Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесін бекіту туралы

Күшін жойған

Қазақстан Республикасы Инвестициялар және даму министрінің м.а. 2016 жылғы 28 қаңтардағы № 108 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2016 жылы 25 ақпанда № 13236 болып тіркелді. Күші жойылды - Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 51/НҚ бұйрығымен

Ескерту. Күші жойылды – ҚР Қорғаныс және аэроғарыш өнеркәсібі министрінің 28.03.2018 № 51/НҚ (алғаш ресми жарияланған күнінен бастап күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының заңы 7-бабының 26) тармақшасына сәйкес **БҰЙЫРАМЫН:**

1. Қоса беріліп отырған Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесі бекітілсін.

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

1) осы бұйрықтың Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелуін;

2) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін оның көшірмелерін баспа және электрондық түрде күнтізбелік он күн ішінде 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 бұйрықты Қазақстан Республикасы Инвестициялар және даму министрлігінің интернет-ресурсында және мемлекеттік органдардың интранет-порталында орналастыруды;

4) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы

Инвестициялар және даму министрлігінің Заң департаментіне осы бұйрықтың 2-тармағының 1), 2) және 3) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

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

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

Қазақстан Республикасы
Инвестициялар және даму
министрінің міндетін атқарушы Ж. Қасымбек

Қазақстан Республикасы
Инвестициялар және даму
министрінің міндетін атқарушының
2016 жылғы 28 қаңтардағы
№ 108 бұйрығымен бекітілген

Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттау жүргізу әдістемесі

1. Жалпы ережелер

1. Осы Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттау жүргізу әдістемесі (бұдан әрі – Әдістеме) "Ақпараттандыру туралы" 2015 жылғы 25 қарашадағы Қазақстан Республикасы заңының 7-бабы 26) тармақшасына (бұдан әрі – Заң) сәйкес әзірленді.

2. Осы Әдістеме ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттау жүргізуге арналған.

3. Осы Әдістемеде мынадай негізгі ұғымдар және қысқартулар пайдаланылады:

1) ақпараттық активтер – дерекқорлары, жүйелік құжаттама, пайдаланушыға арналған басшылықтар, есеп материалдары, аттестаттау объектісін пайдалану немесе қолдау процедуралары, ақпараттық қамтамасыз етудің үздіксіз жұмыс істеуін қамтамасыз ету жөніндегі жоспарлар және басқа құжаттама;

2) ақпараттық жүйе (бұдан әрі – АЖ) – ақпараттық өзара іс-қимыл арқылы белгілі технологиялық іс-қимылдарды іске асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсетуші персоналдың және техникалық құжаттаманың ұйымдастырушылық-реттелген жиынтығы;

3) ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттау (бұдан әрі - аттестаттау) – аттестаттау объектілерінің қорғалу жай-күйін, сондай-ақ олардың ақпараттық қауіпсіздік талаптарына сәйкестігін анықтау бойынша ұйымдастырушылық-техникалық іс-шаралар;

4) ақпараттық қауіпсіздік жөніндегі техникалық құжаттама (бұдан әрі - АҚ жөніндегі ТҚ) – ақпараттық қауіпсіздік саласындағы стандарттарға сәйкес әзірленген және аттестаттау объектісінің ақпараттық қауіпсіздігін қамтамасыз ету бойынша жалпы талаптары мен қағидаттарын реттейтін құжаттар жиынтығы;

5) ақпараттық саласындағы ақпараттық қауіпсіздік (бұдан әрі – АҚ) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және әшкі қатерлерден қорғалу жай-күйі;

6) аутентификация – пайдаланушы (қолжеткізу субъектісі) үшін ол ұсынған сәйкестендіргішті тексеру және оның түпнұсқалығын трастау;

7) аттестаттау объектілері – мемлекеттік органның ақпараттық жүйесі, мемлекеттік органның ақпараттық жүйесімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйе, ақпараттық-коммуникациялық инфрақұрылымның өте маңызды өбъектілеріне жатқызылған ақпараттық жүйе, электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасы, мемлекеттік органның интернет-ресурсы, мемлекеттік емес ақпараттық жүйе, мемлекеттік емес интернет-ресурс;

8) аттестаттау объектісінің инфрақұрылымы компоненттерін аспаптық тексеру – байланыс арналарын, тораптарын, серверлерді, жұмыс станцияларын, қолданбалы және жүйелік бағдарламалық қамтамасыз етуді, дерекқорлары мен желі элементтерін бағдарламалық құрал немесе қашықтықтағы не локальдық диагностика арқылы олардағы осалдықтарды айқындауға қатысты сканерлеу жүргізу;

9) аттестаттау объектісінің осалдығы – аттестаттау объектісінің жұмыс қабілеттігін бұза алатын немесе ақпаратты қорғаудың қолданыстағы құралдарын пайдаланбай, рұқсатсыз қол жеткізуге әкеп соғатын аттестаттау объектісіндегі кемшілік;

10) аттестаттық тексеру – аттестаттау объектісінің техникалық құжаттамасын зерттеуге, талдауға, бағалауға бағытталған ұйымдастырушылық-техникалық іс-шаралар кешені, ақпараттық қауіпсіздік талаптарын орындау бойынша жұмыстарды ұйымдастыру жай-күйін тексеру;

11) бағдарламалық қамтамасыз ету (бұдан әрі – БҚ) – бағдарламалардың, бағдарламалық кодтардың, сондай-ақ бағдарламалық өнімдердің оларды пайдалану үшін қажетті техникалық құжаттамасының жиынтығы;

12) қорғау құралдары кешені (бұдан әрі – ҚҚК) – есептеу техникасы құралдарын немесе ақпараттық жүйелерді ақпаратқа рұқсатсыз қол жеткізуден қорғауды қамтамасыз ету үшін құрылатын және қолдау көрсетілетін бағдарламалық және техникалық құралдар жиынтығы;

13) физикалық активтер – аттестаттау объектісінде пайдаланылатын серверлік жабдық, байланыс жабдығы, магниттік тасығыштар мен техникалық жабдық.

4. Осы Әдістемеде келесі нормативтік құқықтық актілер мен стандарттар қолданылады:

1) "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының заңы;

2) Заңның 6-бабының 5) тармақшасына сәйкес бекітілетін Ақпараттық жүйені , "электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттау жүргізу қағидалары;

3) Заңның 6-бабының 3) тармақшасына сәйкес бекітілетін Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар (бұдан әрі – БТ);

4) ҚР СТ ИСО/МЭК 27002-2009 Қауіпсіздікті қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі қағидалар жинағы (бұдан әрі – ҚР СТ ИСО/МЭК 27002-2009);

5) ҚР СТ ИСО/МЭК 27001-2008 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар (бұдан әрі – ҚР СТ ИСО/МЭК 27001-2008);

6) ҚР СТ ИСО/МЭК 50739-2006 Есептеу техникасы құралдары. Ақпаратқа рұқсатсыз қол жеткізуден қорғау. Жалпы техникалық талаптар (бұдан әрі - ҚР СТ ИСО/МЭК 50739-2006).

5. Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық тұғырнамасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық тексеру мына тәртіппен жүргізіледі:

1) аттестаттау объектісінің құрылымын алдын ала зерттеу;

2) АҚ жөніндегі ТҚ зерделеу, талдау және бағалау;

3) аттестаттау объектісін аспаптық тексеруді қоса алғанда, БТ, ҚР СТ ИСО / МЭК 27001-2008 және ҚР СТ ИСО / МЭК 27002-2009, ҚР СТ ГОСТ Р 50739-95-2006, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстарды ұйымдастыру жай-күйін тексеру;

4) аттестаттық тексеру актісін жасау.

2. Аттестаттау объектісінің құрылымын алдын ала зерттеу

6. Аттестаттау объектісінің құрылымын алдын ала зрттеу аттестаттау объектісінің жұмыс істеу ерекшеліктерін айқындау және аттестаттау объектісінде пайдаланылатын аппараттық-бағдарламалық құралдар, локальдық және корпоративтік желі, ақпаратты қорғау технологиялары мен процедуралар туралы жалпы ақпарат алу мақсатында жүргізіледі.

