ӘОЖ 327.3
https://doi.org/10.48371/ISMO.2023.54.4.009
ҒТАМР 11.25.40

ӘЛЕМДЕГІ ДАМЫҒАН ЕЛДЕРДІҢ ӨҢІРЛІК САЯСАТЫНДАҒЫ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН ТАЛДАУ

*Дмитриева А.С.[1], Жолдасбекова А.Н.[2], Оспанова А.Н.[3]
*[1] докторант, Аймақтану кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті Халықаралық қатынастар факультеті, Астана, Қазақстан
e-mail: dmitriyeva.alyona@gmail.com
[2] саяси ғылымдарының кандидаты, Л.Н. атындағы Еуразия ұлттық университеті Халықаралық қатынастар факультеті Аймақтану кафедрасының профессоры, Астана, Қазақстан
e-mail: eic.astana@gmail.com
[3] Ph.D., қауымдастырылған профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті Халықаралық қатынастар факультеті Аймақтану кафедрасының меңгерушісі, Астана, Қазақстан
e-mail: ospanovaa@mail.ru

Аңдатпа. Цифрлық технологиялардың даму дәуірінде мемлекеттердің IT-технологияларға тәуелділігі мен киберқауіптердің пайда болуына байланысты ақпараттық қауіпсіздікті қамтамасыз ету дипломатия мен әлемдік саясатта маңызды басымдыққа айналды. Сонымен қатар, ақпараттық қауіпсіздік тәуекелдері жаһандық саяси субъектілер үшін олардың саяси және экономикалық ландшафтына әсер ететін күрделі мәселе болып табылады. Бұл зерттеуде авторлар Америка Құрама Штаттары, Еуропалық Одақ және Қытай Халық Республикасы мысалында ақпараттық қауіпсіздік тәуекелдерінің кешенді салыстырмалы талдауын ұсынады, елдердің саяси көзқарастарын, экономикалық амбицияларын және салдарын қарастырады, сондай-ақ негізгі аймақтық ойыншылардың аймақтық саясатындағы киберқауіптердің әсерін талдайды. Мақаланың зерттеу сұрағы мемлекеттердің саяси динамикасының және экономикалық ұмтылыстарының осы аймақтардың ақпараттық қауіпсіздік стратегияларын қалай қалыптастыратынын түсінуге бағытталған. Әдістеме мәліметтерді жинауды, талдауды, жүйелі және салыстырмалы зерттеуді қамтиды, бұл әрбір аймақтың ақпараттық қауіпсіздік ландшафтының тұтас көрінісін алуға мүмкіндік береді. Салыстырмалы талдау негізінде авторлар салыстырылатын елдердегі ақпараттық қауіпсіздіктің экономикалық және саяси аспектілерін зерттейтін кесте құрастырды. Осы орайда, зерттеудің негізгі нәтижелері Америка Құрама Штаттары киберқауіптерге қарсы тұру үшін мемлекеттік-жекеменшік әріптестік пен инновацияларға, Еуропалық Одақ ынтымақтастық пен киберқауіпсіздік ережелерін үйлестіруге, ал Қытай Халық Республикасы кибер егемендік пен ұлттық қауіпсіздікті арттыруға назар аударып отырғанын көрсетеді. Талдау аясында авторлар саясат, экономика және ақпараттық қауіпсіздік тәуекелдері арасындағы байланысты қадағалайды, аймақтар арасындағы конвергенция мен алшақтық аймақтарын анықтайды. Сондай-ақ, авторлар өңірлердегі ақпараттық қауіпсіздіктің тұрақты дамуы үшін келіп түсетін киберқауіптерді жою бойынша қорытындылар мен ұсыныстар берді.

Тірек сөздер: ақпараттық қауіпсіздік, кибертәуекелдер, саяси ландшафт, аймақтық саясат, кибердипломатия, экономикалық амбициялар, саяси салдарлар, салыстырмалы талдау

Кіріспе

Қазіргі жаһандану заманында ақпараттық қауіпсіздік әлемнің дамыған елдері үшін басты мәселеге айналды. Осылайша, ақпараттық технологиялардың қарқынды дамуын және әлемдегі ақпарат ағынының жаһануын ескере отырып, ақпараттық қауіпсіздікті арттыру әрбір мемлекеттің ұлттық қауіпсіздігін дамыту стратегиясында басым бағыт болып табылады.

Халықаралық аренадағы аймақтық ойыншылардың ішінде мемлекеттік ақпараттық жүйелердің қауіпсіздігі мен қорғалуын қамтамасыз етуге ерекше көңіл бөлетін елдердің ең жарқын мысалы АҚШ, ЕО және Қытай болып табылады. Бұл елдер арнайы стратегияларды, заңнамалық құжаттарды әзірлеуде, сондай-ақ ақпараттық қауіпсіздік саласында басқа елдермен ынтымақтастық туралы меморандумдар жасауда. Әрбір аймақтың ақпараттық қауіпсіздік тәуекелдерін басқаруға деген көзқарасына әсер ететін өзіндік саяси құрылымдары мен экономикалық мүдделері бар екенін атап өткен жөн. Осылайша, жоғары дамыған IT- технологиялар және үнемі пайда болатын киберқауіптер дәуірінде ақпараттық қауіпсіздік тәуекелдерін басқару өңірлік және халықаралық деңгейде мемлекеттер үшін өзекті мәселе болып табылады және олардың ұлттық мүдделерін қорғауда шешуші рөл атқарады.

Зерттеудің негізгі мақсаты – ақпараттық қауіпсіздік тәуекелдерін басқару бойынша жалпы тенденцияларды, көзқарастардағы айырмашылықтар мен ұқсастықтарды анықтау, сондай-ақ қабылданған шаралардың тиімділігін бағалау үшін аймақтық ақпараттық қауіпсіздік саясаты саласында АҚШ, ЕО және Қытай арасында салыстырмалы талдау жүргізу.

Бұл мақаланың ғылыми жаңалығы әлемнің дамыған елдері арасында кешенді салыстырмалы талдау жүргізуді қамтитын әдістемелік тәсілде жатыр, бұл өз кезегінде туындайтын киберқауіптерге жауап берудің бірегей стратегиялары мен тетіктерін анықтауға мүмкіндік береді, сонымен қатар аймақтардағы ақпараттық қауіпсіздік тәуекелдерін басқару бойынша практикалық ұсыныстар берілген.

Бұл зерттеуде алға қойылған гипотезаға келетін болсақ, бұл әр аймақтың саяси ландшафтының өзгеруіне байланысты елдердің ақпараттық қауіпсіздік тәуекелдерін басқарудағы сәйкес тәсілдері модификацияланады, әрі ақпараттық қауіпсіздік саласындағы аймақтық саясатты қамтамасыз етудің әртүрлі тәсілдерін қалыптастыруға әкеледі.

Зерттеудің ғылыми-практикалық маңыздылығы ақпараттық қауіпсіздік тәуекелдерінің саяси және экономикалық аспектілерін кешенді бағалауда көрінеді. Бұл зерттеу қазіргі таңда жасалған зерттеулердегі олқылықтарды толтыру және аймақтық саясаттардың әртүрлі саяси жүйелер мен экономикалық мақсаттар арқылы қалай қалыптасатынын түсінуді жақсарту арқылы осы салаға үлес қосады.

