Ақпараттық жүйенің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсының ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесін бекіту туралы

Күшін жойған

Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 51/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 11 сәуірде № 16744 болып тіркелді. Күші жойылды - Қазақстан Республикасының Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 15 маусымдағы № 131/НҚ бұйрығымен

Ескерту. Күші жойылды – ҚР Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 15.06.2019 № 131/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының 7-1-бабының 6) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған Ақпараттық жүйенің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсының ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесі бекітілсін.

2. "Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесін бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушысының 2016 жылғы 28 қаңтардағы № 108 бұйрығының (Қазақстан Республикасының нормативтік құқықтық актілерін мемлекеттік тіркеу тізілімінде № 13236 болып тіркелген, "Әділет" Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесінде 2016 жылғы 4 наурызда жарияланған) күші жойылды деп танылсын.

3. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті заңнамада белгіленген тәртіппен :

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелген күнінен бастап күнтізбелік он күн ішінде оның көшірмелерін қағаз және электронды түрде қазақ және орыс тілдерінде баспа және электрондық түрде Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу және ресми жариялауға " Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді;

3) осы бұйрық мемлекеттік тіркелген күнінен кейін күнтізбелік он күн ішінде оның көшірмесін мерзімді баспа басылымдарына ресми жариялауға жіберуді;

4) осы бұйрық ресми жарияланғаннан кейін оны Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің ресми интернет-ресурсында орналастыруды;

5) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Заң департаментіне осы тармақтың 1), 2), 3) және 4) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер беруді қамтамасыз етсін.

4. Осы бұйрықтың орындалуын бақылауды жетекшілік ететін Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

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

Қазақстан Республикасының
Қорғаныс және аэроғарыш
өнеркәсібі министрі *Б. Атамқұлов*

Қазақстан Республикасы
Қорғаныс және аэроғарыш
өнеркәсібі министрінің
2018 жылғы 28 наурыздағы
№ 51/НҚ бұйрығымен
бекітілген

Ақпараттық жүйенің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсының ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесі

1-тарау. Жалпы ережелер

1. Осы Ақпараттық жүйенің, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасының, мемлекеттік органның интернет-ресурсының ақпараттық қауіпсіздік талаптарына сәйкестігіне

аттестаттық зерттеп-қарауды жүргізу әдістемесі (бұдан әрі – Әдістеме) " Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңының (бұдан әрі – Заң) 7-1-бабының 6) тармақшасына және Қазақстан Республикасы Үкіметінің 2016 жылғы 23 мамырдағы № 298 қаулысымен бекітілген Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестікке аттестаттаудан өткізу қағидаларына сәйкес әзірленді.

2. Осы Әдістеме ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауға жүргізуге арналған.

3. Осы Әдістемеде мынадай негізгі ұғымдар мен қысқартулар пайдаланылады :

1) ақпараттық активтер – деректер базалары, жүйелік құжаттама, пайдаланушыға арналған басшылықтар, есеп материалдары, аттестаттау объектісін пайдалану немесе қолдау рәсімдері, ақпараттық бағдарламалық қамтылымның 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 платформасын, 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 бойынша техникалық құжаттама (бұдан әрі – АҚ бойынша ТҚ) – ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға (бұдан әрі – БТ) сәйкес әзірленген және аттестаттау объектісінің ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жалпы талаптарды, қағидаттармен қағидаларды регламенттейтін құжаттар жиынтығы;

5) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – АҚ) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және

ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі;

6) аутентификация – пайдаланушы (қол жеткізу субъектісі) үшін ол ұсынған сәйкестендіргішті зерттеп-қарау және оның түпнұсқалығын растау;

7) аттестаттау объектілері – ақпараттық жүйе, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасы, интернет-ресурс;

8) аттестаттау объектісінің инфрақұрылымы компоненттерін аспаптық зерттеп-қарау – байланыс арналарын, тораптарын, серверлерді, жұмыс станцияларын, қолданбалы және жүйелік бағдарламалық қамтылымды, деректер базалары мен желі элементтерін бағдарламалық құрал немесе қашықтықтағы не локалдық диагностика арқылы олардағы осалдықтарды айқындауға қатысты сканерлеу жүргізу;

9) осалдық – бағдарламалық қамтылымда жұмыс қабілеттілігін бұзуға немесе белгіленген рұқсаттардан тыс қандай болсын заңсыз іс-әрекеттерді орындауға мүмкіндік беретін бағдарламалық қамтылымдағы кемшілік;

