітілген құжат бар.

14.	Қаржы ұйымы интернет желісін пайдалану қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Интернет желісін пайдалану ережелерін қамтитын құжат жоқ.	-	Интернет желісін пайдалану қағидаларын қамтитын, қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, бекітілген құжат бар.
15.	Қаржы ұйымы қорғалатын ақпараттың тізбесін қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Қорғалатын ақпараттың тізбесін қамтитын құжат жоқ.	-	Қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, қорғалатын ақпараттың тізбесін қамтитын бекітілген құжат бар.
16.	Қаржы ұйымы дербес деректер тізбесін қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Дербес деректер тізбесі бар құжат жоқ.	-	Қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, дербес деректердің тізбесін қамтитын бекітілген құжат бар.
17.	Қаржы ұйымы ақпарат сыныптарының тізбесін, ақпаратты белгілі бір сыныпқа жатқызу қағидаттарын, ақпаратты сыныптау бойынша қызметкерлердің жауапкершілігін айқындауды көрсете отырып, ақпаратты сыныптау қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Ақпаратты жіктеу қағидалары бар құжат жоқ.	-	Қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, ақпаратты жіктеу қағидаларын қамтитын бекітілген құжат бар.
18.	Қаржы ұйымы ақпарат тасымалдағыштарды таңбалау қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Ақпарат тасымалдағыштарды таңбалау қағидаларын қамтитын құжат жоқ.	-	Қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, ақпарат жеткізгіштерді таңбалау қағидаларын қамтитын бекітілген құжат бар.
	Қаржы ұйымы ақпараттық қауіпсіздікті қамтамасыз ету процестеріндегі қаржы	Ақпараттық қауіпсіздікті қамтамасыз ету процестеріндегі қаржы ұйымы бөлімшелерінің	Қаржы ұйымының ақпараттық қауіпсіздік бөлімшесінің немесе ақпараттық қауіпсіздік	Қаржы ұйымының ақпараттық қауіпсіздік бөлімшесінің және басқа бөлімшелерінің немесе қызметкерлерінің

19.	ұйымы бөлімшелерінің н е м е с е қызметкерлерінің рөлі мен функцияларын айқындаған.	н е м е с е қызметкерлерінің рөлі мен функцияларын айқындайтын құжат жоқ.	қызметкерінің функцияларын айқындайтын бекітілген құжат бар.	ақпараттық қауіпсіздікті қамтамасыз ету процестерінде рөлдері мен функцияларын айқындайтын бекітілген құжат бар.
20.	Қаржы ұйымы қызметкерлермен еңбек шарттарында қызметкерлердің ақпараттық қауіпсіздік талаптарын сақтамағаны үшін жауапкершілігін, оның ішінде қаржы ұйымынан шығарылғаннан кейінгі жауапкершілікті көздейді.	Қызметкерлермен еңбек шарттарында қызметкерлердің ақпараттық қауіпсіздік талаптарын сақтамағаны үшін жауапкершілігі көзделмеген.	-	Қызметкерлермен еңбек шарттарында ақпараттық қауіпсіздік талаптарын сақтамағаны үшін қызметкерлердің жауапкершілігі көзделген.
21.	Қаржы ұйымының қызметкерлері қаржы ұйымында ақпараттық қауіпсіздік жөніндегі қағидалар мен рәсімдердің талаптары туралы тұрақты ақпарат алу мақсатында оқудан немесе қайта даярлаудан өтеді.	Ақпараттық қауіпсіздік қағидалары мен рәсімдерінің талаптары туралы қызметкерлермен оқу жүргізілмейді.	Ақпараттық қауіпсіздік қағидалары мен рәсімдерінің талаптары туралы қызметкерлермен оқу тұрақты түрде жүргізілмейді (соңғы 3 жылда жарты жылда кемінде 1 рет).	Ақпараттық қауіпсіздік қағидалары мен рәсімдерінің талаптары туралы қызметкерлермен оқу тұрақты түрде жүргізіледі (соңғы 3 жылда жарты жылда 1 реттен кем емес).
