УКУКТУК МАСЕЛЕЛЕР ЖАНА ЭЛ АРАЛЫК БАЙЛАНЫШТАР БОЮНЧА КОМИССИЯ

V ЖЫЙЫН АНКАРА

2016 ЖЫЛЫ 17 МАЙ

«МҮЧӨ ӨЛКӨЛӨРДҮН АРАСЫНДА КИБЕР КЫЛМЫШТУУЛУК МЕНЕН КҮРӨШҮҮ, УКУКТУК БАЗАНЫ ЖАНА КЫЗМАТТАШТЫКТЫ ӨНҮКТҮРҮҮ»

ОТЧЕТ

КИРИШҮҮ

Ақпараттық технологиялардың жаһандық деңгейге көтерілуіне орай осы саладағы қауіпсіздік бүткіл дүние жүзі қауымдастығы үшін, әрбір ел мен жеке адам үшін күрделі мәселеге айналып отыр. Компьютер желілерінің бір-біріне кірігіп, жаһандануы және де сандық (цифрлы) ортаның ұлғаюы көптеген жаңа өзгерістерден хабардар болуды талап етеді. Технологияның дамуы көптеген жаңа мүмкіндіктерге жол ашады, ал қылмыс туралы түсініктің өзі кеңейіп, информация саласына да жайылады. Информациялық технологиялардан қай салада болмасын дерлік тәуелділік жыл сайын өсе түсіп отыр, осымен қатар киберкеңістік пен киберқылмысқа қатысты проблемалар жаөһандық бола түсуде.

Осының нәтижесінде киберқауіпсіздік тәуекелдері экономика мен ұлттық қауіпсіздікке аса ірі сын-тегеуріндер төндіруде. Осығай сай киберқылмыс концепциясы елдердің күн тәртібіндегі маңызды тақырып болуда.

Технологиялық жетілудің әсерлері мен салдарын ескере отырып, Құқықтық мәселелер және халықаралық қатынастар комиссиясы өзінің 2015 жылы 29 сәуірде Бішкекте өткен төртінші жиналысында киберқылмыспен күрес және соған қатысты заңнамалық негіз мәселелерін, осы саладағы заңнама мен оған парламенттің қосатын үлесі проблематикасын қарастыруды ұйғарды.

Осы себепті Комиссияның Анкара қаласында 2016 жылдың мамыр айында өтетін бесінші жиналысы тақырыбы төңірегінде сөз қозғап, 2016 жылдың қыркүйек айында Қырғызстанда өтетін Ассамблеяның жетінші пленарлық отырысында бекітілу үшін ұсынылатын баяндама мен ұсыныстарды талқылайтын болады.

КИБЕРҚЫЛМЫСПЕН КҮРЕС ЖӘНЕ ТҮРКПА-ҒА МҮШЕ ЕЛДЕРДЕГІ АРНАЙЫ ЗАҢНАМА

1) Жаңа информациялық технологиялар кеңістік пен уақытты кішірейтеді дағы лезде әлем көлеміндегі мәліметтерге қол жеткізіп, тез арада хат-хабар алуға мүмкіндік жаратады. Оның үстіне қазіргі заманда киберкеңістік іс жүзінде кез-келген нәрсені және кімді болсын қамтиды. Бұл өзара байланыстылықтың ауқымы бір жерде бар проблемалар екінші бір жердегі компьютерлерге әсер ететін жағдай туғызады, сөйтіп киберқауіпсіздік пен технологиялық дамудың динамизмімен байланысты киберқылмысқа қатысты алаңдауларды туғызады.

2) Тіршіліктің қай саласында болсын электронды информация ағыны желілері орнығуда. Жаһандық деңгейде өзара байланысқан цифрлы информация мен коммуникация инфраструктурасы қазіргі заманғы тіршіліктің әр саласын демейді және де экономикаға, азаматтық инфраструктураға, қоғам қауіпсіздігіне және ұлттық қауіпсіздікке қолдау көрсетеді.