Әдебиеттерге шолу

Үнемі өзгеріп отыратын қауіп ландшафтына байланысты халықаралық қауіпсіздік тұжырымдамасының аясы жылдар өте келе кеңейді. Бұл тақырып ғылыми ортада кеңінен талқылануда. Сонымен қатар, бүгінгі күні бұл

тұжырымдама дәстүрлі әскери қақтығыстардан бастап ақпараттық қауіп-қатерлерге және мемлекеттердің тұрақтылығы мен олардың ұлттық қауіпсіздігіне әсер ететін мемлекеттік емес субъектілердің қызметіне дейінгі әлемдегі өзара байланысты көптеген проблемаларды қамтиды.

2006 жылы ғалымдар Эриксон мен Джакомелло халықаралық қатынастар теориясы өзінің әртүрлі теориялық құралдарын киберқауіпсіздік тақырыбына қолдану үшін күресіп, «цифрлық әлемнің жаңа сын-қатерлері аясында туындайтын күрделіліктерді талдауда теориялық бейімделу мен қолдануда үлкен қиындықтарға тап болды» деп дәлелдеді». Дегенмен, технология, саясат және ғылым салаларында болып жатқан өзара байланысты өзгерістер ұлттық және ақпараттық қауіпсіздіктің негізгі аспектілерін халықаралық қатынастар теориясының объективі арқылы талдауға болатын жаңа зерттеулермен бірге жүретіндіктен, мұндай мәлімдеме енді шындыққа жанаспайды [1] .

Сонымен қатар, киберқауіпсіздік дискурсы соңғы 20 жылда айтарлықтай өзгерді. Киберқауіпсіздік саясаттың күн тәртібін жоғарылатады және цифрландыру алға жылжыған сайын көптеген қосымша саясат салаларына мәселе аймағы ретінде кеңейеді.

Сонымен бірге, ғалымдардың ғылыми зерттеулерінде киберқауіптер «ұлттық қауіпсіздікке төнетін ең маңызды қатерлердің бірі», сондай-ақ «үлкен экспоненциалды қауіп» ретінде қарастырылады. Ғылыми қауымдастық сондай-ақ кибер операциялардың мемлекетаралық деңгейде экономикалық, саяси және әскери қуат динамикасын өзгертуде шектеулі стратегиялық пайдасы болуы мүмкін деген идеяға қосылды.

Америка Құрама Штаттарындағы ақпараттық қауіпсіздік саласындағы ірі ғалымдардың ішінде киберкеңістіктегі қауіп-қатер саясатын зерттейтін Мириам Данн Кавельти ақпараттық қауіпсіздік саласындағы «ұлттық қауіпсіздікті» анықтаудың іргелі мәселесіне ерекше назар аударады, бұл тақырып саясаттағы талқылаулар мен пікірталастарды қалыптастыруды жалғастыруда. Сонымен қатар, Кавелти жеке сектор мен маңызды инфрақұрылымдарды қорғауға жауапты үкіметтік киберқауіпсіздік субъектілері арасындағы шиеленісті атап көрсетеді [2].

Еуропалық Одақтың киберқауіпсіздік саласындағы негізгі тенденциялары еуропалық ғалымдар Г. Камбуракис, Р. Нейссе, И. Най-Фовино зерттеулерінің орталығында шоғырланған [3]. Сонымен бірге ЕО-да ақпараттық қауіпсіздікті құқықтық реттеу тәжірибесі ресейлік ғалым В.Гирис [4] және қазақстандық ғалым А. Жатқанбаева [5] еңбектерінде зерттелген .

Өз кезегінде, Т.Понка, М.Рамич және Ю.Ву [6] Қытайдың киберсаясатын сыртқы және ішкі деңгейде талдайды, негізгі тәуекелдер мен оларды жою тәсілдерін қарастырады, ал Ц. Ли, С. Гуо және Ц. Хэ [7] ҚХР ішіндегі киберқауіпсіздік мәселесін, сондай-ақ ақпараттық инфрақұрылым арқылы ел ішіндегі және басқа аймақтардағы халыққа саяси әсер ету үшін қолданылатын құралдарды зерттеуге назар аударады.

Сонымен қатар, бар әдебиеттер ақпараттық қауіпсіздік тәуекелдерінің әртүрлі аспектілері туралы құнды түсініктер бергенімен, бұл жұмыстың орнын толтыруға бағытталған кейбір олқылықтар бар екенін атап өткен жөн.

Біріншіден, осы аймақтардағы аймақтық ақпараттық қауіпсіздік саясатына әсер ететін нақты саяси және экономикалық аспектілерді зерттейтін зерттеулер аз. Екіншіден, АҚШ, ЕО және Қытайдағы киберқауіптердің негізгі тәсілдері мен әсерін зерттейтін кешенді салыстырмалы талдаулар жоқ. Осылайша, барлық зерттеулерді ескере отырып, бұл жұмыс халықаралық аренадағы негізгі жаһандық ойындар арасындағы ақпараттық қауіпсіздік тәуекелдерін олардың саяси ландшафты мен экономикалық амбицияларын ескере отырып, кешенді салыстырмалы талдауды жүргізу арқылы олқылықтарды жоюға тырысады. Саясат, экономика және ақпараттық қауіпсіздік тәуекелдері арасындағы қарым-қатынасты зерттей отырып, бұл зерттеу аймақтық ақпараттық қауіпсіздік саясатын қалыптастырудағы және киберқауіптерге қарсы тұрудағы қиындықтар мен мүмкіндіктерді тереңірек түсінуге ықпал етуге бағытталған.

Материалдар мен әдістерді сипаттау

Зерттеу барысында талдау және синтез әдістері қолданылды, мұнда талдау арқылы таңдалған елдердегі ақпараттық қауіпсіздік саласындағы тәуекелдер туралы ақпарат жиналды және өңделді, ал синтез әдісі жинақталған деректерді құрылымдауға мүмкіндік берді, біртұтас зерттеліп отырған мәселенің суретін, сондай-ақ аймақтық және халықаралық деңгейде диалог орнату арқылы пайда болатын киберқауіптерге қарсы әрекетті жақсарту үшін негізделген ұсыныстарды әзірлеу.

Салыстырмалы талдау арқылы АҚШ, ЕО және Қытайда ақпараттық қауіпсіздікті қамтамасыз ету үшін қолданылатын тетіктердегі ұқсастықтар мен айырмашылықтар анықталды, олар салыстырмалы нәтижелерді көрнекі түрде көрсету үшін кестеде ұсынылған. Мақалада сонымен қатар жүйелі әдіс қолданылды, оның шеңберінде ақпараттық қауіпсіздік саяси және экономикалық аспектілерді қамтитын тереңірек жүйенің бөлігі ретінде қарастырылды, бұл сөзсіз осы құрамдас бөліктер арасындағы өзара байланысты және олардың осы аймақтардағы киберқауіпсіздікке әсерін талдауға мүмкіндік берді.

Жалпы алғанда, зерттеу нәтижелері өзгеретін саяси ландшафт пен экономикалық динамиканың жаңадан пайда болған ақпараттық қауіпсіздік тәуекелдері мен елдердің аймақтық киберқауіпсіздік саясаттарына қалай әсер ететіні туралы маңызды түсінік береді. Зерттеу тәсілдердегі конвергенция мен алшақтық аймақтарын анықтайды, саясаттың тиімділігін көрсетеді және киберқауіпсіздік шараларын одан әрі жетілдіру перспективаларын белгілейді.

