Қ.А. ЯССАУИ АТЫНДАҒЫ ХАЛЫҚАРАЛЫҚ ҚАЗАҚ-ТҮРІК УНИВЕРСИТЕТІ

Әлеуметтік ғылымдар факультеті

Қолжазба құқығында

Камбарова Динара Жолдасбекқызы

КИБЕРҚЫЛМЫСТЫҢ ҚҰРАМЫН ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚОЛДАНЫСТАҒЫ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫНА СӘЙКЕС ҚАРАСТЫРУДЫҢ ҚҰҚЫҚТЫҚ МӘСЕЛЕЛЕРІ

«7М04222 – Құқық »

«7М04222 – Құқық » білім беру бағдарламасы бойынша заң ғылымдарының магистрі дәрежесін алу үшін магистрлік диссертация

Ғылыми жетекшісі: Битемиров Қайрат Тұрлыбайұлы
заң ғылымдарының кандидаты,
(PhD), қауым. профессор

Магистрлік диссертация қорғауға жіберілді «____»_____2021 ж.

Кафедра меңгерушісі Есеналиев Асхат Ералыұлы
з.ғ.к., доцент

Түркістан, 2021 ж.

Мазмұны

БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

АҚШ – Америка Құрама Штаттары
БАҚ – Бұқаралық ақпарат құралдары
БҰҰ – Біріккен Ұлттар Ұйымы
БАҚ – Бұқаралық ақпарат құралдары
ДЗМҰ – Дүниежүзілік зияткерлік меншік ұйымы
ЕК – Еуропа Кеңесі
ҚК – Қылмыстық кодекс
ҚР – Қазақстан Республикасы
ҒЗЖ – Ғылыми-зерттеу жұмыстары
РМК – Республикалық мемлекеттік кәсіпорны
РФ – Ресей Федерациясы
СІМ – Сыртқы істер Министрлігі
ТМД – Тәуелсіз Мемлекеттер Достастығы
ШЫҰ – Шанхай Ынтымақтастық Ұйымы
ӨТҚҚ – Өңірлік терроризмге қарсы құрылым
ЭЕМ – Электронды есептегіш машина

Кіріспе

Зерттеу тақырыбының өзектілігі. Ақпараттық саланы дамыту тұтастай алғанда қоғамдық және мемлекеттік дамуға әсер ететін негізгі факторлардың бірі болып табылады, бұл мемлекеттік институттардың жұмыс істеу тиімділігіне, мемлекеттердің экономикасы мен қорғаныс қабілетіне тікелей әсер етеді. Сонымен бірге, жаңа ақпараттық жүйелерді, коммуникациялық технологияларды, компьютерлік технологияларды үнемі құру және оларды жетілдіру ақпараттық желілер мен жалпы қоғам үшін жаңа жаһандық қауіптердің пайда болуына қолайлы негіз болып табылады. Қазақстандық БАҚ-тың ақпараттық жүйелерді пайдалана отырып жасалған жаңа кибершабуылдар, қылмыстар туралы күнделікті жаңалықтары ешкімді таңғалдырмайды.

Қазақстанда азаматтардың кибербуллингтен, азаптаудан және адам саудасынан қорғалмауынан адам құқықтарын қорғау жөнінде жаңа шаралар қабылдау қажет. Бұл туралы Парламент палаталарының бірлескен отырысында Мемлекет Басшысы Қасым-Жомарт Тоқаев мәлімдеді. "Адам құқықтарын қорғау бойынша жаңа шаралар қабылдау өте маңызды. Мен үшін бұл мәселе басымдыққа ие. Бүкіл әлем сияқты, Қазақстан да интернеттегі қудалаудан азаматтардың қорғансыздығына тап болды. Азаматтарды қорғау үшін заңнамалық шаралар қабылдайтын кез келді", - деді Президент[1].

Кибертерроризм қылмыстың аса қауіпті түрлерінің бірі ретінде бағаланады, бұл ақпараттық қауіпсіздікті қамтамасыз етуде құқық қорғау органдарының танымдық және технологиялық дағдылары мен құзыретінің жаһандық дамуын қажет етті [2].

2020 жылы Қазақстан кибершабуылдар саны бойынша әлемде 19-шы орынға ие болды. II тоқсанның қорытындысы бойынша республика мобильді троян-қорқытып алушылардың шабуылына ұшыраған елдер арасында әлемде бірінші орын алды. Қазақстан тұрақты түрде осы рейтингтің ТОП-3 қатарына кіреді. 8-ші орында қаржылық зиянды бағдарламалармен шабуылдар бойынша ел. Шифрлаушы трояндардың шабуылдары – 11-ші орын, кеншілердің шабуылдары бойынша-7-ші орын[3].

ҚР Қорғаныс және аэроғарыш өнеркәсібі министрлігі Ақпараттық қауіпсіздік комитетінің мәліметтері бойынша, егер 2016 жылы мемлекеттік органдарға 1 млрд. шабуыл тіркелген болса, 2017 жылдың қорытындысы бойынша олардың саны 20 млрд.

Ағымдағы жылдың қаңтар айында елімізде интернет-алаяқтықпен байланысты 1 700-ден астам қылмыс тіркелді [4].

Қазақстанда 2019 жылы 21 мыңнан астам ақпараттық қауіпсіздік инциденті анықталды [5].

Көрсетілген себеп бойынша бүкіл әлемдегі, оның ішінде Қазақстан Республикасындағы ең өзекті проблемалардың бірі киберқылмысқа қарсы іс-қимыл болып табылады. Қазақстанда киберқылмыспен күрес үшін арнайы қорғау жүйесін құру қажеттілігі туралы Қазақстанның Тұңғыш Президенті Нұрсұлтан Назарбаев 2017 жылғы қаңтардағы өзінің жыл сайынғы халыққа

Жолдауында мәлімдеді. Сол кезде ол үкіметке және ҰҚК-ге "Қазақстанның киберқалқаны" жүйесін құру бойынша шаралар қабылдауды тапсырды» [6]. "Қазақстан киберқалқаны" киберқауіпсіздік бағдарламасын белсенді іске асыру 2018 жылы басталды және 2022 жылға дейін есептелген.

Қазақстанда киберқылмыспен күрес үшін арнайы қорғау жүйесін құру қажеттілігі туралы Қазақстанның Тұңғыш Президенті Нұрсұлтан Назарбаев 2017 жылғы қаңтардағы өзінің жыл сайынғы халыққа Жолдауында мәлімдеді. Сол кезде ол үкіметке және ҰҚК-ге "Қазақстанның киберқалқаны"жүйесін құру бойынша шаралар қабылдауды тапсырды.

Қазақстанда киберқылмыспен күрес үшін арнайы қорғау жүйесін құру қажеттілігі туралы Қазақстанның Тұңғыш Президенті Нұрсұлтан Назарбаев 2017 жылғы қаңтардағы өзінің жыл сайынғы халыққа Жолдауында мәлімдеді. Сол кезде ол үкіметке және ҰҚК-ге "Қазақстанның киберқалқаны"жүйесін құру бойынша шаралар қабылдауды тапсырды [7].

Қазақстан Республикасының Үкіметі экономиканы цифрландыру жөніндегі іс-шараларды тиімді іске асыру ақпараттық-коммуникациялық инфрақұрылымның бірлігін, орнықтылығын және қауіпсіздігін, деректердің сақталуын және азаматтардың ақпараттық-коммуникациялық технологияларды пайдалануға негізделген шешімдерге негізделген процестерге сенімін қамтамасыз ету кезінде ғана қамтамасыз етілетінін атап өтті.

Қазақстан президенті Қасым-Жомарт Тоқаев ШЫҰ-ның ақпараттық қауіпсіздік орталығын құруды ұсынды. Ол Бішкекте өткен ШЫҰ-ға мүше мемлекеттер басшылары кеңесінің кеңейтілген отырысында өңірдегі қауіпсіздікті қамтамасыз ету мәселелерінің өзектілігін атап өтті. "Терроризм мәселесі жаһандық желіде де сезіледі және киберқауіпсіздікті қамтамасыз ету бойынша қосымша шараларды талап етеді. ШЫҰ-ның ақпараттық қауіпсіздік жөніндегі орталығын құру ұйымның ақпараттық кеңістігін қорғау ісіне маңызды үлес қосар еді. Тәжірибе мен ерекшеліктерді ескере отырып, ШЫҰ ӨТҚҚ Кеңесі (Өңірлік терроризмге қарсы құрылым) осы мәселені ілгерілетуде негізгі рөл атқара алады", - деді Қасым-Жомарт Тоқаев [8].

Қылмыстық құқық және криминология ғылымында киберқылмыстың ұғымы, табиғаты, түрлері және оларға қарсы іс-қимыл шаралары туралы пікірталастар белсенді жүргізілуде.

Қылмыстың бұл жаңа түрі қылмыстық-құқықтық ықпал ету шараларын қамтитын тиімді шараларға қарсы тұруы керек. Алайда қолданыстағы отандық қылмыстық заңнама қазіргі заманғы қылмыстың сын-қатерлеріне ден қоюға әрдайым үлгере бермейді. Сондықтан киберкеңістікте жасалған жаңа нақты қауіпті әрекеттер көбінесе қылмыстық заңның шеңберінен тыс қалады, ал криминализацияланған әрекеттерге қатысты оларды құқықтық бағалау және кінәлілерді жауапқа тарту бойынша маңызды проблемалар туындайды. Бұл жағдай зерттеу тақырыбының өзектілігін анықтайды.

Зерттеудің өзектілігі соңғы жылдары киберқылмыспен келтірілген зиянның мөлшері бірнеше есе өскенін де береді. Көптеген ғалымдардың пікірінше, "Интернет" желісіндегі көлеңкелі бизнестің кірісін есірткінің заңсыз

саудасынан түскен пайдамен салыстыруға болады. Кибершабуылдардың көбеюіне байланысты олардың келтірген залалы да артып келеді: егер өткен жылы экономиканың әртүрлі секторларындағы компаниялардың шығындары 1,5 трлн долларды құраса, 2019 жылы сарапшылардың болжамы бойынша олар 2,5 трлн долларға жетті. 2022 жылға қарай Дүниежүзілік экономикалық форумның болжамы бойынша кибершабуылдардан болатын планетарлық залал сомасы 8 трлн долларға дейін өсуі мүмкін [9].

Киберқылмыстардың өсу үрдісі күн сайын қашықтықтан банктік қызмет көрсету жүйелерінен ұрлық жасалатын Қазақстанда да бар. Сонымен қатар, 2019 жылы қазақстандық киберинциденттер туралы 50 – ге жуық хабарлама тіркелді, 2020 жылы-134 [10].

Сонымен қатар, киберқылмыстарға қарсы іс-қимылдың тиімділігіне киберкеңістікте жасалған экономикалық қылмыстардың да, компьютерлік ақпарат саласындағы қылмыстардың да өте жоғары кідіріс деңгейі теріс әсер етеді.

Диссертациялық зерттеудің мақсаты - киберқылмыс проблемасын, оның осы құбылыстың қоғамдық қауіптілік дәрежесін бағалау үшін қажетті криминологиялық маңызды аспектілерін зерделеу, онымен қылмыстық-құқықтық күрес шараларын талдау және киберқылмыспен күресті қылмыстық-құқықтық реттеудің тиімділігін арттыруға бағытталған ұсыныстар әзірлеу болып табылады.

Осы мақсатқа жету үшін келесі **міндеттер** кешенін қою және шешу қолданылады:

- Киберқылмыс және киберқылмыс түсінігін қалыптастыру, киберқылмыс түрлерін сипаттау.
- Киберқылмыстың жай-күйіне, құрылымына, динамикасына әлемдік (жаһандық) ауқымда криминологиялық талдау жүргізу.
- Киберқылмысқа қарсы іс - қимылдың құқықтық тәжірибесін екі деңгейде-халықаралық және ұлттық деңгейде талдау, оның ішінде шет елдердің заңнамасына салыстырмалы талдау жүргізу.
- Зерттеу тақырыбының призмасы арқылы ҚР-дағы компьютерлік қылмыспен күресуге бағытталған қылмыстық-құқықтық нормалардың кемшіліктерін талдап, қылмыстық заңнаманы жетілдіру бойынша ұсыныстар жасау.

Зерттеудің обьектісі. Киберкеңістікте жасалатын қылмыстар үшін жауапкершілік туралы қылмыстық заңнаманы іске асыру процесінде қалыптасатын қоғамдық қатынастар, сондай-ақ аталған қылмыстарға қарсы іс-қимыл шаралары зерттеу объектісі болып табылады.

Зерттеу пәнін құрайды:

1. Қазақстан Республикасының қолданыстағы қылмыстық заңнамасы экономикалық қатынастарды киберкеңістіктегі қол сұғушылықтан қорғайтын қылмыстық-құқықтық нормалар бөлігінде, сондай-ақ компьютерлік ақпаратқа заңды түрде қол жеткізуді, жасауды, өңдеуді, сатып алуды, пайдалануды қамтамасыз ететін қатынастар;

2. экономикалық қатынастар саласындағы, сондай-ақ компьютерлік ақпарат және ақпараттық-телекоммуникациялық желілер саласындағы адамдардың құқықтары мен мүдделерін киберкеңістіктегі қол сұғушылықтан қорғауға бағытталған қылмыстық-құқықтық нормаларды іске асыру практикасы;

3. қаралатын проблема бойынша алдын ала тергеу органдары мен соттың статистикалық және талдамалық материалдары;

4. шетелдік қылмыстық заңнама, сондай-ақ Еуропа Кеңесінің конвенциялары, БҰҰ Бас Ассамблеясының қарарлары және басқалары сияқты халықаралық актілер;

5. киберкеңістіктегі экономикалық қатынастарға қол сұғушылық, сондай-ақ компьютерлік ақпарат және ақпараттық-телекоммуникациялық желілер саласындағы қол сұғушылық проблемалары бойынша БАҚ және басқа да дереккөздердің материалдары.

Зерттеудің тәжірибелік құндылығы. Диссертациялық зерттеудің практикалық маңыздылығы-алынған нәтижелер қызметкерлердің біліктілігін арттыру бойынша сабақтар мен семинарлар өткізу кезінде соттар мен прокуратура органдарының жұмысына енгізіліп, оны енгізу туралы тиісті актілер жасалды.

Зерттеу нәтижелері "Қылмыстық құқық" және "Криминология" пәндерін оқыту кезінде оқу процесінде, оқулықтарды, оқу және практикалық құралдарды, әдістемелік ұсынымдарды және т. б. дайындаумен байланысты оқу-әдістемелік жұмыста іске асырылды.

Тақырыптың зерттелу деңгейі. Киберқылмыс мәселесі туралы бірнеше іргелі зерттеулер бар. Алайда, олардың барлығы өз уақытының заңнамасына негізделген және олардың көптеген ережелері енді өзекті емес. Сонымен қатар, қолданыстағы зерттеулер барлық киберқылмыстарға арналған, ал нақты экономикалық киберқылмыстарға арнайы зерттеулер жүргізілмеген.

Киберкеңістікте немесе "Интернет" желісінде жасалатын экономикалық қылмыстардың жекелеген қылмыстық-құқықтық және криминологиялық мәселелері отандық ғылымда А.И. Бойцовтың, А.Г.Волводздың, Б.В. Волженкиннің, в. г. Голубевтің, О. С. Гузееваның, М. С. Дашянның, И. А. Клепицкийдің, Н. Н. Ковалеваның, А.Н. Копырюлиннің, Т. М. Лопатинаның, В.Г.Степанов-Егиянецтің, П.С. Яни және басқалардың еңбектерінде қарастырылған.

Компьютерлік қылмыстарды жасағаны үшін киберқылмыс пен жауапкершілікке қарсы тұру тақырыбында бірнеше диссертациялық жұмыстар орындалды. Олар: В.Б. Вехов, Р.И. Дремлюги, Н.В. Зигура, Т. П. Кесареева, Н. Н. Лыткин, М.В.Старичков, Т. Л. Тропинаның еңбектері. Бұл диссертациялар киберқылмыстар мен киберкеңістікті зерттеуге белгілі бір үлес қосты, бірақ киберкеңістікте жасалған экономикалық қылмыстар мәселесі тек ішінара қозғалды. Сондықтан осы жұмыста қолда бар зерттеулер мен қолданыстағы заңнаманы ескере отырып, экономика саласындағы киберқылмыс ұғымы, объектісі және нысанасы, экономикалық киберқылмыстар жасау тәсілдері және

оларға қарсы іс-қимылдың қылмыстық-құқықтық шаралары туралы мәселелер бұрынғыға қарағанда көбірек ашылады.

Зерттеудің ғылыми жаңалығы. Зерттеу автордың теориялық негіздемесін берді және киберқылмыс ұғымын берді, киберқылмыстардың жалпы қылмыс жүйесінде де, экономикалық қылмыстар жүйесінде де орны анықталды, киберкеңістікті қылмыс құрамының белгілері жүйесінде қолдану мәселесі жасалды. Магистрлік диссертация деңгейінде алғаш рет киберқылмыстардың әдістері зерттелді, киберқылмыстардың авторлық жіктемесі берілді. Экономикалық қатынастарды киберқылмыстан қорғауға бағытталған отандық және шетелдік қылмыстық заңнаманың даму үрдістері айқындалды. Киберқылмыс үшін қылмыстық жауапкершілік туралы нормалар практикасын одан әрі дамытудың ғылыми болжамы ұсынылды және мұндай әрекеттерді қылмыстық-құқықтық бағалаудың нақты ұсыныстары жасалды. Киберқылмыстың жалпы және арнайы детерминанттары анықталды. Алынған мәліметтер негізінде киберкеңістікте жасалатын қылмыстардың барлық кешеніне қарсы іс-қимыл шараларының жүйесі әзірленіп, ұсынылды. Қорғауға ұсынылған ережелер де жаңалықтың қажетті деңгейіне ие.

Зерттеу әдістері. Жұмыстың әдіснамалық негізін танымның диалектикалық әдісі, жалпы ғылыми және формальды-логикалық әдістер (салыстыру, гипотеза, жүйелік-құрылымдық талдау), сондай-ақ арнайы - ғылыми және криминологиялық әдістер құрайды, мысалы: құжаттарды талдау әдісі; тарихи-құқықтық және салыстырмалы-құқықтық әдіс.

Қорғауға ұсынылатын қорытынды-тұжырымдамалар:

1.Киберқылмыс ұғымы компьютерлік техниканы, ақпараттық және телекоммуникациялық желілерді және олар құрған киберкеңістікті пайдалану арқылы қашықтықтан жасалған гетерогенді қоғамдық қатынастарға зиян келтіретін қылмыс ретінде анықталады.

2. Экономикалық киберқылмыстардың жасалу тәсіліне қарай олардың авторлық жіктемесі беріледі:

- компьютерлік және өзге де ұқсас техниканы пайдалана отырып, адамға психологиялық әсер ету (алдау, жаңылыстыру, қорқыту) арқылы жасалатын экономикалық киберқылмыс);

- жабдыққа (компьютерлер, смартфондар, маршрутизаторлар және басқа жабдықтар) әсер ету арқылы жасалатын экономикалық киберқылмыстар.

3. Экономикалық киберқылмыс жалпы объект ретінде экономикалық қатынастарға зиян келтіретін киберқылмыс деп саналуы керек.

4. Компьютерлік техника құралдарын, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қашықтықтан қылмыс жасау оның қоғамдық қауіптілігін арттыратын мән-жай болып табылуы мүмкін.

5. Компьютерлік техниканы, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қашықтан қылмыс жасауды жазаны ауырлататын мән-жайлар тізбесіне енгізу қажет, бұл ретте сотқа осы норманы қылмыстың сипаты мен қоғамдық қауіптілік дәрежесіне, оны

жасаудың нақты мән-жайларына және кінәлінің жеке басына қарай өз қалауы бойынша қолдануға мүмкіндік береді.

6. Қазақстанның қылмыстық заңнамасында ақпараттық қауіпсіздік саласындағы қатынастар "ақпараттық алаяқтық", "спам тарату", "ақпараттық жалғандық", "адамдарды терроризм мен экстремизмге насихаттайтын және оқытатын ақпараттық материал жасау және тарату", "компьютерлік диверсия" және т.б. қоғамға қауіпті бірқатар іс-әрекеттерді криминализациялау

7. Еуропалық киберқылмыс туралы конвенцияның ұсынымдарына сәйкес (күрестің мамандануы, қылмыстарды ашу және тергеу процесінің тікелей және үздіксіздігі қамтамасыз етіледі) тәулік бойы - 24/7 жұмыс істейтін тергеу және жедел топтарды қамтитын киберқылмыспен күрес жөніндегі бөлімшелерді ұйымдастыру қажет.

8. Құқық қорғау және арнайы органдарда кадрларды іріктеудің ерекше жүйесін қайта қарап, енгізу қажет. Біз, әдетте, техникалық білімі бар адамдарды заңгерлік дайындық курстарынан өтіп, жедел қызметкерлер мен мамандарды жұмысқа тартатын шет елдердің оң тәжірибесін қолдануға болады деп санаймыз. Бастапқы кезеңде мұндай талапты жедел қызметкерлерге орнатуға болады.

9. Тергеуді әдістемелік қамтамасыз ету. Қылмыстық әрекетті имитациялау және құқық қорғау органдары қызметкерлерінің енгізу әдістерін белсенді пайдалану, сондай-ақ посткеңестік кеңістік елдерінің аумағында киберқылмыстарды тергеу тәжірибесі, қылмыскерлер, бұғатталған сайттар туралы мәліметтер және т. б. бар бірыңғай құқықтық платформа құруға бастамашылық жасау.

10. Тиісті халықаралық құқықтық ынтымақтастық. Қазақстан Республикасының киберқылмыс туралы Еуропалық конвенцияға қосылуы туралы мәселенің оң шешілуі қажетті мәліметтер мен дәлелдемелерді жедел алуға мүмкіндік береді.

Эмпирикалық зерттеулер. Жүргізілген диссертациялық зерттеу осы мәселе бойынша халықаралық-құқықтық актілерді, Қазақстан Республикасының және шет мемлекеттердің заңнамасын, киберқылмысқа қарсы күрес саласындағы халықаралық құқық субъектілері қызметінің тәжірибесін зерделеуге және талдауға негізделеді.

Зерттеу нәтижелерінің сыннан өтуі. Диссертацияның негізгі теориялық және тәжірибелік мәні бар нәтиже-тұжырымдары автордың жарық көрген 2 ғылыми мақаласында жарияланған:

1. Киберқылмыс: жаһандық мәселе // «Егемен мемлекет ретінде Қазақстан республикасының дамуы: қазіргі заман шындығы, жаңа идеялар, құқықтық тәжірибе» атты халықаралық ғылыми-практикалық конференция материалдары. – «Фараби әлемі» атты студенттер мен жас ғалымдардың халықаралық ғылыми конференция материалдары. Алматы, Қазақстан, 6-8 сәуір 2021ж.

2. Қазақстанда киберқылмыспен күресу мәселелері // «Әуезов оқулары-19: тәуелсіз Қазақстанға– 30 жыл» атты Халықаралық ғылыми-тәжірибелік конференциясының еңбектері – Шымкент: М. Әуезов ат. ОҚУ, 2021 ж.

Жұмыстың құрылымы мен көлемі. Диссертация кіріспеден, екі бөлімнен, бес бөлімшеден, қорытындыдан және пайдаланылған әдебиеттер тізімінен тұрады.

1 Киберқылмыс ұғымы және белгілері

1.1 Киберқылмыс ұғымы және оның қоғамдық қауіптілігі

"Киберқылмыс" ұғымы көбінесе "компьютерлік қылмыс" және "компьютерлік ақпарат саласындағы қылмыс" ұғымдарымен шатастырылады, өйткені олардың барлығын бір нәрсе біріктіреді – бұл қылмыс жасау үшін компьютерлік техниканы қолдану, бірақ айтарлықтай айырмашылықтар бар.

Сонымен, ғылыми әдебиеттерде "компьютерлік қылмыс" термині "компьютерлік ақпарат саласындағы қылмыс" ұғымынан әлдеқайда кең деген пікір қалыптасқан» [11, 38 б.].

Бұл пікір компьютерлік қылмыстың объектісі компьютерлік ақпараттың қалыпты айналымы саласында қалыптасқан қатынастар ғана емес, сонымен қатар мүліктік қатынастар, ар-намыс, қадір-қасиет, іскерлік бедел сияқты қылмыстық заңмен қорғалатын басқа да қоғамдық қатынастар болуы мүмкін екендігіне негізделген. қоғамдық тәртіп, тіпті бейбітшілік пен адамзат қауіпсіздігі [12, 106 б.].

Сонымен, В.Б. Вехов компьютерлік қылмыстың келесі анықтамасын береді: бұл электронды есептеу (компьютерлік) құралдарын қолдана отырып жасалған қылмыстық заңда қарастырылған әлеуметтік қауіпті әрекет. Сонымен қатар, бұл әдіс қылмыстың қай кезеңінде қолданылғаны маңызды емес: дайындық кезінде, қылмыс жасау процесінде немесе қылмыстың іздерін жасыру үшін [13, 13 б.].

Демек, "компьютерлік қылмыс" ұғымына компьютерлік техниканы қолдана отырып жасалған кез-келген қылмыс (алаяқтық, бопсалау, жала жабу, тыңшылық, террористік акт, агрессивті соғысты бастауға шақыру және басқалар) кіруі мүмкін, ал компьютерлік ақпарат саласындағы қылмыстар компьютерлік ақпараттың қалыпты айналымы саласында (компьютерлік ақпаратты заңсыз пайдалану) қалыптасқан қатынастар болып табылатын қылмыстардың неғұрлым тар шеңберін қарастыру керек.; зиянды компьютерлік бағдарламаларды жасау, пайдалану және тарату; компьютерлік ақпаратты және ақпараттық-телекоммуникациялық желілерді сақтау, өңдеу немесе беру құралдарын пайдалану қағидаларын бұзу).

Өз кезегінде, барлық компьютерлік қылмыстар материалдық әлемде де, киберкеңістікте де жасалуы мүмкін. Киберкеңістікте жасалған қылмыстардың өзіндік ерекшелігі бар, өйткені олар байланысты қылмыстардан әлеуметтік қауіптің жоғарылауымен ерекшеленеді. Осының негізінде көптеген ғалымдар мұндай қылмыстарды тәуелсіз топқа бөледі [14, 38 б.].

Олар кез – келген қоғамдық қатынастарға, соның ішінде компьютерлік ақпараттың қалыпты айналымы саласындағы қатынастарға, меншік қатынастарына, Экономикалық қызмет саласындағы қатынастарға және т.б. бағытталуы мүмкін. Экономикалық киберқылмыскерлер киберкеңістікте жасалған қылмыстардың барлық спектрінің бір бөлігі ғана, бірақ бұл диссертациялық зерттеуде олар туралы айтылады.

Ғылыми әдебиеттерде қылмыстың бұл түріне көптеген анықтамалар бар. Т. Л. Тропинаның пікірінше, киберқылмыс "компьютерлердің, компьютерлік бағдарламалардың, компьютерлік желілердің жұмысына, компьютерлік деректердің рұқсатсыз модификациясына, сондай-ақ компьютерлердің, компьютерлік желілердің және бағдарламалардың көмегімен немесе көмегімен жасалған басқа да әлеуметтік қауіпті әрекеттерге, сондай-ақ компьютердің көмегімен модельдендірілген кеңістікке қол жеткізудің басқа құрылғыларының көмегімен немесе көмегімен" кінәлі жасалған әлеуметтік қауіпті қылмыстық құқық бұзушылық " деп түсінілуі керек» [14, 10 б.].

Бұл анықтама, біздің ойымызша, компьютерлік құралдарды қолдану арқылы жасалған қылмыстың табиғатын ашады, бірақ ол тым кең және дәл емес. Сонымен, компьютер өзінің негізгі мақсатына сай қолданылмаған, мысалы, егер компьютер басқа адамға соққы берсе, "компьютердің көмегімен жасалған басқа да әлеуметтік қауіпті әрекеттерге" ұшырауы мүмкін деп болжауға болады. Сонымен қатар, мұндай қылмыстарда компьютерді қолданудың әр түрлі деңгейі, қылмыс жасаудың әртүрлі тәсілдері, қол сұғушылықтың әртүрлі объектілері мен объектілері, соның салдарынан – басқа да сипаттағы және қоғамдық қауіптілік дәрежесі.

Біздің ойымызша, бұл анықтама тым тар, өйткені, біріншіден, "Интернет" желісінен басқа ("FidoNet" немесе кез - келген жеке жергілікті желілер) киберкеңістікті құрайтын басқа да ақпараттық және телекоммуникациялық желілер бар; екіншіден, киберкеңістікте тек ақпаратқа ғана емес, сонымен қатар меншікке де, басқа да қоғамдық қатынастарға (қоғамдық қауіпсіздік, қоғамдық мораль) қатысты қылмыстар жасалады.

Бұл анықтама "компьютерлік қылмыс" және "киберқылмыс" (немесе бұл жағдайда "интернеттегі қылмыс") ұғымдарын жалпы және жеке деп бөледі, сонымен қатар соңғысының ерекшелігін белгілейді. Интернет-қылмыс тек қана "Интернет" желісі арқылы жасалуы тиіс, сондай-ақ киберқылмыс тек қана киберкеңістік арқылы жасалуы тиіс.

О. С. Гузеева атап өткендей, киберқылмыс-бұл мақсатқа жетудің негізгі құралы ретінде ғаламдық компьютерлік желілерді қолдана отырып, қол сұғу объектісіне қашықтан қол жеткізу арқылы жасалған қылмыстық заңнамада қарастырылған қоғамдық қауіпті, заңсыз әрекет [15, 12 б.].

Бұл анықтамада, алдыңғы анықтамадағыдай, киберкеңістіктің мүмкіндіктері де қылмыс құралы ретінде бағаланады.

Киберқылмысты анықтау кезінде компьютерлік ақпарат саласындағы қылмыстар немесе "Интернет"желісін пайдалана отырып жасалған қылмыстар үшін ғана емес, барлық киберқылмыстарға тән ерекшеліктерді ескеру қажет сияқты. Біздің ойымызша, анонимдік, трансшекаралық, қашықтық сияқты киберқылмыстың белгілерін, сондай-ақ компьютерді, вирустарды (басқа да зиянды бағдарламаларды), ақпараттық және телекоммуникациялық желілерді және киберкеңістікті пайдалану қажет.

Біріншіден, киберқылмыс қандай жолмен жасалса да, қылмыс болып табылады, яғни Қазақстан Республикасының Қылмыстық кодексінде жазалау

қатерімен тыйым салынған кінәлі, жасалған, қоғамға қауіпті әрекет. "Киберқылмыс" терминінің өзінде "қылмыс" ұғымы қолданылады, бұл бізді оның негізгі белгілерін қайталаудан босатады.

Екіншіден, киберқылмыс компьютерлік ақпарат саласындағы қатынастарға ғана емес, қылмыстық заңмен қорғалатын барлық қоғамдық қатынастарға зиян келтіруі мүмкін. Демек, киберқылмыстарды қол сұғу объектісі бойынша бір ғана жіктеу және оларды Қазақстан Республикасы Қылмыстық кодексінің жеке бөліміне немесе тарауына бөліп көрсету мүмкін емес.