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

11) бағдарламалық қамтылым (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. Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарау мына тәртіппен жүргізіледі:

1) аттестаттау объектісінің құрылымын алдын ала зерделеу;

2) АҚ жөніндегі ТҚ зерделеу, талдау және бағалау;

3) аттестаттау объектісін аспаптық зерттеп-қарауды қоса алғанда, БТ, ҚР СТ ИСО/МЭК 27001 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар " (бұдан әрі – ҚР СТ ИСО/МЭК 27001), ҚР СТ ИСО/МЭК 27002 "Қауіпсіздікті

қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі қағидалар жинағы (бұдан әрі – ҚР СТ ИСО/МЭК 27002) және ҚР СТ МЕМСТ Р 50739 " Есептеу техникасы құралдары. Ақпаратқа рұқсатсыз қол жеткізуден қорғау. Жалпы техникалық талаптар" (бұдан әрі - ҚР СТ МЕМСТ Р 50739), АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстарды ұйымдастыру жай-күйін зерттеп-қарау.

4) аттестаттық зерттеп-қарау актісін қалыптастыру.

2-тарау. Аттестаттау объектісінің құрылымын алдын ала зерделеу

5. Аттестаттау объектісінің құрылымын алдын ала зерделеу аттестаттау объектісінің жұмыс істеу ерекшеліктерін айқындау және аттестаттау объектісінде пайдаланылатын аппараттық-бағдарламалық құралдар, локалдық және корпоративтік желі, ақпаратты қорғау технологиялары мен рәсімдері туралы жалпы ақпарат алу мақсатында жүргізіледі.

6. Құрылымды алдын ала зерделеу процесі мынадай техникалық құжаттамамен танысуды қамтиды:

1) аттестаттау объектісін құруға арналған техникалық тапсырма;

2) аттестаттау объектісінің жалпы функционалдық және локалдық схемасы;

3) аттестаттау объектісінде пайдаланылатын бағдарламалық және техникалық құралдар тізімі;

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

3-тарау. АҚ жөніндегі ТҚ-ны зерделеу, талдау және бағалау

7. АҚ жөніндегі ТҚ-ны зерделеу, талдау және бағалау БТ, ҚР СТ ИСО/МЭК 27001 және ҚР СТ ИСО/МЭК 27002 талаптарына ақпараттық қауіпсіздік бойынша талаптардың толықтығын, өзектілігін және дұрыстығын анықтау мақсатында жүргізіледі.

8. Ақпараттық қауіпсіздік талаптарына сәйкестікке зерделеу, 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 қамтылымды түгендеу мен паспорттандыру қағидалары (бұдан әрі – Түгендеу қағидалары);

6) ішкі ақпараттық қауіпсіздік аудитін жүргізу 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 рәсімін ұйымдастыру қағидалары;

11) вирусқа қарсы бақылауды ұйымдастыру қағидалары;

12) мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану қағидалары (бұдан әрі – Мобильдік құрылғыларды пайдалану қағидалары);

13) ақпаратты өңдеу 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 оқыс оқиғаларына және штаттан тыс (дағдарысты) жағдайларда әрекет етуі бойынша іс-қимыл тәртібі туралы нұсқаулық (бұдан әрі – Штаттан тыс жағдайлар бойынша нұсқаулық).

9. Әрбір АҚ жөніндегі ТҚ таныстыру парағының (ерікті нысанда) бар болуына, оның толықтығы мен өзектілігіне тексеру қажет.

10. АҚ жөніндегі ТҚ зерделеу, талдау және бағалаудың нәтижелері аттестаттық зерттеп-қарау актісінде белгіленеді.

1-параграф. Саясатты зерделеу, талдау және бағалау

11. Саясатты зерделеу, талдау және бағалау Саясаттың негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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) Саясат бұзылған жағдайда қойылатын талаптар;

5) АҚ басқару шеңберіндегі жалпы анықтамалар және қызметкерлердің функциялары;

6) Саясатты мерзімді қайта қарауға қойылатын талаптар;

7) басшылықтың АҚ қамтамасыз ету мәселелерін қолдау бойынша функциялары.

