С.81

8. Братерский П.В. Политика США в Средней Азии: итоги десятилетия //США – Канада . Экономика. Политика. Культура. 2002. №9. -С.55-56

9. Luong P.J., Wientbal E. New Friends, New Fears in Central Asia // Foreign Affairs. 2002. Volume 81. №2. -p.61

10. Токаев К.К. Внешняя политика Казахстана в условиях глобализации. Алматы, 2000, -С.186

11. Буш Дж. Это победа демократии и свободы // Известия. 1991. -26 декабря. -С.5

12. Кременюк В.А. Внешняя политика США на рубеже веков // США. Экономика. Политика. Культура. 2000. №5. -С.3–4

13. Уткин А. Новая империя и постсоветское пространство // Свободная мысль. XXI. 2002. №8. – С.40

14. Токаев К.К. Внешняя политика Казахстана в условиях глобализации. Алматы, 2000, -С.488

* * *

Мақаланың авторы Казақстанмен АҚШ арасындағы қарым-қатынастарының бастапқы құрылымын қарастырған.

* * *

The author examines the origins of the Kazakh-American relations.

Ш. Жандосова, О. Әуелбеков

КИБЕРЛАҢКЕСТІК ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІНЕ ҚАУІП РЕТІНДЕ

Ғаламдануды жеделдеткен ғылыми-техниканың дамыған шағында ақпараттық технологиялар лаңкестерге топ болып бірігуге, еркін әрекет етуге және ұлттық инфрақұрылымдардың элементтеріне шабуыл жасауға көмек беретін құрал ретінде қарастырылады. Электромагнитті импульстардың, күшті микротолқынды сәулелердің көмегімен компьютерлік жүйелерді және өзге электрондық бұйымдарды істен шығаруға мүмкіндік беретін құралдарды лаңкестер еркін қолдануда.

Қоғамдағы ғаламдану процестеріне және интеграцияға, сондай-ақ, заманның өзгеруіне байланысты, әлемдік қауымдастыққа төніп тұрған қауіптің өзгеріске ұшырауы ғажап емес. Жекелеп айтқанда, киберлаңкестік құбылысы. Мұның өте қауіпті екенін американдық, ресейлік және тағы басқа елдердің арнайы қызметтері аңғарып үлгерді. Халықаралық лаңкестікпен күрес жөніндегі мамандар болашақта лаңкестік топтар киберлаңкестік шараларын Америка Құрама Штаттарында, сондай-ақ, онымен одақтас елдерде өткізеді деп жорамалдауда. Олар компьютердің көмегімен инфрақұрылымның маңызды обьектілеріне соққы жасалатынын ескертеді, мұның нәтижесі қантөгіске әкелетіні сөзсіз.

Бүгінгі таңда киберлаңкес компьютердің көмегімен, бомбымен салыстырғанда көбірек зиян тигізе алады. Киберлаңкестікті ақпараттық соғыс, ақпараттық қару және ақпараттық қылмыс шараларынан бөліп алу өте қиын, сондықтан, киберлаңкестік түсінігіне нақты анықтама беру оңай емес. Лаңкестіктің мұндай формасының спецификасын анықтауда қосымша қиындықтар пайда болуы мүмкін. Киберлаңкестіктің психологиялық және экономикалық аспектілері өзара байланысты, сондықтан, екеуінің қайсысы маңызды екенін анықтау мүмкін емес. Бұл құбылыстың жаңа екенін көрсетеді [1].

Ақпараттық қылмыс жеке субьектілердің немесе топтардың пайда табу немесе бұзақылық мақсатпен қорғаныс жүйелерін бұзуға, ақпараттарды ұрлауға немесе бұзуға бағытталған әрекеттерін айтады. Көбінесе мұндай қылмыстар киберкеңістікте нақты бір объектіге қарсы жасалады.

