ӘОЖ 004 (510)

Беков Қ.Б.

Әл-Фараби атындағы Қазақ ұлттық университеті,
Қазақстан Республикасы, Алматы қ.
E-mail:bekov.kairat@gmail.com

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ЭКОНОМИКАЛЫҚ ӨЛШЕМІ: ҚХР МЫСАЛЫ

Интернеттің кең таралуы мемлекеттің ақпараттық қауіпсіздігін сақтау мәселесінің жаңа міндеттерін тудырып отыр. Интернет технологиялары мен қосымша құны жоғары болып табылатын телекоммуникациялық индустрия үлкен қарқынмен өсіп келеді де оларды пайдаланушылар саны көбейген сайын жаңа ақпараттық ортаның социеталды әсерлері де күшеймек. Ақпараттық-коммуникациялық технологиялардың жаңалығы оларға байланысты қауіп-қатерлер туралы қоғамдағы білімнің аздығы, жауапкершілік пен қауіпсіздік шараларын қолдану қажеттігін түсіну, ақпаратты қорғау шараларының әлсіздігіне байланысты көптеген проблемаларды күн тәртібіне қойып отыр. Веб-сайттарды шабуылдау, пайдаланушылардың жеке ақпаратын ұрлау секілді оқиғалар өмірдің үйреншікті көріністеріне айналып барады.

Жеке және коммерциялық ақпаратты қорғау мәселесі қазіргі кезде тиімді басқару мен реттеу жүйесінің жоқтығы, заңнамадағы кемшіліктерге байланысты өз шешімін таба алмай отыр. Қытайдың экономикалық ақпарат қауіпсіздігін сақтаудағы қиындықтарының түрлі себептері бар. Біріншіден, осы саладағы стратегиялық бағдарламлардың жоқтығы. Технологиялардың тез қарқынмен дамуы мен мемлекеттік органдарға тән шешім қабылдаудағы баяулығы қорғау объектілері, қауіп-қатер көздері мен түрлері және оларға қарсы қолданылатын шаралар бойынша жан-жақты және ұзақ мерзімді жоспарлауды қиындатып отыр. Екіншіден, мемлекеттің ақпараттық қауіпсіздікті қамтамасыз ету үшін пайдаланып отырған нормативтік негізі мен институттары әлі де толығымен қалыптаспаған. Қорғаныс немесе құқық қорғау институттарымен салыстырғанда ақпараттық қауіпсіздікті сақтау мекемелері жаңадан құрыла бастап, олардың қызметінде нақты жүйе мен тәжірибе жаңадан қалыптасып келе жатыр. Сонымен бірге, ақпараттық қауіпсіздік институттарының мемлекеттік жүйедегі алатын орны да нақты анықталмаған. Ақпараттық-коммуникациялық технологиялардың әмбебаптық табиғаты оларға қатысты қауіпсіздік механизмдерін орталықтандыру немесе диверсификациялау мәселесін тудырып отыр. Ақпараттық қауіпсіздіктің әскери және азаматтық өлшемдері болуы мүмкін, немесе саяси, экономикалық, әулеметтік аспектілерін де бөліп көрсетуге болады. Көп аспек-

тілі мәселені шешу қажеттігі жағдайында нақты шаралар жоспарын тез арада қабылдау мен іске асыру мемлекет үшін өте қиын мәселеге айналуы мүмкін.

Қазіргі кезде ҚХР-ның азаматтық саладағы (яғни әскери, идеологиялық немесе геосаяси сұрақтардан тыс) ақпараттық қауіпсіздікті қамтамасыз ету саясатының мотивтері, қатысушылары, нәтижелері бойынша зерттеулер аз болғанымен жанама деректер арқылы осы мәселе бойынша біраз ақпарат алуға болады.

