Халықаралық және ұлттық заңнамадағы киберқауіпсіздік

- Жаңа технологиялар, электрондық қызмет көрсетулер біздің күнделікті өміріміздің ажырамас бөлігіне айналды. Қоғамның күн сайын ақпараттық-коммуникациялық технологияларға тәуелді боп бара жатқанын ескерсек, осы технологиялардың қорғанысы мен қолжетімділігі сыни сәт және ұлттық мүдделер үшін маңызды тақырыпқа айналады. Бүгінгі күні киберқауіпсіздік ақпараттық қоғамның дамуының қажетті шарты болып табылады, оның соңынан техникалықтан бастап заңнамалықпен аяқтағанда шегі жоқ қауіпсіздік мәселелерінің тізімі мен олардың шешімі тұрады. Заманауи жағдайда киберқауіпсіздік мәселелері есептеуіш техниканың жеке объектісіндегі ақпаратты қорғау деңгейінен, әр мемлекеттің ақпараттық және ұлттық қауіпсіздігінің құрамдас бөлігі ретінде киберқауіпсіздіктің бірыңғай жүйесін құру деңгейіне шығады. Осылайша, IMD World Competitiveness Center жарияланған Бәсекеге қабылеттілік индексі-2016 сәйкес, киберқауіпсіздікті қамтамасыз ету мәселелерінде 61 елдің ішінде Израиль көш бастап тұр.

- Таяу Шығыстағы ең компьютерленген ел болғандықтан, Израильмен Қауіпсіздіктің жалпы қызметінің (ШАБАК) жанында аса маңызды ұлттық инфрақұрылымдарды, олардың ішінде электр энергиясы, сумен қамтамасыз ету және басқа да өндірістерді бақылайтын ақпараттық қауіпсіздік бөлімі құрылды. Әскери сияқты азаматтық салаларда да кибернетикалық қауіптің өсуін сезіну, жүздеген мамандардан тұратын арнайы топ құру туралы шешімге әкелді, олар бір жылдан соң болашақтағы киберсоғыс қаупіне дайындық үшін ұлттық деңгейдегі біршама жаңалықтар ұсынды. Жаңалықтар тек қана нақты технологияны әзірлеуге ғана емес, сонымен қоса ұлттық қауіпсіздік құрылымдарымен өнеркәсіптік және академиялық ортамен ынтымақтастықты қосатын, мектепте білім беру жүйесі аясында білім бағдарламаларына қажетті инфрақұрылымдарды құру, біліктілікті жоғарылатудың академиялық орталықтарын, маңызды ұлттық жүйелерді және басқа да жобаларды құруға қатысы болды.

- Нәтижесінде 2011 жылы көрсетілген жаңалықтарды бақылауды, жоспарлауды және жүзеге асыруды қамтамасыз ету үшін Израильдік киберқауіпсіздіктің ұлттық бюросы құрылды. Бұл мәселе әлемдік масштабта өзектенуіне қарай, Израильде жинақталған тәжірибе мен үкіметтің тиісті стратегиясы жекелеген жеке компанияларды ел экономикасының мықты секторына айналдырды. Бүгінде Израильдегі киберқауіпсіздік аясындағы инфрақұрылым шамамен алғанда жүздеген компанияның басын қосады, оның ішінде Check Point сияқты аяғына нық тұрған фирмалар, тура осы салаға инвестиция құятын Jerusalem Venture Partners (JVP) Cyber Labs сияқты стартаптар,венчурлік қорлар, сонымен қатар жоғары технологиялық компаниялар мен академиялық орта арасында ынтымақтастықты жүзеге асыратын ғылыми-зерттеу жобаларыкіреді. Басқа сөзбен айтқанда, израильдік компаниялардың санының өсуі мен дамуына қарай жаңа тенденция байқалады. Израиль стартаптарды жеткізушіден біртіндеп жоғары технологиялардың халықаралық орталығына, және бірінші кезекте киберқауіпсіздік саласындағы әлемдік жетекші көшбасшыға айалуда.