Ақпараттық лаңкестіктің киберкеңістіктегі мақсаты – саяси лаңкестіктің мақсатына толық сәйкес келеді. Ақпараттық лаңкестік әрекеттердің жүзеге асырылу әдістері кең ауқымды алуы және ақпараттық соғыстық қарудың барлық түрлерін қамтуы мүмкін. Дегенмен, оны қолдану әдісі ақпараттық соғыстың және ақпараттық қылмыстың әдістерінен өзгеше болып келеді. Ақпараттық лаңкестік әдісіндегі ең бастысы, лаңкестік шараның нәтижесінде қауіпті жағдайдың туындауы және қоғамдағы жұрттың үрейін туғызу болып табылады.

Жеке субъектілермен немесе топтармен компьютерлік ақпаратқа және анықтау жүйелеріне жасалатын ақпараттық шабуылдары киберлаңкестіктің негізгі формасы болып табылады. Мұндай шабуыл белгілі бір жүйеге еніп, ақпараттық айырбас желісінің құралдарын басып тастауға және тағы басқа көптеген деструктивті әрекет жасауға мүмкіндік береді. Киберлаңкестіктің ұлттық шекарасы жоқ және лаңкестік шаралары әлемнің кез келген жерінен жасалуы мүмкін, сол себепті ол өте қауіпті болып табылады. Киберлаңкесті ақпараттық кеңістікте табу аса қиын, өйткені ол бір немесе бірнеше өзге компьютерлер арқылы әрекет етеді.

Жоғарыда көрсетілген мәліметтерге сүйене отырып, киберлаңкестік түсінігіне мынадай анықтама беруге болады: киберлаңкестік екі сөздің қосылуынан пайда болды, кибер – (киберкеңістік) және лаңкестік. Орыс әдебиетінде «виртуалды кеңістік», «виртуалды әлем» терминдері жиі кездесе бастады, ол компьютердің көмегімен жасалатын ақпараттық кеңістікті білдіреді. Ал мұнда компьютерлік бағдарламалар және ақпараттар әрекет етеді. Киберлаңкестік деп адамдардың өміріне, денсаулығына қауіп төндіретін немесе өзге ауыр жағдайға әкелетін, компьютер мен компьютерлік жүйемен өңделетін ақпаратқа арнайы саяси шабуылда көрініс табатын кешенді шараны айтады. Ол белгілі бір саяси немесе өзге мақсаттарға жету мақсатымен ұдайы қорқыныш сезімін ұйымға назар аудартуда көрініс табады. Киберлаңкестік лаңкестік ұйымдардың жаңа қаруы болып табылады, сондықтан, қазіргі кезде оның барлық көріністерін қамту мүмкін емес [2].

Расында да, ақпараттық-коммуникациялық кеңістіктің саласына өтіп кеткен халықаралық лаңкестіктің мүмкіндіктері шексіз. Оның ешбір ұлттық және діни ұстанымдары жоқ. Лаңкестер және киберлаңкестер мәдениетке, өркениетке, қоғамға үлкен қауіп төндіріп тұрған қылмыскерлер, бұлармен келісімге келу мүмкін емес. Әлемдік қауымдастықтың парызы қоғамды және әлемді қорғау болып табылады. Трансұлттық компьютерлік қылмыстардың және киберлаңкестіктің пайда болуымен ақпараттық қауіпсіздікті қамтамасыз ету мәселесі өте маңызды бола бастады.

Киберқылмыс деп виртуалдық кеңістіктегі қылмысты айтады. Бұл виртуалдық кеңістікте субьектілер, заттар, фактілер, оқиғалар, құбылыстар және процестер жайлы толық мағлұматтар болады. Бұл анықтама БҰҰ-ның мамандарының ұсыныстарына сәйкес келеді. Олардың пікірінше, киберқылмысқа компьютерлік жүйенің немесе желістің көмегімен жасалатын кез келген қылмысты жатқызуға болады.

