

Дәріс 4. Мемлекеттік құпияға қатысты негізгі нормативтік басқару құжаттары, нормативтік анықтамалық құжаттар

Жоспары:

- 1 Мемлекеттік құпиялар туралы заңда пайдаланылатын негізгі ұғымдар
- 2 Қазақстан Республикасының мемлекеттік құпиялар туралы заңдары
- 3 Қазақстан Республикасы Президентінің, Қазақстан Республикасы Парламентінің, Үкіметінің, мемлекеттік органдары мен ұйымдарының мемлекеттік құпияларды қорғау саласындағы өкілеттігі
- 4 Қазақстан Республикасының ақпараттық қауіпсіздігінің жай-күйі
- 5 Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелерде ақпараттық қауіпсіздікті қамтамасыз ету

Мемлекеттік құпиялар туралы заңда пайдаланылатын негізгі ұғымдар:

мемлекеттік құпиялар - таратылуын мемлекет жалпы қабылданған халықаралық құқық нормаларына қайшы келмейтін әскери, экономикалық, ғылыми-техникалық, сыртқы экономикалық, сыртқы саяси, барлаушылық, қарсы барлаушылық, жедел-ізвестірушілік және өзге де қызметті тиімді жүзеге асыру мақсатымен шектейтін, мемлекет қорғайтын мемлекеттік және қызметтік құпияларды құрайтын мәліметтер;

мемлекеттік құпияларға жатқызылған, қорғалып орындалған ақпараттық жүйе – мемлекеттік құпияларды қамтитын ақпаратты жасауға, іздеуге, жинауға, өңдеуге, жинақтауға, сақтауға, таратуға, бейнелеуге, пайдалануға және тұтынуға арналған, қолжетімділігі шектелген ақпараттық жүйе;

мемлекеттік құпияларды құрайтын мәліметтерді қамтитын электрондық ақпараттық ресурс – электрондық-цифрлық нысанда берілген және электрондық жеткізгіште, мемлекеттік құпияларға жатқызылған, қорғалып орындалған ақпараттық жүйелерде қамтылған ақпарат;

мемлекеттік құпия - жарияланған немесе жоғалған жағдайда Қазақстан Республикасының ұлттық қауіпсіздігіне нұқсан келтіретін немесе нұқсан келтіруі мүмкін әскери, экономикалық, саяси және өзге де сипаттағы мәліметтер;

қызметтік құпия - мемлекеттік құпияның құрамына кіруі мүмкін, жарияланған немесе жоғалған жағдайда мемлекеттің ұлттық мүдделеріне, Қазақстан Республикасы мемлекеттік органдары мен ұйымдарының мүдделеріне нұқсан келтіруі мүмкін жекелеген деректер сипаты бар мәліметтер;

құпиялылық белгісі - беру көзінің өзінде және (немесе) оған ілеспе құжаттамада көрсетілетін, беру көздерінде қамтылған мәліметтердің құпиялылық дәрежесін куәландыратын деректемелер;

мемлекеттік құпиялар болып табылатын мәліметтерге рұқсат ету - өкілетті лауазымды адамның рұқсатымен нақты адамды мемлекеттік құпиялар болып табылатын мәліметтермен таныстыру;

мемлекеттік құпияларға рұқсат ету - азаматтарға мемлекеттік құпиялар болып табылатын мәліметтерге рұқсат етілу, ал ұйымдарға - осындай мәліметтерді пайдалану арқылы жұмыс жүргізу құқығын ресімдеу рәсімі;

мәліметтер мен олардың көздерін құпияландыру - мемлекеттің ұлттық қауіпсіздігін қамтамасыз ету мүдделерін көздеп, мемлекеттік құпиялар болып табылатын мәліметтер таратуды және олардың көздеріне рұқсат етуді шектеу жөніндегі шаралардың жиынтығы;

мемлекеттік құпиялар болып табылатын мәліметтер көздері - мемлекеттік құпиялар болып табылатын мәлімет нышандар, үлгілер, белгілер, техникалық шешімдер және процестер түрінде өз көрінісін табатын материалдық объектілер, оның ішінде физикалық өрістер;

мәліметтерді құпиясыздандыру - мемлекеттің ұлттық қауіпсіздігі мүдделерін көздеп, мемлекеттік құпиялар болып табылатын мәліметтерді таратуға және олардың көздеріне рұқсат етуге белгіленген шектеулерді алып тастау жөніндегі шаралардың жиынтығы;