Үшіншіден, киберкеңістік трансшекаралық болғанымен, киберқылмыстардың барлығы да трансшекаралық сипатта бола бермейді (мысалы, егер кінәлі мен жәбірленуші бір елде тұратын болса). Анонимділік немесе зиянды бағдарламаларды пайдалану сияқты киберқылмыстың белгілері туралы да айтуға болады. Киберқылмыстардың барлығы жасырын түрде жасалмайды, көбісі (жала жабу немесе террористік әрекетке шақыру немесе терроризмді жария түрде ақтау сияқты) нақты есімдер мен фамилияларды қолдана отырып ашық түрде жасалады. Барлық киберқылмыстар вирустарды немесе өзге де зиянды бағдарламаларды (әлеуметтік желіде немесе электрондық пошта арқылы бопсалау) пайдалана отырып жасалмайтыны сияқты. Киберқылмыстың бұл белгілері негізгі емес (міндетті емес), яғни олар жеке киберқылмыстарға ғана тән болуы мүмкін, бірақ бәрі бірдей емес.

Барлық киберқылмыстардың біріктіруші белгілері оларды жасау құралдары – киберкеңістік, ақпараттық - телекоммуникациялық желілер және компьютерлік техника құралдары болып табылады.

Жоғарыда айтылғандай, киберкеңістік белгілі бір қызмет саласы (виртуалды шындық) ретінде тек ақпараттық және телекоммуникациялық желі аясында өмір сүре алады. Мұндай желі киберкеңістікке қол жеткізуге мүмкіндік беретін көптеген құрылғылар мен байланыс арналарынан құрылған. Құрылғылар ақпараттық және телекоммуникациялық желілер сияқты әртүрлі болуы мүмкін (жұмыс үстелі, ноутбук, планшет немесе смартфон). Бұл ретте бір компьютер бірден бірнеше ақпараттық-телекоммуникациялық желілерге қосылуы мүмкін. Сондықтан "киберқылмыс" ұғымын тек жеке компьютерді немесе "Интернет" желісін пайдалану арқылы шектеу түбегейлі дұрыс емес. Қылмыскер киберкеңістікке қол жеткізу үшін түрлі құрылғылар мен ақпараттық-телекоммуникациялық желілерді пайдаланады. Демек, киберкеңістік киберқылмыс жасаудың міндетті шарты болып табылады.

Ақпараттық-телекоммуникациялық желінің болуы да киберқылмыс жасаудың міндетті шарты болып табылады, өйткені онсыз киберкеңістік болмайды. Киберкеңістікке қол жеткізу үшін компьютерлік техниканы пайдалану барлық киберқылмыстардың ажырамас белгісі болып табылады, өйткені киберкеңістікке басқа жолмен кіруге болмайды.

Қылмыскер компьютерді ең алдымен киберкеңістікке кіру үшін пайдаланады. Егер кінәлі адам компьютерді қолына алып, олардың денсаулығына қасақана зиян келтірсе, онда мұндай әрекетті киберқылмыс деп

атауға болмайды. Киберкеңістікке қол жеткізгеннен кейін қылмыскер жаңа мүмкіндіктерге ие болды – енді ол үйден шықпай-ақ қашықтан қылмыс жасай алады.

Қашықтан қылмыс жасау барлық киберқылмыстарды жасау әдісінің ажырамас сипаттамасы болып табылады. Кінәлі адам киберкеңістіктің мүмкіндіктерін өзі мен жәбірленуші арасында қауіпсіз қашықтық болатындай етіп саналы түрде пайдаланады.

Жоғарыда айтылғандарға сүйене отырып, біз киберқылмыстың келесі анықтамасын ұсынамыз:

киберқылмыс дегеніміз - компьютерлік технологиялар мен ақпараттық-телекоммуникациялық желілерді және олар құрған киберкеңістікті пайдалану арқылы қашықтықтан жасалған гетерогенді қоғамдық қатынастарға зиян келтіретін қылмыс.

Бұл анықтама "киберқылмыс" ұғымын құрал (киберкеңістік) және әдіс (қашықтық әдіс) сияқты міндетті белгілері арқылы ашады. Ол сондай-ақ сыйымды, өйткені ол қылмыстың барлық белгілерін қайталамайды. Бұл анықтама қол сұғу объектісімен де, нақты ақпараттық-телекоммуникациялық желімен де шектелмейді, бұл оны айтарлықтай икемді етеді: "Интернет" желісіндегі алаяқтық та, "FidoNet" немесе "TOP"желісіндегі компьютерлік ақпаратқа заңсыз қол жеткізу де киберқылмыс болып саналады.

Осы логикаға сүйене отырып, мұндай киберқылмыс экономикалық киберқылмыс болып саналады, оның жалпы нысаны экономикалық қатынастар болып табылады.

Киберқылмыс ұғымын ашып, біздің ойымызша, қылмыстардың осы тобының әлеуметтік қауіптілігінің сипаты мен дәрежесін анықтауға толығырақ тоқталу керек. Көптеген ғалымдар киберқылмыстардың материалдық әлемде жасалған ұқсас қылмыстарға қарағанда әлеуметтік қауіптіліктің жоғары деңгейіне ие екендігімен келіседі.

Сонымен, Н.А. Коменский компьютерлік ақпарат пен ақпараттық технологияларды қылмыс жасау құралы ретінде пайдалану оның әлеуметтік қауіптілігін арттыратынын және бұл белгіні жазаны ауырлататын жағдай ретінде бекітуді орынды деп санайды [16, 35 б.].

Т. Л. Тропинаның пікірінше, " киберқылмыс ең төменгі шығындар мен төмен тәуекелмен үлкен зиян келтіру мүмкіндігіне байланысты әлеуметтік қауіпті арттырды» [14, 17 б.].

Экономикалық киберқылмыстардың қоғамдық қауіптілігінің сипатын талдау кезінде, ең алдымен, қол сұғу объектісі мен қылмыс жасау әдісін қарастырған жөн. Біздің ойымызша, киберкеңістікте экономикалық киберқылмыстардың екі тобын құрудың нақты мүмкіндігі бар, олардың арасындағы айырмашылық объект пен әдіспен көрінеді.

Жасау әдісіне байланысты барлық экономикалық киберқылмыстарды бөлуге болады:

* адамға психологиялық әсер ету арқылы жасалатын экономикалық киберқылмыстар (алдау, жаңылыстыру, қорқыту);

* жабдыққа (компьютерлер, смартфондар, маршрутизаторлар және басқа жабдықтар) әсер ету арқылы жасалатын экономикалық киберқылмыстар.

Мұндай бөлу экономикалық киберқылмыстардың бірінші тобына тек бір тікелей объектіге – экономикалық қатынастарға зиян келтіретін әлеуметтік қауіпті әрекеттер кіреді. Екінші топтың экономикалық киберқылмысын жасаған кезде қылмыскер қосымша объектіге – компьютерлік ақпаратты заңды және қауіпсіз пайдалануға байланысты қатынастарға зиян келтіреді.

Бірінші топтың киберқылмыстары оларды жасау кезінде бұрыннан бар сайттар, форумдар және дайын бағдарламалар қолданылатындығымен ерекшеленеді. Қылмыскерлерге компьютерлік ақпаратқа заңсыз қол жеткізудің қажеті жоқ, олар киберкеңістіктің өзі беретін нәрселермен жұмыс істейді.

Мұндай киберқылмыстарға алаяқтықтың негізгі құрамы (ҚР ҚК 190-б.), қорқытып алушылық (ҚР ҚК 194-б.), алдау және сенімге қиянат жасау жолымен мүліктік залал келтіру (ҚР ҚК 195-б.), заңсыз кәсіпкерлік, заңсыз банктік, микроқаржы немесе коллекторлық қызмет (ҚР ҚК 194-б.) жатады. Банктік құпияны, деңгейлес мониторинг барысында алынған салықтық құпияны, микрокредит беру құпиясын, коллекторлық қызмет құпиясын құрайтын мәліметтерді, сондай-ақ мүлікті жария етуге байланысты ақпаратты заңсыз алу, жария ету немесе пайдалану (ҚР ҚК 223-б.2-б.) және басқалары жатады.

Осы киберқылмыстарды жасау тәсілі материалдық әлемде ұқсас қылмыстарды жасау тәсілінен айтарлықтай ерекшеленбейді: алаяқтық кезінде – алдау немесе сенімді теріс пайдалану; қорқытып алушылық кезінде – қауіп; бұрмалау кезінде – көрінеу жалған деректерді беру және т.б. киберкеңістіктегі алдау материалдық әлемдегі алдау сияқты қоғамдық қауіптілік сипатына ие, бірақ қазір олар қашықтықтан жүзеге асырылады. Бұл қауіп-қатермен және бұрын келісілген басқа әдістермен де көрінеді.

Осы қылмыстарды жасаған кезде адам компьютерлік ақпаратқа заңсыз қол жеткізуді кедергісіз жүзеге асыруға мүмкіндік беретін арнайы бағдарламаларды қолдана алады ("BruteForce", "Public Brute/Checker") немесе вирустарды ("Creeper", "Elk Cloner", "Brain","Jerusalem", "March", "CIH", "Nimda"), трояндық бағдарламаларды ("Win64/HackKMS.A"), компьютерлік құрттар ("Melissa"," Sasser"," My Doom"," Conficker") және басқа да зиянды бағдарламалар. Экономикалық киберқылмыстар жасау кезінде осы зиянды бағдарламалық қамтамасыз етуді пайдалана отырып, кінәлі тұлға бірден екі объектіге – экономикалық қатынастарға және компьютерлік ақпарат саласындағы қатынастарға зиян келтіреді.

Қылмыстардың осы тобының екі Объектілік табиғаты олардың әлеуметтік қауіптілігін арттыратын жағдай болып көрінеді. Осы қылмыстарды 205-баптың жиынтығы бойынша саралау қажет. Істің нақты мән-жайларына байланысты" ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге құқыққа сыйымсыз қол жеткізу "және ҚР ҚК 210" зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату".

Экономикалық киберқылмыстардың қоғамдық қауіптілік дәрежесін талдау кезінде келтірілген зиянның мөлшеріне ерекше назар аудару керек. А. К. Киселев атап өткендей, 2007-2008 жылдары бүкіл әлемде киберқылмыстан келтірілген залал 8 миллиард долларға бағаланды [17, 25 б.]. Киберқауіпсіздік бойынша халықаралық сарапшылар 2019 жылы әлемде кибершабуылдар әр 14 секунд сайын болады деп есептеді. Кибершабуылдардың көбеюіне байланысты олардың келтірген залалы да артып келеді: егер өткен жылы экономиканың әртүрлі секторларындағы компаниялардың шығындары 1,5 трлн долларды құраса, 2019 жылы сарапшылардың болжамы бойынша олар 2,5 трлн долларға жетті. 2022 жылға қарай Дүниежүзілік экономикалық форумның болжамы бойынша кибершабуылдардан болатын планетарлық залал сомасы 8 трлн долларға дейін өсуі мүмкін [9].

Көптеген ғалымдардың пікірі бойынша (Т.М. Лопатина, В. А. Номоконов, Т. Л. Тропина) "Интернет" желісіндегі көлеңкелі бизнестің кірістерін есірткінің заңсыз саудасынан түскен пайдамен салыстыруға болады.

Кибершабуылдардың ең көп кездесетін жағдайлары-ботнеттер: 17,7 мың оқиға. Ботнет немесе зомби-желі-бұл зиянкестерге басқа адамдардың машиналарын олардың иелерінің келісімінсіз қашықтықтан басқаруға мүмкіндік беретін зиянды бағдарламамен зақымдалған Компьютерлер желісі. Ботнеттердің көмегімен зиянкестер спам жіберуі, вирустар таратуы, компьютерлер мен серверлерге шабуыл жасауы және басқа да қылмыстар жасауы мүмкін.

Сектордағы оқиғалар арасында екінші орынды фишинг алады: 883 жағдай. Бұл компьютерлік алаяқтықтың негізгі мақсаты-жәбірленушіні алдау арқылы шабуылдаушыға қажетті ақпаратты беруге мәжбүрлеу. Бұл заңмен қудаланатын компьютерлік қылмыс. Бүгінгі таңда фишинг-әлемде ең көп таралған киберқылмыстардың бірі, оның көмегімен аккаунттар мен банк ақпараты жиі ұрланады.

Сондай-ақ зиянды бағдарламалық қамтылым, Интернет-ресурстардағы бұзылыстар, қызмет көрсетуден бас тарту (DDoS-шабуылдар) және т.б. сияқты инциденттер жиі кездеседі.

Cybersecurity Ventures болжамына сәйкес, 2019 жылы бүкіл әлемде хакерлердің шабуылдары әр 14 секунд сайын болды, ал 2021 жылға қарай олардың жиілігі әр 11 секундқа дейін артады. Сондай-ақ, 2021 жылға қарай киберқылмыстан болатын жаһандық залал 6 триллион АҚШ долларына жетеді деп болжануда [18].

Жоғарыда келтірілген мәліметтерден экономикалық киберқылмыстардан келтірілген зиянның мөлшері өте жоғары, бұл мұндай қылмыстардың қоғамдық қауіптілігінің жоғарылағанын көрсетеді. Алайда, бұл сандар басқаша түсіндірілуі мүмкін: киберкеңістік мүмкіндіктері бар бір адам мұндай мүмкіндіктерсіз емес, әлдеқайда көп қылмыс жасай алады. Мәселен, мысалы, бір уақытта хакер он ұрлық жасай алады, ал қарапайым қылмыскер – бір ғана нәрсе. Сондай-ақ, киберкеңістіктің мүмкіндіктерімен кінәлі бір уақытта бірнеше зардап шеккендерге қатысты қылмыс жасай алады, осылайша

келтірілген зиянды көбейтеді.

Екінші жағынан, киберкеңістікті пайдалану қылмыстың қоғамдық қауіптілік дәрежесін арттырмайтын мысалдар бар, мысалы, егер бопсалау кезінде кінәлі адам белгілі бір ақшаны тек бір жәбірленушіден жала жабатын ақпаратты тарату қаупімен аударуды талап етсе. Бұл жағдайда қылмыскер киберкеңістікті тек байланыс құралы (телефон немесе қарапайым пошта) ретінде пайдаланады, бұл қорқытып алушылықтың қоғамдық қауіптілігіне әсер ете алмайды. Бұл жағдайда киберкеңістікті пайдалану арқылы немесе онсыз бопсалаудың қалай жасалғанында ешқандай айырмашылық жоқ[19, 198 б.].

Киберқылмыстардың қоғамдық қауіптілігіне киберкеңістіктің өзі емес, оны қалай пайдалану керектігі әсер етуі мүмкін сияқты. Егер ұрлық жасаған кінәлі адам бірнеше банктік шоттарға бірден қол жеткізу үшін киберкеңістіктің мүмкіндіктерін пайдаланып, көп зиян келтірсе, киберкеңістікті пайдалану осы қылмыстардың қоғамдық қауіптілігін тікелей арттырады.

Сонымен бірге, егер кінәлі адам қандай да бір қылмыс жасаған кезде киберкеңістіктің мүмкіндіктерін тек байланыс құралы немесе ақпаратты іздеу, сақтау құралы ретінде ғана (яғни оның негізгі мақсаты бойынша) пайдаланса, онда киберкеңістікті мұндай пайдалану осы қылмыстардың қоғамдық қауіптілігіне әсер ете алмайды. Алайда, мұны тек сот нақты қылмысқа, істің нақты жағдайларына және кінәлінің жеке басына байланысты анықтай алады.

Бұдан шығатыны, кейбір жағдайларда киберкеңістікті пайдалану қылмыстың қоғамдық қауіптілігін арттыратын жағдай деп танылуы мүмкін, өйткені бұл әдіс қосымша объектіге зиян келтіруі мүмкін, көп зиян келтіруге ықпал етеді және қылмыс жасауды жеңілдетеді.

Біздің ойымызша, авторлармен киберкеңістікті қолдануды жазаны ауырлататын жағдайлар тізіміне енгізу туралы келісу керек. Алайда, сонымен бірге сотқа нақты ақпараттық ресурстар мен технологияларды пайдалану белгілі бір қылмыстың әлеуметтік қауіптілігін арттыратын жағдай ма, жоқ па, соны шешуге мүмкіндік беру керек. Бұл норманы неғұрлым икемді етуге мүмкіндік береді, ал құқық қолданудың күрделілігі Қазақстан Республикасы Жоғарғы Сотының нормативтік қаулысы деңгейінде шешілуі мүмкін.

Біз ұсынған норма қолданыстағы қылмыстық заңнамада жазаны ауырлататын басқа жағдайға – мас болу жағдайына қатысты бар.

1.12 бөлігіне сәйкес. ҚР ҚК 54-бабы сот қылмыстың сипаты мен қоғамдық қауіптілік дәрежесіне, оның жасалу мән-жайларына және кінәлінің жеке басына қарай алкогольді, есірткі құралдарын немесе басқа да есеңгіретететін заттарды пайдаланудан туындаған масаң күйде қылмыс жасауды ауырлататын мән-жай деп тануы мүмкін.

Біздің ойымызша, мұндай заңнамалық құрылымды "компьютерлік техниканы, ақпараттық және телекоммуникациялық желілерді және киберкеңістікті қолдана отырып, қашықтан қылмыс жасау"сияқты жағдайларға қатысты қолдануға болады. Алайда, құқықтық техника тұрғысынан норма шағын редакцияны қажет етеді.

Осы түрдегі 1.12-бөлім. ҚР ҚК-нің 54-бабын жаза тағайындаудың негіз

қалаушы қағидаттарының бірі бұзады: жазаны ауырлататын мән-жайлардың тізбесі жабық, және тізбеге енбеген бірде-бір мән-жайды сот ауырлататын мән-жай деп тани алмайды. Мас болу жағдайы ҚР ҚК 54-бабының 1-бөлігінде көрсетілмеген, сондықтан оны ауырлататын деп тануға болмайды.

Біздің ойымызша, масаң күйді жазаны ауырлататын мән-жайлар тізбесіне енгізу (ҚР ҚК 54-бабының 1-бөлігі) және қылмыстың сипаты мен қоғамдық қауіптілік дәрежесіне, оның жасалу мән-жайына және кінәлі адамның жеке басына қарай, керісінше, оны ауырлататын мән-жай деп танымау құқығын беру заңды тұрғыдан дұрыс шешім болар еді.

Норманың мәні өзгермейді-белгілі бір жағдайларда мас болу жағдайы ауырлататын жағдай деп танылады, бірақ жабық тізім принципі сақталады. Сондай-ақ 1.12 бөлігі. ҚР ҚК-нің 54-бабы кінәлінің жағдайын ауырлатпайды, керісінше, оны жұмсартады.

Зерттеу тақырыбына қайта орала отырып, біз киберқылмыс үшін жаза тағайындау туралы норманың негізі ретінде заңнамалық дизайнның осы моделін алуды ұсынамыз.

ҚР ҚК 3-бабының 1-бөлігін жаңа тармақпен толықтыру ұсынылады:

"с) компьютерлік техника құралдарын, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қылмыс жасау".

Бір мезгілде ҚР ҚК 54-бабы жаңа бөлікпен толықтырылсын:

«1.2. Жаза тағайындайтын судья (сот) қылмыстың сипаты мен қоғамдық қауіптілік дәрежесіне, оның жасалу мән-жайларына және кінәлінің жеке басына қарай компьютерлік техника, ақпараттық-телекоммуникациялық желілер мен киберкеңістікті пайдалана отырып, қылмыс жасауды ауырлататын мән-жай деп танымауы мүмкін".

Бұл жаңашылдық құқық қолдану практикасындағы көптеген мәселелерді шешуге мүмкіндік береді, бұл сотқа киберкеңістіктің қандай жағдайда қылмыс жасау үшін пайдаланылғанын және қайсысы пайдаланылмағанын шешуге мүмкіндік береді; қандай жағдайда оны пайдалану жоғары зиянның себебі болды, ал қайсысында жоқ; киберкеңістікті пайдалану қылмыстың қоғамдық қауіптілігіне әсер етті немесе жоқ. Бұдан басқа, осы норманы қолдану Қазақстан Республикасы Жоғарғы Соты Пленумы қаулысының негізіне алынуы мүмкін тұрақты сот практикасын қалыптастырады.

Алдын ала қорытындылай келе, бірнеше қорытынды жасау керек.

1.Киберқылмыс ұғымы компьютерлік техниканы, ақпараттық және телекоммуникациялық желілерді және олар құрған киберкеңістікті пайдалану арқылы қашықтықтан жасалған гетерогенді қоғамдық қатынастарға зиян келтіретін қылмыс ретінде анықталады.

2. Экономикалық киберқылмыстардың жасалу тәсіліне қарай олардың авторлық жіктемесі беріледі:

- компьютерлік және өзге де ұқсас техниканы пайдалана отырып, адамға психологиялық әсер ету (алдау, жаңылыстыру, қорқыту) арқылы жасалатын экономикалық киберқылмыс);

- жабдыққа (компьютерлер, смартфондар, маршрутизаторлар және басқа

жабдықтар) әсер ету арқылы жасалатын экономикалық киберқылмыстар.

3. Экономикалық киберқылмыс жалпы объект ретінде экономикалық қатынастарға зиян келтіретін киберқылмыс деп саналуы керек.

4. Компьютерлік техника құралдарын, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қашықтықтан қылмыс жасау оның қоғамдық қауіптілігін арттыратын мән-жай болып табылуы мүмкін.

5. Компьютерлік техниканы, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қашықтан қылмыс жасауды жазаны ауырлататын мән-жайлар тізбесіне енгізу қажет, бұл ретте сотқа осы норманы қылмыстың сипаты мен қоғамдық қауіптілік дәрежесіне, оны жасаудың нақты мән-жайларына және кінәлінің жеке басына қарай өз қалауы бойынша қолдануға мүмкіндік береді.

1.2 Киберкеңістік және киберқылмыс арақатынасы және белгілері

Ақпараттық сала бүгінгі таңда барабар құқықтық реттеуді қажет ететін қоғамдық қатынастардың ең серпінді және тез дамып келе жатқан салаларының бірі болып табылады [20, 15 б.]

"Интернет" қазіргі қоғам өмірінің ажырамас бөлігіне айналды, оның өзіндік инфрақұрылымы пайда болды: өзіндік тіл, желілік мәдениет, дүкендер, қоғамдық форумдар, білім беру курстары мен мектептер. Интернетте киберкеңістік сияқты жаңа құбылыс пайда болды.

Қазір "киберкеңістік", "ақпараттық кеңістік", "виртуалды кеңістік" және "Интернет кеңістігі" терминдері отандық және заңнамалық деңгейде, соның ішінде академияда да жиі қолданылады. Алайда, бұл ұғымдар табиғаты жағынан да, мағынасы жағынан да ерекшеленеді және оларды дұрыс пайдаланбау көптеген терминологиялық қиындықтар мен проблемаларды тудыруы мүмкін. Демек, бірінші кезекте қолданылатын терминологияға анықтық енгізу қажет.

"Ақпараттық кеңістік" ұғымы тым кең және өз табиғаты бойынша ақпарат (БАҚ, теледидар, телефония, кітаптар және өзге де баспа өнімдері) бар қоғам өмірінің кез келген саласын қамтиды.

"Киберкеңістік "ақпараттық кеңістіктің" бір бөлігі ғана болып табылады[20, 17 б.].

"Виртуалды кеңістік" термині тым кең, өйткені "виртуалды" "қиял" сөзінің синонимі ретінде компьютерлік технологиялармен шектелгендерге қарағанда құбылыстардың едәуір үлкен шеңберін қамтиды.

"Интернет кеңістігі", керісінше, тым тар термин, өйткені" Интернет"желісінен басқа, басқа да кішігірім ақпараттық-телекоммуникациялық желілер бар ("FidoNet"," CREN"," EARNet"," EUNe"," TOP"," ants P2P","Freenet"). Сонымен қатар," Интернет " өз атауы болып табылады және болашақта оның орнына басқа аты бар басқа дүниежүзілік ақпараттық-телекоммуникациялық желі келеді, ал ондағы киберкеңістік

өзгеріссіз қалады.

"Киберкеңістік" термині шетелдік заңнама мен әдебиетте қолданылады. Ағылшын тілінде "кибер" - бұл тәуелсіз сөз емес, префикс, яғни күрделі сөздердің бастапқы элементі, бірақ ол орыс тіліне "компьютерлермен, ақпараттық технологиялармен,"Интернетпен" байланысты деп аударылады. Терминологиялық шатасуды болдырмау үшін көптеген беделді ғалымдар (В.А. Номоконов, Т. Л. Тропина) бұл терминді аудармайды және "кибер"префиксін қолданады. Алайда, басқа беделді ғалымдардың пікірі бойынша "Киберкеңістік" терминін орыс криминологиялық ғылымында қолдану әлі де сұрақ туындады[11, 42 б.] және англикизмді пайдаланбау үшін басқа терминологияны қолдану қажет[21, 11 б.].

Біздің ойымызша, "киберкеңістік" термині барлық қолданыстағылардың ішіндегі ең оңтайлы болып табылады, ал осы терминді пайдалану ақпараттық желілерде болып жатқан құбылыстардың табиғатын толық ашуға мүмкіндік береді, олардың бірі "Интернет"болып табылады. Оның үстіне, дайындалып жатқан Қазақстан Республикасының киберқауіпсіздік стратегиясына байланысты осы терминді пайдалану анағұрлым өзекті болып табылады.

Сондықтан терминологияның біркелкілігі үшін және зерттеу тақырыбына байланысты бұл жұмыста "киберкеңістік", "киберқылмыс" және "киберқылмыс"сияқты терминдер қолданылады[22, 49 б.].

Компьютерлердің жаппай таралуы және ақпараттық желілердің пайда болуы қылмыстың жаңа түрі - киберқылмыстың пайда болуына түрткі болды, оның Қазақстанда және әлемде қалыптасу тарихын шартты түрде екі кезеңге бөлуге болады: бізге үйреншікті түрде киберкеңістікті туындатқан "Интернет" жаһандық ақпараттық желісі пайда болғанға дейін және кейін[23].

Бірінші кезең (1960-1991 жж.). 1960 жылдары АҚШ-та компьютерлерді кейбір мемлекеттік органдар үлкен шығындарға байланысты ғана қолданды. 1960 жылдардағы компьютерлік қылмыстар оқшауланған және компьютерлік ақпарат пен жеке мәліметтерге заңсыз қол жеткізу, оларды өзгерту немесе жою болды, ал дұрыс емес және толық емес заңнамалық реттеу және дәлелдемелер базасын алу тәсілдерінің болмауына байланысты көптеген істер құлдырады2.

"Компьютерлік бум "және соның салдарынан киберқылмыстың жаңа түрлерінің пайда болуы 1970-ші жылдардың аяғы мен 1980 – ші жылдардың басында АҚШ-та алғашқы IBM 5100 және Apple I дербес компьютерлерінің пайда болуымен, сондай – ақ" Интернет "желісінің негізін қалаушы - "Арпанеттің" пайда болуымен болды.

1975 жылы АҚШ Қорғаныс министрлігінің алдыңғы қатарлы зерттеулер агенттігі (Advanced Research Agency - ARPA) Стэнфорд және Калифорния университеттерімен бірлесіп, жұмыс режимінде "Арпанет" (ағылш. "Arpanet") қазіргі уақытта "Интернет"желісінде пайдаланылатын TCP/IP деректерді беру хаттамасын пайдаланатын [24, 15 б.]. Сонымен қатар, компьютерлер мен "Арпанет"желісін пайдалану арқылы жасалған қылмыстар жаппай пайда болды.

Мемлекет жаңа қауіпке екі жылдан кейін ғана жауап берді.

КСРО-дағы алғашқы жергілікті компьютерлік желілер 1970 жылдардың

аяғында-1980 жылдардың басында пайда болды. КСРО-да компьютерді қолданатын алғашқы қылмыс 1979 жылы Вильнюсте тіркелді, ол 78 584 рубль ұрлады. Бұл қылмыс халықаралық құқық бұзушылықтар тізіліміне енгізілді және КСРО мен Ресейде компьютерлік қылмыстардың дамуының бастапқы нүктесі болып табылады. 1983 жылы Тольяттидегі компьютерлік бағдарламаны өзгерту арқылы 1 миллион рубльге мүліктік залал тіркелді [14, 27 б.]

1980 жылдардың басында АҚШ-та "Милнет" ақпараттық – телекоммуникациялық желісі ("Milnet", Military Network-әскери желі) пайда болды, оны тек АҚШ Қорғаныс министрлігі пайдаланды. Біраз уақыттан кейін" Арпанет "пен" Милнеттің "бір бөлігі біріктіріліп, олардың жалпы атауы үшін" Интернет " (ағылш. «Internet»). Осы уақыт аралығында "Интернет" желісі салыстырмалы түрде аз болды және "жаһандық ақпараттық желі" болмады, сондықтан басқа ақпараттық желілермен бәсекелесті. Сонымен қатар, "NSFNet" ("АҚШ Ұлттық ғылыми қорының ақпараттық телекоммуникациялық желісі") және "USEnet" ("пайдаланушылық желі") сияқты желілер пайда болды. Барлық компьютерлік желілерге қосылатын пайдаланушылар саны жылына 10 000 адамға жеткен ал "бұзу" қоғамда танымал болды. Бұған ішінара кино мен ғылыми-фантастикалық романдар ықпал етті: 80-жылдардың ортасына қарай хакерлер туралы көптеген фильмдер үлкен экранға шықты (1982 ж. "тақ", 1983 ж. "соғыс ойындары", 1985 ж. "нағыз данышпан". және т.б.), ал 1984 жылы Уильям Гибсонның "Нейромант" романы жарық көрді, ол киберкеңістік идеясын сипаттады[24, 17 б.].

Нәтижесінде киберқылмыстың күшеюі болды. Т.Л. Тропина атап өткендей, осы уақыт аралығында "Security Pacific Bank" (10.2 млн.доллар) тонау орын алды, әлемде алғашқы компьютерлік вирус пайда болды (1984 ж.) және 1,2 млн. "Robbins" әуе күштері 17 жастағы хакер (1987)[14, 28 б.].

КСРО-да "Бүкіл планеталық компьютерлік желі" туралы 1980 жылдардың соңында айтылды. Осылайша, "Бүкілодақтық қолданбалы автоматтандырылған жүйелер ҒЗИ" компьютерлері 1988-1989 жылдары барлық әлеуметтік елдердің, сондай-ақ Австрия мен Финляндияның ұлттық компьютерлік желісіне еркін қол жеткізді. Эксперименттік режимде Куба мен АҚШ-тан компьютерлермен мәліметтер жіберілді[25, 78 б.].

1980 жылдардың соңы ақпараттық желілердің жаһандануымен де байланысты.

1989 жылы Еуропалық ядролық зерттеулер кеңесі (CERN) HTTP деректерді беру протоколын, яғни гипермәтіндерді қолдана отырып, "бүкіләлемдік ғаламтор" идеясын ұсынды. Осы уақытқа дейін киберкеңістіктің пайда болуы үшін барлық техникалық жағдайлар жасалды.

Екінші кезең (1991 ж. - біздің уақытымыз бойынша). 1991 жылы" Интернет "әлемдік ақпараттық желіге айналды, яғни әртүрлі елдердің хакерлері бүкіл әлемде кедергісіз қылмыс жасауға мүмкіндік алды, ал компьютерлік қылмыс трансшекаралық белгіге ие болды.

Қазақстандық заңнамамен рұқсат етілмеген қолжетімділіктен ақпаратты қабылдау, беру және жинақтаудың техникалық құралдарының қорғалуы

мәселелерінің ерекше өзектілігі атап өтілді, атап айтқанда "ақпараттық қауіпсіздік" ұғымын енгізумен 1998 жылғы 26 маусымдағы "Ұлттық қауіпсіздік туралы" ҚР Заңымен, сондай-ақ ҚР Президентінің "ҚР ақпараттық қауіпсіздік тұжырымдамасы туралы"Жарлығымен. ҚР Қылмыстық кодексінде осындай әрекеттер үшін жауапкершілікті көздейтін қылмыс құрамымен 227-бапты бекіте отырып, Құқық қорғау органдары компьютерлік техниканы қылмыстық мақсаттарда пайдаланатын адамдармен күресудің нақты мүмкіндігіне ие болды.