- Сонымен қоса, әлемдік аренада қандай да болмасын мемлекетте ақпараттық қауіпсіздік саясаты киберқауіпсіздік Стратегиясын қабылдау арқылы жүзеге асырылады. Осылайша, алғашқы киберқауіпсіздік Стратегиясы 2003 жылы АҚШ-та пайда болды. Осыдан соң виртуалдық кеңістіктегі қауіпсіздік бойынша ұқсас Стратегиялар мен шаралар жоспары барлық Еуропаға тарады. Еуроодақ (ЕО) елдерінің және оның құрамына кірмейтін кейбір елдердің киберқауіпсіздіктің ұлттық Стратегиясы желілер қауіпсіздігі мен ақпараттық қауіпсіздік бойынша Еуропалық агенттікпен (The European Network and Information Security Agency - ENISA) жарияланды.[3]

- Олардың кейбіреулеріне нақтырақ тоқтала кетейік. Германияда киберкеңістіктегі қауіпсіздік Стратегиясы 2011 жылы қабылданды, бұл ретте Германия Стратегиясының басты назары кибершабуылдардың алдын алу мен қылмыстық қудалауға, кездейсоқ фактормен туындауы мүмкін IT-жабдықтардың істен шығуының алдын алуға бағытталды. Бұған қоса, Германия Стратегиясында мемлекет сертификаттаған негізгі қауіпсіздік функциялары арқылы IT-жүйелерді қорғау бойынша қажетті қосымша әрекеттерге, сонымен қоса жаңа жұмыс топтарын құру арқылы шағын және орта бизнесті қолдауға талдау жасалады. Бұдан басқа, 2015 жылғы 11 шілдеде Германия Парламенті киберқауіпсіздік туралы заң қабылдады, соған сәйкес, 2000-нан астам қызмет көрсетуді жеткізушілер екі жылдың ішінде киберкеңістіктегі қауіпсіздіктің жаңа стандарттарын енгізуге мәжбүр болады, бұлай етпеген жағдайда неміс компанияларына 100 мың еуро көлемінде айыппұл төлеу қаупі төніп тұр. Заң, көлік, денсаулық сақтау, коммуналдық қызметтерді сумен қамтамасыз ету, телекоммуникациялық қызмет көрсетулердің провайдерлері сияқты «маңызды инфрақұрылым» ретінде саналатын институттарға, сонымен қатар қаржылық және сақтандыру компанияларына өз әсерін тигізеді. Бұл ретте, жаңа заң компанияларды кез-келген кибершабуылдар туралы Германияның ақпараттық қауіпсіздік бойынша федералдық басқармасына (BSI) хабарлауды міндеттейді.

- Еуроодақ елдерінің ішінен тағы бір мысал ретінде Эстонияны келтіруге болады, оның киберқауіпсіздік Стратегиясы 2014-2017 жылдарға арналып қабылданды және 2008-2013 жылдарға арналған киберқауіпсіздік Стратегиясында табылған көптеген мақсаттарды жүзеге асырушы киберқауіпсіздікті жоспарлаудағы негізгі құжат болып табылады. Киберқауіпсіздік бойынша стратегияның төртжылдық мақсаты – киберқауіпсіздікті қамтамасыз ету бойынша потенциалды ұлғайту және халықтың киберқауіп туралы хабарын жоғарылату, осылайша киберкеңістіктегі сенімділікті қамтамасыз ету, оның ішінде тіршілікті қамтамасыз ету қызметтерінің негізінде жатқан ақпараттық жүйелердің қорғанысын қамтамасыз ету, мемлекеттік және жекеше сектор үшін киберқауіпті еңсеру, киберқауіпсіздік саласында ұлттық бақылау жүйесін енгізу, мемлекеттің цифрлық ресурстарының тұтастығын қамтамасыз ету, аса маңызды ақпарат инфрақұрылымын қорғау саласындахалықаралық ынтымақтастықты ілгерілету, киберқылмыспен күресті жетілдіру, кибертәуекелдер туралы қоғамның хабардар болуын жоғарылату, киберқауіпсіздікті қамтамасыз ету үшін заңнамалық базаны әзірлеу және басқалары.