Экономикадағы ақпараттық қауіпсіздікті қамтамасыз етудегі басты қиындықтардың бірі ретінде мемлекет басшылығының басқа да көкейтесті, тез арада шешімін табуды талап етіп отырған мәселелерге көңілі ауып, осы саладағы стратегиялық шешімдер саяси деңгейде емес, бюрократиялық деңгейде қалып отырғандығын айтуға болады. Осының салдарынан бір-бірімен бәсекелесіп отырған бюрократиялық құрылымдар ақпараттық қауіпсіздік саласындағы стратегиялық шешімдерді қабылдауға кедергі болып отыр.

Ақпараттық қауіпсіздік саласындағы келесі бір мәселе – осы саладағы техникалық кадрлардың үстемдігі мен одан шығып отырған технократиялық философия. Мемлекеттің ақпараттық қауіпсіздігі саласындағы технократиялық бағыттың басты кемшілігі ретінде олардың техникалық мәселелерге шоғырланып, проблеманың экономикалық немесе саяси аспектілеріне аз көңіл аударатындығында жатыр. Осының бәрі экономикадағы ақпарат қауіпсіздігін қамтамасыз етудегі координация мен стратегиялық жоспарлауды басқара алатын саяси көшбасшылықты қажет етіп отыр. Мұндай жағдай Қытайға ғана тән емес. АҚШ секілді ақпараттық технологиялар жағынан дамыған мемлекеттер де дәл осындай қиындықтарға душар болып отыр [1].

Қытайдың экономика саласындағы және жалпы ақпараттық қауіпсіздігін қамтамсыз ету процесіне қатысушылар қатарына ҚКП, үкіметтік құрылымдар, армия, ғылыми қауымдастық, инфрақұрылым операторлары мен ақпараттық-коммуникациялық индустрия өкілдерін қосуға болады. Бұл жердегі Қытайдың бір ерекшелігі – ақпараттық технологиялар мен олардың қауіпсіздігі бойынша шешімдер партия мен Мемлекеттік кеңестің құрамындағы «шағын топтар» ішінде қабылданып отырады. Алғашқы шағын топ болып 1993 жылы мемлекеттік ақпараттық-коммуникациялық технологияларды дамыту саясаты бойынша Мемлекеттік информатизация тобы құрылады. 2001 жылы бұл топ қайта құрылып, оның күнделікті қызметтері Мемлекеттік кеңестің информатизация бойынша басқармасына беріледі. Ал 2008 жылы Мемлекеттік информатизация тобы таратылады. Нақты ақпараттық қауіпсіздіктің технологиялық аспектілерімен Мемлекеттік информатизация тобының ішінде 2002 жылы құрылған мемлекеттік желілер мен ақпараттық қауіпсіздік бойынша «координациялық топ» айналысқан болатын. Осы топтың бастамасымен ҚХР-ның экономикадағы ақпараттық қауіпсіздікті қамтамсыз етудегі басты стратегиялық және реттеуші құжаттары қабылданады. Олардың ішінде 2003 жылы қабылданған «27-ші құжат» ҚХР басшылғының ақпараттық қауіпсіздікке байланысты саяси ұстанымдарын белгілеген болатын [2]. Сонымен қатар бұл топ мемлекеттің ақпараттық қауіпсіздік саласындағы басқа да көптеген стратегиялары мен саясатын анықтаған болатын, олардың ішінде: көп деңгейлі қорғаныс схемасы, міндетті сертификация талаптары, электрондық үкімет қауіпсіздігі, сенімді желілер, ақпараттық қауіпсіздік стандарттары мен ақпараттық қауіпсіздікті қамтамасыз ету бойынша 5 жылдық жоспар [1].