Нәтижелері

Бүгінде қарқынды дамып келе жатқан цифрлық дәуірде ақпараттық қауіпсіздік бүкіл әлем мемлекеттері үшін маңызды мәселелердің біріне айналды. Бұрын-соңды болмаған жаһандық коммуникациялар дәуірінде ақпараттық қауіпсіздікке қауіп төндіретін ортаның тез өзгеріп жатқанын жоққа шығаруға болмайды, бұл бас тартуға болмайтын шындық. Қазіргі заманауи озық тұрақты қауіптер (Advanced Persistent Threat) елдің

қауіпсіздігіне зор кедергі жасайды, өйткені олар маңызды инфрақұрылымға орасан зиян келтіруге қабілетті. Америка Құрама Штаттары әлемдегі жетекші державалардың бірі ретінде киберкеңістікте көптеген тәуекелдерге тап болады, өйткені бұл мемлекеттің сандық құрылымы кең және халықаралық аренада экономикалық гегемон болып табылады. Дегенмен, АҚШ-тың киберқауіпсіздік саясаты киберқауіпсіздік жағдайында ақпараттық қауіпсіздікті қамтамасыз ету тәсілдері үнемі жаңартылып отыратын күрделі жүйе болып табылады. Тәсілдердің өзі жарлықтарды, заңдарды және стратегияларды әзірлеу арқылы жүзеге асырылады. Оның үстіне киберқауіпсіздікті елдің ұлттық қауіпсіздік стратегиясына енгізу өте маңызды шешім болып табылады. Осылайша, ұлттық қауіпсіздік стратегиясын әзірлеу өте маңызды, өйткені киберқауіпсіздік маңызды инфрақұрылым мен активтерді киберқауіптерден туындайтын қауіптерден анықтау және қорғауда маңызды рөл атқарады, сондай-ақ АҚШ үкіметінің жаңа киберқауіптер мен проблемаларды қалайша тиімді және уақтылы шешіп жатқанын түсінуге көмектеседі.

Мысалы, 2003 жылы Америка Құрама Штаттарына киберқауіптерге қарсы тұру шеңберінде Ұлттық киберкеңістік қауіпсіздік стратегиясы қабылданды, ол ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттары мен міндеттерін қамтиды: маңызды инфрақұрылымдарға бағытталған кибершабуылдардың алдын алу, осындай шабуылдарға осалдықты азайту, шабуыл кезінде зақымдануды және қалпына келтіру уақытын азайту және т.б. Құжатта егер Америка Құрама Штаттарына қарсы оның киберқауіпсіздігін бұзу әрекеті жасалса, мемлекет кибер қаруды қолдану арқылы жауап қайтаруы мүмкін деп көрсетілген. Кейінірек 2008 жылы Киберқауіпсіздіктің ұлттық бастамасы іске асырыла бастады, ол 2003 жылғы Стратегиямен бірге ақпарат алмасуға және мемлекеттік-жекеменшік әріптестікке негізделген жаңа волонтаристік, бөлшектенген тәсілді белгіледі.

Америка Құрама Штаттарында киберқауіпсіздікті қамтамасыз ету мәселесі кешенді тәсілге негізделген, мұнда мемлекет мемлекеттік органдармен де, жеке сектормен де тиімді ынтымақтастық орнатады. Атап айтқанда, Қорғаныс министрлігі (DoD), Ішкі қауіпсіздік департаменті (DHS) және Федералдық тергеу бюросы (ФБР) АҚШ федералды үкімет жүйесінің белсенді қатысушылары болып табылады. Бұл департаменттер аймақтық деңгейде ақпараттық қауіпсіздік мәселелерін үйлестіруге, сондай-ақ ұлттық қауіпсіздіктің неғұрлым тиімді стратегияларын әзірлеуге көмектеседі.

Бүгінгі таңда киберсаясатты жүзеге асырудың қазіргі мысалдарының бірі АҚШ Қорғаныс министрлігі 2023 жылдың мамырында Конгресске ұсынылған және оның нәтижесінде жинақталған көп жылдық практикалық тәжірибеге негізделген ақпараттық кеңістікте жүзеге асырылатын операцияларға сүйене отырып, құпия киберстратегияны әзірлеу болып табылады. Бұл стратегия кибершабуылдар елдің АТ-инфрақұрылымына зиянды әсер етпей тұрып, «зиянды кибер әрекетті» жылдам және тиімді жолмен алдын алуға бағытталған.

Сонымен бірге, АҚШ-та мемлекет пен жеке сектор арасындағы ынтымақтастыққа баса назар аударылады, бұл киберқауіптерден алда болу үшін ақпарат алмасуға ықпал етеді. Мемлекеттік және мемлекеттік емес субъектілер жүзеге асыратын осы зиянды әрекеттердің саяси және экономикалық салдарын ескере отырып, мемлекеттік және жеке жүйелерге бағытталған ірі деректердің бұзылуы, инфрақұрылымды бұзу және шабуылдар туралы есептердің кең етек алуымен, бұл ынтымақтастық маңызды секторлардың тұрақтылығын арттырады және елдің жалпы қауіпсіздігін қамтамасыз етеді [8].

Тұтастай алғанда, АҚШ-тың елдің киберқорғанысты жақсарту және нығайту бойынша күш-жігерін қарастырған кезде, киберқауіпсіздік шараларын күшейту және бүгінгі цифрлық кеңістікте дамып келе жатқан қауіптерді жою күн тәртібінде белсенді қарастырылады.

Сонымен қатар, ақпараттық қауіпсіздікті қамтамасыз ету мәселесін талдай келе, пайда болған киберқауіптер елдің әлеуметтік-экономикалық дамуы үшін маңызды экономикалық тәуекелдерді тудыратыны анық болады. Келіп түскен киберқауіптер, сөзсіз, ақпараттық қауіпсіздікті қамтамасыз ету мәселесімен, сондай-ақ мемлекеттің экономикалық мүдделерімен байланысты. Сонау 1976 жылы американдық сарапшы Томас Рона ақпараттық инфрақұрылымның экономиканың негізгі құрамдас бөлігі және сонымен бірге соғыста да, бейбіт уақытта да ең осал нысандардың біріне айналып бара жатқанын атап көрсетті [9]. Осылайша, елдің экономикалық үстемдігі көбінесе технологиялық прогресс пен инновацияға байланысты, бұл киберқауіптерден қорғауды императивті етеді.

Осы тұрғыда деректердің жайылып кетуі, зияткерлік меншік ұрлығы, тыңшылық және басқа қауіптерді қамтитын кибершабуылдар орасан зор зардаптарға әкелуі мүмкін. Деректердің жайылып кету нәтижесінде жеке ақпаратқа қауіп төнеді, бұл жеке және заңды тұлғаларға ғана емес, жалпы мемлекетке де қаржылық шығындарға әкеп соғады. Бұл ұстаным 2011 жылғы АҚШ-тың Ұйымдасқан қылмыспен күресу жөніндегі ұлттық стратегиясында көрсетілген, онда киберқылмыс сезімтал корпоративтік және мемлекеттік компьютерлік желілерге қауіп төндіретіні, сондай-ақ халықаралық қаржы жүйесіне жаһандық сенімге нұқсан келтіретіні атап өтілген [10]. Бұған қоса, зияткерлік меншік пен коммерциялық құпияға кибершабуылдар елдің экономикалық бәсекеге қабілеттілігіне нұқсан келтіреді және Америка Құрама Штаттары көшбасшы болып табылатын инновацияның жақсаруын төмендетеді.