12. Саясатты зерделеу, талдау және бағалау нәтижелері негізінде аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) осы Әдістеменің 11-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Саясат АҚ талаптарына сәйкес;

2) осы Әдістеменің 11-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда – Саясат АҚ талаптарына сәйкес емес.

2-параграф. Сәйкестендіру қағидаларын зерделеу, талдау және бағалау

13. Сәйкестендіру қағидаларын зерделеу, талдау және бағалау Сәйкестендіру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) активтерді (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 класын, маңыздылығы мен активтің иесін көрсетіп);

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

5) активтер тізілімінің мәліметі толықтығына арналған талаптарды орындау.

14. Сәйкестендіру қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Сәйкестендіру қағидалары АҚ талаптарына сәйкес - осы Әдістеменің 13-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Сәйкестендіру қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 13-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

15. Тәуекелдерді бағалау әдістемесін зерделеу, талдау және бағалау Тәуекелдерді бағалау әдістемесі негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 қарау 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) оқыс оқиға 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.

16. Тәуекелдерді бағалау әдістемесін зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Тәуекелдерді бағалау әдістемесі АҚ талаптарына сәйкес – осы Әдістеменің 15-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Тәуекелдерді бағалау әдістемесі – АҚ талаптарына сәйкес емес осы Әдістеменің 15-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

17. Жұмыстың үздіксіздігін қамтамасыз ету қағидаларын зерделеу, талдау және бағалау Жұмыстың үздіксіздігін қамтамасыз ету қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 және оларды өзектендіруді 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 тағайындау бойынша;

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 қалудан және коммуникация қызметтерінің жұмысынан орын алатын бұзушылықтардан жабдықты қорғау тәсілдері;

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

18. Жұмыстың үздіксіздігін қамтамасыз ету қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Жұмыстың үздіксіздігін қамтамасыз ету қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 17-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Жұмыстың үздіксіздігін қамтамасыз ету қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 17-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

5-параграф. Түгендеу қағидаларын зерделеу, талдау және бағалау

19. Түгендеу қағидаларын зерделеу, талдау және бағалау Түгендеу қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 қамтылымды 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.

20. Түгендеу қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Түгендеу қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 19-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Түгендеу қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 19-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

21. Ішкі аудит қағидаларын зерделеу, талдау және бағалау Ішкі аудит қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 жүргізудің кесте-жоспарының болуы мен жүргізілуіне 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.

22. Ішкі аудит қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Ішкі аудит қағидалары АҚ талаптарына сәйкес –;осы Әдістеменің 21-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда.

2) Ішкі аудит қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 21-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

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

1) ҚР СТ ИСО/МЭК 27002 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 тапсырмаға сәйкес криптографиялық шифрлауға қойылатын талаптар.

24. Криптографиялық құралдарды пайдалану қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) осы Әдістеменің 23-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда – Криптографиялық құралдарды пайдалану қағидалары АҚ талаптарына сәйкес;

2) осы Әдістеменің 23-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда – Криптографиялық құралдарды пайдалану қағидалары АҚ талаптарына сәйкес емес.

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

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

1) жаңа пайдаланушыны тіркеу сәтінен бастап пайдаланушыны тіркеуден алып тастағанға дейін пайдаланушыларды тіркеу кезеңінің 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.

26. Қол жеткізу құқықтарын бөлу қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Қол жеткізу құқықтарын бөлу қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 25-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Қол жеткізу құқықтарын бөлу қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 25-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

27. Интернетті және электрондық поштаны пайдалану қағидаларын зерделеу, талдау және бағалау Интернетті және электрондық поштаны пайдалану қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 қолжетімділікті мониторингілеу 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.

28. Интернетті және электрондық поштаны пайдалану қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Интернетті және электрондық поштаны пайдалану қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 27-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Интернетті және электрондық поштаны пайдалану қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 27-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

10-параграф. Аутентификация рәсімін ұйымдастыру қағидаларын зерделеу, талдау және бағалау

29. Аутентификация рәсімін ұйымдастыру қағидаларын зерделеу, талдау және бағалау Аутентификация рәсімдерін ұйымдастыру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) пайдаланушыларды оларға сеніп 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, мысалы, сақталатын макрокомандаларды немесе функционалдық клавишаларды пайдалана отырып, тыйым салу бойынша талаптардың сипаттамасы.