3) Сонымен қатар, компьютерлерді қолдану мен электронды байланыс өзімен бірге өте күрделі киберқауіпсіздік сындарын алып келді. Әркелкі әрі атүсті реттелген цифрлы инфраструктура көптеген адамдарға қызмет ұсынады дағы кейбір

осалдықтар тәуекелдерін ұлғайтады. Кибер шабуылдар кейбір осалдықтарды ірі ауыртпалықтарға ұшырататын алапат күшке айналуы мүмкін.

4) Экономикалар мен ұлттық қауіпсіздіктің информациялық технологиялар мен оның инфраструктурасына тәуелділігі арта түсуде. Көптеген желілерден тұратын құрылым экономиканың барлық секторларындағы операцияларды демейді, атап айтқанда, энергетика (электр қуаты, мұнай және газ), транспорт (темір жол, әуе және теңіз байланыстары), қаржы және банк жүйесі, информация және телекоммуникациялар, денсаулық сақтау, төтенше жағдайлар қызметі, су, химикаттар, қорғаныс саласы, өнеркәсіп, азық-түлік, ауыл шаруашылығы және пошта қызметі. Бұл құрылым, сондай-ақ, электр трансформаторларын, құбыр насостарын, химикаттар контейнерлерін, радарларды және тағы басқаларды қадағалайды.

5) Барлық ұйымдар мен институттар, әсіресе, мемлекеттік органдар интернет арқылы өзінің қызметін ұсына бастағандықтан, интернетте болуы ықтимал теріс жағдайлар жеке адамдардың, қоғам және экономика өміріне үлкен ықпал ететін қауқарға ие болды. Осындай теріс оқиғалар бола қалған жағдайда олар материалдық және моральдық зиян шектіруі мүмкін. Осы ретте информациялық желілерге жасалған кибер шабуылдар аса қажетті салалардың жұмысын ақсатуы мүмкін. Қазіргі кездегі ауқымы өсе түсіп отырған тәуекелдердің ішінде кибер қылмыс бой көрсете бастады.

6) Осы қылмыспен күресті көздеген бастамалар мен осы іспен айналысып жүрген халықаралық ұйымдар мен институттардың, сондай-ақ, үкіметтік емес ұйымдардың жұмысы киберқылмыс қаупі ауқымының орасан зор екендігін және онымен күрес аянбай бірлесе күш салуды қажет екенін айқындап берді. Осы салада айтарлықтай табысқа қол жеткенімен, алда тындырылатын көп шаруаның күтіп тұрғанын айтқан жөн.

7) Жүргізілген зерттеу жұмыстарында киберқылмыс информациялық технологиялардың дамуын пайдаланған және информациялық технологияларды қолдану арқылы істелген қылмыстарды білдіретін негізгі концепция ретінде танылады. Мұндай қылмыстардың ауқымы үлкен, мысалы, олар информациялық технологиялар мен олардың өнімдерін көздейді (*заңсыз компьютерлік қорғанысты бұзып ену, деректерді, информациялық технологияларды бұзу, т.с.с.*), информациялық технологияларды пайдалану арқылы қауіп төндіреді (*қолдан жасау, жеке куәліктер, кредит кардтар, т.с.с*.) не интернет мазмұнын ластайды (*балалар порнографиясын, нәсілшілдік материалдарды, т.б. теріс мазмұнды ақпаратты енгізу*).

8) Аса күрделі киберқылмыспен күресте жаңа, тың тәсілдерді ойлап тапқан жөн. Киберқылмыс және терроризммен тек цифрлы майданда ғана емес, жеке адамдар мен қоғам деңгейінде және саяси майдандарда күресу керек.

9) Киберқауіпсіздік және киберқылмысты ауыздықтауды көздейтін стратегиялар киберқылмыстың алдын алу, халықаралық ынтымақтастық, қылмысқа шұғыл жауап қату, компьютер желілеріндегі ақша аударымына санкциялар енгізу және ақпараттық қауіпсіздік сияқты шараларды қамтиды және де аталғандардың барлығы дүниежүзілік ақпарат және коммуникация инфрақұрылымының қауіпсіздігімен және тұрақтылығымен өзара қабысқан.