АҚШ-тың ақпараттық қауіпсіздігіне бірнеше рет қауіп төнді. Дегенмен, бүкіл әлемде талқыланған ең танымал оқиға – Ресей Федерациясының 2016 жылғы АҚШ президенттік сайлауына кибершабуылдар мен жалған ақпарат арқылы араласуы.

Ресей Федерациясының араласуы АҚШ-тың ұлттық қауіпсіздігін қамтамасыз етудің, сондай-ақ компьютерлік және әлеуметтік салалардағы маңызды мәселелердің біріне айналды. Бұған қоса, бұл оқиғаға қатысты тергеу жүргізілді, оның барысында арнайы прокурор Роберт Мюллер Ресейдің «кең

ауқымда және жүйелі түрде» араласқанын атап өткен қорытынды есебін жариялады. Дегенмен, АҚШ-тағы сайлауға араласу мәселесі әлі де зерттелуде және кеңірек дискурстың бір бөлігіне айналды, осыған байланысты АҚШ президенті Джо Байден Ресей Федерациясын 2020 жылғы АҚШ сайлауына бірнеше рет араласты деп айыптап, оған қарсы санкциялар қолданылатынын атап өтті. Алайда 2016 жылғы сайлауға араласу үшін ғана сенімді дәлелдер келтірілді, ал 2020 жылғы сайлауға араласу туралы мәлімдемелер дәлелденбеді [11].

Осыған байланысты киберқауіпсіздіктің ұлттық қауіпсіздікке ықтимал әсерін түсіну киберқауіпсіздіктің тиімді саясатын әзірлеудегі маңызды қадам болып табылады. Маңызды инфрақұрылымға кибершабуылдар, сондай-ақ жалған ақпарат кең ауқымды бұзылулар тудыруы және ұлттық қауіпсіздік пен экономикалық салдарларға әкелуі мүмкін.

Айта кетейік, киберқауіпсіздік жекелеген мемлекеттер үшін ғана емес, сонымен қатар аймақтық блоктар үшін де маңызды аспект болып табылады, олардың арасында 27 мүше мемлекеттің саяси және экономикалық интеграциялық бірлестігі болып табылатын Еуропалық Одақ бар.

ЕО-ның ақпараттық қауіпсіздікке деген көзқарасы аймақтағы киберқауіпсіздікті нығайту үшін маңызды болып табылатын барлық мүше елдердегі заңдар мен ережелерді үйлестіруге бағытталған. Мемлекеттерді үйлестіру осы саладағы келісілген реттеуге, трансшекаралық ынтымақтастыққа және кибер инциденттерге жедел ден қоюға мүмкіндік береді. ЕО-ның көп деңгейлі шешім қабылдау процесі Еуропарламент, Еуропалық Кеңес және Еуропалық Комиссия арасындағы ынтымақтастықты қамтиды. Мұндай механизм туындайтын кибертәуекелдерді әртүрлі перспективалардан жан-жақты бағалауға мүмкіндік береді және киберқауіпсіздік саясатын әзірлеу кезінде барлық мүше мемлекеттердің мүдделерінің ескерілуін қамтамасыз етеді [4].

Еуропалық Комиссия киберқауіпсіздікке бірыңғай көзқарасты қамтамасыз ету үшін заңнама мен саясатты әзірлеуде орталық рөл атқарады және пайда болған киберқауіптермен күресте табысты болды. Сонымен қатар, бұл киберқауіптер мүше мемлекеттердің әртүрлілігіне және олардың экономикалық өзара тәуелділігіне негізделген ықтимал тәуекелдерден туындайды, сондықтан интеграциялық бірлестік тиімді киберқауіпсіздік саясатын әзірлеуде бірегей қиындықтарға тап болады.

Өз кезегінде ЕО елдері ақпараттық ресурстарды қорғау үшін әртүрлі техникалық, ұйымдастырушылық және құқықтық шараларды қолданады. Осылайша, киберқауіпсіздік саласындағы бірыңғай стратегияны әзірлеуге және оның халықаралық қоғамдастықтағы ұстанымын нығайтуға жауапты негізгі орган 2004 жылы құрылған Еуропалық киберқауіпсіздік орталығы (ENISA) болып табылады. Ақпараттық қауіпсіздік саласында компаниялар мен мемлекеттік органдардың қызметін реттейтін жалпыеуропалық стандарттар мен ережелер де бар. Бұл нормалар мен стандарттар ЕО азаматтарының жеке деректерін өңдеу ережелерін белгілейтін Деректерді қорғаудың жалпы ережесі, сондай-ақ желілік және ақпараттық қауіпсіздік

директивасын (NIS және NIS2) қоса алғанда, басқа директивалар сияқты құжаттарға негізделген ақпараттық қауіпсіздікті, киберқауіпсіздікті және т.б. қамтамасыз ету жөніндегі техникалық және ұйымдастырушылық шараларды реттейтін нормативтік құқықтық актілер [5].

Одақтың саяси құрылымы мен алға қойылған экономикалық мақсаттар ЕО-ның киберқауіпсіздік саясатын қалыптастыруда шешуші рөл атқарады, ортақ басқару, үйлестірілген реттеу және экономикалық бәсекеге қабілеттілік ЕО-ның цифрлық ландшафтты қамтамасыз етуге ұмтылысын қалыптастырады. Бірегей саяси құрылымы мен үйлестірілген заңнамасының арқасында ЕО киберкеңістіктің күрделілігін жақсырақ шарлап, тұрақты және қауіпсіз цифрлық болашақты құруға қабілетті. Осының аясында ЕО басқа аймақтармен салыстырғанда ақпараттық қауіпсіздікті бұзу қаупімен салыстырмалы түрде азырақ бетпе-бет келеді, бірақ әлі де мұндай қауіптерден толықтай қорғалған деуге келмейді.

Мысалы, ЕО елдерінде мемлекеттік органдар мен ірі компанияларға бағытталған кибершабуылдар қаупі бар, бұл ақпараттың жайылып кетуіне және жалпы ақпараттық қауіпсіздіктің бұзылуына әкеледі. 2021-2022 жылдары қылмыскерлермен күресу үшін әзірленген Pegasus бағдарламалық жасақтамасы басқа мақсаттарда пайдаланылғаны анықталған кезде ЕО-да маңызды ақпараттық қауіпсіздік қаупі анықталды. Осылайша, бұл бағдарлама саяси тыңшылық үшін пайдаланылды, соған байланысты Еуропарламент тыңшылық бағдарламасы еуропалық саясаткерлерді, журналистерді және белсенділерді бақылап отырғанын растап, алаңдаушылық білдірді [12].

Бағдарламалық қамтамасыз ету жанжалы жаһандық қоғамдастықта кең тараған пікірталас тудырды, ол киберқауіпсіздік саясатын, трансшекаралық ынтымақтастықты жақсарту және озық технологияларды теріс пайдалану қауіп-қатерлерінің өсуіне сәйкес мемлекеттік қадағалауды күшейту бойынша шұғыл қажеттілігін көрсетті.

Ақпараттық қауіпсіздік саласындағы жетекші ойыншылардың бірі ретінде Қытайды бөлек қарастырған жөн. Осылайша, Қытайдың ірі экономикалық және технологиялық держава ретінде пайда болуы оның жаһандық ақпараттық қауіпсіздік ландшафтындағы маңыздылығын арттырды. Дегенмен, цифрлық технологияларға тәуелділіктің артуына байланысты Қытай көптеген жылдар бойы киберқауіпсіздік тәуекелдеріне де тап болды.

