РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

ҰЛТТЫҚ ЗАҢНАМАДАҒЫ КИБЕРНЕТИКАЛЫҚ ҚАУІПСІЗДІКТІҢ КЕЙБІР МӘСЕЛЕЛЕРІ

Ясинова Альбина Пархатовна
muxametnur@mail.ru
Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «Құқықтану» мамандығының 1-курс студенті, Астана, Қазақстан
Ғылыми жетекшісі: з.ғ.м., аға оқытушы Мырзатаев Н.Д.

Түйіндеме

Мақалада қазіргі таңда мемлекеттің өмірінде, оның экономикасы мен қауіпсіздігінде маңызды рөл атқаратын киберқауіпсіздік туралы кейбір мәселелер талқыланады.

Түйін сөздер: киберкеңістік, киберқауіпсіздік, киберқорғаныс.

Жаңа технологиялар мен электрондық қызметтер біздің күнделікті өміріміздің ажырамас бөлігі болды. Қоғам ақпараттық-коммуникациялық технологияларға күннен күнге тәуелді болуын ескере отырып, осы технологиялардың қорғалуы мен қол жетімділігі ұлттық мүдделер үшін өте маңызды тақырып болып табылады.

Қазіргі таңда киберқауіпсіздік ақпараттық қоғамды дамытудың міндетті шарты болып табылады, ондатехникалық қауіпсіздіктен бастап заңнамалық қауіпсіздікке дейінгі проблемалар мен олардың шешімдерінің шексіз тізбегі сақталуы мүмкін.

Қазіргі жағдайда киберқауіпсіздік мәселелері компьютерлік технологияның жекелеген объектісінде ақпараттық қауіпсіздіктің деңгейінен бастап, әрбір мемлекеттің ақпараттық қауіпсіздігі мен ұлттық қауіпсіздігінің ажырамас бөлігі ретінде киберқауіпсіздіктің бірыңғай жүйесін құру деңгейіне дейін шығады.Мысалы, 61 елдің киберқауіпсіздікті қамтамасыз ету мәселелері бойынша IMD Дүниежүзілік бәсекеге қабілеттілік орталығы жариялаған бәсекеге қабілеттілік индексіне сәйкес, Израиль жетекшілік етеді [1].

Таяу Шығыстағы ең көп компьютерленген ел ретінде Израиль жалпы қауіпсіздік қызметі (ШАБАК) жанындағы маңызды ақпараттық инфрақұрылымдарды бақылайтын ақпараттық қауіпсіздік бөлімін құрды, оның ішінде электр энергиясын өндіру, сумен қамтамасыз ету және т.б.

Әскери және азаматтық салаларда өсіп келе жатқан киберқауіптер туралы түсіне отырып, жүздеген адамнан тұратын мамандар тобын құру туралы шешім қабылдауға әкелді, олар бір жылдан кейін болашақта киберқауіптерге дайындалу үшін ұлттық деңгейде салыстырмалы жаңалықтарды ұсынды.

Инновациялар нақты технологиялардың дамуын ғана емес, сондай-ақ ұлттық қауіпсіздік құрылымдарымен өнеркәсіптік және академиялық топтар арасындағы ынтымақтастықты, білім берудің мектептік жүйесіндегі білім беру бағдарламаларын, біліктілікті арттырудың академиялық орталықтарын құруды, сыни ұлттық жүйелерді және басқа да көптеген жобаларды қамтыды[2].

Нәтижесінде 2011 жылы осы инновацияларды бақылауды, жоспарлауды және іске асыруды қамтамасыз ету үшін Израиль киберқауіпсіздігінің ұлттық бюросы құрылды. Бұл проблема жаһандық деңгейде өзекті болғандықтан, Израильде жинақталған тәжірибе және тиісті мемлекеттік стратегия біртіндеп жеке компанияларды ел экономикасының қуатты секторына айналдырды. Бүгінгі күні Израильдегі киберқауіпсіздіктің инфрақұрылымына шамамен бір жарым жүз компаниялар кіреді, оның ішінде Check Point сияқты фирмалар, сондай-ақ, осы салаға инвестиция салатын венчурлық қорлар, мысалы, Jerusalem Venture Partners (JVP) Cyber Labs, сондай-ақ жоғары технологиялық компаниялар мен академиялық топтардың арасындағы ынтымақтастықты жүзеге асыратын зерттеу жобалары да бар. Басқаша айтқанда, Израильдік компаниялардың саны мен дамуы көбейген сайын, жаңа үрдіс белгіленді. Стартаптарды жеткізушіден Израиль бірте-бірте халықаралық жоғары технологиялық орталыққа, бірінші кезекте киберқауіпсіздік саласындағы жетекші әлемдік көшбасшыға айналды [2]. Сонымен қатар, әлемдік аренада белгілі бір мемлекеттегі

ақпараттық қауіпсіздік саясаты Киберқауіпсіздік стратегияларын қабылдау арқылы қамтамасыз етіледі.