10) Кибер ортаның осал тұстарын жетілдіру және информациялық технологиялар революциясының толық потенциалын әлем қауымдастығына таныту үкіметтердің негізгі жауапкершілігі. Үкіметтер бір жағынан өздерінің экономикалық қажеттіліктері мен ұлттық қауіпсіздікке қатысты талаптар бойынша жұмыс атқаруы қажет, екіншіден, киберқылмыспен күресу тәсілдерін зерттеуге қомақты қаражат бөлулері қажет. Бұл істе қоғамның хабардарлығын арттырып, киберортаның қауіпсіздігіне комплексті түрде қараған жөн.

11) Басқа елдер сияқты ТүркПА-ға мүше елдер де кибер қауіпсіздікті қамдап, киберқылмыстармен күресу үшін тиісті жұмыстар атқарады. Бұл жерде мүше елдер бір жағынан сақтықты, қауіпсіздікті және құпиялық хақын қамтамасыз ету, екінші жағынан инновация мен технологиялық дамуға дем беретін ортаны қорғау мәселелерінің өзара қайшылығына тап болуда.

12) Европа комиссиясының «Киберқылмыс жөніндегі конвенциясына» (European Commission's "Convention on Cybercrime") қол қойған Түркия елдің Көлік, теңіз қатынасы және коммуникация министрлігінің күш салуымен «Ұлттық киберқауіпсіздікті жүзеге асыру, басқару және үйлестіру туралы қарардың» жобасын әзірледі. Ұлттық киберқауіпсіздік жаттығулары жыл сайын Информациялық технологиялар мен коммуникациялар институтының, Көлік, теңіз қатынасы және коммуникация министрлігінің және Түркияның ғылыми-техникалық зерттеу институтының (TÜBİTAK) қатысуымен өтеді. 2012 жылғы шілде айында TÜBİTAK-BİLGEM (Түркияның ғылыми-техникалық зерттеу институты мен Информатика және информациялық қауіпсіздікті зерттеу орталығы) аясында Киберқауіпсіздік институты құрылды.

13) Түркияда киберқауіпсіздікке қатысты мәселелерді реттейтін заңнамаға келесі құжаттар кіреді: №5237 «Түркия қылмыс кодексі», №5651 «Интернет арқылы жариялау мен хабар тарату және осыған қатысты қылмыстармен күресу туралы» заң және №5070 «Электронды қол қою» туралы заң.

14) Әзербайжан Республикасы Европа Кеңесінің «Киберқылмыс жөніндегі конвенциясын» (European Council's "*Convention on Cyber Crime"(Budapest Convention))* 2009 жылдың 30 қыркүйегінде ратификациялап, оған ел Президенті қол қойғаннан кейін күшіне енді. Бұған қоса Әзербайжан Европа комиссиясының 1981 жылғы «Жеке тұлғаға қатысты мәліметті автоматты өңдеуге қатысты жеке тұлғаларды қорғау туралы конвенциясына» қосылып, №209 заң қабылдады. Сонымен бірге «Электронды қол қою» мен «Үкімет қауіпсіздігі» туралы заңдар осы саладағы маңызды негізгі заңнамалық құжаттар қатарынан табылады.

15) Әзербайжанның қылмыс кодексінде киберқылмысқа қатысты бірқатар ережелер бар (30 тармақ, 271, 272, 273 баптар). Кодексте бөтен компьютерге заңсыз ену, теріс мазмұндағы материалдар мен компьютерлік программалардың жариялануын қамтитын баптар бар. Аталған кодекс интернет ортада тіл тигізетін, зиян келтіретін және жала жабатын материалдардың жариялануына қатысты жазалау шараларын қамтиды (147 мен 148 баптар). Бұған қоса, Әкімшілік тәртіп бұзушылықтар туралы заңның 16-тармағы және басқа да баптар ақпаратты қолдану, тарату және қорғау мәселелерін қамтиды.

16) Қазақстан Республикасының Президенті қол қойып, 2015 жылдың 1 қаңтарынан бастап күшіне енген елдің Қылмыстық кодексінде киберқылмыстар бойынша жауапкершілік көзделген бөлек тарау бар. Бұған компьютердегі деректерге заңсыз қол жеткізу, оларды иеленіп алу, жою немесе түрлендіру, қоғамға зиян келтіретін бағдарламалар мен ақпаратты тарату кіреді. Сондай-ақ, Қылмыстық кодексте жала жабу мен қорлау мәліметтерді тарату бойынша баптар көзделген. Сонымен қатар, киберқылмыспен күрестегі ынтымақтастық Тәуелсіз Мемлекеттер Достастығы (ТМД) аясында және басқа да халықаралық деңгейде қол қойған құжаттар шеңберінде жалғасуда.