7. Құрылымды алдын ала зерттеу процесі келесі техникалық құжаттамамен танысуды қамтиды:

1) аттестаттау объектісін құрудың техникалық тапсырмасы;

2) аттестаттау объектісінің жалпы функционалдық және локальдық схемасы;

3) аттестаттау объектісінде пайдаланылатын бағдарламалық және техникалық құралдар тізбесі;

4) көрсетілетін ақпараттық-коммуникациялық қызметтерді пайдалануға арналған шарт (аттестаттау объектісі ақпараттық-коммуникациялық қызметтерді пайдаланған жағдайда).

3. АҚ жөніндегі ТҚ зерттеу, талдау және бағалау

8. АҚ жөніндегі ТҚ зерттеу, талдау және бағалау ақпараттық қауіпсіздік бойынша талаптардың толықтығын, өзектілігін және БТ, ҚР СТ ИСО/МЭК 27001 -2008 және СТ РК ИСО/МЭК 27002-2009 талаптарына дұрыстығын тексеру мақсатында жүргізіледі.

9. Ақпараттық қауіпсіздік талаптарына сәйкестігіне зерттеу, талдау және бағалау жүргізілетін АҚ жөніндегі ТҚ:

1) ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат);

2) ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және маркалау қағидалары (бұдан әрі – Сәйкестендіру қағидалары);

3) ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі (бұдан әрі – Тәуекелдерді бағалау әдістемесі);

4) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмыс істеуін қамтамасыз ету қағидалары (бұдан әрі – Жұмыстың үздіксіздігін қамтамасыз ету қағидалары);

5) есептеу техникасы құралдарын, телекоммуникациялық жабдықты және бағдарламалық қамтамасыз етуді түгендеу мен паспорттандыру қағидалары (бұдан әрі – Түгендеу қағидалары);

6) ішкі ақпараттық қауіпсіздік аудитін өткізу қағидалары (бұдан әрі – ішкі аудит қағидалары);

7) ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары (бұдан әрі – Криптографиялық құралдарды пайдалану қағидалары);

8) электрондық ресурстарға қол жеткізу құқықтарын бөлу қағидалары (бұдан әрі – Қол жеткізу құқықтарын шектеу қағидалары);

9) Интернетті және электрондық поштаны пайдалану қағидалары;

10) аутентификация процедурасын ұйымдастыру қағидалары;

11) вирусқа қарсы бақылауды ұйымдастыру қағидалары;

12) мобильдік құрылғыларды және ақпаратты тасығыштарды пайдалану қағидалары (бұдан әрі - Мобильдік құрылғыларды пайдалану қағидалары);

13) ақпаратты өндеу құралдарын физикалық қорғауды және ақпараттық ресурстардың қауіпсіз жұмыс істеу ортасын ұйымдастыру қағидалары (бұдан әрі – Физикалық қорғауды ұйымдастыру қағидалары);

14) әкімшінің аттестаттау объектісін сүймелдеу жөніндегі басшылығы (бұдан әрі – Әкімші басшылығы);

15) Ақпаратты резервтік көшіру және қалпына келтіру регламенті (бұдан әрі - Резервтік көшіру регламенті);

16) пайдаланушылардың АҚ инциденттеріне және штаттан тыс (дағдарысты) жағдайларда әрекет етуі бойынша іс-қимыл тәртібі туралы нұсқаулық (бұдан әрі – Штаттан тыс жағдайлар бойынша нұсқаулық).

10. Әрбір АҚ жөніндегі ТҚ таныстыру парағының болуына қатысты, оның толықтығы мен өзектілігін тексеру қажет.

11. АҚ жөніндегі ТҚ зерттеу, талдау және бағалаудың нәтижелері аттестаттық тексеру актісінде белгіленеді.

1-параграф. Саясатты зерттеу, талдау және бағалау

12. Саясатты зерттеу, талдау және бағалау Саясаттың негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) АҚ маңыздылығын ақпаратты бірлесіп пайдалану мүмкіндігін қамтамасыз ететін аспап ретінде ашу арқылы Саясаттың негізгі мақсаттары мен қағидаттары;

2) АҚ қамтамасыз ету бойынша мақсаттарға қол жеткізу жөніндегі басшылық іс-әрекеттерінің сипаттамасы;

3) мемлекеттік орган немесе ұйым үшін барынша маңызды қауіпсіздік саясаттарының, қағидаттардың, қағидалар мен талаптардың сипаттамасы;

4) Саясатты бұзу жағдайындағы талаптар;

5) АҚ басқару шеңберіндегі жалпы анықтамаларды және қызметкерлердің функциялары;

6) Саясатты мерзімді қайта қарауға қойылатын талаптар;

7) басшылықтың АҚ мәселелерін қолдау бойынша функциялары.

13. Саясатты зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 12-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Саясат АҚ талаптарына сәйкес;

2) осы Әдістеменің 12-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Саясат АҚ талаптарына сәйкес емес.

2-параграф. Сәкестендіру қағидаларын зерттеу, талдау және бағалау

14. Сәкестендіру қағидаларын зерттеу, талдау және бағалау Сәкестендіру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) активтердің құқықтық талаптарына, олардың құпиялығына, сондай-ақ құндылығы мен маңыздылығына сүйене отырып, оларды (ақпараттық активтер, физикалық активтер және басқа) сәйкестендіруді және сыныптауды жүргізу тәртібі;

2) сәйкестендірілген активтерге жауапты тұлғаларды бекіту;

3) активтер тізілімін құру және жүргізу (актив тобын, актив түрін, маңыздылығы мен активтің иесін көрсетумен);

4) активтердің белгіленген тобына, құпиялығына, құндылығы мен маңыздылығына байланысты маркалау тәртібі;

5) мәліметтердің толықтығына қатысты активтер тізілімінің нысаны бойынша талаптар.

15. Сәкестендіру қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 14-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Сәкестендіру қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 14-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Сәкестендіру қағидалары АҚ талаптарына сәйкес емес.

3-параграф. Тәуекелдерді бағалау әдістемесін зерттеу, талдау және бағалау

16. Тәуекелдерді бағалау әдістемесін зерттеу, талдау және бағалау Тәуекелдерді бағалау әдістемесі негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) тәуекелдерді бағалау әдістемесін таңдау, тәуекелдерді сәйкестендіруді орындау;

2) ақпараттың құндылығы мен маңыздылығын анықтау бойынша әдістемелердің сипаттамасы;

3) АҚ тәуекелдерінің мониторингі, қайта қаару және өзгерту тәртібінің сипаттамасы;

4) аттестаттау объектісінің ақпараттық қауіпсіздік тәуекелдерін анықтау әдістерінің және реттілігінің сипаттамасы;

5) айқындалған тәуекелдерді бағалау әдісінің және реттілігінің сипаттамасы;

6) тәуекелдерді өңдеу әдісінің сипаттамасы;

7) ақпараттық қауіпсіздік қатерлерін және көздерін айқындау және талдау әдісінің сипаттамасы;

8) инциденттің ықтималдығын айқындау әдісінің сипаттамасы;

9) тәуекелдерді түзетуді, сақтауды, болдырмауды және бөлуді ескере отырып, өңдеу тәртібінің сипаттамасы;

10) тәуекелдерді қайта қарау мен қайта бағалауға қойылатын талаптардың сипаттамасы;

11) тәуекелді жүзеге асыру жағдайында салдарларды анықтау және бағалау;

12) тәуекелдерді жүргізу және өңдеу үшін жауапты тұлғаларды белгілеу;

13) тәуекелдер картасын құру тәртібінің сипаттамасы;

14) тәуекелдерді бағалау мен талдау нәтижелері бойынша өңдеу жоспарын қалыптастыру тәртібінің сипаттамасы.

17. Тәуекелдерді бағалау әдістемесін зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 16-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Тәуекелдерді бағалау әдістемесі АҚ талаптарына сәйкес;

2) осы Әдістеменің 16-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Тәуекелдерді бағалау әдістемесі АҚ талаптарына сәйкес емес.

