Ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың біліктілігін арттыру жөніндегі талаптарды қоса алғанда, ақпараттық қауіпсіздік бөлімшелерінің басшылары мен жұмыскерлерінің құзыретіне қойылатын талаптарды бекіту туралы

Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2020 жылғы 21 қыркүйектегі № 89 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2020 жылғы 23 қыркүйекте № 21251 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 Заңы 13-6-бабының 3) тармақшасына сәйкес Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Қоса беріліп отырған Ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың біліктілігін арттыру жөніндегі талаптарды қоса алғанда, ақпараттық қауіпсіздік бөлімшелерінің басшылары мен жұмыскерлерінің құзыретіне қойылатын талаптар 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 қаулының осы тармағының 2) тармақшасында көзделген іс-шаралардың 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 агенттігі

Басқармасының
2020 жылғы 21 қыркүйегі
№ 89 қаулысына
қосымша

Ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың біліктілігін арттыру жөніндегі талаптарды қоса алғанда, ақпараттық қауіпсіздік бөлімшелерінің басшылары мен жұмыскерлерінің құзыретіне қойылатын талаптар

1-тарау. Жалпы ережелер

1. Осы Ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың біліктілігін арттыру жөніндегі талаптарды қоса алғанда, ақпараттық қауіпсіздік бөлімшелерінің басшылары мен жұмыскерлерінің құзыретіне қойылатын талаптар (бұдан әрі – Талаптар) "Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы" 2003 жылғы 4 шілдедегі Қазақстан Республикасының Заңына сәйкес әзірленген және меншік нысанына қарамастан Қазақстан Республикасының қаржы ұйымдарының және Қазақстан Республикасы бейрезидент-банктері филиалдарының, Қазақстан Республикасы бейрезидент-сақтандыру (қайта сақтандыру) ұйымдары филиалдарының, Қазақстан Республикасы бейрезидент-сақтандыру брокерлері филиалдарының (бұдан әрі – ұйымдар) ақпараттық қауіпсіздігін қамтамасыз етуге жауапты адамдардың біліктілігін арттыру жөніндегі талаптарды қоса алғанда, ақпараттық қауіпсіздік бөлімшелерінің басшылары мен жұмыскерлерінің (бұдан әрі – жұмыскерлер) құзыретіне қойылатын талаптарды белгілейді.

Ескерту. 1-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 17.02.2021 № 34 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

2. Талаптарда мынадай ұғымдар пайдаланылады:

1) ақпараттық қауіпсіздік – ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қауіптерден қорғалу жағдайы;

2) домен – белгілі бір пән саласындағы білімдер жиынтығы;

3) құзырет – оқу және жеке тәжірибе барысында алынған ақпаратты игеру нәтижесі; оқыту немесе жұмыс саласына жататын білімнің, теорияның және практиканың жиынтығы; бағалауға ұшырайтын біліктілік құрауышы.

Талаптарда "Сәйкестікті бағалау. Қызметкерлерді сертификаттау жөніндегі органдарға қойылатын жалпы талаптар" ISO/IEC 17024-2014 Мемлекетаралық стандартына (бұдан әрі – Стандарт) сәйкес терминдер мен ұғымдар қолданылады.

Ескерту. 2-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 20.10.2022 № 71 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

3. Талаптар мына қағидаттарға негізделеді:

1) типтік лауазымдар бойынша функционалдық міндеттердің ара-жігін ашу;

2) киберқауіпсіздікті қоса алғанда, ақпараттық технологиялар және ақпараттық қауіпсіздік саласындағы білім мен дағдыны бағытқа алу;

3) бағдарламалық қамтамасыз ету және аппараттық жабдықтарды өндірушілердің жұмыскерлерге қойылатын талаптардан тәуелсіздігі;

4) типтік лауазымдарға қойылатын теориялық білімнің және практикалық дағдының , кәсіби құзыреттердің теңгерімі;

5) типтік домендерді пайдалану.