Киберқылмыстың ең қауіпті түрі – киберлаңкестік болып табылады. Лаңкестік құбылыс ретінде көптеген мемлекеттер үшін күнделікті жәйтқа айналып кетті. Ақпараттық процестердің нәтижесінде оның жаңа формасы –киберлаңкестік пайда болды. Алайда, киберқылмыс пен киберлаңкестікті ажырату қиынға түседі. Дегенмен, киберлаңкестіктің киберкеңістікке қауіп төндіріп тұрған өзге қылмыстық формалардан айырмашылығы бар: оның мақсаттары саяси лаңкестікке тән болады. Киберлаңкес пайда көру немесе бұзақылық мақсатта әрекет ететін хакерден, компьютерлік бұзақыдан және ұрыдан ерекшеленеді. Киберлаңкестіктің басты мақсаты қоғамға үлкен зардап тигізу және қарапайым халықтың, билік басындағы тұлғалардың үрейін туғызу.

Киберлаңкестік мемлекеттің ақпараттық инфрақұрылымын істен шығаратын түрлі формаларын және әдіс-тәсілдерін пайдалануға бағдарланады. Киберлаңкестіктегі жасалып жатқан қылмыстың өсу деңгейі ең жылдам болып есептеледі.

Лаңкестіктің осы формасының ерекше спецификасы бар екенін көрсетіп кеткен жөн. Жалпы адамзаттық құндылықтарға қайшы келетін экстремистік топтардың, сепаратистік күштердің, түрлі ойларды уағыздаушылардың өздерінің идеологияларын үгіттегенде және мақсаттарына жетуде қазіргі заманға сай ақпараттық технологияларды белсенді түрде қолдануға ұмтылуы қатты уайымдатады. Мысалы, бүгінгі таңда Интернетте барлық исламдық ұйымдардың сайттары орналасқан («халықаралық исламдық майдан», «Косованы азат етуші армия», «Исламдық топ» және т.б.). Бұлардың басты мақсаты ақпараттық-үгіт-насихаттық әсер және ұйымдастырушылық қызмет. Сонымен қатар, радикалдық топтар интернетті байланыс құралы ретінде пайдаланады. Израильдің контрбарлауы Шин-Бет мамандарының айтуынша, лаңкестер электрондық пошта арқылы жасырын түрде карталарды, схемаларды және тағы басқа көптеген мәліметтерді жібереді.

Мамандар халықаралық исламдық ұйымның жаңа түрі пайда болғанын айтуда, оның негізі нақты ұйымдық байланыстар емес, ортақ ақпараттық орта болып табылады. Бұл лаңкестік құбылысының шынайы кеңістіктен виртуалды кеңістікке өтіп жатқанын білдіреді. Ақпараттық желістер лаңкестік топтарға мақсаттарын орындауға көмектеседі [3].

Қазіргі таңда адамдардың өміріне және барша мемлекеттің қауіпсіздігіне қауіп төндіріп тұрған халықаралық лаңкестер санының өсуі үкіметтің мемлекеттік органдарына деген сенімін жояды. Расында да, мұндай қылмыстың түрінен сақтау міндеті үкіметке жүктелген. Сондықтан, үкімет лаңкестікке және киберлаңкестікке қарсы күрес шараларына үлкен назар аударуы қажет. Сондай-ақ, осы қылмыстың түріне қатысты нормативтік және құқықтық құжаттарды қайта қарастыру жұмыстарын жүргізу қажет. Желістік шабуылдарды жою салаларындағы ғылыми жұмыстардың маңызы өте жоғары. Бірақ, мұның барлығын іс-жүзіне асыру ақпараттық қауіпсіздік саласындағы кәсіби мамандар дайындау жүйесін жақсартпағанша мүмкін емес.

Қазақстан ТМД елдерінің арасындағы жедел қарқынмен дамып келе жатқан елдердің алдың-

ғы қатарында деуге болады. Өзінің географиялық орнына байланысты маңызды геосаяси жағдайға ие болып отыр. Сол себепті біздің еліміз өзге мемлекеттердің арнайы қызмет органдарының назарын аудартуда. Мысалы, Қазақстанда соңғы бес жылда ұсталған барлаушылардың саны, бастапқыдағы 80 жылдың ішінде ұсталғандардан асып түскені мәлім болды. Батыстың арнайы қызмет органдарын ең алдымен республикамыздың саяси, экономикалық және қорғаныс жағдайы қызықтырады. Жекелеп алғанда шетелдің арнайы қызмет органдарының зерттейтін мәселесі елміздің экономикасы, ең алдымен мұнай өндірісі, металлургия, атомдық және энергетикалық өнеркәсіп объектілері, көлік және коммуникация болып отыр.