30. Аутентификация рәсімін ұйымдастыру қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Аутентификация рәсімдерін ұйымдастыру қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 29-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Аутентификация рәсімдерін ұйымдастыру қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 29-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

31. Вирусқа қарсы бақылауды ұйымдастыру қағидаларын зерделеу, талдау және бағалау Вирусқа қарсы бақылауды ұйымдастыру қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында

жүргізіледі және мынадай мәліметтердің болуын анықтау мен сапалы бағалау бойынша жұмыстар жүргізуді қамтиды:

1) лицензияланған вирусқа қарсы бағдарламалық қамтылымдарды пайдалану бойынша талаптар;

2) вирусқа қарсы бағдарламалық қамтылымдарды жаңарту мерзімділігі бойынша талаптар;

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

4) веб-парақтарды зиянды бағдарламалық қамтылымның болуына қатысты зерттеп-қарау талаптары;

5) күдікті немесе авторланбаған ақпарат тасымалдауыштардағы барлық файлдарды немесе жалпыға қолжетімді желілерден алынған файлдарды вирустардың болуына қатысты зерттеп-қарау бойынша талаптар;

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

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

8) вирустық шабуыладардан кейін ақпаратты қалпына келтіру рәсімдерінің сипаттамалары.

32. Вирусқа қарсы бақылауды ұйымдастыру қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Вирусқа қарсы бақылауды ұйымдастыру қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 31-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Вирусқа қарсы бақылауды ұйымдастыру қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 31-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

33. Мобильдік құрылғыларды пайдалану қағидаларын зерделеу, талдау және бағалау Мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану қағидалары негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 ақпарат тасымалдауыштарды физикалық қорғау бойынша талаптар;

3) мобильдік құрылғылардың және ақпарат тасымалдауыштардың тізбесін құру және оларды маркалау бойынша талаптар;

4) ақпарат тасымалдауыштарды беру журналын жүргізуге қойылатын талаптар;

5) ақпарат тасымалдауыштарды пайдалану тәртібі;

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

7) алмалы тасымалдауыштарды 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 тасымалдауыштарын пайдалану, сондай-ақ жоғалту және жою кезінде қызметкерлердің рұқсат етілмеген іс-қимыл жасау фактілері айқындалған кезіндегі іс-әрекет тәртібі.

34. Мобильдік құрылғыларды пайдалану қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану қағидалары АҚ талаптарына сәйкес - осы Әдістеменің 33-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Мобильдік құрылғыларды және ақпарат тасымалдауыштарды пайдалану қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 33-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

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

1) БТ және ҚР СТ ИСО/МЭК 27002 сәйкес серверлік үй-жайды физикалық қорғауға қойылатын талаптар;

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

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

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

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

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

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

8) БТ және ҚР СТ ИСО/МЭК 27002 сәйкес жабдықты қауіпсіз кәдеге жаратуға немесе қайтадан пайдалануға қойылатын талаптар;

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

36. Физикалық қорғауды ұйымдастыру қағидаларын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Физикалық қорғауды ұйымдастыру қағидалары АҚ талаптарына сәйкес – осы Әдістеменің 35-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Физикалық қорғауды ұйымдастыру қағидалары АҚ талаптарына сәйкес емес – осы Әдістеменің 35-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

14-параграф. Әкімші басшылығын зерделеу, талдау және бағалау

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

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

2) оқыс оқиғалар, штаттан тыс жағдайлар, апатты табиғат-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 рәсімдері.

38. Әкімші басшылығын зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Әкімшінің басшылығы АҚ талаптарына сәйкес – осы Әдістеменің 37-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Әкімшінің басшылығы АҚ талаптарына сәйкес емес – осы Әдістеменің 37-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

39. Резервтік көшіру регламентін зерделеу, талдау және бағалау Резервтік көшіру регламенті негізгі ережелерінің толықтығын, өзектілігін және дұрыстығын айқындау мақсатында жүргізіледі және мынадай 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 рәсімдерінің сипаттамасы;

7) ақпаратты резервте сақтау 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 зерттеп-қарау журналын, резервтік ақпаратты электрондық тасымалдауыштарды есепке алу журналын, резервтік ақпаратты электрондық тасымалдауыштарды алып кіру/алып шығу журналын жүргізу бойынша талаптар.

