Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы

Күшін жойған

Қазақстан Республикасы Президентінің 2006 жылғы 10 қазандағы N 199 Жарлығы. Күші жойылды - Қазақстан Республикасы Президентінің 2011 жылғы 11 сәуірдегі № 5 Жарлығымен

Ескерту. Күші жойылды - ҚР Президентінің 2011.04.11 № 5 Жарлығымен.

"Президент пен Үкімет актілерінің жинағында" жариялануға тиіс

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету мақсатында **ҚАУЛЫ ЕТЕМІН:**

1. Қоса беріліп отырған Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы мақұлдансын.

2. Қазақстан Республикасының мемлекеттік органдары мен ұйымдары өз қызметінде осы тұжырымдаманың ережелерін басшылыққа алсын.

3. Осы Жарлық қол қойылған күнінен бастап қолданысқа енгізіледі.

Қазақстан Республикасының Президенті

Қазақстан Республикасы
Президентінің
2006 жылғы 10 қазандағы
N 199 Жарлығымен
МАҚҰЛДАНҒАН

Қазақстан Республикасының ақпараттық қауіпсіздік ТҰЖЫРЫМДАМАСЫ

Кіріспе

Ел Президентінің 1997 жылғы 10 қазандағы "Қазақстан - 2030. Барлық қазақстандықтардың өсіп-өркендеуі, қауіпсіздігі және әл-ауқатының артуы" атты Қазақстан халқына Жолдауында ұзақ мерзімді басымдық ретінде ұлттық қауіпсіздік айқындалды, оның құрамының бірі ақпараттық қауіпсіздік болып табылады.

Қоғам мен мемлекеттің әлеуметтік-экономикалық және мәдени өміріндегі ақпараттық технологиялардың даму серпіні ақпараттық қауіпсіздік мәселелерін

шешуге жоғары талаптар қояды.

Мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету ақпарат алу саласында адамның және азаматтың конституциялық құқықтары мен бостандықтарын іске асыруға қабілетті ұйымдастырушылық, техникалық, бағдарламалық, әлеуметтік тетіктерді қамтитын кешенді көзқарасты пайдалануды, оны конституциялық құрылыстың мызғымастығын, Қазақстан Республикасының егемендігі мен аумақтық тұтастығын, саяси, экономикалық және әлеуметтік тұрақтылықты, заңдылық пен құқықтық тәртіпті қорғау мақсатында пайдалануды, ақпараттық қауіпсіздік саласында өзара тиімді халықаралық ынтымақтастықты дамытуды талап етеді.

1. Жалпы ережелер

Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы (бұдан әрі - Тұжырымдама) Қазақстан Республикасы Конституциясының және " Қазақстан Республикасының Ұлттық қауіпсіздігі туралы" 1998 жылғы 26 маусымдағы, "Мемлекеттік құпиялар туралы" 1999 жылғы 15 наурыздағы, " Терроризмге қарсы күрес туралы" 1999 жылғы 13 шілдедегі, "Электрондық құжат және электрондық цифрлық қолтаңба туралы" 2003 жылғы 7 қаңтардағы, " Ақпараттандыру туралы" 2003 жылғы 8 мамырдағы, "Экстремизмге қарсы іс-қимыл туралы" 2005 жылғы 18 ақпандағы Қазақстан Республикасы заңдарының, Қазақстан Республикасы Президентінің 2006 жылғы 18 тамыздағы N 163 Жарлығымен мақұлданған Қазақстан Республикасы ақпараттық кеңістігінің бәсекеге қабілеттілігін дамытудың 2006-2009 жылдарға арналған тұжырымдамасының негізінде әзірленді.

Сондай-ақ Тұжырымдаманы әзірлеу кезінде ақпараттық қауіпсіздік саласындағы халықаралық тәжірибе және 1999 жылғы 4 шілдедегі Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің әскери саладағы ақпараттық қауіпсіздік тұжырымдамасының ережелері ескерілді.

Тұжырымдама ақпараттық қауіпсіздікті қамтамасыз ету саласында Қазақстан Республикасының бірыңғай мемлекеттік саясатын қалыптастыру мен іске асыру кезінде негіз болып қызмет етеді, оның ережелері Қазақстанның бірыңғай ақпараттық кеңістігін құру мен дамыту және ақпараттандыру саласында мемлекеттік саясатты одан әрі жетілдіру кезінде ескерілетін болады.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету саласындағы мемлекеттік саясат (бұдан әрі - мемлекеттік саясат) ашық болып табылады және Қазақстан Республикасының қолданыстағы заңнамалық актілерінде көзделген шектеулерді ескере отырып, қоғамның мемлекеттік органдар мен қоғамдық институттардың ақпараттық қауіпсіздік саласындағы

қызметі туралы хабардар болуын көздейді. Ол жеке және заңды тұлғалардың кез келген заңды тәсілмен ақпаратты еркін жасауға, іздестіруге, алуға және таратуға құқықтарын қамтамасыз етуге негізделеді.

Мемлекет ақпараттық ресурстар меншік объектісі болып табылатынын, және ақпараттық ресурстардың меншік иелерінің, иелерінің және өкімдік етушілерінің заңды мүдделері сақталған жағдайда оларды шаруашылық айналымға енгізуге ықпал ететінін негізге алады.

Мемлекет ұлттық телекоммуникациялық желілер құруды және халықаралық ақпарат алмасуды қамтамасыз етуге қабілетті қазіргі заманғы ақпараттық және телекоммуникациялық технологияларды және техникалық құралдарды дамытуды басым деп санайды.

