Ақпараттық жүйелердің аудитін жүргізу қағидаларын бекіту туралы

Күшін жойған

Қазақстан Республикасы Инвестициялар және даму министрінің м.а. 2016 жылғы 28 қаңтардағы № 134 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2016 жылы 25 ақпанда № 13258 болып тіркелді. Күші жойылды - ҚР Ақпарат және коммуникациялар министрінің 2018 жылғы 13 маусымдағы № 263 бұйрығымен

Ескерту. Күші жойылды - ҚР Ақпарат және коммуникациялар министрінің 13.06.2018 № 263 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы 7-бабы 22) тармақшасына сәйкес, **БҰЙЫРАМЫН:**

1. Қоса беріліп отырған Ақпараттық жүйелердің аудитін жүргізу қағидалары бекітілсін.

2. "Ақпараттық жүйелердің аудитін жүргізу ережесін бекіту туралы" Қазақстан Республикасы Байланыс және ақпарат министрінің 2010 жылғы 20 тамыздағы № 200 бұйрығының (Қазақстан Республикасы нормативтік құқықтық актілерін мемлекеттік тіркеудің тізіліміне N 6488 тіркелген, "Казахстанская правда" газетінде 2010 жылғы 6 қарашада және "Егемен Қазақстан" газетінде 2010 жылғы 9 қарашада жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы Инвестициялар және даму министрлігінің Байланыс, ақпараттандыру және ақпарат комитетіне (Т.Б. Қазанғап):

1) осы бұйрықтың Қазақстан Республикасының Әділет министрлігінде белгіленген заңнама тәртіппен мемлекеттік тіркеуді;

2) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін күнтізбелік он күннің ішінде оның көшірмелерін қағаз және электрондық түрде мерзімді баспа басылымдарында және "Әділет" ақпараттық-құқықтық жүйесінде ресми жариялауға, сондай-ақ тіркелген бұйрықты алған күннен бастап күнтізбелік он күн ішінде Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу үшін Республикалық құқықтық ақпарат орталығына жіберуді;

3) осы бұйрықтың Қазақстан Республикасы Инвестициялар және даму министрлігінің интернет-ресурсында және мемлекеттік органдардың интранет-порталында орналастырылуын;

4) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Инвестициялар және даму министрлігінің Заң департаментіне осы бұйрықтың 3-тармағының 1), 2) және 3) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Инвестициялар және даму вице-министріне жүктелсін.

5. Осы бұйрық оның алғаш ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасы
Инвестициялар және даму
министрінің міндетін атқарушысы Ж. Қасымбек

Қазақстан Республикасы
Инвестиция және даму министрінің
міндетін атқарушысының
2016 жылғы 28 қаңтардағы
№ 134 бұйрығымен бекітілген

Ақпараттық жүйелердің аудитін жүргізу қағидалары

1. Жалпы ереже

1. Осы Ақпараттық жүйелердің аудитін жүргізу қағидалары (бұдан әрі - Қағидалар) "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы

Қазақстан Республикасының Заңы 7-бабының 22) тармақшасына (бұдан әрі - Заң) сәйкес әзірленді және мемлекеттік органдардың ақпараттық жүйелерінің, сондай-ақ мемлекеттік емес ақпараттық жүйелердің аудитін жүргізу тәртібін айқындайды.

2. Ақпараттық жүйелердің аудиті ақпараттық жүйелердің, онда болып жатқан іс-қимылдармен оқиғалардың, техникалық регламенттерге, ақпараттандыру саласындағы стандарттарға, нормативті-техникалық құжаттамаға және (немесе) тапсырыс берушінің талаптарына, сондай-ақ ақпараттық қауіпсіздік талаптарына сәйкестік деңгейін айқындайтын ағымдағы жай-күйін бағалау мақсатында жүзеге асырылады.

3. Осы қағидаларда мынадай ұғымдар пайдаланылады:

1) ақпараттық жүйелердің аудиті – ақпараттық жүйенің қолданылу тиімділігін артыру мақсатында оны тәуелсіз зерттеу;

2) ақпараттық-коммуникациялық инфрақұрылым – электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділікті беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз ету үшін арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

3) ақпараттандыру саласындағы уәкілетті орган (бұдан әрі – уәкілетті орган) – ақпараттандыру және "электрондық үкімет" саласындағы басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган.

