Ақпараттық жүйелердің аудитін жүргізу қағидаларын бекіту туралы

Қазақстан Республикасы Ақпарат және коммуникациялар министрінің 2018 жылғы 13 маусымдағы № 263 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 29 маусымда № 17141 болып тіркелді.

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

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

2. "Ақпараттық жүйелердің аудитін жүргізу қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 28 қаңтардағы № 134 бұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 13258 болып тіркелген, 2016 жылғы 10 наурызда " Әділет" ақпараттық-құқықтық жүйесінде жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы Ақпарат және коммуникациялар министрлігінің Ақпараттандыру департаменті заңнамада белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық мемлекеттік тіркелген күннен бастап күнтізбелік он күн ішінде оны " Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкінде ресми жариялау және енгізу үшін жіберуді;

3) осы бұйрықты Қазақстан Республикасы Ақпарат және коммуникациялар министрлігінің интернет-ресурсында орналастыруды;

4) осы бұйрық мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде осы тармақтың 1), 2) және 3) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді Қазақстан Республикасы Ақпарат және коммуникациялар министрлігінің Заң департаментіне ұсынуды қамтамасыз етсін.

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Ақпарат және коммуникациялар вице-министріне жүктелсін.

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

Қазақстан Республикасының
Ақпарат және коммуникациялар министрі *Д. Абаев*

"КЕЛІСІЛДІ"
Қазақстан Республикасының

Қорғаныс және аэроғарыш
өнеркәсібі министрі
Б. Атамқұлов
2018 жылғы "__"_____

Қазақстан Республикасы
Ақпарат және коммуникациялар
министрінің 2018 жылғы
13 маусымдағы № 263
бұйрығымен бекітілген

Ақпараттық жүйелердің аудитін жүргізу қағидалары

1-тарау. Жалпы ережелер

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 ақпараттық жүйелерге аудит жүргізу тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар пайдаланылады:

1) ақпараттандыру объектілерінің иеленушісі – ақпараттандыру объектілерінің меншік иесі заңда немесе келісімде айқындалған шектерде және тәртіппен ақпараттандыру объектілерін иелену және пайдалану құқықтарын берген субъект;

2) ақпараттық жүйенің аудиті – ақпаратық жүйені пайдалану тиімділігін арттыру мақсатында оны тәуелсіз зерттеп-қарау;

3) ақпараттық-коммуникациялық инфрақұрылым – электрондық ақпараттық ресурстарды қалыптастыру және оларға қол жеткізуді ұсыну мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

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

5) нормативтік-техникалық құжаттама – ақпараттандыру объектілерін құруға және пайдалануға (іске қосуға), сондай-ақ олардың ақпараттандыру саласындағы белгіленген талаптарға сәйкестігін бақылауға қойылатын жалпы міндеттерді, қағидаттар мен талаптарды айқындайтын құжаттар жиынтығы.

3. Ақпараттық жүйенің аудиті:

1) ақпараттық жүйенің ағымдағы жай-күйінің, онда болып жатқан олардың ақпараттандыру саласындағы техникалық регламенттерге, стандарттарға сәйкестік деңгейін айқындайтын әрекеттер мен оқиғалардың бағасын алу;

2) нормативтік-техникалық құжаттаманың тапсырыс берушінің талаптарына, сондай-ақ ақпараттық қауіпсіздік талаптарына сәйкестігін белгілеу мақсатында жүзеге асырылады.

4. Ақпараттық жүйелер аудитінің міндеттері:

1) Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға (бұдан әрі – бірыңғай талаптар) сәйкестігін бағалау;

2) ақпараттық жүйелерді қорғау жөніндегі қауіпсіздік саясатының әзірлемелерін және басқа да ұйымдастырушылық-өкімдік құжаттарды талдау және бағалау;

3) ақпараттық жүйелер ресурстарына қатысты қауіпсіздік қатерлерін жүзеге асыру мүмкіндігіне байланысты тәуекелдерді талдау;

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

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

6) ақпараттық жүйелерді қорғау жүйесінде осал жерлерді оқшаулау;

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

8) жаңа ақпараттық жүйелерді енгізу және ақпараттық жүйелердің қолданыстағы қауіпсіздік тетіктерінің тиімділігін арттыру жөнінде ұсынымдар әзірлеу;

9) ақпараттық жүйе функцияларының оның мақсаттары мен міндеттеріне сәйкестігін бағалау;

10) ақпараттық жүйені әзірлеудің, енгізу мен пайдаланудың ақпараттандыру саласындағы техникалық регламенттерге, стандарттарға сәйкестігін бағалау;

11) қолданбалы бағдарламалық қамтылымды және деректер базасын қоса алғанда, ақпараттық жүйелердің қорғалу деңгейін бағалау;

12) ақпараттық-коммуникациялық инфрақұрылымның жай-күйін, оның техникалық жай-күйі мен топологиясын бағалау;

13) нормативтік-техникалық құжаттаманың Қазақстан Республикасының ақпараттандыру саласындағы заңнамасының талаптарына сәйкестігін бағалау болып табылады.

2-тарау. Ақпараттық жүйелердің аудитін жүргізу тәртібі

5. Ақпараттық жүйелердің аудиті ақпараттық жүйелердің меншік иесінің немесе иеленушісінің бастамасы бойынша ақпараттық жүйелерді жасау, енгізу және пайдалану кезеңінде жүргізіледі.

6. Ақпараттық жүйелердің аудитін жүргізуді ақпараттық-коммуникациялық технологиялар саласында арнайы білімі және жұмыс тәжірибесі бар жеке немесе заңды тұлғалар (бұдан әрі – аудитор) жүзеге асырады.