Мемлекеттік саясат, мемлекеттік құпияларды қорғау саласын қоспағанда, мемлекеттік органдар мен ұйымдардың ақпараттық қауіпсіздікті қамтамасыз ету саласындағы монополиясына жол бермейді.

2. Қазақстан Республикасының ақпараттық қауіпсіздігінің жай-күйі

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.

3. Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен міндеттері

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі мақсаттары:

ақпарат қорғаудың ұлттық жүйесін, оның ішінде мемлекеттік ақпараттық ресурстарды құру және нығайту;

мемлекеттік ақпараттық ресурстарды, сондай-ақ ақпарат саласында адам құқықтары мен қоғам мүдделерін қорғау;

Қазақстанның ақпараттық тәуелділігін, басқа мемлекеттер тарапынан ақпараттық өктемдікті немесе тосқауылды, Президенттің, Парламенттің,

Үкіметтің және басқа да мемлекеттік органдар мен ұйымдардың ақпараттық оқшауланuын төмендету немесе оған жол бермеу болып табылады.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі негізгі міндеттер:

ақпараттық қауіпсіздік саласында ұлттық заңнаманы жетілдіру;

ақпараттық қауіпсіздік қатерлерінің көздерін анықтау, бағалау, болжау, қорғалатын объектілердің барлауға қолжетімділік өлшемдерін айқындау;

ақпараттық қауіпсіздіктің мемлекеттік саясатын қамтамасыз етудің, іс-шаралар кешенін және оларды іске асыру әдістерін әзірлеу;

ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік органдар мен ұйымдардың қызметін құқықтық реттеу және үйлестіру;

ақпараттық қауіпсіздікті қамтамасыз ету жүйесін дамыту, оны ұйымдастыруды, нысандарын, әдістерін және ақпараттық қауіпсіздік қатерлерін бейтараптау құралдарын, оны бұзу зардаптарын жоюды жетілдіру;

Қазақстанның жаһандық ақпараттық желілер мен жүйелерді құру және пайдалану процестеріне белсенді қатысуын қамтамасыз ету;

техникалық барлауларға қарсы іс-әрекет ету жөніндегі нормативтік құқықтық және әдістемелік базаны әзірлеу және жетілдіру жолымен техникалық барлауларға қарсы іс-қимыл жасау жүйесін құру болып табылады.

4. Ақпараттық қауіпсіздікті қамтамасыз ету объектілері, қатерлері, әдістері, құралдары және негізгі бағыттары

Қазақстан Республикасының ақпараттық қауіпсіздік объектілеріне:

жеке және заңды тұлғалардың, мемлекеттің ақпарат алуға, таратуға және пайдалануға, құпия ақпаратты және зияткерлік меншікті қорғауға арналған құқықтары;

сақтау нысандарына байланыссыз, мемлекеттік құпияларды, коммерциялық құпияны және басқа құпия ақпаратты, сондай-ақ ашық (жалпыға қолжетімді) ақпаратты қамтитын мәліметтері бар ақпараттық ресурстар;

әртүрлі сыныптағы және мақсаттағы ақпараттық жүйелерді, кітапханаларды, мұрағаттарды, деректер қорлары мен банктерін, ақпараттық технологияларды, ақпарат жинау, өңдеу, сақтау және беру регламенттері мен рәсімдерін, ғылыми-техникалық және қызмет көрсететін персоналды қамтитын ақпараттық ресурстарды қалыптастыру, сақтау, тарату және пайдалану жүйесі;

бұқаралық ақпарат және насихат құралдарына негізделетін қоғамдық сананы (дүниетаным, саяси көзқарастар, моралдық құндылықтар және өзгелер) қалыптастыру жүйесі;

арнайы мақсаттағы телекоммуникация желілері, сондай-ақ байланыстың

спутниктік жүйелері;

жаңалықтар, патенттелмеген технологиялар, математикалық және технологиялық алгоритмдер, өнеркәсіп үлгілері, пайдалы моделдер мен эксперименттік жабдық;

күрделі зерттеу кешендерін басқару жүйелері (ядролық реакторлар, қарапайым бөлшектерді жеделдетушілер, ғарыш кешендері және тағы басқалар);

ақпараттандыру құралдары мен жүйелері (есептегіш техника құралдары, ақпараттық-есептеу кешендері, желілері мен жүйелері), бағдарламалық құралдар (операциялық жүйелер, дерекқорларды басқару жүйелері, басқа да жалпыжүйелік және қолданбалы бағдарламалық қамтамасыз ету), автоматтандырылған басқару жүйелері, мемлекеттік құпияларды қамтитын ақпарат қабылдауды, өңдеуді, сақтауды және беруді жүзеге асыратын мемлекеттік органдар мен ұйымдардың байланыс және деректер беру жүйелері;

саяси шешімдерді қабылдау жүйелері жатады.

Қазақстан Республикасының ақпараттық қауіпсіздік қатерлерін олардың шығу тегіне байланысты сыртқы және ішкі деп бөлуге болады.

Ақпараттық қауіпсіздік қатерлерінің көздері:

жекелеген шетелдік саяси, экономикалық, әскери және ақпараттық құрылымдар;

шетел мемлекеттерінің барлау және арнайы қызметтері;

халықаралық террористік және экстремистік ұйымдар;

құрылымға қарсы бағыттағы заңсыз саяси, діни және экономикалық құрылымдар;

ұйымдасқан қылмыстық қоғамдастықтар мен топтар;

жекелеген жеке және заңды тұлғалар;

дүлей зілзалалар және апаттар болып табылады.