мемлекеттік құпияларды қорғау жүйесі - мемлекеттік құпияларды қорғау органдарының, олардың мемлекеттік құпиялар болып табылатын мәліметтерді және солардың көздерін қорғауда пайдаланатын құралдары мен әдістерінің, сондай-ақ осы мақсатта жүргізілетін шаралардың жиынтығы;

мемлекеттік құпиялар болып табылатын мәліметтерді қорғау құралдары - мемлекеттік құпиялар болып табылатын мәліметтерді қорғауға арналған техникалық, криптографиялық, бағдарламалық және басқа да құралдар, олар іске асырылған құралдар, сондай-ақ мемлекеттік құпияларды қорғаудың тиімділігіне бақылау жасау құралдары;

мемлекеттік құпияларды жария ету - мемлекеттік құпияларды олармен танысуға құқық берілмеген заңды және жеке тұлғаларға хабарлау, беру, табыс ету, жіберу, жариялау немесе кез-келген басқа әдістермен жеткізу;

мемлекеттік құпияларды жоғалту - мемлекеттік құпиялар болып табылатын мәліметтердің жоғалтылуы не ұрлануы салдарынан заңды иеленуден немесе пайдаланудан шығып қалуы, соның ішінде уақытша да шығып қалуы. Қазақстан Республикасының мемлекеттік құпиялар туралы заңдары Қазақстан Республикасының Конституциясына, Қазақстан Республикасы бекіткен халықаралық шарттарға негізделеді және осы Заңнан және Қазақстан Республикасының мемлекеттік құпияларды қорғау саласындағы қатынастарды реттейтін өзге де нормативтік құқықтық актілерінен тұрады.

2-1-бап. Мемлекеттік құпияларды қорғаудың мақсаты мен міндеттері

1. Мемлекеттік құпияларды қорғаудың мақсаты оларды жария ету және жоғалту қаупінен қорғауды қамтамасыз ету болып табылады.

2. Мемлекеттік құпияларды қорғаудың міндеттері мыналар болып табылады:

1) Қазақстан Республикасының ұлттық қауіпсіздігін қамтамасыз ету мақсатында мемлекеттік құпияларды қорғау жүйесін дамыту;

2) мәліметтерді мемлекеттік құпияларға жатқызуға, оларды құпияландыруға, оларға билік етуге, оларды қорғау мен құпиясыздандыруға байланысты туындайтын қоғамдық қатынастарды реттеу;

3) таратылуын шектеу Қазақстан Республикасының ұлттық қауіпсіздік мүдделеріне негізделген, құпияландыруға жататын мәліметтер тізбесін айқындау;

4) мемлекеттік құпияларды құрайтын мәліметтер пайдаланылатын жұмысқа жіберілетін адамдар тобын айқындау;

5) мемлекеттік құпияларды қорғау әдістері мен құралдарын әзірлеу, ендіру, қолдану және жетілдіру.

Ескерту. 2-1-баппен толықтырылды – ҚР 23.12.2023 № 51-VIII (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) Заңымен.

3-бап. Қазақстан Республикасының мемлекеттік құпиялары мен олардың көздеріне меншік құқығы

Мемлекеттік құпиялар мен мемлекеттік құпия болып табылатын мәліметтердің көздері Қазақстан Республикасының меншігі болып табылады.

4-бап. Мемлекеттік құпияларды қорғау органдары

1. Мемлекеттік құпияларды қорғау органдарына:

Қазақстан Республикасының мемлекеттік құпияларын қорғау жөніндегі уәкілетті мемлекеттік органы;

Қазақстан Республикасының Ұлттық қауіпсіздік комитеті мен оның органдары;

мемлекеттік органдар мен ұйымдар, олардың мемлекеттік құпияларды қорғау жөніндегі құрылымдық бөлімшелері жатады.