22.	Қаржы ұйымы ақпараттық қауіпсіздік жөніндегі қағидалар мен рәсімдерді бұзғаны үшін тәртіптік жауапкершілікті белгілеген.	Ақпараттық қауіпсіздік қағидалары мен рәсімдерін бұзғаны үшін тәртіптік жауапкершілікті айқындайтын құжат жоқ.	Ақпараттық қауіпсіздік жөніндегі қағидалар мен рәсімдерді бұзғаны үшін тәртіптік жауапкершілік айқындалған бекітілген құжат бар.	-
23.	Қаржы ұйымы қызметкерлерді жұмыстан шығарған кезде олар пайдаланған активтердің қайтарылуын бақылауды қамтамасыз етеді.	Қызметкерлер жұмыстан босатылған кезде қаржы ұйымының активтерін қайтаруды бақылау процесі жоқ.	Қызметкерлер жұмыстан босатылған кезде қаржы ұйымының активтерін қайтаруды бақылау процесі қол режимінде жүзеге асырылады.	Қызметкерлер жұмыстан босатылған кезде қаржы ұйымының активтерін қайтаруды бақылау процесі ішінара немесе толық автоматтандырылған.
24.	Қаржы ұйымы жұмыстан босатылған кезде қызметкерлердің ақпаратты өңдеу құралдарына қол жеткізуінің күшін жоюды қамтамасыз етеді.	Қызметкерлер жұмыстан босатылған кезде ақпаратты өңдеу құралдарына берілген рұқсаттың күшін жою процесі жоқ.	Қызметкерлер жұмыстан босатылған кезде ақпаратты өңдеу құралдарына берілген рұқсаттың күшін жою процесі қол режимінде жүзеге асырылады.	Қызметкерлер жұмыстан босатылған кезде ақпаратты өңдеу құралдарына берілген рұқсаттың күшін жою процесі ішінара немесе толық автоматтандырылған.

25.	Қаржы ұйымында ақпаратты өңдеу құралдарына жеке қол жетімділік тек уәкілетті қызметкерлерге беріледі.	Ақпаратты өңдеу құралдарына нақты қол жеткізуді шектеу процесі жоқ.	Ақпаратты өңдеу құралдарына нақты қол жеткізуді шектеу процесі қолмен жасау режимінде жүзеге асырылады.	Ақпаратты өңдеу құралдарына нақты қол жеткізуді шектеу процесі ішінара немесе толық автоматтандырылған.
26.	Қаржы ұйымында серверлік жабдық жабдықты өндіруші ұсынған микроклиматты қамтамасыз ете отырып, бөлінген үй-жайларда орналасады.	Серверлік жабдық қызметкерлер жұмыс істейтін кабинеттерде орналастырылады.	Серверлік жабдық микроклимат сақталатын бөлек бөлмелерде орналастырылады. Микроклимат мониторингі жүргізілмейді.	Серверлік жабдық микроклимат сақталатын жеке үй-жайларда орналасады. Жауапты қызметкерлерді хабардар ете отырып, микроклиматты мониторингтеу жүзеге асырылады.
27.	Қаржы ұйымында серверлік жабдық кедергілерден қорғалған үздіксіз қорек көзімен қамтамасыз етіледі.	Кедергілерден қорғаныс және серверлік жабдықтың резервтік қорек көзі жоқ.	Сервер жабдығы үшін кедергіден және резервтік қоректен 1 сағатқа дейін қорғау бар.	Сервер жабдығы үшін кедергіден және резервтік қоректен 1 сағаттан артық қорғау бар.
28.	Қаржы ұйымы қауіпсіздіктің нақты аясы шеңберінен шығатын байланыс арналарын қорғауды жүзеге асырады.	Байланыс арналарын қорғау жүзеге асырылмайды.	Қаржы ұйымының стационарлық офистері мен құрылғылары арасындағы байланыс арналарын шифрлау жүзеге асырылады.	Қаржы ұйымының стационарлық кеңселері мен құрылғылары арасындағы байланыс арналарын, сондай-ақ қаржы ұйымының мобильдік құрылғыларымен байланыс арналарын шифрлау жүзеге асырылады.