7. Мемлекеттік құпияларға жатқызылған, қорғалып орындалатын ақпараттық жүйелердің аудиті жүргізілмейді.

8. Ақпараттық жүйелер аудитінің тапсырыс берушісі ақпараттық жүйенің меншік иесі және (немесе) иеленушісі болып табылады.

9. Ақпараттық жүйелердің аудиті тапсырыс беруші мен аудитор арасындағы шартқа сәйкес жүргізіледі.

10. Ақпараттық жүйенің аудитін жүргізу мерзімі ақпараттық жүйенің функционалдық күрделілігіне, құрылымдық компоненттердің (кіші бағдарламалардың) санына, оны пайдалану (жұмыс орындарын ұйымдастыру, серверлерге қол жеткізу, өңірлік (аумақтық) ақпараттық жүйені сүйемелдеу орталықтарының болуы) шарттарына, сондай-ақ тапсырыс беруші тарапынан ақпараттық жүйе аудитінің нақты мақсаттарына байланысты болады және шартта көрсетіледі.

11. Мемлекеттік заңды тұлғалардың ақпараттық жүйелерінің аудитін жүргізген кезде аудиторды таңдау "Мемлекеттік сатып алу туралы" 2015 жылғы 4 желтоқсандағы Қазақстан Республикасының Заңына сәйкес жүзеге асырылады.

12. Ақпараттық жүйелердің аудиті бойынша жұмыстар бірқатар сатылы кезеңдерді:

ақпараттық жүйелердің аудиті рәсіміне бастамашылық жасауды;

ақпараттық жүйелер аудитінің ақпаратын жинауды;

ақпараттық жүйелер аудитінің деректерін талдауды;

ұсынымдар әзірлеуді;

қорытынды дайындауды және қол қоюды қамтиды.

13. Ақпараттық жүйелер аудиті бойынша жұмыстардың түрлеріне:

талдауды сараптамалық әдіспен жүргізу;

ақпараттық қауіпсіздік жөніндегі стандарттардың ұсынымдарына және бірыңғай талаптарға сәйкестігін бағалау;

ақпараттық жүйелердің компоненттерін ақпараттық зерттеп-қарау жатады.

14. Сараптамалық әдіспен талдау жүргізу барысында зерттеп-қарау рәсіміне қатысатын сарапшылардың тәжірибесі негізінде ақпаратты қорғау шаралары жүйесіндегі кемшіліктер анықталады.

15. Әкімшілік, рәсімдік және физикалық қорғау шараларын қоса алғанда, ұйымдастыру деңгейінің қауіпсіздік тетіктерін бағалау үшін өлшемшарттар ретінде ҚР СТ ИСО/МЭК 27002-2015 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару құралдары жөніндегі қағидалар жиынтығы және ҚР СТ МЕМСТ Р 50739-2006 "Есептеу техникасының құралдары. Ақпаратқа санкцияланбаған қол жеткізуден қорғау. Жалпы техникалық талаптар" стандарттары пайдаланылады.

16. Ақпараттық жүйелердің компоненттерін аспаптық зерттеп-қарау кезінде компоненттер жүйенің бағдарламалық-аппараттық қамтылымының осалдықтарын анықтауға және жоюға бағытталады.

17. Ақпараттық жүйелер аудиті нәтижелерін ресімдеу:

1) ҚР СТ ИСО/МЭК 27002-2015 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару құралдары бойынша қағидалар жиынтығы" және ҚР СТ МЕМСТ Р 50739-2006 "Есептеу техникасының құралдары. Ақпаратқа санкцияланбаған қол жеткізуді қорғау. Жалпы техникалық талаптар" стандарттарына сәйкестігін бағалауды;

2) аспаптық зерттеп-қарау нәтижелерін шығаруды;

3) ұсынымдар әзірлеуді;

4) қорытынды дайындауды қамтиды.

18. Ақпараттық жүйенің аудиті аяқталған күннен бастап күнтізбелік 30 күннен аспайтын мерзімде осы Қағидаларға қосымшаға сәйкес нысан бойынша аудиторлық қорытынды (бұдан әрі – қорытынды) дайындалады.

19. Қорытынды қазақ және орыс тілдерінде екі данада жасалады, оның біреуі тапсырыс берушіге беріледі, екіншісі аудиторда қалады.

20. Қорытынды ұсынымдық сипатта болады.

Ақпараттық жүйелердің аудитін
жүргізу қағидаларына
қосымша
Нысан

Ақпараттық жүйелердің аудитін жүргізу нәтижелері бойынша аудиторлық қорытынды

_____

_____(ақпараттық жүйенің атауы)

_____

(тапсырыс беруші ұйымның атауы)

_____

_____саласында

(аудит жүргізу саласы)

20__жылғы "__"_____

_____

_____

(ақпараттық жүйелердің аудитін жүзеге асыратын жеке тұлғаның және (немесе) заңды тұлғаның тегі, аты, әкесінің аты (бар болған жағдайда)

_____

20_ жылғы "__" _____ шартқа сәйкес Ақпараттық жүйелердің аудитін

жүргізу қағидаларына сәйкес аудит жүргізіледі. Аудиторлық тексеру барысында осы ақпараттық жүйе мынадай бағалау көрсеткіштеріне ие екені анықталады:

1._____

2. _____

3. _____

_____саласындағы

(аудитті жүргізу саласы)

белгіленген талаптар мен стандарттарға сәйкес келеді/сәйкес келмейді_____

Ақпараттық жүйені сүйемелдеу және дамыту жөніндегі ұсынымдар

_____

_____

_____

20__жылғы"__"_____

_____

(тегі, аты, әкесінің аты (бар болған жағдайда), қолы)

Мөр (бар болған жағдайда) орны