Осылайша, 2003 жылы киберқауіпсіздіктің алғашқы стратегиясы АҚШ-та пайда болды. Осыдан кейін Виртуалды кеңістіктегі қауіпсіздіктің стратегиясы мен іс-қимыл жоспарлары бүкіл Еуропа бойынша таралды. Еуропалық Одақ (ЕО) елдерінің және онымен шектелмеген кейбір елдердің барлық ұлттық киберқауіпсіздік стратегияларының тізімі Еуропалық желілік және ақпараттық қауіпсіздік агенттігі (ENISA) арқылы жарияланды [3].

Олардың кейбіреулері туралы толығырақ айтып өтейік. Германиядағы киберкеңістіктегі қауіпсіздік стратегиясы 2011 жылдың басында қабылданды, және басты назар кибершабуылды алдын-алу және кудалау, кездейсоқ факторлармен туындауы мүмкін IT-жабдықтарының істен шығуын болдырмауға бағытталды. Сондай-ақ, Германия стратегиясы қоғамдық қауіпсіздіктің маңызды функцияларын қамтамасыз ету арқылы IT жүйелерін қорғау бойынша қосымша іс-әрекеттердің қажеттігін талдайды, сондай-ақ жаңа жұмыс тобын құру арқылы шағын және орта бизнесті қолдау. Бұдан басқа, 2015 жылдың 11 шілдесінде Германия парламенті киберқауіпсіздік туралы заң қабылдады, оған сәйкес 2000-нан астам қызмет берушілер екі жыл ішінде киберкеңістікте жаңа қауіпсіздік стандарттарын енгізуге мәжбүр болады, әйтпесе неміс компаниялары 100 мың еуро айыппұл төлейді. Заң көлік, денсаулық сақтау, су шаруашылығы, телекоммуникация қызметтері, қаржы және сақтандыру компаниялар сияқты маңызды инфрақұрылым ретінде көрсетілген мекемелерге әсер етеді. Сонымен қатар, жаңа заң компанияларды Германияның ақпараттық қауіпсіздігінің федералды ведомствосына (BSI) кибер-шабуыл туралы хабардар етуді міндеттейді [4].

Еуропалық Одақ елдерінен тағы бір мысал ретінде Эстонияны әкелуге болады, оның киберқауіпсіздіктің 2014-2017 жылдарға арналған стратегиясы қабылданды және бұл киберқауіпсіздікті жоспарлаудың негізгі құжаты болып табылады. Сондай ақ, ол 2008-2013 жылдардағы киберкеңістікті қорғау стратегиясының көптеген мақсаттарын жүзеге асыруды жалғастырады. Киберқауіпсіздік стратегиясының төрт жылдық мақсаты - киберқауіпсіздікті қамтамасыз ету және киберқауіптер туралы қоғамның хабардарлығын арттыру, осылайша киберкеңістікке сенімділікті қамтамасыз ету,өмір тіршілігін қамтамасыз ететін қызметтердің негізін қалайтын ақпараттық жүйелерді қорғау, мемлекеттік және жеке секторлардағы кибершақауіптерді жеңу, ұлттық киберқауіпсіздікті мониторингтеу жүйесін енгізу, мемлекеттің сандық ресурстарының тұтастығын қамтамасыз ету, маңызды ақпараттық инфрақұрылымды қорғау саласындағы халықаралық ынтымақтастықты дамыту, киберқылмыспен күресуді жетілдіру, киберқауіпсіздікті қамтамасыз ету үшін заңнамалық базаны құру және т.б. [5].