4) нормативтік-техникалық құжаттама - ақпараттандыру объектілерін жасауға және пайдалануға, сондай-ақ олардың ақпараттандыру саласындағы белгіленген талаптарға сәйкестігін бақылауға жалпы міндеттерді, қағидаттар мен талаптарды айқындайтын құжаттар жиынтығы;

4. Ақпараттық жүйелердің аудиті ақпараттық жүйелердің меншік иесі немесе иеленушісі бастамасы бойынша ақпараттық жүйелерді жасау, енгізу және пайдалану кезеңінде өткізіледі.

5. Ақпараттық жүйелердің аудитін жүргізу ақпараттық-коммуникациялық технологиялар саласындағы арнайы білімі және жұмыс өтіліне ие жеке және (немесе) заңды тұлғалармен жүзеге асырылады.

6. Мемлекеттік құпияларға жатқызылатын қорғалған орындалудағы ақпараттық жүйелердің аудиті өткізілмейді.

7. Ақпараттық жүйелер аудитінің Тапсырыс берушісі ақпараттық жүйелердің меншік иесі және (немесе) иеленушісі және (немесе) әзірлеушісі болып табылады .

8. Ақпараттық жүйелер аудитінің негізгі бағыттары мыналар:

1) ақпараттық жүйе функциясының оның мақсаты мен міндеттеріне сәйкестігін;

2) ақпараттық жүйені әзірлеу, енгізу, сүйемелдеу және пайдаланудың ақпараттандыру саласындағы стандартқа сәйкестігін;

3) қолданбалы бағдарламалық қамтамасыз ету және деректер қорын қоса алғанда ақпараттық жүйелердің қорғалу деңгейін;

4) ақпараттық-коммуникациялық инфрақұрылым қауіпсіздігінің
жай-күйін, оның техникалық жай-күйі мен топологиясын;

5) нормативтік-техникалық құжаттаманың стандарттық талаптарға сәйкестігін;

6) ақпараттық қауіпсіздік талаптарына сәйкестігін бағалау болып табылады.

9. Ақпараттық жүйелердің аудиті ақпараттық-коммуникациялық технологиялар саласындағы арнайы білімі және жұмыс өтіліне ие тапсырыс беруші мен тұлғаның арасындағы шартқа сәйкес өткізіледі.

10. Мемлекеттік органдардың ақпараттық жүйелерінің аудитін өткізген кезде ақпараттық-коммуникациялық технологиялар саласындағы арнайы білімі және жұмыс өтіліне ие тұлғаларды таңдау, ақпараттық жүйелердің аудитін өткізуге мемлекеттік сатып алу туралы қол қойылатын тиісті шарттың қорытындысы бойынша "Мемлекеттік сатып алу туралы" 2015 жылғы 4 желтоқсандағы Қазақстан Республикасының Заңының 4 тарауына сәйкес жүзеге асырылады.

11. Ақпараттық жүйелердің аудитін өткізу шығыстарын ақпараттық жүйелердің меншік иесі және (немесе) иеленушісі арасындағы келісілген шешім бойынша анықталған тарап көтереді.

12. Ақпараттық жүйенің аудитін өткізу мерзімі ақпараттық жүйенің функционалдық күрделілігіне, құрылымдық құрауыштар (кіші бағдарламалар) санына, оны пайдалану (жұмыс орындарын ұйымдастыру, серверлерге қол жеткізу, өңірлік (аумақтық) ақпараттық жүйеге сүйемелдеу орталықтарының болуы) шартына, сондай-ақ тапсырыс беруші тарапынан ақпараттық жүйелер аудитінің нақты мақсаттарына байланысты болады және шартта көрсетіледі.

13. Ақпараттық жүйе аудитінің нәтижесі бойынша осы Қағидалардың қосымшасына сәйкес нысан бойынша ақпараттық жүйенің аудитін өткізу нәтижелеріне сәйкес (бұдан әрі – қорытынды) аудиторлық қорытынды дайындалады.

14. Қорытынды ақпараттық жүйелердің аудитін жүзеге асыратын тұлғалардың және тапсырыс берушінің қолтаңбаларымен куәландырылады, ақпараттық жүйелердің аудитін жүзеге асыратын тұлғалардың мөрлерімен бекітіледі.