Жалпы, Қытай саясаты орталықтандырылған басқару құрылымымен сипатталады, онда шешім қабылдауды бақылау Қытай Коммунистік партиясына (ҚКП) жүктеледі. Орталықтандырылған бақылау үкіметке киберқауіптерді жоюға бағытталған саясатты жылдам әзірлеуге және енгізуге мүмкіндік беретін ақпараттық қауіпсіздікке де таралады. ҚІЖК-нің ақпараттық қауіпсіздік саласындағы белсенді жұмысы 1999 жылдың желтоқсанында, партия ақпараттық істер бойынша жетекші топ құру туралы бастама көтерген кезде басталды, топтың жұмыс ауқымына мемлекеттің ақпараттық қауіпсіздігін қамтамасыз етілуі кірді. Сондай-ақ, ҚКП 18-ші съезінің қорытындысы бойынша елдің киберқауіпсіздігін қамтамасыз етуді ғана емес, сонымен қатар ұлттық экономиканы дамыту үшін желілік әлеуетті

пайдалануды көздейтін «Желісі күшті мемлекет» стратегиясы алға қойылды [6].

Соңғы жылдары Қытай ақпараттық қауіпсіздікке көбірек көңіл бөле бастады. 2017 жылы Қытай елдің цифрлық инфрақұрылымының қауіпсіздігін қамтамасыз ету және маңызды ақпараттық жүйелерді қорғау үшін Киберқауіпсіздік туралы заң қабылдады. Сонымен бірге, Заң деректер ағынын мемлекеттік бақылауға, мазмұнды сүзуге және ақпараттың ұлттық мүдделерге сәйкестігін қамтамасыз етуге ерекше мән береді. 2023 жылдың қаңтарында Қытайдың Индустрия және ақпараттық технологиялар министрлігі елдің ақпараттық қауіпсіздігін дамытудың жол картасын жариялады, ол «елдің цифрлық экономикасын құрудың» негізін қалайтын киберқауіпсіздік саласын дамыту жоспарларын ашты, соның ішінде ғылыми орталықтармен, университеттермен және әртүрлі компаниялармен ынтымақтастық орнату да кірді.

Дегенмен, бүкіл қабылданған құжаттарда Қытайдың өзінің кибер егемендігіне баса назар аударуы деректердің құпиялылығы мен жеке бас бостандығына қатысты алаңдаушылық тудыратынын атап өткен жөн. Кең таралған қадағалау және деректерді жинау практикасы жеке деректерді ел ішінде де, Қытайда жұмыс істейтін шетелдік жеке тұлғалар мен ұйымдар үшін де қиындықтар туғызады.

Дегенмен, Қытайдың ақпараттық саясат жүйесі ақпараттық қауіпсіздікке ықтимал қауіп төндіретін элементтерді қамтиды, мысалы, тиімді интернетті басқару жүйелері, қуатты АТ корпорациялары және жаңа технологияларды, соның ішінде жасанды интеллект пен 5G көмегімен бұлтты есептеулерді енгізу, киберқауіпсіздік саясаты аясында мұқият үйлестіруді және басқаруды қажет етеді [7].

Сонымен қатар, Қытайдың ақпараттық қауіпсіздігін қамтамасыз ету тағы бір маңызды аспектіні қамтиды, атап айтқанда елдің сыртқы қауіпсіздігін қамтамасыз ету. Қытайдың экономикалық өсуі және оның халықаралық сахнаға жаһандық ықпал ету амбициясы тағы бір ірі ойыншы АҚШ-пен шиеленісті күшейтуде. Елдер арасындағы негізгі айырмашылықтардың қатарында киберқауіпсіздік пен зияткерлік меншікті қорғау мәселелері бар, бұл ішінара кибершабуылдарға аса осал қаржылық және АТ секторларында да айтарлықтай өсуде. Парадоксальды түрде айтсақ, оқиғалардың бұлайша дамуы олардың киберкеңістіктен келетін қауіптерге төзімділігін арттырады [13]. Осылайша, Қытай өз шекарасында ел экономикасының осал секторларын кибершабуылдардың қауіп-қатерінен қорғауға арналған қауіпсіз орта құруда.

Сонымен қатар, Қытайдың экономикалық өсуі азаматтық және әскери қолданбалы қосарлы мақсаттағы технологиялардың дамуына әкелді, бұл кейбір технологияларды зиянды пайдалану әлеуетіне байланысты киберқауіпсіздік саясатын дамытуды айтарлықтай қиындатты. Қытай ел ішіндегі ақпарат ағынын бақылауға тырысып, сол арқылы жергілікті халық арасында шиеленіс тудырса да, оның киберқауіпсіздік саясаты елдің ақпараттық жүйелерінде сақталған деректердің жайылып кету қаупін де тудырады.

Киберқылмыстық топтар ақпараттық инфрақұрылымды бұзып, нәтижесінде қытай деректерінің жайылып кетуіне әкеліп соғады, кейін олар Darknet-те үлкен сомаға (190 мың доллардан астам) сатылды. Мысалы, 2022 жылы белгісіз хакерлер Қытай үкіметінің қауіпсіздік желісінің бөлігі болып табылатын Alibaba Cloud жергілікті жеке бұлтына шабуыл жасау арқылы Шанхай ұлттық полициясының дерекқорында қамтылған 1 миллиард қытайлықтардың деректеріне қол жеткізді. Деректердің жайылып кетуі Қытайдың АТ қауымдастығын таң қалдырды, олар бұл қалай болуы мүмкін деген сауалдарға Қытай полициясы немесе үкіметі тарапынан ешқандай түсініктеме болған жоқ. Қытай қоғам сенімін сақтауға тырысып, ішкі ақпараттық жүйелерінің осалдығын мойындамау үшін бұл жағдайға түсініктеме бермеген шығар. Бұл ретте мемлекеттің өзі кибербарлау жүргізген болуы мүмкін, бұл ықтимал қатеге байланысты ашық деректердің сыртқа шығуына әкелді [14].

Сонымен қатар, Қытайдың өзі басқа мемлекеттерден мәліметтер алуға ұмтылады, бірақ бұл тек кибер барлау және киберқорғаныс мақсаттары үшін ғана емес, сонымен қатар геосаяси және экономикалық мүдделер үшін де орын алады. Осылайша, соңғы жылдары Қытай АҚШ, ЕО, Ресей, Украина және Африкадағы мемлекеттік органдар мен ірі компанияларға кибершабуылдар циклінің бастамашысы ретінде әрекет етті. Мемлекеттік деректер мониторинг және анықтау арқылы ҚХР ақпараттық қауіпсіздік саласында үлкен тәуекелдер тудыратын қуатты кибершабуылдар ағынын жүзеге асырып жатқанын растайды. Осы киберқауіптерге қарсы тұру Қытайдың саяси басымдықтары мен экономикалық ұмтылыстарын жан-жақты түсінуді, сондай-ақ барлық мүдделі тараптар үшін қауіпсіз және тұрақты киберкеңістікті қамтамасыз ету үшін халықаралық ынтымақтастыққа ұмтылуды талап етеді. Цифрлық әлем дамып келе жатқандықтан, ұлттық мүдделер, экономикалық өсу және жаһандық киберқауіпсіздік арасындағы нәзік тепе-теңдікті табу үшін тұрақты бағалау және диалог қажет.