Жалпы, компьютерлік ақпаратқа заңсыз қол жеткізу, ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату үшін ҚР ҚК 227-бабында көзделген тіркелген қылмыстардың саны туралы статистикалық деректер мұндай қылмыстардың саны қарқынды өсіп келе жатқанын көрсетеді. Сонымен, егер 2000 жылы елде осындай қылмыстар тіркелген болса, онда 2008 жылы олар 5 есе көп болды. Бұл ретте тергеу органдарына осындай сипаттағы әрекеттердің 10 пайызынан аспайтын компьютерлік қылмыстардың жасалғаны туралы белгілі болады. Мұндай қылмыстардың ашылу көрсеткіші одан да аз. Жасалған қылмыстардың жалпы санына қатысты мұндай іс-әрекеттер онша көп емес. Кішкентай компьютерлік алаяқтар-жалған құжаттарды жасаушылар әлдеқайда көп зиян келтіреді. Жалған құжаттарды жасау, Компьютерлік техниканы пайдалана отырып ірі көлемдегі ақша қаражатын ұрлау үйреншікті іске айналды [26, 27 б.].

Бүгінгі таңда компьютерлік техника мен желінің қарапайым қарапайым пайдаланушысы принтерде әртүрлі түрдегі құжаттарды, бланкілерді, куәліктерді, мөртабандарды, сертификаттарды және т.б. басып шығара алады, осылайша соңғы бірнеше жылда ҚР ҚК-нің 325-бабында көзделген "жалған құжаттарды, мөртабандарды, мөрлерді, бланкілерді, мемлекеттік наградаларды қолдан жасау, дайындау немесе өткізу" қылмыстарының 20 мыңға жуығы тіркелген. 2004 жылдан бастап 2008 жылға дейін жалған құжаттарды, мөртабандарды, мөрлерді, бланкілерді және мемлекеттік наградаларды қолдан жасау, дайындау немесе өткізу фактілерінің саны 1645-тен 2017-ге дейін 22,6% - ға ұлғайды. Алайда, ҚР аумағында компьютерлік техника мен коммуникация құралдары қол сұғу объектілері ретінде емес (салыстыру үшін, компьютерлік ақпаратқа заңсыз қол жеткізу, машиналық уақытты ұрлау, сондай - ақ электрондық транзакция арқылы ақша қаражаты-бұл АҚШ, Канада, Еуропа елдерінің құқық қорғау органдары күресуге мәжбүр болатын қылмыстардың толық тізбесі және т.б.), көп жағдайда қылмыстық іс-әрекет құралы ретінде пайдаланылады.

Киберқылмыс жеке адамдарға немесе ұйымдарға ғана емес, сонымен бірге экономиканың маңызды салаларын компьютерлендірудің маңызды деңгейіне жеткен кез - келген елдің ұлттық қауіпсіздігіне қауіп төндіреді.

Ақпараттық кеңістіктегі Интернеттің рөлінің өсуімен адам мен қоғамның құқықтары мен бостандықтарын зорлық-зомбылық пен қатыгездікті насихаттайтын ақпараттан, оларға жалған және жалған ақпарат енгізуден, жас ұрпақтың теріс дүниетанымын мақсатты түрде қалыптастырудан қорғау қажеттілігі туындайды. Бұл ретте, сыртқы қауіп-қатер көздері ҚР

заңнамасының юрисдикциясынан тыс болуы мүмкін, бұл құқықтық шаралар жүйесін қолдануды айтарлықтай қиындатады.

Өзекті проблемалардың бірі отандық ақпараттық технологиялардың болмауы болып табылады, бұл жаппай тұтынушыны ақпараттық қауіпсіздік талаптарына сәйкестігін растамайтын импорттық техниканы сатып алуға мәжбүр етеді. Бұл деректер базалары мен банктерінің ақпараттық қауіпсіздігіне, сондай-ақ елдің компьютерлік және телекоммуникациялық техника мен ақпараттық өнімнің шетелдік өндірушілеріне ықтимал тәуелділігіне қатер төндіреді.

Қылмыскерлердің құрбандары-бухгалтерлік құжаттарды өңдеу, төлемдер және басқа да операцияларды жүргізу үшін автоматтандырылған ақпараттық жүйелерді пайдаланатын мекемелер, кәсіпорындар мен ұйымдар. Көбінесе киберқылмыскерлердің нысаны банктер немесе сол банктер мен қаржы ұйымдарындағы жеке тұлғалардың шоттары болады [27, 35 б.].

Бірақ, мүмкін, бүкіләлемдік желідегі ақпараттық қоқыс ағынына ең осал балалар. Не покажется емес, тамаша, егер ескеру полвина балалар шығады Интернет жоқ кез келген бақылау, ата-аналар тарапынан немесе педагог. Сонымен қатар, олардың көпшілігі соншалықты сенімді, олар Интернеттегі "виртуалды досқа" жеке мәліметтерін және жақын және таныстарының мәліметтерін (ата-аналардың несие карталарының pin-кодтарына дейін) беруге дайын.

Кейде компьютерлік қылмыстың құрбандары (олардан, жеке кәсіпкерлерден) өздерінің немқұрайлылығы мен компанияның немесе ұйымның сенімсіз жұмысы туралы пікірдің таралуынан қорқып, құқық қорғау органдарымен байланысқа барғысы келмейді, бұл да қылмысқа қарсы тұруда айтарлықтай проблемалар туғызады.

Киберқылмыскердің негізгі мақсаты-әртүрлі процестерді басқаратын компьютерлік жүйе және оларда таратылатын ақпарат. Нақты әлемде әрекет ететін қарапайым қылмыскерден айырмашылығы, киберқылмыскер пышақ немесе атыс қаруы сияқты дәстүрлі қаруды қолданбайды. Оның арсеналы-ақпараттық қару, желіге кіру, бағдарламалық жасақтаманы бұзу және өзгерту, рұқсатсыз ақпарат алу немесе компьютерлік жүйелердің жұмысын бұғаттау үшін қолданылатын барлық құралдар. Киберқылмыскердің қаруына қосуға болады: компьютерлік вирустар, бағдарламалық бетбелгілер, компьютерлік жүйеге рұқсатсыз кіруді неғұрлым тиімді және тиімді ететін шабуылдардың әртүрлі түрлері. Қазіргі заманғы компьютерлік қылмыскерлердің арсеналында дәстүрлі құралдар ғана емес, сонымен қатар ең заманауи ақпараттық қару мен жабдықтар бар. Осы себепті адамның ақпараттық қылмысқа қатыстылығын дәлелдеу оңай емес.

Қазақстандағы ақпараттық қауіпсіздіктің қазіргі жай-күйі оның деңгейі қазіргі уақытта адамның, қоғам мен мемлекеттің қажеттіліктеріне сәйкес келмейтінін көрсетеді. Елдің саяси және әлеуметтік-экономикалық дамуының қазіргі жағдайлары қоғамның еркін ақпарат алмасуды кеңейту қажеттіліктері мен оның таралуына жеке шектеулерді сақтау қажеттілігі арасындағы

қайшылықтардың шиеленісуін тудырады.

Компьютерлік қылмыстармен күресудің арнайы әдістері криминалистер де, заңгерлер де, практиктер де, IT мамандары да ерекшеленбейді, бүкіл әлемдегі әдістер мен құралдар қолданылады. Әлемдік практикада жиынтығында техникалық, ұйымдастырушылық және құқықтық әдістер қолданылады. Техникалық әдістерге компьютерлік желіге заңсыз енуді анықтау үшін арнайы жабдық қолданылатын барлық әдістер кіреді. Ұйымдық-киберқылмыстарды ашудың тиімділігін арттыруға бағытталған іс-шаралар, оның ішінде еркін айналымда тыйым салынған өнімдер мен ақпаратты анықтауға бағытталған, экстремизмді, терроризмді, қатыгездік пен зорлық-зомбылыққа бас ұруды және балалар порнографиясын насихаттайтын бірлескен жедел-алдын алу іс-шаралары. Құқықтық әдістерге компьютерлік қылмыстар үшін жауапкершілікті белгілейтін нормаларды әзірлеу және жетілдіру, бағдарламашылардың авторлық құқықтарын қорғау, осы саладағы халықаралық шарттарды қабылдау жатады.

Компьютерлік қылмыстарды ашумен байланысты барлық проблемалар мемлекеттердің шекарасынан өтіп, халықаралық маңызға ие болды. Қазіргі уақытта бұрынғы ТМД және алыс шет елдермен Ақпарат және тәжірибе алмасу жүзеге асырылуда [28].

Осындай қылмыстармен жүйелі күрес үшін 2006 жылы ақпараттық технологиялар саласындағы қылмыстармен күрес бойынша ұлттық байланыс пункті құрылды, жаңа технологиялармен байланысты қылмыстар үшін қылмыстық жауапкершілікті жетілдіру мәселелері бойынша ҚР заңнамасына қажетті өзгерістер енгізілді. Сондай-ақ банк құрылымдарының өкілдерімен кездесулер өткізілді, онда электрондық алаяқтық фактілерін анықтау бойынша ынтымақтастық туралы келісулер мен уағдаластықтарға қол жеткізілді. Ақпараттық технологиялар саласындағы қылмыстар, жоғарыда айтылғандай, көбінесе халықаралық болып табылады, яғни қылмыскерлер бір мемлекетте әрекет етеді, ал олардың құрбандары басқа мемлекетте болады. Сондықтан мұндай қылмыстармен күресу үшін халықаралық ынтымақтастықтың маңызы ерекше.

Компьютерлік ақпарат саласындағы қылмыс туралы Еуропа Кеңесінің конвенциясына (ETSN 185) 2001 жылы 23 қарашада Будапештте қол қойылды. Ол Еуропа Кеңесіне мүше мемлекеттердің де, оны әзірлеуге қатысқан мүше емес мемлекеттердің де қол қоюы үшін ашық. Атап айтқанда, оған Ресей, АҚШ және Жапония қол қойды.Еуропа Кеңесінің киберқылмыс туралы конвенциясы осы саладағы қылмыстарды келесі топтарға бөледі.

Компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қолжетімділігіне қарсы бағытталған қылмыстар: заңсыз қол жеткізу (2-бап), заңсыз ұстап алу (3-бап), компьютерлік деректерге әсер ету (компьютерлік деректерді құқыққа қарсы әдейі бүлдіру, алып тастау, сапасының нашарлауы, өзгерту немесе бұғаттау) немесе жүйелер (4-бап, 5-бап). Сондай-ақ қылмыстардың бұл тобына арнайы техникалық құрылғыларды (қылмыс жасау үшін әзірленген немесе бейімделген компьютерлік бағдарламаларды,

компьютерлік парольдерді, қол жеткізу кодтарын, олардың аналогтарын, олар арқылы компьютерлік жүйеге тұтастай немесе оның кез келген бөлігіне қол жеткізуге болатын компьютерлік бағдарламаларды) заңсыз пайдалану кіреді (6-бап).

Компьютерлік құралдарды пайдалануға байланысты қылмыстар. Оларға компьютерлік технологияны қолдану арқылы жалған және алаяқтық жатады (6, 7 және 8-баптар). Компьютерлік технологияларды пайдалана отырып жасалған жалғандық, деректердің түпнұсқалылығын бұзуға әкеп соғатын, компьютерлік деректерді оларды түпнұсқалылық ретінде заңды мақсаттарда қарау немесе пайдалану ниетімен зиянды құқыққа қарсы енгізуді, Өзгертуді, жоюды немесе бұғаттауды қамтиды.

Балалар порнографиясын өндіру, ұсыну немесе пайдалануға беру, тарату және сатып алу, сондай-ақ компьютер жадында орналасқан балалар порнографиясын иелену (9-бап).

Авторлық құқықты және сабақтас құқықтарды бұзумен байланысты қылмыстар [29].

Конвенцияға сәйкес әрбір қатысушы мемлекет киберқылмыспен күрес жөніндегі құзыретті органдарға мынадай міндеттер құқығын беру үшін қажетті құқықтық жағдайлар жасауға міндетті: компьютерлік жүйені, оның бір бөлігін немесе жеткізгіштерін алу; компьютерлік деректердің көшірмелерін жасау және тәркілеу; іске қатысты сақталатын компьютерлік деректердің тұтастығы мен сақталуын қамтамасыз ету; компьютерлік жүйедегі компьютерлік деректерді жою немесе бұғаттау.

Конвенция сондай-ақ Интернет-провайдерлерді қолда бар техникалық құралдардың көмегімен қажетті ақпаратты жинауды және тіркеуді немесе ұстап алуды жүргізуге міндеттеуге, сондай-ақ осыған құқық қорғау органдарына жәрдемдесуге қажетті құқықтық жағдайлар жасауды талап етеді. Бұл ретте провайдерлерді осындай ынтымақтастық фактілері туралы толық құпиялылықты сақтауға міндеттеу ұсынылады.

2002 жылдың басында қылмыстар тізбесіне нәсілдік, ұлттық, діни немесе этникалық тегіне негізделген жеке адамды немесе адамдар тобын зорлық-зомбылыққа, жеккөрушілікке немесе кемсітушілікке итермелейтін нәсілшіл және басқа сипаттағы ақпарат таратуды қосатын киберқылмыс туралы конвенцияға №1 Хаттама қабылданды.

Соңғы жылдары әлемнің көптеген елдерінде ақпараттық қылмыс фактісін болдырмау үшін компьютерлік қауіпсіздік мамандары Хакер деп аталатын Профильді құрайтын психологтармен, яғни компьютерлік ақпарат пен технология саласындағы қылмыскермен ынтымақтастық орнатты, бұл оның біліктілігі мен техникалық дайындық деңгейін анықтауға мүмкіндік береді. Бірақ айта кету керек, компьютер мамандары хакер туралы және оның жұмыс әдістері туралы көп нәрсе айта алады, бірақ олар ешқашан оның қылмыстық ойлау психологиясын түсіне алмайды. Мұндай мәселелермен клиникалық психологтар, сот сарапшылары және басқа да мамандар ішкі істер органдарымен бірлесіп айналысады. Мұндай тәжірибе киберқылмыс кеңінен

дамып келе жатқан АҚШ, Еуропа және басқа елдерде белсенді қолданылады. Кейбір ғалымдардың пікірінше, ақпараттық технологиялар саласындағы қылмыстар әлі дамымаған біздің елімізде мұндай тәжірибені құру киберқылмыс негіздерін қарапайым түрде жоюға мүмкіндік береді. Ол үшін халықаралық ынтымақтастық қажеттілігін жандандыру қажет. Бірақ қазіргі жағдайда киберқылмыспен күрес құралдарының едәуір бөлігі, сондай-ақ халықаралық сипаттағы басқа да қылмыстар әр жеке мемлекеттің ішкі құзыретіне жататындығына байланысты, компьютерлік қылмыстармен күресуге бағытталған ұлттық заңнаманы халықаралық құқық нормаларымен үйлестіре отырып және қолданыстағы оң тәжірибеге сүйене отырып дамыту қажет.

Мемлекеттік органдарды толық, дұрыс және уақтылы ақпаратпен қамтамасыз ету үшін негізделген шешімдер қабылдау, оның ішінде мемлекеттік ақпараттық ресурстарды қорғау үшін, сондай-ақ отандық ақпаратты қорғау құралдарын және импортталатын техникалық құралдардың белгіленген талаптарға сәйкестігін растау жүйесін әзірлеу, сондай-ақ техникалық барлауға қарсы іс-қимыл, ақпараттық қарудан қорғау және осы саладағы нормативтік құқықтық базаны жетілдіру мәселелерін одан әрі пысықтау талап етіледі. Ақпараттың тұтастығы мен құпиялылығын қамтамасыз ету үшін жалпы мемлекеттік ауқымда және ведомстволық деңгейде ақпаратты қорғау жөніндегі шараларды кешенді үйлестіру қажет.

Жаңа ақпараттық технологиялар заң бұзушылардың қылмыс жасау құралы, құралы ғана емес, сонымен бірге әртүрлі қауіп-қатерлерге, оның ішінде оның барлық көріністерінде қылмысқа қарсы күресте тиімді шабуыл құралы болуы керек, сондықтан мемлекеттік құрылымдарға компьютерлік қылмысқа қарсы күресте жоғары білікті мамандарды тарту қажет.

Жаһандық киберқауіпсіздік индексінде (Global Cybersecurity Index) Қазақстан өз позициясын қарқынды түрде жақсартуда. Осылайша, соңғы есепте Қазақстан бірден 42 пунктке - 40-орынға көтерілді. Өткен жылғы рейтингте ел 82-ші орынды иеленді.

Айта кетейік, ТМД елдері арасында Қазақстан Ресейден кейінгі екінші орында тұр (26 орын). Рейтингтегі көрші орындар ел Ирландия (38 орын), Израиль (39 орын), Индонезия (41 орын), Португалия (42 орын) және Монакомен (43 орын) бөліседі. Индекс көшбасшылары Ұлыбритания (бірінші орын), АҚШ (екінші орын) және Франция (үшінші орын) болды. Төртінші орында Латвия, бесінші орында Эстония. Бұл шолуда Өзбекстан – 52 орын, Украина – 54 орын, Беларусь – 69 орын, Тәжікстан – 107 орын, Қырғызстан-111 орын алды.

Сарапшылар елдің құқықтық саладағы жетістіктерін атап өтеді. Атап айтқанда, Қазақстан ақпараттық-коммуникациялық технологиялар мен ақпараттық қауіпсіздік саласындағы талаптарды біріздендіргені туралы айтылады. Цифрландыру бастамасы тиімді киберқауіпсіздік стратегиясына көбірек мән береді. Өткен екі жыл ішінде елімізде киберқауіпсіздік саласын дамытудың негізгі тұжырымдамалық тәсілдері әзірленді. "Қазақстан киберқалқаны" киберқауіпсіздік тұжырымдамасы, сондай-ақ бірқатар

заңнамалық актілер мен салалық бұйрықтардың үлкен саны әзірленіп, бекітілді. Бұдан басқа, зиянды кодты зерттеу бойынша сынақ зертханалары құрылды, ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы іске қосылды, осы мамандық бойынша гранттар саны артты және т. б.

"Қазақстан киберқалқаны" бағдарламасы аясында мемлекет киберқауіпсіздік үшін аса маңызды 336 нысанды анықтады, оларға мемлекеттік құрылымдар, банктер және шабуылдары елдік немесе мемлекетаралық әсер етуі мүмкін өнеркәсіптік кәсіпорындар жатады. Қыркүйек айында бұл тізімге 219 нысан кірді. Тізімді толықтыру жалғасуда",-деді цифрлық даму, инновациялар және аэроғарыш өнеркәсібі вице-министрі Асхат Оразбек Нұр-Сұлтандағы киберқауіпсіздік жөніндегі американдық сауда палатасының форумында сөйлеген сөзінде.

Ол "Қазақстан киберқалқаны" киберқауіпсіздік бағдарламасын белсенді іске асыру 2018 жылы басталғанын және 2022 жылға дейін есептелгенін еске салды. Қазақстанда киберқылмыспен күрес үшін арнайы қорғау жүйесін құру қажеттілігі туралы Қазақстанның Тұңғыш Президенті Нұрсұлтан Назарбаев 2017 жылғы қаңтардағы өзінің жыл сайынғы халыққа Жолдауында мәлімдеді. Сол кезде ол үкіметке және ҰҚК-ге "Қазақстанның киберқалқаны"жүйесін құру бойынша шаралар қабылдауды тапсырды.

Вице-министр қазіргі уақытта "кибер қалқан" жобасының екінші кезеңі жүзеге асырылып жатқанын еске салды, ол барлық қорғаныс инфрақұрылымын іске қосуды көздейді. Бірінші кезең нормативтік-құқықтық базаны дайындау және жабдықтарды сатып алу болды.

Киберқауіпсіздік бойынша халықаралық сарапшылар 2019 жылы әлемде кибершабуылдар әр 14 секунд сайын болады деп есептеді. Кибершабуылдардың көбеюіне байланысты олардың келтірген залалы да артып келеді: егер өткен жылы экономиканың әртүрлі секторларындағы компаниялардың шығындары 1,5 трлн долларды құраса, 2019 жылы сарапшылардың болжамы бойынша олар 2,5 трлн долларға жетті. 2022 жылға қарай Дүниежүзілік экономикалық форумның болжамы бойынша кибершабуылдардан болатын планетарлық залал сомасы 8 трлн долларға дейін өсуі мүмкін.

Айтпақшы, кибершабуылдарға кез — келген адам ұшырауы мүмкін-ірі компаниялар да, қарапайым пайдаланушылар да. Көптеген адамдар өздерінің теледидарлары мен басқа да тұрмыстық техникалары хакерлерді қызықтырмайды деп ойлайды. Алайда, бұл құрылғылар арқылы әртүрлі мақсаттарда қолдануға болатын жеке деректерге қол жеткізуге болатынына назар аударатындар аз.

Securing Sam қорғаныс бағдарламалық жасақтамасын жасаушының айтуынша, әр еуропалық үйде интернетке қосылған 14 құрылғы бар, ал АҚШ-та олардың саны 17-ге жетеді. Олардың әрқайсысы бұзылған болуы мүмкін, өйткені оларға қол жеткізе отырып, шабуылдаушылар пайдаланушылардың жеке деректерін ұрлап, оларды бопсалау немесе басқа мақсаттар үшін пайдалана алады. Securing Sam зерттеуі бойынша, ең ауыр шабуылдар IP

камераларына (CCTV камералары) бағытталған, олар үй желілерінде орнатылған осал құрылғылардың 47% құрайды. Ең әлсіз қорғанысы бар құрылғылар арасында екінші орынды сақтау құрылғылары алады. Сондай-ақ, Үздік 5-ке принтерлер, iP телефондары және теледидарлар кірді[30].

Жалпы, киберқылмыстың жедел өсуінің себептерінің бірі, мамандардың пікірінше, технологиялық трендтер болып табылады. 2022 жылға қарай интернетке бір трлн құрылғы қосылатын болады. 2023 жылға қарай адамдардың 80% - ында сандық әлемде аватар пайда болады. Бұл ретте үй шаруашылықтарының интернет-трафигінің 50% - дан астамы 2024 жылы "ақылды" құрылғылар мен тұрмыстық техниканы тұтынатын болады".

Егер еліміздегі кибершабуылдар туралы айтатын болсақ, ҚР цифрлық даму, инновациялар және аэроғарыш өнеркәсібі вице-министрі Асхат Оразбектің айтуынша, Қазақстанның ақпараттық қауіпсіздігі жөніндегі ұлттық үйлестіру орталығы 2018 жылдан бастап отандық инфрақұрылымға 2 млрд астам кибершабуыл көрсеткен.

2018-2019 жылдары ақпараттық қауіпсіздік бойынша ұлттық үйлестіру орталығымен 2,2 млрд кибершабуыл көрсетілді. Бұл тек мүмкін болатын шабуылдардың барлық түрлері (мемлекеттік органдардың, жеке ұйымдардың инфрақұрылымына және т. б.).

Сонымен қатар, Citibank Қазақстан Бас директоры Андрей Курилин секунд сайын ірі халықаралық банктерге кибершабуылдар жүріп жатқанын айтты.

Әлемдегі ең ірі банктердің бірі – Citi. Бізге әлемдегі барлық есептеулердің кем дегенде 11% - ы келеді және ақшалай алғанда бұл күніне кемінде төрт триллион (доллар), яғни бұл жылына квадриллионнан көп. Әрине, бұл үлкен мақсат. Шабуылдар әр секунд сайын жүреді және күрес қиындайды, өйткені қателікке тәбет нөлге тең. Кез-келген кибершабуыл бүкіл шығындар тізбегімен, беделді тәуекелдермен аяқталуы мүмкін, бұған қатысы бар адамдар үшін мансаптық салдар туралы айтпағанда.

"Кибершабуылдар мен киберқылмыскерлерді 100 жыл бұрын банк қарақшыларымен салыстыруға болады. Алғашқы Фильмдер тонау туралы түсірілген. Банктерді тонау тақырыбында көптеген батыстықтар түсірілді. Бұрын банкті тонау үшін тапаншасы бар адамдар қажет болатын. Олар материалдық мекемеге келді – енді бұл (тонау) үшін тапаншалар қажет емес, материалдық ештеңе қажет емес, кейде адамдар да қажет емес, өйткені мұның бәрі жасанды интеллект көмегімен жасалуы мүмкін. Қазіргі әлемде кибершабуылдар банк ғимаратынан қолма-қол ақша шығарумен салыстырғанда әлдеқайда үлкен проблемаларға алып келеді. Бір жылдан кейін бүкіл әлем кибершабуылдардан алты трлн доллар жоғалтады[31].

Baker McKenzie заң компаниясының серіктесі Андрей Ерш Қазақстанның бірқатар компанияларындағы лицензияланбаған бағдарламалық қамтамасыз ету мәселесі туралы айтады[31].

Біздің Ұлттық компанияларымыздың көпшілігі кіретін және "Самұрық-Қазына" ережесі бойынша сатып алуды жүзеге асыратын "Самұрық-

Қазына"сатып алу ережесін алайық. Тендерлерді лицензияланбаған бағдарламалық жасақтаманы сататын компаниялардың қатысуынан қорғауға мүмкіндік беретін нормалар бар ма? Жоқ. "ҚазМұнайГаз" сатып алу ережесі де "Самұрық-Қазына" ережесіне негізделген-жоқ. Бұл практикадағы ерекшелік дәрілік препараттарды сатып алу ережелері болып табылады. Олар 2019 жылы денсаулық сақтау министрлігімен ұзақ талқылаудан кейін зияткерлік меншік құқығына ие емес тұлғаларды тендерге қатысуға шектейтін нормалар пайда болды. Бірақ зияткерлік меншік объектілеріне қатысты басқа да мәселелер бар[31].

Андрей Ерш "даркнетте" ай сайын төлем карталарын пайдаланушылардың 686 мың деректері жарияланатынын айтады.

Бұл кейбір конференцияларда айтылған орташа бағалар. Неліктен бұл орын алады? Ең алдымен, негізгі себептердің бірі – бағдарламалық жасақтаманың осалдығы. Лицензиялық БҚ ақпараттық технологиялардың жеткілікті қорғалуын қамтамасыз етеді және технологиялардың қауіпсіздігіне байланысты проблемаларды жеткілікті түрде тез арада тоқтатуға мүмкіндік береді. Алайда, адамдар лицензияланбаған бағдарламалық жасақтаманы қолданудың тұрақты тенденциясы байқалады. Әлеуметтік тұрғыдан алғанда, азаматтар қандай да бір жолмен түсінуге тырысуы мүмкін, өйткені барлық кірістер бұған мүмкіндік бермейді, бірақ, әрине, бұл үшін ешқандай себеп жоқ, өйткені бұл әлі де зияткерлік меншік құқықтарын бұзу болып табылады. Бірақ бұл коммерциялық ұйымдарға қатысты өте күлкілі көрінеді. Лицензияланған бағдарламалық жасақтаманы пайдалану коммерциялық ұйымдардың қауіпсіздігі үшін өте маңызды. Лицензияланбаған" жарылған "бағдарламаларды қолдануға болмайды, олар іс жүзінде кәсіпорынның ішкі ақпараттық жүйелеріне кез келген қаскүнем үшін қақпа болып табылады[31].

Сонымен қатар, ол жабдықтың өзінде осалдық қаупі бар деп санайды.

"Өкінішке орай, бұған мүмкіндік беретін техникалық шешім жоқ. Бұл ең осал бөліктердің бірі. Әдеттегі мәселе – Wi-Fi маршрутизаторлары оларға орнатылған және сол "даркнетте"толығымен еркін алуға болатын зауыттық құпия сөздерді өзгертпестен қолданылған кезде. Көптеген өндірушілер типтік парольдерді орнатады. Тағы бір мәселе – "фишинг", қандай да бір күдікті файлдарды жүктеу және басқа әрекеттерді жасау арқылы алаяқтар пайдаланушылардың дербес деректеріне, оның ішінде төлем карталары мен банктік шоттарға қол жеткізе алады. Бұл тек жеке тұлғалардың өздеріне ғана емес, сонымен бірге олар жұмыс істейтін ұйымдарға, компанияларға, банктерге де әсер етеді", - дейді Ерш.

Маман сондай – ақ, 2019 жылдың қыркүйегінде Алматыда өткен бағдарламалық қамтамасыз ету жөніндегі жұмыс тобының соңғы отырысында Қазақстандағы компьютерлерде орнатылған бағдарламалық қамтамасыз етудің шамамен 74% - ы лицензиясыз болып табылатындығы айтылды.

Біз орналасуды бере алмаймыз қайда көп, қайда аз, бірақ, әрине, жеке компьютерлер мен телефондарда лицензияланбаған бағдарламалық жасақтама орнатылды, бірақ тәжірибе көрсеткендей, коммерциялық кәсіпорындардың

лицензияланбаған жабдықты сатып алу фактілері әлі де анықталуда. Ең алдымен, мұнай, газ, майнинг және т.б. өндіріс инфрақұрылымына кіретін коммерциялық кәсіпорындар туралы сөз болып отыр.

Сонымен қатар, "Кселл" АҚ Бас атқарушы директоры Каспарс Кукелис компаниялар мен банктер, оның пікірінше, қауіпсіздікті қамтамасыз ету үшін үлкен инвестициялар салуды жалғастыра алады, бірақ пайдаланушылардың мінез-құлық әдеттерімен тікелей байланысты орындар жаңа осалдықтарды тудырады[31].

Киберқауіпсіздік мәселелері білім беру саласымен тығыз байланысты, өйткені егер сіз 12345 паролін немесе Атыңызды және басқа заттарды орнатсаңыз, ешқандай Мемлекеттік, тергеу және басқа органдар сізге көмектесе алмайды. Бұзушылықтар мен енулердің үлкен саны пайдаланушылардың жағымсыз мінез-құлқымен немесе бұл деректерді жүйелік әкімшіден немесе басқа "фишинг"әдісімен ашуға дайын болуымен байланысты. Егер білім беру жүйесі бұл қауіпті ескерсе және Оқу уақытының бір бөлігін каллиграфияға, қолмен жазылған дәптерге арнаса, бұл ұрпақ ешқашан өмірде пайдалы болмайды, суретші немесе басқа адам болатын адамдардың аз санынан басқа, бірақ киберқауіпсіздік аспектілеріне арнайтын[31].

Оның айтуынша, ұялы байланыс компаниялары, банктер сияқты, аптасына жеті күн және тәулігіне 24 сағат ақпараттық қауіпсіздік мәселелеріне тап болады.

Біздің ойымша, төлемдер, пайдаланушылардың авторизациясы және адамдар өз құрылғыларынан жасайтын кез – келген басқа әрекеттерге байланысты сандық транзакциялық оқиғалардың үштен бірі біз арқылы өтеді.

Mastercard кибер және зияткерлік шешімдер жөніндегі директоры Игорь Волков пайдаланушыларды аутентификациялау процесінде белсенді жұмыс істеу керек деп санайды, өйткені бұл өте маңызды.