Сонымен қатар, 2008 жылғы 4 мамырда НАТО-ның Брюссельдегі кеңесі отырысында Таллинде НАТО-ның Кибер-қорғаныс орталығын құру туралы Өзара түсіністік туралы меморандумға қол қойылды, кейіннен «НАТО-ның киберқауіпсіздікті жетілдіру орталығы» атауын алды. (NATO cooperative cyber defence centre of excellence). Аталған орталықтың мақсаты - Киберкеңістіктегі қауіпсіздікті қамтамасыз ету бойынша Альянстың мүмкіндіктерін кеңейту, оның ішінде ақпаратты қорғаудың жаңа жолдарын зерттеу және дамыту, мүше елдердің ақпараттық жүйелеріне зиянды әсерлерді анықтау, келтірілген зиянды бағалау, олардың жұмысқа қабілеттілігін қалпына келтіру, сондай-ақ кибершабуылдың алдын-алу шаралары, киберқауіпсіздік саласындағы НАТО-ның қызметін құқықтық қамтамасыз ету, ақпараттық қауіпсіздікті қамтамасыз ету саласындағы тәжірибені зерттеу, синтездеу және тарату, оқу-әдістемелік жұмыс және мүше елдердің ақпараттық қауіпсіздігі саласындағы мамандарды дайындау. Бұл орталық кибер-кеңістіктегі зерттеулерге ерекше назар аударады, оның негізгі бағыттары кибер-кеңістіктегі қауіпсіздікті қамтамасыз етудің тұжырымдамалары мен стратегияларын әзірлеу, сондай-ақ НАТО-да және жекелеген мүше елдерде киберпрофилактиканы жүргізу концепцияларын әзірлеу, сондай-ақ Альянстың және мүше елдердің цифрлы есептеу жүйелерінің қауіпсіздігін қамтамасыз ету бойынша техникалық шешімдерді әзірлеу, кибершабуылдың салдарын анықтау және жою, сырттан

кіруі әдістерін анықтау болып табылады. Осылайша, әлемдік тәжірибе бүгінгі таңда киберқауіпсіздік мәселелері жаһандық деңгейде екенін көрсетеді, бұл өз кезегінде ұлттық ғана емес, сондай-ақ тиісті халықаралық қауіпсіздік стратегиясын да дамытуды талап етеді [6].

Қазақстандағы ақпараттық-коммуникациялық технологиялардың дамуының жоғары қарқыны тиісті инфрақұрылымды қорғау мәселелерін өзекті етеді, себебі оның зақымдануы немесе жойылуы елдің қауіпсіздігі үшін елеулі салдар тудыруы мүмкін. «Касперский зертханасының» мәліметтері бойынша, Қазақстан ең көбі веб-шабуылға ұшырайтын елдердің тізімінде 6- шы, «троянцы вымогатели» шабуылдаушылардың шабуылына ұшырайтын елдердің тізімінде 9-шы орында тұр [7]. Сонымен бірге, Қазақстан Республикасының заңнамасын талдау барысында заңнамада киберқылмыс, киберкеңістік, киберқауіпсіздік, киберқорғаныс секілді негізгі тұжырымдамаларға анықтама берілмегенін көрсетеді. Соның салдарынан қолданыстағы заңнамада кейбір кемшіліктер пайда болады. Осыған байланысты Қазақстан Республикасы Білім және ғылым министрлігінің «Ғаламдық байланыс желілеріндегі құқық бұзушылықтарға қарсы іс-қимылдың құқықтық негізі» атты іргелі зерттеулер ҒЗЖ шеңберінде «ақпараттық қауіпсіздік» және «киберқауіпсіздік» ұғымдарының ара қатынасын, сондай-ақ Қазақстан Республикасының заңнамасындағы «киберқауіпсіздік» ұғымы мәселелерін қарастыруды жөн көрдім. Бұрынғы кеңестік кеңістіктің аумағында киберқауіпсіздікті түсіну үшін әдетте ақпараттық қауіпсіздіктің кең тұжырымдамасы қолданылады, ол ақпараттық саладағы сыртқы және ішкі қауіптерден адамның, қоғамның, мемлекеттің өмірлік маңызды мүдделерін қорғауды, пайдалануды және дамытуды білдіреді. Сонымен қатар, Батыстың демократиялық елдерінде «киберқауіпсіздік» термині қандай ақпарат таратылатынына қарамастан (балалар порнографиясы мен ұқсас қылмыстық мазмұннан басқа) компьютерлік желілердің сенімділігін, тұрақтылығын және қол сұғылмауын білдіреді.

