"Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді ратификациялау туралы" Қазақстан Республикасы Заңының жобасы туралы

Қазақстан Республикасы Үкіметінің 2010 жылғы 28 қаңтардағы № 26 Қаулысы

Қазақстан Республикасының Үкіметі **ҚАУЛЫ ЕТЕДІ:**

«Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді ратификациялау туралы» Қазақстан Республикасы Заңының жобасы Қазақстан Республикасының Парламенті Мәжілісінің қарауына енгізілсін.

Қазақстан Республикасының

Премьер-Министрі К. Мәсімов

жоба

Қазақстан Республикасының Заңы Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді ратификациялау туралы

Екатеринбургте 2009 жылғы 16 маусымда қол қойылған Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісім ратификациялансын.

Қазақстан Республикасының

Президенті

Шанхай ынтымақтастық ұйымына мүше-мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы

КЕЛІСІМ

Бұдан әрі "Тараптар" деп аталатын, Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері,

жаһандық ақпараттық кеңістікті қалыптастыратын ең жаңа ақпараттық-коммуникациялық технологиялар мен құралдарды дамыту мен енгізудегі

айтарлықтай прогресті атап өте отырып,

азаматтық та, әскери де салаларда қолдануға болатын осындай технологиялар мен құралдарды халықаралық қауіпсіздік пен тұрақтылықты қамтамасыз ету міндеттеріне сәйкес келмейтін мақсаттарда пайдалану мүмкіндіктеріне байланысты қауіптерге алаңдаушылық білдіре отырып,

халықаралық қауіпсіздік жүйесінің түйінді элементтерінің бірі ретінде халықаралық ақпараттық қауіпсіздікке маңызды мән бере отырып,

халықаралық ақпараттық қауіпсіздікті қамтамасыз ету мәселелерінде Тараптардың сенімдерін одан әрі тереңдету мен өзара іс-қимылын дамыту қауырт қажеттілік болып табылатынына және олардың мүдделеріне жауап беретініне сенімді бола отырып,

адам мен азаматтың құқықтары мен негізгі бостандықтарын қамтамасыз етудегі ақпараттық қауіпсіздіктің маңызды рөлін назарға ала отырып,

БҰҰ Бас Ассамблеясының "Халықаралық қауіпсіздік тұрғысынан ақпараттандыру мен телекоммуникация саласындағы жетістіктер" атты қарарларын ескере отырып,

халықаралық ақпараттық қауіпсіздікке қауіпті шектеуге, Тараптардың ақпараттық қауіпсіздік мүдделерін қамтамасыз етуге және бейбітшілік, ынтымақтастық пен үйлесімділік тән болатын халықаралық ақпараттық орта құруға ұмтыла отырып,

халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы Тараптар ынтымақтастығының құқықтық және ұйымдық негіздерін жасауға ниет ете отырып,

төмендегілер туралы келісті:

1-бап
Негізгі ұғымдар

Осы Келісімді орындау барысында Тараптардың өзара іс-қимыл жасау мақсаты үшін осы Келісімнің ажырамас бөлігі болып табылатын 1-қосымшада («Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі ұғымдардың тізбесі») келтірілген негізгі ұғымдар пайдаланылады.

1-қосымша Тараптардың келісімі бойынша қажеттілігіне қарай толықтырылуы, нақтылануы және жаңартылуы мүмкін.

2-бап
Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі қауіптер

Тараптар осы Келісімге сәйкес ынтымақтастықты іске асыра отырып, халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мынадай негізгі қауіптердің болуын негізге алады:

1. Ақпараттық қаруды әзірлеу және қолдану, ақпараттық соғысты дайындау және

ж ү р г і з у ;

2. ақпараттық терроризм;

3. ақпараттық қылмыс;

4. ақпараттық кеңістіктегі үстем жағдайды басқа мемлекеттердің мүдделері мен қауіпсіздігіне залал келтіретіндей пайдалану;

5. басқа мемлекеттердің қоғамдық-саяси және әлеуметтік-экономикалық жүйелеріне , рухани, адамгершілік және мәдени орталарына залал келтіретін ақпаратты тарату;

6. ғаламдық және ұлттық ақпараттық инфрақұрылымдардың қауіпсіз, тұрақты жұмыс істеуіне табиғи және (немесе) техногендік сипаттағы қауіптер.