"Мұнда заманауи нюанстар бар, өйткені статикалық парольдер немесе оларды өзгерту керек, олар артта қалады. Есте сақтау қиын және қиын. Біз әртүрлі биометриялық үлгілерге сүйенеміз. Жеке пайдаланушылардың карталарымен алаяқтық әрекеттер және қаржы институттарының жүйелеріне шабуылдар, тікелей қаржылық шығындардан басқа, жанама шығындарға ие, атап айтқанда беделге. Өкінішке орай, қандай-да бір шабуылға ұшыраған және көпшілікке танымал болған банкті қарастырайық, содан кейін тікелей қаржылық шығындардан басқа, ол әлі де беделге ие. Тікелей карта ұстаушылар осы банкпен ынтымақтастықты жалғастырғысы келмеуі мүмкін, сондықтан клиенттік базаның бір ойыншыдан екінші ойыншыға ауысуының нюанстары болуы мүмкін", – дейді Волков[31].

Оның айтуынша, соңғы уақытта алаяқтар мен хакерлердің технологиялық жарақтандырылуы мен біліктілігінің деңгейі айтарлықтай өсті, бұл төлем жүйелері мен қаржы институттарының сенімділігіне қиындық туғызады, сондықтан олар дамуға мәжбүр.

"Іс жүзінде төлем қалай жүреді? 1960 жылдары төлем қарапайым магниттік картадан басталды, қазір бұл толық атавизм, өйткені алаяқтар оны

оңай ұстап алады, яғни сізге деректерді оқитын қарапайым құрылғы қажет және сіз оны үйде басқа картаға қайта жаза аласыз. Сондықтан технологиялар үнемі дамып келеді", - дейді ол ApplePay-дің дамуын мысал ретінде келтіре отырып.

Сонымен қатар, қазір пайдаланушылар көбінесе төлем картасын алып емес, тек смартфонды немесе смарт-сағатты алып, үйден шыға алады. Жеке құрылғылардың дамуы қызметтерді дамытуға үлкен мүмкіндіктер берді, бірақ сонымен бірге айтарлықтай тәуекелдер әкелді.

"Егер сіз статистиканы қарасаңыз, онда киберқылмыстардың дамуына ең күшті серпін 2010-2011 жылдар аралығында болады. Мұны екі фактормен түсіндіру оңай: біріншісі – смартфондардың дамуы, көптеген адамдар ұялы телефондары арқылы қашықтықтан арналарды қолдана бастайды, екіншісі – банктік қашықтықтан қызметтерді дамыту, бұл бір жағынан артықшылық береді, ал екінші жағынан алаяқтарға түрлі шабуылдар жасауға мүмкіндік береді", – деп түйіндейді Волков.

Қорытындылай келе, киберқылмыс пен киберқауіпсіздік - бұл біртұтас ғаламдық виртуалды кеңістіктің екі амбиваленттілігі. Осыдан он жыл бұрын Ақпараттық қауіпсіздік мәселесін негізінен ақпараттық технологиялар саласындағы мамандардың тар тобы түсінді. Нақты инженерлік-техникалық және физика-математикалық мамандықтармен бірге киберсоциология сияқты әлеуметтік ғылымдар тиімді шешімдерді іздеуге қосылды. Ақпараттық қауіпсіздіктің жаңа парадигмасы – киберқауіпсіздік парадигмасы пайда болды. Оның институционализациясының барлық белгілері бар: кибер алаяқтармен күресте құқықтық нормалар қалыптасады, Киберқауіпсіздік бойынша халықаралық институттар пайда болады, киберқылмыскерлерге қарсы іс-қимылға бағытталған жаңа қызмет салалары дамуда және т. б.

2019 жылдың қазан айында Оңтүстік Кореяда camp (cybersecurity Alliance for Mutual Progress, өзара прогреске арналған киберқауіпсіздік Альянсы) 4-ші жыл сайынғы конференциясы өтті. Конференцияда ұйымдастырушылар Қазақстан альянстың ұйымдастыру комитетінің құрамына кіргенін ресми түрде жариялады. Осылайша, ұйымдастыру комитетінің құрамына он әріптес ел, оның ішінде Қазақстан да кірді.

Оңтүстік Кореяда жұмыс істейтін өзара прогреске арналған киберқауіпсіздік Альянсының құрамына 45 елден 59 ұйым кіреді. Бұдан басқа, CAMP-ға мүше ұйымдар Альянсты барынша күрделене түсетін және бүкіл әлем бойынша пайдаланушылар мен ұйымдарды көбірек қозғайтын киберқауіптердің алдын алу үшін жаһандық ұйымға айналдыру мақсатында киберқауіпсіздік мәселелері бойынша оқу бағдарламаларымен және ақпаратпен алмасу мүмкіндігіне ие.

Киберкеңістік пен киберқылмыстың пайда болу тарихын талдай отырып, бұл құбылыстар ақпараттық технологиялардың дамуымен тікелей байланысты деп толық сеніммен қорытынды жасауға болады. Жаңа технологиялардың пайда болуымен қылмыстың жаңа, неғұрлым күрделі түрінің пайда болуы байқалады. Бұл қылмыскерлер ғылыми-техникалық прогрестің нәтижелерін өз мақсаттары үшін тез пайдаланатынын көрсетеді. Бұл тенденция киберкеңістікте

қалыптасқан барлық қоғамдық қатынастарға елеулі қауіп төндіреді, өйткені дамудың осы кезеңінде киберкеңістік пен қоғам бөлінбейді.

Алайда, киберкеңістік дегеніміз не? Бұл сұрақты көптеген ғалымдар мен философтар қойды. Сонымен, С.Н. Хуторная өзінің диссертациялық зерттеуінде киберкеңістік-бұл гипермәтін мен гиперреалдылықтың, интерактивтіліктің, кеңістік-уақыт белгілерінің модификациясының, кеңістік-уақыт ағындарының көп бағытты және олардың көп өлшемді және дискреттілігімен сипатталатын компьютерлік-технологиялық виртуалды шындық екенін көрсетеді[32, 7 б.].

Р.И. Вылковтың пікірінше, киберкеңістік-бұл адамдардың ақыл-ой қызметін жеңілдететін және едәуір тездететін маңызды шындық пен заманауи технологияны біріктіретін проективтік мәдени кеңістіктің түбегейлі жаңа түрі[33, 128 б.].

Р.А.Барышев киберкеңістік виртуалды шындықтың көптеген формаларының бірі екенін, ал егер виртуалды шындық кино мен музыкалық шығармадан бастап айна бейнесіне, армандар мен қиялдарға дейінгі құбылыстардың үлкен шеңберін білдірсе, онда киберкеңістік өз кезегінде виртуалды шындықты адам мен компьютердің өзара әрекеттесу шекараларымен нақты анықтайды ... - бұл компьютерлік желіде кең таралған нысандарды сипаттау үшін қолданылатын метафизикалық абстракция[34, 56 б.].

Осы авторлардың жұмысын талдағаннан кейін біз бір жалпы белгіні бөліп көрсете аламыз: олардың барлығы киберкеңістікті абстрактілі виртуалды шындықтың бір түрі ретінде ұсынады, оның болуы тек компьютерлік технологиялар аясында мүмкін болады. Яғни, киберкеңістік-бұл компьютерлерді (желіні) біріктіру ғана емес, басқа нәрсе. Сонда сұрақ туындайды: киберкеңістіктің ақпараттық желіден, мысалы, "Интернет"желісінен айырмашылығы неде?

А. Г. Волеводз дұрыс атап өткендей, ақпаратты жеткізетін серверлердің кең жүйесін қамтитын "Интернет" желісі әлемдік ақпараттық кеңістікті құрады[24, 17 б.].

"Интернет" желісі – бұл киберкеңістіктің нақты әлемдегі материалдық көрінісі. "Интернет" бүкіл әлем бойынша (спутник, микротолқынды және электромагниттік сигналдар, Wi-Fi, 3G, LTE арқылы) бір-бірімен сымды және сымсыз біріктірілген жеке компьютерлерден, серверлерден және басқа да техникалық құрылғылардан тұрады, яғни бұл дүниежүзілік ақпараттық-телекоммуникациялық желі.

Киберкеңістік-қолданушылары әкімшілік, азаматтық, қылмыстық және басқа да құқықтық қатынастарға еркін кіре алатын ақпараттық-телекоммуникациялық желімен шектелген жасанды құрылған орта. Киберкеңістік кез келген ақпараттық-телекоммуникациялық желіде пайда болуы мүмкін. Мысалы, "Интернет" желісі аясында "Интернет-кеңістік" туралы айтуға болады. Демек, "Интернет" – бұл "киберкеңістіктің" өзі емес, ол өмір сүре алатын шарт қана.

Дәл осындай көзқарасты АҚШ Жоғарғы соты 1997 жылы Рино американдық азаматтық бостандықтар Одағына қарсы іс қозғады[35].

АҚШ Жоғарғы сотының шешіміне сәйкес, киберкеңістік "географиялық кеңістікте орналаспаған, бірақ "Интернет"желісіне қол жеткізу арқылы әлемнің кез келген нүктесінде барлығына қол жетімді бірегей Орта" деп түсініледі.

"Интернет" АҚШ Жоғарғы Соты "нақты иесі жоқ және жеке және заңды тұлғалардың интерактивті байланысы үшін қызмет ететін компьютерлік желілер мен ақпараттық ресурстардың Ғаламдық бірлестігі" деп анықтайды.

Қазақстанда ресми деңгейде "киберкеңістік" термині алғаш рет Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысымен қабылданған киберқауіпсіздік туралы тұжырымдамада 2017 жылы ғана қолданылды [7].

Онда ақпараттық кеңістіктің киберкеңістікке, жалпы жеке кеңістікке қатынасы көрсетілген. Ақпараттық-Телекоммуникациялық желінің киберкеңістіктің материалдық құрамдас бөлігі ретіндегі айырмашылығы және киберкеңістіктің өзі ерекше орта немесе адам қызметінің саласы ретінде, сондай-ақ "Интернет" желісі қолданыстағы ақпараттық-телекоммуникациялық желілердің бірі емес екендігі ерекше атап өтілді. Сондықтан бұл жұмыста дәл осы анықтама қолданылады.

Жоғарыда айтылғандарға сүйене отырып, келесі қорытынды жасауға болады:

1. "киберкеңістік" ұғымы "Интернет-кеңістік" ұғымына қарағанда кең және оны қамтиды;
2. киберкеңістік - бұл "Интернет" желісінің коммуникациялық арналарының және басқа да телекоммуникациялық желілердің, олардың жұмыс істеуін қамтамасыз ететін технологиялық инфрақұрылымның және оларды пайдалану арқылы жүзеге асырылатын адам белсенділігінің (жеке тұлға, ұйым, мемлекет) кез келген нысандарының жиынтығымен құрылған ақпараттық кеңістіктегі қызмет саласы;
3. "Интернет" желісі - бұл киберкеңістіктің нақты әлемдегі материалдық көрінісі: бұл "киберкеңістіктің" өзі емес, ол өмір сүре алатын шарт қана;
4. жаңа технологиялардың (киберкеңістіктің) пайда болуымен қылмыстың жаңа, неғұрлым күрделі түрінің (киберқылмыстың) пайда болуы байқалады. Бұл қылмыскерлер ғылыми-техникалық прогрестің нәтижелерін өз мақсаттары үшін тез пайдаланатынын көрсетеді. Бұл тенденция киберкеңістікте қалыптасқан барлық қоғамдық қатынастарға елеулі қауіп төндіреді, өйткені дамудың осы кезеңінде киберкеңістік пен қоғам бөлінбейді.

1.3 Киберкеңістікте жасалатын қылмыстарға қарсы іс-қимыл саласындағы халықаралық тәжірибе

Көптеген елдердің қылмыстық заңнамасында компьютерлік алаяқтық қылмыстың дербес құрамы ретінде ерекшеленеді, әдетте, ұрлық туралы жалпы

нормалармен салыстырғанда қатаң санкциялар қарастырылған. Атап айтқанда, Германияның қылмыстық кодексінің 263 а параграфы қылмыс ретінде арнайы бағдарламалар арқылы деректерді өңдеу нәтижесіне әсер ету, дұрыс емес немесе толық емес деректерді пайдалану, деректерді заңсыз пайдалану немесе деректерді өңдеу нәтижесіне басқа да әсер ету арқылы мүліктік зиян келтіруді анықтайды[36, 203 б.].

Швецияның Қылмыстық кодексінде қылмыстың білікті құрамының белгісі ретінде қылмыстың жасалу әдісі көрсетілген:"алаяқтық үшін жалған немесе толық емес ақпаратты қолдана отырып, бағдарламаларды өзгерте отырып немесе кез-келген басқа жолмен деректерді автоматты түрде өңдеу процестеріне, басқа автоматты процестерге заңсыз араласқан адам жауапқа тартылуы керек.процестер, меншік иесінің мүлкіне зиян келтіріп, өзі үшін пайда әкеледі" [37, 172 б.].

148а-бапта арнайы бағдарламалар арқылы деректерді автоматтандырылған өңдеу процестеріне әсер ету, деректерді енгізу, өзгерту немесе жою арқылы немесе деректерді өңдеу процесіне әсер ететін басқа жолмен қылмыскер немесе үшінші тұлға үшін заңсыз пайда алу мақсатында келтірілген материалдық зиян үшін жауапкершілік қарастырылған[38, 132 б.].

Әрине, объективті түрде, бір елде киберкеңістікті заңнамалық реттеу мүмкін емес. Заңнамалық реттеу тек халықаралық құқық шеңберінде ғана қажет. Оның үстіне, жоғары технологиялар саласындағы қылмыспен күресте халықаралық ынтымақтастықты кеңейту үрдісі көптеген халықаралық ұйымдардың қызметінде байқалады. Олардың бірі - Еуропа Кеңесі (SE), оның пікірінше, компьютерлік қылмыстың өсуі мемлекеттердің онымен күресуге бағытталған нормаларды әзірлеуге келісілген көзқарасын талап етеді. Мұны жүзеге асыру 1997 жылы ақпанда ЕК Министрлер комитетінің киберкеңістіктегі қылмыс жөніндегі сарапшылар комитетінің құрылуына әкелді, оған компьютерлік қылмыстарды тергеу кезінде туындайтын құқықтық мәселелерді зерттеу міндеті қойылды. Зерттеу нәтижелері бойынша ол киберқылмыс туралы конвенцияның жобасын жасады. 2001 жылғы 18-22 маусым аралығындағы кезеңде жоба қылмыс проблемалары жөніндегі Еуропалық комитеттің отырысында талқыланды және 2001 жылғы 23 қарашадан бастап конвенцияға ек-ге мүше елдер қол қоя бастады, оны ратификациялады. 2005 жылдың соңына қарай оған Кеңеске мүше 38 мемлекет, сондай-ақ Канада, Жапония, ОАР және АҚШ қол қойды. Конвенция киберқылмыстардың жіктелуін қамтитын алғашқы құжат болды. Қылмыстық интернет-әрекеттердің тізіміне, атап айтқанда, ақпараттық ортаға заңсыз кіру, ақпараттық ресурстарды заңсыз ұстап алу, компьютерлік жүйеге араласу және магниттік тасымалдағыштардағы ақпарат кіреді. Құжат қылмыскер мен жәбірленуші әртүрлі елдерде болған және әртүрлі заңдарға бағынатын жағдайларда жекелеген мемлекеттердің құқық қорғау органдарының өзара әрекеттесу мәселелерін егжей-тегжейлі сипаттайды. Конвенция, сондай-ақ, киберқылмыстарды тергеу кезінде осындай мәліметтер талап етілген жағдайда, клиенттердің жеке ақпаратын сақтаудың барлық Интернет-провайдерлері үшін

ортақ ережелерін қарастырады. Қазір Ұлыбританияда ақпараттық қатынастарды реттеу екі бағытта жүзеге асырылады: компьютерлік қылмыстар үшін қылмыстық жауапкершілікті белгілеу (computer crime) және интернетке байланысты қылмыстар үшін қылмыстық жауапкершілікті белгілеу (Internet - related crime)[39, 111 б.].

Компьютерлік желілерді мемлекеттік бақылаусыз жасауға болмайды. Интернет сияқты ғаламдық компьютерлік желілер, кез-келген өте тиімді технология сияқты, тек жақсылық үшін ғана қолданыла алмайды. Бұл қарама-қайшылықты тек халықаралық құқық аясында жоюға болатыны анық. Осыған байланысты жоғары технологиялар саласындағы қылмыспен күресте халықаралық ынтымақтастықты кеңейту тенденциясы көптеген халықаралық ұйымдардың қызметінде байқалады. Олардың бірі - Еуропа Кеңесі (SE), оның пікірінше, компьютерлік қылмыстың өсуі мемлекеттердің онымен күресуге бағытталған ережелерді әзірлеуге келісілген көзқарасын талап етеді. Бұл мәселеге бірқатар қабылданған ұсыныстар арналған[40], онда тұжырымдаманы анықтауға және "компьютерлік технологияны қолданумен байланысты қылмыстар" шеңберін құруға әрекет жасалды. Алайда, бұл құжаттардың ұсынымдық сипаты практикада туындайтын қайшылықтарды шешуге ықпал етпейді, ол үшін толыққанды халықаралық-құқықтық құжаттар қажет.

Мұны жүзеге асыру 1997 жылы ақпанда ЕК Министрлер комитетінің киберкеңістіктегі қылмыс жөніндегі сарапшылар комитетінің құрылуына әкелді, оған компьютерлік қылмыстарды тергеу кезінде туындайтын құқықтық мәселелерді зерттеу міндеті қойылды. Зерттеу нәтижелері бойынша ол киберқылмыс туралы конвенцияның жобасын жасады.

Құқық қорғау ұйымдарының конвенция жобасына реакциясы әбден күтілді. Құқық қорғау топтарының ЕК-ге жолдаған ашық хатында жоба "белгілі жеке қорғаныс нормаларына қарсы тұру, ұлттық үкіметтердің өкілеттіктерін негізсіз күшейтеді, ақпарат қауіпсіздігін қамтамасыз ету әдістерінің дамуына нұқсан келтіреді, бұл мемлекеттердің заң алдындағы жауапкершілігін азайтады" делінген".

Ашық талқылаудан кейін жоба жеке өмірге қол сұғылмаушылық кепілдіктерін күшейту талаптарын ескере отырып пысықталды және ек атқарушы органдарының талқылауына дайындалды. 2001 жылғы 18-22 маусым аралығындағы кезеңде жоба оған кейбір өзгерістер енгізілген қылмыс проблемалары жөніндегі Еуропалық комитеттің отырысында талқыланды және Конвенция жобасын ЕК Министрлер комитетіне қабылдау және қол қою үшін шығару туралы шешім қабылданды [41].

2001 жылғы 23 қарашада конвенцияға мүше елдер қол қойды, оны ратификациялау басталды.

Киберқылмыс туралы Конвенция - бұл құқықтың әртүрлі салаларына айтарлықтай әсер етуге арналған нормаларды қамтитын кешенді құжат: қылмыстық, қылмыстық іс жүргізу, авторлық, азаматтық, ақпараттық. Ол халықаралық құқықтың негізгі қағидаттарына негізделеді: адам құқықтарын құрметтеу, ынтымақтастық және міндеттемелерді адал орындау.

Конвенция нормалары мәселелердің үш негізгі блогын реттеуге бағытталған:

* компьютерлік ақпарат саласындағы қылмыстарды қылмыстық-құқықтық бағалауды жақындастыру;

* осындай қылмыстарды тергеу кезінде дәлелдемелер жинауды қамтамасыз етуге бағытталған Ұлттық қылмыстық іс жүргізу шараларын жақындастыру;

* шетелде осындай қылмыстардың жасалуының дәлелдерін жинауға бағытталған қылмыстық іс жүргізу қызметіндегі халықаралық ынтымақтастық.

Қылмыстық-құқықтық мәселелер

Конвенция қатысушы елдердің заңнамасына "киберқылмыскерлер" үшін қылмыстық жауапкершілік туралы бірыңғай нормаларды енгізу ұсынылады, олардың тізбесіне (1) компьютерлік ақпаратқа қарсы бағытталған іс-әрекеттер (қылмыстық әрекеттің нысанасы ретінде) және оны қылмыс жасаудың бірегей құралы ретінде пайдаланатын іс - әрекеттер және (2) қол сұғу нысанасы заңмен қорғалатын өзге де игіліктер болып табылатын іс - әрекеттер, ал ақпарат, Компьютерлер және т.б. кіреді.д. олар қылмыстың объективті жағының элементтерінің бірі ғана, мысалы, оны жасау құралы, аяқтау немесе жасыру әдісінің ажырамас бөлігі.

Конвенцияға сәйкес киберқылмыстардың объектісі компьютерлік ақпаратты өндіру, жинау, өңдеу, жинақтау, сақтау, іздеу, беру, тарату және тұтыну бойынша, сондай - ақ компьютерлер, компьютерлік жүйелер мен желілер пайдаланылатын өзге де салаларда ақпараттық процестерді жүзеге асыру кезінде туындайтын қоғамдық қатынастардың құқық нормаларымен қорғалатын кең спектрі болып табылады. Олардың ішінде, жоғары қоғамдық маңыздылығын ескере отырып, компьютерлік деректер мен жүйелердің құпиялылығын, тұтастығын және қол жетімділігін қамтамасыз ету, компьютерлер мен компьютерлік ақпаратты (деректерді), авторлық және сабақтас құқықтарды заңды пайдалану саласында туындайтын құқықтық қатынастар ерекшеленеді.

Киберқылмыстардың объективті жағы әлеуметтік қауіпті әрекеттердің төрт тобының бөлінуімен сипатталады.

Компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қол жетімділігіне қарсы

* Заңсыз қол жеткізу - қылмыс ретінде қарастырылуы мүмкін компьютерлік жүйеге тұтастай немесе оның кез келген бөлігіне қол жеткізу, ЕО-ма қауіпсіздік шараларын айналып өтіп және компьютерлік деректерді немесе өзге де арам ниетті иелену ниетімен, немесе басқа компьютерлік жүйеге қосылған компьютерлік жүйеге қатысты (2-бап).

* Деректерді заңсыз ұстап алу-компьютерлік деректерді компьютерлік жүйеге, одан немесе осындай компьютерлік деректерді тасымалдайтын компьютерлік жүйенің электромагниттік сәулеленуін қоса алғанда, егер ол қауіпсіздік шаралары аясында және компьютерлік деректерді иелену ниетімен немесе басқа компьютерлік жүйемен біріктірілген компьютерлік жүйеге

қатысты техникалық құралдарды пайдалана отырып жүзеге асырылған ұстап алу (3 - бап).

* Деректердің тұтастығын бұзу – компьютерлік деректерді бұған құқықсыз бүлдіру, өшіру, бүлдіру, өзгерту немесе бұғаттау, оның ішінде тек ауыр зардаптарға әкеп соққан жағдайларда ғана (4 - бап).

* Жүйенің жұмыс істеуіне араласу - компьютерлік деректерді енгізу, беру, бүлдіру, жою, бүлдіру, өзгерту немесе бұғаттау жолымен компьютерлік жүйенің жұмыс істеуіне бұған құқықсыз бірқатар кедергілер жасау (5 - бап).

* Құрылғыларды құқыққа қарсы пайдалану - (a) пайдалану үшін өндіру, сату, сатып алу, импорттау, көтерме сату немесе пайдалануға берудің өзге де нысандары: (1) ең алдымен қылмыс жасау мақсаттары үшін әзірленген немесе бейімделген компьютерлік бағдарламаларды қоса алғанда, құрылғылар; (2) компьютерлік парольдерді, қол жеткізу кодтарын немесе олардың көмегімен компьютерлік жүйеге тұтастай немесе оның кез келген бөлігін қылмыс жасау мақсатында пайдалану ниетімен алу мүмкін болатын өзге де осыған ұқсас деректер.; және (b) жоғарыда аталған заттардың біреуін қылмыс жасау мақсатында пайдалану ниетімен иелену (6-бап).

Компьютерлерді пайдалануға байланысты

* Компьютерлерді қолдану арқылы жалғандық - компьютерлік деректерді енгізу, өзгерту, өшіру немесе блоктау, бұл деректерді тікелей оқылатын және түсінікті болғанына қарамастан, оларды заңды мақсаттар үшін қарау немесе пайдалану үшін қолдану арқылы деректердің түпнұсқалығын бұзуға әкеледі (7 - бап).

* Компьютерлерді пайдалану арқылы алаяқтық жасау - компьютерлік деректерді енгізу, өзгерту, өшіру немесе жасыру немесе өзіне немесе өзге адамға экономикалық пайданы заңсыз алу мақсатында компьютердің немесе жүйенің жұмыс істеуіне араласу жолымен басқа адамның меншігінен айыру (8-бап).

Деректердің мазмұнына байланысты (9-бап):

* Балалар порнографиясына байланысты құқық бұзушылықтар (кәмелетке толмаған адамның немесе кәмелетке толмаған болып көрінетін адамның жыныстық ашық әрекеттерге қатысуын көзбен көрсететін порнографиялық материалдар, сондай - ақ жыныстық ашық әрекеттерге қатысатын кәмелетке толмағандарды білдіретін реалистік бейнелеу өнері), атап айтқанда: компьютерлік жүйелер арқылы тарату мақсатында іс жүргізу; компьютерлік жүйелер арқылы ұсыну немесе ұсыну; компьютерлік жүйелер арқылы тарату немесе беру; компьютерлік жүйелер арқылы тарату немесе беру; өзіне немесе басқа адамға компьютерлік жүйе арқылы; компьютерлік жүйеде немесе компьютерлік деректерді сақтау ортасында балалар порнографиясын иелену.

Авторлық және сабақтас құқықтарды бұзуға байланысты (10-б.):

* 1971 жылғы 24 шілдедегі Париж актісінің әдебиет және өнер туындыларын қорғау туралы Берн Конвенциясына, Зияткерлік меншік құқықтарының саудамен байланысты аспектілері туралы келісімге және

Дүниежүзілік зияткерлік меншік ұйымының (ДЗМҰ) Авторлық құқығы туралы шартқа талаптарын ескере отырып, мемлекетішілік заңнаманың нормаларында көзделген авторлық құқықты бұзу, мұндай іс - әрекеттер коммерциялық ауқымда және компьютерлік жүйенің көмегімен жасалған кезде осы конвенциялар беретін моральдық құқықтарды қоспағанда.

* Орындаушылардың, дыбыс жазбаларын өндірушілердің және радиохабар ұйымдарының құқықтарын қорғау туралы халықаралық конвенцияның (Рим конвенциясы), зияткерлік меншік құқықтары саласындағы сауда - саттықпен байланысты келісімнің және ДЗМҰ - ның орындаушылар мен дыбыс жазбалары туралы шартының талаптарын ескере отырып, мемлекетішілік заңнаманың нормаларында көзделген авторлық құқыққа (сабақтас құқықтарға) байланысты құқықтарды бұзу, осы конвенцияларда берілген кез келген моральдық құқықтарды қоспағанда, мұндай әрекеттер қасақана коммерциялық ауқымда және компьютерлік жүйенің көмегімен жасалады.

Конвенцияда аталған әрекеттердің зиянды салдары ретінде компьютерлік ақпаратты, компьютерлерді, олардың жүйелерін немесе желілерін заңды пайдаланушылардың құқықтарын бұзу танылады. Конвенцияда неғұрлым ауыр салдардың (материалдық залалдың, алынған компьютерлік ақпаратты құқыққа қарсы пайдаланудың және т.б.) міндетті белгісі ретінде белгілеу мемлекеттердің қарауына қалдырылды. Жалпы алғанда, бақылау нормалары зиянды салдардың міндетті түрде туындауын көздемейді.

Жоғарыда көрсетілген әрекеттерді жасаған жеке тұлға киберқылмыстың субъектісі бола алады.

Әр түрлі елдерде қалыптасқан тәжірибеге сүйене отырып, Конвенцияның 12 - бабы заңды тұлғалардың онымен қарастырылған құқық бұзушылықтар үшін жауапкершілігін белгілеуді талап етеді. Заңды тұлғаның жауапкершілігінің басталу шарттары мыналар болып табылады: (1) заңды тұлғаның пайдасына пайда алу мақсатында іс - әрекет жасау (2) (3) оның басшылық лауазымдағы лауазымды тұлғасы, (4) заңды тұлғаны ұсыну, шешім қабылдау немесе оның іс - әрекетіне бақылауды жүзеге асыру жөніндегі өкілеттіктерін пайдалана отырып. Бұдан басқа, конвенция заңды тұлғаның пайдасына пайда алу мақсатында өзге қызметкер басшылық қызмет атқаратын лауазымды адамның басшылығымен құқыққа қарсы әрекеттер жасаған жағдайларда да заңды тұлғалардың жауапкершілігін белгілеуге нұсқама береді.

Субъективті жағы. Конвенцияда аталған барлық қылмыстар тек олар қасақана жасалған жағдайда ғана жауапкершілікке әкеп соғады. Компьютерді немесе компьютерлік ақпаратты пайдалану арқылы жасалған "дәстүрлі" қылмыстардың қылмысын белгілейтін кейбір мақалаларда кінәнің қасақана нысаны әрекеттің өзін ғана емес, сонымен бірге оларды заңсыз пайдалануды да сипаттауы керек, дегенмен бұл осындай қылмыстардың біліктілік белгісі болып табылады (мысалы, 8 - бап - компьютерді пайдалану алаяқтық).

Конвенция аяқталған қылмыстармен қатар қастандық жасағаны, оған қатысқаны немесе оны жасауға айдап салғаны үшін жауапкершілікті белгілеу

қажеттілігін көздейді (11 - бап).

Конвенцияның 13-бабының 1-бөлігіне сәйкес аталған іс-әрекеттерді жасағаны үшін нақты Санкциялар белгілеу мемлекеттердің қарауына жатқызылған. Олардың қалауы бойынша жеке тұлғалар үшін қылмыстық жауапкершілік, сондай - ақ заңды тұлғалардың қылмыстық, азаматтық - құқықтық немесе әкімшілік жауапкершілігі белгіленуі мүмкін.

Қылмыстық іс жүргізу аспектілері

Конвенцияның басты ерекшеліктерінің бірі компьютерлік қылмыс саласындағы қылмыстарды тергеудің қылмыстық процесін реттеудегі басым рөл ұлттық заңнамаға тиесілі деген ережені негізге алу ұсынысы болып табылады. Осыған орай Конвенция "ұлттық деңгейде қабылдануы тиіс шаралар" деген 2 - тарауды қамтиды, онда ұлттық бұрыштық процеске компьютерлік қылмыстар туралы істер бойынша тергеп - тексеруге және сот талқылауына тән процестік әрекеттер туралы нормаларды енгізу көзделген (14-23-Б.).

Ұлттық заңнамаға енгізу үшін Конвенция ұсынатын іс жүргізу нормаларының шеңберіне, ең алдымен, компьютерлік деректер түріндегі дәлелдемелік ақпаратқа тән ерекшеліктермен байланысты бірқатар ерекшеліктермен толықтырылған белгілі тергеу әрекеттері кіреді.