Бұл топ стратегиялық жоспарлау бойынша өз міндетін орындағаннан кейін 2008 жылы таратылып, 2009 жылы қайта құрылған болатын. Бірақ енді оның функциялары бойынша ашық ақпарат өте аз. Топ дайындаған стратегиялық бағыттар бойынша ағымдық жұмыс басқа орындаушы органдарға жүктелген. Олардың арасында Қоғамдық қауіпсіздік министрлігін айтуға болады. Бұл мекеме ақпараттық қауіпсіздіктің кибер-қылмыстармен күресу мен өмірлік маңызы бар ақпараттық инфрақұрылымды қорғау функцияларына жауапты. Осы міндеттерді атқару үшін министрлік бүкіл Қытайды қамтитын зерттеу лабораториялар жүйесін басқарып отыр. Мемлекеттік шифрлеу бюросы (немесе Қытай коммунистік партиясының Орталық бөлімінің құпия бюросы, Орталық криптографиялық комиссия ретінде де белгілі) партия, қарулы күштер мен азаматтық саладағы шифрлеу ісін басқарады (барлау криптографиясымен айналыспайды). Мемлекеттік құпиялар бюросы (немесе партия хатшылығының құпия ақпаратты сақтау бөлімі) құпия желілер үшін жауапты және 2009 жылы мемлекеттік құпия бойынша жаңа заң қабылданғаннан бері бұл ұйымның белсенділігі едәуір артқан болатын [1].

Қытай спецификасына сай армия экономиканың басқа да салаларындағыдай ақпараттық қауіпсіздікте басты акторлардың бірі болып келеді. Қарулы күштер құрамында ақпараттық

қауіпсіздік бойынша жұмыс Қытай халық азаттық армиясының Бас штабының бөлімшелерінде (3, 4, шифрлеу бөлімдері мен мемлекеттік құпиялар бөлімі) іске асырылады [1].

Профильді министрліктерге келетін болсақ ақпараттық қауіпсіздік үшін Индустрия мен ақпараттық технологиялар министрлігі жауапты болып табылады. Бұл министрліктің құрамындағы Ақпараттық қауіпсіздік бойынша координациялық департамент телекоммуникация және интернет қауіпсіздігін қамтамасыз ету бағытында қызмет атқарып отыр [1].

Жоғарыда аталған мемлекеттік құрылымдар ақпараттық қауіпсіздіктің технологиялық және инфрақұрылымдық аспектілері үшін жауапты екендігін есте сақтау қажет. Электрондық контентті реттеу мен қауіпсіздік шараларын 1-тарауда аталып өткен қытай коммунисттік партиясының Орталық пропаганда бөлімі мен Мемлекеттік радио, кино және теледидар басқармасы айналысады.

Атқарушы органдардың арасында Мемлекеттік қауіпсіздік министрлігін атап өту қажет. Бұл барлау қызметінің ақпараттық қауіпсіздік саласындағы қызметі бойынша толыққанды ақпарат аз болғанымен бұл мекемені кем дегенде техникалық жағынан ең дамыған және қабілетті деп санауға болады. Мемлекеттік қауіпсіздік министрлігінің ішінде ақпараттық қауіпсіздік мәселелерімен 13-ші бюро, ғылыми-техникалық бюро мен Қытайдың ақпараттық технологиялар қауіпсіздігін сертификациялау орталығы шұғылданады [1].

Ақпараттық қауіпсіздіктің экономикалық секторының кадрлық потенциалына келетін болсақ бұл сфераның элитасын ҚХР басшылығының аналогиясы бойынша «бірінші ұрпақтағы» мамандар құрайды. Олардың басым көпшілігі Қытай инженерлік академиясы мен Қытай ғылым академиясынан шыққан, техникалық тұрғыдан білікті мамандар болып табылады. Қазіргі кадрлар осы ғалымдар/мамандардың жетекшілігімен білім алып немесе ғылыми-зерттеу жұмысымен айналысқан болатын. Ақпараттық қауіпсіздік саясатын анықтауға жауапты мамандардың көбінесе ғылыми-зерттеу жұмысымен айланысып, академиялық немесе техникалық ортадан шыққандығына байланысты олардың саяси немесе экономикалық проблемалар бойынша білімі мен тәжиірбесі аз деуге болады.