Осы бапта тізбектелген негізгі қауіптердің мәнін Тараптардың келісілген түсіністігі осы Келісімнің ажырамас бөлігі болып табылатын 2-қосымшада («Халықаралық ақпараттық қауіпсіздік саласындағы қауіп түрлерінің, олардың көздері мен белгілерінің т і з б е с і ») к е л т і р і л г е н ;

2-қосымша Тараптардың келісімі бойынша қажеттілігіне қарай толықтырылуы, нақтылануы және жаңартылуы мүмкін.

3-бап
Ынтымақтастықтың негізгі бағыттары

Осы Келісімнің 2-бабында баяндалған қауіптерді ескере отырып, Тараптар, олардың уәкілетті өкілдері және осы Келісімнің 5-бабына сәйкес айқындалатын Тараптар мемлекеттердің құзыретті органдардары халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласында мынадай негізгі бағыттар бойынша ынтымақтастықты ж ү з е г е а с ы р а д ы :

1) халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласында бірлескен қажетті шараларды айқындау, келісу және жүзеге асыру;

2) мониторинг және осы салада пайда болатын қауіптерге бірлесе әрекет ету ж ү й е с і н қ ұ р у ;

3) қорғаныс қабілеттілігіне, ұлттық және қоғамдық қауіпсіздікке қауіп төндіретін ақпараттық қаруды тарату мен қолдануды шектеу саласындағы халықаралық құқық нормаларын дамыту жөнінде бірлескен шараларды әзірлеу;

4) ақпараттық-коммуникациялық технологияларды терроризм мақсаттарында пайдалану қауіптеріне қарсы іс-қимыл;

5) ақпараттық қылмысқа қарсы іс-қимыл;

6) ақпараттық қауіпсіздікті қамтамасыз ету саласында осы Келісімнің мақсаттары үшін қажетті сараптамалар, зерттеулер және бағалаулар жүргізу;

7) Интернеттің ғаламдық желісін басқарудың қауіпсіз, тұрақты қызметін және интернационалдандыруды қамтамасыз етуге жәрдемдесу;

8) Тараптар мемлекеттердің аса маңызды құрылымдарының ақпараттық

қауіпсіздігін қамтамасыз ету;

9) халықаралық ақпараттық қауіпсіздікті қамтамасыз етуге жәрдемдесетін бірлескен сенім шараларын әзірлеу және жүзеге асыру;

10) трансшекаралық ақпарат алмасу кезінде электрондық цифрлық қолтаңбаны пайдалану мен ақпаратты қорғау мүмкіндіктерін іске асыру жөніндегі келісілген саясатты және ұйымдастыру-техникалық рәсімдерді әзірлеу және жүзеге асыру;

11) ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша Тараптар мемлекеттердің заңнамасы туралы ақпарат алмасу;

12) халықаралық ақпараттық қауіпсіздікті қамтамасыз етудегі Тараптар ынтымақтастығының халықаралық-құқықтық базасын және практикалық тетіктерін жетілдіру;

13) осы Келісімді іске асыру мақсатында Тараптар мемлекеттері құзыретті органдарының өзара іс-қимылы үшін жағдайлар жасау;

14) халықаралық ұйымдар мен форумдар шеңберінде халықаралық ақпараттық қауіпсіздікті қамтамасыз ету проблемалары жөнінде өзара іс-қимыл жасау;

15) ақпараттық қауіпсіздік саласында тәжірибе алмасу, мамандар даярлау, Тараптардың уәкілетті өкілдері мен сарапшыларының жұмыс бабындағы кездесулерін, семинарлары мен басқа да форумдарын өткізу;

16) осы бапта санамаланған негізгі бағыттар бойынша ынтымақтастықты жүзеге асыруға байланысты мәселелер бойынша ақпарат алмасу.

Тараптар немесе Тараптар мемлекеттерінің құзыретті органдары өзара уағдаластық бойынша ынтымақтастықтың басқа да бағыттарын айқындауы мүмкін.