40. Резервтік көшіру регламентін зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Резервтік көшіру регламенті АҚ талаптарына сәйкес – осы Әдістеменің 39-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Резервтік көшіру регламенті АҚ талаптарына сәйкес емес – осы Әдістеменің 39-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

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

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

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

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

3) штаттан тыс жағдай орын алған кезде хабарлау тәртібі;

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

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

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

7) оқыс оқиғалардың және басқа штаттан тыс жағдайлардың орын алу оқиғаларын зерттеп-қарау бойынша талаптар.

42. Штаттан тыс жағдайлар жөніндегі нұсқаулықты зерделеу, талдау және бағалау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Штаттан тыс жағдайлар жөніндегі нұсқаулық АҚ талаптарына сәйкес– осы Әдістеменің 41-тармағында көрсетілген барлық мәліметтер болған және олар АҚ талаптарына сәйкес келген жағдайда;

2) Штаттан тыс жағдайлар жөніндегі нұсқаулық АҚ талаптарына сәйкес емес – осы Әдістеменің 41-тармағында көрсетілген мәліметтердің бірі болмаған немесе олар АҚ талаптарына сәйкес келмеген жағдайда.

4-тарау. Аттестаттау объектісін аспаптық зерттеп-қарауды қоса алғанда, БТ, ҚР СТ ИСО/МЭК 27001 және ҚР СТ ИСО/МЭК 27002, ҚР СТ МЕМСТ Р 50739, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстар ұйымдастырудың жай-күйін тексеру

43. Аттестаттау объектісін аспаптық зерттеп-қарауды қоса алғанда, БТ, ҚР СТ ИСО/МЭК 27001 және ҚР СТ ИСО/МЭК 27002, ҚР СТ МЕМСТ Р 50739, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстар ұйымдастырудың жай-күйін зерттеп-қарау мыналарды зерттеп-қарау 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 оқыс оқиғаларды басқаруды ұйымдастыруды;

10) бизнестің үздіксіздігін басқаруды;

11) құқықтық талаптарға сәйкестік дәрежесін;

12) ҚР СТ МЕМСТ Р 50739 талаптарына сәйкес ақпаратты рұқсатсыз қол жеткізуден қорғау жүйесіне қойылатын талаптарды.

44. Аттестаттау объектісін аспаптық зерттеп-қарауды қоса алғанда, БТ, ҚР СТ ИСО/МЭК 27001 және ҚР СТ ИСО/МЭК 27002, ҚР СТ МЕМСТ Р 50739, АҚ жөніндегі ТҚ талаптарын орындау бойынша жұмыстар ұйымдастырудың жай-күйін зерттеп-қарау нәтижелері Аттестаттық зерттеп-қарау актісінде белгіленеді.

1-параграф. Саясат ережелерін зерттеп-қарау және талдау

45. Саясат ережелерін зерттеп-қарау 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 зерттеп-қарау қажет.

46. Саясат ережелерін зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Саясат ережелерінің орындалуы АҚ талаптарына сәйкес – осы Әдістеменің 45-тармағы орындалған жағдайда;

2) Саясат ережелерінің орындалуы АҚ талаптарына сәйкес емес – осы Әдістеменің 45-тармағы орындалмаған жағдайда.

2-параграф. Ақпараттық қауіпсіздікті басқару бойынша процестерді зерттеп-қарау және талдау

47. Ақпараттық қауіпсіздікті басқару бойынша процестерді зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарауды жүзеге асыру қажет:

1) аттестаттау объектісінің ақпараттық қауіпсіздігін қамтамасыз ету үшін жауапты 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.

48. Ақпараттық қауіпсіздікті басқару бойынша процестерді зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) ақпараттық қауіпсіздікті басқару АҚ талаптарына сәйкес – осы Әдістеменің 47-тармағының барлық тармақшалары орындалған жағдайда;

2) ақпараттық қауіпсіздікті басқару АҚ талаптарына сәйкес емес – осы Әдістеменің 47-тармағының барлық тармақшалары орындалмаған жағдайда.

3-параграф. Активтерді басқаруды ұйымдастыруды зерттеп-қарау және талдау

49. Активтерді басқаруды ұйымдастыруды зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарауды 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, сезгіштігі мен ұйым үшін маңыздылығы тұрғысынан сыныптауды талдау;

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

50. Активтерді басқаруды ұйымдастыру процестерін зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) активтерді басқаруды ұйымдастыру процесі АҚ талаптарына сәйкес –осы Әдістеменің 49-тармағының барлық тармақшалары орындалған жағдайда;

2) активтерді басқаруды ұйымдастыру процесі АҚ талаптарына сәйкес емес – осы Әдістеменің 49-тармағының барлық тармақшалары орындалмаған жағдайда.