2. Мемлекеттік құпияларды қорғау органдары өздеріне жүктелген міндеттерге сәйкес және өз құзыреттері шегінде мемлекеттік құпиялар болып табылатын мәліметтердің қорғалуын қамтамасыз етеді. Мемлекеттік органдар мен ұйымдарда мемлекеттік құпиялар болып табылатын мәліметтердің қорғалуын ұйымдастыру үшін жауапкершілік олардың басшыларына жүктеледі. Мемлекеттік органдар мен ұйымдардың басшылары мемлекеттік құпиялар болып табылатын мәліметтер пайдаланылатын жұмыстардың көлеміне қарай міндеттері Қазақстан Республикасының Үкіметі бекітетін нормативтік құқықтық актілерге сәйкес және олар жүргізетін жұмыстардың ерекшеліктерін ескере отырып, аталған басшылар белгілейтін мемлекеттік құпияларды қорғау жөнінде құрылымдық бөлімшелер құрады.

3. Мемлекеттік құпияларды қорғау мемлекеттік орган мен ұйымның негізгі қызметінің бір түрі болып табылады

Қазіргі уақытта Қазақстанның саяси өміріндегі және экономикасындағы болып жатқан қайта құру процестері оның ақпараттық қауіпсіздігінің жай-күйіне тікелей әсерін тигізеді. Бұл ретте ақпараттық қауіпсіздіктің нақты жай-күйін

бағалау және осы саладағы негізгі проблемалар мен бағыттарды айқындау кезінде ескеруді қажет ететін жаңа факторлар туындайды.

Көрсетілген факторларды саяси, экономикалық және ұйымдастырушылық-техникалық деп бөлуге болады.

Саяси факторлар:

әлемнің түрлі өңірлерінде геосаяси жағдайдың өзгеруі;

әлемдік саяси, экономикалық, әскери, экологиялық және басқа да процестердің жаһандық мониторингін жүзеге асыратын, ақпаратты біртарапты артықшылықтар алу мақсатында тарататын әлемнің дамыған елдерінің ақпараттық өктемдігі;

демократия, заңдылық, ақпараттық ашықтық, елдің қауіпсіздігін қамтамасыз ету жүйесін жетілдіру принциптері негізінде жаңа Қазақстан мемлекеттілігінің қалыптасуы;

ішкі саяси дағдарыстардың туындауы: билік тармақтары арасындағы, аумақтық мемлекеттік құрылым субъектілері арасындағы жанжалдар, қорғалатын тұлғаларға қастандық жасалуы;

ішкі саяси блоктардың, одақтардың, альянстардың қызметі, әлемде күштердің геосаяси орналасуына әсер ететін жаңа әскери-саяси бірлестіктердің құрылуы;

реформалар жүргізу процесінде Қазақстанның шетелдермен неғұрлым тығыз ынтымақтастық жасауға ұмтылуы;

терроризм және экстремизм, криминогенді жағдайдың ушығуы, әсіресе кредит-қаржы саласында компьютерлік қылмыстар санының өсуі болып табылады.

Экономикалық факторлар арасында:

Қазақстанның дүниежүзілік экономикалық кеңістікке белсенді кіруі, көптеген отандық және шетелдік мемлекеттік емес құрылымдардың - ақпаратты өндірушілер мен тұтынушылардың, ақпараттандыру және ақпаратты қорғау құралдарының пайда болуы, ақпараттық өнімнің тауарлық қатынастар жүйесіне қосылуы;

Қазақстанның ақпараттық инфрақұрылымын дамыту мүддесінде шетелдермен кеңейіп келе жатқан кооперация;

бүкіл әлемдегі экономикалық процестердің дамуына өспелі әсерін тигізетін коммуникациялық жаһандану;

қазіргі әлемде экономикалық-технологиялық даму деңгейін барынша жоғары дәрежеде айқындайтын жаңа ақпараттық технологияларды дамыту мен енгізуде Қазақстанның артта қалуы неғұрлым елеулі болып табылады.

Ұйымдастырушылық-техникалық факторлардың ішінен мыналар айқындаушы болып табылады:

ақпараттық қатынастар саласында, оның ішінде ақпараттық қауіпсіздікті қамтамасыз ету саласында, нормативтік құқықтық базаның жеткіліксіздігі;

мемлекеттің Қазақстандағы ақпараттандыру құралдары, ақпараттық өнімдер мен қызмет көрсетулер нарығының жұмыс істеу және даму процестерін нашар реттеуі;

ақпаратты сақтау, өңдеу, беру және қорғау үшін мемлекеттік басқару саласында, кредит-қаржы және басқа салаларда ақпараттың сыртқа шығып кетуінен және сыртқы әсерден қорғалмаған импорттық техникалық және бағдарламалық құралдардың кеңінен пайдаланылуы;

ашық байланыс арналары және деректер беру жүйелері бойынша берілетін ақпараттар көлемінің өсуі.