4-бап
Ынтымақтастықтың жалпы принциптері

1. Осы Келісім шеңберіндегі ынтымақтастықты және халықаралық ақпараттық кеңістіктегі өзінің қызметін Тараптар мұндай қызмет әлеуметтік және экономикалық дамуға жәрдемдесетіндей және халықаралық қауіпсіздік пен тұрақтылықты қолдау міндеттеріне лайық болатындай, дау-жанжалдарды бейбіт жолмен реттеу, күш қолданбау, ішкі істерге араласпау, адамның құқықтары мен негізгі бостандықтарын құрметтеу принциптерін қоса алғанда, халықаралық құқықтың жалпыға бірдей принциптері мен нормаларына, сондай-ақ өңірлік ынтымақтастық пен Тараптар мемлекеттерінің ақпараттық ресурстарға араласпау принциптеріне сәйкес болатындай түрде жүзеге асырады.

2. Осы Келісім шеңберіндегі Тараптардың қызметі әрбір Тараптың ақпаратты іздеу, алу және тарату құқығымен сәйкес болуға тиіс, мұндай құқық ұлттық және қоғамдық қауіпсіздік мүдделерін қорғау мақсатында заңнамамен шектелуі мүмкін екендігі ескерілуге тиіс.

3. Әрбір Тарап өз мемлекетінің ұлттық ақпараттық ресурстарын және аса маңызды құрылымдарын заңға қайшы келетін пайдаланудан және рұқсатсыз араласудан, оның ішінде оларға ақпараттық шабуыл жасаудан қорғауға тең құқылы болады.

Әрбір Тарап басқа Тарапқа қатысты осыған ұқсас әрекет жүргізбейді және жоғарыда көрсетілген құқықты іске асыруда басқа Тараптарға жәрдем көрсетеді.

5-бап
Ынтымақтастықтың негізгі нысандары және тетіктері

1. Осы Келісім күшіне енген күнінен бастап алпыс күн ішінде Тараптар депозитарий арқылы осы Келісімді іске асыруға жауапты Тараптар мемлекеттерінің құзыретті органдар және ынтымақтастықтың нақты бағыттары бойынша тікелей ақпарат алмасу арналары туралы деректер алмасады.

2. Осы Келісімді орындау, ақпарат алмасу, ақпараттық қауіпсіздікке төнетін қауіптерді талдау және бірлесіп бағалау барысын қарау, сондай-ақ мұндай қауіптерге ден қоюдың бірлескен шараларын айқындау, келісу және үйлестіру мақсатында Тараптар тұрақты негізде Тараптардың уәкілетті өкілдерінің және Тараптар мемлекеттерінің құзыретті органдардың консультацияларын (бұдан әрі - консультациялар) өткізіп тұрады.

Кезекті консультациялар Тараптардың келісімі бойынша, әдеттегідей, жарты жылда бір рет Шанхай ынтымақтастық ұйымының Хатшылығында немесе Тараптардың бірінің шақыруымен оның мемлекетінің аумағында өткізіледі.

Тараптардың кез келгені өткізу уақыты мен орнын, сондай-ақ кейіннен барлық Тараптармен және Шанхай ынтымақтастық ұйымының Хатшылығымен келісу үшін күн тәртібін ұсына отырып, кезектен тыс консультациялар өткізуге бастамашылық ете алады.

3. Осы Келісімде көзделген ынтымақтастықтың нақты бағыттары бойынша практикалық өзара іс-қимылды Тараптар Келісімді іске асыруға жауапты Тараптар мемлекеттерінің құзыретті органдар желісі бойынша жүзеге асыра алады.

4. Нақты бағыттар бойынша ынтымақтастықтың құқықтық және ұйымдастырушылық негіздерін жасау мақсатында Тараптар мемлекеттерінің құзыретті органдары ведомствоаралық сипаттағы тиісті шарттар жасаса алады.

6-бап
Ақпаратты қорғау

1. Егер мұндай ақпаратты ашу ұлттық мүдделерге нұқсан келтіретін болса, осы Келісім ынтымақтастық шеңберінде Тараптарға ақпарат беру жөнінде міндеттемелер жүктемейді және осы ынтымақтастық шеңберінде ақпарат беру үшін негіз болып табылмайды.