Сыртқы қатерлерге:

шетел мемлекеттерінің жаһандық ақпараттық мониторинг, ақпарат тарату және жаңа ақпараттық технологиялар саласындағы сындарлы емес саясаты;

шетелдік барлау және арнайы қызметтердің іс-әрекеттері;

халықаралық топтардың, құралымдар мен жеке тұлғалардың қылмыстық іс-әрекеттері, өнеркәсіптік және банктік шпионаж;

дүлей зілзалалар және апаттар;

халықаралық террористік және экстремистік ұйымдардың қызметі;

шетелдік саяси және экономикалық құрылымдардың Қазақстан Республикасының мүдделеріне қарсы бағытталған қызметі жатады.

Мыналар ішкі қатерлер болып табылады:

ақпарат түзу, тарату және пайдалану саласындағы саяси және экономикалық құрылымдардың заңға қарсы қызметі;

жеке және заңды тұлғалардың, мемлекеттің ақпарат саласындағы заңдық құқықтары мен мүдделерін бұзуға әкелетін мемлекеттік құрылымдардың заңға қайшы іс-әрекеттері;

ақпарат жинаудың, өңдеудің, сақтаудың және берудің белгіленген регламенттерін бұзу;

ақпараттық жүйелер персоналының әдейі жасаған заңсыз іс-әрекеттері және әдейі жасамаған қателері;

ақпараттық және телекоммуникациялық жүйелердегі техникалық құралдардың істен шығуы және бағдарламалық қамтамасыз етудің іркілістері.

Жоғарыда санамаланған қатерлерді іске асыру әр түрлі:

ақпараттық, бағдарламалық-математикалық, физикалық, радиотехникалық және ұйымдастырушылық-құқықтық әдістермен жүзеге асырылуы мүмкін.

Ақпараттық тәсілдерге:

мекенжайдың және ақпараттық алмасу уақтылығының бұзылуы, заңға қарсы ақпарат жинау және пайдалану;

ақпаратқа және ақпараттық ресурстарға рұқсат етілмеген қолжетімділік, ақпарат саласындағы деректерді заңсыз жою, түрлендіру және көшіру;

ақпаратқа рұқсат етілмеген әсер ету және/немесе ақпаратпен айла-амалдар жасау (теріс ақпарат, ақпаратты жасыру немесе бұрмалау);

ақпараттық жүйелердегі деректерді заңсыз көшіру;

бұқаралық ақпарат құралдарын адам, қоғам және мемлекет мүдделеріне қайшы келетін ұстанымда пайдалану;

кітапханалардан, мұрағаттардан, деректер банктерінен және қорларынан ақпарат ұрлау;

ақпарат өңдеу технологиясын бұзу жатады.

Бағдарламалық-математикалық тәсілдер:

вирустар бағдарламаларын енгізуді;

бағдарламалық және аппараттық салынған қондырғыларды орнатуды;

ақпарат жүйелеріндегі деректерді жоюды және түрлендіруді қамтиды.

Физикалық тәсілдер:

ақпарат өңдеу және байланыс құралдарын жоюды немесе бұзуды;

ақпарат тасығыштардың машиналық немесе басқа түпнұсқаларын жоюды, бұзуды немесе ұрлауды;

бағдарламалық немесе аппарат кілттерін және криптографиялық ақпарат қорғау құралдарын ұрлаудан;

персоналға әсер етуді қамтиды.

Радиотехникалық тәсілдер:

қорғау объектісіне жақын орналастырылған не байланыс арналарына немесе ақпарат өңдеудің техникалық құралдарына қосылған техникалық құралдарды

пайдалану арқылы ақпарат қармау;

техникалық құралдарда және үй-жайларда ақпарат қармаудың электрондық қондырғылары;

деректер беру және байланыс желілерінде жалған ақпаратты қармау, цифрды жай жазуға айналдыру және таңу;

парольдық-кілт жүйелеріне әсер ету;

байланыс желілері мен басқару жүйелерін радиоэлектрондық тұмшалау болып табылады.

Ұйымдастырушылық-құқықтық тәсілдер:

жетілмеген немесе ескірген және сәйкестігін растаудан өтпеген техникалық құралдар мен ақпараттандыру құралдарын сатып алуды;

заңнама талаптарын орындамауды және ақпарат саласында қажетті нормативтік құқықтық актілер қабылдауды кешіктіруді;

тұтынушыларға сенімсіз, толық емес, бұрмаланған ақпаратты қасақана немесе жауапсыз беруді;

жеке және заңды тұлғалар үшін маңызды ақпаратты қамтитын құжаттарға қолжетімділікті заңсыз шектеуді қамтиды.

Ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдары мемлекет қызметінің түрлі салалары үшін ортақ болып табылады және былайша топтастырылады:

1) құқықтық: қоғамдағы ақпараттық қатынастарды регламенттейтін нормативтік құқықтық актілер кешенін, ақпараттық қауіпсіздікті қамтамасыз ету жөнінде басшылыққа алынатын және нормативтік-әдістемелік құжаттар әзірлеу;

2) бағдарламалық-техникалық:

рұқсат етілмеген қол жеткізуді немесе оған әсер етуді болдырмау жолымен жанама электромагнит сәулелері мен нысаналар есебінен өңделетін ақпараттың сыртқа шығып кетуін болдырмау;

ақпараттың бұзылуын, жойылуын, бұрмалануын немесе ақпараттандыру құралдары жұмысында іркілістер тудыратын арнайы әсер етудің алдын алу;

енгізілген бағдарламалық немесе аппараттық салынған қондырғыларды анықтау;