Қазақстандағы ақпараттық қауіпсіздіктің қазіргі жай-күйін талдау оның қазіргі заманғы деңгейінің адам, қоғам және мемлекет қажеттіліктеріне сәйкес келмейтінін көрсетті.

Елдің саяси және әлеуметтік-экономикалық дамуының бүгінгі жағдайы ақпаратпен еркін алмасуды кеңейтудегі қоғам қажеттілігі мен оны таратуға жекелеген шектеулерді сақтау қажеттілігі арасында қайшылықтардың шиеленісуін тудырады.

Мемлекеттік органдарды толық, сенімді және қазіргі заманғы ақпаратпен қамтамасыз ету үшін негізделген, оның ішінде мемлекеттік ақпараттық ресурстарды қорғауға арналған шешімдер қабылдау, сондай-ақ отандық ақпаратты қорғау құралдарын және импортталатын техникалық құралдардың белгіленген талаптарға сәйкестігін растау жүйелерін әзірлеу талап етіледі.

Ақпаратты қорғау саласында кәсіби мамандар сандарының жеткіліксіздігі республикада ақпараттық қауіпсіздікті ұйымдастыруға кері әсерін тигізеді.

Техникалық барлауларға қарсы іс-әрекеттер, ақпараттық қарудан қорғау мен осы саладағы нормативтік құқықтық базаны жетілдіру мәселелерін одан әрі пысықтау талап етіледі.

Осы мақсаттарда ақпараттың тұтастығы мен құпиялығын қамтамасыз ету үшін ақпаратты жалпымемлекеттік ауқымда және ведомстволық деңгейде қорғау жөніндегі іс-шараларды кешенді үйлестіру қажет.

Ақпараттық кеңістікте Интернеттің ролінің өсуімен адамның және қоғамның құқықтары мен бостандықтарын зорлық жасау мен қатыгездікті насихаттайтын ақпараттан, оларға өтірік және жалған ақпаратты таңудан, болашақ ұрпақтың мақсатты бағытталған теріс дүниетанымын қалыптастырудан қорғау қажеттілігі туындайды. Бұл ретте, сыртқы қатер көздері Қазақстан Республикасының заңнамалық құзырынан тыс болуы мүмкін, бұл құқық шаралары жүйесін қолдануды елеулі қиындатады.

Отандық ақпараттық технологиялардың болмауы өзекті проблема болып табылады, бұл жаппай пайдаланушыларды ақпараттық қауіпсіздік талаптары бойынша сәйкестігі расталмаған импорттық техниканы сатып алуға мәжбүр етеді. Бұл деректер базалары мен банктерінің ақпараттық қауіпсіздігіне қатер, сондай-ақ елдің шетелдік компьютер мен телекоммуникация техникасын және ақпарат өнімдерін өндірушілерге ықтимал тәуелділігін тудырады.

Ақпарат саласындағы құқық қатынастарының субъектілері меншік нысанына қарамастан жеке және заңды тұлғалар болып табылады.

Ақпараттың меншік иелері: мемлекет (мемлекеттік органдар мен ұйымдар, лауазымды тұлғалар тұрғысында), жеке және заңды тұлғалар болып табылады.

Ақпараттық қатынастар субъектілері ақпаратты жасау және пайдалану тұрғысынан авторлар, меншік иелері, иеленушілер немесе пайдаланушылар ретінде болуы мүмкін.

Ақпарат және ақпараттық ресурстар заттай меншік немесе зияткерлік меншік бола алады. Сондықтан ақпараттық жүйелерде ақпаратты өңдеу кезінде ақпараттың құпиялығын қамтамасыз ету ғана емес, оның тұтастығы мен қол жетімділігін, ал электрондық құжаттар үшін әрбір электрондық құжаттың авторлығын электрондық цифрлы қолтаңбамен растау талап етіледі.

Мемлекеттік құпияларды құрайтын мәліметтерді қамтитын ақпаратқа қатысты барлық қатынас субъектілері үшін белгіленген құпиялық режимі жұмыс істейді. Осы ақпараттың меншік иесі мемлекет болып табылады.

Мемлекет меншік иесі болып табылатын қол жеткізу шектелген ақпаратты қорғауды қамтамасыз ету үшін мемлекеттік ақпаратты қорғау жүйесі жұмыс істейді.