2. Осы Келісімге сәйкес ынтымақтастық шеңберінде Тараптар мемлекеттерінің заңнамасына сәйкес мемлекеттік құпияға жататын ақпарат алмасуды Тараптар жүзеге асырмайды. Осы Келісімді орындау мақсаты үшін нақты жағдайларда қажетті деп саналуы мүмкін осыған ұқсас ақпаратты беру және онымен жұмыс істеу тәртібі Тараптардың арасындағы тиісті шарттардың негізінде және талаптары бойынша реттеледі.

3. Тараптар осы Келісімнің шеңберіндегі ынтымақтастық барысында берілетін немесе жасалатын, Тараптардың кез келген мемлекеттерінің заңнамасы бойынша мемлекеттік құпияға жатпайтын, оған қол жеткізу және оны тарату Тараптардың кез келген мемлекеттерінің ұлттық заңнамасына және (немесе) тиісті нормативтік-құқықтық актілеріне сәйкес шектелген ақпаратты тиісінше қорғауды қамтамасыз етеді.

Мұндай ақпаратты қорғау алушы Тараптың мемлекеттік заңнамасына және (немесе) тиісті нормативтік-құқықтық актілеріне сәйкес жүзеге асырылады. Бұл ақпараттың бастапқы дереккөзі болып табылатын Тараптың жазбаша келісімінсіз мұндай ақпарат ашылмайды және берілмейді.

Мұндай ақпарат Тараптардың мемлекеттік заңнамасына және (немесе) тиісті нормативтік-құқықтық актілеріне сәйкес тиісінше белгіленеді.

7-бап
Қаржыландыру

1. Осы Келісімді орындау жөніндегі тиісті іс-шараларға өз өкілдері мен сарапшыларының қатысуы жөніндегі шығыстарды Тараптар дербес көтереді.

2. Осы Келісімді орындауға байланысты басқа шығыстарға қатысты Тараптар әрбір жекелеген жағдайда Тараптар мемлекеттерінің заңнамасына сәйкес қаржыландырудың өзге тәртібін келісе алады.

8-бап
Басқа халықаралық шарттарға қатысы

Осы Келісім Тараптардың әрқайсысының оның мемлекеті қатысушысы болып табылатын басқа халықаралық шарттар бойынша құқықтары мен міндеттемелерін қозғамайды.

9-бап
Дауларды шешу

Осы Келісімнің ережелерін түсіндіруге немесе қолдануға байланысты туындауы мүмкін даулы мәселелерді Тараптар консультациялар және келіссөздер арқылы шешеді .

10-бап
Жұмыс тілдері

Осы Келісім шеңберіндегі ынтымақтастықты жүзеге асыру кезінде орыс және қытай тілдері жұмыс тілдері болып табылады.

11-бап
Депозитарий

Шанхай ынтымақтастық ұйымының Хатшылығы осы Келісімнің депозитарийі болып табылады.

Осы Келісімнің түпнұсқа данасы депозитарийде сақталады, ол оған қол қойылған күнінен бастап он бес күн ішінде Тараптарға оның куәландырылған көшірмелерін жібереді.

12-бап
Қорытынды ережелер

1. Осы Келісім белгіленбеген мерзімге жасалады және оның күшіне енуі үшін қажетті мемлекетішілік рәсімдерді Тараптардың орындағаны туралы жазбаша нысандағы төртінші хабарламаны депозитарий алған күнінен бастап отызыншы күні күшіне енеді. Мемлекетішілік рәсімдерді кеш орындаған Тарап үшін осы Келісім оның тиісті хабарламасын депозитарий алған күнінен бастап отызыншы күні күшіне енеді.

2. Өзара келісім бойынша Тараптар осы Келісімге жеке хаттамамен рәсімделетін өзгерістер ұсына алады.

3. Осы Келісім қандай да бір мемлекеттерге және ұйымдарға қарсы бағытталмаған және ол күшіне енгеннен кейін депозитарийге қосылу туралы құжат беру жолымен осы Келісімнің мақсаттары мен принциптерін бөлісетін кез келген мемлекеттің оған қосылуы үшін ашық. Осы Келісім қосылатын мемлекет үшін оған қол қойған және оған қосылған мемлекеттердің мұндай қосылуға келісетіні туралы соңғы жазбаша хабарламаны депозитарий алған күнінен бастап отыз күн өткен соң күшіне енеді.