Ақпараттық қауіпсіздіктің экономикалық саласындағы стратегия 2003 жылы шыққан «27-ші құжат: Ақпараттық қауіпсіздікті нығайту жұмысы бойынша ой-пікірлер» атты документте көрсетілген болатын. Ол бойынша қауіпсіздікті қамтамасыз етуде «белсенді қорғаныс» принципі басшылыққа алынып, инфраструктураны қорғау, криптография, динамикалық мониторинг, отандық инновациялар, кадрларды дамыту, басқару мен қаржыландыру сұрақтары бойынша саясаттың негіздерін қалаған болатын. [2] 27-ші құжаттың оң әсерімен қатар теріс салдары да болды. Мысалы, құжатта бірыңғай координациялық органның анықталмағандығы түрлі бюрократиялық құрылымдар арасында антагонистік қарым-қатынастар жүйесін қалыптастырады. Бір мекеменің бастамасы басқаларымен қақтығыс тудырып, жаңа құрылған органдардың қызметі қарсылық пен кедергілерге кезігіп отырды.

Мемлекеттік информатизация тобы мен Мемлекеттік кеңестің апараттандыру бөлімдері ақпараттық қауіпсіздік саясатының негіздерін қалағанымен, олардың 2008 жылы таратылуы осы салада бытыраңқылыққа алып келген болатын. Осындай децентрализацияланған саяси бастамалардың арасындағы негізгілері:

- Көп деңгейлі қорғаныс схемасы – Қытайдың өмірлік маңызы бар ақпараттық инфрақұрылымын қорғау талаптары мен ережелері. Бұл ережелерді жүзеге асырудың арқасында ақпараттық қауіпсіздіктің өндірістік (индустриалдық) негізі қаланған болатын;

- Ақпараттық өнімдердің қауіпсіздігін анықтау – ақпараттық технология өнімдерінің қауіпсіздігін тексеру жүйесі. Ақпараттық қауіпсіздікке жауапты әрбір мемлекеттетік органның өзінің қауіпсіздікті сертификациялау жүйелері бар (Қоғамдық қауіпсіздік министрлігінің үшінші ғылыми зерттеу институты, Қытайдың ақпартық технологиялар қауіпсіздігін бағалау орталығы, әскер бөлімшелері). Осының салдарында кейбір ірі экономикалық акторлар ақпараттық қауіпсіздік бойынша барлық органдардың тексерісі мен сертификациясынан өтуге мәжбүр болып отыр. Осы жүйе кемшіліктерінің тағы бір мысалы ретінде қытайлық интернет өнімдерде мәліметтермен алмасу қауіпсіздігін қамтамасыз ететін «https» механизмінің қолданылмауын келтіруге болады. Жаңадан құрылған Қытайдың сертификация және аккредитация басқармасы 2004-2008 жылдары аралығында бірыңғай тексеріс пен сертификация стандарттарын енгізуге ұсынғанымен басқа органдардың қарсылығының салдарынан бұл бастама өз жалғасын таппай отыр.

- Шифрлеу саясаты 1999 жылғы «Мемлекеттік шифрлеуді басқару комиссиясының» құрылуымен бірге орталықтандырылған болатын. Комиссия көбінесе үкімет пен партия қызметіне

қатысты элекрондық қолтаңбаларды шифрлеудің отандық схемаларын дамыту мен сертификация бойынша басқару мен реттеу функцияларын атқарады.

- Ақпараттық қауіпсіздік саласындағы қауіп-қатерлерді бағалау осы саладағы мемлекеттік саясатынан тыс қалып, қазіргі кезде бұл мәселелер Ұлттық даму мен реформа комиссиясының құрамындағы Мемлекеттік ақпараттық орталықтың қарамағында болып отыр.