- Бұдан басқа, 2008 жылғы 4 мамырда Брюссельде НАТО Кеңесінің отырысында Таллинде НАТО кибернетикалық қорғаныс орталығын құру бойынша өзара түсіністік туралы Меморандумға қол қойылды, кейіннен «Киберқорғаныс мәселелері бойынша НАТО ынтымақтастығының алдыңғы қатарлы орталығы» деген атауға ие болды (NATO cooperativecyberdefencecentreofexcellence). Көрсетілген орталықты құрудың мақсаты киберкеңістіктегі қауіпсіздікті қамтамасыз ету бойынша, оның ішінде ақпаратты қорғаудың жаңа тәсілдерін зерттеу мен әзірлеу, оның ішінде мүше елдердің ақпараттық жүйесіне зиянды әсерлерді анықтау, тигізілген зиянды бағалау, олардың жұмыс қабылетін қалпына келтіру, сонымен қатар кибершабуылдардың дер кезінде алдын алу бойынша шаралар қабылдау, киберқауіпсіздік саласында НАТО қызметін заңды түрде сүйемелдеу, ақпараттық қауіпсіздік саласындағы тәжірибені зерделеу, жинақтау және тарату, оқу-әдістемелік жұмыстар, мүше елдердің ақпараттық қауіпсіздігін қорғау мен қамтамасыз ету саласында мамандарды даярлау бойынша Альянстың мүмкіндіктерін кеңейту

- Киберкеңістіктегі қауіпсіздікті қамтамасыз ету стратегиясы мен тұжырымдамасын дамыту негізгі бағыты болып табылатын киберсаладағы зерттеулер өткізуге, сонымен қатарНАТО аясындағы сияқты және де жекелеген мүше елдерде кибероперациялар (шабуылдық, қорғаныстық, пайдаланушылық) өткізуге, сонымен қоса, Альянс пен мүше елдердің цифрлық есептеуіш жүйелерінің қауіпсіздігін қамтамасыз етудің техникалық шешімдерін әзірлеуге, кибершабуылдардың салдарын анықтау мен жоюға, сырттан басып кіруді анықтау тәсілдерін әзірлеуге орталық ерекше мән береді. Кибероралықтың бастапқы құрамына Эстония, Германия, Италия, Латвия, Литва, Словакия менИспания өкілдері кірді. 2010 жылы оларға Вегрияның, ал 2011 жылы АҚШ пен Польшаның мамандары қосылды. Орталыққа мүше болу барлық мүше елдер үшін ашық, олар қаржыландыру мен мемлекет-қатысушының персонал бөлуі мәселесін айқындайтын өзара түсіністік туралы Меморандумға қол қойған соң құрылымның мүшелері бола алатындығын айта кеткен жөн. Орталық НАТО блогына енбейтін елдермен де, зерттеу институттарымен және қатысушы-демеуші ретінде өнеркәсіптермен қызметтес бола алады. Бұл жағдайда мүшелік Басқарушы комитетпен құпталуы керек. Қатысушы-демеушілер орталықтың белгілі бір жобаларына ғана қатыса алады. Әр нақты жағдай бойынша шешім жеке негізде қабылданады және Басқарушы комитетпен бекітіледі. Қатысушы-демеуші Басқарушы комитеттің құрамына кірмейді, сондықтан бюджетпен немесе Орталықтың жұмыс бағдарламасымен байланысты мәселелер бойынша шешім қабылдау кезінде дауыс беру құқығына ие емес

- Соған қоса, аз уақыттан бері еуроодақ ел-қатысушыларымен және Еуропарламент депутаттарымен киберқауіпсіздік туралы Еуроодақтағы алғашқы заң бекітілді, ол «Желілік және ақпараттық қауіпсіздік бойынша директива» деп аталады. Желілік және ақпараттық қауіпсіздік бойынша директива (Директива NIS) 2016 жылғы 6 шілдеде қабылданды, бұл ретте ұлттық заңнамаларды бейімдеу үшін еуроодақтың мемлекет-мүшелері үшін өтпелі кезең көздестірілген. NIS Директивасы мемлекет-қатысушылар арасында ақпарат алмасу және стратегиялық ынтымақтастыққа көмектесу мен қолдау көрсету мақсатында, ынтымақтастық тобын құру жолымен барлық мемлекет-қатысушылары арасында ынтымақтастықты қамтамасыз ете отырып, Еуроодақта киберқауіпсіздіктің жалпы деңгейін көтеру үшін құқықтық шараларды, сонымен қатар экономика мен қоғам үшін өмірлік маңызы бар энергетика, көлік, сумен қамтамасыз ету, банк ісі, қаржылық нарық, денсаулық сақтау инфрақұрылымдары, және цифрлық инфрақұрылымды қарастырады. Осылайша, бүгінгі күні әлемдік тәжірибе көрсеткендей, киберқауіпсіздік мәселелері жаһандық сипатқа ие, бұл өз кезегінде тек ұлттық қана емес, сонымен қоса тиісінше қауіпсіздіктің әлемдік стандартын да әзірлеу қажеттігін көрсетеді. [6] Әлбетте, қазіргі заманда, мемлекет өмірінде, оның экономикасы мен қауіпсіздік жүйесінде киберкеңістік пен заманауи ақпараттық технологиялар үлкен рөл атқаратындықтан, жоғары технологияларды қолданумен байланысты қауіпті айналып өтуге болмайды. Бұл жерде Қазақстан Республикасы да шет қалмады, Қазақстандағы ақпараттық-коммуникациялық технологиялардың дамуының жоғарғы қарқыны сәйкес инфрақұрылымдардың қорғаныс мәселесін өзектендіреді, себебі олардың ақаулары немесе бұзылуы ел қауіпсіздігі үшін маңызды салдарға ие болуы мүмкін. Осылайша, «Касперский зертханасының» мәліметтері бойынша пайдаланушылары ең жиі веб-шабуылдарға ұшырайтын елдер тізімінде Қазақстан 6-шы орында және пайдаланушыларының саны жағынан мобильдік құрылғыларға арналған троян-бопсалаушылармен шабуылданғандар ішінде 9-шы орында тұр. [7]

- Сонымен қатар, Қазақстан Республикасының заңнамасына жасалған талдау бүгінгі күні заңнамада киберқылмыс, киберкеңістік, киберқауіпсіздік, киберқорғаныс сияқты маңызды ұғымдар анықталмағандығы жөнінде қорытынды шығаруға мүмкіндік береді. Сонымен қоса, ақпараттық қауіпсіздік терминін қолдану байқалады. Қазақстан Республикасының 2015 жылғы 24 қарашадағы «Ақпараттандыру туралы» Заңының (бұдан әрі – Заң) 1- бабымен келесі терминдер және олардың анықтамалары көзделген: Ақпараттандыру саласындағы ақпараттық қауіпсіздік – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі; Ақпараттық қауіпсіздік оқиғасы – ақпараттандыру объектілерінің қазіргі бар қауіпсіздік саясатын ықтимал бұзу туралы не ақпараттандыру объектілерінің қауіпсіздігіне қатысы болуы мүмкін, бұрын белгісіз болған жағдай туралы куәландыратын жай-күйі; Ақпараттық қауіпсіздіктің оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жекелей немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қатер төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшірмесін түсіріп алу, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын іркілістер. Заңның 14-бабына сәйкес, ақпараттық жүйелердің және мемлекеттік органдардың телекоммуникациялар желілерінің орнықты жұмыс істеуін қамтамасыз ету үшін ақпараттық қауіпсіздікке төнетін қатерлерді анықтау, талдау және болғызбау бөлігінде ақпаратты қорғау құралдарын әзірлеу бойынша жұмысты мемлекеттік техникалық қызмет жүзеге асырады. Бұдан басқа, мемлекеттік техникалық қызмет жыл сайынғы негізде меншік иелерінің өтініші бойынша ақпараттық жүйеге, «электрондық үкіметтің» ақпараттық-коммуникациялық платформасына және мемлекеттік органның интернет-ресурсына олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізеді, аттестаттау объектілерінің қорғалу жай-күйін, сонымен қатар олардың ақпараттық қауіпсіздік талаптарына сәйкестігін анықтау бойынша іс-шараларды жүргізеді

- Бұл ретте, Заңның 51-бабына сәйкес, міндетті түрде аттестатталуға жататын аттестаттау объектілеріне мыналар жатады: 1) мемлекеттік органның ақпараттық жүйесі; 2) мемлекеттік органның ақпараттық жүйесі мен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйе; 3) ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйе; 4) «электрондық үкіметтің» ақпараттық-коммуникациялық платформасы; 5) мемлекеттік органның интернет-ресурсы

- Осылайша, жоғарыда келтірілген шет елдердегі сияқты, олардың бұзылуы немесе қызметін тоқтатуы әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайларға немесе қорғаныс, қауіпсіздік, халықаралық қатынастар, экономика, шаруашылықтың жекелеген салалары, Қазақстан Республикасының инфрақұрылымы немесе тиісті аумақта тұратын халықтың тіршілік әрекеті үшін елеулі теріс әсерге әкеп соғатын ақпараттық-коммуникациялық инфрақұрылымның маңызды объектілерін, соның ішінде «электрондық үкіметтің» ақпараттық-коммуникациялық инфрақұрылымын қорғау Қазақстан Республикасы заңнамасының да негізгі бағдарлауышы мен басымдылығы болып табылады. Дегенмен, киберқауіпсіздік мәселелері Қазақстан Республикасының ұлттық заңнамасында ұрықтану деңгейінде, пайдаланушылары ең жиі веб-шабуылдарға ұшырайтын елдер тізімінде Қазақстан Республикасы 6-шы орында және пайдаланушыларының саны жағынан мобильдік құрылғыларға арналған троян-бопсалаушылармен шабуылданғандар ішінде 9-шы орында тұруы жоғарыда келтірілген статистикамен куәлендіріледі. Осыған байланысты, Еуроодақ мемлекет-мүшелерінің аналогиясы мен тәжірибесі бойынша, әлемдік тәжірибені ескере отырып,ақпараттық қауіпсіздікті қамтамасыз етуге қолданылып жүрген барлық тәсілдерді және ұлттық стратегияны әзірлеудіқайтадан қарауға қажеттілік туындайды. Шетелдік тәжірибе көрсеткендей, белгілі бір уақыт аралығында қол жеткізілуі тиіс ұлттық мүдделер мен басымдықтардың түрлі саласын көрсететін киберқауіпсіздік бойынша ұлттық стратегия ұлттық ақпараттық инфрақұрылым мен қызмет көрсетулердің қауіпсіздік деңгейін жақсарту мен арттыруға арналған құрал болып табылады. Бұдан басқа, ақпараттық қауіпсіздік саласындағы ұлттық стандарттар мен әдістерді әзірлеу, халықаралық стандарттар мен техникалық регламенттермен үйлестіруді қоса алғанда – ақпаратты қорғау саласында Қазақстан Республикасы үшін басым және өзекті мәселелердің бірі

- Сонымен қоса, бүгінгі күні, ақпараттандыру мен байланыс аясында ақпараттық қауіпсіздік (киберқауіпсіздік) саласындағы мемлекеттік саясатты жүзеге асыру мақсатында, 2016 жылғы 6 қазанда Қазақстан Республикасы Президентінің Жарлығымен Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрлігі құрылды. Осы Жарлықпен Қазақстан Республикасы Үкіметіне Ақпараттық қауіпсіздік комитетін құруды қамтамасыз ету тапсырылды, ол ұлттық ақпараттық қауіпсіздік саласындағы мемлекеттік саясатты әзірлеу бойынша өкілетті органның (реттеушінің) қызметін атқаратын болады, бұл, әрине, елдің киберқауіпсіздігін қамтамасыз ету мәселелерінде маңызды қадам болып табылатыны сөзсіз