ақпарат өңдеудің техникалық құралдарын техникалық барлау құралдарынан арнайы қорғау;

ақпарат қорғаудың криптографиялық әдістері мен құралдарын қолдану;

3) ұйымдастырушылық-экономикалық:

құпия және жасырын ақпаратты қорғау жүйелерінің жұмыс істеуін қалыптастыру және қамтамасыз ету;

ақпараттық қауіпсіздік саласындағы қызметті лицензиялау;

ақпараттық қауіпсіздік саласында техникалық реттеу;

қорғалған ақпарат жүйелерінде персоналдың іс-әрекеттерін бақылау және дәлелдеу (экономикалық ынталандыру, психологиялық қолдау және басқа);

ақпараттық жүйелерді және ақпарат ресурстарын қорғауды және оған қол жеткізу режимін қамтамасыз ету;

халықтың қоғамдық пікірін, қатер көздерін, олардың пайда болуына әсер ететін шарттар мен факторларды зерделеу жөнінде әлеуметтік зерттеулер (мониторинг) жүргізу.

Сонымен қатар, мемлекеттің, жеке және заңды тұлғалардың қызметтері саласының әрқайсында ақпараттық қауіпсіздікті қамтамасыз етудің өз ерекшеліктері бар, бұл ең алдымен, қойылған міндеттерді шешу ерекшелігіне, ақпараттық қауіпсіздіктің әрбір саласына тән әлсіз элементтер мен осал буындардың болуына байланысты.

Сондықтан, әрбір сала үшін арнайы жұмыстарды ұйымдастыру, оның жай-күйіне әсер ететін ерекше факторларды ескере отырып, ақпараттық қауіпсіздікті қамтамасыз ету нысандары мен тәсілдерін пайдалану талап етіледі.

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттары:

нормативтік құқықтық базаны жетілдіру, әдістемелік және техникалық құжаттар әзірлеу;

ақпарат қорғау саласында бірыңғай техникалық саясат әзірлеу және жетілдіру ;

мемлекеттік құпияларды қорғауды қамтамасыз ету;

техникалық барлауларға қарсы іс-әрекет ету;

ақпараттық қарудың әсерінен қорғау;

ақпараттық ресурстарды, ақпараттық-телекоммуникациялық жүйелерді және ақпараттық инфрақұрылымды ұйымдастырушылық-техникалық қорғау;

ақпараттық жүйелер мен ақпараттандыру объектілерінің ақпарат және ақпарат қорғау саласындағы стандарттар мен нормативтік құқықтық актілердің талаптарына сәйкестігі;

техникалық құралдардың ақпараттық қауіпсіздік талаптарына сәйкестігін растау ;

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

ақпарат қорғау және ақпараттық қауіпсіздікті қамтамасыз ету бағыттары бойынша ғылыми-техникалық қамтамасыз ету және ғылыми-зерттеу қызметі;

ақпараттық технологиялар мен ақпарат қорғау саласында кадрлар даярлау;

халықаралық ынтымақтастық.

Саяси салада

Саяси салада ақпараттық қауіпсіздікті қамтамасыз ету объектілері:

отандық және шетелдік бұқаралық ақпарат құралдарының әсерімен қалыптасатын халықтың түрлі санаттарының қоғамдық санасымен саяси бағдары ;

көбінесе оның ақпараттық қамтамасыз етілу сапасы мен уақтылығына байланысты саяси шешімдер қабылдау жүйесі;

мемлекеттік органдардың халықты елдің қоғамдық-саяси және әлеуметтік-экономикалық өмір сүру аспектілері туралы ақпараттандыру және қоғамдық пікір қалыптастыру жүйесі;

саяси партиялар мен қоғамдық ұйымдардың өз көзқарастарын бұқаралық ақпарат құралдарында насихаттауға қатысу жүйесі болып табылады.

Саяси салада ақпараттық қауіпсіздікті қамтамасыз ету объектілеріне қатер қазіргі кезеңде мыналар болып табылады:

бұқаралық ақпарат құралдарын мемлекеттік немесе мемлекеттік емес монополияландыру, сондай-ақ оларға жеке, оның ішінде қылмыстық топтар тарапынан саяси немесе экономикалық қысым көрсету;

жекелеген саяси күштер пайдасына әлеуметтік, ұлтаралық, конфессияаралық және рулық араздықты қоздыратын, халықтың түрлі санаттарын ел басшылығына қарсы қоятын отандық және шетелдік бұқаралық ақпарат құралдарының қоғамға теріс насихаттық және психологиялық әсер етуі;

мемлекет пен бұқаралық ақпарат құралдарының өзара қарым-қатынасы саласындағы қолданыстағы заңнаманың жетілмегендігі;

қоғамдық пікірді қалыптастыру жүйесін саясаттандыру, халық арасында сауалнама жүргізетін түрлі әлеуметтік құрылымдар қызметінің нәтижелерін, олар алған ақпаратты бұрмалап пайдалану немесе біржақты түсіндіру;

компьютерлік қылмыстар.

Саяси салада ақпараттық қауіпсіздікті қамтамасыз етудің негізгі әдістері:

ақпарат саласында саяси өмір субъектілерінің өзара қарым-қатынасын реттейтін құқықтық және ұйымдастырушылық тетіктерді айқындайтын заңнаманы үнемі жетілдіру;

өкілді органдар базасында мемлекеттік бұқаралық ақпарат құралдарының, әлеуметтану және саясаттану орталықтарының, институттар мен қызметтердің іс-әрекеттерін тәуелсіз және жария бақылау жүйелерін қамтамасыз ету;

Қазақстанның бірыңғай ақпараттық кеңістігін қалыптастыру;

елдің ақпарат нарығын теңгерімді дамыту;

отандық бұқаралық ақпарат құралдарының сапасын және бәсекеге қабілеттілігін арттыру;

сыртқы ақпараттық ықпал етуді біртіндеп төмендетуге жәрдемдесу, республика аумағында шетел бұқаралық ақпарат құралдарының қызметін регламенттеу;

бұқаралық ақпарат құралдарының заңнаманы бұзу фактілеріне құқық қорғау органдары мен басқа да мемлекеттік органдардың (прокуратураның, қаржы полициясы мен ішкі істер органдарының, бұқаралық ақпарат құралдары саласындағы уәкілетті органның, облыстардың (республикалық маңызы бар қалалардың, астананың) жергілікті атқарушы органдарының) тиімді ден қоюы;

қолда бар техникалық құралдар мен ақпарат арналарын дер кезінде жаңғырту мен жетілдіру бойынша жағдайлар жасау, осы салада шетелдің озық тәжірибесін үнемі зерделеп отыру;

елдің ішкі істеріне араласуды болдырмау үшін ақпараттық және дипломатиялық деңгейлерде белсенді қарсы насихат қызметінің жүйесін құру бола алады.

Экономика саласында

Экономика саласы объектілерінің арасында мыналар ақпараттық қауіпсіздік қатерлерінің әсеріне:

мемлекеттік басқару және статистика жүйесі;

барлық меншік нысандарындағы шаруашылық жүргізуші субъектілердің коммерциялық қызметі туралы ақпарат көздері;

қаржылық, биржалық, салықтық, кедендік ақпаратты, мемлекеттің сыртқы экономикалық қызметі және коммерциялық құрылымдар туралы ақпаратты, ғылыми-техникалық ақпаратты жинау, беру, сақтау және өңдеу жүйелері неғұрлым жиі ұшырағыш болып келеді.

Мемлекеттік статистикалық есептіліктің ақпараттық-есептеу жүйесі оның ақпараттық ресурстарына рұқсат етілмеген қол жеткізуден жеткілікті қорғаушылыққа ие болады. Бұл ретте бастапқы ақпарат көздерін және оларды рұқсатсыз пайдалану ұлттық қауіпсіздік мүдделеріне залал келтіруі мүмкін кейбір жалпы деректерді қорғауға басты назар аударылатын болады.

Шаруашылық жүргізуші субъектілердің қалыпты жұмыс істеуі коммерциялық қызмет туралы ақпарат көздерінің мәліметтердің сенімсіздігі және оны жасырғаны үшін (нақты шаруашылық қызметі нәтижелері туралы, инвестициялар туралы және басқа) жауапкершілік белгілейтін нормативтік құқықтық актілердің болмауынан бұзылады. Екінші жағынан, қорғауға жататын ақпараттың таралу (сыртқа шығып кету) салдарынан мемлекеттік және кәсіпкерлік құрылымдарға елеулі экономикалық залал келтірілуі мүмкін.

Қаржылық, биржалық, салықтық, кедендік ақпаратты жинау, беру, сақтау

және өңдеу жүйелерінде ақпараттық қауіпсіздік тұрғысынан ақпаратты ұрлау және қасақана бұрмалау неғұрлым үлкен қауіптілікті білдіреді. Олардың мүмкіндігі ақпаратпен жұмыс істеу технологиясын қасақана немесе кездейсоқ бұзумен, оған рұқсат етілмеген қол жеткізумен байланысты, бұл ақпаратты қорғау шараларының жеткіліксіздігімен түсіндіріледі. Тақылеттес қатер сыртқы экономикалық қызмет туралы ақпаратты қалыптастырумен және таратумен айналысатын органдарда да (министрліктердің орталық аппараты, сауда өкілдіктері, кеден және басқа) бар.

Тұтастай алғанда, экономика саласының қалыпты жұмыс істеуі үшін қылмысты элементтердің компьютер жүйелері мен желілеріне кіруіне байланысты барынша әккі компьютерлік қылмыстар (алдау, ұрлау және басқа) елеулі қауіп туғызады.

Стандарттық әдістер мен құралдарды кеңінен пайдаланумен қатар, экономика саласы үшін ақпараттық қауіпсіздікті қамтамасыз етудің басым бағыттары:

жеке және заңды тұлғалардың ақпаратқа рұқсатсыз қол жеткізуге және оны ұрлауға, ақпаратты бұзуға және бұрмалауға, қасақана жалған ақпарат таратуға, қолжетімділігі шектеулі ақпарат таратуға жауапкершілігін белгілейтін құқықтық нормалар әзірлеу және қабылдау;

бастапқы ақпарат көздерінің жауапкершілігін енгізу, ақпарат өңдеу және талдау қызметтерінің іс-әрекеттерін пәрменді бақылауды ұйымдастыру, ақпаратты техникалық қорғаудың арнайы ұйымдастырушылық және бағдарламалық-техникалық құралдарын пайдалану арқылы ақпараттың сенімділігін, толықтығын, салыстыруға келетіндігін және қорғалуын арттыру;

қаржылық және коммерциялық ақпаратты, сондай-ақ адамның денсаулығының жай-күйіне қатысты жеке сипаттағы ақпаратты арнайы қорғауды құру және жетілдіру;

экономика саласындағы ерекше қызметті ескере отырып, ақпараттық қызмет технологиясын жетілдіру және шаруашылық, қаржылық, өнеркәсіптік және басқа экономикалық құрылымдарда ақпарат қорғау жөнінде ұйымдастырушылық-техникалық іс-шаралар кешенін әзірлеу;

экономикалық ақпаратты жинау, өңдеу, талдау және тарату үшін персоналды кәсіби іріктеу және даярлау жүйесін жетілдіру болып табылады.

Қорғаныс саласында

Қорғаныс саласындағы қатердің барлық кешені тарапынан неғұрлым осал ақпараттық қауіпсіздік объектілеріне:

әскери іс-қимылдарды дайындау және жүргізудің жедел және стратегиялық жоспарлары туралы, әскерлердің құрамы және орналасуы туралы, жұмылдыру

дайындығы, қару-жарақ пен әскери техниканың тактикалық-техникалық деректері мен сипаттамалары туралы мәліметтер мен деректерді қамтитын Қазақстан Республикасы Қарулы Күштерінің, басқа да әскерлері мен құралымдары әскери басқару органдарының, құрамаларының, бөлімдері мен мекемелерінің ақпараттық ресурстары;

қорғаныс кешені кәсіпорындарының ғылыми-техникалық және өнеркәсіптік әлеуеті, шикізат пен материалдардың стратегиялық түрлерінің жеткізілім көлемдері мен қорлары, қару-жарақтың, әскери техниканың негізгі даму бағыттары, олардың жауынгерлік мүмкіндіктері туралы және қорғаныс мүддесінде өткізілетін іргелі және қолданбалы ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстары туралы мәліметтер мен деректерді қамтитын олардың ақпараттық ресурстары;

байланыс жүйесі және әскерлер мен қару-жарақты басқарудың автоматтандырылған жүйелері, оларды ақпараттық қамтамасыз ету;

ақпараттық-насихаттық әсер етуге тәуелді бөлігінде әскерлердің моралдық-психологиялық жай-күйі;

ақпараттық инфрақұрылым, оның ішінде Қазақстан Республикасы Қарулы Күштерінің, басқа да әскерлері мен әскери құралымдары әскери басқару органдарының, құрамаларының, бөлімдері мен мекемелерінің ақпараттарын өңдеу, талдау және сақтау орталықтары;

қару-жарақ және әскери техника жатады.

Сыртқы қатер көздерінен қорғаныс саласы объектілерінің ақпараттық қауіпсіздігіне едәуір дәрежеде әсер ететін мыналар:

шетелдік арнайы қызметтер мен шетел мемлекеттері ұйымдарының барлау қызметінің барлық түрлері;

ақпараттық-техникалық әсер ету (радиоэлектрондық күрес әдістері, компьютерлік желілерге кіру және басқалар);

арнайы әдістермен және бұқаралық ақпарат құралдарының қызметі арқылы жүзеге асырылатын психологиялық операциялар;

қорғаныс саласында Қазақстан Республикасының мүдделеріне қарсы бағытталған шетелдік саяси және экономикалық құрылымдарының қызметі;

ақпараттық соғыстар, компьютерлік қылмыстар.

Ішкі қатер көздерінен мыналар біршама қауіп төндіреді:

Қазақстан Республикасы Қарулы Күштерінің, басқа да әскерлері мен әскери құралымдарының әскери басқару органдарында, құрамаларында, бөлімдері мен мекемелерінде ақпаратты жинау, өңдеу және берудің белгіленген регламенттерін бұзу;

арнайы мақсаттағы ақпараттық жүйелер персоналының қасақана іс-әрекеттері мен әдейі жасалмаған қателіктері;

арнайы мақсаттағы ақпараттық және телекоммуникациялық жүйелерде техникалық құралдардың істен шығуы және бағдарламалық қамтамасыз етудің іркілістері;

мемлекет мүдделеріне қарсы бағытталған, Қарулы Күштердің беделіне және олардың әскери дайындығына нұқсан келтіретін ұйымдар мен жекелеген тұлғалардың ақпараттық-насихаттау қызметі.

Бұл қатер көздері әскери-саяси жағдай шиеленіскен кезде ерекше қауіп төндіреді.

Қорғаныс саласында ақпараттық қауіпсіздікті жетілдірудің негізгі бағыттары:

қорғаныс саласында ақпараттық қауіпсіздікті қамтамасыз ету мақсаттарын құрылымдауды, одан туындайтын практикалық міндеттерді қамтитын тұжырымдамалық;

қорғаныс саласында ақпараттық қауіпсіздік жүйесінің функционалдық органдарының оңтайлы құрылымы мен құрамын қалыптастыру және олардың тиімді өзара іс-қимылын үйлестіру қажеттілігіне байланысты ұйымдастырушылық, стратегиялық және жедел жасырыну мен теріс хабар беру, барлау және радиоэлектрондық күрес тәсілдері мен жолдарын, ақпараттық-насихаттау және психологиялық операцияларға белсенді қарсы іс-әрекет жасау әдістері мен құралдарын жетілдіру;

ақпараттық ресурстарды оларға рұқсат етілмеген қол жеткізуден қорғау құралдарын үнемі жетілдірумен, қорғалатын жүйелерді, оның ішінде байланыс және әскерлер мен қару-жарақты басқару жүйелерін дамытумен сипатталатын техникалық, арнайы бағдарламалық қамтамасыз ету сенімділігін арттыру болып табылады.

Бұдан басқа, қорғаныс саласында ақпараттық қауіпсіздікті жетілдірудің басты бағыттарының бірі қару-жарақ пен әскери техниканы әзірлеу, өндіру және олардың тактикалық-техникалық сипаттамалары туралы ақпаратты қорғау тиімділігін арттыру болып табылады.

