

Қазақстан Республикасы мемлекеттік органдары мен ұйымдарының ақпараттық желілері мен ресурстарының қорғалуы жай-күйіне тексеру жүргізу жөніндегі нұсқаулығын бекіту туралы

Қазақстан Республикасы Премьер-Министр Кеңесі Басшысының 2012 жылғы 21 мамырдағы № 25-1-50 Бұйрығы. Қазақстан Республикасы Әділет министрлігінде 2012 жылы 18 маусымда № 7740 тіркелді.

Қазақстан Республикасы Үкіметінің 2002 жылғы 11 қыркүйектегі № 993 қаулысымен бекітілген, Қазақстан Республикасы Премьер-Министрінің кеңесі туралы ереженің 12-тармағының 21) тармақшасына сәйкес **БҰЙЫРАМЫН:**

1. Қоса беріліп отырған Қазақстан Республикасы мемлекеттік органдары мен ұйымдарының ақпараттық желілері мен ресурстарының қорғалуы жай-күйіне тексеру жүргізу жөніндегі нұсқаулығы бекітілсін.

2. Қазақстан Республикасы Премьер-Министрі Кеңесінің Мемлекеттік құпияларды қорғау бөлімі (М.И. Толымбеков) осы бұйрықты заңнамада белгіленген тәртіппен Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелуін қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау Қазақстан Республикасының Премьер-Министрі Кеңесінің Мемлекеттік құпияларды қорғау бөлімінің меңгерушісі М.И. Толымбековке жүктелсін.

4. Осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелген күннен бастап қолданысқа енгізіледі.

Кеңсе Басшысы

Е. Қошанов

КЕЛІСІЛДІ

Қазақстан Республикасы

Бас прокуроры

_____ А. Дауылбаев

2012 жылғы 14 мамыр

Қазақстан Республикасы

Ұлттық қауіпсіздік

комитетінің төрағасы

_____ Н. Әбіқаев

2012 жылғы 14 мамыр

КЕЛІСІЛДІ

Қазақстан Республикасы
Қаржы министрі
_____ Б. Жәмішев
2012 жылғы 15 мамыр

Қазақстан Республикасы
Көлік және коммуникация
министрі
_____ А. Жұмағалиев
2012 жылғы 15 мамыр

Қазақстан Республикасы
Премьер-Министр Кеңесі
Басшысының
2012 жылғы 21 мамырдағы
№ 25-1-50 бұйрығымен
бекітілген

Қазақстан Республикасының мемлекеттік органдары мен ұйымдарының ақпараттық желілері мен ресурстарының қорғалуы жай-күйіне тексеру жүргізу жөніндегі нұсқаулық

Қазақстан Республикасының мемлекеттік органдары мен ұйымдарының ақпараттық желілері мен ресурстарының қорғалуы жай-күйіне тексеру жүргізу жөніндегі нұсқаулық (бұдан әрі – Нұсқаулық) Қазақстан Республикасының 2011 жылғы 6 қаңтардағы "Қазақстан Республикасындағы мемлекеттік бақылау және қадағалау туралы", 2007 жылғы 11 қаңтардағы "Ақпараттандыру туралы", 2004 жылғы 9 қарашадағы "Техникалық реттеу туралы" заңдарына, Қазақстан Республикасы Үкіметінің 2009 жылғы 30 желтоқсандағы № 2280 қаулысымен бекітілген Мемлекеттік ақпараттық жүйелерді және мемлекеттік ақпараттық жүйелермен интеграцияланатын мемлекеттік емес ақпараттық жүйелерді олардың ақпараттық қауіпсіздік талаптарына және Қазақстан Республикасының аумағында қабылданған стандарттарға сәйкестігіне аттестаттау жүргізу ережесіне (бұдан әрі – қаулы), "Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Ақпаратты қорғаудың басқару жөніндегі ережелерінің жиынтығы" ҚР СТ ИСО/МЭК 17799-2006, "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" МЕМСТ Р ИСО/МЭК 27001-2006, "Есептегіш техника құралдары. Ақпаратқа рұқсатсыз қол жеткізуден қорғау. Жалпы техникалық талаптар" ҚР СТ МЕМСТ Р 50739-2006, "Ақпаратты қорғау. Ақпараттық жүйелерді жолдары жобалаудың, салуын, ретке-келтіру, эксплуатациялау және қорғауды қамтамасыз ету" ҚР СТ 34.022-2006

стандарттарына сәйкес әзірленді және қорғалған қолданыстағы ақпараттық жүйелерді тексеруді* қоспағанда мемлекеттік органдардың және ұйымдардың ақпараттық жүйелері мен ресурстарының қорғалу жай-күйіне тексеру жүргізу тәртібін белгілейді.

*ҚР СТ 34.025-2006 "Ақпаратты қорғау. Қорғалған қолданыстағы автоматтандырылған жүйелерді құру тәртібі. Жалпы ереже"

1. Жалпы ережелер

1. Мемлекеттік органдар мен ұйымдардың ақпараттық желілері мен ресурстарының қорғаныстық жай-күйіне тексеру (бұдан әрі – тексеру) – мемлекеттік құпияларды қорғау және ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі уәкілетті мемлекеттік органмен (бұдан әрі – уәкілетті орган), ұлттық қауіпсіздік органдарының, ақпараттандыру саласындағы уәкілетті органның, ақпараттандыру саласындағы уәкілетті ұйымның және тексерілетін мемлекеттік органдар мен ұйымдардың мемлекеттік құпияларды қорғау жөніндегі тиісті бөлімшелерінен тиісті мамандарды тарта отырып жүргізіледі. Уәкілетті органмен тексеру жүргізу үшін уәкілетті органның ұйғарымында көрсетілетін тексеру комиссияның құрамы жасақталады (бұдан әрі – Комиссия).

2. Тексеру мемлекеттік органдар мен ұйымдар іске асыратын нормативтік, ұйымдастырушылық, тәжірибелік және техникалық шаралардың Қазақстан Республикасының нормативтік құқықтық актілерінің және ақпараттық қауіпсіздікті қамтамасыз ету, ақпаратты қорғау саласындағы стандарттарының талаптарына сәйкестігін анықтау мақсатында жүзеге асырылады.

3. Тексеру уәкілетті органның бірінші басшысы қол қойған және елтаңба мөрі басылып расталған ұйғарымның негізінде, тексерушілердің жеке басын куәландыратын құжаттарды көрсете отырып жүргізіледі. Ұйғарым 2 данада әзірленеді, оның бірінші данасы тексерілетін ұйымда қалады.

4. Уәкілетті орган ұйымды алдағы тексеру туралы тексеру басталмас бұрын 10 күн алдын жазбаша хабардар етеді.

2. Тексерулер жүргізу

5. Тексеру мыналарды:

1) объектілерде қойылған ақпаратты өңдеу технологиялық режимін, қолданатын ақпараттық жүйелерді, ақпараттық жүйелердің айналымындағы ақпараттардың сипатын анықтау;

2) әр түрлі деңгейдегі және міндеттерге арналған есептеу техникалық құралдарының (қолданушылардың жұмыс станциялары, серверлік және өзге де сырт жабдықтар, ақпаратты техникалық қорғау құралдары, оның ішінде мемлекеттік

шифрлеу құралдарын қоспағанда ақпаратты криптографиялық қорғау құралдары) нақты қызметтік жағдайын ескеретін ұйымдық-өкімдік құжаттардың болуы, есептеу техникалық құралдарды пайдалану кезіндегі ұйым қызметкерлерінің жұмыс тәртібі (қаулыға сәйкес):

ақпараттық қауіпсіздікті қамтамасыз етудегі ұйымдастыру тәртібін регламенттейтін ұйым басшысының бұйрығы;

ұйымның ақпараттық қауіпсіздік саясаты;

Есептеу техникасы құралдарын паспорттандыру және корпоративтік желілердегі ақпараттық ресурстарды пайдалану ережесі;

Парольдік қорғау туралы нұсқаулық;

Штаттан тыс (дағдарыстық) жағдайларда пайдаланушылардың іс-қимыл тәртібі туралы нұсқаулық;

Вирусқа қарсы қорғауды ұйымдастыру жөніндегі нұсқаулық;

Пайдаланушының компьютерлік жабдықтар мен бағдарламалық қамтамасыз етуді пайдалану жөніндегі нұсқаулығы;

Ақпаратты резервтік көшіру туралы нұсқаулық;

Ұйымдардың корпоративтік ақпараттық желілерін пайдаланушыларды тіркеу ережесі;

Жүйелік әкімшілердің жұмысы үшін жадынама;

Есептеу техникасы құралдарын пайдаланушыға жадынама;

3) есептеу техникасы құралдарына, ақпараттық жүйелерге және деректер базасына қол жеткізуге мүмкіндігі бар техникалық мамандар тобын анықтау, ұйым қызметкерлерінің функционалды бекітілген міндеттерін тексеру;

4) есептеу техникасы құралдарын, ақпараттық жүйелер мен деректер базаларын басқа ұйымдарды тарта отырып техникалық қызмет көрсету, жөндеу және басқа да жұмыстар жүргізу кезінде ақпаратты қорғау жөніндегі жұмыстардың ұйымдастыру және ақиқат жағдайы;

5) рұқсатсыз қолжетімділіктен есептеу техникасы құралдарын, ақпараттық жүйелер мен деректер базаларын қорғауды қамтамасыз етуде қабылданған (бағдарламалық, техникалық, ұйымдастырушылық) шараларды талдау. Ақпараты қорғаудағы ұйымдастырушылық үдерістің өнімділігін бағалау. Ақпараты техникалық өңдеу және қорғау құралдарының жеткіліктілігі, ақпараттық қауіпсіздік талаптары жөніндегі сәйкестікті растаудың (сертификаттың) болуы;

6) ақпаратты қорғау жүйесіндегі осал жерлерді анықтау мақсатында белсенді желілік жабдықтардың, маршрутизаторлардың, коммутаторлардың, серверлердің үйлесімділігіне талдау жүргізу;