4-параграф. Персоналға байланысты қауіпсіздікті қамтамасыз етуді зерттеп-қарау және талдау

51. Персоналға байланысты қауіпсіздікті қамтамасыз етуді зерттеп-қарау және талдау кезінде:

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

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

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

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

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

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

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

52. Персоналға байланысты қауіпсіздікті қамтамасыз етуді зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) Персоналға байланысты қауіпсіздікті қамтамасыз ету АҚ талаптарына сәйкес – осы Әдістеменің 51-тармағының барлық тармақшалары орындалған жағдайда;

2) Персоналға байланысты қауіпсіздікті қамтамасыз ету АҚ талаптарына сәйкес емес – осы Әдістеменің 51-тармағының барлық тармақшалары орындалмаған жағдайда.

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

53. Жабдықты және қоршаған орта қауіпсіздігін физикалық қорғауды зерттеп-қарау мен талдау кезінде мынадай процестерді зерттеп-қарау қажет:

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

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

3) ҚР СТ ИСО/МЭК 27002 сәйкес сыртқы қатерлерден қорғауды ұйымдастыру;

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

5) ҚР СТ ИСО/МЭК 27002 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 мен БТ сәйкес орналастыру;

7) ҚР СТ ИСО/МЭК 27002 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 және БТ сәйкес кәбілдік желінің ақпараттық қауіпсіздігін қамтамасыз ету;

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

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

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

54. Жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғауды зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғау АҚ талаптарына сәйкес – осы Әдістеменің 53-тармағының барлық тармақшалары орындалған жағдайда;

2) жабдықты және қоршаған ортаның қауіпсіздігін физикалық қорғау АҚ талаптарына сәйкес емес – осы Әдістеменің 53-тармағының барлық тармақшалары орындалмаған жағдайда.

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

55. Ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз етуді зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарауды жүзеге асыру қажет:

1) ҚР СТ ИСО/МЭК 27002 сәйкес операциялық рәсімдерды құжатпен ресімдеу, аттестаттау объектісіндегі өзгерістерді бақылауды жүргізу, аттестаттау

объектісінде міндеттемелерді бөлу және әзірлеу, тестілеу мен пайдалану құралдарын бөлу;

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

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

4) ҚР СТ ИСО/МЭК 27002 сәйкес зиянды кодтан қауіпсіз қорғауды қамтамасыз ету;

5) ҚР СТ ИСО/МЭК 27002 сәйкес аттестаттау объектілерінде ақпаратты резервте сақтау рәсімдерін жүргізген кезде ақпараттық қауіпсіздік талаптарын сақтау;

6) ҚР СТ ИСО/МЭК 27002 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 және БТ сәйкес ақпарат тасымалдаушылармен (таспалар, дискілер, флеш-жинақтағыштар) жұмыс кезінде ақпараттық қауіпсіздікті сақтау;

9) ҚР СТ ИСО/МЭК 27002 сәйкес ақпарат алмасу кезінде ақпараттық қауіпсіздікті сақтау;

10) ҚР СТ ИСО/МЭК 27002 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.

56. Ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз етуді зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз ету АҚ талаптарына сәйкес – осы Әдістеменің 55-тармағының барлық тармақшалары орындалған жағдайда;

2) ақпаратты өңдеу құралдарының тиісінше және қауіпсіз жұмыс істеуін қамтамасыз ету АҚ талаптарына сәйкес емес – осы Әдістеменің 55-тармағының барлық тармақшалары орындалмаған жағдайда.

7-параграф. Ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды зерттеп-қарау және талдау

57. Ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарау қажет:

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

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

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

4) ҚР СТ ИСО/МЭК 27002 сәйкес желілік сервистерге қол жеткізуге рұқсат беру кезінде ақпараттық қауіпсіздікті қамтамасыз ету;

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

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

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

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

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

58. Ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыруды зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) осы Әдістеменің 57-тармағының барлық тармақшалары орындалған жағдайда – ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыру АҚ талаптарына сәйкес;

2) осы Әдістеменің 57-тармағының барлық тармақшалары орындалмаған жағдайда – ақпараттық ресурстарға қолжетімділікті басқаруды ұйымдастыру АҚ талаптарына сәйкес емес.