4-параграф. Жұмыстың үздіксіздігін қамтамасыз ету қағидаларын зерттеу, талдау және бағалау

18. Жұмыстың үздіксіздігін қамтамасыз ету қағидаларын зерттеу, талдау және бағалау Жұмыстың үздіксіздігін қамтамасыз ету қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) аттестаттау объектісінің жұмыс істеу процестерін бұзудың себебі болып табылатын оқиғаларды сәйкестендіру бойынша (жоспарлау тәуекелдерді бағалаумен сүйемелденуі тиіс);

2) активтер істен шыққан жағдайда активтер тізбесінде белгіленген жұмысының үздіксіздігін қамтамасыз ету процестерін анықтау;

3) Ақпаратты өңдеу құралдарымен байланысты активтер жұмысының үздіксіздігін қамтамасыз ету жоспарын әзірлеуді көздейтін;

4) тестілеу және активтер жұмысының үздіксіздігі бойынша қолданыстағы процестерді дамыту жоспарларын жаңарту тәртібі туралы;

5) аттестаттау объектісінің жұмыс істеу процестері үшін жауапты тұлғаларды тағайынду байынша;

6) Активтер жұмысының үздіксіздігін қамтамасыз ету жоспарын талдауды жүргізу бойынша;

7) аттестаттау объектісін қалпына келтіру жоспарын әзірлеу бойынша;

8) қатерлердің, қауіптердің және рұқсатсыз қол жеткізу мүмкіндіктерінің пайда болу тәуекелдерін төмендететін жабдықты орналастыру тәсілдері;

9) электрмен жабдықтау жүйесіндегі жұмыс істемей қалулардан және коммуникация қызметтерінің жұмысынан орын алатын бұзушылықтардан жабдықты қорғау тәсілдері;

10) жұмыс істеуінің үздіксіздігін, қолжетімділігі мен тұтастығын қамтамасыз ету үшін жабдыққа техникалық қызмет көрсетудің мерзімділігіне қойылатын талаптар.

19. Жұмыстың үздіксіздігін қамтамасыз ету қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 18-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Жұмыстың үздіксіздігін қамтамасыз ету қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 18-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Жұмыстың үздіксіздігін қамтамасыз ету қағидалары АҚ талаптарына сәйкес емес.

5-параграф. Түгендеу қағидаларын зерттеу, талдау және бағалау

20. Түгендеу қағидаларын зерттеу, талдау және бағалау Түгендеу қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) құндылығы мен маңыздылығын ескере отырып, есептеу техникасы құралдарын (бұдан әрі - ЕТҚ) сәйкестендіруге қойылатын талаптар;

2) ЕТҚ паспорттарын ресімдеу тәртібі;

3) ЕТҚ түгендеу мен паспорттандыруды жүргізу мерзімділігіне қойылатын талаптар;

4) ЕТҚ, телекоммуникациялық жабдықты және бағдарламалық қамтамасыз етуді кәдеге жаратуға және (немесе) шығысқа шығаруға, соның ішінде деректерді сақтау құрылғыларын кәдеге жарату мен жабдықты қайтадан пайдаланған кезде ақпаратты кепілдікті жоюға қойылатын талаптар;

5) ЕТҚ түгендеу мен паспорттандыру үшін жауапты тұлғаларды тағайындау бойынша талаптар;

6) лицензияланған БҚ пайдалануға, сатып алуға және есепке алуға қойылатын талаптар.

21. Түгендеу қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 20-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Түгендеу қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 20-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Түгендеу қағидалары АҚ талаптарына сәйкес емес.

6-параграф. Ішкі аудит қағидаларын зерттеу, талдау және бағалау

22. Ішкі аудит қағидаларын зерттеу, талдау және бағалау Ішкі аудит қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын

айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) ішкі ақпараттық қауіпсіздік аудитінің негізгі мақсаттары;

2) аудиторларға қолжетімділік беру бойынша талаптар;

3) аспаптық аудитке қойылатын талаптар;

4) ішкі аудитті жүргізудің мерзімділігі бойынша талаптар;

5) ішкі аудитті кезеңмен жүргізуді кесте-жоспарының болуы мен жүргізулуіне қойылатын талаптар;

6) ішкі аудит жүргізу жөніндегі жұмыс тобын қалыптастыру тәртібі бойынша талаптар;

7) аттестаттау объектілері үшін аудит жүргізуді жоспарлау, тәртібі мен құрамы бойынша талаптар;

8) ішкі ақпараттық қауіпсіздік аудитінің нәтижелерін ресімдеу тәртібі мен нысаны.

23. Ішкі аудит қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 22-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Ішкі аудит қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 22-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Ішкі аудит қағидалары АҚ талаптарына сәйкес емес.

7-параграф. Криптографиялық құралдарды пайдалану қағидаларын зерттеу, талдау және бағалау

1. Криптографиялық құралдарды пайдалану қағидаларын зерттеу, талдау және бағалау Криптографиялық құралдарды пайдалану қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) ҚР СТ ИСО / МЭК 27002-2009 15.1.6–бөліміне сәйкес ақпаратты криптографиялық қорғау құралдарын пайдалану саясаты;

2) кілттерді басқару жүйесіне қойылатын талаптар;

3) кілттерді активациялау және дезактивациялау мерзімдеріне қойылатын талаптар;

4) ашық кілттер сертификаты жөніндегі талаптар;

5) құпия ақпаратты сақтау, өңдеу және телекоммуникациялар желілері бойынша жіберген кезде қауіпсіздік бойынша тапсырмға сәйкес криптографиялық шифрлауға қойылатыын талаптар.

25. Криптографиялық құралдарды пайдалану қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 24-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Криптографиялық құралдарды пайдалану қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 24-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Криптографиялық құралдарды пайдалану қағидалары АҚ талаптарына сәйкес емес.

8-параграф. Қол жеткізу құқықтарын бөлу қағидаларын зерттеу, талдау және бағалау

26. Қол жеткізу құқықтарын бөлу қағидаларын зерттеу, талдау және бағалау Қол жеткізу құқықтарын бөлу қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) жаңа пайдаланушыны тіркеу сәтінен бастап пайдаланушыны тіркеуден алып тастағанға дейін пайдаланушыларды тіркеу кезеінің сипаттамасы;

2) берілетін ресурстарға қол жеткізу құқықтар тізбесінің сипаттамасы;

3) қол жеткізу құқығын беру тәртібінің сипаттамасы;

4) барлық тіркелген пайдаланушылардың есебін жүргізу бойынша талаптар;

5) пайдаланушылардың қол жеткізу құқықтарын қайта қарауды жүргізу бойынша талаптар;

6) пайдаланушыларды алынған сәйкестендіргіштерді жариялауға немесе басқа біреуге беруге тыйым салумен таныстыру бойынша талаптар;

7) есеп жазбасын бұғаттау бойынша талаптардың сипаттамасы.

27. Қол жеткізу құқықтарын бөлу қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 26-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Қол жеткізу құқықтарын бөлу қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 26-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Қол жеткізу құқықтарын бөлу қағидалары АҚ талаптарына сәйкес емес.

9-параграф. Интернетті және электрондық поштаны пайдалану қағидаларын зерттеу, талдау және бағалау

28. Интернетті және электрондық поштаны пайдалану қағидаларын зерттеу, талдау және бағалау Интернетті және электрондық поштаны пайдалану қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) электрондық поштаны пайдалану тәртібі;

2) электрондық хабарламаны ресімдеуге қойылатын талаптар;

3) Интернетке қол жеткізуге рұқсат беру тәртібі мен әдістері;

4) Интернетке қолжетімділік мониторингі және бақылау;

5) мемлекеттік органның ведомстволық электрондық поштасының сыртқы электрондық пошта жүйелерімен тек қана электрондық поштаның бірыңғай шлюзі арқылы электрондық өзара іс-қимылды жүзеге асыру туралы талаптар.

29. Интернетті және электрондық поштаны пайдалану қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 28-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Интернетті және электрондық поштаны пайдалану қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 28-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Интернетті және электрондық поштаны пайдалану қағидалары АҚ талаптарына сәйкес емес.