- Ақпараттық қауіпсіздік стандарттары бойынша жұмыс қауіпсіздік органдарының өкілдерінен құралған Ақпараттық қауіпсіздік стандарттары бойынша Қытайдың ұлттық техникалық комитетімен іске асырылады. Бұл комитеттің жұмысы шетелдік қатысушылар үшін жабық және Қытай коммуникациялық стандарттар ассоциациясымен тығыз байланысты.

- ақпараттық технологиялар бойынша ғылым-зерттеу жұмыстары Ғылым мен технология министрлігі, Ұлттық даму мен реформа комиссиясы және Қытай ғылым академиясының құрамында жүзеге асырылады. Осы саладағы ғылыми-зерттеу жұмыстары «Жоба 973», «Жоба 863», «Үлкен жобалар» мен Ұлттық даму мен реформа комиссиясының Индустриялық даму қорының құрамына қосылған [3], [4], [1]. Сонымен қатар Қытай ғылым академиясының ішінде Ақпараттық қауіпсіздік лабораториясы қызмет етуде.

2008 жылы Мемлекеттік кеңестің ақпараттандыру бөлімінің таратылуынан кейінгі ақпараттық қауіпсіздік саласындағы саясат орталықтанбаған, пассивті реакция түрінде өткен болатын. Осы кезеңдегі ақпараттық қауіпсіздік бойынша келесі шаралар жүзеге асқан болатын: SCADA жүйелерінің қауіпсіздігі, электрондық үкімет жүйелерінің қауіпсіздігі, сенімді желілерді өзара байланыстыру, ботнеттермен күрес пен телекоммуникация қауіпсіздігі.

Ақпараттық өнімдер мен коммуникациялар қауіпсіздігін растау бойынша координация мен даму деңгейі әлі де болса төмен болып отыр. Осы салада ең үлкен жетістіктерге әзірше Мемлекеттік қауіпсіздік бюросы жеткен болатын. Бұл бюро қызметінің фокусы «құпия жүйелерде» шоғырланып, оның басшысы 2009 жылы вице-министрлік деңгейге көтеріледі де 2011 жылы компьютерлік қауіпсіздік бойынша университет мәртебесі бар мемлекеттік құпия бойынша ғылыми-зерттеу институттарын ашып отыр. Осыдан көріп отырғанымыздай қазіргі Қытайдың ақпараттық қауіпсіздіктің экономикалық өлшемінде мемлекеттік саясат децентрализацияланған болып келеді. Қауіпсіздік мәселелері жекелеген органдардың арасында бөлініп, орталық координациялаушы құрылым қажет болып отыр. Осындай ортада Индустрия мен ақпараттық технологиялар министрлігінің қызметі Мемлекеттік кеңес деңгейінде жаңа атқарушы орган қызметімен толықтырылуы қажет болуы мүмкін.

Қытайдағы онлайн бизнес пен виртуалдық қызметтердің өсуі елдегі ақпараттық кеңістіктің және осы кеңістікте әрекет ететін адамдар санының елеулі түрде өсуіне алып келген болатын. Дегенмен Қытай азаматтары мен компаниялары олардың табысы мен ақпаратына төніп отырған түрлі қауіп-қатерлерге душар болуда. Осы ақпараттық қатерлердің көзі ретінде виртуалдық сипаттағы және түрлі ақпараттық технологияларды кең қолданып отырған ауқымы зор заңсыз экономика жатыр. Ақпараттық кеңістіктегі заңсыз экономика ғаламдық мәселеге айналып келе жатқанымен Қытайдың бұл тұста өзіне тән ерекшеліктері бар. Бұл ерекшеліктер ҚХР-ның Батыс елдеріне қарағандағы экономикалық, саяси, құқықтық және мәдени өзгешеліктерінде жатыр. Виртуалды қылмыстық экономика мәселесі әлі де болса аз зерттелген проблема болып келеді. Оның ішінде әсіресе виртуалдық заңсыз нарықтың көлемін өлшеу, кибер қылмыстың технологиялық және коммуникативті аспектілеріне қатысты эмпирикалық зерттеулер аз болғанымен осы мәселенің кейбір жақтары бойынша ақпарат алуға болады.