Статистика бойынша, ай сайын республикамыздың үкіметінің әрбір мүшелеріне қатысты 500-ге жуық заңсыз ену әрекеттері жасалуда, оның ішінде «Трояндықтарды» – вирус программаларын енгізу талпыныстары көбірек жасалады. Мұндай әрекет іс жүзіне асатын болса, кез-келген ақпараттың алынуына мүмкіндік береді.

Қазақстан Республикасы жедел қарқынмен дамып жатқан елдердің қатарында болғандықтан, «Ақпараттық қарудың» әсеріне душар бола алады. 1991 жылы Ираста «Шөлдегі боран» шарасын жүзеге асыруда Американдық арнайы қызмет органдарының әскері барлық байланыс желістерін істен шығарып тастады, нәтижесінде бұл Ирак әскерінің мобилділігінің жойылуына әкелді. Жоғары айтылып кеткен ақпараттық қауіпсіздіктің қауіпі тек қана мемлкеттке емес, сонымен қатар, жеке азаматтарға да төніп тұрғанының ескеру қажет. Мұндай қауіптің объектісі жеке мәліметтер, қаржы туралы мәліметтер, коммерциялық құпия және т.б [4].

Сондай-ақ, азаматтарға деструктивті идеологиялық және психологиялық әсер тигізу үлкен қауіп төндіреді деуге болады. Бүгінгі таңда ақпараттық қауіпке тек жақсы ұйымдастырылыған ақпараттық қауіпсіздікті қамтамасыз етудің мелекеттік жүйесі қарсы тұра алады, әрине ол еліміздің барлық мемлекеттік мекемелердің, мемлекеттік емес құрылымдардың және азаматтардың бірігіп, қызмет етуімен жүзеге асырылу керек. Қазақстан Республикасы әлемдік ақпараттық алмасуға қатысып жатыр, сонымен қатар, қауіпсіздік сұрақтары жөнінде шетелдің арнайы қызмет органдарымен тығыз қарым-қатынас орнатып, ақпараттық технологиялар саласындағы қылмыспен күресудегі тәжірибелерін алуда.

Әрбір мемлекет өздерінің құпияларын қорғау керек. Бұл үшін арнайы бөлімдер құрылады, сондай-ақ, қорғаныс саласын және қорғалатын ақпараттың қолданысын бақылайтын қажетті заңдар қабылданады. Қазақстанда Ұлттық Қауіпсіздік Комитеті мемлекеттік құпиялардың контрбарлаушылық қорғанысын, мемлкеттік мекемелердегі жабық ақпараттардың сақталуын қамтамасыз етілуіне бақылау жасау, белгілі бір ұйымдарға мемлекеттік құпияны қолданумен байланысты қызметке арнайы рұқсаттарды және лицензияларды береді.

Соңғы жылдары Қазақстан Республикасында ақпараттық қауіпсіздігін қамтамасыз ету жүйесін жақсартуда бірқатар шаралар іс жүзіне асырылды. Қазақстан Республикасының ұлттық қауіпсіздік стратегиясына байланысты ақпараттық қауіпсіздіктің концепциясы өнделіп, қабылданды. Бұл концепция бойынша ақпараттық қауіпсіздік саласындағы қауіпті жағдайды болжауға, аңықтауға, алдын алуға және төтеп беруге бағытталған құқықтық, ұйымдық және ғылыми техникалық шаралар іс жүзіне асырылуы керек.