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

59. Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестерін зерттеп-қарау және талдау кезінде:

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

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

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

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

5) ҚР СТ ИСО/МЭК 27002 сәйкес аттестаттау объектісін әзірлеу және енгізу процесінде ақпараттық қауіпсіздікті қамтамасыз етуді;

6) ҚР СТ ИСО/МЭК 27002 сәйкес аттестаттау объектісінің осалдықтарын жою, мониторингілеу 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 зерттеп-қарау қажет.

60. Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестерін зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестері АҚ талаптарына сәйкес –осы Әдістеменің 59-тармағының барлық тармақшалары орындалған жағдайда;

2) Аттестаттау объектілерін әзірлеу, енгізу және қызмет көрсету процестері АҚ талаптарына сәйкес емес – осы Әдістеменің 59-тармағының барлық тармақшалары орындалмаған жағдайда.

9-параграф. Ақпараттық қауіпсіздік саласындағы оқыс оқиғаларды басқаруды ұйымдастыруды зерттеп-қарау және талдау

61. Ақпараттық қауіпсіздік саласындағы оқыс оқиғаларды басқаруды ұйымдастыруды зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарау қажет:

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

2) ҚР СТ ИСО/МЭК 27002 сәйкес басшылық жауаптылығын белгілеу;

3) ҚР СТ ИСО/МЭК 27002 сәйкес ақпараттық қауіпсіздік оқыс оқиғаларын тіркеу және мониторингілеу, ақпараттық қауіпсіздік саласындағы оқыс оқиғалар

туралы хабарлаудың жеделдігі, ақпараттық қауіпсіздік оқыс оқиғалары туралы есептер құру рәсімдері;

4) ҚР СТ ИСО/МЭК 27002 сәйкес ақпараттық қауіпсіздік оқыс оқиғасы сот талқылауына әкеп соғу жағдайында ақпараттық қауіпсіздік оқыс оқиғалары туралы ақпаратты жинау, сақтау және ұсыну;

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

62. Ақпараттық қауіпсіздік саласындағы оқыс оқиғаларды басқаруды ұйымдастыруды зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) ақпараттық қауіпсіздік оқыс оқиғаларын басқару АҚ талаптарына сәйкес – осы Әдістеменің 61-тармағының барлық тармақшалары орындалған жағдайда;

2) ақпараттық қауіпсіздік оқыс оқиғаларын басқару АҚ талаптарына сәйкес емес – осы Әдістеменің 61-тармағының барлық тармақшалары орындалмаған жағдайда.

10-параграф. Бизнестің үздіксіздігін басқаруды зерттеп-қарау және талдау

63. Бизнестің үздіксіздігін басқаруды зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарау қажет:

1) ҚР СТ ИСО/МЭК 27002 сәйкес ақпараттық қауіпсіздік бойынша процестерді қамтитын бизнестің үздіксіздігін дамыту және қолдау;

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

3) ҚР СТ ИСО/МЭК 27002 сәйкес бизнестің үздіксіздігі жоспарларын іске асыру;

4) ҚР СТ ИСО/МЭК 27002 сәйкес бизнестің үздіксіздігін қамтамасыз ету жөніндегі жоспарларды тестілеуді, қолдау мен қайта қарауды жүргізу.

64. Бизнестің үздіксіздігін басқаруды зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) бизнестің үздіксіздігін басқару бойынша рәсімдер АҚ талаптарына сәйкес – осы Әдістеменің 63-тармағының барлық тармақшалары орындалған жағдайда;

2) бизнестің үздіксіздігін басқару бойынша рәсімдер АҚ талаптарына сәйкес емес – осы Әдістеменің 63-тармағының барлық тармақшалары орындалмаған жағдайда.

11-параграф. Құқықтық талаптарға сәйкестік деңгейін зерттеп-қарау және талдау

65. Құқықтық талаптарға сәйкестік деңгейін зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарау қажет:

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

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

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

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

5) ҚР СТ ИСО/МЭК 27002 сәйкес ақпараттық қауіпсіздік аудитін жүргізген кезде басқару және келісу бойынша шараларды қолдану;

6) ҚР СТ ИСО/МЭК 27002 сәйкес аспаптық аудит құралдары қолжетімді болған кезде ақпараттық қауіпсіздікті қамтамасыз ету.