Заңсыз экономиканы құрылымдық жағынан сараптаудың негізінде осы нарықтағы басты ойыншылар мен олардың қолданатын технологияларын және пайда табу жолдарын анықтауға болады. Жалпы виртуалды қылмыс арқылы пайда табудың төрт басты жолы бар. Олар:

- ақша ұрлау: ұрланған кредиттік карталар мен банктағы шоттардан ақша шығару;

- виртуалды ақша ұрлау: виртуалды ақша немесе интернеттегі ойыншылардың аккаунттарынан олар сатып алған виртуалды тауарларды ұрлау мен сату;

- интернет қызметтері мен ресурстарын заңсыз пайдалану: интернеттегі ресурстар мен қызметтерден ақпарат ұрлау үшін серверлер, сайттар мен смартфондарға бұзып кіру, пайда табу үшін интернет қызметтерін заңсыз пайдалану;

- Заңсыз ақпарат пен технологияларды тарату немесе сату: шабуылдау құралдарын және трояндық бағдарламаларды сату, қылмыскерлерге техникалық қолдау көрсету мен оларды дайындау.

Қытайлық зерттеушілердің құрылымдық сараптау негізінде жүргізген санағы бойынша 2011 жылы қылмыстық экономиканың ҚХР азаматтары мен компанияларына әкелген шығыны 5,36 млрд юань (0,852 млрд АҚШ долл) құрап, олардан зардап шеккен қытайлық пайдаланушылардың саны 110,8 млн адамға (барлық пайдаланушылардың 22%) жеткен болатын. Ал шабуылға ұшыраған сайттардың саны 1,1 миллионға жетті (барлық сайттардың 20%) [5].

Осы зерттеудің нәтижелері бойынша интернеттегі заңсыз нарықтың өте жоғары өсу деңгейін көрсетіп отыр. 2011 жылы түрлі форумдар мен чаттардағы заңсыз сауда операцияларына кем дегенде 90 000 адам қатысып, олар 80 000 тақырыпқа байланысты 320 000 астам хабарлама жіберген болатын [5].

Осындай қылмыстарға қарсы күрестің бірден бір жолы ретінде қытайлық мамандар интернеттегі заңсыз әрекеттердің тұрақты мониторингін ұсынып отыр. Қылмыскерлер бір бірімен байланысқа шығу үшін және заңсыз тауарлар туралы хабарлама беру үшін көбінесе бұқаралық ресурстарды (форумдар, әлеуметтік желілер) пайдаланады. Осындай бұқаралық ресурстардың қызметіне қатысушылардың лақап аттары немесе желілік адрестерін бақылау немесе олардың виртуалдық жүріс-тұрысын сараптау құқық қорғау органдарына жасалған қылмыстармен ғана күресіп қоймай олардың алдын алуға да мүмкіндік бере алады [5].

Ақпараттық технологиялар дамуының тағы бір маңызды әсері ретінде мемлекеттегі инновациялық белсенділікті келтіруге болады. Инновациялар мен ақпараттық қауіпсіздік арасындағы арақатынас бір жақтан қарағанда анық емес болуы мүмкін. Бірақ басқа жағынан алып қарағанда қауіпсіздік мүдделерінің көп жағдайда инновациялардың қозғаушы күші болып табылатындығын естен шығармау керек. Оған қоса технологиялық даму өз алдына жаңа қауіпсіздік мәселелерін тудырып отыратындығы тағы бар. Ал қауіпсіздікке тым көп назар аударып, оған барлық ресурстарды жұмылдыру инновациялық даму қарқынын төмендетуі мүмкін. Әлеуметтік факторларды қарастыратын болсақ инновациялар елдің «ақпараттық мәдениетіне» де байланысты болады.