15. Қорытынды 2 (екі) данада мемлекеттік және орыс тілдерінде жасалады, олардың біреуі тапсырыс берушіге табысталады, екіншісі ұйымда қалады.

16. Мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланған мемлекеттік ақпараттық жүйелер және мемлекеттік емес ақпараттық жүйелер бойынша аудиторлық қорытындының көшірмесін тапсырыс беруші ақпараттандыру саласындағы уәкілетті органға тапсырады.

17. Аудиторлық қорытынды ұсынымдық сипатта болады.

2. Ақпараттық жүйелердің аудитін өткізу тәртібі

18. Ақпараттық жүйелер аудитінің міндеті мен негізгі мақсаттары:

1) ақпараттық ресурстардың ағымдағы қорғалу жай-күйін объективті және тәуелсіз бағалауды алу;

2) ақпараттық қауіпсіздік жүйесін құруға инвестицияланған қаржылардан барынша қайтарым алу;

3) санкцияланбаған іс-әрекеттерден келетін мүмкін болатын залалдарды бағалау;

4) ақпаратты қорғау жүйесін құруға қойылатын талаптарды әзірлеу;

5) бөлімше қызметкерлерінің жауапкершілік аймағын айқындау;

6) ақпараттық қауіпсіздік жүйесін енгізу тәртібін және бірізділігін әзірлеу болып табылады.

19. Ақпараттық жүйелер қауіпсіздігі аудитінің міндеттері:

1) ақпараттық жүйелерді қорғау жөніндегі қауіпсіздік саясатын әзірлеуді және басқа да ұйымдастыру-өкім беру құжаттарын талдау және бағалау;

2) ақпараттық жүйелер ресурстарына қатысты қауіпсіздігіне қауіп төндіру мүмкіндігіне байланысты тәуекелдерді талдау;

3) ақпаратты қорғауды қамтамасыз етуге қатысты персонал үшін міндеттердің қойылымын бағалау;

4) ақпараттық қауіпсіздікті бұзуға байланысты тосын оқиғаларды шешуге қатысуды бағалау;

5) ақпараттық жүйелерді қорғау жүйесінде осал жерлерді жою;

6) ақпараттық жүйелерді пайдаланушылар мен қызмет көрсететін персоналды ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне үйретуге қатысу дәрежесін айқындау;

7) ақпараттық жүйелердің қолданыстағы қауіпсіздік тетіктерінің тиімділігін арттыру және жаңаларын енгізу жөніндегі ұсынымдарды әзірлеу болып табылады.

20. Ақпараттық жүйелердің аудиті жөніндегі жұмыстар, жалпы алғанда ақпараттық жүйелердің аудитін өткізу кезеңдеріне сәйкес келетін бірқатар реттік кезеңдерді қамтиды:

1) ақпараттық жүйелердің аудитін өткізуге бастамашылық жасау;

2) ақпараттық жүйелер аудитінің ақпаратын жинау;

3) ақпараттық жүйелер аудитінің деректерін талдау;

4) ұсынымдар қалыптастыру;

5) қорытынды дайындау.

21. Ақпараттық жүйелер аудиті бойынша негізгі жұмыс түрлеріне:

1) талдауды сарапшылық әдіспен жүргізу;

2) Заңның 6-бабының 3) тармақшасына сәйкес бекітілген ақпараттық коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ақпараттық қауіпсіздік және бірыңғай талаптар жөніндегі стандарттардың ұсынымдарға сәйкестігін бағалау;

3) ақпараттық жүйелер құрауыштарын аспаптық тексеру жатқызылады.

22. Сарапшылық әдіспен талдау жүргізу барысында зерттеу рәсіміне қатысушы сарапшылардың тәжірибесі негізінде ақпаратты қорғау шаралары жүйесінде кемшіліктер анықталады.

23. Әкімшілік, рәсімдік және физикалық қорғау шараларын қоса алғанда ұйымдастыру деңгейінің қауіпсіздік тетіктерін бағалау үшін өлшем шарттар ретінде ҚР СТ ИСО/МЭК 27001-2008 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету шаралары мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар", ҚР СТ ИСО/МЭК 27002-2009 "Ақпараттық технология. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы"

және ҚР СТ МЕМСТ Р 50739-2006 "Есептеу техникасының құралдары. Ақпаратқа заңсыз қол жеткізуден қорғау. Жалпы техникалық талаптар" стандарттары қолданылады.