Ұлттық киберқауіпсіздік индексі [15] әзірленді, ол 176 мемлекеттің ақпараттық қауіпсіздік саясатын сәтті жүзеге асырудағы қызметін бағалауға мүмкіндік береді.

2023 жылғы Ұлттық киберқауіпсіздік индексінде рейтингте жоғары орындарға ие болған ЕО мемлекеттерінің 80%-ға жуығы тәуекелдер мен киберқауіптерге қарсы тұруда ең табысты мемлекеттер болды. Бұл ұлттық деңгейде ақпараттық қауіпсіздікті қамтамасыз етудегі елдердің біртұтас және келісілген көзқарасын растайды. Өз кезегінде, Америка Құрама Штаттары осы салаға белсенді түрде инвестиция салып, озық технологияларды енгізіп жатқанына қарамастан, мемлекет 46-шы орынды иеленді, бірақ бұл көрсеткіш оң, өйткені олар тізімнің басында. Қытай 72-ші орында тұр, бұл да жалпы алғанда жақсы нәтиже көрсетеді, бірақ сонымен бірге елдің киберқауіпсіздік саласындағы қиындықтарға тап болғанын көрсетеді.

Осы тұрғыда елдер саяси және экономикалық аспектілерді ескере отырып, ақпараттық қауіпсіздік тетіктерін үнемі жаңартуға тырысуда. Осылайша, талдау арқылы халықаралық аренадағы ықпалды ойыншылар

арасындағы нәзік динамикаға баса назар аударылды, негізгі тәсілдер мен саяси жүйелердің ақпараттық қауіпсіздік стратегияларына әсері қарастырылды. Сонымен қатар, 1-кестеде саяси және экономикалық тұрғыдан сәйкес киберқауіпсіздік ландшафтарын қысқаша түсінуге ықпал ететін негізгі көрсеткіштер мен талдау нәтижелеріне толық шолу берілген.

1 Кесте. Мемлекеттердің ақпараттық қауіпсіздік тәуекелдерінің салыстырмалы талдауы

АҚШ	Еуропа Одағы	Қытай
Ақпараттық қауіпсіздіктің саяси аспектілері		
Америка Құрама Штаттары жеке бостандықтар мен демократиялық құндылықтарға баса назар аудара отырып, федералды жүйеде жұмыс істейді. Мұндай саяси жүйе киберқауіпсіздік саясатындағы ашықтық пен есеп беруді қамтамасыз етеді, қоғамдық пікірталастарға және шешім қабылдау процестеріне қатысуға мүмкіндік береді. Биліктердің бөлінуі тепе-теңдік пен тепе-теңдікті қамтамасыз етеді, бірақ ол мемлекеттік органдарда киберқауіпсіздік шараларының бөлінуіне әкелуі мүмкін. АҚШ үкіметі киберқауіптермен бірлесіп күресу үшін мемлекеттік және жеке секторлардың ынтымақтастығына мән беруде.	ЕО-ның саяси құрылымы мүше мемлекеттер арасындағы ынтымақтастық пен консенсусқа негізделген. Мұндай ынтымақтастықтың нәтижесі ақпараттық қауіпсіздікке қатысты заңдар мен нормативтік құқықтық актілерді үйлестіру болып табылады. ЕО-ның көп деңгейлі шешім қабылдау процесі мүше мемлекеттердің әртүрлі мүдделерін ескере отырып, ақпараттық қауіпсіздік тәуекелдерін тұтас түсінуге ықпал етеді. киберқауіптерге ұжымдық түрде қарсы тұру үшін трансшекаралық ынтымақтастықты дамытады .	Қытайдың саяси жүйесі ҚКП орталықтандырылған бақылауымен сипатталады, бұл киберқауіпсіздік мәселелері бойынша жылдам шешім қабылдауға мүмкіндік береді. Кибер егемендік принципі ақпараттың ағыны мен мазмұнын мемлекеттік бақылауға баса назар аударады, бұл қадағалау мен цензураның күшеюіне әкеледі. Қытай үкіметі ұлттық қауіпсіздікке белсенді көзқарас танытты, бұл кибермүмкіндіктерді өзінің саяси күн тәртібіндегі басымдыққа айналдырады.
Ақпараттық қауіпсіздіктің экономикалық аспектілері		
Америка Құрама Штаттары экономикалық держава ретінде ауқымды цифрлық инфрақұрылымы мен технологияға негізделген экономикасына байланысты маңызды киберқауіптерге тап болады. Экономикалық тыңшылық экономикалық бәсекеге қабілеттілік пен инновацияға айтарлықтай қауіп төндіреді. Қаржы және энергетика сияқты маңызды салаларға кибершабуылдар маңызды қызметтерді бұзып, қаржылық шығындарға әкеліп соқтыратын маңызды экономикалық әсер етуі мүмкін.	ЕО-ның экономикалық ұмтылыстары цифрлық бірыңғай нарықты құруды және жаһандық цифрлық ландшафтта экономиканың бәсекеге қабілеттілігін арттыруды қамтиды. Киберқауіпсіздік ЕО-ның экономикалық мақсаттарына жетудің ажырамас бөлігі болып табылатын цифрлық қызметтер мен деректер ағынына деген сенімді сақтау үшін маңызды. Киберқауіптер саудаға, инвестицияға және трансшекаралық іскерлік транзакцияларға әсер ететін кең таралған экономикалық әсер етуі мүмкін.	Қытайдың экономикалық амбициялары жаңа киберқауіптерді тудырып, технологиялық прогреске қомақты инвестиция құюда. Қытайдың өндірістік орталық және технологиялық өнімдерді жеткізуші ретіндегі рөлі жаһандық салдары болуы мүмкін жеткізу тізбегі тәуекелдерін тудырады. Мемлекет қаржыландыратын өнеркәсіптік тыңшылық Қытайдың экономикалық өсімін арттыруы мүмкін, сонымен бірге әділ сауда тәжірибесі мен халықаралық қатынастар туралы алаңдаушылық тудыруы мүмкін.

Дереккөз: Салыстырмалы талдау негізінде авторлар құрастырған

Осы саяси тәсілдерді зерделеу кезінде мемлекеттердің ақпараттық қауіпсіздік стратегияларына саяси жүйелердің ықпалын бағаламауға

болмайтыны белгілі болады. Америка Құрама Штаттары ақпараттық қауіпсіздіктің аймақтық саясатына көзқарасында экономикалық ойларға басымдық береді деп күтілуде. Бұл киберқауіпсіздік технологиясы мен инновацияға инвестицияның артуына ықпал етуі мүмкін. Киберқауіптердің көп қырлы мәселесін тиімді шешу саясаттың жауаптары олардың экономикалық әсерлерін, әсіресе миссиясы маңызды салаларда мұқият қарастыруды талап етеді. Өз кезегінде ЕО саясаты цифрлық бірыңғай нарықты құру және экономиканы бәсекеге қабілетті етуді қамтитын экономикалық мақсаттарына қол жеткізуге бағытталған. Осы мақсаттарға сәтті жету үшін бұл қауымдастыққа цифрлық қызметтерді тиімді қорғау және оларға деген халықтың сенімін сақтау үшін ұтымды ақпараттық қауіпсіздік шараларын жүзеге асыруы қажет. Сонымен қатар, Қытай өзінің стратегиялық мақсаттарына ұмтылуда, мұнда технологиялық дамулар жеткізу тізбегіндегі ықтимал осалдықтарды тиімді шешу және ішкі және халықаралық экономикалық мүдделерді қорғау үшін сенімді киберқауіпсіздік жүйесін құруды қажет етеді.