29.	Қаржы ұйымы оларды қайталап пайдаланар алдында тасымалдағыштардан алынған ақпаратты жоюды жүзеге асырады.	Тасымалдағыштардан ақпаратты жою регламенттелмеген және жүргізілмейді.	Тасымалдағыштардан ақпаратты жою регламенттелген және операциялық жүйелердің штаттық құралдарымен жүргізіледі.	Тасымалдағыштарда ақпаратты жою регламенттелген және ақпаратты арнайы кепілдендірілген жою құралдарымен жүргізіледі.
30.	Қаржы ұйымы жабдықтың қауіпсіздіктің нақты аясының шекарасы арқылы өтуін бақылауды жүзеге асырады.	Жабдықтың қауіпсіздіктің нақты периметрінің шекарасы арқылы өтуін бақылау регламенттелмеген және жүргізілмейді.	Жабдықтың қауіпсіздіктің нақты периметрінің шекарасы арқылы өтуін бақылау регламенттелген және қолмен жүргізу режимінде жүзеге асырылады.	Жабдықтың қауіпсіздіктің нақты периметрінің шекарасы арқылы өтуін бақылау регламенттелген және ішінара немесе толық автоматтандырылған.
31.	Қаржы ұйымы негізгі ақпараттық жүйелердегі өзгерістерді басқару қағидаларын айқындаған.	Негізгі ақпараттық жүйелердегі өзгерістерді басқару қағидалары анықталмаған.	Негізгі ақпараттық жүйелердегі өзгерістерді басқару қағидалары анықталған, өзгерістерді басқару процесі қолмен жүргізу режимінде жүзеге асырылады.	Негізгі ақпараттық жүйелердегі өзгерістерді басқару қағидалары анықталған, өзгерістерді басқару процесі ішінара немесе толық автоматтандырылған.

32.	Қаржы ұйымы негізгі ақпараттық жүйелерді әзірлеу, тестілеу және өнеркәсіптік пайдалану үшін бөлек орталарды қолданады.	Негізгі ақпараттық жүйелерді әзірлеу, тестілеу және өнеркәсіптік пайдалану орталары бөлінбеген.	Негізгі ақпараттық жүйелерді тестілеу және өнеркәсіптік пайдалану орталары бөлінген.	Негізгі ақпараттық жүйелерді әзірлеу, тестілеу және өнеркәсіптік пайдалану орталары бөлінген.
33.	Қаржы ұйымында негізгі ақпараттық жүйелер үшін өзгерістер әзірлейтін қызметкерлер оларды өнеркәсіптік ортаға енгізуді жүзеге асырмайды.	Қызметкерлер негізгі ақпараттық жүйелерге өзгерістерді әзірлеу және енгізу бойынша міндеттерді қоса атқарады.	Өзгерістерді әзірлеу және негізгі ақпараттық жүйелерге енгізу бойынша міндеттер қызметкерлер арасында бөлінген, өнеркәсіптік ортаға әзірлеушілердің кіруі шектелмеген.	Негізгі ақпараттық жүйелерге өзгерістерді әзірлеу және енгізу бойынша міндеттер қызметкерлер арасында бөлінген, әзірлеушілердің өнеркәсіптік ортаға кіруі шектелген.
34.	Қаржы ұйымы бағдарламалық қамтамасыз етуді орнату және зиянды бағдарламалық кодты анықтаған бағдарламалық қамтамасыз етуді үнемі жаңарту, сондай-ақ компьютерлер мен ақпарат тасымалдағыштарында зиянды бағдарламалық кодтың болуына тексеруді жүзеге асырады.	Зиянды бағдарламалық кодты анықтайтын бағдарламалық қамтамасыз ету барлық компьютерлерде орнатылмаған.	Зиянды бағдарламалық кодты анықтайтын бағдарламалық қамтамасыз ету барлық компьютерлерде орнатылған, компьютерлер мен ақпарат тасымалдағыштардың зиянды бағдарламалық кодын тұрақты жаңарту немесе сканерлеу жүзеге асырылмайды.	Зиянды бағдарламалық кодты анықтайтын бағдарламалық қамтамасыз ету барлық компьютерлерде орнатылған, компьютерлер мен ақпарат тасмыалдағыштарында зиянды бағдарламалық кодтың болуын үнемі жаңарту немесе сканерлеу.