Осыған байланысты іс жүргізу институттарының шеңберін жаңа іздеу және алу үйін толықтыру ұсынылады. Конвенцияның "сақталған компьютерлік деректерді тінту және алу" 19-бабында мыналар туралы нұсқаулар бар:

* компьютерлік жүйелер немесе олардың бөліктері, сондай - ақ онда сақталатын компьютерлік деректер және (b) қажетті компьютерлік деректер сақталатын компьютерлік деректерді сақтауға арналған орта тінтуге немесе дәлелдемелік ақпаратты қоршаған ортадан алуды қамтамасыз ететін өзге де ұқсас тергеу әрекетіне ұшырауы мүмкін;

* егер тінту барысында іздестіріліп жатқан деректер басқа компьютерлік жүйеде немесе оның бір бөлігінде сақталады деп пайымдауға негіз болса және мұндай деректер бірінші жүйеден қолжетімді болса немесе оның көмегімен алынуы мүмкін болса, құзыретті органдар жүргізілген тінтуді осы басқа жүйеге дереу "таратуға" құқылы болуы тиіс;

* қажетті компьютерлік деректер табылған кезде құзыретті органдар: (a) компьютерлік деректерді сақтау үшін есептеу жүйесін, оның бір бөлігін немесе ортасын алуға не оларға өзгеше түрде тыйым салуға; (b) тиісті компьютерлік деректердің көшірмелерін дайындауға және сақтауға; (c) іске қатысты сақталатын компьютерлік деректердің тұтастығын сақтауды қамтамасыз етуге; (d) осы компьютерлік деректерді компьютерлік жүйеде қол жеткізілмеген етіп жасауға немесе одан алып тастауға құқылы.

* талап етілетін компьютерлік деректерді алуды қамтамасыз ету үшін құзыретті органдар тиісті компьютерлік жүйенің жұмыс істеуі немесе қолданылатын қорғау шаралары туралы білімі бар кез келген тұлғаны тиісті көмек көрсетуге міндеттеуге құқылы.

Сонымен қатар, Конвенция жаңа іс жүргізу әрекеттерінің құқықтық

негіздерін ішкі мемлекеттік деңгейде қалыптастыру қажеттілігін қарастырады.

Оларға, біріншіден, сақталған компьютерлік деректердің, соның ішінде ақпарат ағындары туралы деректердің сақталуын дереу қамтамасыз ету кіреді4, олар генерацияланған және компьютерлік жүйенің көмегімен сақталған, бұл деректер әсіресе жоғалту немесе модификациялау қаупіне ұшырайды деп болжауға негіз болған кезде (16-бап). Ол иелігінде немесе бақылауында компьютерлік деректер бар кез келген тұлғаға берілген құзыретті органдардың өкімі негізінде жүзеге асырылуға тиіс. Сақтаудың нақты мерзімі белгіленбеген, бірақ "құзыретті органдарға осы компьютерлік деректерді ашуға мүмкіндік беретін уақыттың барабар кезеңі"ретінде белгіленген. Бұл ұсынылған процессуалдық институт билік органдарының компьютерлік ақпаратқа қол жетімділігіне құқықтық негіз бермейді, тек алдын - ала сипаттағы шара бола отырып, басқаларға жағдай жасайды. Бұл ретте деректердің сақталуы деп оларды кез келген сыртқы әсерлерден қорғай отырып, ЭЕМ-де қандай күйде қалдыруды түсіну керек.

Екіншіден, ақпарат ағындары туралы деректердің сақталуын дереу қамтамасыз ету және ішінара ашу (17-бап). Ол алдыңғысынан Компьютерлік желілер арқылы берілетін электр байланысы хабарлары туралы мәліметтерді сақтау қажеттілігі туралы сөз болған жағдайларда қолданылуға жататындығымен ерекшеленеді. Бұл ақпарат ағындары туралы деректерді "қызмет көрсетушілердің бір немесе одан да көп саны тиісті хабарламаны беруге тартылғанына қарамастан" бірден сақтауға, ал екінші жағынан бұл деректерді құзыретті органдарға "қызмет көрсетушілерді және байланыс берілген жолды сәйкестендіру" үшін, яғни компьютерлік ақпараттың енгізу нүктесінен соңғы адресатқа дейінгі желілерде өтуін жедел қадағалау үшін нақты көлемде дереу ашуға мүмкіндік беруі тиіс.

Үшіншіден, ұсыну туралы өкім беру (18-бап). Мұндай өкім (1) адамға - компьютерлік жүйеде немесе компьютерлік деректерді сақтау үшін өзге ортада сақталатын осы тұлғаның бақылауындағы компьютерлік деректерді ұсыну туралы, (2) Қызмет көрсетушіге – оның абоненттері туралы мәліметтерді беру туралы берілуі мүмкін. Соңғысына қызмет көрсетушіде бар, компьютерлік деректер нысанында да, сондай - ақ кез келген басқа нысанда да (ақпарат ағындары немесе мазмұны туралы деректерді қоспағанда) көрсетілген пайдаланушылар туралы кез келген ақпарат алып тасталды, оның көмегімен мыналарды: пайдаланылған байланыстың түрін, оның техникалық шарттары мен жүзеге асырылу уақытын; пайдаланушының жеке басын, оның мекенжайын, телефон нөмірлерін және өзге де қол жеткізу құралдарын, оған қойылған шоттар және ол жасаған төлемдер туралы мәліметтерді; коммуникациялық жабдықты орнату орны туралы кез келген басқа Конвенция жаңа өкілеттіктердің осы түрін нақты қылмыстық істерді тергеу міндеттерін шешу үшін қатаң жеке негізде қолдануға мүмкіндік беретінін атап өткен жөн. Осыған байланысты, бұл өкілеттіктер барлық қызмет жеткізушілерін өз абоненттері туралы ақпаратты, олар беретін барлық компьютерлік ақпаратты және т. б. үнемі жинақтау және сақтау үшін пайдаланылмауы керек екенін

түсіну керек.

Төртіншіден, компьютерлік жүйелер арқылы берілетін ақпарат ағындары туралы деректерді нақты уақыт режимінде техникалық құралдарды қолдана отырып жинау және жазу (20-бап). Конвенцияда осы қызметті мемлекеттің құзыретті органдарына да, сондай-ақ олардың қызмет көрсетушілердің нұсқауы бойынша да жүзеге асыруға өкілеттік беру көзделген. Қызметтің бұл түрі электр байланысы желілері арқылы берілетін, осындай өкілеттіктерді іске асыру кезінде орта есеппен қалыптасатын (құрылатын) хабарламалар туралы мәліметтерге қатысты қолдануға есептелген. Бұл ретте материалдық емес объектілерді беру жүзеге асырылады (мысалы, электромагниттік импульстар түрінде), ал оларды жинау және жазу адресатқа дейін электр байланысы желілері бойынша хабарламаның өзінің өтуіне кедергі келтірмейді.

Бесіншіден, мемлекеттің құзыретті органдары да, қызметтерді жеткізушілер де олардың нұсқауы бойынша жүзеге асыратын, компьютерлік жүйелердің көмегімен берілетін хабарламалардың мазмұны туралы деректерді ұстап алу (жинау және жазу) (21 - бап). Бұл институт алдыңғы институтқа ұқсас, бірақ тікелей байланыс желілері арқылы берілетін хабарламалардың маңызды бөлігіне қатысты.

Конвенцияда компьютерлік ақпаратты жинаудың соңғы екі әдісін іске асыруды құқықтық реттеу тетігі егжей - тегжейлі жазылмаса да, қолданыстағы тәжірибе және Ресей Федерациясының және басқа елдердің заңнама нормаларына сәйкестігі, олар қазіргі уақытта жедел іздестіру шараларын жүргізу арқылы қолданылуы мүмкін деп айтуға мүмкіндік береді. "Жедел-іздестіру қызметі туралы" Федералдық заңның 6-бабы.

Жедел-іздестіру қызметін тек мемлекеттік органдардың уәкілетті бөлімшелері ғана жүзеге асыра алады (аталған Федералды Заңның 1 - бабы). Мұндай жағдайларда қызмет көрсетушілердің нақты уақыт режимінде Ақпарат ағындары туралы деректерді жинау және жазу, хабарлардың мазмұны туралы деректерді ұстап алу (жинау және жазу) жөніндегі өкілеттіктерді тікелей іске асыруы заңнаманың Конституциялық қағидаттарына қайшы келетін болып ұсынылады. Сонымен бірге, Конвенцияда қарастырылған осы салада көмек көрсету өте қолайлы, бірақ қайтадан Ресей Федерациясының Қылмыстық кодексіне тиісті нормаларды енгізуді талап етеді.

Айта кету керек, Ресей Федерациясында электр желілері (SORM) 5 желілерінде (қызметтерінде)жедел-іздестіру іс - шараларының функцияларын қамтамасыз ету үшін әзірленген және жүзеге асырылатын жүйе, негізінен, Конвенцияның соңғы екі бұйрығын жүзеге асыруға дайын механизм болып табылады. Оның тұжырымдамасы қызмет көрсету операторларының мүмкіндіктерін Ресей Федерациясының Конституциясының талаптарына қайшы келмейтін дәрежеде пайдалануға мүмкіндік береді.

Отандық Summ-ді нормативтік реттеудің тұжырымдамасы мен практикасының Конвенцияның нұсқауларына бірден-бір қарама-қайшылығы, соңғысы, ең алдымен, осы қызметті заңнамалық реттеуді талап етеді. Ресей Федерациясында мұндай қызметті ведомстволық нормативтік реттеуге басты

назар аударылады. Осыған байланысты таратылатын құжатқа қол қою және ратификациялау алдында осыған байланысты туындауы мүмкін проблемаларды мұқият пысықтау қажет болып көрінеді.

Халықаралық ынтымақтастық мәселелері

Конвенцияда Ұлттық қылмыстық іс жүргізу заңнамасына енгізілуге жататын нормаларды егжей-тегжейлі баяндау онда оған қатысушылардың халықаралық ынтымақтастығының негізгі қағидаттарын айқындау үшін қажетті жағдайлар жасады, оларға 23 - бап жатқызылды:

* құқықтық негізі халықаралық құжаттар, бірыңғай және бірін - бірі толықтыратын заңнама негізінде келісілген уағдаластықтар, сондай-ақ мемлекетішілік құқық нормалары болып табылатын ынтымақтастықтың барынша кең шектері;

* кез-келген компьютерлік жүйелер мен компьютерлік мәліметтерге қатысты қылмыстарды тергеу немесе қудалау кезінде ынтымақтастық орнату.

Жалпы, әртүрлі мемлекеттердің құзыретті органдарының компьютерлік қылмыстарға қарсы күрестегі ынтымақтастық мәселелері "Халықаралық ынтымақтастық" конвенциясының 3-тарауына арналған. Оның мазмұнында бірнеше негізгі аспектілерді бөліп көрсету керек.

Қарым-қатынас тәртібі

Компьютерлік ақпарат саласындағы қылмыстарды тергеу кезінде өзара құқықтық көмек туралы сұраулардың көпшілігі азаматтардың конституциялық құқықтарына әсер ететін мәселелерге қатысты. Осыған орай Конвенция осы өтініштер бойынша шешімдер қабылдау нақты қылмыстық істердің тергеулігі мен ведомстволық бағыныстылығына қарамастан (алдын ала және сот тергеу сатыларының ерекшелігін ғана ескере отырып) бір - екі орталық органның ерекше құзыретінде болуға тиіс екендігін негізге алады. Дәл осы арнайы тағайындалған орталық органдар бір-бірімен тікелей байланыста болуы керек.

Осындай қылмыстарды тергеу ерекшелігін ескере отырып, Конвенция өзара құқықтық көмек көрсету кезінде қатынастардың жалпы тәртібін толықтыруды көздейді.

Мәселен, 25 - баптың 3 - бөлігіне сәйкес кейінге қалдыруға болмайтын мән-жайларда, егер мұндай құралдар қауіпсіздіктің және түпнұсқалықты растаудың тиісті деңгейлерін қамтамасыз ететін болса, Сұрау салынатын Тараптың талабы бойынша кейіннен ресми бекіте отырып, факсимильдік хабарламаларды немесе электрондық поштаны қоса алғанда, жедел байланыс құралдарын пайдалана отырып, өзара құқықтық көмек туралы сұрау салуларды немесе осындай сұрау салуларға байланысты хабарламаларды жіберуге жол беріледі. 9-бөлімнің "А" және "b" тармақтарына сәйкес. 27 Конвенция өзара құқықтық көмек туралы сұрау салуларды немесе олармен байланысты хабарламаларды тараптардың сот органдары тікелей, сондай-ақ моп (Интерпол) арқылы жібере алады.

Сонымен қатар, Конвенциямен күн сайын тәулік бойы қол жеткізу желісін ("24/7 Network" халықаралық белгісі, ол "аптасына 7 тәулік 24 сағат қол жеткізу"ретінде түсіндірілуі мүмкін) құру жолымен халықаралық - құқықтық

құжаттармен бұрын реттелмеген қатынастар тәртібін енгізу ұсынылады.

Конвенцияның 35 - бабы күн сайынғы тәулік бойы қол жеткізу желісінің байланыс пункттерін қалыптастыруды көздейді ("24/7 Network"халықаралық белгісі). Әрбір Тарап қылмыстық істер бойынша дәлелдемелерді электрондық нысанда жинау кезінде есептеу жүйелерімен және компьютерлік деректермен байланысты қылмыстар туралы қылмыстық істерді тергеуге немесе сот талқылауларына дереу көмек көрсетуге кепілдік беру үшін тәулігіне 24 сағат аптасына 7 күн болатын байланыс нүктесін тағайындауға міндетті. Мұндай көмек жәрдем көрсетуді немесе егер бұған ұлттық заңнамаға және практикаға сәйкес рұқсат етілсе, тікелей: (А) техникалық консультациялар беруді; (б) компьютерлік деректер мен ақпарат ағындары туралы деректердің сақталуын қамтамасыз етуді; (с) дәлелдемелерді жинауды, құқықтық ақпарат беруді және күдіктілерді анықтауды қамтуы тиіс. Байланыс нүктелерінің негізгі міндеттерінің бірі – Конвенцияда қарастырылған функциялардың тез орындалуын қамтамасыз ету, тіпті егер олар тармақтың құзыретіне кірмесе де. Мысалы, егер соңғысы полиция бөлімінің немесе басқа құқық қорғау органының ажырамас бөлігі болса, онда ол шет мемлекет сұраған құқықтық көмек көрсете алатын басқа ведомстволармен және олардың бөлімшелерімен шұғыл байланыс орната алуы керек. Бұл қызметті жүзеге асыру үшін ұлттық байланыс нүктесі екінші тараптың байланыс нүктесімен шұғыл түрде байланыс орнатуға, осы желінің жұмыс істеуін қамтамасыз ететін оқытылған және жабдықталған персоналға ие болуы керек6.

Бұдан басқа, Конвенция өзінің жеке тергеуі шеңберінде алынған ақпаратты, ол мұндай ақпаратты ашу осы мәліметтерді алушы Тарапқа қылмыстық қылмыстарға қатысты тергеуді немесе сот талқылауын бастауға немесе жүргізуге көмектесе алады деп пайымдаса, Тараптардың бірінің жіберу мүмкіндігін айқындайды (26-бап).

Конвенция (27-б.,7-б.) өзара құқықтық көмек көрсетуге байланысты өтініш жасаған кезде Сұрау салынатын Тарап сұрау салушыға көмек туралы сұрау салудың орындалу барысы туралы хабарлауға, көмек көрсетуді кейінге қалдыру себептері туралы немесе бас тарту туралы хабардар етуге тиіс екенін көздейді.

Құқықтық көмектен бас тарту

Конвенцияда құқықтық көмек көрсетуден бас тарту негіздері екі негізгі топқа бөлінеді.

Егер сұрау салынатын көмекті сот төрелігінің мақсаттарымен салыстыруға болмайтыны анық болса, мыналар: (1) сұрау салу сұрау салынатын тарап саяси қылмыс ретінде немесе саяси қылмысқа байланысты құқық бұзушылық ретінде қарайтын құқық бұзушылыққа қатысты болса немесе (2) сұрау салуды орындау сұрау салынатын тараптың егемендігіне, қауіпсіздігіне, қоғамдық тәртібіне (ordre public) немесе өзге де елеулі мүдделеріне нұқсан келтіруге әкеп соғатын ықтималдық болса (27-б., 4-б.), императивтік негіздер пайдалануға жатады.

Екінші топ сұралған мемлекеттің ішкі заңнамасының осы немесе басқа

ережелеріне ресми түрде қайшы келуі мүмкін бас тартудың дискрециялық шарттары болып табылады. Құқықтық көмектен бас тарту үшін осындай негіздерді қолдану мүмкіндігі Келісімнің 26 - бабының 4 - бөлігінде көзделген халықаралық шарттарға негізделген. Мұндай дискрециялық шарттарға осы адамның Сұрау салынатын мемлекетте қылмыстық ізіне түсуін жүзеге асыру, қылмыс құрамын екі рет айқындау, қылмыстық жауаптылыққа тартудың ескіру мерзімінің өтуі, ақтау немесе айыптау үкімінің, сұрау салынатын мемлекетте қылмыстық іс қозғаудан бас тарту немесе іс бойынша тергеуді тоқтату туралы қаулының болуы жатады.

Бұдан басқа, құқықтық көмек туралы сұрау салулардың нысанасы болып табылатын компьютерлік деректердің ерекшелігін ескере отырып, Конвенцияның 29-бабының 6-бөлігі "егер сұрау салынатын тарап [компьютерлік деректердің] сақталуын қамтамасыз ету болашақта тиісті деректердің қолжетімділігіне кепілдік бермейді немесе құпиялылыққа қатер төндіреді немесе сұрау салушы тарап жүргізетін тергеп-тексеруге өзге де жолмен залал келтіреді деп ұйғарса, ол бұл туралы сұрау салушы сотороға дереу хабарлайды, ол кейіннен осы сұрау салудың осыған қарамастан орындалуға Осылайша, Конвенция тараптармен келісілген құқықтық көмектен бас тарту деп аталатын процедураны енгізеді.

Компьютерлік технологияларды қолдана отырып жасалған қылмыстар туралы көптеген қылмыстық істерді тергеу кезінде қаржылық құжаттарды талап ету қажеттілігі туындайтындықтан, Конвенцияда банктік құпияны қорғау туралы әртүрлі елдердің ішкі заңнамасының әрекетіне қатысты басым күшке ие болатын тәртіпті бекіту маңызды болып көрінеді. Кейбір құқықтық жүйелерде банктік құпияны қорғау құқықтық көмек көрсетудегі негізгі кедергілердің бірі болды және болып табылады. Осы себепті 4-б. Конвенцияның 26 - тармағы өзара көмектен бас тарту құқығын сұрау салу сұрау салынатын тарап қаржылық деп қарайтын құқық бұзушылыққа қатысты негізде ғана пайдалануға тыйым салу туралы тармақ тек қана оң бағалануы мүмкін.

Құпиялылық және ақпаратты пайдалануға шектеулер

Сұрау салушы тарап берілетін компьютерлік ақпараттың немесе материалдардың құпиялылығын сақтау мүмкін болмаған жағдайда, сондай - ақ егер Сұрау салушы Тарап бұл ақпарат немесе материалдар құқықтық көмек туралы сұрау салуда көрсетілгендерден басқа, қандай да бір тергеулер немесе сот талқылаулары жүргізу үшін пайдаланылмайтынына кепілдік бермесе, құқықтық көмектен бас тартуға рұқсат алу Конвенцияда көзделген ерекше шарттардың бірі болып табылады (28-бап).

Бұл нормаларды енгізу, ең алдымен, азаматтардың жеке өміріне қол сұғылмаушылық құқығын және одан туындайтын басқа да конституциялық құқықтарды мемлекеттік органдардың қамтамасыз ету қажеттілігімен байланысты. Бұдан басқа, олар мемлекеттік мүдделерді (жалпыға қолжетімді болып табылмайтын ақпарат ұсынылған жағдайда) және құқықтық көмек туралы өтінішхатты орындау мүдделері қозғалатын азаматтардың құқықтарын қорғауға қызмет етеді.

Құпиялылық қағидаларының сақталуын бақылау үшін сұрау салынатын тарапқа сұрау салушы тараптан өзара құқықтық көмек көрсету тәртібімен берілген компьютерлік ақпараттың қалай пайдаланылғаны туралы түсініктеме беруді талап ету құқығы берілген. Конвенцияны әзірлеушілер талап етілетін есептілік сұрау салушы тарап үшін тым ауыр болмауы тиіс деп шешті.

Процестік әрекеттер

Конвенцияда шетелдік құқық қорғау органдарының сұрау салулары бойынша өзара құқықтық көмек сұрау салынатын тараптың заңы белгілейтін шарттарда көрсетілуге тиіс екендігі көзделген. Алайда, бұл сұрау салушы тарап көрсеткен рәсімдерге сәйкес сұрау салулардың орындалуын, олар сұрау салынатын тараптың заңдарымен үйлеспейтін жағдайларды қоспағанда, жоққа шығармайды (27-б.3-б.). Бұл ретте конвенция жобасына түсіндірме баяндамада: "мұндай рәсімнің сұрау салынатын тараптың құқықтық жүйесінде белгісіз болу фактісі сұрау салушы тарап ұсынған рәсімді орындаудан бас тарту үшін жеткілікті негіз болып табылмайды"деп көрсетілген. Осы алғышарттарды ескере отырып, өзара құқықтық көмек туралы өтініштерді мәлімдеу кезінде рұқсат етілген іс жүргізу және тергеу әрекеттерінің ауқымы Ұлттық қылмыстық іс жүргізу заңнамасына енгізу үшін Конвенция ұсынған олардың тізіміне ұқсас.

Біріншіден, құқықтық көмек сұрау салынатын тараптың аумағындағы компьютерлік жүйенің көмегімен сақталатын компьютерлік деректердің сақталуын дереу қамтамасыз ету жолымен көрсетілуге жатады (29 - бап). Егер мүдделі тарап бұл туралы сұрау салуда жүйеге тінтуге немесе өзге де осындай қол жеткізуге, деректерді тәркілеуге немесе оларды өзге де осындай жолмен игеруге немесе осы сақталатын компьютерлік деректерді ашуға қатысты өзара көмек туралы өтініш білдірсе, бұл көмек көрсетілуі мүмкін. Талап етілетін компьютерлік деректер сұрау салушы тарапқа тінту немесе оларға өзге де қол жеткізу туралы өтініш беруге мүмкіндік беру үшін кемінде 60 күн сақталуы тиіс.

Екіншіден, құқықтық көмек ақпарат ағындары туралы сақталған деректерді жедел ашу арқылы көрсетілуге тиіс (30 - б.). Конвенцияның 17 - бабында регламенттелген жағдайлардағыдай, ол енгізу нүктесінен соңғы адресатқа дейінгі желілерде компьютерлік ақпараттың өту жолдарын белгілеу қажеттілігі туралы сөз болғанда, ЕО хабарламаны беруге әртүрлі мемлекеттердің қызметтерін жеткізушілер тартылған жағдайда да рұқсат етіледі. Компьютерлік желілер арқылы берілетін Электр байланысының хабарламалары туралы сақталған деректерді құқықтық көмек көрсету тәртібімен тарату "қызмет көрсетушілерді және хабар берілген жолды сәйкестендіру"үшін жеткілікті көлемде жүзеге асырылуы тиіс.

Үшіншіден, сақталған компьютерлік деректерге қол жеткізуді сұрау салынатын тараптың өтініші бойынша тінту немесе жүйеге өзге де осындай қол жеткізу, деректерді тәркілеу немесе олардың өзге де осындай жолмен алып қою жолымен қамтамасыз етуде немесе сұрау салынатын тараптың аумағындағы компьютерлік жүйенің көмегімен сақталатын деректерді ашуда өзара құқықтық көмек көрсету көзделген (31 - бап). Конвенцияның 2 және 3 тарауларының

мазмұнын салыстыру бұл құқықтық көмек ұлттық заңнамаға 18 және 19-баптарды енгізуге ұсынылатын тетіктерді пайдалана отырып, іздестіруге, сақталатын компьютерлік деректерді ұсынуға және алуға өкім беру жолымен көрсетілуге тиіс екенін айғақтайды.

Төртіншіден, Конвенцияда компьютерлік жүйелер арқылы берілетін ақпарат ағындары туралы деректерді нақты уақыт режимінде техникалық құралдарды қолдана отырып жинау жолымен құқықтық көмек көзделген (33 - бап).

Бесіншіден, компьютерлік жүйелермен берілетін хабарламалардың мазмұны туралы деректерді ұстап алу (жинау және жазу) жолымен өзара құқықтық көмек көрсету мүмкіндігі көзделген (34 - бап).

Құқықтық көмектің соңғы екі түрін қолдануға жол берілетіндігі олардың мемлекетішілік құқық нормаларында көзделген шарттар мен рәсімдерге сәйкестігімен түсіндіріледі.

Конвенция өзара құқықтық көмек көрсетудің көрсетілген нысандарынан басқа, сақталатын компьютерлік деректерге трансшекаралық қол жеткізуді регламенттейтін норманы енгізуге осындай деректерді ашуға уәкілеттік берілген адамның келісімімен немесе олар жария қол жетімді болған кезде ұсынады (32 - б.).

Осы баптың "А" тармағының мазмұны қандай да бір қайта қарауға алып келуі екіталай. Интернет сияқты халықаралық ғаламдық компьютерлік желілер - бұл пайдаланушыларға ұлттық, кәсіби, мемлекеттік және басқа да қатыстылығына қарамастан, олар орналасқан мемлекеттің шекарасынан тыс жерлерде белгілі бір әрекеттерді орындау мүмкіндігін беретін жабық орта.

"Б" тармағына келетін болсақ, ол іс жүзінде талап етілетін компьютерлік ақпаратты табу және алу мақсатында шетелде компьютерлік желілерді (немесе компьютерлік деректерді сақтау ортасында) іздеуден басқа ештеңені реттейтін норманы білдіреді.

Бұл қорытынды компьютерлік деректерді мүдделі тарапқа компьютерлік жүйе арқылы ашуға заңды негізде уәкілеттік берілген адам деп, ең алдымен, қызмет көрсетушілерді түсіну керек (яғни, пайдаланушыларға компьютерлік жүйелер арқылы ақпарат алмасу мүмкіндігін қамтамасыз ететін кез - келген мемлекеттік немесе жеке құрылым, сондай - ақ байланыс қызметі немесе осындай қызметті пайдаланушылар атынан компьютерлік деректерді өңдеуді немесе сақтауды жүзеге асыратын кез - келген басқа құрылым). Ғаламдық компьютерлік желілердің архитектурасын ескере отырып, әлемнің кез - келген елінде белгілі бір қызмет жеткізушісін (провайдерді) табуға болады, оның қызметінде шетелде сақталған компьютерлік деректерге қол жеткізудің заңды техникалық тетіктері бар (электр байланысы желілері арқылы берілетін хабарламалар туралы мәліметтер де, хабарламалардың өздері де) немесе өзі (физикалық серверлерге ие) шетелдік пайдаланушының компьютерлік деректерін сақтайды. Мұндай жағдайларда шет мемлекеттің аумағында компьютерлік ақпаратқа қол жеткізу іс жүзінде бақылаусыз, шетелдік мемлекеттің егемендік құқықтарын бұза отырып жүзеге асырылады.

Бұдан басқа, осы нұсқаманы іс жүзінде іске асыру ұлттық заңнамада "компьютерлік деректерді ашуға уәкілеттік берілген адамның заңды негізінде"ұғымын нақты түсінуді және регламенттеуді талап етеді.

Жоғарыда келтірілген қарсылықтарға қарамастан, байланыс операторларының шетелде орналасқан электр байланысы желілері арқылы берілетін хабарламалар туралы мәліметтерге қол жеткізу мүмкіндіктері тәжірибеде сәтті пайдаланылатындығын атап өткен жөн.

Конвенция ұсынған ақпаратқа трансгра-ниялық қол жеткізу тәртібі кейбір мәселелерді ашық қалдыратынына назар аударады:

* компьютерлік деректерді осылай жинау туралы шешімге шағымдану тәртібі;

* жоғарыда аталған іс жүргізу әрекеттері бойынша мүдделі азаматтарды хабардар ету;

* осы жолмен алынған ақпараттың құпиялылығын қорғау;

* ұлттық соттар мен құзыретті органдардың шетелдік органдар іс - қимылдарының заңдылығын сот және ведомстволық бақылауы.

Мемлекеттердің осы мәселелерді пысықтауы үшін жағдайлар өзге де халықаралық-құқықтық құжаттарда жасалатынын атап өткен жөн. Біріншіден, ақпараттық желілер арқылы жаңа ақпараттық технологияларды қолдана отырып, жеке деректерді жинау, өңдеу және әсіресе беру ерекшеліктері деректерді автоматтандырылған өңдеуге қатысты жеке тұлғаны қорғау туралы Келісімнің ережелерімен реттеледі.

Бұдан басқа, бұл проблемалар ЕК-ге мүше елдердің Министрлер комитетінің құжаттарында қарастырылады: төлемдер мен басқа да аралас операциялар кезінде пайдаланылатын дербес деректерді қорғау туралы № R (90) 19 Ұсынымдар, мемлекеттік ұйымдардың қарамағындағы дербес деректерді үшінші тұлғаларға беру туралы № R (91) 10 Ұсынымдар[42], телекоммуникация саласындағы, әсіресе телефониядағы дербес деректерді қорғау туралы № R (95) 4 ұсынымдар[43].

2 Киберкеңістікте жасалатын қылмыстармен күресідің құқықтық аспектілері

2.1 Киберкеңістікте жасалған қылмыстардың қылмыстық-құқықтық сипаттамасы

Қылмыстық-құқықтық ғылым үшін және заңнама үшін ғылыми және саяси талқылаулар мен әзірлемелердің жаңа болжамы пайда болады.Ал Қазақстанның қылмыстық заңнамасы бойынша компьютерлік ақпарат саласындағы қылмыстың мәні неде? Бұл ҚР ҚК-нің ақпарат пен ақпараттық технологияларды пайдаланумен байланысты қатынастарды регламенттейтін нормаларында негізделетін ұстанымдар, осы нормаларға талдау жүргізу жаңа коммуникациялық технологиялар саласындағы ықтимал қылмыстық әрекеттердің барлық ауқымын ашады. Әрбір пайдаланушы компьютерлік ақпаратты таратады, сондай-ақ тұрмыстық деңгейде қорғайды, дегенмен, ҚР ҚК сәйкес компьютерлік ақпарат шектеулі нысанда болса да, қылмыстық-құқықтық қорғауға жатады.

Қылмыстық заңның нормаларына қатысты мұндай ақпаратқа қойылатын негізгі талап-мұндай ақпаратқа қол жеткізу шектеулі болуы керек. "Жеке тұлға, қоғам, мемлекет" триадасына сүйене отырып, қол жетімділігі шектеулі ақпаратты құрайтын барлық құпияларды үш санатқа бөлуге болады: жеке құпия; отбасылық құпия, коммерциялық құпия, кәсіби Құпия; мемлекеттік және қызметтік құпия [44, 45 б.].