Қазақстанның ұлттық заңнамасында «киберқауіпсіздік» және «киберқорғаныс» ұғымдары жоқ, яғни қолданыстағы заңнамада тек «ақпараттық қауіпсіздік» және «ақпаратты қорғау» ұғымдары қолданылады. Осылайша, Қазақстан Республикасының «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V Заңының 1-бабының 33-тармағында [8] «электрондық ақпараттық ресурстарды қорғау» тұжырымдамасына анықтама берілген: «Электрондық ақпараттық ресурстарды, ақпараттық жүйелерді қорғау – ақпаратты алу, көшірмесін түсіру, тарату, бұрмалау, жою немесе бұғаттау жөніндегі заңсыз іс-әрекеттерді қоса алғанда, электрондық ақпараттық ресурстарды, ақпараттық жүйелерді сақтауға, оларға заңсыз қол жеткізуді болғызбауға бағытталған құқықтық, ұйымдастырушылық және техникалық іс-шаралар кешені». «Ақпараттық қауіпсіздік» ұғымына тоқталатын болсақ «Қазақстан Республикасының ұлттық қауіпсіздігі туралы» Заңының 4-бабының 5-тармағына сәйкес: «ақпараттық қауіпсіздік – елдің орнықты дамуы және ақпараттық тәуелсіздігі қамтамасыз етілетін, ақпарат саласындағы нақты және ықтимал қауіп-қатерлерден Қазақстан Республикасы ақпараттық кеңістігінің, сондай-ақ адамның және азаматтың құқықтары мен мүдделерінің, қоғам мен мемлекеттің қорғалуының жай-күйі».

«Ақпараттандыру туралы» Қазақстан Республикасының Заңында «ақпараттық қауіпсіздік» терминінің анықтамасы жоқ, бірақ осы Заңның 1-бабының 4-тармағында ақпарат саласындағы ұлттық операторға сілтеме жасайды: «ақпараттандыру саласындағы оператор – Қазақстан Республикасы Үкіметінің шешімімен құрылған, мемлекеттік ақпараттық жүйелер мен мемлекеттік электрондық ақпараттық ресурстарды интеграциялау жөніндегі, ақпараттандыру саласындағы бірыңғай техникалық саясатты іске асыруға қатысу жөніндегі міндеттер, «электрондық үкіметтің» инфрақұрылымы жобалық интеграторының функциялары жүктелген заңды тұлға;» -деп түсіндіріледі. Осылайша, Қазақстан Республикасының заңнамасында қарастырылып отырған терминдердің ара қатынасын зерттей отырып, біз тек «ақпараттық қауіпсіздік» және «ақпаратты қорғау» терминдеріне және ол заңнамада жоқ, бірақ арнайы әдебиеттерде бар «киберқауіпсіздік» және «киберқорғаныс» терминдеріне сүйене аламыз.

Ақпараттық қауіпсіздікті екі жолмен көрсетуге болады: біріншіден, бұл мемлекеттік басқару жүйесінің ұйымдастырушылық элементі, ал екіншіден, бұл мемлекеттік басқару тиімділігінің көрсеткіші. Яғни, қауіптердің іске асуы мемлекеттік басқару жүйесінің жұмыс істеуінің тиімсіздігін көрсетеді. Қазіргі уақытта ақпараттық кеңістіктегі кез-келген қауіп-қатерлерді олардың пайда болуы мен қалай іске асқанын ескере отырып қарастыру керек. «Ақпаратты қорғау» ұғымын аша отырып, бұл тұжырымдама шексіз диапазоны бар ақпаратты қорғауға бағытталғанын, яғни жеке адамға да, бүкіл мемлекетке де қатысты болуы мүмкін екенін атап өту керек. Сондықтан да, Қазақстан Республикасының заңнамасында «ақпараттың қорғалуы» терминінің нақты анықтамасы жоқ, әрбір нормативтік құқықтық актіге белгілі бір нормативтік құқықтық актіге тікелей қатысы бар ақпаратты қорғау туралы анықтама беріледі. Осыдан «ақпараттық қауіпсіздік» және «ақпаратты қорғау» ұғымдарының іс жүзінде де, заңмен де байланысты екендігі туралы қорытынды жасауға болады.

Қарастырылып отырған ұғымдардың тығыз қарым-қатынастарына сүйене отырып, ақпарат пен ақпараттық қауіпсіздікті қамтамасыз ететін негізгі қағидалар әзірленді: - деректердің тұтастығы - ақпаратты жоғалтуға әкелетін сәтсіздіктерден қорғау, сондай-ақ деректерді рұқсатсыз жасау немесе жоюдан қорғау;-ақпараттың құпиялылығы;-барлық уәкілетті қолданушыларға арналған ақпараттың қол жетімділігі.