Елімізде «Электронды құжат және электронды сандық қолтаңба» туралы және «Ақпараттандыру» туралы заңдар қабылданды. Бұл заңдар қашан және қаншалықты тиімді әрекет ететінін уақыт көрсетеді. Қазақстан Республикасында ақпараттандыру және қорғаныс құралдары негізіндегі нормативті-методикалық база жоқ деуге болады. Сондай-ақ, Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету саласында кәсіби дайындалған қызметкерлер жоқтың қасы. Сол себепті мұндай мамандарды дайындау жүйесін өндеп шығару қажет.

Осылайша, ақпараттық қауіпсіздікті қамтамасыз ету кез келген мемлекеттің ұлттық қауіпсіздігінің ең маңызды элементтерінің бірі болып табылады. Қазақстанда ақпараттық қауіпсіздікті қамтамасыз ету саласында көптеген шешілмеген мәселелер бар, олар құқықтық, ұйымдастырушылық, технологиялық және тағы басқа. Ең бастысы елімізде ақпараттық қауіпсіздік мәселесінің шешілу керек екенін түсінді. Ал бұл Қазақстандық мәдениеттің, ұлттық ділдің және мемлекеттік бүтіндіктің сақталуына өз септігін тигізеді.

---

1. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безапостности. www. Crime-research.org.

2. Алексеева И.Ю. Информационные вызовы национальной и международной безопасности. М.: ПИР-Центр, 2001. 301б

3. Щетилов А. Некоторые проблемы борьбы с кибер преступностью и кибертерроризмом. www. Crime-research.org.

4. Смолян Г.Л., Черешкин Д.С. Сетевая информационная революция. Информационные ресурсы России. -1997. -№4. -56-64б.

* * *

В данной статье рассматривается кибертерроризм как угроза национальной безопасности Республики Казахстан.

* * *

This article focuses on cyberterrorism as a threat to national security of the Republic of Kazakhstan.

5 - Б Ө Л І М

ШЕТЕЛ БАСЫЛЫМДАРЫ

James Petrik

"ENANTIOMORPHS AND KANT'S NEGLECTED ALTERNATIVE: AN ARGUMENT FOR THE NON-SPATIALITY OF THINGS IN THEMSELVES"

One of the more striking aspects of Kant's transcendental idealism is the contention that the space we experience is actually contributed to that experience by our faculty of outer sense. While it is clear both why Kant draws this conclusion and the important role this conclusion plays in answering the question of how synthetic *a priori* judgments are possible, what is less clear is why Kant believes he is entitled to make the following further claim: Things as they are in themselves – and independently of how they are experienced by us – do not and cannot have spatial properties. From the fact that the space we experience is supplied by our faculty of outer sense and not the objects that engage them it does follow that the space *we experience* is not a property of the objects themselves. Nonetheless, there would seem to remain the possibility that things in themselves partake of their own spatial relations and properties where these relations and properties are qualitatively similar to those imposed upon our experiences by our faculty of outer sense. This objection, which has come to be known as the "Problem of the Neglected Alternative," is most often associated with Adolf Trendelenberg in the mid-19th century [4], versions of it can be traced to Kant's contemporaries in the late 18th century [3, pp. 128-132].

In what follows, I will draw upon Kant's discussion of enantiomorphs in the *Prolegomena* to point the way to an argument that is unique in the secondary literature and that would allow Kant to eliminate this Neglected Alternative. Additionally, I will argue that there is textual evidence for believing that Kant himself had this argument in mind.

1. Enantiomorphs and the Transcendental Ideality of Space.

In Sections 6-12 of the *Prolegomena* [3], Kant argues for the conclusion that space and time are mere forms of sensibility by noting that this supposition is the only plausible way to account for the synthetic *a priori* judgments of mathematics. Realizing, however, that readers may nonetheless be reluctant to accept such a counterintuitive conclusion, in Section 13, Kant approaches the matter from a very different angle. He notes that those who still cannot shake the belief that space and time are properties of things in themselves can overcome this inclination by considering the geometric paradox posed by enantiomorphs. Enantiomorphs – sometimes also called "incongruent counterparts" – are chiral geometric pairs that seem to share all the same intrinsic properties and yet cannot be substituted for each other. The examples of enantiomorphs that Kant