4. Тараптардың әрқайсысы болжамды шығу күнінен кем дегенде тоқсан күн бұрын депозитарийге осы Келісімнен шығатыны туралы жазбаша хабарлама жіберу арқылы одан шыға алады. Осындай хабарламасын алған күнінен бастап отыз күн ішінде Депозитарий бұл ниет туралы басқа Тараптарға хабарлайды.

5. Осы Келісімнің қолданылуы тоқтатылған жағдайда, Тараптар ақпаратты қорғау

жөніндегі міндеттемелерді, Келісім шеңберінде жүзеге асырылатын және Келісімнің қолданылуы тоқтатылған сәтке аяқталмаған, бұрын келісілген бірлескен жұмыстарды, жобаларды және басқа да іс-шараларды толық орындау шараларын қабылдайды.

2009 жылғы 16 маусымда Екатеринбург қаласында орыс және қытай тілдерінде бір түпнұсқа данада жасалды, әрі екі мәтіннің де бірдей күші бар.

Қазақстан Республикасының Үкіметі үшін

Қытай Халық Республикасының Үкіметі үшін

Қырғыз Республикасының Үкіметі үшін

Ресей Федерациясының Үкіметі үшін

Тәжікстан Республикасының Үкіметі үшін

Өзбекстан Республикасының Үкіметі үшін

Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімге
1-ҚОСЫМША

Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі ұғымдардың ТІЗБЕСІ

«Ақпараттық қауіпсіздік» - тұлғаның, қоғам мен мемлекеттің және олардың мүдделерінің ақпараттық кеңістіктегі қауіптерден, ыдыратушылық және өзге де келеңсіз әсерлерден қорғалу жағдайы;

«ақпараттық соғыс» - ақпараттық жүйелерге, процестер мен ресурстарға, аса маңызды және басқа да құрылымдарға залал келтіру, саяси, экономикалық және әлеуметтік жүйелерге нұқсан келтіру, қоғам мен мемлекетті тұрақсыздандыру үшін халық арасында жаппай психологиялық өңдеу жүргізу, сондай-ақ мемлекетті тайталасушы тараптың мүдделеріне сай шешім қабылдауға мәжбүрлеу мақсатында ақпараттық кеңістіктегі екі және одан да көп мемлекеттер арасындағы тайталас;

«ақпараттық инфрақұрылым» - ақпаратты қалыптастырудың, түзудің, қайта тузудің, берудің, пайдалану мен сақтаудың техникалық құралдары мен жүйелерінің жиынтығы;

«ақпараттық қару» - ақпараттық соғыс жүргізу мақсатында қолданылатын ақпараттық технологиялар, құралдар және әдістер;

«ақпараттық қылмыс» - ақпараттық кеңістікте заңға қайшы келетін мақсаттарда ақпараттық ресурстарды пайдалану және (немесе) оларға әсер ету;

«ақпараттық кеңістік» - ақпаратты қалыптастыруға, түзуге, қайта түзуге, беруге, пайдалануға, сақтауға байланысты, оның ішінде жеке және қоғамдық санаға, ақпараттық инфрақұрлымға және ақпараттың өзіне әсер ететін қызмет саласы;

«ақпараттық ресурстар» - ақпараттық инфрақұрылым, сондай-ақ ақпараттың өзі және оның ағымдары;

«ақпараттық терроризм» - ақпараттық кеңістікте терроризм мақсатында ақпараттық ресурстарды пайдалану және (немесе) оларға әсер ету;

«аса маңызды құрылымдар» - оларға әсер ету тұлғаның, қоғамның және мемлекеттің қауіпсіздігін қоса алғанда, тікелей ұлттық қауіпсіздікті қозғайтын салдарларға әкеп соғуы мүмкін мемлекеттің объектілері, жүйелері мен институттары;

«халықаралық ақпараттық қауіпсіздік» - ақпараттық кеңістікте әлемдік тұрақтылықты бұзуды және мемлекеттер мен әлемдік қоғамдастықтың қауіпсіздігіне қауіп тудыруды болдырмайтын халықаралық қатынастар жағдайы;