35.	Қаржы ұйымы ақпараттың резервтік көшірмелерін және негізгі ақпараттық жүйелердің бағдарламалық қамтамасыз етілуін тұрақты негізде құру, тексеру және тестілеу бойынша процестерді регламенттейді және жүзеге асырады.	Негізгі ақпараттық жүйелердің ақпараттары мен бағдарламалық қамтамасыз етуінің резервтік көшірмелері жасалмайды.	Ақпараттың және негізгі ақпараттық жүйелердің бағдарламалық қамтамасыз етуінің резервтік көшірмелерін жасау регламенттелген және бекітілген регламентке сәйкес жүзеге асырылады. Резервтік көшірмелерді тестілеу жүргізілмейді.	Негізгі ақпараттық жүйелердің ақпараттары мен бағдарламалық қамтамасыз етуінің резервтік көшірмелерін жасау және тестілеу регламенттелген және бекітілген регламентке сәйкес жүзеге асырылады.
	Қаржы ұйымы болашақта жүргізілетін тексерулерге және қол жеткізуді бақылау мониторингін жүргізуге көмектесу мақсатында пайдаланушылардың	Негізгі ақпараттық жүйелердің аудит журналдарын жүргізу реттелмеген, аудит		Негізгі ақпараттық жүйелердің аудит журналдарын жүргізу, теңшеу және сақтау ішкі

36.	іс-әрекеттерін, ақпараттық қауіпсіздіктің штаттан тыс жағдайлары мен оқиғаларын тіркейтін аудит журналдарын жүргізуді және сақтауды жүзеге асырады.	журналдары "әдеттегі" теңшеулермен жүргізіледі немесе жүргізілмейді.	-	бекітілген құжаттарда сипатталған, аудит журналдары бекітілген құжаттарға сәйкес реттеледі, жүргізіледі және сақталады.
37.	Қаржы ұйымы негізгі ақпараттық жүйелерде артықшылықты пайдаланушылардың іс-қимылдарын тіркеуді және тұрақты талдауды қамтамасыз етеді.	Негізгі ақпараттық жүйелерде артықшылықты пайдаланушылардың іс-әрекеттері тіркелмейді.	Негізгі ақпараттық жүйелердегі артықшылықты пайдаланушылардың іс-әрекеттері тіркеледі, бірақ кезең-кезеңмен талданбайды.	Негізгі ақпараттық жүйелердегі артықшылықты пайдаланушылардың іс-әрекеттері кезең-кезеңмен тіркеледі және талданады.
38.	Қаржы ұйымы нақты уақыттың бірыңғай көзі арқылы негізгі ақпараттық жүйелердің жүйелік уақытын синхрондайды.	Қаржы ұйымы шегінде негізгі ақпараттық жүйелердің жүйелік уақыты синхрондалмайды.	-	Қаржы ұйымы шегіндегі негізгі ақпараттық жүйелердің жүйелік уақыты дәл уақыттың бірыңғай көзі арқылы синхрондалады.
39.	Қаржы ұйымында пайдаланушылардың негізгі ақпараттық жүйелерге қолжетімділігі бірегей дербес сәйкестендіргіштер бойынша жүзеге асырылады.	Бір немесе бірнеше негізгі ақпараттық жүйелерге қол жеткізу үшін бірегей дербес сәйкестендіргіш талап етілмейді.	-	Негізгі ақпараттық жүйелерге қолжетімділік бірегей дербес сәйкестендіргіштер бойынша жүзеге асырылады .
40.	Қаржы ұйымында негізгі ақпараттық жүйелерде пайдаланушылардың қолжетімділік деңгейлерін шектеу функционалы пайдаланылады.	Пайдаланушылардың қол жетімділік деңгейлерін ажырату барлық негізгі ақпараттық жүйелерде қолданылмайды.	-	Пайдаланушылардың қол жетімділік деңгейлерін ажырату барлық негізгі ақпараттық жүйелерде қолданылады.