10-параграф. Аутентификация процедурасын ұйымдастыру қағидаларын зерттеу, талдау және бағалау

30. Аутентификация процедурасын ұйымдастыру қағидаларын зерттеу, талдау және бағалау Аутентификация процедураларын ұйымдастыру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) пайдаланушыларды оларға сенім тапсырылған сәйкестендіргіштердің құпиялығын сақтау қажеттігі туралы хабарландыру бойынша талаптар;

2) пайдаланушыларды парольдерді, пин-кодтарды олардың қауіпсіз сақталуы қамтамасыз етілмесе, қағазға, дербес компьютерге немесе тасымалдау құрылғыларына жазуға рұқсат етілмейтіні туралы хабарландыру бойынша талаптар;

3) уақытша парольдерді берудің қауіпсіз тәсілі тәртібінің сипаттамасы;

4) уақытша парольдерге қойылатын талаптардың сипаттамалары;

5) сәйкестендіргішті жария ету мүмкіндігінің кез келген белгілері болған кезде сәйкестендіру деректерін өзгерту қажеттілігі туралы талаптар;

6) сапалы парольдерді таңдау бойынша талаптар;

7) уақыттың тең аралықтарында парольдік аутентификацияны өзгерту бойынша талаптардың сипаттамасы;

8) жүйеде алғашқы рет тіркеген кезде уақытша парольдерді ауыстыру бойынша талаптардың сипаттамасы;

9) парольдерді автоматты тіркеу процесіне енгізуге, мәселең сақталатын макрокомандаларды немесе функционалдық клавишаларды пайдаланумен, тыйым салу бойынша талаптардың сипаттамасы.

31. Аутентификация процедурасын ұйымдастыру қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 30-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Аутентификация процедураларын ұйымдастыру қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 30-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Аутентификация процедураларын ұйымдастыру қағидалары АҚ талаптарына сәйкес емес.

11-параграф. Вирусқа қарсы бақылауды ұйымдастыру қағидаларын зерттеу, талдау және бағалау

32. Вирусқа қарсы бақылауды ұйымдастыру қағидаларын зерттеу, талдау және бағалау Вирусқа қарсы бақылауды ұйымдастыру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) лицензияланған вирусқа қарсы бағдарламалық қамтамасыз етулерді пайдалану бойынша талаптар;

2) вирусқа қарсы бағдарламалық қамтамасыз етулерді жаңарту мерзімділігі бойынша талаптар;

3) вирусқа қарсы бағдарламалық қамтамасыз етулерді пайдаланған кезде ақпараттық қауіпсіздікті сақтау жөніндегі пайдаланушыларға арналған талаптар;

4) веб-парақтарды зиянды бағдарламалық қамтамасыз етудің болуына қатысты тексеру талаптары;

5) күдікті немесе авторланбаған ақпаратты тасығыштардағы барлық файлдарды немесе жалпыға қолжетімді желілерден алынған файлдарды вирустардың болуына қатысты тексеру бойынша талаптар;

6) электрондық поштаны және көшірілетін ақпаратты зиянды бағдарламалық қамтамасыз етудің болуына қатысты талдау бойынша талаптар;

7) зиянды бағдарламалық қамтамасыз етумен күресу үшін ақпараттық қауіпсіздікті басқару бойынша іс-шараларды ұйымдастыру бойынша талаптар;

8) вирустық шабуыладардан кейін ақпаратты қалпына келтіру процедураларының сипаттамалары.

33. Вирусқа қарсы бақылауды ұйымдастыру қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 32-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Вирусқа қарсы бақылауды ұйымдастыру қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 32-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Вирусқа қарсы бақылауды ұйымдастыру қағидалары АҚ талаптарына сәйкес емес.

12-параграф. Мобильдік құрылғыларды пайдалану қағидаларын зерттеу, талдау және бағалау

34. Мобильдік құрылғыларды пайдалану қағидаларын зерттеу, талдау және бағалау Мобильдік құрылғыларды және ақпаратты тасығыштарды пайдалану қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) мобильдік құрылғыларды ұйымнан тыс жерде пайдаланған жағдайда, тәуекелдерді талдау бойынша талаптар;

2) мобильдік құрылғыларды және ақпаратты тасығыштарды физикалық қорғау бойынша талаптар;

3) мобильдік құрылғылардың және ақпаратты тасығыштардың тізбесін құру және оларды маркалау бойынша талаптар;

4) ақпаратты тасығыштарды беру журналын жүргізуге қойылатын талаптар;

5) ақпаратты тасығыштарды пайдалану тәртібі;

6) дербес деректердің алмалы тасығыштарын есепке алу, сақтау мен қолдану және оларды пайдаға асыру тәртібі;

7) алмалы тасығыштарды пайдалану кезінде қызметкерлерге қойылатын талаптар;

8) жұмыс орнына тыс орналасқан мобильдік құрылғыны ұйымдастыру үй-жайлары аумағынан тыс жұмыс істеудің түрлі тәуекелдерін ескере отырып, қорғау тәсілдері;

9) дербес деректердің алмалы тасығыштарын пайдалану, сондай-ақ жоғалту және жою кезінде қызметкерлердің рұқсат етілмеген іс-қимыл жасау фактілері айқындалған кезіндегі іс-әрекет тәртібі.

35. Мобильдік құрылғыларды пайдалану қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 34-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Мобильдік құрылғыларды және ақпаратты тасығыштарды пайдалану қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 34-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Мобильдік құрылғыларды және ақпаратты тасығыштарды пайдалану қағидалары АҚ талаптарына сәйкес емес.

13-параграф. Физикалық қорғауды ұйымдастыру қағидаларын зерттеу, талдау және бағалау

36. Физикалық қорғауды ұйымдастыру қағидаларын зерттеу, талдау және бағалау Физикалық қорғауды ұйымдастыру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.1.1, 9.1.3, 9.1.4 бөліміне сәйкес серверлік үй-жайды физикалық қорғауға қойылатын талаптар;

2) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.1.2 бөліміне сәйкес серверлік үй-жайларға кіруді бақылауды ұйымдастыруға қойылатын талаптар;

3) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.1.5 бөліміне сәйкес серверлік үй-жайларда жұмыстарды орындау бойынша талаптар;

4) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.2.1 бөліміне сәйкес серверлік жабдықты қауіпсіз орналастыру бойынша талаптар;

5) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.2.2 бөліміне сәйкес қосымша қызметтерді ұйымдастыру бойынша талаптар;

6) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.2.3 бөліміне сәйкес кәбілдік желіні қауіпсіз пайдалану бойынша талаптар;

7) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.2.4 бөліміне сәйкес серверлік жабдыққа қауіпсіз техникалық қызмет көрсету бойынша талаптар;

8) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.2.6 бөліміне сәйкес жабдықты қауіпсіз пайдаға асыру немесе қайтадан пайдалануға қойылатын талаптар;

9) БТ және ҚР СТ ИСО / МЭК 27002-2009 9.2.7 бөліміне сәйкес жабдықты кіргізу/шығаруға қойылатын талаптар.

37. Физикалық қорғауды ұйымдастыру қағидаларын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 36-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Физикалық қорғауды ұйымдастыру қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 36-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Физикалық қорғауды ұйымдастыру қағидалары АҚ талаптарына сәйкес емес.

14-параграф. Әкімші басшылығын зерттеу, талдау және бағалау

38. Әкімші басшылығын зерттеу, талдау және бағалау Әкімші басшылығы негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) әкімшінің негізгі үлгілік жұмыстар бойынша іс-әрекеттеріне қойылатын талаптар;

2) инциденттер, штаттан тыс жағдайлар, апатты табиғаттық-климаттық және техногендік әсерлер орын алған кездегі әкімшінің іс-әрекеттеріне қойылатын талаптар;

3) серверлер мен жұмыс станцияларына БҚ орнату, жаңарту және жою тәртібі ;

4) жүйелік БҚ өзгерген жағдайда БҚ өзгерулерін басқару және талдау процедуралары.

39. Әкімші басшылығын зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 38-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Әкімшінің басшылығы АҚ талаптарына сәйкес;

2) осы Әдістеменің 38-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Әкімшінің басшылығы АҚ талаптарына сәйкес емес.

15-параграф. Резервтік көшіру регламентін зерттеу, талдау және бағалау

40. Резервтік көшіру регламентін зерттеу, талдау және бағалау Резервтік көшіру регламенті негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) резервтік көшіруге жататын ақпараттың құрамы бойынша талаптардың сипаттамасы;

2) резервтік көшірудің көлемін анықтау;

3) резервтік жабдық пен резервтік көшірмелерді орналастыру және резервтік көшірмелерді сақтау орнын таңдау бойынша талаптардың сипаттамасы;

4) резервтік көшірмелерді және резервтік жабдықты тестілеу бойынша талаптардың сипаттамасы;

5) резервтік серверлік жабдықты орналастыру және оны физикалық қорғау бойынша талаптардың сипаттамасы;

6) ақпаратты көшіру мен ақпаратты қалпына келтіру процедураларының сипаттамасы;

7) ақпаратты резервілеу және резервтік көшіру кестесін құру мерзімділігі туралы талаптар;

8) эталондық көшірмелер тізілімін, резервтік көшіруге жататын ақпараттық ресурстар тізілімін, резервтік көшіруді жазу журналын, резервтік көшірмелерді қалпына келтіруге қатысты тексеру журналын, резервтік ақпаратты электрондық тасығыштарды есепке алу журналын, резервтік ақпаратты электрондық тасығыштарды алып кіру/алып шығу журналын жүргізу бойынша талаптар.