Қазақстандық заңнамада «ақпараттық қорғау» ұғымының жоқтығы осы ұғымға «киберқауіпсіздік» және «киберқорғаныс» ұғымын жақындатады. Осыған байланысты «киберқауіпсіздік» және «киберқорғаныс» ұғымдарын ашу үшін «киберқауіпсіздік» термині «кибернетикалық қауіпсіздік» терминімен жиі ауыстырылатын арнайы әдебиетке сілтеме жасауды жөн деп көрдім. М.С. Соколовтың ойынша, «Кибернетикалық қауіпсіздік - бұл оны бұзу мүмкін емес қауіпсіздік жағдайындағы басқару» [9].

Бұл жағдайда киберқауіпсіздік қоғамның барлық салаларына әсер ететін ұлттық маңызды стратегиялық мәселе ретінде қабылданатындықтан, «мүмкін емес» деген сөзді «жағымсыз» деген сөзбен ауыстырған жөн. Сондықтан да, мемлекеттің ұлттық қауіпсіздігі тұрғысынан кез-келген араласулар, атап айтқанда, компьютерлік желілердің, ақпараттық кеңістіктің бұзылуы мүлдем жағымсыз. Сонымен қатар, Финляндияның «Sitr» тәуелсіз инвестициялық қорының өкілі Микко Козоненнің айтуынша, «киберқауіпсіздік қоғамның барлық мүшелерінің электронды және желілік қауіпсіздігі» [10].

«Киберқорғаныс» терминіне келетін болсақ, бұл термин зерттелмеген, тіпті арнайы әдебиетте де оның қолданылуы сирек кездеседі. Бір нәрсе белгілі, «киберқауіпсіздік» және «киберқорғаныс» кибернетикалық кеңістікпен тікелей байланысқа ие, ол өз кезегінде компьютерлер мен компьютерлік желілерде орналасқан «екінші әлем». Демек, «киберқауіпсіздік» және «киберқорғаныс» терминдерін анықтау мәселесі аса өзекті болып табылады. Осыған байланысты бүкіл әлем қоғамдастығының ортақ мақсаттарын одан әрі қалыптастыру мақсатында осы терминдердің жалпы қабылданған түсіндірілуімен (анықтамасымен) келісу қажет.

Егер Қазақстан Республикасының ішкі заңнамасы туралы айтатын болсақ, онда «ақпараттық қауіпсіздік» және «ақпаратты қорғау» терминдері Республиканың кейбір нормативтік-құқықтық актілерінде ғана бар екендігін көрсетті, сонымен қатар, олар толық көлемде жария етілмеген, бұл заңдардың нормаларын жүзеге асыруды қиындатады. Атап айтқанда, оны «ақпараттандыру туралы» және «ақпаратты қорғау» ұғымдары қолданылатын «Ақпараттандыру туралы» ҚР Заңынан үлгі ретінде келтіруге болады, бірақ бұл нормативтік құқықтық актіде «киберқауіпсіздік» және «киберқорғаныс» ұғымдары жоқ, және бұл түсінікті, өйткені бұл терминдер белгілі бір ерекшелікке ие. Ал «Ақпараттандыру туралы» Заң жан-жақты нормаларды өзінде сақтай алмайды. Осылайша, ағымдағы шындық «киберқауіпсіздік» және «киберқорғаныс» ұғымдарына анықтамаларды қамтитын, сонымен қатар киберқауіпсіздікті қамтамасыз етудің мемлекеттік үлгісін реттеуге, жеке және мемлекеттік органдардың киберқауіпсіздікке қатысты саясатты талқылау және бекітуге мүмкіндік беретін тиісті механизмді анықтауға бағытталған нормаларды қамтитын

«Ғаламдық байланыс желілеріндегі құқық бұзушылықтарға қарсы күрес туралы» Заң қабылдау қажеттілігін көрсетеді.

Жоғарыда айтылғандардан, ақпараттық қауіпсіздік – кімнің және қандай құралмен ақпаратқа қол сұғылғандығына байланысты емес, кез-келген ақпараттың қауіпсіздігін білдіретін кең түсінік.