Қазіргі заманғы қоғамының табысты жұмыс істеуі онда болып жатқан ақпараттық процестердің қаншалықты тиімді ұйымдастырылғанына және жолға қойылғанына тұтастай байланысты. Осыған байланысты Қазақстан Республикасы үшін аталған процестердің мемлекет шеңберінде ақпараттық кеңістікке бірлесуі барған сайын маңызды бола түсуде.

Бірыңғай ақпараттық кеңістік жеке және заңды тұлғалардың ақпараттық қажеттіліктерін қанағаттандыруды қамтамасыз етуге мүмкіндік береді, ақпаратты өндірушілер мен тұтынушылар қызметін ынталандыруға, елдің әлемдік ақпараттық кеңістікке кіруіне жәрдем ететін болады.

Бірыңғай ақпараттық кеңістікті қалыптастыру барысында құрылуы Қазақстан Республикасы Президентінің 2004 жылғы 10 қарашадағы N 1471 Жарлығымен бекітілген Қазақстан Республикасында "электрондық үкімет" қалыптастырудың 2005-2007 жылдарға арналған мемлекеттік бағдарламасымен көзделген "электрондық үкіметтің" рөлі өсе түсуде. "Электрондық үкімет" барлық билік тармақтарының қызметін ақпараттық қолдау мен олардың арасындағы, сондай-ақ экономика субъектілерімен және халықпен арадағы ақпараттық өзара іс-қимылды серпінді ұйымдастыру есебінен олардың жұмыс істеу тиімділігін елеулі түрде көтеруге мүмкіндік береді.

Қазақстан Республикасында "электрондық үкімет" қалыптастырудың 2005-2007 жылдарға арналған мемлекеттік бағдарламасы шеңберінде "Жеке тұлғалар", "Заңды тұлғалар", "Жылжымайтын мүлік тіркелімі", "Мекенжай тіркелімі" мемлекеттік деректер базасы құрылуда, олардың қауіпсіздігі ақпараттық қатынастар субъектілері арасындағы қорғалған ақпараттық өзара іс-қимыл нәтижесінде қамтамасыз етілетін болады.

Жалпы мемлекеттік ақпараттық және телекоммуникациялық жүйелерде ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері:

мемлекеттік және нарықтық басқарудың ақпараттық жүйелері және құжатталған ақпараттық массивтер мен дерекқорлар түрінде ұсынылған мемлекеттік құпияларға жататын мәліметтерді және жабық ақпаратты қамтитын ақпараттық ресурстар;

ақпараттандыру құралдары мен жүйелері (есептегіш техника құралдары, ақпараттық-есептеу кешендері, желілер мен жүйелер), бағдарламалық құралдар (операциялық жүйелер, дерекқорларды басқару жүйелері, басқа да жалпыжүйелік және қолданбалы бағдарламалық қамтамасыз ету), автоматтандырылған басқару жүйелері, байланыс және деректер беру жүйелері, қолжетімділігі шектеулі ақпаратты өңдеу үшін пайдаланылатын ақпарат қабылдаудың, берудің және өңдеудің техникалық құралдары, олардың ақпараттық физикалық өрістері;

ақпарат өңдемейтін, алайда мемлекеттік құпияларға жатқызылған мәліметтері бар ақпарат өңдейтін үй-жайларға орнатылатын техникалық құралдар мен жүйелер, сондай-ақ құпия келіссөздер мен құпия жұмыстар жүргізуге бөлінген үй-жайлар;

мемлекеттік құпияны құрайтын мәліметтерді қамтитын мемлекеттік ақпараттық ресурстар;

әскери іс-қимылдарды дайындау мен жүргізудің жедел және стратегиялық жоспарлары туралы, олардың сандық және кадрлық құрамы, қызметінің бағыттары, жұмылдыру дайындығы, байланыс және әскерлер мен қару-жарақты басқару жүйелері туралы мәліметтерді қамтитын әскери басқару, ұлттық қауіпсіздік, ішкі істер органдарының ақпараттық ресурстары, олардың ақпараттық қамтамасыз етілуі, олардың ақпараттық инфрақұрылымы;

режимдік және стратегиялық объектілер, қолжетімділігі шектеулі ақпарат өңделетін есептегіш техника құралдарының объектілері;

"электрондық үкіметтің" ақпараттық инфрақұрылымы болып табылады.