41. Резервтік көшіру регламентін зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 40-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Резервтік көшіру регламенті АҚ талаптарына сәйкес;

2) осы Әдістеменің 40-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Резервтік көшіру регламенті АҚ талаптарына сәйкес емес.

16-параграф. Штаттан тыс жағдайлар жөніндегі нұсқаулықты зерттеу, талдау және бағалау

42. Штаттан тыс жағдайлар жөніндегі нұсқаулықты зерттеу, талдау және бағалау Штаттан тыс жағдайлар жөніндегі нұсқаулықтың негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және келесі мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) ықтимал штаттан тыс және дағдарысты жағдайлардың тізбесін құру, АҚ бойынша инциденттерді сәйкестендіру бойынша талаптар;

2) ақпараттық қауіпсіздік инциденттері жағдайында хабарлау үшін жауапты тұлғаларды тағайындау туралы талап;

3) штаттан тыс жағдай орын алған кезде хабарлау тәртібі;

4) АҚ инциденттері, штаттан тыс (дағдарысты) жағдайлар орын алған кезде әрекет ету шараларын қабылдау жөніндегі талаптар;

5) жұмыстар тоқатылған жағдайда оларды қалпына келтіру процедураларын әзірлеу бойынша талаптар;

6) штаттан тыс немесе дағдарысты жағдайлардың орын алуына жол бермеуге арналған сақтандыру іс-қимылдарының орындалуын бақылауды жүзеге асыру бойынша талаптар;

7) инциденттердің және басқа штаттан тыс жағдайлардың орын алу оқиғаларын тексеру бойынша талаптар.

43. Штаттан тыс жағдайлар жөніндегі нұсқаулықты зерттеу, талдау және бағалау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 42-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Штаттан тыс жағдайлар жөніндегі нұсқаулық АҚ талаптарына сәйкес;

2) осы Әдістеменің 42-тармағында көрсетілген мәліметтердің біреуі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда - Штаттан тыс жағдайлар жөніндегі нұсқаулық АҚ талаптарына сәйкес емес.

4. Аттестаттау объектісін аспаптық тексеруді қоса алғанда, БТ, ҚР СТ ИСО / МЭК 27001-2008 және ҚР СТ ИСО / МЭК 27002-2009, ҚР СТ ГОСТ Р 50739-95-2006, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстар ұйымдастырудың жай-күйін тексеру

44. Аттестаттау объектісін аспаптық тексеруді қоса алғанда, БТ, ҚР СТ ИСО / МЭК 27001-2008 және ҚР СТ ИСО / МЭК 27002-2009, ҚР СТ ГОСТ Р 50739-95-2006, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстар ұйымдастырудың жай-күйін тексеру мыналарды тексеру және талдау мақсатында жүргізіледі:

1) Саясат ережелерін;

2) ақпараттық қауіпсіздікті басқару бойынша процестерді;

3) активтерді басқаруды ұйымдастыруды;

4) персоналға байланысты қауіпсіздікті қамтамасыз етуді;

5) жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғауды;

6) ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз етуді;

7) ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды;

8) аттестаттау объектілерін әзірлеу, енгізу мен қызмет көрсету процестерін;

9) ақпараттық қауіпсіздік саласындағы инциденттерді басқаруды ұйымдастыруды;

10) бизнестің үздіксіздігін басқаруды;

11) құқықтық талаптарға сәйкестік дәрежесін;

12) ҚР СТ ГОСТ Р 50739-95-2006 талаптарына сәйкес ақпаратты рұқсатсыз қол жеткізуден қорғау жүйесіне қойылатын талаптарды.

45. Аттестаттау объектісін аспаптық тексеруді қоса алғанда, БТ, ҚР СТ ИСО / МЭК 27001-2008 және ҚР СТ ИСО / МЭК 27002-2009, ҚР СТ ГОСТ Р 50739-95-2006, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстар ұйымдастырудың жай-күйін тексеру нәтижелері Аттестаттық тексеру актісінде белгіленеді.

1-параграф. Саясат ережелерін тексеру және талдау

46. Саясат ережелерін тексеру және талдау кезінде:

1) Саясатты басшылықтың мақұлдауын, жариялануын және барлық қызметкерлер мен байланысты сыртқы ұйымдардың назарына жеткізілуін;

2) ұйым қызметкерлерінің Саясатты түсінуі мен қабылдауын;

3) Саясатты мерзімді түрде қайта қарауды;

4) құжаттарда қойылған талаптарының барабарлығын және орындалатындығын;

5) жоспарланған уақыт аралығында немесе елеулі өзгерістер орын алған жағдайда Саясатты талдаудың нәтижелерін;

6) Саясатты әзірлеуге, талдауға және бағалауға басшылық ету үшін жауапты тұлғаның болуын тексеру қажет.

47. Саясат ережелерін тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 46-тармағы орындалған жағдайда – Саясат ережелерінің орындалуы АҚ талаптарына сәйкес;

2) осы Әдістеменің 46-тармағы орындалмаған жағдайда - Саясат ережелерінің орындалуы АҚ талаптарына сәйкес емес.

2-параграф. Ақпараттық қауіпсіздікті басқару бойынша процестерді тексеру және талдау

48. Ақпараттық қауіпсіздікті басқару бойынша процестерді тексеру және талдау кезінде келесі процестерді тексеруді жүзеге асыру қажет:

1) аттестаттау объектісінің ақпараттық қауіпсіздігін қамтамасыз ету үшін жаупты бөлімшенің және (немесе) ақпараттық қауіпсіздігін қамтамасыз ету үшін жаупты тұлғаның жұмыс істеу;

2) ұйымның жоғары басшылығының қатысуымен ақпараттық қауіпсіздік саясаттарын, тәуекелдері мен басқа мәселелерін талқылауға арналған ақпараттық қауіпсіздік мәселелері жөніндегі органның (ақпараттық қауіпсіздік жөніндегі техникалық кеңес, жұмыс тобы) жұмыс істеуі;

3) ұйымда басшылықтың қауіпсіздік режимін қолдау бойынша іс-қимылдарды үйлестіру жөніндегі тұрақты кеңестерін өткізу;

4) ақпараттық қауіпсіздік саласындағы рольдерді және жауапкершілікті ұйым қызметкерлері арасында бөлу;

5) мемлекеттік органның немесе ұйымның бөлімшелері ішінде және бөлімшелері арасында АҚ мәселелері жөніндегі қызметті үйлестіру;

6) ұйым тәуекелдері мен сыртқы ұйымдарға (бөгде ұйымдар тартылған жағдайда) қатысты бизнес-процестер тарапынан ақпаратты өңдеу құралдарын сәйкестендіруді енгізу;

7) бөгде ұйымдарға ұйымдарға (бөгде ұйымдар тартылған жағдайда) ұйымның ақпаратына немесе активтеріне қолжетімділік құқығын беру алдында қауіпсіздікке қойылатын талаптарды сақтау;

8) бөгде ұйыммен (бөгде ұйымдар тартылған жағдайда) жасалған ақпаратқа қолжетімділікті, өңдеуді, жіберуді немесе оны өңдеу құралдарын басқаруды қамтитын келісімде қауіпсіздік талаптарын сақтау.

49. Ақпараттық қауіпсіздікті басқару бойынша процестерді тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 48-тармағының барлық тармақшалары орындалған жағдайда – ақпараттық қауіпсіздікті басқару АҚ талаптарына сәйкес;

2) осы Әдістеменің 48-тармағының барлық тармақшалары орындалмаған жағдайда - ақпараттық қауіпсіздікті басқару АҚ талаптарына сәйкес емес.

3-параграф. Активтерді басқаруды ұйымдастыруды тексеру және талдау

50. Активтерді басқаруды ұйымдастыруды тексеру және талдау кезінде келесі процестерді тексеруді жүзеге асыру қажет:

1) аттестаттау объектісімен байланысты барлық активтердің түгендеу тізімдемесін сәйкестендіруді, ресімдеу мен жұмыс жай-күйінде қолдауды талдау;

2) ұйымның немесе мемлекеттік органның ақпаратты және ақпаратты өңдеу құралдарымен байланысты активтерді иелену деңгейін анықтау;

3) активтерді лауазымды тұлғаларға бекіту және активтердің АҚ басқару жөніндегі іс-шараларды іске асыру үшін олардың жауапкершілік көлемін анықтау;

4) ақпаратты оның құндылығына, заңнамалық талаптар, әсерленгіштігі мен ұйым үшін маңыздылығы тұрғысынан сыныптауды талдау;

5) ұйымда қабылданған сыныптау және оларды орындау схемасына сәйкес ақпаратты маркалау мен жұмыс істеу.

51. Активтерді басқаруды ұйымдастыру процестерін тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 50-тармағының барлық тармақшалары орындалған жағдайда – активтерді басқаруды ұйымдастыру процесі АҚ талаптарына сәйкес;

2) осы Әдістеменің 50-тармағының барлық тармақшалары орындалмаған жағдайда - активтерді басқаруды ұйымдастыру процесі АҚ талаптарына сәйкес емес.

4-параграф. Персоналға байланысты қауіпсіздікті қамтамасыз етуді тексеру және талдау

52. Персоналға байланысты қауіпсіздікті қамтамасыз етуді тексеру және талдау кезінде:

1) персоналдың қауіпсіздікті қамтамасыз ету бойынша функцияларын және ҚР СТ ИСО/МЭК 27002-2009 8.1.1 бөліміне сәйкес АҚ бойынша бекітілген функциялардың орындалуын;

2) жұмысқа қабылдаған кезде ҚР СТ ИСО/МЭК 27002-2009 8.1.2 бөліміне сәйкес қызметкерлер үшін белгіленетін ақпараттық қауіпсіздік бойынша талаптардың толықтығын;

3) ҚР СТ ИСО/МЭК 27002-2009 8.1.3 бөлімі мен ЕТ 24-тармағына сәйкес еңбек шартының ақпараттық қауіпсіздікке қатысты шарттарын;

4) ҚР СТ ИСО/МЭК 27002-2009 8.2.1 бөліміне сәйкес қызметкерлердің, мердігерлер мен үшінші тарап пайдаланушыларының ұйымның саясаттарымен және процедураларымен белгіленген қауіпсіздікті сақтау туралы басшылық талаптарының сақталуын;

5) ҚР СТ ИСО/МЭК 27002-2009 8.2.2 бөліміне сәйкес қызметкерлердің ақпараттық қауіпсіздік саласы бойынша хабардарлығын, оқыту мен қайта даярлауды;

6) ҚР СТ ИСО/МЭК 27002-2009 8.2.3 бөліміне сәйкес қауіпсіздік талаптарын бұзған қызметкерлер үшін нысандандырылған тәртіптік процестің болуы мен оның нақты пайдаланылуын;

7) ҚР СТ ИСО/МЭК 27002-2009 8.3 бөліміне және БТ сәйкес жұмыспен қамту мерзімі аяқталған немесе жағдайлары өзгерген кезде қызметкерлердің ақпараттық қауіпсіздік бөлігіндегі (активтерді қайтару, қолжетімділік құқығын жою) жауапкершілігінің болуын тексеру қажет.

53. Персоналға байланысты қауіпсіздікті қамтамасыз етуді тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 52-тармағының барлық тармақшалары орындалған жағдайда – Персоналға байланысты қауіпсіздікті қамтамасыз ету АҚ талаптарына сәйкес;

2) осы Әдістеменің 52-тармағының барлық тармақшалары орындалмаған жағдайда - Персоналға байланысты қауіпсіздікті қамтамасыз ету АҚ талаптарына сәйкес емес.

5-параграф. Жабдықты және қоршаған орта қауіпсіздігін физикалық қорғауды тексеру және талдау

54. Жабдықты және қоршаған орта қауіпсіздігін физикалық қорғауды тексеру мен талдау кезінде келесі процестерді тексеру қажет:

1) ҚР СТ ИСО/МЭК 27002-2009 9.1.1 бөліміне сәйкес периметр мен серверлік үй-жайды физикалық қорғауды қамтамасыз ету;

2) ҚР СТ ИСО/МЭК 27002-2009 9.1.2 бөліміне және БТ сәйкес серверлік үй-жайларға кіруді бақылауды ұйымдастыру;

3) ҚР СТ ИСО/МЭК 27002-2009 9.1.4 бөліміне сәйкес сыртқы қатерлерден қорғауды ұйымдастыру;

4) ҚР СТ ИСО/МЭК 27002-2009 9.1.5 бөліміне сәйкес серверлік үй-жайларда жұмысты ұйымдастыру;

5) ҚР СТ ИСО/МЭК 27002-2009 9.1.6 және 9.2.7 бөлімдеріне сәйкес қоғамдық қолжетімділік аймақтарында (мұндайлар болған жағдайда) материалдық

құндылықтарды қабылдау және жіберу кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

6) қорғау мен ақпараттық қауіпсіздікті қамтамасыз етуге арналған жабдықты ҚР СТ ИСО/МЭК 27002-2009 9.2.1 және 9.2.5 бөлімдері мен БТ сәйкес орналастыру;

7) ҚР СТ ИСО/МЭК 27002-2009 9.2.2 бөліміне сәйкес электр энергиясын берудегі кідірулер мен қосымша қызметтерді қамтамасыз етуде орын алатын кірірулерге байланысты тоқтап қалулардан қорғауды қамтамасыз ету;

8) ҚР СТ ИСО/МЭК 27002-2009 9.2.3 бөліміне және БТ сәйкес кәбілдік желінің ақпараттық қауіпсіздігін қамтамасыз ету;

9) ҚР СТ ИСО/МЭК 27002-2009 9.2.4 бөліміне сәйкес серверлік жабдыққа техникалық қызмет көрсету кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

10) ҚР СТ ИСО/МЭК 27002-2009 9.2.5 бөліміне сәйкес серверлік үй-жайдан тыс жерде пайдаланылатын серверлік жабдықтың ақпараттық қауіпсіздігін қамтамасыз ету;

11) ҚР СТ ИСО/МЭК 27002-2009 9.2.6 бөліміне сәйкес жабдықты қауіпсіз қайтадан пайдаға асыруды (шығысқа шығаруды) ұйымдастыру.

55. Жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғауды тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 54-тармағының барлық тармақшалары орындалған жағдайда – жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғау АҚ талаптарына сәйкес;

2) осы Әдістеменің 54-тармағының барлық тармақшалары орындалмаған жағдайда - жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғау АҚ талаптарына сәйкес емес.

6-параграф. Ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз етуді тексеру және талдау

56. Ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз етуді тексеру және талдау кезінде келесі процестерді тексеруді жүзеге асыру қажет:

1) ҚР СТ ИСО/МЭК 27002-2009 10.1 бөліміне сәйкес операциялық процедураларды құжатпен ресімдеу, аттестаттау объектісіндгі өзгерістерді бақылауды жүргізу, аттестаттау объектісінде міндетемелерді бөлу және әзірлеу, тестілеу мен пайдалану құралдарын бөлу;

2) ҚР СТ ИСО/МЭК 27002-2009 10.2 бөліміне сәйкес бөгде ұйымдардан қызметтер алған және (немесе) бгде ұйымдарға қызмет көрсеткен кезде ақпараттық қауіпсіздік талаптарын сақтау;

3) ҚР СТ ИСО/МЭК 27002-2009 10.3 бөліміне сәйкес аттестаттау объектілерінің өнімділігін басқару кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

4) ҚР СТ ИСО/МЭК 27002-2009 10.4 бөліміне сәйкес зиянды кодтан қауіпсіз қорғауды қауіпсіздікті қамтамасыз ету;

5) ҚР СТ ИСО/МЭК 27002-2009 10.5 бөліміне сәйкес аттестаттау объектілерінде ақпаратты резервілеу процедуруларын жүргізген кезде ақпараттық қауіпсіздік талаптарын сақтау;

6) ҚР СТ ИСО/МЭК 27002-2009 10.6 бөліміне сәйкес желіні басқару кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

7) БТ белгіленген локалдық және ведомстволық (корпоративтік) желіге қойылатын талаптарды орындау;

8) ҚР СТ ИСО/МЭК 27002-2009 10.7 бөліміне және БТ сәйкес ақпаратты тасығыштармен (таспалар, дискілер, флеш-жинақтағыштар) жұмыс кезінде ақпараттық қауіпсіздікті сақтау;

9) ҚР СТ ИСО/МЭК 27002-2009 10.8 бөліміне сәйкес ақпаратпен алмасу кезінде ақпараттық қауіпсіздікті сақтау;

10) ҚР СТ ИСО/МЭК 27002-2009 10.10 бөліміне және БТ сәйкес аттестаттау объектісінде ақпараттық қауіпсіздік мониторингін қамтамасыз ету;

11) БТ талаптарына сәйкес виртуалдау мен "бұлтты" есептеу технологияларын іске асыратын есептеу ресурстарының тиісінше және қауіпсіз жұмысын қамтамасыз ету.

57. Ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз етуді тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 56-тармағының барлық тармақшалары орындалған жағдайда – ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз ету АҚ талаптарына сәйкес;

2) осы Әдістеменің 56-тармағының барлық тармақшалары орындалмаған жағдайда - ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз ету АҚ талаптарына сәйкес емес.

7-параграф. Ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды тексеру және талдау

58. Ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды тексеру және талдау кезінде келесі процестерді тексеру қажет:

1) ҚР СТ ИСО/МЭК 27002-2009 11.1 бөліміне сәйкес ақпаратқа және аттестаттау объектісіне қолжетімділікті бақылау бойынша ақпараттық қауіпсіздікті қамтамасыз ету;

2) ҚР СТ ИСО/МЭК 27002-2009 11.2 бөліміне және БТ сәйкес пайдаланушылардың аттестаттау объектісінде қолжетімділігін басқару кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

3) ҚР СТ ИСО/МЭК 27002-2009 11.3 бөліміне және БТ сәйкес пайдаланушыларды қолжетімділікті басқару бойынша олардың функционалдық міндеттері туралы хабарландыру мен олардың орындалуы;

4) ҚР СТ ИСО/МЭК 27002-2009 11.4 бөліміне сәйкес желілік сервістерге қол жеткізуге рұқсат беру кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

5) ҚР СТ ИСО/МЭК 27002-2009 11.5 бөліміне және БТ сәйкес операциялық жүйеге қол жеткізуге рұқсат беру кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

6) ҚР СТ ИСО/МЭК 27002-2009 11.6 бөліміне және БТ сәйкес қолданбалы бағдарламалар мен ақпаратқа қолжетімділікті бақылауды қамтамасыз ету;

7) ҚР СТ ИСО/МЭК 27002-2009 11.7 бөліміне сәйкес тасымалдау құрылғыларымен жұмыс кезінде ақпараттық қауіпсіздік талаптарын сақтау және қашықтық режимінде жұмыс істеу;

8) БТ белгіленген талаптарды (ақпараттық жүйелерге арналған) орындай отырып, АЖ тәжірибелік және өнеркәсіптік пайдалану орталарын әзірлеу, тестілеу немесе стендтық сынақтан өткізу орталарынан бөлу;

9) БТ сәйкес интернет-ресурстың ақпараттық қауіпсіздігін қамтамасыз ету.

59. Ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 58-тармағының барлық тармақшалары орындалған жағдайда – ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыру АҚ талаптарына сәйкес;

2) осы Әдістеменің 58-тармағының барлық тармақшалары орындалмаған жағдайда - ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыру АҚ талаптарына сәйкес емес.

8-параграф. Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестерін тексеру және талдау

60. Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестерін тексеру және талдау кезінде:

1) ҚР СТ ИСО/МЭК 27002-2009 12.1 бөліміне сәйкес өміршеңдік кезеңнің әр сатысында ақпараттық қауіпсіздікті қамтамасыз етуді;

2) ҚР СТ ИСО/МЭК 27002-2009 12.2 бөліміне сәйкес аттестаттау объектісіндегі деректерді өңдеген кезде ақпараттық қауіпсіздікті қамтамасыз етуді;

3) ҚР СТ ИСО/МЭК 27002-2009 12.3 бөліміне сәйкес ақпаратты криптографиялық қорғау құралдарын пайдаланудың дұрыстығын;

4) ҚР СТ ИСО/МЭК 27002-2009 12.4 бөліміне сәйкес аттестаттау объектісінің жүйелік файлдарының ақпараттық қауіпсіздігін қамтамасыз етуді;

5) ҚР СТ ИСО/МЭК 27002-2009 12.5 бөліміне сәйкес аттестаттау объектісін әзірлеу және енгізу прцесінде ақпараттық қауіпсіздікті қамтамасыз етуді;

6) ҚР СТ ИСО/МЭК 27002-2009 12.6 бөліміне сәйкес аттестаттау объектісінің осалдықтарын жою, мониторингі бойынша жұмыстар жүргізуді;

7) БТ белгіленген талаптарды (ақпараттық жүйелерге арналған) орындай отырып, АЖ тәжірибелік және өнеркәсіптік пайдалану орталарын әзірлеу, тестілеу немесе стендтық сынақтан өткізу орталарынан бөлуді;

8) БТ сәйкес интернет-ресурстың ақпараттық қауіпсіздігін қамтамасыз етуді тексеру қажет.

61. Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестерін тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 60-тармағының барлық тармақшалары орындалған жағдайда – аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестері АҚ талаптарына сәйкес;

2) осы Әдістеменің 60-тармағының барлық тармақшалары орындалмаған жағдайда - Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестері АҚ талаптарына сәйкес емес.

9-параграф. Ақпараттық қауіпсіздік саласындағы инциденттерді басқаруды ұйымдастыруды тексеру және талдау

62. Ақпараттық қауіпсіздік саласындағы инциденттерді басқаруды ұйымдастыруды тексеру және талдау кезінде келесі процестерді тексеру қажет:

1) ҚР СТ ИСО/МЭК 27002-2009 13.1 бөліміне сәйкес ақпараттық қауіпсіздік саласындағы инциденттерге жылдам, нәтижелі және жүйелі әрекет етуді қамтамасыз етуге мүмкіндік беретін ақпараттық қауіпсіздікті бұзу оқиғалары туралы хабарлау;

2) ҚР СТ ИСО/МЭК 27002-2009 13.2.1 бөліміне сәйкес басшылық жауаптылығын белгілеу;

3) ҚР СТ ИСО/МЭК 27002-2009 13.2.2 бөліміне сәйкес ақпараттық қауіпсіздік инциденттерін тіркеу және мониторингі, ақпараттық қауіпсіздік саласындағы инциденттер туралы хабарлаудың жеделдігі, ақпараттық қауіпсіздік инциденттері туралы есептер құру процедуралары;

4) ҚР СТ ИСО/МЭК 27002-2009 13.2.3 бөліміне сәйкес ақпараттық қауіпсіздік инциденті сот талқылауына әкеп соғу жағдайына ақпараттық қауіпсіздік инциденттері туралы ақпаратты жинау, сақтау мен ұсыну;

5) БТ сәйкес ақпараттық қауіпсіздік жай-күйіне байланысты оқиғаларды тіркеу мен оқиғалар журналын талдау жолымен бұзуларды айқындау.

63. Ақпараттық қауіпсіздік саласындағы инциденттерді басқаруды ұйымдастыруды тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 62-тармағының барлық тармақшалары орындалған жағдайда – ақпараттық қауіпсіздік инциденттерін басқару АҚ талаптарына сәйкес;

2) осы Әдістеменің 62-тармағының барлық тармақшалары орындалмаған жағдайда - ақпараттық қауіпсіздік инциденттерін басқару АҚ талаптарына сәйкес емес.

10-параграф. Бизнестің үздіксіздігін басқаруды тексеру және талдау

64. Бизнестің үздіксіздігін басқаруды тексеру және талдау кезінде келесі процестерді тексеру қажет:

1) ҚР СТ ИСО/МЭК 27002-2009 14.1.1 бөліміне сәйкес ақпараттық қауіпсіздік бойынша процестерді қамтитын бизнестің үздіксздігін дамыту мен қолдау;

2) ҚР СТ ИСО/МЭК 27002-2009 14.1.2 бөліміне сәйкес бизнес-процестерді үзудің себебі болып табылатын оқиғаларды сәйкестендіру;

3) ҚР СТ ИСО/МЭК 27002-2009 14.1.3 бөліміне сәйкес бизнестің үздіксздігі жоспарларын іске асыру;

4) ҚР СТ ИСО/МЭК 27002-2009 14.1.5 бөліміне сәйкес бизнестің үздіксздігін қамтамасыз ету жөніндегі жоспарларды тестілеуді, қолдау мен қайта қарауды жүргізу.

65. Бизнестің үздіксіздігін басқаруды тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 64-тармағының барлық тармақшалары орындалған жағдайда – бизнестің үздіксіздігін басқару бойынша процедуралар АҚ талаптарына сәйкес;

2) осы Әдістеменің 64-тармағының барлық тармақшалары орындалмаған жағдайда - бизнестің үздіксіздігін басқару бойынша процедуралар АҚ талаптарына сәйкес емес.

11-параграф. Құқықтық талаптарға сәйкестік деңгейін тексеру және талдау

66. Құқықтық талаптарға сәйкестік деңгейін тексеру және талдау кезінде келесі процестерді тексеру қажет:

1) ҚР СТ ИСО/МЭК 27002-2009 15.1.3 бөліміне сәйкес ұйым жазбаларын жоғалудан, бұзудан және бұрмалаудан заңнамалық, басқа міндетті, келісімдік талаптар мен бизенс-талаптарға сай қорғау;

2) ҚР СТ ИСО/МЭК 27002-2009 15.1.4 бөліміне сәйкес дербес құпия ақпаратты тасымалдаған кезде ақпараттық қауіпсіздікті қамтамасыз ету;

3) ҚР СТ ИСО/МЭК 27002-2009 15.1.5 бөліміне сәйкес ақпаратты қорғау құралдарын мақсатсыз пайдалануды бақылау;

4) ҚР СТ ИСО/МЭК 27002-2009 15.2.2 бөліміне сәйкес техникалық осалдықтарды қолмен және (немесе) тиісті аспаптық және бағдарламалық құралдардың көмегімен басқару бойынша іс-шаралар өткізу;

5) ҚР СТ ИСО/МЭК 27002-2009 15.3.1 бөліміне сәйкес ақпараттық қауіпсіздік аудитін жүргізген кезде басқару мен келісу бойынша шараларды қолдану;

6) ҚР СТ ИСО/МЭК 27002-2009 15.3.2 бөліміне сәйкес аспаптық аудаит құралдары қолжетімді болған кезде ақпараттық қауіпсіздікті қамтамасыз ету.

67. Құқықтық талаптарға сәйкестік деңгейін тексеру және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 66-тармағының барлық тармақшалары орындалған жағдайда – құқықтық талаптарға сәйкестік деңгейі АҚ талаптарына сәйкес;

2) осы Әдістеменің 66-тармағының барлық тармақшалары орындалмаған жағдайда - құқықтық талаптарға сәйкестік деңгейі АҚ талаптарына сәйкес емес.

12-параграф. ҚР СТ ГОСТ Р 50739-95-2006 сәйкес ақпаратқа рұқсатсыз қолжетімділіктен қорғау жүйесін тексеру және талдау

68. ҚР СТ ГОСТ Р 50739-95-2006 сәйкес ақпаратқа рұқсатсыз қолжетімділіктен қорғау жүйесін тексеру және талдау кезінде келесі процестерді тексеру қажет:

1) ҚР СТ ГОСТ Р 50739-2006 4 бөліміне сәйкес ақпаратты аттестаттау объектісінде өңдеген кезде оны РҚЖ қорғаулын қамтамасыз ету;

2) ҚР СТ ГОСТ Р 50739-2006 5.1 бөліміне сәйкес қолжетімділік құқықтарын қорғалу көрсеткіштерімен бөлуді іске асыру;

3) ҚР СТ ГОСТ Р 50739-2006 5.2 бөліміне сәйкес ЕТҚ ақпараттың қорғалуына қатысы бар оқиғаларды тіркеуді қолдауы тиістілігін көздейтін талаптарды орындау;

4) ҚР СТ ГОСТ Р 50739-2006 5.3 бөліміне сәйкес ЕТҚ құрамында ЕТҚ қолжетімділікті бөлуге және есепке алуға қойылатын талаптардың орындалуын қамтамасыз ететіне кепілдік алуға мүмкіндік беретін техникалық және бағдарламалық механизмдердің бар болу қажеттігін көздейтін кепілдіктерге қойылатын талаптардың орындалуы;

5) ҚР СТ ГОСТ Р 50739-2006 6 бөліміне сәйкес кешенді қорғау құралдарының толық және жан-жақты сипаттамасы.

69. Аттестаттау объектілерін рұқсатсыз қолжетімділіктен қорғау талаптарына сәйкестігіне зерттеу және талдау нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осы Әдістеменің 68-тармағының барлық тармақшалары орындалған жағдайда – аттестаттау объектісін рұқсатсыз қолжетімділіктен қорғау жүйесі АҚ талаптарына сәйкес;

2) осы Әдістеменің 68-тармағының барлық тармақшалары орындалмаған жағдайда - аттестаттау объектісін рұқсатсыз қолжетімділіктен қорғау жүйесі АҚ талаптарына сәйкес емес.

13-параграф. Аттестаттау объектісін аспаптық тексеру

70. Аттестаттау объектісі инфрақұрылымы компоненттерін аспаптық тексеру өтініш беруші ұсынған аттестаттау объектісі компоненттеріне қол жеткізуге арналған есеп жазбаларының негізінде мамандандырылған бағдарламалық аппаратық кешеннің (бұдан әрі - БАК) көмегімен аттестаттау объектісіндегі осалдықтарды айқындау мақсатында жүргізіледі.

71. Аттестаттау объектісін аспаптық тексеру мыналарды қамтиды:

1) БАК күйге келтіру (локальдық және қашықтықтан тексерулер жүргізуге арналған есеп жазбасын жазу, аспаптық тексеру режимін таңдау және т.б.);

2) БАК іске қосу;

3) айқындалған осалдықтардың сипаттамасы, саны мен деңгейі көрсетілген тізбесін қамтитын бағдарламалық есепті қалыптастыру және беру;

4) аспаптық тексеру нәтижелерін сараптамалық бағалау мен аттестаттық тексеру актісіне (қосымша аттестаттық) қоса берілетін есепті қалыптастыру.

72. Аспаптық тексеру нәтижелерінің нәтижелерінің негізінде Аттестаттық тексеру актісіне келесі шешімдердің біреуі енгізіледі:

1) осалдықтар жоқ болған жағдайда – сыртқы және ішкі басып енуден қорғау жүйесі АҚ талаптарына сәйкес;

2) осалдықтар орын алған жағдайда - сыртқы және ішкі басып енуден қорғау жүйесі АҚ талаптарына сәйкес емес.

5. Аттестаттық тексеру актісін жасау

73. Аттестаттық тексерудің нәтижелері барлық жұмыстар бойынша тексеру парақтарының толық жинағы негізінде аттестаттық тексеруге кіретін барлық жұмыс түрлері аяқталғаннан кейін жасалатын Аттестаттық тексеру актісі түрінде ресімделеді.

74. Аттестаттық тексеру актісі еркін нысанда жасалады және мыналарды қамтиды:

1) АҚ жөніндегі ТҚ зерттеу, талдау және бағалау нәтижелері;

2) БТ, ҚР СТ ИСО / МЭК 27001-2008, ҚР СТ ИСО / МЭК 27002-2009 және ҚР СТ ГОСТ Р 50739-95-2006, АҚ жөніндегі ТҚ стандарттары талаптарын орындау бойынша жұмыстарды ұйымдастыру жай-күйі туралы есеп;

3) аттестаттау объектісін аспаптық тексеру бойынша есеп;

4) аттестаттық тексерудің барлық жұмыс түрлерінің нәтижелері бойынша қорытынды мен сәйкессіздіктер орын алған жағдайда оларды жою жөніндегі ұсынымдар.

75. Аттестаттық тексеру актісі бес данада жасалады және біреуі мемлекеттк техникалық қызметте қалады, ал қалған даналары аттестациялық комиссия мүшелері мен өтініш беруші үшін уәкілетті органға жіберіледі.