Киберқауіпсіздік ақпараттық дерекқорлардың, сондай-ақ компьютерлік желілерге кіретін түрлі бағдарламалардың қауіпсіздігін білдіреді. Демек, «киберқауіпсіздіі» және «ақпараттық қауіпсіздік» бір нәрсе емес екені анық, себебі күрделі ақпарат инфрақұрылымдарының қауіпсіздігінің киберқауіпсіздікке тек жартылай қатысы бар. Сонымен қатар көптеген мемлекеттерде «киберқауіпсіздік» терминінің анықтамасының болмауы және оның орнына «ақпараттық қауіпсіздік» терминін пайдалануды артық көрулері демократияның белгілі бір тапшылығын сезіндіреді, өйткені олар компьютерлік желілерді қорғаудан басқа, өздерінің саяси, экономикалық және әлеуметтік тұрақтылығына қауіп төндіретін ақпаратты таратуға жол бермеуге ұмтылады. Ақпаратты қорғау және «киберқорғаныс» терминдерінің арасындағы ара-қатынасты алатын болсақ, бұл аз корреляциялық терминдер. Ақпаратты қорғау - мүдделі тұлғаның ақпараттың меншік иесі белгілеген құқықтар мен оған қол жеткізу ережелерін бұза отырып, қорғалатын ақпараттарды алуына жол бермеуге бағытталған кең ауқымды іс-шаралар. Киберқорғаныс компьютерлік желілерді қорғауды, компьютерлік бағдарламаларды, желілерді және дерекқорларды өзгертуге, жоюға немесе бүлдіруге қабілетті компьютерден тыс қол сұғушылықтан қорғауды қамтиды. Дегенмен, бұл екі термин Қазақстан Республикасының ұлттық заңнамасында іс жүзінде қолданылмайды. Осыған байланысты «киберқауіпсіздік» және «киберқорғаныс» терминдерін анықтайтын «Жаһандық коммуникациялық желілерде құқық бұзушылықтарға қарсы күрес туралы» Заңды қабылдау қажет.

Біздің ойымша, «Жаһандық коммуникациялық желілерде құқық бұзушылыққа қарсы күрес туралы» Заңның 2-бабындағы «Негізгі ұғымдар» терминдерінің біреуі «киберқауіпсіздік» және «киберқорғаныс» болады, оларға келесідей анықтама беруге болады: -киберқауіпсіздік - адамның, азаматтың, қоғамның және мемлекеттің киберкеңістіктегі өмірлік мүдделерін қорғау;-кибернетикалық кеңістік – ақпараттық, жаһандық телекоммуникациялық жүйелерінің ережелері және олардың бірігіп жұмыс істеуі нәтижесінде пайда болатын орта. Сондай-ақ, ұсыныс ретінде, киберқауіпсіздікке қатысты қауіпсіздік мәселелері бойынша кейбір нормативтік құқықтық актілерге түзетулер енгізудің маңыздылығын атап өту керек. Мысалы, «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы» Қазақстан Республикасы Заңының 6-бабының 16,17-тармақтарына мынадай мазмұндағы толықтыру енгізу: -«Қазақстан Республикасына қарсы қарулы агрессия дайындау және жасау үшін кибернетикалық кеңістікті пайдалану».

Бүгінгі күні ақпараттандыру және байланыс саласындағы ақпараттық қауіпсіздік саясатын іске асыру барысында Қазақстан Республикасы Президентінің 2016 жылғы 6 қазандағы Жарлығымен Қазақстан Республикасы Қорғаныс және Аэроғарыштық өнеркәсіп министрлігі құрылды.Осы Жарлыққа сәйкес Қазақстан Республикасының Үкіметіне ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі комитетті құруды тапсырды, ол қазіргі уақытта ұлттық ақпараттық қауіпсіздік саласындағы мемлекеттік саясатты әзірлеуге уәкілетті орган (реттеуші) ретінде әрекет етеді, бұл елдің киберқауіпсіздігін қамтамасыз етудегі маңызды қадам болып табылатындығы сөзсіз.

Қолданылған әдебиеттер тізімі:

1 IMD-2016: Израиль признан мировым лидером в обеспечении кибер-безопасности31/05/2016 г.

2 Есмуханова Ә., Қази А. Халықаралық және ұлттық заңнамадағы киберқауіпсіздік 21.12.201

3 DPI for network security | Download DPI application | adlinktech.com

ADLINK DPI solutions with high performance, availibility, throughput and densit

4 John ScottAnatomy of a cyber risks stress test. November 25, 2016. Zurich Insurance Group. 5 Стратегия кибербезопасности эстонии 2014-2017. Министерство экономики и коммуникаций.21 окт. 2015 г.

7 «Лаборатории Касперского» 3 нояб. 2016 г. 8 Закон Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации» (с изменениями и дополнениями по состоянию на 03.07.2013 г.).

9 Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция

10 Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция