"Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы" Қазақстан Республикасының Президенті Жарлығының жобасы туралы

Қазақстан Республикасы Үкіметінің 2006 жылғы 21 қыркүйектегі N 894 Қаулысы

Қазақстан Республикасының Үкіметі **ҚАУЛЫ ЕТЕДІ:**

"Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы" Қазақстан Республикасының Президенті Жарлығының жобасы Қазақстан Республикасы Президентінің қарауына енгізілсін.

Қазақстан Республикасының Премьер-Министрі

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ПРЕЗИДЕНТІНІҢ ЖАРЛЫҒЫ

Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы

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 "__" _____ N ___ Жарлығымен мақұлданған

Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы

Кіріспе

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

Қоғам мен мемлекеттің әлеуметтік-экономикалық және мәдени өміріндегі ақпараттық технологиялардың маңызды ролі ақпараттық қауіпсіздік мәселелерін шешуге жоғары талаптар қояды.

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

1. Жалпы ережелер

Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы (бұдан әрі - Тұжырымдама) Қазақстан Республикасы Конституциясының және Қазақстан Республикасының "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 заңдарының және 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.

Тұжырымдама ақпараттық қауіпсіздікті қамтамасыз ету саласында Қазақстан Республикасында бірыңғай мемлекеттік саясатты айқындау, қалыптастыру, жүргізу және іске асыру кезінде негіз болып қызмет етеді, оның ережелері Қазақстанның мемлекеттік ақпараттандыру саясатын, мемлекеттік ақпараттық жүйелер мен мемлекеттік ақпараттық ресурстарды қорғауды қалыптастыру, Қазақстанның бірыңғай ақпараттық кеңістігін құру және дамыту кезінде ескеріледі.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз етудің мемлекеттік саясаты (бұдан әрі - Мемлекеттік саясат) ашық болып табылады және қоғамның қолданыстағы заңнамада көзделген шектеулерді ескере отырып, ақпараттық қауіпсіздік саласындағы мемлекеттік органдар мен қоғамдық институттардың 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, ақпараттық ресурстардың меншік иелерінің, иелерінің және таратушыларының заңды мүдделері сақталған жағдайда оларды шаруашылық айналымға енгізуге ықпал ететінін негізге алады.

Мемлекет жаһандық ақпараттық желілерде және мониторинг жүйелерінде 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 жағдайын бағалау және осы саладағы негізгі проблемалар мен бағыттарды айқындау кезінде ескеру қажет жаңа факторлар туындайды.

Көрсетілген факторларды саяси, экономикалық және ұйымдастыру-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, бір тарапты артықшылықтар алу мақсатында ақпаратты тарататын әлемнің дамыған елдерінің ақпараттық экспансиясы;

демократия, заңдылық, ақпараттық ашықтық, елдің қауіпсіздігін қамтамасыз ету жүйесін жетілдіру қағидаттары негізінде Қазақстанның жаңа мемлекеттігінің қалыптасуы;

ішкі саяси дағдарыстар: билік тармақтарының, аумақтық мемлекеттік құрылым субъектілерінің жанжалдары, төңкерістер, қорғалатын тұлғаларға қастандық жасау;

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 кірігуі, көптеген отандық және шетел коммерциялық құрылымдардың - ақпаратты жасаушылар мен пайдаланушылардың, 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 неғұрлым жоғары дәрежеде айқындайтын жаңа ақпараттық технологияларды дамыту мен енгізуде Қазақстанның артта қалуы барынша 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 қызметтер нарығында жұмыс істеу және даму процестерін нашар реттеуі;

ақпаратты сақтау, өңдеу, беру және қорғау үшін мемлекеттік басқару саласында, кредит-қаржы және басқа салаларда ақпараттың сыртқа 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 уақыттағы деңгейі адамның, қоғамның және мемлекеттің қажеттіліктеріне сәйкес келмейді.

Елдің саяси және әлеуметтік-экономикалық дамуының бүгінгі жағдайы қоғамның ақпаратпен еркін алмасуды кеңейтудегі 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 сәйкестігін растау жүйелерін әзірлеу талап етіледі.

Ақпаратты қорғау саласында кәсіби мамандарды даярлау жөніндегі жоғары және арнайы оқу орындары сандарының жеткіліксіздігі республикада ақпараттық қауіпсіздікті ұйымдастыруға елеулі әсерін тигізеді.

Техникалық барлауларға қарсы іс-әрекеттер және 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 жалпы мемлекеттік ауқымда, ведомстволық деңгейде қорғау жөніндегі іс-шараларды кешенді үйлестіру қажет.

Ақпараттық кеңістікте Интернет 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 қауіп көздері Қазақстан Республикасының заңи құзыретінен тыс болуы мүмкін, бұл құқық шаралары жүйесін қолдануды елеулі қиындатады.

Отандық ақпараттық технологиялардың болмау проблемасы өзекті болып табылады , бұл жаппай пайдаланушыларды ақпараттық қауіпсіздік талаптары бойынша сәйкестігі расталмаған импорттық техниканы сатып алуға мәжбүр етеді, бұл деректер базалары мен банктерінің ақпараттық қауіпсіздігіне қауіп, сондай-ақ елдің компьютер мен телекоммуникация техникасын өндірушілерге және ақпарат өнімдеріне тәуелділігін тудыруы мүмкін.

Қазіргі заманғы қоғамының табысты жұмыс істеуі онда болып жатқан ақпараттық процестердің қаншалықты тиімді ұйымдастырылғанына және қалыптасқанына тұтастай байланысты. Осыған байланысты Қазақстан Республикасы үшін осы процестердің мемлекет шеңберінде бірыңғай ақпараттық кеңістікке түйісуі үлкен маңызды болуда.

Қазақстан Республикасы Президентінің 2004 жылғы 10 қарашадағы N 1471 Жарлығымен бекітілген Қазақстан Республикасында "электрондық үкімет" қалыптастырудың 2005 - 2007 жылдарға арналған мемлекеттік бағдарламасында көзделген "электрондық үкіметті" әзірлеу және енгізу қадам болып табылатын Қазақстан Республикасының бірыңғай ақпараттық кеңістігін қалыптастыру барлық жинақталған ақпаратты пайдалану және өздерінің арасында да, экономика субъектілері мен халықтың арасында да ақпараттық өзара іс-әрекетті неғұрлым серпінді ұйымдастыру негізінде олардың қызметін ақпараттық қолдауды қамтамасыз ету есебінен барлық билік тармақтарының жұмыс істеу тиімділігін елеулі арттыруға мүмкіндік береді. Бірыңғай ақпараттық кеңістік ақпараттық қажеттіліктерді қанағаттандыруды қамтамасыз етіп қана қоймай, сондай-ақ ақпаратты өндірушілер мен тұтынушылар қызметін ынталандыратын да болады.

Ақпараттық ресурстар және ақпараттық жүйелер туралы мәліметтер мынадай мақсаттарда Мемлекеттік тіркелімде тіркелуге жатады:

ақпараттық ресурстар және ақпараттық жүйелер туралы ақпаратты жүйелендіру;

Қазақстан Республикасының жеке және заңды тұлғаларын мемлекеттік тіркелімдегі ақпараттар туралы хабардар ету;

Қазақстан Республикасының мемлекеттік органдарын ақпараттық қамтамасыз ету;

ақпараттық ресурстар мен ақпараттық жүйелердің бірігуін ұйымдастыру, сондай-ақ ақпараттық ресурстар мен ақпараттық жүйелер арасында деректермен алмасу үшін ақпараттық ресурстар мен ақпараттық жүйелерді әзірлеушілерге ақпарат беру.

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.

Ақпаратты жасау және пайдалану тұрғысынан ақпараттық қатынастар субъектілері авторлар, меншік иелері, иеленушілер немесе пайдаланушылар ретінде түсуі мүмкін.

Ақпарат және ақпараттық ресурстар заттай 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.

3. Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен міндеттері

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі мақсаттары:

ұлттық ақпаратты қорғау 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 экспансияны 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 қауіптерінің 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 қауіптерін бейтараптау құралдарын, оны бұзу салдарларын 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, қауіптері, әдістері, құралдары және негізгі бағыттары

Қазақстан Республикасының ақпараттық қауіпсіздік объектілеріне:

жеке және заңды тұлғалардың, мемлекеттің ақпаратты 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 қол жетімді) ақпаратты қамтитын мәліметтері бар ақпараттық ресурстар;

әртүрлі сыныптағы және мақсаттағы ақпараттық жүйелерді, кітапханаларды, мұрағаттарды, деректер қорлары мен банктерін, ақпараттық технологияларды, ақпаратты 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 (дүниетанымдар, 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 модельдер мен эксперименттік жабдық;

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

ақпараттандыру құралдары мен жүйелері (есептеуіш 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 ақпаратты 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 қауіптерін олардың шығу тегіне байланысты сыртқы және ішкі деп бөлуге болады.

Ақпараттық қауіпсіздік қауіптерінің 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.

Сыртқыға:

шетел мемлекеттерінің жаһандық ақпараттық мониторинг, ақпарат пен жаңа ақпараттық технологияларды тарату 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;

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

Мыналар ішкі болып табылады:

ақпаратты қалыптастыру, 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 ;

ақпаратты 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 қауіптерді іске асыру әр түрлі: ақпараттық, бағдарламалық-математикалық, физикалық, радиотехникалық және ұйымдастыру-құқықтық әдістермен жүзеге асырылуы мүмкін.

Ақпараттық тәсілдерге:

мекен-жайдың және ақпараттық алмасу уақтылығының бұзылуы, заңға қарсы ақпарат жинау және пайдалану;

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

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

ақпараттық жүйелердегі деректерді заңсыз көшіру;

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

кітапханалардан, мұрағаттардан, деректер банктерінен және қорларынан ақпаратты ұрлау;

ақпаратты 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:

ақпаратты өңдеу және байланыс құралдарын жоюды немесе бұзуды;

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

бағдарламалық немесе аппарат кілттерін және криптографиялық ақпаратты қорғау құралдарын ұрлауды;

персоналға әсер етуді қамтиды.

Радиотехникалық тәсілдер:

қорғау объектісіне жақын орналастырылған не байланыс арналарына немесе ақпаратты өңдеудің техникалық құралдарына қосылған техникалық құралдарды пайдалану арқылы ақпаратты ұстап қалу;

техникалық құралдарда және үй-жайларда ақпаратты ұстап қалудың электрондық қондырғылары;

деректер беру және байланыс желілерінде жалған ақпаратты ұстап қалу, шифрды жай жазуға айналдыру және таңу;

парольдық-кілт жүйелеріне әсер ету;

байланыс желілері мен басқару жүйелерін радиоэлектрондық басу болып табылады.

Ұйымдастыру-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 кесімдерді қабылдауды кешіктіруді;

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

жеке және заңды тұлғалар, мемлекет үшін маңызды ақпаратты қамтитын құжаттарға қол жеткізуді 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 жөніндегі басқаратын және нормативтік-әдістемелік құжаттарды әзірлеу;

2) бағдарламалық-техникалық:

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

ақпараттың бұзылуын, жойылуын, бұрмалануын немесе ақпараттандыру құралдары жұмысында іркілістер тудыратын арнайы әсер етуді болдырмау;

енгізілген бағдарламалық немесе аппараттық салынған қондырғыларды анықтау;

ақпаратты өңдеудің техникалық құралдарын техникалық барлау құралдарынан арнайы қорғау;

ақпаратты қорғаудың криптографиялық әдістері мен құралдарын қолдану;

3) ұйымдастыру-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, қауіп көздерін, олардың пайда болуына әсер ететін шарттар мен факторларды зерттеу 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 мәселелерді шешу ерекшелігіне, ақпараттық қауіпсіздіктің әрбір саласына тән әлсіз элементтер мен осал буындардың болуына байланысты.

Сондықтан, әрбір сала үшін арнайы жұмыстарды ұйымдастыру, оның жағдайына 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 құжаттарды әзірлеу;

ақпаратты қорғау саласында бірыңғай техникалық саясатты 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 ұйымдастыру-техникалық қорғау;

ақпарат және ақпаратты қорғау саласындағы стандарттардың және нормативтік құқықтық актілердің талаптарына ақпараттық жүйелерді және ақпараттандыру объъектілерін аттестаттау;

техникалық құралдардың ақпараттық қауіпсіздік талаптарына сәйкес келуін растау;

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

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

ақпараттық технологиялар мен ақпаратты қорғау саласында кадрларды 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 ету сапасы мен уақтылығына байланысты саяси шешімдерді қабылдау жүйесі;

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

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

Саяси салада ақпараттық қауіпсіздікті қамтамасыз ету объектілеріне қауіп 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 сананаттарын 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, халықтың арасында сұрақ-жауап жүргізетін түрлі әлеуметтік құрылымдардың қызметін бұрмалауда немесе олардың нәтижелерін біржақты түсіндіруде пайдалану;

компьютерлік қылмыстар.

Саяси салада ақпараттық қауіпсіздікті қамтамасыз етудің негізгі әдістері:

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

өкілеттік органдар базасында мемлекеттік және мемлекеттік емес бұқаралық ақпарат құралдарының, әлеуметтік және саяси орталықтардың, 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 құралдарды және ақпарат арналарын қазіргі заманға сай жаңғырту мен жетілдіру бойынша жағдай жасау, осы салада шетелдің озық тәжірибесін үнемі үйрену;

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

Экономика саласында

Экономика саласы объектілерінің арасында ақпараттық қауіпсіздік қатерлері әсеріне мыналар неғұрлым бейім болуы мүмкін:

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.

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 ақпаратты тарату (сыртқа шығару) 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 аса қауіпті білдіреді, оның мүмкіндігі ақпаратпен жұмыс істеу технологиясын қасақана немесе кездейсоқ бұзумен, оған рұқсат етілмеген қол жеткізумен байланысты, бұл ақпаратты қорғау шараларының жеткіліксіздігімен түсіндіріледі. Осындай қауіп 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 кіруімен байланысты барынша әккі компьютерлік қылмыстар (алдау, ұрлау және басқа) үлкен қауіп туғызады.

Стандарт 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, жалған ақпаратты қасақана таратуға, қол жеткізу шектелген ақпаратты таратуға жауапкершілігін белгілейтін құқықтық нормаларды әзірлеу және қабылдау;

бастапқы ақпарат көздерінің жауапкершілігін енгізу, ақпаратты 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 денсаулығына 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 ақпаратты қорғау жөнінде ұйымдастыру-техникалық іс-шаралар кешенін әзірлеу;

экономикалық ақпаратты жинау, өңдеу, талдау және тарату жүйелерінің персоналын кәсіби жағынан іріктеу және даярлау жүйелерін жетілдіру болып табылады .

Қорғаныс саласында

Қорғаныс саласындағы қауіптің 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, тактикалық-техникалық деректер және қару-жарақ пен әскери техника туралы мәліметтер мен деректерді қамтитын Қазақстан Республикасы Қарулы Күштерінің, басқа да әскерлері мен құралымдары әскери басқару органдарының, құрамаларының, бөлімдері мен мекемелерінің ақпараттық ресурстары;

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

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

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

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

қару-жарақ және әскери техника жатады.

Сыртқы қауіп 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, компьютер желілеріне 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 қауіп көздерінен едәуір қауіпті мыналар төндіреді:

Қазақстан Республикасы Қарулы Күштерінің, басқа 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 қауіп 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 және 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 жағдайларда

Төтенше жағдайларда (бұдан әрі - ТЖ) ақпараттық қауіпсіздік қатері үшін ең осал объектілер оларды дамытуға арналған жедел іс-әрекеттер (реакциялар) бойынша шешімдер қабылдау жүйесі мен зардаптарды жою барысы, сондай-ақ ТЖ пайда болу мүмкіндігі туралы ақпаратты жинау мен өңдеу және хабарлау жүйесі болып табылады.

Осы объектілер мен азаматтық қорғанысты басқару пункттерінің қалыпты жұмыс істеуі үшін аварияларапаттар және дүлей зілзала салдарынан ақпараттық инфрақұрылымды (ақпаратты жинау және талдау орталықтарын, телекоммуникация жүйелерін және байланыс арналарын) бүлінуден және бұзылудан қорғау үлкен мәнге и е .

ТЖ жағдайында ақпараттық әсер етудің ерекшелігі психикалық күйзеліске ұшыраған адамдар тобын қозғалысқа келтіру, үрейлі сыбыстарды, жалған және сенімсіз ақпаратты тез тарату болып табылады. Көбінесе, ТЖ жағдайында оның салдарларын жою кезінде қиындыққа келтіретін ақпаратты жасыру орын алады.

Осы сала үшін ақпараттық қауіпсіздікті қамтамасыз етудің ерекше бағыттарына:

ТЖ-ны алдын ала білдіруші белгілердің автоматтандырылған мониторингін және ТЖ және азаматтық қорғаныс туралы хабарлаудың тиімді жүйелерін әзірлеу;

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

адамдар тобының жалған немесе сенімді ақпараттың әсерінен болатын мінез-құлқын талдау және оларды ТЖ жағдайында басқару жөніндегі шараларды ә з і р л е у ;

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

ақпаратты өңдеу және беру құралдарымен және ТЖ жағдайында автономды режимде жұмыс жүргізуді қамтамасыз етуге арналған құралдарымен жарақталған ұтқыр кешендер құру.

Жалпымемлекеттік ақпараттық және телекоммуникациялық жүйелерде

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 берілген мемлекеттік құпияларға жататын мәліметтерді және құпия ақпаратты қамтитын ақпараттық ресурстар;

ақпараттандыру құралдары мен жүйелері (есептеуіш техника құралдары,

ақпараттық-есептеу кешендері, желілер және жүйелер), бағдарламалық құралдар (операциялық жүйелер, дерекқорларды басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз ету), автоматтандырылған басқару жүйелері, байланыс және деректер беру жүйелері, қол жеткізу шектелген ақпаратты өңдеу үшін пайдаланылатын ақпаратты қабылдау, беру және өңдеудің техникалық құралдары, олардың ақпараттық физикалық өрістері;

ақпаратты өңдемейтін, алайда мемлекеттік құпияларға жатқызылған мәліметтері бар ақпаратты 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, оларды ақпараттық қамтамасыз ету, олардың ақпараттық инфрақұрылымы;

режимдік және стратегиялық объектілер, қол жеткізу шектелген ақпарат өңделетін есептеуіш 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 үздіксіз жұмыс істеуін қамтамасыз ету;

ақпаратты техникалық барлау құралдарынан арнайы қорғау;

техникалық құралдарда өңделетін немесе сақталатын ақпаратқа рұқсатсыз қол жеткізуді болдырмау;

есептеуіш техника құралдарының объектілерінде жанама электромагнит сәулелері мен нысаналар есебінен өңделетін ақпараттың сыртқа шығуын болдырмау;

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

объектілерге және техникалық құралдарға енгізілген электрондық ақпаратты ұстап қалу қондырғыларын (салынған қондырғыларды) анықтау;

техникалық құралдардың сөз ақпаратын үй-жайлардан және объектілерден ұстап қалудың алдын алу болып табылады.

Байланыс арналары бойынша берілетін ақпаратты техникалық құралдардың көмегімен ұстап қалудың алдын алуға криптографиялық және өзге әдістер мен қорғау құралдарын қолданумен, сондай-ақ қажетті ұйымдастыру-техникалық іс-шараларды

жүргізумен қол жеткізіледі.

Берілетін, өңделетін немесе техникалық құралдарда сақталатын ақпаратқа рұқсат етілмеген қол жеткізуді және әсерді 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 шығуын 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 орнатумен және басқа ұйымдастырушылық және техникалық шаралармен қол жеткізіледі.

Ақпараттың бұзылуын, жойылуын, бұрмалануын немесе ақпараттандыру құралдары жұмысында іркілістер тудыратын бағдарламалық-техникалық әсерлердің 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 ақпаратты ұстап қалу қондырғыларын (салынған қондырғыларды) анықтауға арнайы зерттеулер жүргізумен қол жеткізіледі.

Техникалық құралдардың сөз ақпаратын үй-жайлардан және объектілерден ұстап қалуын болдырмауға техникалық қорғау құралдарын, үй-жайлардың дыбыс өткізбеуін қамтамасыз ететін жобалау және конструкторлық шешімдерді, орнатылған ұстап қалу құралдарын анықтау және олардың белсенділігін азайту бойынша режимді үй-жайларды арнайы зерттеуді және басқа ұйымдастыру және режимдік іс-шараларды қолдану есебінен қол жеткізіледі.

Жалпы мемлекеттік ақпараттық және телекоммуникациялық жүйелерде ақпаратты қорғау жөніндегі негізгі ұйымдастыру-техникалық іс-шаралар мыналар болып табылады:

ақпаратты техникалық қорғау саласындағы ұйымдастыру 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;

ақпаратты 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;

ақпаратты 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;

ақпараттық-телекоммуникация жүйелерінде және жергілікті есептеуіш желілерінде ақпаратты рұқсат етілмеген қол жеткізуден және әсерден, компьютерлік вирустардың жұғуынан қорғауды ұйымдастыру;

есептеуіш техника құралдары объектілерінде жанама электромагнит сәулелері мен нысаналар есебінен өңделетін ақпараттың сыртқа кетуін болдырмау жөніндегі шараларды әзірлеу;

сенімді қорғауды қамтамасыз ету және объектінің қорғалатын аймағына рұқсатсыз кіру фактілерін анықтау үшін біріктірілген күзет жүйелерін, бейнебақылауды, ақпаратты жинау мен өңдеуді кешенді қолдана отырып, бірнеше күзету 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 кетуінен объектілерді қорғау тиімділігіне бақылау жүргізу;

объектілерге және техникалық құралдарға енгізілген электрондық ақпаратты ұстап қалу қондырғыларын (салынған қондырғыларды) анықтау жөнінде режимдік үй-жайларды арнайы зерттеу;

жергілікті есептеуіш желілерді ақпаратқа рұқсат етілмеген қол жеткізуден қорғау тиімділігіне бақылау жүргізу;

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

ақпараттық қауіпсіздікті қамтамасыз ету және арнайы мақсаттағы телекоммуникация желілерін жетілдіру саласын перспективалық дамыту мақсатында техникалық шешімдерді 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 және техникалық жарақтануы туралы ақпаратты жинау;

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

Қазақстан Республикасына қарсы ақпараттық қауіп көздерінің қолданатын іс-әрекеттері туралы ақпаратты алуға бағытталған қарсы барлау іс-шаралары;

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

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

Ақпаратты қорғаудың әдістері, тәсілдері және шаралары сыртқа кетуі, бұзылуы немесе жойылуы жағдайында мүмкін болатын 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 білімдерді қамтитын іргелі, іздестіру және қолданбалы ғылыми зерттеулердің нәтижелері;

құпиялылық мәртебесі әлі айқындалмаған және сондықтан Қазақстан Республикасының заңнамасында қамтылмайтын әрі шетелге сатылуы мүмкін патенттелмеген технологиялар, ноу-хау, модельдің өнеркәсіптік үлгілері мен эксперименттік жабдық;

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

Бұл саладағы қауіптерді жіктеу кезінде шетел мемлекеттерінің арнайы қызметтерінің және қылмыстық құрылымдардың өнеркәсіптік шпионажы мүмкіндігін зерделеуге ерекше назар аудару қажет.

Ғылыми және зияткерлік әлеуетті заңсыз беруді немесе пайдалануды болдырмау мақсатында таратудың әрбір нақты жағдайы немесе ғылыми-техникалық немесе технологиялық өнім үшін ұсынымдар тұжырымдайтын қоғамдық ғылыми кеңестер мен тәуелсіз сарапшылар институтын қамтитын қауіптердің көрсетілген объектілерге әсер етуінің ықтимал салдарларын бағалаудың жүйесі ұйымдастырылатын болады.

Мемлекет тарапынан қауіптерге қарсы әрекет етудің шынайы жолы осы саладағы заңнаманы және оны іске асыру тетіктерін үнемі жетілдіру болып табылады. Бұл саладағы қауіптердің алдын алу немесе залалсыздандыру жөніндегі, әсіресе ғылыми кадрларға қатысты бөлігіндегі көптеген іс-шаралар мемлекеттің әлеуметтік және экономикалық саясаты саласында жатыр.

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 басқалары;

жеке тұлғаның әлеуметтік және жеке бағдарлануы;

көбінесе адамдардың дүниетанымын айқындайтын мәдени және эстетикалық сұраныстар;

жеке тұлғаның психикалық саулығы.

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

Рухани өмір саласындағы ақпараттық қауіпсіздікке қауіптерді болдырмау және зазалсыздандыру ең алдымен, халықтың басым бөлігі үшін қолайлы әрі елде тұратын көптеген этностардың мүдделерін, мәдени және тарихи дәстүрлерін ескеретін, әзірленген мемлекеттік идеологияны талап етеді. Мұндай идеология негізінде ақпараттық қауіпсіздікке қатерлерді бағалаудың нақты өлшемдері, осы саладағы негізгі басымдықтар мен мемлекеттік саясат әзірленуі мүмкін.

Сонымен қатар, бұқаралық ақпарат құралдарын елдің ұлттық мүдделеріне жауап беретін рухани құндылықтарды қалыптастыруға және таратуға, азаматтық және патриоттық борышты тәрбиелеуге және оларды дүшпандық немесе достық емес насихаттан қорғауға тарту мақсатында оларға ықпал етудің өркениетті, демократиялық нысандары мен әдістерін әзірлеу және жүзеге асыру, оған қарсы дұрыс дәлелденген ақпаратты дереу жариялау, мұндай насихат көздерін, олардың алға қойған мақсаттарын , ықпал ету әдістерін мүлтіксіз ашу, қасақана енгізілген бұрмалауларды, насихаттау бағытындағы ақпараттағы жарым-жартылықты көрсету талап етіледі.

Трафикті зиянды және теріс ақпараттың болуын бақылау мақсатында Интернет саласын заңнамалық реттеу 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 мен ыдырайтын материалдардың заңсыз саудасына қарсы күрес жүргізетін халықаралық құқық қорғау ұйымдарындағы ақпаратқа рұқсат етілмеген қол жеткізуді болдырмау;

ақпарат алмасудың жаңа жүйелерін әзірлеу, технологиялық базаны жетілдіру және ақпараттық жүйелер мен ақпараттық ресурстардың ақпараттық қауіпсіздігі жүйелерін жасау жөніндегі бірлескен халықаралық жобаларды жасау.

Ынтымақтастық барысында шегінде сабақтас телекоммуникациялық жүйелер мен байланыс желілері пайдаланылатын бұрынғы КСРО аумағында біртұтас ақпараттық кеңістік құру перспективаларын ескере отырып, Тәуелсіз Мемлекеттер Достастығы елдерімен өзара іс-қимыл жасау проблемаларына ерекше назар аударылатын болады.

Ынтымақтастықтың көрсетілген бағыттарын іске асыру үшін:

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

ақпараттық қауіпсіздікті қамтамасыз ету саласында, оның ішінде халықаралық және отандық баспа шығарылымдары арқылы тәжірибе алмасу;

қазақстандық мамандардың халықаралық конференцияларға, семинарларға, көрмелерге қатысуын кеңейту қажет.

Баяндалған қағидаттар мен ережелер негізінде мемлекет қызметінің саяси, әскери, экономикалық және басқа да салаларындағы ақпараттық қауіпсіздік саясатын қалыптастыру мен іске асырудың жалпы бағыттары айқындалады.

Ақпараттық қатынастар субъектілерінің мүдделерін келісу және ымыралық шешімдер табу тетігі ретінде мемлекеттік саясат мамандар мен барлық мүдделі құрылымдардың кеңінен өкілдік етуімен, түрлі кеңестердің, комитеттер мен

комиссиялардың тиімді жұмысын қалыптастыруды және ұйымдастыруды көздейді.

Мемлекеттік саясатты іске асыру тетіктері икемді, елдің саяси және экономикалық өмірінде болып жатқан өзгерістерді уақтылы көрсететін болады.