66. Құқықтық талаптарға сәйкестік деңгейін зерттеп-қарау және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) құқықтық талаптарға сәйкестік деңгейі АҚ талаптарына сәйкес – осы Әдістеменің 65-тармағының барлық тармақшалары орындалған жағдайда;

2) құқықтық талаптарға сәйкестік деңгейі АҚ талаптарына сәйкес емес –осы Әдістеменің 65-тармағының барлық тармақшалары орындалмаған жағдайда.

12-параграф. ҚР СТ МЕМСТ Р 50739 сәйкес ақпаратқа рұқсатсыз қолжетімділіктен қорғау жүйесін зерттеп-қарау және талдау

67. ҚР СТ МЕМСТ Р 50739 сәйкес ақпаратқа рұқсатсыз қолжетімділіктен қорғау жүйесін зерттеп-қарау және талдау кезінде мынадай процестерді зерттеп-қарау қажет:

1) ҚР СТ МЕМСТ Р 50739 сәйкес ақпаратты аттестаттау объектісінде өңдеген кезде оны РҚЖ қорғаулын қамтамасыз ету;

2) ҚР СТ МЕМСТ Р 50739 сәйкес қолжетімділік құқықтарын қорғалу көрсеткіштерімен бөлуді іске асыру;

3) ҚР СТ МЕМСТ Р 50739 сәйкес ЕТҚ ақпараттың қорғалуына қатысы бар оқиғаларды тіркеуді қолдауы тиістілігін көздейтін талаптарды орындау;

4) ҚР СТ МЕМСТ Р 50739 сәйкес ЕТҚ құрамында ЕТҚ қолжетімділікті бөлуге және есепке алуға қойылатын талаптардың орындалуын қамтамасыз ететіне кепілдік алуға мүмкіндік беретін техникалық және бағдарламалық

механизмдердің болу қажеттігін көздейтін кепілдіктерге қойылатын талаптардың орындалуы;

5) ҚР СТ МЕМСТ Р 50739 сәйкес кешенді қорғау құралдарының толық және жан-жақты сипаттамасы.

68. Аттестаттау объектілерін рұқсатсыз қолжетімділіктен қорғау талаптарына сәйкестігіне зерделеу және талдау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі енгізіледі:

1) аттестаттау объектісін рұқсатсыз қолжетімділіктен қорғау жүйесі АҚ талаптарына сәйкес – осы Әдістеменің 67-тармағының барлық тармақшалары орындалған жағдайда;

2) аттестаттау объектісін рұқсатсыз қолжетімділіктен қорғау жүйесі АҚ талаптарына сәйкес емес – осы Әдістеменің 67-тармағының барлық тармақшалары орындалмаған жағдайда.

13-параграф. Аттестаттау объектісін аспаптық тексеру

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

70. Аттестаттау объектісін аспаптық зерттеп-қарау мыналарды қамтиды:

1) БАК күйге келтіру (локалдық және қашықтықтан тексерулер жүргізуге арналған есеп жазбасын жазу, аспаптық зерттеп-қарау 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 зерттеп-қарау нәтижелерін сараптамалық бағалау мен аттестаттық зерттеп-қарау актісіне (қосымша аттестаттық) қоса берілетін есепті қалыптастыру.

71. Аспаптық зерттеп-қарау нәтижелері негізінде Аттестаттық зерттеп-қарау актісіне мынадай шешімдердің бірі 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-тарау. Аттестаттық зерттеп-қарау актісін жасау

72. Аттестаттық зерттеп-қараудың нәтижелері барлық жұмыстар бойынша зерттеп-қарау парақтарының толық жинағы негізінде аттестаттық зерттеп-қарауға кіретін барлық жұмыс түрлері аяқталғаннан кейін жасалатын Аттестаттық зерттеп-қарау актісі түрінде ресімделеді.

73. Аттестаттық зерттеп-қарау актісі еркін нысанда жасалады және мыналарды қамтиды:

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

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

3) аттестаттау объектісін аспаптық зерттеп-қарау бойынша есеп;

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

74. Аттестаттық зерттеп-қарау актісі үш данада жасалады және бір данасы мемлекеттік техникалық қызметте қалады, ал қалған 2 даналары уәкілетті органға уәкілетті орган мен өтінім берушіге жіберіледі