17) Қырғыз Республикасының Қылмыс кодексінде (28 тармақ) «Информациялық технологиялардағы қылмысқа» қатысты үш бап бар. Сондай-ақ, Қырғыз Республикасының Әкімшілік жауапкершілік туралы заңының 21-тармағы «Телекоммуникация желісі мен байланысындағы заң бұзушылықтарға» тоқталады.

18) Кибер проблемалармен айналысу үшін тек қана ұлттық заңдарды қабылдап, оларды орындау жеткілікті емес. Жан-жақты електен өткен заңдар мен ережелер киберқылмыспен күресу үшін қабылдануы керек және оларды қажет кезінде өзгертіп отыру керек. Себебі, информация және коммуникация желілері ұлттық және халықаралық деңгейлерде жекеменшіктің қолында әрі желілер жұмысын солар жүргізеді. Осыған байланысты үкіметтік-жеке әріптестік және халықаралық әрекеттестік пен нормалар киберқауіпсіздік проблемаларымен айналысу үшін қажет арнайы стратегияны түзгенде маңызды элементтер ретінде қолданылатын болады.

19) Парламенттер кибер ортаға және киберқылмыспен күресуге қатысты белсенді әрекет етіп, орнықты дамудың басты шарттарының бірі болып табылатын кибер қауіпсіздіктің нығаюына үлес қосулары қажет.

20) Парламенттер қазіргі заңнамалық механизмдерді жоғарғы деңгейде пайдалана отырып, кибер қауіпсіздік және киберқылмыс жөнінде ұлттық деңгейде кең көлемде мәлімет тарату арқылы, ең алдымен, кибершабуылдан болатын зияндарды азайтуға және жеңілдетуге, содан кейін, технологиялық дамудың пайдалы жақтары жөнінде түрлі орталарға ақпарат таратуға талпынулары қажет.

21) Кибершабуылдар және килігулермен күрестегі басқа да әріптес институттар мен құрылымдарға қолдау көрсету үшін қауіпсіздік агенттіктері мен сот биілігі арасындағы өзара әрекеттестік пен үйлестіруді дамытуға ерекше көңіл бөлінуі керек.

22) Мүше елдердің парламенттері киберқауіп пен киберқылмысқа қарсы комплексті түрде бағытталған халықаралық стратегияның жасалуы ісінде алдыңғы орындарда болып, осы мәселеге қатысты ұлттық қылмыс кодекстерін гармонизациялау үшін ортақ халықаралық заңнамалық механизм ойластыруы қажет.

23) Киберқауіпсіздік туралы заңдардың халықаралық стандарттар аясында гармонизацияланғаны маңызды. Сонымен қатар, олардың ғылыми және технологиялық жетістіктерге сүйенген орнықты дамуға қатысты халықаралық келісімдерді мақұлдағанда белсенді рөл атқарғаны да маңызды..

Халықаралық белсенділіктер

Ғаламдық киберақпарат және желілердегі қауіпсіздік мәселелерімен, сондай-ақ, осыларға қатысты қылмыстармен халықаралық сахнада бүткіл тараптарды қамтитын халықаралық ынтымақтастық стратегиясын қабылдап, орындағанда және киберқауіпсіздігі мәдениетін дамытқанда ғана оңды айналысуға болады. Көптеген елдерге теріс әсер етіп отырған киберқылмыстармен күресте халықаралық диалог пен әрекеттестіктің қажет екені баршаға мәлім.

24) Халықаралық киберқауіпсіздікті нығайту бойынша құралдардың бірі болып Европа Кеңесі пысықтап, 2001 жылдың 23 қарашасында Будапештте қол қойылған, 2004 жылдың 1 шілдесінен бастап күшіне енген «Киберқылмыс бойынша конвенция» табылады. Конвенция ұлттық заңнамалық негіздерді қалай үйлестіруге болатыны және киберқылмыспен күресте халықаралық әрекеттестіктің элементтері қандай болуы керектігі хақында жол сілтейді. Бұл заңнамалық құжат практикалық та, саяси тұрғыданда маңызды. Конвенция Европа нормаларына қатысты маңызды құрал, себебі ол киберқылмысқа қарсы ұлттық заңнамалық қаңқа қалыптастыруға қатысты жол сілтейді. Бұған қоса, Конвенцияға қосылу практикалық істерде, оның ішінде киберқылмыскерлерді қайтарып беру бар, халықаралық әрекеттесуге сеп болады. Европа Кеңесі жеке сектор және мүше елдермен бірлесе отырып Конвенцияны дүние жүзінде ілгерілету үшін Киберқылмыс бойынша жаһандық жоба атты шараны қолға алды. Конвенцияға қосылып жатқан елдер санының ұлғаюы қылмысты топтар мен кибершабуылдарға өз аумағындағы сыбайластары арқылы дем беретін үкіметтердің айылын жиғызуда.

25) Экономикалық ынтымақтастық және даму ұйымының (ОЭСР - OECD) Информацияның қауіпсіздігі мен оңашалығы атты үкіметаралық жұмыс тобы (OECD inter-governmental Working Party on Information Security and Privacy (WPISP)) ақпараттық қоғам және қауіптерді тойтаруға қатысты ұсыныстар мен баяндамалар әзірлейді. Үкіметтер мемлекет жүйесіндегі, бизнестегі және азаматтық қоғамдағы эксперттер желілері арқылы ағымдағы тенденцияларды бақылап, тиісті ақпарат алмасуды қамдайды. OECD болса технологияның ақпараттық қауіпсіздік пен оңашалыққа әсері жөнінде тұрақты баяндамалар жасап тұрады.

26) Европадағы қауіпсіздік және ынтымақтастық ұйымы (ЕҚЫҰ-ОБСЕ) 2008 жылы киберқауіпсіздік туралы талқылауларды бастады. Содан бері ОБСЕ-ге қатысушы

елдер киберқауіпсіздікке қатысты бірнеше жоғары деңгейдегі кездесулер өткізіп, онда киберқауіпсіздікке қатысты хабардарлықты арттыру, киберқылмыс және терроризммен күресу үшін елдердің мүмкіндігін арттыру және киберкеңістіктегі мемлекеттердің жауапкершілігін анықтау сияқты басты тақырыптар төңірегінде әңгіме болды. Пікіралмасулар осы мәселедегі ОБСЕ-нің рөлі қандай болмақ деген сауалға әлі ортақ жауап берген жоқ, себебі елдердің киберқауіпсіздікке қатысты позициялары әртүрлі болып қалып отыр.

27) БҰҰ Бас ассамблеясы киберқауіпсіздікке қатысты қарарлар қабылдады. БҰҰ Әлеуметтік және экономикалық комитеті аясында №56/121 «Информациялық технологияларды қылмыс үшін қолданумен күрес» және №57/239 «Киберқауіпсіздіктің жаһандық мәдениетін қалыптастыру» атты қарарлар қабылданды. Екі қарар да халықаралық ынтымақтастықтың маңыздылығын, киберқылмыскерлер тығылатын баспаналарды жоюдың қажеттілігін, заңды күшіне енгізу практикалары бойынша әрекеттестікті ілгерілетудің, сондай-ақ, киберқауіпсіздік мәселелеріне қатысты хабардарлықты арттырудың маңыздылығын баса айтады. №64/422 «Глобализация және өзара тәуелділік: ғылым мен технология даму үшін» атты қарар БҰҰ-ға мүше елдердегі киберсақтық мәселелеріне қатысты өздерін-өздері бағалау міндетін қамтиды. Аталған бастамалар киберқауіпсіздікке көптеп көңіл бөлуге, бұл мәселе жайлы жаһандық деңгейде білім мен мәлімет қордалауға сеп болды, сондай-ақ, киберқауіпсіздікке қатысты елдердің өз ұлттық стратегияларын жасауына және тиісті шаралар қолдануына түрткі болды.