24. ҚР СТ ИСО/МЭК 27001-2008 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйесі . Талаптар", ҚР СТ ИСО/МЭК 27002-2009 "Ақпараттық технологиялар. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы" стандарттары бойынша ақпараттық жүйелер аудитінің негізгі басты өлшем шарттарына келесі тараулар:

1) қауіпсіздік саясаты;

2) қорғауды ұйымдастыру;

3) ресурстарды жіктеу және оларды бақылау;

4) персонал қауіпсіздігі;

5) физикалық қауіпсіздік;

6) ақпараттық жүйелерді және есептеу желілерін әкімшілендіру;

7) қолжетімділікті басқару;

8) ақпараттық жүйелерді әзірлеу және сүйемелдеу;

9) ұйымның үздіксіз жұмысын жоспарлау;

10) қауіпсіздік саясаты талаптарының орындалуын бақылау жатқызылады.

25. ҚР СТ МЕМСТ Р 50739-2006 "Есептеу техникасының құралдары. Ақпаратты заңсыз қолжетімділіктен қорғау. Жалпы техникалық талаптар" бойынша ақпараттық жүйелер аудитінің басты негізгі өлшемдеріне:

1) қолжетімділікті шектеуге қойылатын негізгі талаптарды іске асыру (қолжетімділікті бақылаудың дискретизациялық қағидаты);

2) қолжетімділікті бақылаудың мандатты қағидатын іске асыру;

3) пайдаланушылардың қолжетімділігін сәйкестендірілуді және бірдейлестіруді іске асыру;

4) тіркеу көрсеткіші;

5) құжаттарды таңбалау;

6) кепілдіктерге қойылатын негізгі талаптар;

7) құжаттамаларға қойылатын талаптар жатқызылады.

26. Ақпараттық жүйелердің құрауыштарын аспаптық зерттеу кезінде олар жүйенің бағдарламалық-аппараттық қамтамасыз етудің осалдықтарын анықтау және жоюға бағытталады.

27. Ақпараттық жүйелер аудиті нәтижелерін ресімдеу:

1) ҚР СТ ИСО/МЭК 27001-2008 "Ақпараттық технология". Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар", ҚР СТ ИСО/МЭК 27002-2009 "Ақпараттық технологиялар. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы"

және ҚР СТ МЕМСТ Р 50739-2006 "Есептеу техникасының құралдары. Ақпаратты заңсыз қолжетімділіктен қорғау. Жалпы техникалық талаптар" стандарттарына сәйкестігін бағалау;

2) аспаптық тексеру нәтижелері;

3) ұсынымдар әзірлеу;

4) аудиторлық қортындыны дайындауды қамтиды.

Ақпараттық жүйелердің аудитін
жүргізу қағидаларына қосымша

Нысан

Ақпараттық жүйелердің аудитін өткізу нәтижелері бойынша аудиторлық қорытынды

_____
___
(ақпараттық жүйенің атауы)

_____
___
(тапсырыс беруші ұйымның атауы)

_____
саласында
(аудит өткізу саласы)
20__ ж. "___" _____

_____
___
(ақпараттық жүйелер аудитін жүзеге асыратын тұлғаның атауы)
20__ ж. "___" _____ шартқа сәйкес Ақпараттық жүйелердің аудитін өткізу қағидасына сәйкес аудит өткізілді (өткізілген аудиттің ұйымдастырушылық, техникалық, әдістемелік аспектілерімен ақпараттық жүйелердің аудитін өткізу туралы есептеме қоса беріліп отыр).
Аудиторлық тексеру барысында осы ақпараттық жүйе мынадай бағалау көрсеткіштеріне ие екені анықталды:

1. _____
__
2. _____
__
3. _____
__

_____
саласындағы

белгіленген талаптар мен стандарттарға сәйкес келеді/сәйкес келмейді_____
__
(аудитті өткізу саласы)
Ақпараттық жүйені сүйемелдеу және дамыту жөніндегі ұсынымдар
_____
___
_____
___
20__ ж. "___" _____ _____
(ТАӘ, қолы)