Сонымен қатар, киберқауіптердің экономикалық әсері мемлекеттің саяси жүйесіне сәйкес киберқорғанысты күшейту, сондай-ақ аймақтық және халықаралық деңгейдегі ықтимал ынтымақтастық арқылы жаһандық ауқымда цифрлық тұрақтылық үшін киберқауіпсіздік шараларын күшейту қажеттілігін айқын еске салады. Осылайша, халықаралық ынтымақтастық саласы кибершабуылдардан тиімді қорғау және дереу әрекет ету үшін ақпараттық қауіпсіздік тәуекелдерінің болашақ өсуін шешудің маңызды перспективасын білдіреді.

Қазіргі геосаяси жағдайда АҚШ, Еуропалық Одақ және Қытай сияқты жаһандық маңызы бар өңірлер үшін қауіптер туралы жедел ақпарат алмасуға және әрекет ету тетіктерін үйлестіруге бағытталған бірлескен іс-шараларды жандандыру үшін өз әлеуетін стратегиялық пайдалану өте маңызды. Осы мүмкіндіктерді пайдалана отырып, қуатты аймақтар өздерінің ұжымдық қауіпсіздігін тиімді нығайтып, көп қырлы сын-қатерлер мен туындайтын қауіптерге қарсы тұра алады.

Киберқауіптерге қарсы тұрудың тағы бір маңызды құралы АҚШ-та қолданылып жүрген мемлекеттік-жекеменшік әріптестікті нығайту болуы мүмкін. Сонымен қатар, Қытай мен Еуропалық Одақ да жеке сектормен ынтымақтастықты пайдаланады, бірақ ол әлі белсенді кезеңге өткен жоқ. Осылайша, мемлекеттік-жекеменшік әріптестік өзгермелі киберқауіптер ландшафтын жақсырақ түсінуге және оларға қарсы тұрудың тиімді шараларын әзірлеуге ықпал етеді.

Киберқауіпсіздік саласындағы ақпараттық саясатты дамытуда персоналды оқыту және олардың біліктілігін үздіксіз арттыру да маңызды аспект болып табылады. Мемлекеттер киберқауіпсіздік саласындағы мамандардың жетіспеушілігін жабу ғана емес, сонымен қатар аймақтың киберқауіптерден қорғану қабілетін жақсарту үшін жұмыс күшін дамытуға инвестиция салуды жалғастыруы керек.

Бұл ретте әлемдік қауымдастық ақпараттық қауіпсіздік саласындағы туындайтын тәуекелдерді ескере отырып, киберкеңістіктегі қызметтің бірыңғай ережелері мен қағидаларын әзірлеуі, сондай-ақ, мемлекеттер мен халықаралық ұйымдар арасында жаһандық саяси кеңістікте тұрақтылық пен ақпараттық қауіпсіздікті қамтамасыз ету үшін диалог орнатуы қажет.

Қорытынды

Осылайша, зерттеу әрбір аймақтың саяси және экономикалық мүдделеріне сәйкес туындайтын киберқауіптерді шешудің, сондай-ақ дамыған әлем үшін қиындықтар мен мүмкіндіктерді көрсететін неғұрлым қауіпсіз цифрлық болашақты құру үшін халықаралық ынтымақтастық пен ынтымақтастықты дамытудың маңыздылығын көрсетеді.

Саяси ландшафт пен экономикалық динамика аймақтық мүдделерді қалыптастыруды жалғастыруда, дамыған аймақтар үшін ақпараттық кеңістіктегі киберқауіптерді тиімді шешу үшін ынтымақтастыққа, инновацияларға және саясатты бейімдеуге басымдық беру өте маңызды. Сонымен қатар, әлемдік қауымдастықтың өңірлік ландшафтын ескере отырып, тұрақты ақпараттық кеңістікті, сондай-ақ әлемдік қауымдастықтың болашағын құру үшін қазіргі заман талабына сай жаңа киберқауіпсіздік технологияларын дамыту басым қадамдар ретінде қабылданады, әрі мемлекеттік-жекеменшік әріптестік, ал белсенді шаралар мен стратегиялық жоспарлау ақпараттық қауіпсіздіктің өңірлік саясатын нығайтуға мүмкіндіктер жасай отырып, ықтимал қауіптер мен проблемаларды жеңуге көмектеседі.

ӘДЕБИЕТ

[1] Eriksson J., Giacomello G. The information revolution, security, and inter-national relations: (IR)relevant theory? // International Political Science Review. – 2006. – № 27. – P. 221–244.

[2] Cavelty M., Egloff F.J. The Politics of Cybersecurity: Balancing Different Roles of the State // St. Antony's International Review. – 2019. – Volume 1. №156. – P 37–57.

[3] Kambourakis G., Neisse R., Nai-Fovino I. Information security in the age of EU-Institutions digitalisation, a landscape analysis. - European Commission, Joint Research Centre, 2021. – 52 p.

[4] Гирис В.А. Правовой статус органов и учреждений Европейского Союза в области обеспечения кибербезопасности // Международное право и международные организации. – 2023. – №1. – С. 26–41.

[5] Жатканбаева А.Е. Об опыте правового регулирования обеспечения информационной безопасности в США и ЕС // Вестник КазНУ. Серия Юридическая. – 2016. – № 3 (79). – С. 300-306.

[6] Понька Т.И., Рамич М.С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. –2020. – № 20 (2). – С. 382–394.

[7] Li Z., Guo X., He Q. A Study of Chinese Policy Attention on Cyber-security // IEEE Transactions on Engineering Management, In press, 2020. – 60 p.

[8] Hampson F.O., Sulmeyer M., Hathaway M. [et al.] Getting Beyond Norms: New Approaches to International Cyber Security Challenges: Special Report, Centre for International Governance Innovation. Waterloo, 2017. – 46 p.

[9] Rona T.P. Weapons Systems and Information War. Boeing Aerospace Company. - Seattle, Washington,1976. – 86 p.

[10] Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security, The White House, 2011. – 28 p. https://obamawhitehouse.archives.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf

[11] Whyte C. Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Information Warfare // Journal of Cybersecurity. – 2020. – Volume 1. № 6. – P. 1-17.

[12] Филлипс А. Пегас угрожает Евросоюзу изнутри как троянский конь // Euronews. – 2022.https://ru.euronews.com/my-europe/2022/02/21/eu-parliament-pegasus-investigation.

[13] Fei G. China's Cybersecurity Challenges and Foreign Policy // Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity. – 2011. – P. 185-190.

[14] В даркнете продают данные 1 млрд китайцев // Аналитическое агентство Tadviser. – 2023. https://www.tadviser.ru/index.php/Статья:DLP:_громкие_утечки_информации.

[15] National Cyber Security Index. https://ncsi.ega.ee/ncsi-index/?order=ncsi.

REFERENCES

[1] Eriksson J., Giacomello G. The information revolution, security, and inter-national relations: (IR) relevant theory?. International Political Science Review, 2006, No. 27, pp. 221–244.

[2] Cavelty M., Egloff F.J. The Politics of Cybersecurity: Balancing Different Roles of the State. St Antony's International Review, 2019, vol. 1, No.156, p. 37–57.