«ақпараттық ресурстарды заңсыз пайдалану» - ақпараттық ресурстарды тиісті құқықсыз немесе белгіленген ережелерді, Тараптар мемлекеттерінің заңнаманы немесе халықаралық құқық нормаларын бұза отырып пайдалану;

«ақпараттық ресурстарға рұқсатсыз араласу» - ақпаратты қалыптастыру, түзу, өңдеу, қайта түзу, беру, пайдалану және сақтау процестеріне заңсыз ықпал ету;

«ақпараттық қауіпсіздікке қауіп төнуі» - ақпараттық кеңістікте тұлғаға, қоғамға, мемлекетке және олардың мүдделеріне қауіп туғызатын факторлар.

Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімге
2-ҚОСЫМША

Халықаралық ақпараттық қауіпсіздік саласындағы негізгі қауіп түрлерінің, олардың көздері мен белгілерінің ТІЗБЕСІ

1. Ақпараттық қаруды әзірлеу және қолдану, ақпараттық соғысқа дайындалу және оны жүргізу.

Қауіптердің шығу көзі мемлекеттердің аса маңызды құрылымдары үшін тікелей қауіп төндіретін ақпараттық қаруды жасау және дамыту болып табылады, бұл қайтадан

жанталаса қаруланууға алып келуі мүмкін және халықаралық ақпараттық қауіпсіздік саласына басты қауіп төндіреді.

Оның белгілері ақпараттық соғысқа дайындалу әзірлеу және оны жүргізу, сондай-ақ тасымалдау, коммуникациялар және қорғаныс объектілерінің әуе, зымыранға қарсы және басқа да түрлерін басқару жүйелеріне әсер ету мақсатында ақпараттық қаруды қолдану, соның нәтижесінде мемлекет басқыншының алдында қорғаныс қабілетін жоғалтады және өзін өзі қорғаудың заңды құқығын пайдалана алмайды; ақпараттық инфрақұрылымдар объектілерінің жұмыс істеуін бұзу, соның нәтижесінде мемлекеттерде басқару және шешімдер қабылдау жүйесі істен шығады, аса маңызды құрылымдарға ыдыратушылық әсер ету болып табылады.

2. Ақпараттық терроризм

Терроризмдік қызметке қатысы бар, өздерінің заңсыз іс-қимылдарын ақпараттық ресурстар арқылы немесе соларға қатысты жүзеге асыратын террорлық ұйымдар мен тұлғалар қауіп көзі болып табылады.

Оның белгілері террорлық қызметті жүзеге асыру және өз қатарларына жаңа жақтастар тарту үшін террорлық ұйымдардың ақпараттық желілерді пайдалануы; ақпараттық ресурстарға қоғамдық тәртіпті бұзуға әкеп соғатын ыдыратушылық әсер ету; бұқаралық ақпарат беру арналарын бақылау немесе оқшаулау, терроризмді насихаттау, қоғамда үрей мен дүрбелең ахуалын қалыптастыру үшін Интернетті немесе басқа да ақпараттық желілерді пайдалану, сондай-ақ ақпараттық ресурстарға басқа да теріс ықпал ету болып табылады.

3. Ақпараттық қылмыс

Ақпараттық ресурстарды заңсыз пайдалануды немесе қылмыстық мақсатта мұндай ресурстарға санкциясыз араласуды жүзеге асыратын тұлғалар немесе ұйымдар қауіп көзі болып табылады.

Оның белгілері ақпараттың тұтастығын, қол жетімділігін және құпиялылығын бұзу үшін ақпараттық жүйеге кіру; компьютерлік вирустарды және басқа да зиян келтіретін бағдарламаларды қасақана дайындау және өзге де; DOS-шабуыл (қызмет етуден қабыл алмау) және өзге де теріс әсер етуді жүзеге асыру; ақпараттық ресурстарға залал келтіру; азаматтардың ақпараттық саладағы заңды құқықтары мен бостандықтарын, оның ішінде зияткерлік меншік және жеке өмірге қол сұғылмаушылық құқығын бұзу; алаяқтық, ұрлық, бопсалау, контрабанда, есірткінің заңсыз саудасы, балалар порнографиясын тарату және т.б. секілді қылмыстар жасау үшін ақпараттық ресурстар мен әдістерді пайдалану болып табылады.