ҚР Қылмыстық кодексінің бөлімін талдау және түсіндіру экономикалық қызмет саласындағы қылмыстық құқық бұзушылықтар бізге қарастырылып отырған қылмыстардың мәні ретінде компьютерлік ақпарат ұғымын кеңейтуден және толығымен дұрыс түсіндірмеуден, сонымен бірге мұндай ұғымдарды Қазақстан Республикасының заңнамасында тар және нақты пайдаланбаудан туындайтын шексіз бірқатар проблемаларды береді. Сонымен, соңғы жылдары құқық қорғау органдары машиналық медиаға жазылған ЭЕМ-ге арналған бағдарлама компьютерлік ақпарат болып табылатындығына сүйене отырып, Сондықтан машиналық медиадағы бағдарламаға заңсыз қол жеткізу машиналық медиадағы, электрондық-есептеу машинасындағы (ЭЕМ), ЭЕМ жүйесіндегі немесе олардың желісіндегі ақпаратқа қол жеткізу ретінде сараланады немесе заң шығарушы заңсыз қол жеткізу жоюға, бұғаттауға, түрлендіруге немесе көшіруге, сондай-ақ компьютерлік техниканың бұзылуына әкеп соқтырды деп мәлімдейді., олардың желілері мен жүйелерін жоғарыда аталған объектілерге рұқсаты бар адам заңмен жазалайды, бұл мұндай құқық қолдану практикасы қолданыстағы заңнамаға сәйкес келмейді және толық жүзеге асырылмайды. Компьютерлік ақпаратқа заңсыз қол жеткізуді әрбір адам құқықсыз және оған қол жеткізу мүмкіндігінсіз жасай алады, сондай-ақ жоғарыда аталған заңсыз әрекеттердің әрқайсысы олардың жойылуына, бұғатталуына, модификациясына және т.б. әкелуі мүмкін емес, бұл тіпті пайдаланушылардың өздері де, ұйымдар да, мемлекет те, тіпті мұндай қол

сұғушылықтарды анықтауға арналған бағдарламалық қамтамасыз ету де жиі анықталмайды. Компьютерлік жүйенің, желінің немесе компьютердің өзін жоюға, бұғаттауға, көшіруге, өзгертуге немесе бұзуға әкеліп қана қоймай, сонымен бірге моральдық зиян келтіріп, авторлық және сабақтас құқықтарды бұзды, пайдаланушының ар-намысы мен қадір-қасиетін қорлады немесе қарапайым пайдаланушылардың мақсаттарына жетуге кедергі болды, үздіксіз жұмыстың тоқтауына әкелді немесе түсініксіз және анықталмады, бірақ пайдаланушылардың құқықтары мен заңды мүдделеріне қайшы келді. Компьютерлік бағдарлама авторлық құқықтың объектісі болып көрінетін сияқты, бірақ оған қатысты заңсыз әрекеттер компьютерлік ақпаратқа заңсыз қол жеткізу емес. Бағдарламаларды лицензиясыз пайдалану бағдарлама жасаушылардың авторлық және сабақтас құқықтарын бұзады және бұл бұзушылықтар заңсыз қол жеткізуге тікелей қатысы жоқ, бірақ бағдарламада немесе компьютерлік бағдарламаның көмегімен сақталатын нәрсе компьютерлік ақпаратқа заңсыз қол жеткізу арқылы ұрлау объектісі болып табылады және сонымен бірге авторлық құқық объектісі бола алады [45].

Компьютерлік технологиялар мен олармен байланысты қызметтер бүкіл адамзат өмірінің ажырамас бөлігі болды. Іс жүзінде көптеген заңсыз әрекеттер көбінесе компьютерлік техниканы немесе жаңа технологияны қолдана отырып жасалады, онда компьютерлік бағдарламалар немесе компьютерлік ақпарат пайдаланылады, бұл, әрине, компьютерлік ақпаратқа, компьютерге, компьютерлік жүйеге және компьютерлік желіге заңсыз қол жеткізу әдіс, құрал, объект рөлін атқара алады деген ойға әкеледі., және көбінесе қылмыс жасау әдісі. Сондықтан компьютерлік желіге, ақпаратқа және жүйеге қылмыс жасаудың топтық белгілерінің бірі ретінде, жалпы қылмыс сипаты ұғымы ретінде рұқсатсыз қол жеткізуді қылмыстық заңнама мен құқықты зерттеудің жалпы бөлігіне жатқызуға болады. Қылмыстық заңның ерекше бөлімінде компьютерлік ақпаратпен байланысты бірқатар қылмыстық құрамдарды айыптау және пенализациялау, содан кейін жаңа технологиялардың дамуы және осы саланың әдіснамалық және теориялық мәселелерінің толық дамуы, компьютерлік ақпаратқа және бүкіл компьютерлік жүйеге арналған бүкіл бөлімді бөліп көрсету.

Әр түрлі елдердің халықаралық қатынастарында компьютерлік ақпарат саласындағы қылмыстарды түсінудің әртүрлі тәсілдері, олардың компьютерлік қылмыстар, киберқылмыстар, жоғары технологиялық қылмыстар ұғымымен байланысы қарастырылады. 2000 жылы Американдық ғалымдар 52 елдің қылмыстық заңнамасына жаһандық зерттеу жүргізді және "ақпараттық кеңістікте" (cyberspace) жасалған қылмыстар қарастырылған елдерде осындай қылмыстардың төрт санатқа біріктірілген 10 түрін бөлуге болады деген қорытындыға келді:

1. ақпаратқа байланысты қылмыстар, оның ішінде оны ұстап алу, өзгерту және ұрлау;
2. компьютерлік желілерге қатысты қылмыстар, соның ішінде олардың жұмысына араласу және диверсия;

3. кіруге байланысты қылмыстар, соның ішінде хакерлік және вирустың таралуы; және

4. компьютерлерді пайдалануға байланысты қылмыстар, соның ішінде көмек көрсету және қылмысқа қатысу, компьютерлік алаяқтық және компьютерлік жалғандық.

Ғылыми зерттеулердің нәтижелерін және әртүрлі мемлекеттердің, сондай-ақ халықаралық қоғамдастықтың заңнамалық тәжірибесін ескере отырып, компьютерлік қылмыстар қатарына компьютерлік ақпарат саласындағы қылмыстар мен ақпараттық технологияларды қолдана отырып жасалған қылмыстар жатады. Қол сұғу объектісіне және объектісіне байланысты отандық және шетелдік қылмыстық заңда қарастырылған барлық компьютерлік қылмыстарды екі топқа бөлуге болады:

1. Компьютерлік ақпарат саласындағы қылмыстар. Мұндай қылмыстардың тақырыбы Компьютерлік ақпарат болып табылады, мысалы, ҚР ҚК 227, РФ ҚК 272-274-баптарында, Украина ҚК 361-363-баптарында, §1030 (a)(1) АҚШ заңдарының жиынтығы "ұлттық қауіпсіздікке, халықаралық қатынастарға, атом энергетикасына қатысты қол жетімділігі шектеулі ақпаратқа рұқсатсыз қол жеткізу", Австралия ҚК 478.1-бабы "қорғалатын компьютерлік ақпаратқа немесе бағдарламаға рұқсатсыз қол жеткізу немесе модификациялау" және тағы басқа.

2. Компьютерлік ақпарат басқа қылмыс жасау құралы немесе құралы болып табылатын қылмыстар. Қылмыстардың бұл құрамдары Қылмыстық кодекстердің басқа тарауларында, мысалы, Беларусь Республикасы ҚК-нің 212-бабында "компьютерлік техниканы пайдалану арқылы ұрлау"; §1030(a)(7) АҚШ заңдарының жинағы "компьютерді пайдалана отырып қорқытып алу, зиян келтіру қаупі"; Канада ҚК-нің 206(1)(e) - бабында "қаржы пирамидаларын құру жолымен пайда табу мақсатында компьютерлік деректер мен технологияларды пайдалану" және басқалары. Ресей Федерациясының Қылмыстық кодексіне сәйкес, осы топтың қылмыстары үшін жауапкершілік кодекстің басқа баптарына сәйкес, олардың жалпы және тікелей объектілеріне сәйкес келуі керек. Алайда, қажет болған жағдайда мұндай әрекеттер Ресей Федерациясының Қылмыстық кодексінің 272-274-баптарында көзделген қылмыстармен бірге саралануы мүмкін. Өкінішке орай, Қазақстан Республикасында қылмыстық кодекстің компьютерлік техниканы немесе олардың қосымша құрылғыларын пайдалану туралы баптары жоқ.

Мұндай қылмыстардың бірқатары У.В. Зининаның ғылыми жұмысының мысалында, сондай-ақ А.Т.Нұғманова мен Т.Б.Сеитовтың еңбектерінде келтірілген [46, 14 б.].

Отандық ғылыми еңбектерінің жеткіліксіздігі, компьютерлік ақпарат саласындағы талдау, шетелдік арнайы ғылыми еңбектер мен ғылыми әдебиеттерді, кітаптар мен оқу құралдарын қарастыру қажеттілігі бар. Талдау негізінде компьютерлік қылмыстарды жасаудың 20-дан астам әдісін және киберқылмыстарға қатысты қылмыстық әрекеттердің 40-қа жуық түрін ажыратуға болады. Бұл сандар өсу жағына қарай типтік белгілерге, жалпы

белгілерге, қылмыскерлердің қылмыс жасауының комбинациясына, жаңа технологиялардың дамуына, сондай-ақ қылмыстық әрекеттер алгоритмдерінің логикалық өзгеруіне байланысты өзгеруі мүмкін.

Осыған байланысты компьютерлік қылмыстарды 5 негізгі топқа бөлуге болады, оны әйгілі ғалым-заңгер, көптеген монографиялар мен ғылыми еңбектердің авторы, сонымен қатар компьютерлік қылмысқа арналған диссертация Ю.М. Батурин жасаған. Бұл негізгі топтарға мыналар жатады:

* компьютерлік техникалық құрылғылар мен аспаптарды ұрлау;
* компьютерлік ақпаратты көшіру және қайта бағыттау;
* компьютерлік техникалық құрылғыларға заңсыз қол жеткізу;
* ақпараттық және басқарушы топтарды басқару;
* кешенді әдістерді қолданатын әрекеттер [47, 81 б.].

Отандық аренада ҚР Президенті өзінің ақпараттық қауіпсіздік тұжырымдамасында қылмыс жасаудың жақсы тәсілдері мен түрлерін келтіреді, бұл қазіргі уақытта өзінің практикалық жалғасын таппады. ҚР Президентінің 2006 жылғы 10 қазандағы "Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы" Жарлығында ҚР Қылмыстық кодексінде де, отандық қайраткерлердің бірде-бір ғылыми еңбегінде де бұрын толық көрсетілмеген қылмыстар, қылмыс жасау тәсілдері мен қылмыстық іс-әрекеттер көрсетілген.

Компьютерлік ақпарат саласында қылмыс жасау әдістерінің, әдістерінің, түрлерінің үлкен тізімінен бірнеше негізгі бөлуге болады:

* уақтылы емес ақпараттық хат алмасу немесе мекен-жай қатесі, ақпаратты заңсыз жинау және пайдалану;
* ақпарат пен ақпараттық ресурстарға заңсыз қол жеткізу, компьютерлік ақпаратты заңға қарсы жою, өзгерту және көшіру;
* ақпаратты заңсыз манипуляциялау немесе ақпаратқа әсер ету (дұрыс емес ақпарат, ақпаратты өзгерту немесе жасыру);
* ақпараттық жүйелердегі мәтіндерді заңсыз көшіру;
* БАҚ-ты адамның, қоғамның және мемлекеттің мүдделеріне қарсы пайдалану;
* кітапханалардан, мұрағаттардан және деректер базасынан ақпаратты ұрлау;
* ақпаратты өңдеу технологиясының бұзылуы;
* вирус бағдарламаларын жасау және тарату;
* бағдарламалық және ақпараттық перифериялық құрылғыларды орнату;
* байланыс пен ақпаратты өңдеу құрылғыларын жою және бұзу;
* машиналық және басқа да ақпараттық тасығыштарды жою, бұзу және ұрлау;
* ақпаратты қорғаудың криптографиялық құралдарын ұрлау, бағдарламалық немесе ақпараттық кілттерді, парольдерді ұрлау;
* байланыс желілері мен байланыс желілерінде жалған ақпаратты жіберу, шифрлау және қайта бағыттау;
* пайдаланушыларға жалған, толық емес немесе дұрыс емес ақпаратты қасақана немесе ұқыпсыз ұсыну;

* компьютерлік ақпарат саласындағы басқа да құқыққа қарсы әрекеттер [48].

Шетелдік және халықаралық қылмыстық заңнамада ұқсас қылмыс құрамын сипаттау кезінде "рұқсатсыз қол жеткізу"термині қолданылады. Көптеген заңгерлердің пікірінше, бұл термин қылмыстық заңмен тыйым салынған әрекетті сипаттау үшін дәлірек, өйткені ақпаратқа қол жеткізудің заңдылығы оның ақпарат иесінің санкцияланғанын (рұқсат етілгенін) білдіреді.

Компьютерлік ақпаратқа заңсыз қол жеткізудің бірнеше тәсілдері бөлінеді: тікелей қол жеткізу тәсілдері; жанама (қашықтан) қол жеткізу тәсілдері; қол жеткізудің аралас тәсілдері. Бүкіл әлемде компьютерлерге, жүйеге немесе компьютерлік желіге қашықтан қол жеткізу арқылы жасалатын қылмыстық әрекеттердің үлесі компьютерлік қылмыстардың жалпы санында тұрақты өсуді жалғастыруда және мамандардың бағалауы бойынша шамамен 39,2% құрайды [44, 64 б.].

Сот практикасынан алынған мысалдар ретінде тергеу және сот органдарының Интернет желісіне заңсыз қосылуы ҚР ҚК 227-бабы бойынша қылмыс ретінде жиі сараланатынын көрсетеді, бірақ қашықтан қол жеткізуді пайдалану арқылы ғана. Интернетке қосылған кезде біреудің аты мен паролі қолданылады, сондықтан бұл қол жеткізу заңсыз деп саналады. Сонымен бірге, бұл мәселені зерттеген көптеген авторлар құқық қолдану практикасында мұндай көзқараспен келіспейді. Мұндай жағдайларда Интернетке заңсыз қосылу биллинг жүйесіндегі статистикалық ақпараттың өзгеруіне әкеледі. Биллинг жүйесі (яғни есеп айырысудың автоматтандырылған жүйесі) байланыс қызметтерін тұтынуды есепке алуға, осындай қызметтер үшін есеп айырысуларды басқаруға, байланыс операторы осы қызметтерді көрсететін абоненттер туралы ақпаратты сақтаумен бір мезгілде қызметтердің өзін басқаруға арналған бағдарламалық-аппараттық кешен болып табылады [49].

Автоматтандырылған жүйенің өзі белгілі бір субъектінің абоненттің деректерін енгізгенін немесе енгізбегенін анықтай алмайды. Осылайша, компьютерлік ақпарат саласындағы қылмыстың ресми статистикасына құқық қолдану органдарының ҚР Қылмыстық Заңында көзделген қылмыс құрамының элементтерін кеңінен түсіндіруді, сондай-ақ телекоммуникациялық қызметтердің жұмыс істеуінің техникалық шарттарын түсінбеуді куәландыратын қылмыстық заңды толығымен дұрыс қолданбау жағдайлары енгізіледі. Бүгінгі таңда зиянды бағдарламалардың ең көп таралған түрлері: компьютерлік вирустар, трояндық бағдарламалар, желілік құрттар. Сондай-ақ, бұл жүйеде зомби деп аталатын компьютерлер бар, олар рұқсат етілмеген және қашықтағы пайдаланушыларға (хакерлерге) вирус жұққан компьютерлерден спам жіберуге немесе әртүрлі интернет-сайттарға немесе ақпараттық жүйелерге үйлестірілген Dos шабуылдарын жасауға мүмкіндік беретін шексіз қол жетімділікті қамтамасыз етеді. Мамандардың айтуынша, қазіргі уақытта барлық спамның 50%-дан астамы зомби желілерінің көмегімен жіберіледі. 2007 жылы зомби-компьютерлердің саны 2006 жылмен салыстырғанда 29% - ға өсіп, 6 млн.жуықты құрады, ал оларды бақылайтын серверлердің саны, керісінше,

төмендеді [50].

ТМД және Балтық елдерінің, сондай-ақ Қазақстанның, сондай-ақ басқа да көптеген еуропалық мемлекеттердің Қылмыстық заңдарында ЭЕМ-ді пайдалану ережелерін бұзу сияқты қылмыс мүлде көзделмеген (мысалы, Ұлыбританияда, АҚШ-та, Жапонияда, Эстонияда және басқаларында). Объективті жағынан, бұл қылмыс компьютерді, олардың жүйесін немесе желісін пайдалану ережелерін бұзудан тұрады, яғни.ЭЕМ-ге қол жеткізе алатын адам басшылыққа алатын ережелерді орындамау немесе тиісінше орындамау. Ережелерді бұзу іс-әрекет түрінде де, әрекетсіздік түрінде де жасалуы мүмкін, мысалы, компьютерлердің қалыпты жұмыс істеуін қамтамасыз ету үшін белгіленген ережелерді сақтамау. Мұндай ережелердің екі түрі бар:

1) ЭЕМ дайындаушылар әзірлейтін және ЭЕМ-мен бірге жеткізілетін ережелер;

2) ақпарат иеленуші немесе ақпараттық жүйелер операторы белгілейтін қағидалар қамтылуға тиіс.

Компьютерлік қылмыстың, оның ішінде компьютерлік ақпарат саласындағы қылмыстардың өсуі және оған қарсы күреске бағытталған қылмыстық-құқықтық және қылмыстық іс жүргізу рәсімдерін жасауға мемлекеттердің келісілген тәсілінің қажеттілігі 1997 жылы Еуропа Кеңесінің Министрлер комитетінің киберкеңістіктегі қылмыс жөніндегі сарапшылар комитетінің құрылуына әкелді. Осы жұмыстың нәтижелері бойынша 2000 жылы Еуропа Кеңесінің киберқылмыс жөніндегі конвенциясының жобасы әзірленді. Конвенция 2001 жылғы 23 қарашаға дейін Будапештте қол қоюға ашылды және 2004 жылғы 18 наурызда күшіне енді. 2007 жылғы 7 сәуірдегі жағдай бойынша Конвенцияны 19 мемлекет ратификациялады. Киберқылмыс туралы Еуропалық Конвенция-бұл әртүрлі құқық салаларының нормаларын қамтитын кешенді құжат: қылмыстық, қылмыстық іс жүргізу, авторлық құқық, Азаматтық, ақпараттық. Конвенцияда бұрын қабылданған халықаралық құжаттарда пайдаланылған "компьютерлік қылмыс" немесе "компьютерлік технологияларды пайдалануға байланысты қылмыс" ұғымдарының анықтамасы берілмейді. Құжатта "киберқылмыс" ұғымы пайдаланылады, оның мазмұны тізбенің көмегімен ашылады, оған мыналар кіреді: 1) компьютерлік ақпаратқа қарсы бағытталған әрекеттер (қылмыстық қол сұғу нысанасы ретінде); 2) заңмен қорғалатын өзге де игіліктерге қол сұғатын әрекеттер, бұл ретте ақпарат, Компьютерлер және т.б. мысалы, оларды жасау құралы не оларды жасау немесе жасыру тәсілінің құрамдас бөлігі ретінде әрекет ете отырып, олардың объективті жағының элементтерінің бірі болып табылады.

Осы Конвенцияны 2006 жылғы қаңтарда Франция ратификациялады, содан кейін 2006 жылғы қыркүйекте АҚШ, Қазақстан Ресей сияқты конвенцияны ратификациялауды кешірек уақытқа кейінге қалдырды [51].

Бүгінгі таңда компьютерлік қылмыстарға қарсы іс-қимылдың келісілген шараларын әзірлеу кезінде халықаралық деңгейде келесі мәселелерге ерекше назар аударылады:

а) компьютерлік қылмыс жасаған құқық бұзушыны анықтау және

сәйкестендіру;

б) жіберілетін хабарламалардың мазмұнына қол жеткізу;

в) дәлелдемелерді жинау саласындағы халықаралық ынтымақтастық және егер бір елдің құқық қорғау органдарының қызметкері дәлелдемелерді алу үшін басқа елдегі компьютерге кіруді талап еткен жағдайда көмек көрсету (яғни "трансшекаралық жедел-іздестіру іс-шаралары»);

г) мемлекеттік органдар мен бизнес қоғамдастықтың тиісті мүдделі өкілдері (мысалы, интернет-провайдерлер) арасында ынтымақтастық орнату.

Қазақстанда киберқылмыстарды, сондай-ақ ақпараттық технологияларды пайдалана отырып жасалатын қылмыстарды анықтау, жолын кесу және ашу жөніндегі жұмысты 2003 жылы ІІМ құрылымында құрылған "К"басқармасы жүзеге асырады. Ақпараттық қылмыстармен жүйелі күрес үшін 2006 жылы ақпараттық технологиялар саласындағы қылмыстармен күрес бойынша ұлттық байланыс пункті құрылды, ол ТМД елдерімен және алыс шет елдермен тұрақты ақпарат алмасуды жүзеге асырады.

Ақпараттық қауіпсіздік саласының білікті кадрлық қамтамасыз етілуі ақпараттық құқық бұзушылықтарға қарсы күрестің нәтижелілігіне әсер ететін негізгі факторлардың бірі болып табылады. Ақпараттық қауіпсіздікті қамтамасыз ету және киберқылмыспен күрес саласында жұмыс істейтін мамандарды оқыту, олардың біліктілігін арттыру процестері мен тәсілдерін жетілдіру талап етіледі.

Ақпараттық қылмысқа қарсы іс-қимылдың тиімділігіне көптеген елдерде, оның ішінде Қазақстанда да ақпараттық саланы құқықтық қамтамасыз етудің жетілмегендігі әсер етеді. Бірақ соңғы бірнеше жылда Қазақстан ақпараттық қатынастармен байланысты мәселелерді реттеу саласында заңнамалық реформа жүргізді, бірқатар нормалар бойынша ҚР Қылмыстық кодексіне жасалған іс-әрекеттер әсіресе сәтті және уақтылы криминализацияланды. 2014 жылғы 3 шілдеде қабылданған ҚР жаңа Қылмыстық Кодексінде, отандық Заңтану тарихында алғаш рет киберқылмыстарға арналған тұтас тарау пайда болды.

"Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар" деген жеке тарау бөлінді, ол 205-тен 213-б.қоса алғанда 9 жеке баптан тұрады [52].

205-бап. Ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге заңсыз қол жеткізу.

206-бап. Ақпаратты заңсыз жою немесе өзгерту.

207-бап. Ақпараттық жүйенің немесе ақпараттық-коммуникациялық желінің жұмысының бұзылуы.

208-бап. Ақпаратты заңсыз иелену.

209-бап. Ақпаратты беруге мәжбүрлеу.

210-бап. Зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату.

211-бап. Қолжетімділігі шектеулі электрондық ақпараттық ресурстарды заңсыз тарату.

212-бап. Құқыққа қайшы мақсаттарды көздейтін интернет-ресурстарды

орналастыру үшін қызметтер көрсету.

213-бап. Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абоненттің сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгерту үшін бағдарламаларды жасау, пайдалану, тарату.

Осы баптар бойынша жаза айыппұл салу тұрғысынан да - 200 - ден 3000 АЕК-ке дейін, сондай-ақ бас бостандығынан айыру мерзімдері бойынша-2 жылдан 5 жылға дейін өзгереді.

Олардың кейбіреулері сол нормаларды бөлек бөлгенімен бұрын 1997 жылғы ҚР ҚК 227-бабында кодификацияланған [45].

Бірақ соған қарамастан, осы нормалардың құрамында аздап өзгеріс болды. Мысалы," ақпаратты беруге мәжбүрлеу " деген атау, әрине, екіұшты түсінікке ие, бірақ заңнамадағы мұндай ұсақ олқылықтар орын алуы мүмкін, дегенмен біз бұл тарауды жаңа, әлеуметтік қажетті нормалармен жақында жетілдіруге және толықтыруға үміттенеміз. Бұрын Қазақстандағы ақпараттық қылмыстар экономикалық қылмыстар ретінде және олардың құрамында қаралған, Өзбекстанның қылмыстық заңнамасында да ұқсас проблема байқалады: "ақпараттандыру ережелерін бұзу" қылмысының құрамы (174-бап) меншікке қарсы қылмыстарға жатқызылған және Өзбекстан ҚК-нің "Бөтен мүлікті ұрлау" тарауында көзделген [53].

ТМД елдерінің және посткеңестік кеңістіктегі кейбір мемлекеттердің қылмыстық заңнамасындағы киберқылмыстардың жалпы нысаны әртүрлі жолдармен шектелген. Ресейдің (28-тарау, 272-274-баптар), Әзірбайжанның (30-тарау, 271-273-баптар), Қырғызстанның (28-тарау, 289-291-баптар), Түркіменстанның (33-тарау, 333-335-баптар), Арменияның (9-бөлім. 24 – тарау, 251-257-баптар) және Эстония ("компьютерлік ақпарат саласындағы қылмыстар", 268-274-баптар) жеке тарауларда компьютерлік ақпарат саласындағы қылмыстар үшін қылмыстық жауапкершілік туралы нормалар біріктірілген (компьютерлік Ақпарат қауіпсіздігі-Армения Қылмыстық кодексі). Беларусь Республикасының қылмыстық заңнамасы (XII бөлім. 31-тарау, 349-355-баптар) және Тәжікстан (XII бөлім, 298-304-баптар) киберқылмыстардың тектік объектісі ретінде қоғамдық қауіпті іс-әрекеттерді "ақпараттық қауіпсіздікке қарсы қылмыстар"тарауына (бөліміне) біріктіре отырып, ақпараттық қауіпсіздікті көздейді. Грузия ҚК бойынша қылмыстық-құқықтық қорғалуға жататын киберқылмыстардың рулық объектісін анықтауда қиындықтар туындайды (35-тарау.

"Компьютерлік қылмыстар", 284-286 баптар) және Молдовалар ("информатика саласындағы қылмыстар" тарауы, 259-261 баптар). Украинаның Қылмыстық кодексінде жалпы объект XVI бөлімде компьютерлерді (компьютерлерді), жүйелер мен компьютерлік желілерді және әлеуметтік қауіпті әрекеттерді пайдалану саласындағы қатынастар ретінде анықталған. "ЭЕМ (компьютерлер), жүйелер мен компьютерлік желілерді пайдалану саласындағы қылмыстар" (Б. 361-363, 361-1, 361-2, 361-3) [54].

Көптеген еуропалық күш-жігерде (Германия, Франция, Нидерланды,

Италия және т.б.) Заңнамалық база да әр түрлі, Германия Қылмыстық кодексінде, мысалы, "ақпараттық алаяқтық" атты мақала бар, ал Франциядағы көрші елде мұндай қылмыстық іс заңмен қарастырылмаған. Талдау көрсеткендей, киберқылмыс үшін жауапкершілік саласындағы мемлекеттердің ұлттық қылмыстық заңнамасы салыстырмалы әртүрлілікпен сипатталады. Жоғарыда аталған мемлекеттерде киберқылмыспен күрес жөніндегі ұлттық заңнаманың дамуы мен өзгеруі киберқылмыстың пайда болуы мен үрдістеріне байланысты және егжей-тегжейлі талдау кезінде тек кейбір заңдылықтарды анықтайды. Ақпараттық технологияларды жетілдіру және олардың адам өмірінің өсіп келе жатқан салаларына енуі қылмыстық қол сұғушылықтың жаңа түрлерінің пайда болуына және олармен күресудің тиімді шараларын жасау қажеттілігіне әкеледі, бұл өз кезегінде жаңа әрекеттерді криминализациялауға, қолданыстағы қылмыстық заңнамаға өзгерістер енгізуге және жаңа нормаларды қабылдауға әкеледі. Егер әрекет бір елдің заңнамасында криминализацияланған болса, ал екінші елдің заңнамасында қылмыстық жауапкершілік көзделмесе, киберқылмыспен күресте тиімді халықаралық ынтымақтастық мүмкін емес екені даусыз. Елдердің ұлттық қылмыстық заңнамасында біркелкіліктің болмауы киберқылмыспен тиімді күрес әдістерінің дамуына теріс әсер етуі мүмкін-бұл үшін мемлекеттік шекаралар жоқ құбылыс. Ғаламдық ақпараттық желілердің болуы ақпараттық кеңістіктің шекараларын бұлдыратады, ал мемлекеттер арасындағы" виртуалды " шекараларды киберкеңістіктің кез-келген жерінде, мемлекеттердің юрисдикциясына қарамастан, компьютер мен Интернетке қол жеткізе отырып, киберқылмыскерлер оңай кесіп өтеді. Егер қылмыстарды тергеу, құқық бұзушыларды ұстап беру, оларды сотта қудалау елдердің ұлттық қылмыстық заңнамасындағы айырмашылыққа байланысты қиын болса немесе тіпті мүмкін болмаса, ақпараттық қылмысқа оның трансшекаралық сипатын ескере отырып, тиімді қарсы тұру мүмкін емес. Шын мәнінде, бұл айырмашылықтар киберқылмыскерлерді қудалаудан қорғайды, олар үшін өзіндік "кедергі" бола отырып, олардың әрекеттерін жазасыз қалдырып, жауапкершіліктен кетуге мүмкіндік береді. Нәтижесінде өз азаматтарын киберқылмыскерлерден қорғауға күш салған мемлекеттер оларды ысырап етеді.

Екінші жағынан, ақпараттық технологиялар саласындағы қатынастарды қылмыстық-құқықтық реттеудің айырмашылығына байланысты өз мемлекетінің заңдарын ұстанатын адамдар басқасында қылмыстық қудалауға ұшырауы мүмкін. Мұндай жағдай киберқылмыстарға қарсы күрестің халықаралық стратегиясын әзірлеу және ақпараттық технологиялар саласындағы қатынастарды қылмыстық-құқықтық реттеу саласындағы ұлттық заңнаманы біріздендіру қажеттілігін негіздейді.

Қылмыстық-құқықтық саладағы талданған қатынастарды заңнамалық реттеу компьютерлік ақпараттық технологиялардың қарқынды дамуынан артта қалатынын мойындауымыз керек. Киберқылмыс үшін жауапкершілік туралы қылмыстық заңнаманың қазіргі жағдайы адамзаттың ақпараттық дамуының үздіксіз, қарқынды процесі жүріп жатқан сәттен бастап киберкеңістіктегі

жаһандық өзгерістерді толық көрсетпейді. Қылмыстық заңнама ақпараттық қылмыстар жасау кезінде қалыптасқан қатынастарды тиімді реттемейді, соның салдарынан оның қорғау және алдын алу функциялары іске асырылмайды. Қазақстанның заңнамасында, сондай-ақ ТМД-ның кейбір мемлекеттерінің заңнамасында компьютерлік қылмыстар үшін қылмыстық жауапкершілік көзделген, яғни, компьютерлер мен компьютерлік ақпаратқа қатысты жасалған қылмыстар үшін, бұл ретте оларды пайдалана отырып жасалатын және қылмыстық-құқықтық қорғаудың басқа объектілеріне қол сұғатын әрекеттер қылмыстық жауапкершілік аясынан тыс қалады. Қазақстанның қылмыстық заңнамасында бүгінгі таңда ақпараттық қауіпсіздік саласындағы қатынастар "Ақпараттық алаяқтық", "спам тарату", "ақпараттық жалғандық", "адамдарды терроризм мен экстремизмге насихаттайтын және оқытатын ақпараттық материал жасау және тарату", "компьютерлік диверсия" және тағы басқалар сияқты қазіргі заманғы қоғамға қауіпті бірқатар іс-әрекеттерді криминализациялауды талап ететін жағдай қалыптасты, бұл қоғамға қауіпті болып табылады және қазіргі заманғы шындықтағы ақпараттық қатынастардың қазіргі талаптарына жауап береді.

2.2 Қазақстан Республикасындағы киберқылмыспен күрес мәселелері және оларды шешу жолдары

Киберқылмыс проблемасы ақпараттық қоғам дәуірінде, компьютерлер мен телекоммуникациялық жүйелер адам мен мемлекет өмірінің барлық салаларын қамтыған кезде, ғаламдық интернет телекоммуникациялық технологияларды дамытудың ең жылдам бағыттарының бірі болып табылады.