Төтенше жағдайлар кезінде

Төтенше жағдайлар (бұдан әрі - ТЖ) кезінде ақпараттық қауіпсіздік қатері үшін неғұрлым осал объектілер олардың дамуына қарсы жедел іс-әрекеттер (ден қою) жөнінде шешімдер қабылдау жүйесі мен зардаптарды жою барысы, сондай-ақ ТЖ-ның пайда болу мүмкіндігі туралы ақпарат жинау мен өңдеу және хабарландыру жүйесі болып табылады.

Осы объектілер мен азаматтық қорғаныстың басқару пункттерінің қалыпты жұмыс істеуі үшін авариялар, апаттар және дүлей зілзала салдарынан ақпараттық

инфрақұрылымды (ақпаратты жинау және талдау орталықтарын, хабарландыру жүйелерін, телекоммуникация жүйелерін және байланыс арналарын) бүлінуден және бұзылудан қорғау үлкен мәнге ие.

ТЖ кезінде ақпараттық әсер етудің ерекшелігі психикалық күйзеліске ұшыраған бұқара халықтың қозғалысқа келуі, үрейлі алып-қашпа сөздердің, жалған және сенімсіз ақпараттың тез таралуы болып табылады. Көбінесе, ТЖ кезінде оның зардаптарын жоюда қиындыққа тірейтін жай-ақпаратты жасыру жиі орын алады.

Аталған сала үшін ақпараттық қауіпсіздікті қамтамасыз етудің ерекше бағыттарына:

ТЖ-ны алдын ала білдіруші белгілердің автоматтандырылған мониторингі және ТЖ мен азаматтық қорғаныс туралы хабарландырудың тиімді жүйелерін әзірлеу;

ТЖ бойынша шешімдер қабылдау орталықтарының қызметін, олардың автономды режимде ұзақ уақыт жұмыс істеу мүмкіндігін қамтамасыз ететін ақпарат өңдеу және беру құралдарының сенімділігін арттыру;

бұқара халықтың жалған немесе сенімді ақпараттың әсерінен болатын мінез-құлқын талдау және оларды ТЖ кезінде басқару жөнінде шаралар тұжырымдау;

ТЖ және азаматтық қорғаныс кезінде халықты ақпараттандыру және хабардар етуді арттырудың арнайы шараларын әзірлеу;

ақпаратты өңдеу және беру құралдарымен, сондай-ақ ТЖ кезінде автономды режимде жұмыс жүргізуге арналған құралдармен жарақталған ұтқыр кешендер құру жатады.

Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелерде

Жалпымемлекеттік 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.

Жалпымемлекеттік 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 (вирусқа қарсы процессорлар, вирусқа 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.

Ғылым мен техника саласында

Ғылым мен техника саласындағы ақпараттық қауіпсіздіктің неғұрлым осал объектілері мыналар болып табылады:

жоғалуы Қазақстан Республикасының ұлттық мүдделеріне залал келтіруі мүмкін, елдің ғылыми-техникалық, технологиялық және әлеуметтік-экономикалық дамуы үшін әлеуетті маңызы бар мәліметтерді, деректер мен білімді қамтитын іргелі, іздестіру және қолданбалы ғылыми зерттеулердің нәтижелері;

құпиялылық мәртебесі әлі айқындалмаған және сондықтан Қазақстан Республикасының заңнамасының күші жүрмейтін әрі шетелге сатылуы мүмкін патенттелмеген технологиялар, ноу-хау моделдің өнеркәсіптік үлгілері мен эксперименттік жабдық;

құқықтық қорғалғандығына қарамастан ұрлануы және заңсыз таратылуы немесе пайдаланылуы мүмкін зияткерлік меншік объектілері (жаңалықтар, өнертабыс патенттері, өнеркәсіптік үлгілер, бағдарламалық өнімдер және басқалары).

Бұл саладағы қатерлер жіктеу кезінде шетел мемлекеттері арнайы қызметтері мен қылмыстық құрылымдардың өнеркәсіптік шпионаж жасау мүмкіндігін зерделеуге ерекше назар аудару қажет.

Ғылыми және зияткерлік әлеуетті заңсыз иеленудің немесе пайдаланудың алдын алу мақсатында қатердің таралуының әрбір нақты жағдайы немесе ғылыми, техникалық және технологиялық өнім үшін ұсынымдар тұжырымдайтын қоғамдық ғылыми кеңестер мен тәуелсіз сарапшылар институтын қамтитын қатерлердің көрсетілген объектілерге әсер етуінің ықтимал зардаптарын бағалау жүйесі ұйымдастырылатын болады.

Мемлекет тарапынан қатерлерге қарсы әрекет етудің шынайы жолы осы

саладағы заңнаманы және оны іске асыру тетіктерін үнемі жетілдіру болып табылады. Бұл саладағы қатерлердің алдын алу немесе залалсыздандыру жөніндегі, әсіресе ғылыми кадрларға қатысты бөлігіндегі көптеген іс-шаралар мемлекеттің әлеуметтік және экономикалық саясаты саласына жатады.

Рухани өмір және жеке тұлғаның ақпараттық қауіпсіздігі саласында

Рухани өмір саласындағы ақпараттық қауіпсіздікті қамтамасыз ету объектілері мыналар болып табылады:

адамдардың дүниетанымы, олардың өмірлік құндылықтары мен идеалдары, атап айтқанда, мемлекет пен қоғам үшін маңызды патриотизм, азаматтық борыш, этникалық және діни төзімділік және сол сияқтылар;

жеке тұлғаның әлеуметтік және жеке бағдарлануы;

көбінесе адамдардың дүниетанымын айқындайтын мәдени және эстетикалық құраныстар;

жеке тұлғаның психикалық саулығы.