4. Ақпараттық кеңістіктегі үстем жағдайды басқа елдердің мүдделері мен қауіпсіздігіне нұқсан келтіріп пайдалану

Түрлі мемлекеттердегі ақпараттық технологияларды дамытудағы әркелкілік пен дамыған және дамушы елдердің арасындағы "цифрлық алшақтықты" арттыруға деген ағымдағы үрдіс қауіп көзі болып табылады. Ақпараттық технологияларды дамытуда

артықшылығы бар бірқатар мемлекеттер өзге елдердің дамуын және ақпараттық технологияларға қол жетімділікті қасақана шектейді, бұл ақпараттық мүмкіндіктері жеткіліксіз мемлекеттер үшін айтарлықтай қауіптің туындауына алып келеді.

Оның белгілері бағдарламалық қамтамасыз ету және ақпараттық инфрақұрылымдар жабдықтарының өндірісін монополияландыру, мемлекеттердің дамуына кедергі келтіретін және бұл елдердің неғұрлым дамыған мемлекеттерге тәуелділігін арттыратын халықаралық ақпараттық-технологиялық ынтымақтастыққа олардың қатысуын шектеу. Бұл елдердің ақпараттық ресурстарына және (немесе) аса маңызды құрылымдарына бақылау жасау және ықпал ету үшін басқа елдерге жеткізілетін бағдарламалық қамтамасыз ету мен жабдыққа жасырын мүмкіндіктер мен функцияларды орнату; мемлекеттердің мүдделері мен қауіпсіздігіне залал келтіре отырып, ақпараттық технологиялар мен өнімдер нарығын бақылау және монополияландыру болып табылады.

5. Басқа мемлекеттердің қоғамдық-саяси және әлеуметтік-экономикалық жүйелеріне, рухани, адамгершілік және мәдени ортасына нұқсан келтіретін ақпарат тарату

Басқа мемлекеттердің қоғамдық-саяси және әлеуметтік-экономикалық жүйелеріне, рухани, адамгершілік және мәдени ортасына нұқсан келтіретін ақпарат тарату үшін ақпараттық инфрақұрылымды пайдаланатын мемлекеттер, ұйымдар, адамдар тобы немесе жеке адам қауіп көзі болып табылады.

Оның белгілері электрондық (радио және телевизия) және өзге де бұқаралық ақпарат құралдарында, Интернетте және басқа да ақпарат алмасу желілерінде:

мемлекеттегі саяси жүйе, қоғамдық құрылыс, ішкі және сыртқы саясат, маңызды саяси және қоғамдық процестер, оның халқының рухани, адамгершілік және мәдени құндылықтары туралы түсінікті бұрмалайтын;

терроризм, сепаратизм және экстремизм идеясын насихаттайтын;

ұлтаралық, нәсіларалық және конфессияаралық өшпенділікті тұтататын ақпараттың пайда болуы және таралымға шығарылуы болып табылады.

6. Жаһандық және ұлттық ақпараттық инфрақұрылымдардың қауіпсіз, тұрақты жұмыс істеуіне табиғи және/немесе техногенді сипаттағы қауіптер

Аяқ астынан немесе ұзақ процесс нәтижесінде пайда болатын мемлекеттің ақпараттық ресурстарына ауқымды қиратқыш әсер етуге қабілетті табиғи апаттар және басқа да қауіпті табиғи құбылыстар, сондай-ақ техногенді сипаттағы апаттар қауіп көзі болып табылады.

Оның белгілері ақпараттық инфрақұрылым объектілері жұмысының бұзылуы және соның салдарынан нәтижелері мемлекет пен қоғамның қауіпсіздігін тікелей қозғайтын аса маңызды құрылымдарды, басқарудың және шешім қабылдаудың мемлекеттік жүйелерін тұрақсыздандыру болып табылады.

Екатеринбургте 2009 жылғы 16 маусымда қол қойылған Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтасу туралы Шанхай ынтымақтастық ұйымына мүше-мемлекеттердің үкіметтері арасындағы Келісімнің аутентикалық көшірмесі екенін растаймын.

Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті
Төраға аппараты басшысының
міндеттерін уақытша атқарушы *Ә. Дүйсебаев*