Бүгінде виртуалды кеңістікте жұмыс істейтін қылмыскерлердің құрбандары тек адамдар ғана емес, бүкіл мемлекеттер болуы мүмкін. Сонымен қатар, мыңдаған пайдаланушылардың қауіпсіздігі бірнеше қылмыскерлерге байланысты болуы мүмкін. Зиянды бағдарламаларды тарату, несие карталарының нөмірлерін және басқа да банктік деректемелерді ұрлау, құқыққа қарсы ақпаратты тарату, діни экстремизмді насихаттау, терроризмді қаржыландыру, Қылмыстық жолмен алынған кірістерді жылыстату мемлекеттік инфрақұрылымның бұзылуына әкеп соғады.

Құқық қорғау жүйесі мен сараптама мекемелерін қазіргі заманғы техникалық жарақтандырудың болмауына байланысты киберқылмыс құқық қорғау және өзге де құзыретті органдардың қолынан келмейді және жеке адамдарға немесе ұйымдарға ғана емес, экономиканың өмірлік маңызды салаларын компьютерлендірудің айтарлықтай деңгейіне жеткен кез келген елдің әлеуетті – ұлттық қауіпсіздігіне тікелей қауіп төндіреді.

Киберкеңістікте жасалған қылмыстар саны компьютерлік желілерді пайдаланушылар санына пропорционалды түрде өсуде.

Ғылым мен техниканың жетістіктерін қылмыстық мақсатта пайдалану мәселесі интегративті процестердің маңызды бағыттарының бірі - жердің әртүрлі нүктелерінде орналасқан миллиондаған компьютерлерді біріктіретін

Интернет желісінің халықаралық және ғаламдық нысанын құрумен байланысты. Ақпарат алу және оны бөлісу үшін кең мүмкіндіктер ашқан Дүниежүзілік Интернет өте жылдам қарқынмен дамуда. 1990 жылдардың аяғында, кейбір болжамдар бойынша, 2005 жылы бүкіл әлемде шамамен 1 миллиард компьютер интернетке қосылады деп күтілген және бұл өте үлкен сан болып көрінген. Алайда, нәтижелер тіпті күткеннен де асып түсті - 2008 жылы Интернетті пайдаланушылар саны 1,5 млрд. адамды құрады - бұл жер халқының төрттен бір бөлігі, ал 2013 жылы виртуалды кеңістікке жердің үштен бір бөлігі (2,2 миллиард) [55].

1. Кәсіби компьютерлік қылмыскерлер қылмыстың объектісі ретінде анонимділік қаупі тұрғысынан әсіресе осал болып табылатын ірі компаниялардың жергілікті желілері мен серверлерін таңдайтынын атап өткен жөн. Шоттың орталық серверінің болмауына байланысты, әдетте, құқық қорғау органдары тиісті тергеу жүргізу үшін күдікті операциялардың сызбаларын қадағалап, анықтай алатын клиенттер туралы атаулар немесе басқа ақпарат жоқ. 2017 жылдың соңында Қазақстандағы ұйымдар мен жеке тұлғалардың 81% - ы кибершабуылдарға ұшырады. Кибершабуылдардың жиілеп кетуі интернеттегі операцияларды жүргізу кезінде қауіпсіздікке алып келді[56, 8 б.].

Киберқылмыскерлердің жіктемесін беретін алғашқы халықаралық құжат 2001 жылғы 23 қарашада Еуропа Кеңесі қабылдаған киберқылмыс туралы Конвенция болып табылады, 2005 жылдың соңына қарай киберқылмыс туралы конвенцияға Еуропа Кеңесіне мүше 38 ел, сондай – ақ АҚШ, Канада, Жапония және ОАР қол қойды. Ресей де осы халықаралық келісімге қосылуға ниет білдірді, бірақ кейіннен Конвенцияға қосылудан бас тартты, өйткені Ресей компьютерлік жүйелерге трансшекаралық қол жетімділіктің қолайлы шарттары туралы келісе алмады.

Бұл халықаралық құжатта киберқылмыскер мен оның құрбаны әртүрлі мемлекеттерде тұрып, әртүрлі заңдарға бағынатын жағдайдағы құқық қорғау органдарының өзара іс-қимылының проблемалық мәселелері көрсетілген. Халықаралық келісімде интернет-провайдерлер клиенттерінің киберқылмыстарды тергеу кезінде қажет болған жағдайда жеке ақпаратын сақтау мәселелері жазылған. Конвенция түрлі мемлекеттердің құқық қорғау құрылымдары арасындағы тығыз кооперацияны көздейтін киберқылмыспен күресті күшейтуге бағытталғандықтан, ол қатысушы мемлекеттердің құқық қорғау органдарына кең өкілеттіктер береді [57, 21 б.].

Көптеген елдерде, соның ішінде посткеңестік елдерде (Ресей, Молдова, Грузия, Украина, Әзірбайжан) киберқылмыспен күрес туралы ұлттық заңнама бар. Біздің елімізде 2011 жылғы сәуірде күші жойылған ҚР Президентінің 2006 жылғы 10 қазандағы № 199 "Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы" Жарлығы бес жылдан астам уақыт бойы қолданыста болды.

"Қазақстан үшін өзекті талап ақпараттық қауіпсіздіктің ұлттық доктринасын әзірлеу болып табылады, ол ақпараттық еркіндік пен қауіпсіздікті қамтамасыз етудің шекаралары мен шарттарын қарайтын, қазіргі қазақстандық

қоғамның ақпараттық саласындағы теріс үрдістерді еңсеру міндетіне қызмет ететін базалық тұжырымдамалық құжат болуы тиіс"деп санайтын авторлармен ынтымақтасамыз[58, 17 б.].

Қазақстанды неғұрлым кибер-криминогендік елдерге жатқызуға болмайды, өйткені ақпараттық технологиялар саласында жасалатын қылмыстардың жалпы қылмыстық құқық бұзушылықтар санынан үлесі 5% - ды ғана құрайды. Бұл қылмыстарға Астана, Алматы, Қарағанды сияқты ірі қалалар ұшырайды, өйткені мұнда әртүрлі меншік нысандары бар көптеген қаржы және банк мекемелері, оқу орындары, өнеркәсіптік кәсіпорындар мен мекемелер шоғырланған.

Киберқылмыспен күресу үшін Алматы қаласында осыдан он екі жыл бұрын "К"бөлімі деген атқа ие болған жедел бөлімше құрылды. Бұл бөлімшеде IT-технологияларды пайдаланатын жоғары білікті жедел қызметкерлер қызмет атқарады. Мұндай мамандар хакерлердің ізіне оңай түсе алады. Сонымен қатар, осы бөлімшенің негізінде құқық қорғау қызметінің қызметкерлері дайындықтан өтеді.

"К" полиция бөлімі шетелдік сайттармен жұмыс істемейді, олардың жұмысы отандық сайттармен шектеледі, сондықтан олардың қызметінің нәтижелері соншалықты маңызды болып көрінбеуі мүмкін. 2015 жылы "К" бөлімінің мамандарымен Авторлық және сабақтас құқықтар саласында 47 қылмыстық құқық бұзушылық ашылды, порнографиялық өнімдерді сатудың екі фактісі бойынша, техникалық байланыс құралдарын таратудың екі фактісі бойынша, қатыгездікке табынуды насихаттау фактісі бойынша және интернет-алаяқтық пен ақша қаражатын ұрлаудың бес фактісі бойынша сотқа дейінгі іс жүргізу жүргізілді. Компьютерлік ақпарат саласында ашылған қылмыстық құқық бұзушылықтардың аз ғана саны мұндай қылмыстық құқық бұзушылықтардың сирек жасалатынын білдірмейді. Компаниялар өздерінің IT-инфрақұрылымына шабуылдар туралы хабарлауға міндетті елдерге қарағанда, біздің республикамызда компаниялар беделін жоғалтпау үшін мұндай шабуылдар туралы жиі үндемейді.

Қазіргі уақытта адамзат терроризмнің өсуіне тап болды. Бұл жерде деструктивті күштерді қаржыландырумен және шетелдік террористік ұйымдармен байланыстармен күрес мәселелері түйінді болып табылады. Интернетте және әлеуметтік желілерде діни экстремизмді насихаттаудың алдын алу бойынша жұмыс жүргізу қажет. Ұйымдастырушылық іс-шараларға діни экстремизмді, терроризмді, қатыгездік пен зорлық-зомбылықты насихаттайтын еркін айналымда тыйым салынған өнімдер мен ақпаратты анықтауға бағытталған бірлескен профилактикалық іс-шаралар жатады.

Біздің республикамыздың прокуратура органдарының қызметкерлері киберқылмыс мемлекеттің іргетасына нұқсан келтіретінін атап өтті. Елдің банк жүйесін тұрақсыздандыруға бағытталған бірқатар банктердің қаржылық жағдайына қатысты арандатушылық SMS-шабуылдардың мысалдары келтіріледі. Осы іс-әрекеттердің нәтижесінде жүйе құрушы банктерге елеулі зиян келтірілді, бұл қоғамдағы әлеуметтік шиеленістің өсуіне әкелді, сондай-ақ

халықтың елдің қаржы институттарына деген сеніміне нұқсан келтірді [59, 17 б.].

"Киберқылмыс-бұл тек спам, вирустар, ботенттер және DOS - шабуылдар ғана емес, сонымен қатар банктік шоттар туралы ақпаратты ұрлайтын банктік инсайдерлері бар қылмыстық топтар бар, оларды кейіннен олардың серіктестері интернетте сатады. Бұл топтар үшін географиялық шекаралар жоқ. Мұндай құбылыстармен күресу үшін тиісті нормативтік база қажет".

Компьютерлік желілердің қарқынды дамуы және олардың адам қызметінің әртүрлі салаларына енуі, жоғарыда айтылғандай, қылмыстық шабуылдардың сипатын өзгертті және олардың жаңа формаларын тудырды. Сонымен қатар, қазіргі уақытта ең өзекті қауіптер желілердің нақты қызмет салаларына енуіне байланысты болды. Осылайша, XX ғасырдың 60-жылдарында, Компьютерлік желілер негізінен әскери және ғылыми мекемелерде қолданылған кезде, негізгі қауіп құпия ақпараттың жоғалуы, сондай-ақ оған рұқсатсыз қол жеткізу болып саналды. 70 — ші жылдары компьютерлік технологиялар саласындағы экономикалық қылмыс-банктік компьютерлік желілерді бұзу, өнеркәсіптік тыңшылық проблемалары бірінші орынға шықты. 80-ші жылдары компьютерлік бағдарламаларды бұзу және заңсыз тарату кең таралған қылмыстарға айналды. 90-шы жылдары Интернет желісінің пайда болуымен және дамуымен жеке ақпараттың құпиялылығына қылмыстық қол сұғушылықпен, балалар порнографиясын таратумен және экстремистік бағыттағы виртуалды желілік қауымдастықтардың жұмыс істеуімен байланысты бірқатар проблемалар пайда болды [60].

2005-2008 жылдары "боттар" деп аталатын желілердің таралуына байланысты жаңа қауіптер пайда болды — пайдаланушылар білместен шабуыл жасай алатын вирус жұққан компьютерлер. Сонымен қатар, телекоммуникациялық желілердің интеграциясы және олардың конвергенциясы, Интернетке "мобильді" қол жеткізу мүмкіндігінің пайда болуы және желіге қол жеткізу құрылғыларының, оның ішінде "портативті" ұялы телефондардың, коммуникаторлардың жетілдірілуі ақпараттық технологияларды теріс пайдалану үшін жаңа мүмкіндіктер туғызады. Symantec Security киберқауіптер саласындағы қауіпсіздікті қамтамасыз ету жөніндегі халықаралық қызметінің деректері бойынша әлемде әр секунд сайын 12 адам кибершабуылға ұшырайды, ал жыл сайын әлемде 556 млн-ға жуық киберқылмыс жасалады, оның шығыны 100 млрд АҚШ долларын құрайды. АҚШ. Киберқылмыстың Ғаламдық табиғаты оның трансұлттық сипатында да көрінеді: киберқылмыс бір елде дайындалып, жасалады, ал екіншісіне зиян келтіріледі. Осы қылмыстың салдарынан виртуалды кеңістікте немесе киберқылмыс Ұлттық қауіпсіздік саласындағы сарапшылардың ерекше назарына айналады, ал киберқылмыстардың алдын алу және ескерту бұқаралық ақпарат құралдарында, мемлекеттік құжаттарда және ғылыми жұмыстарда айтылады.

Киберқылмыстың алдын алу үшін бұл құбылысты түсіну қажет. Тұжырымдаманы анықтаудан бастайық. Киберқылмыс-бұл Интернетке қол

жетімділігі бар кез-келген техникалық құрал арқылы жеке адамға, ұйымға немесе мемлекетке экономикалық, саяси, моральдық, идеологиялық, мәдени және басқа да зиян келтіру мақсатында әлеуметтік ауытқу актісі. Киберқылмыскерлер өздерінің мақсаттары, әсер ету объектілері, заңсыз әрекеттерді жасау тәсілдері мен құралдары бойынша ерекшеленеді. Біз киберқылмыстарды таңдалған негіздерге сәйкес сипаттаймыз.

Киберқылмыс көбінесе экономикалық мақсаттар үшін жасалады. Бұл, мысалы, ақша ұрлау және құпия ақпарат түрінде экономикалық зиян келтіруі мүмкін. Мақсаттардың басқа түрлеріне саяси-негізгі мемлекеттік және саяси институттарға зиян келтіру, билік қатынастары мен билікке деген сенім жүйесіне нұқсан келтіру жатады. Мақсаттардың үшінші түрі - идеологиялық: интернет-пайдаланушыларды, мысалы, радикалды террористік және ұлтшыл топтардың қатарына тарту мақсатында идеялар мен идеологияларды тарату. Сонымен, біз мақсаттардың төртінші түріне әлеуметтік психологиялық, мысалы, азаматтарға моральдық, психологиялық зиян келтіру жатады. Киберқылмыскерлердің іс-әрекеттері қарапайым азаматтарға, ұйымдарға, мемлекеттік институттарға, олардың жеке ақпараттарына, бостандыққа және жеке киберқауіпсіздікке бағытталуы мүмкін.

Киберқылмыскерлер жұмыс істейтін барлық құралдарды жүйелеу және сипаттау әлі де қиын. Кешегі ақпаратты "тарқату" әдісі қысқа мерзім ішінде ескіреді, себебі кибералаяқтар киберқылмыстар жасау үшін түрлендірілген технологиялық құралдарды пайдаланады. Киберқылмыстың белгілі әдістерінің екі түрін ажыратуға болады: әлеуметтік инженерия (әлеуметтанудағы әлеуметтік инженериямен шатастырмау керек) және вирустық бағдарламалар. Бірінші түрдің ерекшелігі-жеке ақпарат алу үшін адамға телефон немесе компьютерлік шабуыл жасау. Жеке психологияның ерекшеліктеріне жүгініп, алаяқтар басқа адамды алдап, сол арқылы адамды адастырады. Әлеуметтік инженерияны ақпараттық қауіпсіздік саласындағы мамандардың тар тобы адам психологиясының ерекшеліктерін білуге негізделген жеке ақпаратты "ұрлау" тәсілдерін, бопсалауды, сенімді теріс пайдалануды сипаттау үшін қолданады. Жеке ақпарат алудың бұл психологиялық әдісін 1990 - шы жылдары қарапайым алаяқтар кеңінен қолданған, бірақ Интернет арқылы жәбірленушімен жасырын байланыс кибер алаяқтарға үлкен еркіндік береді. Әлеуметтік инженерияның ең көп таралған түрі - алаяқтық fishing (ағылшын тілінен. балық аулау және phone - телефон) немесе сауатсыз интернет пайдаланушыларында олардың құпия деректерін "аулау".

Киберқылмыстың екінші түрінің ерекшелігі - вирустық бағдарламалар - бұл киберқылмыскерлерге "жетілдірілген" заманауи бағдарламалық жасақтаманы қолдана отырып, компьютерлерді қолданушылары білместен қашықтан басқаруға мүмкіндік береді. Оларды боттар деп атайды, ал зиянды кодты жұқтырған Компьютерлер желісі ботнеттер деп аталады. Айта кету керек, қарапайым пайдаланушылардың көпшілігі осы қауіп-қатерлерге қарсы қорғансыз болып қалады және киберқылмыскерлердің кәсіби әрекеттеріне қарсы тұра алмайды. Бұл екі негізгі факторға байланысты. Біріншіден,

қарапайым адамдар өздерін қорғау үшін компьютерлік сауаттылықтың жеткілікті деңгейіне ие емес. Екіншіден, бізде дәстүрлі түрде өз қауіпсіздігімізді қамтамасыз етуге арналған қондырғылар нашар дамыған. Мәселе жалпы орыстарға тән әлеуметтік-мәдени сипатқа ие жеке онтологиялық қауіпсіздіктің жетіспеушілігінде жатыр деп болжауға болады. Э. Гидденс енгізген "онтологиялық қауіпсіздік" (ontological security) ұғымы "жеке өмірге немесе сенімге негізделген субъективті қауіпсіздік сезімін" білдіреді [61].

Анонимділік виртуалды шындықтың басты атрибуты ретінде шын мәнінде басқа коммуниканттарға қатысты бірінші көзқараста көрінетін сенім мен қауіпсіздікке ие. Жеке киберқауіпсіздік туралы субъективті идеяларды виртуалды қылмыскерлер өз мақсаттары үшін пайдаланады. Виртуалды кеңістіктегі ықтимал қылмыстардан қорғауды қамтамасыз ету үшін сізде осы мәселе бойынша азаматтардың қалыптасқан көзқарастары туралы ақпарат болуы керек, ықтимал құрбандар ықтимал кибершабуыл қаупін түсінетіндігін, жеке деректерін сақтау үшін қандай қауіпсіздік шараларына жүгінетінін түсіну керек.

Осы салада жүргізілген әлеуметтанулық зерттеулер жоғарыда айтылғандарды суреттейді және барлық Интернет қолданушылары киберкеңістікте өздерін қорғауға дайын емес және оны қалай жүзеге асыруды білетіндігін анықтайды [62]. 2013 жылы зерттеушілер 12-17 жас аралығындағы 1203 жасөспірімге (Интернетті пайдаланушылардың ең осал тобы ретінде) және олардың ата-аналарына сауалнама жүргізді. Ғалымдар сандық құзіреттіліктің компоненттеріне жатқызды: білім, дағдылар, интернетті пайдалану кезіндегі ынталандыру және жауапкершілік. Зерттеушілер онлайн-тәуекелдермен соқтығысу ықтималдығын арттыратын маңызды фактор қарапайым қауіпсіздік ережелерін сақтамау: бейтаныс адамдармен қарым-қатынас кезінде өзіңіз туралы артық ақпаратты тарату, парольдерді сақтау ережелерін сақтамау деген қорытындыға келді. Жасөспірімдер өздерінің "қарапайым" интернет-мінез-құлқына әкелетін жағымсыз салдарды жиі бағаламайды: музыканы, фильмдерді, онлайн ойындарды, әлеуметтік желілерді жүктеу. Олар интернетті еркін пайдаланудың ықтимал теріс салдарын уақытында кешіктіреді, олар кейінірек, мысалы, жұмысқа қабылдау кезінде пайда болуы мүмкін. Зерттеушілер жастарға интернеттегі қауіпсіз мінез-құлық ережелерін үйрету және желідегі еркін мінез-құлықтың ықтимал қауіптерін түсіндіру қажет деп санайды. Ата-аналар мектепте балаларға интернет-қауіптер туралы хабарлау керек, сонымен қатар оларды заманауи ақпараттық-коммуникациялық технологияларды тиімді пайдалануға үйрету керек деп санаса да, ата-аналардың интернет-жауапкершілік деңгейі өте төмен. Бұл жағдайда адамның өзі өзін және жеке мәліметтерін қорғауы керек пе немесе елдің де, оның азаматтарының да деректерінің сақталуын қамтамасыз ету мемлекеттің жауапкершілігі ме?

Виртуалды қылмыскерлерге тиімді қарсы тұру үшін қарапайым азаматтар мен мемлекеттік институттарды қорғайтын көп деңгейлі институционалды киберқауіпсіздік жүйесі қажет. Киберқауіпсіздік жүйесіне сан алуан компоненттер кіреді, оның ішінде халықтың цифрлық сауаттылық деңгейін

арттыру, жеке ақпаратты қорғаудың жеке тәсілдерін ілгерілетуге жәрдемдесу, киберқауіптерге қарсы іс-қимыл және оның алдын алу тетіктері. Мұндай киберқауіпсіздік жүйелерін құрудың алғашқы әрекеттері АҚШ пен Еуропалық Одақ елдерінде жасалды. Осылайша, американдық киберқауіпсіздік жүйесі интернет-қарақшылыққа тыйым салу актісіне (Stop Online Piracy Act) негізделген. Осы заң жобасына сәйкес қылмыстық құқық бұзушылық деп авторлық құқықпен тыйым салынған контентті түрмеге қамау және айыппұл түрінде жазамен тарату немесе тарату саналады. Интернеттегі кез-келген қатысушы, провайдерлерден, іздеу жүйелерінен және жарнама берушілерден бастап, құқық иесінің кез-келген өтініші бойынша қарақшылық жасады деп айыпталған ресурсқа қызмет көрсетуді тоқтатуға және онымен кез-келген өзара әрекеттесуді тоқтатуға міндетті.

ЕО киберқауіпсіздік жүйесі Еуропа 2020 бастамасына негізделген. ЕО өзінің сандық күн тәртібін (Digital Agenda) кең ауқымды міндеттерді орындау міндеттемесімен анықтады. Міндеттердің бірінші тобы Интернетті одан әрі танымал етуге бағытталған. Мәселен, ЕО - да 2015 жылға қарай интернетті пайдаланушылар санын тиісінше 60% - дан 75% - ға дейін, ал мүгедектер арасында-41% - дан 60% - ға дейін арттыру; ЕО халқының басым бөлігін электрондық үкімет қызметтерін пайдалануға үйрету және онлайн сатып алу үшін төлем жүргізу және т. б. жоспарлануда. Еурокомиссия өзіне алған міндеттердің екінші тобы өз азаматтарының киберқауіпсіздігін қамтамасыз етуге дейін азаяды. ЕО базасында желілер және ақпараттық қауіпсіздік агенттігі (ENISA) құрылды, ол желіні пайдаланушылардың пікірлеріне үнемі мониторинг жүргізеді, осыған сәйкес заңға айналатын және ЕО елдері сақтайтын қабылданған жобаларға түзетулер енгізеді. Мүмкін, осы бастаманың ең қажеттісі-заң шығарушылар жыл сайын саясаткерлермен, IT-мамандармен, ғалымдармен интернетті қауіпсіз пайдалану дағдыларын үйрету және жетілдіру үшін кездесулер өткізеді, осылайша виртуалды мәдениетке үйренеді.

Қазақстан киберқауіптерге қарсы іс-қимыл жөніндегі халықаралық стратегияны әзірлеуді және виртуалды кеңістікті реттеудің бірыңғай халықаралық-құқықтық тетіктерін құруды жақтайды. Осындай тетіктердің бірі-2001 жылы Еуропа Кеңесі аясында қол қою үшін ашылған киберқылмыс туралы Конвенция. Конвенцияға сәйкес киберқылмыстарға мыналар жатады: компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қол жетімділігіне қарсы қылмыстар; балалар порнографиясына және авторлық құқықты бұзуға байланысты құқық бұзушылықтар; компьютерлік технологияларды пайдалану арқылы алаяқтық жасау және т.б. 2007 жылы балаларды жыныстық сипаттағы эксплуатация мен қол сұғушылықтан қорғау туралы ек Конвенциясына қол қою үшін ашылды.

Осылайша, киберқылмыс пен киберқауіпсіздік бірыңғай жаһандық виртуалды кеңістіктің екі амбиваленттілігі екенін атап өтеміз. Осыдан он алты жыл бұрын ақпараттық қауіпсіздік мәселесін негізінен ақпараттық технологиялар саласындағы мамандардың тар тобы түсінді. Нақты инженерлік-техникалық және физика-математикалық мамандықтармен бірге әлеуметтік

ғылымдар тиімді шешімдерді іздеуге қосылды, мысалы киберсоциология. Ақпараттық қауіпсіздіктің жаңа парадигмасы - киберқауіпсіздік парадигмасы пайда болды. Оның институционализациясының барлық белгілері бар: кибер алаяқтармен күресте құқықтық нормалар қалыптасады, киберқауіпсіздік бойынша халықаралық институттар пайда болады, киберқылмыскерлерге қарсы іс-қимылға бағытталған қызметтің жаңа салалары дамуда және т.б. соған қарамастан, киберқылмыспен күресу үшін одан әрі жүйелі талдау, оның ішінде әлеуметтік ғылымдарды тарта отырып, қажет екенін атап өтеміз.

Әрине, Қазақстан да қазірден бастап әрекет ету қажет сын-қатерлерге тап болды. Құқық қорғау органдарының мәліметінше, Қазақстанда киберқылмыстардың саны жыл сайын артып келеді. Азаматтардың дербес деректері, мемлекеттік органдардың құпия деректері, ұялы байланыс, банктік шоттар туралы деректер және тағы басқалары қылмыскерлердің жіті назарында болды. Күрделілік пен жеткіліксіз даму - бұл қылмыстардың интеллектуалды сипаты, оларды тергеу тәжірибесінің болмауы, қылмыстың орны мен уақытын бақылаудың күрделілігі, кибершабуылдарды көрсетудің жаңа технологияларын жеткіліксіз қолдану.

Осыған байланысты Мемлекет басшысының "Әлем. XXI ғасыр" манифесі, онда Нұрсұлтан Әбішұлы тіпті қорғанысты басқарудың электрондық жүйелерінің ықтимал іркілісі салдарынан да жаһандық соғыстың басталу қаупі күшейе түсетінін айтады, бұл киберқылмыс түріндегі жаһандық қатермен күресуге шақыру болып табылады. Бағдарламалау тілі барлығына бірдей қол жетімді емес екенін нақты түсініп, түсіну керек. Басқа біреудің жүйесіне басып кіру қабілетіне ие бола отырып, қылмыскерлер елдің ұлттық қауіпсіздігіне үлкен зиян келтіруі мүмкін. Интернеттің мемлекетаралық шекаралары жоқ, көбінесе қылмыскерлер жүздеген шақырым жерде, басқа елде тұра алады. Бұл қылмыскерлерді тергеу және ұстау процесін қиындатады.

"Интернет-банкинг" электрондық жүйесін пайдалана отырып, кәсіпкерлердің шоттарынан ақша ұрлаумен айналысқан Алматыда анықталған қылмыстық топ көрнекі мысал болып табылады. Тергеу анықтағандай, қылмыскерлер тек Бас прокуратураның атынан ғана емес, Салық комитетінен, Қаржы министрлігінен, ҚР Қаржы министрлігінің Мемлекеттік кірістер комитетінен және түрлі қызметтерден хаттар жіберген. Кәсіпкерлер зиянды бағдарламаны іске қосқаннан кейін оны іске қосты. Содан кейін вирус жұққан компьютерлер мен құпия ақпаратқа қашықтан қол жеткізе отырып, қылмыскерлер ақшаны екінші деңгейдегі банктерде алдын ала ашылған шоттарға аударды.

Кибертерроризм сияқты құбылыс қауіпті тенденцияларға ие. Жаңа және жеткілікті зерттелмеген құбылыс бола отырып, ол ерекше назар аударуға лайық және ерекше көзқарасты қажет етеді. Сонымен қатар, террористердің қатарына жалдау Интернеттің коммуникациялық арналары арқылы жиі жүретіні дәлелденді. Зомбилеу мен бағдарламалаудың ең жаңа технологиялары террористер арнайы жасаған сайттарды таратады.

Кибертерроризм қылмыстың ең қауіпті түрлерінің бірі ретінде бағаланады, бұл ақпараттық қауіпсіздікті қамтамасыз етуде құқық қорғау органдарының танымдық және технологиялық дағдылары мен құзыреттілігінің жаһандық дамуын қажет етті[63].

Ақпараттық технологиялар саласындағы қылмыстарға ақпаратқа және банктік шоттарға рұқсатсыз қол жеткізу, зиянды вирустарды, спамды және заңсыз ақпаратты тарату, сондай-ақ компьютерлік технологиялардың көмегімен басқарылатын жүйелердің жұмысына желілер арқылы араласу сияқты түрлер кіреді. Ақпараттық технологиялардың таралуы мен желілерге қосылған компьютерлер арқылы басқарылатын процестер санының артуымен бүкіл әлемде киберқылмыстың ауқымы мен қауіптілігі артып келеді. 2010 жылы БҰҰ Бас Ассамблеясы киберқылмысты басты мәселелердің бірі деп атады.

Киберқауіпсіздік киберқылмыспен күрес жөніндегі техникалық, ұйымдастырушылық және құқықтық шараларды білдіреді. Киберқылмысқа қарсы тұру үшін бағдарламалық құралдар әзірленуде, ірі компаниялардың құрылымында киберқауіпсіздік бөлімшелері бар. Көптеген елдердің, соның ішінде Қазақстан Республикасының заңнамасында Ақпараттық технологиялар саласындағы құқық бұзушылықтар үшін әкімшілік және қылмыстық жауапкершілік белгіленген. Кейбір жағдайларда киберқылмыскерлер қоғамдық қауіпсіздік пен қоғамық тәртіпке қарсы қылмыстар санатына жатуы мүмкін, кейбір жағдайларда олар арнайы заңдармен жазаланады.

Киберқылмыс қылмыскер мен қылмыстың құрбаны әртүрлі елдерде болған жағдаймен сипатталады, бұл осындай қылмыстармен күресті халықаралық үйлестіруді қажет етеді. Атап айтқанда, 2001 жылғы 23 қарашада Будапештте компьютерлік ақпарат саласындағы қылмыс туралы Еуропа Кеңесінің ETS № 185 конвенциясы қабылданды.

2020 жылы Қазақстанда ақпараттық қауіпсіздікті бұзу бойынша 21 мыңнан астам инцидент анықталды 2021 жылға қарай киберқылмыстың жаһандық шығыны алты триллион АҚШ долларына жетеді[64].

Көрсетілген себеп бойынша бүкіл әлемдегі, оның ішінде Қазақстан Республикасындағы ең өзекті проблемалардың бірі киберқылмысқа қарсы іс-қимыл болып табылады. Мемлекет басшысы 2017 жылғы 31 қаңтардағы Қазақстан халқына Жолдауында осы мәселені зерттеудің өзектілігін растайтын ерекше назар аударды, онда ұлттық қауіпсіздік комитетіне және Үкіметке "Қазақстан киберқалқаны" жүйесін құру тапсырылды[65].

Қазақстанда киберқауіпсіздік бойынша шаралар да мемлекет деңгейінде қабылдануда. 2017 жылғы маусымда ҚР Үкіметі киберқауіпсіздік Тұжырымдамасын ("Қазақстанның Киберқалқаны") бекітті. Тұжырымдаманы іске асыру екі кезеңнен тұрады: бірінші кезең – 2017 жылдан бастап 2018 жылға дейін, екінші кезең-2019-2022 жылдар. Қазір "қалқанды" іске асыру шеңберінде нормативтік-құқықтық база жетілдірілді, ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы және киберқауіпсіздік мәселелері жөніндегі кеңес құрылды. "Оң серпінді одан әрі қамтамасыз ету үшін экономикамызды халықаралық және жергілікті киберқылмыстың өскелең қаупінен қорғау үшін

күш-жігер жұмсау қажет. Дүниежүзілік экономикалық форумның болжамдарына сәйкес, 2022 жылға қарай киберқылмыстардан әлемдік экономикаға келтірілген залал 8 трлн доллардан асуы мүмкін". Зерттеу нәтижелеріне сәйкес, Қазақстан компанияларының 93% – ы сыртқы киберқауіптермен, 87% - ы ішкі қауіптермен бетпе-бет келді. Бизнес үшін ең көп таралған қауіптер спам (респонденттердің 79%-ы оны мультивариативті сауалнамада атап өтті), зиянды бағдарлама (66%), фишинг (25%), шифрлаушылар (18%), корпоративтік тыңшылық (13%), DDoS-шабуылдар (11%) және мақсатты шабуылдар (10%) болды.