Жалпы мемлекеттік ақпараттық және телекоммуникациялық жүйелерде ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттары:

мемлекеттік басқару органдарының ақпараттық жүйелерінің іркіліссіз жұмыс істеуін қамтамасыз ету;

ақпаратты техникалық барлау құралдарынан арнайы қорғау;

техникалық құралдарда өңделетін немесе сақталатын ақпаратқа рұқсатсыз қолжетімділікті болдырмау;

есептегіш техника құралдарының объектілерінде жанама электромагнит сәулелері мен нысаналар есебінен өңделетін ақпараттың сыртқа шығып кетуінің алдын алу;

ақпараттандыру құралдары жұмысында ақпараттың бұзылуын, жойылуын, бұрмалануын немесе іркілісін тудыратын бағдарламалық-техникалық әсер етудің алдын алу;

объектілерге және техникалық құралдарға енгізілген электрондық ақпарат қармау қондырғыларын (салынған қондырғыларды) анықтау;

үй-жайлардан және объектілерден сөз түріндегі ақпаратты техникалық құралдармен қармаудың алдын алу болып табылады.

Байланыс арналары бойынша берілетін ақпаратты техникалық құралдардың көмегімен қармаудың алдын алуға криптографиялық және өзге әдістер мен қорғау құралдарын қолданумен, сондай-ақ қажетті ұйымдастырушылық-техникалық іс-шаралар жүргізумен қол жеткізіледі.

Берілетін, өңделетін немесе техникалық құралдарда сақталатын ақпаратқа рұқсат етілмеген қолжетімділікті және әсер етуді болдырмауға арнайы бағдарламалық-техникалық қорғау құралдарын қолданумен, криптографиялық қорғау тәсілдерін пайдаланумен, сондай-ақ ұйымдастырушылық және режимдік іс-шаралармен қол жеткізіледі.

Жанама электромагнит сәулелері мен нысаналар, сондай-ақ электроакустикалық өзгеру есебінен өңделетін ақпараттың сыртқа шығып кетуін болдырмауға қорғалған техникалық құралдарды, техникалық қорғау құралдарын, оның ішінде ақпаратты криптографиялық қорғау құралдарын, белсенді қорғау құралдарын қолданумен, объектілерді экрандаумен, қорғау объектілерінің айналасына бақыланатын (тексерілетін) аймақты жасаумен және басқа ұйымдастырушылық және техникалық шаралармен қол жеткізіледі.

Ақпараттың бұзылуын, жойылуын, бұрмалануын немесе ақпараттандыру құралдары жұмысында іркіліс тудыратын бағдарламалық-техникалық әсердің алдын алуға лицензиялық бағдарламалық қамтамасыз етуді, арнайы бағдарламалық және аппараттық қорғау құралдарын (вирускқа қарсы процессорлар, вирускқа қарсы бағдарламалар) қолданумен, бағдарламалық қамтамасыз ету қауіпсіздігін бақылау жүйесін ұйымдастырумен қол жеткізіледі.

Объектілерге және техникалық құралдарға енгізілген электрондық ақпарат қармау қондырғыларын (салынған қондырғыларды) анықтауға арнайы зерттеулер жүргізумен қол жеткізіледі.

Үй-жайлардан және объектілерден сөз түріндегі ақпарат техникалық құралдармен қармаудың алдын алуға техникалық қорғау құралдарын, үй-жайлардың дыбыс өткізбеуін қамтамасыз ететін жобалау және конструкторлық шешімдерді, орнатылған қармау құралдарын анықтау мен олардың белсенділігін азайту бойынша режимді үй-жайларды арнайы тексеру мен басқа да ұйымдастыру әрі режимдік іс-шаралар жүргізу есебінен қол жеткізіледі.

Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелерде ақпарат қорғау жөніндегі негізгі ұйымдастырушылық-техникалық іс-шаралар мыналар болып табылады:

ақпаратты техникалық қорғау саласындағы ұйымдардың қызметін лицензиялау;

жеке және заңды тұлғалардың мемлекеттік құпияларға жіберу мен қол жеткізуіне рұқсат ету жүйесін құру;

ақпараттық қауіпсіздікті қамтамасыз ету талаптарын орындау жөніндегі ақпараттандыру объектілерін аттестаттау;

ақпарат қорғау мен оның тиімділігін бақылау техникалық құралдарының, ақпараттандыру және байланыс құралдарының ақпараттық қауіпсіздік талаптарына сәйкестігін растау;

қорғалып орындалған ақпараттық және автоматтандырылған басқару жүйелерін құру және қолдану;

ақпарат қорғаудың техникалық құралдарын және оның тиімділігін бақылау әдістерін әзірлеу және пайдалану;

қорғау әдістерін, техникалық шараларды және техникалық құралдарды, оның ішінде байланыс арналары бойынша берілетін ақпаратты ұстап қалуды болдырмайтын ақпаратты криптографиялық қорғау құралдарын қолдану;

ақпаратты ақпараттық-телекоммуникация жүйелерінде және жергілікті есептегіш желілерінде рұқсат етілмеген қолжетімділіктен және әсер етуден, компьютерлік вирустардың жұғуынан қорғауды ұйымдастыру;

есептегіш техника құралдары объектілерінде жанама электромагнит сәулелері мен нысаналар есебінен өңделетін ақпараттың сыртқа шығып кетуінің алдын алу жөнінде шаралар әзірлеу;

сенімді қорғауды қамтамасыз ету және объектінің қорғалатын аймағына рұқсатсыз кіру фактілерін анықтау үшін кіріктірілген күзет жүйелерін, бейнебақылауды ақпарат жинау мен өңдеуді кешенді қолдана отырып, бірнеше күзет шептерін көздейтін объектілерді күзету жүйелерінің жұмыс істеуін қамтамасыз ету жөніндегі ұйымдастыру және инженерлік-техникалық шараларды іске асыруды қамтитын іс-шаралар жүргізу;

жанама электромагнит сәулелері мен нысаналар есебінен ақпараттың сыртқа шығып кетуінен объектілердің қорғалғандығының тиімділігіне бақылау жүргізу;

объектілерге және техникалық құралдарға енгізілген электрондық ақпарат қармау қондырғыларын (салынған қондырғыларды) анықтау жөнінде режимдік үй-жайларды арнайы тексеру;

жергілікті есептегіш желілердің ақпаратқа рұқсат етілмеген қолжетімділіктен қорғалғандығының тиімділігіне бақылау жүргізу;

ақпараттық қауіпсіздікті қамтамасыз ету саласында ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстар ұйымдастыру, үйлестіру және қаржыландыру;

ақпараттық қауіпсіздікті қамтамасыз ету және арнайы мақсаттағы телекоммуникация желілерін жетілдіру саласында перспективалық дамуға қол жеткізу мақсатында техникалық шешімдер әзірлеу;

ақпараттық қауіпсіздік қатерлерінің көздерін анықтау, бағалау және болжамдау, техникалық барлау құралдарына қарсы іс-әрекет етудің барабар шараларын жедел қабылдау;

техникалық барлаулар, олардың ниеті, мүмкіндіктері, олардың жұмыс істеу әдістері мен техникалық жарақтануы туралы ақпаратты жинау;

ақпараттық қауіпсіздік саласында қылмыспен күрес проблемалары бойынша тәжірибе алмасуға бағытталған мемлекеттер арасында жасалған келіссөздер шеңберіндегі мемлекетаралық ынтымақтастықты кеңейту;

Қазақстан Республикасына қарсы ақпараттық қатер көздерінің қолға алғалы жатқан іс-әрекеттері туралы ақпарат алуға бағытталған қарсы барлау іс-шаралары;

ақпараттық қауіпсіздікті қамтамасыз ету саласында мамандар даярлаудың оқу-әдістемелік және материалдық базасын құру;

құпиялық режимін және ақпарат қорғауды қамтамасыз ету, мемлекеттік органдар мен ұйымдардың жеке қауіпсіздігін нығайту.

Ақпарат қорғаудың әдістері, тәсілдері және шаралары ақпарат сыртқа шығып кеткен, бұзылған немесе жойылған жағдайлардағы ықтимал залалдың дәрежесіне байланысты әзірленеді.

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов/ С. А. Нестеров. - Санкт-Петербург : Лань, 2021., 324 с. — ISBN 978-5-8114-6738-9.

2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3

4. <https://adilet.zan.kz/kaz/docs/Z990000349>

Қосымша әдебиеттер:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534- 07248-8

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0