III. ҚОРЫТЫНДЫЛАР

- ✓ Қазіргі кезде адамдарға, институттарға және ұйымдарға қатысты хабарлар көлемі және түрлілігі жағынан орасан зор ұлғайғаны жақсы мәлім. Информациялық деректердің көпшілігі цифрланған, соның арқасында қоғамдық және кәсіпкерлік жұмыс шапшаңдай түсті. Бұл бұрын-соңды болмаған жаңа қызметтер түрін ұсынуда. Аталған жайттардан басқа киберқауіпсіздік пен киберқылмыстар үлкен мәселеге айналып отыр және оларға қатысты тиісті шаралар тез арада қолға алынуы керек.

- ✓ Киберкеңістікте шекаралардың мән-маңызы мардымсыз. Ғаламдық ауқымдағы киберкеңістіктің осалдықтары баршаға белгілі және де қолында тиісті керек-жарақ бар кез-келген адам бөтен желіге заңсыз ене алады. Үкіметтер кейбір жайттарға жіті көңіл бөлгені жөн; көп жағдайларда кибершабуылшы мен киберқұрбан әртүрлі елдерде орналасады, сондықтан, елдер арасындағы әрекеттестіктің жаңа деңгейге көтерілгені лазым, керек болса, аймақтық және халықаралық ұйымдар аясында осы мәселе кеңінен талқылануы қажет.

- ✓ Бұл жерде үкіметтер бір жағынан сақтықты, қауіпсіздікті және құпиялық хақын қамтамасыз ету, екінші жағынан инновация мен технологиялық дамуға дем беретін ортаны қорғау мәселелерінің өзара қайшылығына тап болуда. Киберқауіпсіздікті қамтамасыз ету үкіметтер, кәсіпкерлер және қоғамдар үшін ұлттық және халықаралық деңгейдегі негізгі проблемаға айналып отыр.

- ✓ Кибержелілерді көздеген шабуылдардың өсе түсуінің нәтижесінде қауіпсіз және шыдамды киберкеңістікті қалыптастыру және киберқауіпсіздікке қатысты информация мен инновацияларды қолдау үшін тиісті заңнаманы жетілдіру шешуші рөл атқарады. Халықаралық заңнамалық нормаларды ұлттық деңгейде ратификациялау - киберқылмысқа қарсы күресті жүйелендірудегі қажетті қадам.

- ✓ Заңнаманы әзірлеу процесіне мемлекеттік-жеке сектордың қатысуының маңызы зор. Мемлекеттік-жеке сектордың қатысуы қоғамның мәселе жөнінде хабардарлығын арттыру, білім беру, технологиялық даму, осал тұстарды жойып, нығайту жұмыстарын жүзеге асырғанда түрлі форматта болуы мүмкін.

- ✓ Заңнама сарапшылары, технология мамандары, социолог не физиолог сияқты түрлі әлеуметтік саланың ғалымдары және басқа да эксперттердің киберқылмыспен күреске бағытталған киберқауіпсіздік заңдарын пысықтағанда қатысуы заңнамалық және технологиялық инфраструктураның гармонизациясы үшін маңызды.

- ✓ Мүше елдеріміз киберқылмыс бойынша көптеген эксперттердің әзірленуіне мұқтаж. Бұл ретте информациялық технология саласымен айналысатын және осы салада мамандар дайындайтын университеттер мен институттар киберқауіпсіздікті қамтамасыз ету процесінің тыңғылықты ілгерілеуіне қомақты үлес қоса алады. Заңнамалық және техникалық ережелер өте қажет әрі нәзік инфраструктураны қорғау үшін, мемлекеттік және жекеменшік секторларға нұқсан келтірмей тез арада әзірленуі тиіс. Осы саладағы ғылыми зерттеулерге қолдау көрсету аса пайдалы болар еді.

- ✓ Киберқауіпсіздік мәдениетінің жаһандық деңгейде кибершабуылдармен күресу үшін ілгерілетілуі, қолдау көруі және бұлтартпай жүзеге асырылуы керек.

- ✓ ТүркПА-ға мүше елдер киберқылмысқа қарсы күреске қатысты заңнаманы жетілдіруге күш салулары керек және ақпараттық желілерді қорғауда өзара әрекеттестікті жолға қою үшін тығыз ынтымақтасуылары қажет.