Басқаларға қарағанда рухани өмір саласы негізінен бұқаралық ақпарат құралдары арқылы жүзеге асырылатын ақпараттық-насихаттық әсер етуге, идеологиялық қысымға, мәдени өктемдікке сезімтал болады.

Осыған байланысты жеке тұлғаның рухани өмірін қалыптастыруда бұқаралық ақпарат құралдары айқындаушы рөл атқарады, бұл олардың қоғам алдындағы ерекше жауапкершілігін негіздейді. Бұл ретте Интернет халықаралық ақпарат желісі ерекше орын алады, ол өзінің ашықтығы мен қол жетімділігіне байланысты халықаралық терроризм мүдделерінде жеке тұлғаға зорлық-зомбылыққа, ұлтаралық араздыққа, діни экстремизмге шақыратын теріс ақпаратпен ықпал ету құралы ретінде пайдаланылуы мүмкін.

Рухани өмір саласында ақпараттық қауіпсіздікке қатерлердің алдын алу мен залалсыздандыру, ең алдымен, халықтың басым бөлігі үшін қолайлы әрі елді мекен ететін көптеген этностардың мүдделерін, мәдени және тарихи дәстүрлерін ескеріп әзірленген мемлекеттік идеологияны талап етеді. Мұндай идеология негізінде ақпараттық қауіпсіздікке қатерлерді бағалаудың нақты өлшемдері, осы саладағы негізгі басымдықтар мен мемлекеттік саясат тұжырымдалуы мүмкін.

Сонымен қатар, елдің ұлттық мүдделеріне жауап беретін рухани құндылықтарды қалыптастыруға және таратуға, оларды дұшпандық немесе достық емес насихаттан қорғауға тарту мақсатында бұқаралық ақпарат құралдарымен өзара іс-қимылдың өркениетті, демократиялық нысандары мен әдістері талап етіледі.

Интернет саласын заңнамалық реттеу, зиянды және теріс ақпараттың

бар-жоғына трафикті бақылау мақсатында ұйымдастырушылық-құқықтық шараларды іске асыру талап етіледі.

Мәдениетті коммерцияландыруға кедергі келтіретін және тарихи-мәдени мұраны құрайтын ақпараттық ресурстарды сақтау мен дамытуды қамтамасыз ететін құқықтық және ұйымдастыру шараларын әзірлеу қажет.

Халықаралық ынтымақтастық саласында

Ақпараттық қауіпсіздік саласындағы халықаралық ынтымақтастық (бұдан әрі - ынтымақтастық) - әлемдік қоғамдастыққа қатысушы елдердің өзара іс-қимыл жасауының саяси, әскери, экономикалық, мәдени және басқа да түрлерінің ажырамас құрауышы.

Қазақстан Республикасының мүдделеріне жауап беретін ынтымақтастықтың негізгі бағыттары мыналар болып табылады:

трансшекаралық ақпарат алмасудың ақпараттық қауіпсіздігін және алмасу регламентін, сондай-ақ ақпаратты телекоммуникациялық арналар бойынша беру кезінде оның сақталуы мен бұрмаланбауын қамтамасыз ету;

халықаралық ынтымақтастыққа қатысушы мемлекеттердің компьютерлік қылмыстардың алдын алу жөніндегі қызметін үйлестіру;

халықаралық банктік желілердегі және әлемдік сауданы ақпараттық қамтамасыз ету арналарындағы қорғалатын ақпаратқа, халықаралық саяси, экономикалық және әскери одақтардағы, блоктар мен ұйымдардағы қорғалатын ақпаратқа, халықаралық ұйымдасқан қылмысқа, халықаралық терроризмге, есірткі таратуға және қару-жарақ пен радиоактивтік материалдардың заңсыз саудасына қарсы күрес жүргізетін халықаралық құқық қорғау ұйымдарындағы ақпаратқа рұқсат етілмеген қолжетімділікті алдын алу;

ақпарат алмасудың жаңа жүйелерін әзірлеу, технологиялық базаны жетілдіру және ақпараттық жүйелер мен ақпараттық ресурстар қауіпсіздігі жүйелерін қалыптастыру жөнінде бірлескен халықаралық жобалар жасау.

Тәуелсіз Мемлекеттер Достастығы елдерімен, Еуразиялық экономикалық қоғамдастығына, Ұжымдық қауіпсіздік туралы шарт ұйымына, Шанхай ынтымақтастық ұйымына мүше мемлекеттермен ынтымақтастыққа айрықша назар аударылатын болады.

Ынтымақтастықтың көрсетілген бағыттарын іске асыру үшін:

Қазақстанның ақпараттық қауіпсіздікті қамтамасыз ету саласында әрекет ететін халықаралық ұйымдарға белсене қатысуы;

ақпараттық қауіпсіздікті қамтамасыз ету саласында, оның ішінде халықаралық және отандық басылымдары арқылы тәжірибе алмасу.

Баяндалған принциптер мен ережелер негізінде мемлекет қызметінің саяси,

әскери, экономикалық және басқа да салаларындағы ақпараттық қауіпсіздік саясатын қалыптастыру мен іске асырудың басым бағыттары айқындалады.

Ақпараттық қауіпсіздік саласындағы мемлекеттік саясат ақпараттық қатынастар субъектілері мүдделерінің келісілуін, қоғамдық және үкіметтік емес ұйымдардың кеңінен өкілдік етуімен мемлекеттік органдар мен ұйымдардың тиімді жұмысын ұйымдастыруды көздейді.