41.	Қаржы ұйымы негізгі ақпараттық жүйелерде пайдаланушылардың парольдерін басқару қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Негізгі ақпараттық жүйелерде пайдаланушылардың парольдерін басқару қағидалары бар құжат жоқ.	-	Қаржы ұйымының барлық қызметкерлеріне жеткізілген , негізгі ақпараттық жүйелерде пайдаланушылардың парольдерін басқару қағидаларын қамтитын бекітілген құжат бар.
	Қаржы ұйымында пайдаланушылардың негізгі ақпараттық жүйелерге	Негізгі ақпараттық жүйелерде		

42.	қолжетімділігінің қолданыстағы құқықтарын кезең-кезеңімен қайта қарау қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	пайдаланушылардың қолжетімділігінің қолданыстағы құқықтарын мерзімді қайта қарау қағидаларын қамтитын құжат жоқ.	-	Негізгі ақпараттық жүйелерде пайдаланушылардың қолжетімділігінің қолданыстағы құқықтарын мерзімді қайта қарау қағидаларын қамтитын бекітілген құжат бар.
43.	Қаржы ұйымында пайдаланушыларды нақты қауіпсіздік аясынан тыс қосу үшін екі немесе көп факторлы аутентификая пайдаланылады.	Пайдаланушыларды нақты қауіпсіздік периметрінен тыс қосу үшін аутентификацияныңбір факторы пайдаланылады.	-	Пайдаланушыларды нақты қауіпсіздік периметрінен тыс қосу үшін екі немесе көп факторлы аутентификация пайдаланылады.
44.	Қаржы ұйымының ақпараттық желісі топтарға бөлінген (VLAN).	Қаржы ұйымының ақпараттық желісін топтарға бөлу көзделмеген.	Қаржы ұйымының ақпараттық желісі ақпаратты өңдеу құралдарының функционалдық белгісі бойынша топтарға бөлінген.	Қаржы ұйымының ақпараттық желісі өңделетін ақпаратты жіктеу негізінде топтарға бөлінген.
45.	Қаржы ұйымында негізгі ақпараттық жүйелерде парольдерді автоматтандырылған басқару функционалы пайдаланылады.	Негізгі ақпараттық жүйелерде парольдерді автоматтандырылған басқару функционалы пайдаланылмайды.	Негізгі ақпараттық жүйелерде пайдаланушылардың парольдерді өз бетінше өзгерту, парольдің мерзімді өзгеруін бақылау функционалы пайдаланылады.	Негізгі ақпараттық жүйелерде пайдаланушылардың парольдерді өз бетінше өзгерту, парольдің мерзімді өзгеруін бақылау, парольдің күрделілігін бақылау, алдыңғы парольдердің қайталануын бақылау функционалы пайдаланылады.
46.	Қаржы ұйымы қашықтан жұмыс жасау режимінде жұмыс істеу қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Қашықтан жұмыс жасау режимінде жұмыс істеу қағидалары бар құжат жоқ.	-	Қашықтан жұмыс жасау режимінде жұмыс істеу қағидаларын қамтитын, қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, бекітілген құжат бар.
47.	Қаржы ұйымы ақпаратты криптографиялық қорғау құралдарын пайдалану қағидаларын қамтитын құжатты бекіткен және қаржы	Ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары бар құжат жоқ.	-	Ақпаратты криптографиялық қорғау құралдарына қолжетімділігі бар қаржы ұйымының барлық қызметкерлерінің назарына жеткізілген, ақпаратты криптографиялық қорғау құралдарын

	ұйымының барлық қызметкерлерінің назарына жеткізген.			пайдалану қағидаларын қамтитын бекітілген құжат бар.
48.	Қаржы ұйымы криптографиялық кілттерді басқару қағидаларын қамтитын құжатты бекіткен және қаржы ұйымының барлық қызметкерлерінің назарына жеткізген.	Криптографиялық кілттерді басқару қағидалары бар құжат жоқ.	-	Криптографиялық кілттерді басқару қағидалары бар бекітілген құжат бар.