4. Ұйымдағы типтік лауазымдар:

1) маман – функционалдық міндеттеріне ұйымның ақпараттық қауіпсіздігін қамтамасыз ету кіретін ақпараттық қауіпсіздік бөлімшесінің жұмыскері;

2) басшы – функционалдық міндеттеріне ұйымның ақпараттық қауіпсіздік бөлімшесінің қызметін ұйымдастыру кіретін ақпараттық қауіпсіздік бөлімшесінің жұмыскері;

3) жауапты жұмыскер – маман мен басшының функционалдық міндеттерін қатар орындайтын жұмыскер.

5. Құзыреттерді домендерге бөлу:

1) ақпараттық қауіпсіздікті қамтамасыз етуді ұйымдастыру мүмкіндіктері мен ерекшелігінің теңгеріміне;

2) жұмыскерлердің біліктілігін, құзыретін және ұйымның бизнес-процестерінің ерекшеліктерін ескере отырып талаптар қалыптастыруға;

3) жаңа домендер құру есебінен талаптарды кеңейтуге арналған.

2-тарау. Домендердің құрамы

6. Домендер ұйымның қалауы бойынша қажет кезде толықтырылатын, кеңейтілетін құзыреттердің ең аз қажетті тізбесін қамтиды.

7. Типтік домендер құрамы:

1) базалық;

2) құқықтық;

3) ұйымдық;

4) бағдарламалық-аппараттық;

5) телекоммуникациялық;

6) ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдары;

7) ақпараттық қауіпсіздік тәуекелдерін басқару;

8) ақпараттық қауіпсіздік оқыс оқиғаларын басқару.

8. "Базалық" доменінің құрамы – СТ ISO/IEC 27001-2022 "Ақпараттық қауіпсіздік, киберқауіпсіздік және конфиденциалдылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар" Қазақстан Республикасының ұлттық стандартына

немесе ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection – Information security management systems - Requirements" (Информэйшн секьюрити, сайберсекьюрити энд прайвэси протекшн. Информэйшн секьюрити мэнэджмент системс - Реквайрментс) (Ақпараттық қауіпсіздік, киберқауіпсіздік және жеке өмірді қорғау - Ақпараттық қауіпсіздік менеджменті жүйелері – Талаптар) халықаралық стандартына сәйкес киберқауіпсіздікті басқару жүйесінің терминологиясы және талаптары.

Ескерту. 8-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 20.03.2025 № 11 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

9. "Құқықтық" доменінің құрамы:

1) ақпараттық қауіпсіздік саласындағы ұлттық, халықаралық стандарттар;

2) ақпараттық қауіпсіздік саласындағы заңнамалық және нормативтік құқықтық актілер;

3) уәкілетті органдардың ақпарат қорғау жөніндегі әдістемелік құжаттары.

10. "Ұйымдық" доменінің құрамы:

1) басқару қызметінің негіздері, мақсаттары, қағидаттары;

2) ақпараттық-талдау қызметінің негіздері;

3) ақпаратты қорғау жөніндегі негізгі ұйымдық шаралар және іс-шаралар.

11. "Бағдарламалық-аппараттық" доменінің құрамы:

1) бағдарламалық-аппараттық құралдардың жұмыс істеуінің жалпы қағидаттары;

2) ақпаратты қорғайтын бағдарламалық-аппараттық кешендердің құрылуы, жұмыс қағидаттары;

3) ақпаратты қорғайтын бағдарламалық-аппараттық құралдардың ақауларын жою тәртібі.

12. "Телекоммуникациялық" доменінің құрамы:

1) ақпараттық жүйелерді және телекоммуникациялық желілерді құру қағидаттары;

2) телекоммуникациялар желілеріндегі ақпараттық қауіпсіздік қауіптерінің көздері және олардың алдын алу жөніндегі шаралар;

3) телекоммуникациялар объектілерінде пайдаланылатын ақпарат қорғау құралдарының мәні, мақсаттары, мүмкіндіктері;

4) телекоммуникациялар желілерінде ақпараттық рұқсатсыз пайдаланудан қорғау әдістері мен құралдары.