Инновациялық мүдделер мен қауіпсіздік мүдделері арасындағы байланыс ҚХР технологиялық саясатының бірнеше мысалдарынан көруге болады. Қытайдың WAPI сымсыз байланыс стандартын дамытудың басты себебі ретінде дүниежүзінде кең таралған IEEE 802.11 стандартының қауіпсіздігіне байланысты күмәндарға байланысты енгізілген болатын. WAPI жобасында коммерциялық мүдденің болғанымен де қауіпсіздікке байланысты мотивацияның басты орында болғандығы анық. Көп деңгейлі қорғаныс схемаларының мысалында біз сертификация жүйесін енгізудегі қауіпсіздік мәселелерінің приоритетін көре аламыз. Бұл жерде екінші орындағы коммерциялық мүдделермен қатар ұлттық инновациялық мүмкіндіктерді дамытуға деген ұмтылыс та байқалады.

Ақпараттық қауіпсіздік мүдделерін Қытайдың жүзеге асырып отырған ғылыми-зерттеу жобаларынан да көруге болады. ҚХР-дағы «Wintel» платформаларының қауіпсіздігіне деген сенімсіздік отандық чиптер мен бағдарламалық өнімдерді шығару бойынша ғылыми-зерттеу жұмыстарының басталуына түрткі болды. Қытайдың ғылыми-технологиялық дамуының орта және ұзақ мерзімді жоспары мен Жаңа стратегиялық индустрия бастамасы Қытайдың ұлттық интеллектуалдық өнімін жасап шығарудың негіздерін қалаған болатын [6], [7]. Бірақ көп жағдайда ұлттық инновациялық өнімдерді тез арада жасап шығаруға мүмкін емес болғандықтан қытайлық мамандар шетелдік технологияны азғантай модификациядан өткізіп ұлттық интеллектуалдық меншік ретінде жариялау тәжиірбесіне көшкен болатын. Батыс елдеріндегі ҚХР-н өнеркәсіптік шпионажға байланысты айыптаулар да осы процестің бір көрінісі болуы мүмкін. Ғылыми-технологиялық дамудың орта және ұзақ мерзімді жоспары мен Жаңа стратегиялық индустрия бастамасындағы ақпараттық-коммуникациялық технологияларды дамытуға көп көңілдің бөлінуі мен әсіресе қытайлық интеллектуалдық меншік пен ұлттық техникалық стандарттарға қойылып отырған акценттер осы мәселелерде мемлекеттің ақпараттық қауіпсіздігі мүдделерінің басымдығы мен жалпы қытайлық ақпараттық мәдениеттің ерекшеліктерін айқын көрсетіп отыр.

Әдебиеттер

1 Goodrich Jimmy Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy // China and Cybersecurity: Political, economic and Strategic dimensions. Report from Workshops held at the University of California. – San Diego, April 2012, – P. 5.

2 Document 27 // http://www.btpta.gov.cn/publish/portal7/tab550/info92345.htm Accesed: 04/12/2014.

3 Profile of 973 Program // http://www.973.gov.cn/English/Index.aspx Accessed: 15/02/2015.

4 National High-tech R&D Program (863 Program) // http://www.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm.

5 Zhuge Jianwei, Gu Lion, Duan Haixin Investigating the Chinese Underground Economy of Information Security // China and Cybersecurity: Political, economic and Strategic dimensions. Report from Workshops held at the University of California. – San Diego, April 2012, – P. 10.

6 China issues guidelines on sci-tech development program // http://www.gov.cn/english/2006-02/09/content_184426.htm Accesed: 11/11/2014.

7 Yao Lu China Releases 12th Five-Year Plan for National Strategic Emerging Industries // http://www.china-briefing.com/news/2012/07/25/china-releases-12th-five-year-plan-for-national-strategic-emerging-industries.html 11/11/2014.