[3] Kambourakis G., Neisse R., Nai-Fovino I. Information security in the age of EU-Institutions digitalisation, a landscape analysis. European Commission, Joint Research Centre, 2021, 52 p.

[4] Giris V.A. Pravovoj status organov i uchrezhdenij Evropejskogo Soyuza v oblasti obespecheniya kiberbezopasnosti [Legal status of the bodies and institutions of the European Union in the field of cybersecurity]. Mezhdunarodnoe pravo i mezhdunarodnye organizacii, 2023. No. 1, p. 26–41 [in Russ.].

[5] Zhatkanbaeva A.E. Ob opyte pravovogo regulirovaniya obespecheniya informacionnoj bezopasnosti v SSHA i ES [On the experience of legal regulation of information security in the United States and the EU]. Vestnik KazNU. Seriya Yuridicheskaya, 2016, vol. 3, No. 79, p. 300-306 [in Russ.].

[6] Pon'ka T.I., Ramich M.S., U Yu. Informacionnaya politika i informacionnaya bezopasnost' KNR: razvitie, podhody i realizaciya [Information Policy and Information Security of PRC: Development, Approaches and Implementation]. Vestnik Rossijskogo universiteta druzhby narodov. Seriya: Mezhdunarodnye otnosheniya, 2020, vol. 2. No. 20, p. 382-394 [in Russ.].

[7] Li, Z., Guo, X., He, Q. A Study of Chinese Policy Attention on Cyber-security. IEEE Transactions on Engineering Management., In press, 2020, 60 p.

[8] Hampson, F.O., Sulmeyer, M., Hathaway, M. [et al.] Getting Beyond Norms: New Approaches to International Cyber Security Challenges. Special Report, Centre for International Governance Innovation, Waterloo, 2017, 46 p.

[9] Rona T.P. Weapons Systems and Information War, Boeing Aerospace Company. Seattle, Washington, 1976, 86 p.

[10] Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security. The White House, 2011, 28 p. https://obamawhitehouse.archives.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf.

[11] Whyte C. Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Information Warfare. Journal of Cybersecurity, 2020, vol. 1, No. 6, pp. 1-17.

[12] Fillips A. Pegas ugrozhaet Evrosoyuzu iznutri kak troyanskij kon' [Pegasus threatens the EU from within like a trojan horse]. Euronews, 2022. https://ru.euronews.com/my-europe/2022/02/21/eu-parliament-pegasus-investigation [in Russ.].

[13] Fei G. China's Cybersecurity Challenges and Foreign Policy. Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, 2011, p. 185-190.

[14] V darknete prodayut dannye 1 mlrd kitajcev [The darknet sells data of 1 billion Chinese]. Analiticheskoe agentstvo Tadviser, 2023. https://www.tadviser.ru/index.php/Статья:DLP: громкие утечки информации [in Russ.].

[15] National Cyber Security Index. https://ncsi.ega.ee/ncsi-index/?order=ncsi

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕГИОНАЛЬНОЙ ПОЛИТИКЕ РАЗВИТЫХ СТРАН МИРА

*Дмитриева А.С.[1], Жолдасбекова А.Н.[2], Оспанова А.Н.[3]

*[1]докторант кафедры регионоведения факультета международных отношений, ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

e-mail: dmitriyeva.alyona@gmail.com

[2]кандидат политических наук, профессор кафедры регионоведение, факультета международных отношений, ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

e-mail: eic.astana@gmail.com

[3]Ph.D., ассоциированный профессор, заведующий кафедрой регионоведения факультета международных отношений, ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

e-mail: ospanovaa@mail.ru

Аннотация. В эпоху цифровых технологий обеспечение информационной безопасности стало важной приоритетной задачей в дипломатии и мировой политике, ввиду аддиктивной зависимости государств от IT-технологий и возникающих киберрисков на данном фоне. При этом риски информационной безопасности представляют собой сложную проблему для акторов мировой политики, оказывая влияние на их политический и экономический ландшафт. В данном исследовании представлен комплексный сравнительный анализ рисков информационной безопасности США, Европейского союза и Китая, рассматриваются их политические подходы, экономические амбиции и влияние на региональные политики информационной безопасности. Исследовательский вопрос фокусируется на понимании того, как меняющаяся политическая динамика и экономические устремления формируют стратегии информационной безопасности этих регионов. Методология исследования включает в себя сбор, анализ и сравнительное исследование данных, что позволяет получить целостное представление о ландшафте информационной безопасности каждого региона. Кроме того, на основе сравнительного анализа авторами была составлена таблица, в рамках которой изучены экономические и политические аспекты информационной безопасности в сравниваемых странах. В связи с этим, результаты исследования показали, что в США для противодействия киберугрозам особое внимание уделяется государственно-частному партнерству и инновациям, в Европейском Союзе - сотрудничеству и гармонизации нормативных актов, в то время как в Китае - киберсуверенитету и национальной безопасности. Проведенный анализ подчеркивает взаимосвязь между политикой, экономикой и рисками информационной безопасности, выявляя области сближения и расхождения между странами. Также авторами даны выводы и рекомендации для устранения поступающих киберугроз в целях устойчивого развития кибербезопасности в регионах.

Ключевые слова: информационная безопасность, киберриски, политический ландшафт, региональная политика, кибердипломатия, экономические амбиции, политические последствия, сравнительный анализ

INFORMATION SECURITY RISK ANALYSIS IN REGIONAL POLICIES OF DEVELOPED COUNTRIES OF THE WORLD

*Dmitriyeva A.S.[1], Zholdasbekova A.N.[2], Ospanova A.N.[3]
*[1]Doctoral student of the Department of Regional Studies, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
e-mail: dmitriyeva.alyona@gmail.com
[2]Candidate of Political Sciences, Professor, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
e-mail: eic.astana@gmail.com
[3]Ph.D., Associate Professor, Head of the Department of Regional Studies, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
e-mail: ospanovaa@mail.ru

Abstract. In the era of digital technology development, ensuring information security has become an important priority in diplomacy and world politics, due to the addiction of states from IT technologies and the emerging cyber risks against this background. At the same time, information security risks pose a complex problem for global political actors, influencing their political and economic landscape. In this study, the authors present a comprehensive comparative analysis of information security risks using the example of the United States, the European Union and China, examine the countries' political approaches, economic ambitions and consequences, and also analyze the impact of cyber threats on the regional policies of key regional players. The article's research question focuses on understanding how changing political dynamics and economic aspirations shape the information security strategies of these regions. The research methodology includes the collection, analysis, systematic and comparative study of data, which allows us to obtain a holistic view of the information security landscape of each region. In addition, based on the comparative analysis, the authors compiled a table in which the economic and political aspects of information security in the compared countries were studied. Key results show that in the United States, special attention is paid to public-private partnerships and innovation to counter cyber threats, the European Union emphasizes cooperation and harmonization of cybersecurity regulations, while China focuses on enhancing cyber sovereignty and national security. As part of the analysis, the authors trace the relationship between politics, economics and information security risks, highlighting areas of convergence and divergence between regions. The authors also provided conclusions and recommendations for eliminating incoming cyber threats for the sustainable development of cybersecurity in the regions.

Keywords: information security, cyber risks, political landscape, regional policy, cyber diplomacy, economic ambitions, political consequences, comparative analysis

Статья поступила 08.11.2023