13. "Ақпараттық қауіпсіздік әдістері мен құралдары" доменінің құрамы:

1) ақпараттық қауіпсіздіктің ұйымдық аспектілері;

2) ақпараттық активтерді басқару;

3) қолжетімділікті басқару.

14. "Ақпараттық қауіпсіздік тәуекелдерін басқару" доменінің құрамы:

1) ақпараттық қауіпсіздік тәуекелдерін басқару процесі;

2) тәуекелдер менеджментінің негізгі өлшемшарттары;

3) ақпараттық қауіпсіздік тәуекелдерін бағалау;

4) ақпараттық қауіпсіздік тәуекелдерін өңдеу, қабылдау.

15. "Ақпараттық қауіпсіздік оқыс оқиғаларын басқару" доменінің құрамы:

1) оқыс оқиғаларға ден қою тобының мақсаттары мен міндеттері;

2) оқыс оқиғаларды басқару жоспары.

3-тарау. Білімге және жұмыс тәжірибесіне қойылатын талаптар

16. "Базалық" домені барлық лауазымдар үшін міндетті болып табылады.

17. Маманға "базалық" доменіне қоса кемінде домендердің бірі бойынша құзыреттің болуы туралы талап қойылады.

18. Маманға мына өлшемшарттардың біріне сәйкес келу туралы талап қойылады:

1) домендердің бірі бойынша орташа арнайы немесе жоғары білімнің болуы;

2) бір немесе одан да көп домен бойынша оқудан өту;

3) бір немесе одан да көп домен бойынша кемінде екі жыл жұмыс тәжірибесі;

4) Стандарттың немесе "Conformity assessment - general requirements for bodies operating certification of persons" (Комфомити ассесмент – дженерал реквайрментс фор бодиес операting сертификэйшн оф персонс) (Сәйкестікті бағалау. Қызметкерлерді сертификаттау жөніндегі органдарға қойылатын жалпы талаптар) ISO/IEC 17024:2012 Халықаралық стандартының (бұдан әрі – Халықаралық стандарт) сәйкес берілген, бір немесе одан да көп домен бойынша білімі мен тәжірибесін растайтын сертификаттың болуы.

Ескерту. 18-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 20.10.2022 № 71 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

19. Басшыға қойылатын талаптар ақпараттық қауіпсіздік бөлімшесіне жүктелген міндеттерге сәйкес ең аз қажетті құзыреттер тізбесінен тұрады.

20. Басшыға жоғары білімнің және домендердің бірі бойынша кемінде үш жыл жұмыс тәжірибесінің болуы туралы талап қойылады.

21. Басшының құзыреттерін бағалауды ұйымның ішкі құжаттарына сәйкес жүзеге асырылады. Оның сәйкес келуі туралы шешім құжатпен ресімделеді.

21-1. Талаптардың 4-тармағында көрсетілген, ұйымдағы ақпараттық қауіпсіздік бөлімшесі қызметкерлерінің кемінде бес пайызы Талаптардың 18-тармағы 4) тармақшасының өлшемшарттарына сәйкестігін растайды.

Ескерту. Қағида 21-1-тармақпен толықтырылды - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 20.10.2022 № 71 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

4-тарау. Ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың біліктілігін арттыру жөніндегі талаптар

22. Мамандар мен басшылар 3 (үш) жылда кемінде бір рет домендерде көрсетілген тақырыптар бойынша оқудан немесе сертификаттаудан өту арқылы біліктілік арттырады.

23. Оқудан өту туралы құжаттардың және (немесе) Стандарттың немесе Халықаралық стандарттың сәйкес берілген сертификаттың болуы ақпараттық қауіпсіздікті қамтамасыз етуге жауапты мамандар мен басшылардың біліктілігін арттырудың растауы болып табылады.

Ескерту. 23-тармақ жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 20.10.2022 № 71 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.