49.	Қаржы ұйымында негізгі ақпараттық жүйелердің бастапқы кодтарына кіруді бақылау қамтамасыз етіледі.	Негізгі ақпараттық жүйелердің бастапқы кодтарына кіру шектелмеген.	Негізгі ақпараттық жүйелердің бастапқы кодтарына тек әзірлеушілер ғана кіре алады.	Негізгі ақпараттық жүйелердің бастапқы кодтарына қол жетімділік тек әзірлеушілерге беріледі, бастапқы кодтардағы барлық өзгерістер туралы ақпарат автоматты түрде журналға жазылады.
50.	Қаржы ұйымы негізгі ақпараттық жүйелердің техникалық осалдықтары туралы ақпаратты талдауды, осындай осалдықтардың қауіптілігін бағалауды және оларды жою жөнінде шаралар қабылдауды қамтамасыз етеді.	Негізгі ақпараттық жүйелердің техникалық осалдықтары туралы ақпаратты талдау жүзеге асырылмайды.	-	Негізгі ақпараттық жүйелердің техникалық осалдықтары туралы ақпаратты кезең-кезеңмен талдау, осындай осалдықтардың қауіптілігін бағалау жүзеге асырылады және оларды жою бойынша шаралар қабылданады.
51.	Қаржы ұйымының қызметкелері ақпараттық қауіпсіздіктің кез келген байқалған немесе болжанатын бұзушылықтары туралы дереу хабардар ету қажеттігі туралы біледі.	Қызметкерлерді ақпараттық қауіпсіздікті бұзушылықтар туралы хабардар ету процесі жоқ.	Қызметкерлер ақпараттық қауіпсіздіктің бұзушылықтары туралы хабарлау қажеттігі туралы кезең-кезеңімен хабарланып отырады.	Қызметкерлер ақпараттық қауіпсіздік бұзушылықтары туралы хабарлау қажеттігі туралы кезең-кезеңімен хабарланып отырады, ақпараттық қауіпсіздік бұзушылықтары анықталған кезде қызметкерлердің іс-әрекеттеріне кезең-кезеңімен тексеру жүргізіліп отырады.
52.	Қаржы ұйымы ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою рәсімдерін қамтитын құжатты бекіткен.	Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою рәсімдері қамтылған құжат жоқ.	-	Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою рәсімдері қамтылған, бекітілген құжат бар.
	Қаржы ұйымы ақпараттық қауіпсіздіктің оқыс оқиғаларын тіркеуді	Ақпараттық қауіпсіздіктің оқыс	Ақпараттық қауіпсіздіктің оқыс оқиғаларын тіркеу жүргізіледі,	Ақпараттық қауіпсіздіктің оқыс оқиғаларын тіркеу жүргізіледі, өткен жыл ішінде талдау

53.	және оларды кейіннен талдауды жүргізеді.	оқиғаларын тіркеу жүргізілмейді.	өткен жыл ішінде талдау жүргізілген жоқ.	нәтижелері құжатпен бекітілді.
54.	Қаржы ұйымы ақпараттық инфрақұрылымның енуін тұрақты тестілеуді қамтамасыз етеді.	Қаржы ұйымының ақпараттық инфрақұрылымының енуін тестілеу жүзеге асырылмайды.	Қаржы ұйымының ақпараттық инфрақұрылымының енуін тестілеу жылына бір реттен кем жүзеге асырылады.	Қаржы ұйымының ақпараттық инфрақұрылымының енуін тестілеу жылына кемінде бір рет жүзеге асырылады.
55.	Қаржы ұйымы негізгі ақпараттық жүйелердің бастапқы кодтарының осалдықтарына осындай бастапқы кодтарға қолжетімділік болған кезде талдауды тұрақты түрде жүзеге асырады.	Негізгі ақпараттық жүйелердің бастапқы кодтарын осалдыққа талдау жүзеге асырылмайды.	Негізгі ақпараттық жүйелердің бастапқы кодтарын осалдыққа талдау өнеркәсіптік ортадағы әрбір өзгеріс бойынша емес, ішінара жүзеге асырылады.	Негізгі ақпараттық жүйелердің бастапқы кодтарын осалдыққа талдау өнеркәсіптік ортадағы әрбір өзгеріс алдында жүзеге асырылады.

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