7) программалық-аппараттық құралдарды пайдалана отырып локалды-есептеу желілерінің, ақпараттық жүйелер мен деректер базаларының желілік және серверлік жабдықтарына құралдық талдау жүргізу;

8) компьютерлік шабуылдарды табу және болдырмауда қолданылатын бағдарламалық-аппараттық құралдардың жұмысқа қабілеттілігін тексеру;

9) зиян келтіретін бағдарламалар мен вирусқа қарсы лицензияланған қорғау құралдарының немесе сертификатталған еркін таратылатын вирусқа қарсы қорғау құралдарының болуын тексеру;

10) ғаламдық ақпараттық Интернет желісіне ұйым қызметкерлерінің қолжетімділігін қамтамасыз ету жөніндегі жұмыстарды ұйымдастыру, Интернет желісінен рұқсатсыз қолжетімділігінен/енуден есептеу техникасы құралдарының қорғалғандығына талдау;

11) серверлік және кроссалық бөлмелеріне бақылау қолжетімділік және өрт сөндіру, температуралық режимді қамтамасыз ету құралдарымен жабдықталғандығын тексеру, серверлік және кроссалық бөлмелерге қолжетімділік регламентінің болуы;

12) электрмен қоректендіру жүйесінің жаңылысынан (сбой) ақпараттық ресурстардың қорғалу жағдайы (резерв схемасы, резервті автоматты қосу жүйесі);

13) локалды-есептеу жүйесіндегі сызықтық-кабельдік жабдақтардың жай-күйі (құлыптау және мөрлеу керек-жарақтарының, тарату шкафтары жабдықтарының болуы)

6. Тексерілетін ұйым өз қызметкерлерінің Комиссия мүшелерінің сұрақтарына түсіндірмелер (ауызша және жазбаша түрде) ұсынуын, ақпаратқа, оның ішінде автоматтандырылған жүйелерге қолжетімділігін қамтамасыз етеді. Комиссия мүшелеріне қажетті құжаттардың көшірмелерін түсіруіне мүмкіндік береді, сондай-ақ, тексеруді комиссияның уақытылы жүргізуіне және аяқтауына көмек көрсетеді.

7. Комиссия мүшелері тексеру жүргізу кезінде ұйымнан алынған құжаттардың сақталуын және олардағы ақпараттың құпиялылығын қамтамасыз етеді.

8. Комиссияның (тексеруші) жұмысы тексеру нәтижелерінің қорытындысын шығарумен (жинақтаумен) және еркін нұсқадағы акт жасаумен аяқталады.

9. Акт мыналарды:

1) актінің жасалған күні, уақыты және орны;

2) бақылау және қадағалау органының атауы;

3) оның негізінде тексеру жүргізілген, тексеруді тағайындау туралы акті жасалған күні мен оның нөмірі;

4) тексеру жүргізген адамның (адамдардың) тегі, аты, әкесінің аты (ол болған жағдайда) және лауазымы;

5) тексерілетін субъектінің атауы немесе тегі, аты, әкесінің аты (ол болған жағдайда), тексеруді жүргізу кезінде сол жерде болған жеке немесе заңды тұлға өкілінің лауазымы;

6) тексерудің жүргізілген күні, орны және кезеңі;

7) тексерудің нәтижелері туралы, оның ішінде анықталған бұзушылықтар туралы, олардың сипаты туралы мәліметтер;

8) тексерілетін субъекті өкілінің, сондай-ақ тексеруді жүргізу кезінде қатысқан адамның актімен танысуы туралы немесе танысудан бас тартуы туралы мәліметтер, олардың қолы немесе қол қоюдан бас тартуы;

9) тексеруді жүргізген лауазымды адамның (адамдардың) қолы көрсетіледі.

10) ұйымдардың ақпараттық желілер мен ресурстардың қорғалу жай-күйін, тиісті құжаттар мен фактілерге жасай отырып табылған кемшіліктер мен бұзушылықтарды, оларды жою жөнінде нақты мерзімдерді көрсете отырып қорытындылар мен ұсыныстарды анық және дәлелді жазуды құрайды;

11) ақпараттық қауіпсіздікті қамтамасыз етуге жауапты ақпараттандыру бөлімшелерінің, және ақпараттық желілер мен ресурстардың қорғалуын қамтамасыз ету жөніндегі ұйым басшыларының тәжірибелік қызметтерін объективті көрсетеді.

Акт екі данада жасалады. Оның біріншісі тексерілетін ұйым үшін, ал екіншісі уәкілетті орган үшін.

10. Актімен ұйым басшылары және қажет болған жағдайда оларға қатысты бөлігінде олар қол қоятын немесе оған өздерінің ескертулері мен қарсылықтарын жазбаша түсіндірмелермен қосымша салып, жекелеген орындаушылар танысады.

11. Тексеру нәтижесінде табылған кемшіліктер мен бұзушылықтарды жою және ұсыныстарды іске асырғандығы туралы тексерілген ұйымның басшысы актіде белгіленген мерзімде уәкілетті органға және белгіленген (қажетті) жағдайда жоғары тұрған ұйымға хабарлайды.