Сол жылғы 30 Маусымда Қазақстан Республикасы Үкіметінің № 407 қаулысымен киберқауіпсіздік тұжырымдамасы бекітілді ("Қазақстан киберқалқаны") [7].

Алайда, статистикалық мәліметтерге сәйкес Қазақстан Республикасында ақпараттық технологияларды қолдана отырып жасалған қылмыстарға қарсы іс-қимыл тиісті деңгейде жүзеге асырылмайды [66].

2020 жылдың қараша айында Нұр-Сұлтанда "Hi-tech"операциясы барысында киберқауіпсіздік саласында 155 құқық бұзушылық анықталды. ШҚО полициясына жаңа жылдық мерекелерде 1200-ден астам қоңырау түсті "ҚР Ішкі істер министрлігі киберқылмыстардың, оның ішінде интернет-алаяқтықтың алдын алуға және ашуға бағытталған "Hi-tech" жедел-алдын алу іс-шарасын өткізді. Бірнеше күн ішінде осындай 155 құқық бұзушылық анықталды, бұрын жасалған 161 қылмыс ашылды, олардың негізгі бөлігі интернет-алаяқтық болып табылады» [67].

Халықаралық Электр байланысы одағы Қазақстанның 2018 жылғы жаһандық киберқауіпсіздік индексіндегі орнын 40-шы орынға дейін көтерді, ал бір жыл бұрын ол 83-ші орында болған еді.

Қазақстанның әрбір онынші компаниясы қызметкерлердің іс-әрекеттеріне байланысты корпоративтік деректердің қасақана ағып кетуінен зардап шекті. Зерттеу барысында компаниялардың 75% - ы қаржылық ақпаратты жоғалтудан қорқатыны белгілі болды. Ақпараттық қауіпсіздіктің өзектілігіне байланысты Қазақстанның көптеген компанияларының киберқауіптерге қарсы тұратыны таң қаларлық емес. Респонденттердің 96% жұмыс станцияларын зиянды бағдарламалардан қорғау үшін вирусқа қарсы шешімдерді пайдаланады. 61% бағдарламалық жасақтаманы басқаруға және жаңартуға назар аударады, 55% корпоративтік желіге қосылған сыртқы құрылғыларды басқарады, ал 23% маңызды желілерді бөледі. Бұл ретте компаниялардың тек 20% - ы киберқауіптерге қарсы тұру тұрғысынан корпоративтік желінің сыртқы аудитін жүргізеді. Сондай-ақ, ірі компаниялар DDoS-шабуылдардан қорғау жүйелерін (16%) және ақпараттың жария болуын болдырмау үшін DLP жүйелерін (14%) енгізеді. Қазақстанда кибервирусты жұқтыру деңгейі 8% - ды құрайды. Егер Еуропа, АҚШ және Жапония елдерінде бұл нөлге тең деп санасақ, онда бұл сегіз пайыз бұдан былай оптимистік емес көрінеді.

Қазақстанның Орталық Азияның басқа елдерімен салыстырғанда киберқауіпсіздігі сөзсіз жақсы. Сонымен қатар, ол қазақстандықтардың 74% – ы қарақшылық софтты пайдаланатынын, бірақ бұл - егер жалпы үй пайдаланушылары мен компания туралы айтатын болсақ. Ал көршілес Өзбекстанда компаниялардың 80% - ы қарақшылық бағдарламалық жасақтаманы пайдаланады. "Касперский Зертханасының "деректері бойынша биылғы жылдың алғашқы жеті айында қазақстандық пайдаланушылардың шамамен 6% - ы ұялы телефондарға шабуыл жасаған. Бұдан басқа, Қазақстандықтардың 58% – ы құрылғыларға желіден емес, түрлі алмалы-салмалы тасығыштардан, мысалы, USB-жинақтауыштардан түсетін жергілікті қауіптер деп аталатын шабуылдарға ұшырады. Киберқылмыскерлер ұйымдарға, атап айтқанда, шағын және орта бизнеске көбірек шабуыл жасайтыны туралы ақпарат алаңдата алмайды. Мәселен, 2020 жылғы қаңтар-шілде аралығында Қазақстанда корпоративтік пайдаланушылардың 10% – ы интернеттен киберқауіптерге, ал 39% - ы жергілікті қылмыскерлерге тап болды. Заңды тұлғалардан ақша ұрлау мақсатында 4000 компанияға банктік "трояндар" шабуыл жасады. Зиянкестер келесідей әрекет етті: олар стандартты хабарламалар түрінде компанияға жұқтырған құжаттарды жіберді, мысалы, салықтан немесе дебиторлық берешекті төлеу туралы. Жұқтырған файл болуы мүмкін сондай-ақ, замаскирован және қарапайым түйіндеме. Қаражатты ұрлау төлем тапсырмаларын ауыстыру арқылы жүзеге асырылады, оны компания бірден байқамауы мүмкін.

2020 жылдың бірінші жартыжылдығының қорытындысы бойынша Қазақстанда ақпараттық қауіпсіздікті бұзудың 7,8 мың оқиғасы тіркелді - өткен жылдың ұқсас кезеңімен салыстырғанда (10,4 мың) 25,1% - ға аз. Бұл ретте ағымдағы жылы кибершабуылдардың ең көп саны "карантиндік" сәуірде (1,5 мың инцидент) және мамырда (1,7 мың инцидент) байқалады. Пандемия кезінде киберқауіпсіздік маңызды бола бастайды, өйткені көптеген адамдар мәжбүрлі оқшаулау немесе қозғалысты шектеу салдарынан қашықтан жұмыс істейді немесе оқуын жалғастырады. Ағымдағы жылдың 5 шілдесінен бастап Қазақстанда жұқтырудың өсуіне байланысты мемлекеттік комиссия шектеу шараларын енгізу туралы шешім қабылдады. Оның ішінде мемлекеттік органдар, кеңселер, ұлттық компаниялар мен өзге де ұйымдар қызметкерлерінің кемінде 80% - ы қашықтықтан жұмыс істеу нысанын сақтау тапсырылды. Сонымен қатар, жеке ұйымдардың көптеген қызметкерлері қашықтықтан жұмыс істеуге ауыстырылды. Қашықтан жұмыс істеуге жаппай шығу қазақстандықтарды интернеттегі алаяқтыққа осал етеді.

Киберқылмыскерлердің әртүрлі ұйымдардың, соның ішінде ауруханалардың ақпараттық жүйелерін қашықтан өшіруі, сондай-ақ олардың қызмет процестерін бұзуы өте қауіпті. Ағымдағы жылы интернет-ресурсқа қолжетімділіктің болмауына байланысты инциденттер саны едәуір артты: бір жыл ішінде көрсеткіш 2,7 еседен астам, 1,5 мың жағдайға дейін өсті. Сондай-ақ, DDoS - шабуылдардың саны (компьютерлік жүйеге қызмет көрсетуден бас тартуға алып келу мақсатында шабуылдар) айтарлықтай өсті-өткен жылдың

тиісті кезеңімен салыстырғанда 68,8% - ға. Осындай шабуылдардың нәтижесінде заңды пайдаланушыларға, желілерге, жүйелерге және өзге де ресурстарға қызмет көрсету бұзылады немесе толығымен бұғатталады. Мұндай шабуылдардың құрбандары коммерциялық және ақпараттық сайттар. Жақында хакерлер шабуылдың бұл түрін шабуылды тоқтату үшін ақша талап етіп, бопсалау үшін қолданады. Сонымен қатар, фишингтік шабуылдардың өсуі байқалады: жылына 13,8%, 700 жағдайға дейін. Бүгінгі таңда фишинг-әлемде ең көп таралған киберқылмыстардың бірі, оның көмегімен аккаунттар мен банк ақпараты жиі ұрланады [68].

Қазақстанда, ТМД-ға қатысушы жекелеген елдердегідей (Қырғызстан, Өзбекстан) киберқылмысқа қарсы іс-қимылға маманданған дербес тергеу-жедел бөлімшелері жоқ. Қазақстанда тергеу бөлімшелерінен бөлек арнайы органдарда жедел бөлімшелер жұмыс істейді, ал қалған құқық қорғау органдарында (прокуратура, Ұлттық бюро, ЭТҚ) олар мүлдем жоқ. Киберқылмыстарды анықтауды және тергеп-тексеруді жоғары заң білімі бар (біліктілік талаптарына сәйкес), жалпы қылмыстық, оның ішінде сыбайлас жемқорлық және экономика саласындағы қылмыстарды тергеп-тексеруге маманданған қызметкерлер жүзеге асырады. Қазақстанның құқық қорғау органдарының тергеу қызметкерлерінде киберқылмыстар туралы қылмыстық істерді тергеуде арнайы танымдардың болмауы; жедел бөлімшелер қызметкерлерінің дағдыларының жеткіліксіз деңгейі қылмыстарды уақтылы ашуға, дәлелдемелер белгілеуге және кінәлі адамдарды жауапкершілікке тартуға мүмкіндік бермейді.

ҚР Қылмыстық-процестік кодексі (79,80-б.) істің нәтижесіне мүдделі емес және тергеп-тексеруді жүзеге асыруға уәкілеттік берілмеген жекелеген процестік әрекеттерді қорытынды беру немесе техникалық сүйемелдеу үшін жоғары білімі бар адамдарды тек сарапшылар немесе мамандар ретінде тартуға мүмкіндік береді. Террористік, экстремистік, сыбайлас жемқорлық, экономикалық сипаттағы және т.б. қылмыстар, оның ішінде ақпараттық-коммуникациялық технологиялар арқылы жасалатынын және оларды тергеп-тексеру арнайы танымдарды талап ететінін назарға ала отырып, Қазақстанның құқық қорғау органдарында киберқылмыстарды анықтауды, жолын кесуді және ашуды, тергеп-тексеруді жүзеге асыратын, сондай-ақ жедел-техникалық және ақпараттық сүйемелдеуді орындайтын мамандандырылған бөлімшелер құру қажеттігі туындайды.

Айта кету керек, істердің едәуір саны ашылмаған күйінде қалып отыр - 2017 жылы істердің 23,4% - ы бойынша қылмыс жасаған адамдар анықталмаған, яғни әрбір 4-ке жуық. Мұның себебі ақпараттық технологиялар саласындағы қылмыстарды тергеу бойынша ғылыми негізделген және дәлелденген тактикалар мен әдістемелердің, ұсынымдар мен түсіндірмелердің, киберқылмыс бойынша жалпыланған сот тәжірибесінің жеткіліксіз болуы болып табылады.

Ағымдағы жылы Бас прокуратура қылмыстық тергеу органдары ҚР ҚК 174-бабы (Әлеуметтік, ұлттық, рулық, нәсілдік, тектік-топтық немесе діни алауыздықты қоздыру) және ҚР ҚК 256-бабы (терроризмді насихаттау немесе

терроризм актісін жасауға жария түрде шақыру) бойынша қылмыстық істер бойынша қабылдаған шаралардың заңдылығына талдау жасады. Талдау көрсеткендей, интернет-кеңістікті (әлеуметтік желілерді) қылмыскерлер экстремистік және террористік материалдарды тарату, терроризмді насихаттау және террористік әрекетке тарту үшін белсенді пайдаланады.

Мұндай істерді тергеу кезінде әлеуметтік желілерде заңсыз материалдарды орналастыру ниетін, уәжі мен мақсатын, террористік материалдарды орналастырған және пайдаланған адамдардың іс-әрекеттері арасындағы байланысты дәлелдеу бойынша қиындықтар туындады. АҚШ ФБР қызметкерлерінің осы санаттағы істерді тергеу тәжірибесі қылмыскерлермен тікелей байланыс орнату үшін экстремистік және террористік материалдары бар әлеуметтік парақтардың "жазылушылары" ретінде қызметкерлерді енгізу және қылмыстық әрекеттерді модельдеу әдістерін белсенді қолдануды көрсетеді. Шет мемлекеттің халықаралық тапсырмаларды орындауына байланысты сотқа дейінгі тергеп - тексеру мерзімдерін үзу фактілері бар: 2017 жылы-2 іс және 2015 жылы-1 іс.

Facebook, Instagram, Whatsapp, Twitter және т. б. ақпараттық технологияларды пайдалана отырып жасалған қылмыстарды тергеу тәжірибесі көрсетіп отырғандай, әлеуметтік желілердің ресми өкілдерімен тиісті өзара іс-қимылдың болмауы да проблемалардың бірі болып табылады [69].

Қазақстанның құқық қорғау органдарында ақпараттық қауіпсіздік саласындағы қылмыстарды тергеу кезінде, сондай-ақ діни терроризмнің таралу фактілері бойынша IP-мекенжайлары, әлеуметтік желілерді пайдаланушылар туралы мәліметтер алу кезінде проблемалар туындайды. Аталған корпорациялардың көп бөлігі АҚШ-та орналасқанын ескере отырып, дәлелдемелерді алу халықаралық тапсырмаларды жіберу арқылы ғана мүмкін болады. Тапсырмаларды ұзақ, жедел емес орындау нәтижесінде кінәлі адамдар жасырылады, олардың тұрған жерін анықтау мүмкін емес.

Құқықтық көмек көрсету туралы халықаралық тапсырманы жіберу және орындау процесі ақпаратты жедел алуға және киберқауіпсіздікке байланысты қылмыстарды ашуға мүмкіндік бермейді. Сонымен қатар әлемдік қоғамдастық киберқылмысқа қарсы іс-қимылдың тиімді тетіктерін әзірледі және қолдануда. Мәселен, Еуропалық Одаққа қатысушы елдер арасында олардың аумағында мәліметтер алудың оңайлатылған тетігі қолданылады - 2001 жылғы 23 қарашада Будапештте қол қойылған компьютерлік қылмыстар туралы Еуропалық конвенция (киберқылмыс туралы) (бұдан әрі - Конвенция). Орталық Азия елдерінің аумағында халықаралық тапсырмалар Минск және Кишинев конвенциялары арқылы орындалуға тиіс.

Конвенция киберқылмысқа қарсы жоғарыда аталған мәселелерді шешу қажеттілігін атап өтті және келесі үш негізгі ұсыныс анықталды: Бірінші. Компьютерлік ақпарат (криминализация) саласындағы қылмыстардың қылмыстық-құқықтық сипаттамасы мәселелері. Екінші. Компьютерлік қылмыстарды тергеу кезінде дәлелдемелер жинауға бағытталған қылмысқа қарсы күрестің қылмыстық іс жүргізу аспектілері. Үшінші. Халықаралық

ынтымақтастық мәселелері: құқықтық көмек көрсету, экстрадициялау, мүлікке тыйым салу және тәркілеу және т. б. Аймақтық Еуропалық Конвенция халықаралық ынтымақтастықтың көптеген мәселелерін шешетін ең ауқымды халықаралық актілердің біріне айналды. Біріккен Еуропа елдерінен басқа Конвенцияны АҚШ, Жапония, ОАР, Грузия, Канада және т. б. ратификациялады.

Алайда, Қазақстан, Ресей Федерациясы сияқты, Конвенцияны осы уақытқа дейін ратификацияламады. Талқылау мен келіспеудің негізгі тақырыбы Конвенцияның 32-бабының талабы болды, ол тараптардың кез келгенінің екінші тараптың келісімінсіз өз аумағында компьютерлік жүйе арқылы екінші тараптың аумағында орналасқан компьютерлік деректерге қол жеткізу құқығын көздейді. К.Н. Евдокимовтың айтуынша, бұл норма Ресей заңнамасына қайшы келеді және мемлекеттің егемендігін бұзады, өйткені онда қарастырылған әрекеттер осы әрекеттер жасалған тараптың алдын-ала ескертусіз және келісімінсіз жасалуы мүмкін. Сонымен қатар, Ресей Федерациясының Қылмыстық кодексінде компьютерлік ақпарат саласындағы қылмыстар үшін заңды тұлғалардың қылмыстық жауапкершілігін белгілейтін нормалар жоқ.

Конвенцияға қосылу ұлттық заңнамаға қайшы келетін кейбір ережелер мен нормаларды қолданбау туралы ескертпемен жүзеге асырылуы мүмкін деп ойлаймыз, бұл түпкі нәтижесінде ынтымақтасушы мемлекеттердің құзыретті органдарының өзара іс-қимыл жасау тәртібіне оң әсерін тигізеді. Мысалы, Грузияда конвенцияның талаптарын орындау үшін криминалдық полиция департаментінде 2012 жылы киберқылмысқа қарсы іс-қимыл жөніндегі арнайы бөлімше құрылды, оның құрылымында техникалық бөлім және тергеу бөлімі бар. Техникалық бөлімнің қызметкерлері ақпараттық-техникалық саланың (білім беру) мамандары болып табылады және қылмыстарды анықтаумен және ашумен, сондай-ақ тергеу бөлімінің тергеушілеріне әдіснамалық көмек көрсетумен айналысады. Тергеу бөлімі қандай да бір зиян келтірген немесе қылмыстық құқық бұзушылық белгілері бар әрекеттерге құқықтық біліктілік береді.

Грузияның Қылмыстық кодексінде киберқылмыстар туралы 5 құрам бар, олар Қазақстан Республикасының Қылмыстық кодексінің құрамдарына ұқсас: 1. 255-бап. Порнографиялық туындыларды немесе өзге де заттарды заңсыз дайындау немесе өткізу; 2. 2551-бап. Кәмелетке толмағандарды порнографиялық туындыларды немесе порнографиялық сипаттағы өзге де заттарды (балалар порнографиясы) заңсыз өндіруге және сатуға тарту); 3. 284-бап. Компьютерлік ақпаратқа заңсыз қол жеткізу; 4. 285- бап. ЭЕМ - ге арналған зиянды бағдарламаларды жасау, пайдалану немесе тарату; 5. 28-бап. ЭЕМ-ді, ЭЕМ жүйесін немесе олардың желісін пайдалану ережелерін бұзу.

Электрондық пошталарды бұзу, Банктік карталар мен интернет-төлемдерді қолдана отырып ақша ұрлау, сонымен қатар фишинг жасаудың ең көп таралған тәсілдері болып табылады [69].

Чех Республикасында киберқылмыстарды тергеу саласында құқық қорғау органдарының әлеуетін дамыту Тұжырымдамасы әзірленді (Ұлттық Қауіпсіздік

Кеңесі бекіткен). 2016 жылы ұйымдасқан қылмысқа қарсы күрес жөніндегі агенттік құрылды, оның құрамына кибер-қылмысқа қарсы іс-қимыл тобы кірді. Топтың функциялары үйлестіру және тәулік бойы техникалық қолдау (24/7 Contact point), қылмыстарды анықтау және тергеу, халықаралық өзара іс-қимыл, осы салада ғылыми-білім беру қызметін жүзеге асыру болып табылады.

Кибер-қылмыстарды жедел ашу мақсатында, аса маңызды мемлекеттік жүйелерді бұзудың және олардың жұмысын бұзудың қоғамға қауіпті зардаптарының ауырлығын ескере отырып, мемлекеттік жүйелер объектісі болып табылатын киберқылмыстардың кейбір құрамдарын террористік санатқа енгізу туралы мәселе пысықталуда. Осыған байланысты 2018 жылы топ штатын 250 полицей (тергеуші) мен IT-мамандықтарға дейін ұлғайту жоспарланып отыр. Құрамына киберқылмыспен күрес жөніндегі бөлімдер кіретін 14 өңірлік басқарма бар. Тағы бір проблема-халықтың, заңды тұлғалардың компьютерлік сауаттылығының төмен деңгейі. Хакерлер алдау арқылы қарапайым ақпараттық қауіпсіздікті қамтамасыз ету туралы білімнің жоқтығын қолдана отырып, жеке және заңды тұлғалардың жеке, коммерциялық ақпараттарына қол жеткізе алады, бұл ақша қорқытып алу құралына айналады.

Мемлекеттік органдар ақпараттандыру және байланыс саласындағы қылмыстардың алдын алу бойынша профилактикалық жұмыстарды жеткіліксіз деңгейде жүргізуде, компьютерлердің, смарт-телефондардың және т.б. қауіпсіздік құралдарын бұзудың неғұрлым кең таралған тәсілдері жарияланбайды, ақпараттық қауіпсіздікті қамтамасыз етудің қарапайым тәсілдері насихатталмайды. Осыған байланысты Мемлекет басшысы Қазақстан Республикасының 2025 жылға дейінгі Стратегиялық даму жоспарында азаматтардың ақпараттық қауіпсіздік мәселелері бойынша хабардар болуын арттыруды, сондай-ақ мектептерде ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалану негіздеріне оқытуды енгізуді көздейтін 2.11 бастамасын ұсынды.

Қазақстандағы ақпараттық қауіпсіздіктің қазіргі жай-күйін талдау оның деңгейі қазіргі уақытта адамның, қоғамның және мемлекеттердің қажеттіліктеріне сәйкес келмейтінін көрсетеді. Ақпараттың тұтастығы мен құпиялылығын қамтамасыз ету үшін жалпы мемлекеттік ауқымда және ведомстволық деңгейде ақпаратты қорғау жөніндегі шараларды кешенді үйлестіру қажет [60, 15 б.].

Киберқылмысты тергеудің тиімділігіне байланысты маңызды проблемалардың бірі азаматтардың құқық қорғау жүйесіне сенімсіздігі болып табылады. Мәселен, Қазақстан Республикасы Статистика агенттігінің мемлекеттік тапсырысы бойынша жүргізілген сауалнама нәтижелері бойынша 356 мың респонденттің 12 мыңы (3,5 %) қылмыс құрбаны болды деп мәлімдеді, олардың 46% - ы немесе жалпы сұралғандардың 1,6% - ы ғана құқық қорғау органдарына жүгінді. Демек, өздерін жазасыз сезінетін қылмыскерлер мен құқық қорғау органдарына рұқсатсыз кіру туралы өтініш бергісі келмейтін жәбірленушілердің құқықтық нигилизмі, өйткені олар әлі де қылмыскерлер үшін тиісті жазаға қол жеткізе алмайтындығын түсінеді.

Осындай құқық бұзушылықтардың алдын алу үшін желілік ақпараттық технологиялар шеңберінде заңнаманы дамыту мен құрудың маңыздылығын атап өткен жөн, бұл перспективада тиісті құқық бұзушылықтарға қарсы күрес мәселелерінде сенімді мамандармен жасақталған құзыретті органдардың тиімділігін арттыруға мүмкіндік береді.

Бүгінде біздің республикамызда қылмысқа алдын ала әсер етудің қазіргі заманғы әдістеріне және инновациялық технологияларға негізделген қылмыстық істерді тергеуге кезең-кезеңімен көшу жүзеге асырылуда. Сонымен қатар, киберқылмыспен күрес жөніндегі мамандандырылған бөлімшелердің қаржылық тергеулерге, криминалистикалық сараптамаға, кірістерді тәркілеуге, интернет желісіндегі қылмыстарға байланысты істерді тергеу мақсатында ақшаны жылыстатуға қарсы күрес жөніндегі шараларға жауап беретін түрлі мемлекеттік органдармен белсенді түрде ынтымақтасу қажеттілігі пісіп-жетілді. Құқық қорғау органдарының шетелдік әріптестермен осы саладағы ведомствоаралық ынтымақтастығы жоғары ақпараттық технологияларды пайдалана отырып жасалатын қылмыстарға қарсы іс-қимыл бойынша табыстың кепілі болады.

Осы мақсатта алдымен барлық облыс орталықтарында "К" бөліміне ұқсас арнайы бөлімшелер құру қажет. Құқық бұзушылықтарды қадағалау және интернетті қылмыстық мақсаттарда пайдаланудың алдын алу мақсатында компьютерлік желіге кіру үшін арнайы жабдықты әзірлеу қажеттілігі бар. 2018 жылдың соңында Қазақстанда "кибер қалқан"ақпараттық қауіпсіздік жүйесі іске қосылды.

Компьютерлік қауіпсіздік мәселелері бойынша халықтың сауаттылығының төмендігі маңызды факторлардың бірі болып табылады, сондықтан киберқауіпсіздік мәселелері бойынша сауаттылықты арттыру курстары қажет. Осы қылмыстарды тергейтін қызметкерлердің біліктілігі жеткіліксіз. Басқаша айтқанда, мұндай қызметкерлерге IT-технологиялар бойынша білім де қажет. Тиісінше, бұл істердің үлкен пайызы адамның анықталмағаны үшін үзіледі. Осылайша, проблемалар тиісті тұлғаларды таба алмайтындығында көрінеді. адамдар шетелде жасырылады. Қашықтан қол жеткізу арқылы қылмыс жасаңыз. Соңғы уақытта мемлекеттік серверлерге күніне 100 мыңға дейін кибершабуыл жасалады. Алдын ала жұмыс істеп, қазірдің өзінде киберқылмысқа қарсы іс-қимылға қатысты заң жобаларын әзірлеу қажет.

Осылайша, біз киберқылмысқа қарсы іс-қимыл құқық қорғау органдарының бірінші кезектегі міндеттері дәрежесіне көтерілуі тиіс деген қорытындыға келдік, оның тиімділігіне мынадай факторлар ықпал ететін болады:

1. 23.11.2001 ж. Еуропалық киберқылмыс туралы конвенцияның ұсынымдарына сәйкес (күрестің мамандануы, қылмыстарды ашу және тергеу процесінің тікелей және үздіксіздігі қамтамасыз етіледі) тәулік бойы - 24/7 жұмыс істейтін тергеу және жедел топтарды қамтитын киберқылмыспен күрес жөніндегі бөлімшелерді ұйымдастыру қажет.

Қылмыстық қудалау органдарының тергеу бөлімшелеріне киберқылмыстарға қарсы іс-қимыл жасауға мамандanған топтарды енгізу осы санаттағы қылмыстарды білікті тергеп-тексеруді қамтамасыз етеді (бүгінде мұндай мамандандыру орталық және облыстық деңгейлерде жоқ). Перспективаға-жедел және тергеу қызметтерін нақты тік бағыныстылық пен мамандандыруды айқындаумен біріктіру, оның ішінде: киберқылмысқа қарсы іс-қимыл бойынша (ҚР ІІМ бөлімшелерінің материалдарды жинауының қолданыстағы жүйесі, кейіннен оларды өзге ұйымдық құрылымдағы, Ақпараттық технологиялар саласында арнайы білімі жоқ тергеушілердің іс жүргізу арқылы бекітуі қылмыстың осы түрлерімен күрестің қазіргі заманғы талаптарына жауап бермейді).

2. Құқық қорғау және арнайы органдарда, сондай-ақ ҚР ӘМ сараптамалық бөлімшелерінде (техникалық білімі бар жедел қызметкерлер) кадрларды іріктеудің ерекше жүйесін қайта қарап, енгізу қажет. Біз, әдетте, техникалық білімі бар адамдарды заңгерлік дайындық курстарынан өтіп, жедел қызметкерлер мен мамандарды жұмысқа тартатын шет елдердің оң тәжірибесін қолдануға болады деп санаймыз. Бастапқы кезеңде мұндай талапты жедел қызметкерлерге орнатуға болады.

3. Тергеуді әдістемелік қамтамасыз ету. Қылмыстық әрекетті имитациялау және құқық қорғау органдары қызметкерлерінің енгізу әдістерін белсенді пайдалану, сондай-ақ посткеңестік кеңістік елдерінің аумағында киберқылмыстарды тергеу тәжірибесі, қылмыскерлер, бұғатталған сайттар туралы мәліметтер және т. б. бар бірыңғай құқықтық платформа құруға бастамашылық жасау.

4. Тиісті халықаралық құқықтық ынтымақтастық. Қазақстан Республикасының киберқылмыс туралы Еуропалық конвенцияға қосылуы туралы мәселенің оң шешілуі қажетті мәліметтер мен дәлелдемелерді жедел алуға мүмкіндік береді.

Қорытынды

Киберкеңістікте жасалған қылмыстарды зерттеу бізге бірқатар ғылыми негізделген ережелерді ұсынуға мүмкіндік берді.

1. Жаңа технологиялардың пайда болуымен қылмыстың жаңа, неғұрлым күрделі түрінің пайда болуы байқалады. Бұл қылмыскерлер ғылыми-техникалық прогрестің нәтижелерін өз мақсаттары үшін тез пайдаланатынын көрсетеді. Бұл тенденция киберкеңістікте қалыптасқан барлық қоғамдық қатынастарға елеулі қауіп төндіреді, өйткені дамудың осы кезеңінде киберкеңістік пен қоғам бөлінбейді.

2. Киберқылмыс-бұл компьютерлік қылмыстардың жаңа, тәуелсіз түрі (яғни компьютерлік техниканы қолдану арқылы жасалған қылмыстар). Киберқылмыс дегеніміз-компьютерлік техниканы, ақпараттық және телекоммуникациялық желілерді және олар құрған киберкеңістікті пайдалану арқылы қашықтықтан жасалған гетерогенді қоғамдық қатынастарға зиян келтіретін қылмыс. Экономикалық киберқылмыс экономикалық қатынастарға зиян келтіретін киберқылмыс деп саналуы керек. Экономикалық сипаттағы киберқылмыстар "Интернет" желісіндегі ең көп таралған қылмыстар болып табылады.

Киберқылмыс ұғымы компьютерлік техниканы, ақпараттық және телекоммуникациялық желілерді және олар құрған киберкеңістікті пайдалану арқылы қашықтықтан жасалған гетерогенді қоғамдық қатынастарға зиян келтіретін қылмыс ретінде анықталады.

Экономикалық киберқылмыстардың жасалу тәсіліне қарай олардың авторлық жіктемесі беріледі:

- компьютерлік және өзге де ұқсас техниканы пайдалана отырып, адамға психологиялық әсер ету (алдау, жаңылыстыру, қорқыту) арқылы жасалатын экономикалық киберқылмыс);
- жабдыққа (компьютерлер, смартфондар, маршрутизаторлар және басқа жабдықтар) әсер ету арқылы жасалатын экономикалық киберқылмыстар.

Экономикалық киберқылмыс жалпы объект ретінде экономикалық қатынастарға зиян келтіретін киберқылмыс деп саналуы керек.

Компьютерлік техника құралдарын, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қашықтықтан қылмыс жасау оның қоғамдық қауіптілігін арттыратын мән-жай болып табылуы мүмкін.

Компьютерлік техниканы, ақпараттық-телекоммуникациялық желілерді және киберкеңістікті пайдалана отырып, қашықтан қылмыс жасауды жазаны ауырлататын мән-жайлар тізбесіне енгізу қажет, бұл ретте сотқа осы норманы қылмыстың сипаты мен қоғамдық қауіптілік дәрежесіне, оны жасаудың нақты мән-жайларына және кінәлінің жеке басына қарай өз қалауы бойынша қолдануға мүмкіндік береді.

3. Экономикалық киберқылмыстың болуының негізгі себептері мен шарттары киберкеңістікті пайдаланушылардың анонимділігі және ақпараттық желілердің анонимділігі, киберкеңістіктің эксаумақтылығы, киберкеңістіктің

техникалық жетілмегендігі, сондай-ақ азаматтардың ақпараттық қауіпсіздігінің төмен деңгейі болып табылады.

4. Қоғамда қалыптасқан жағдай экономикалық киберқылмыстардың кешігуінің жоғары деңгейімен күрделене түседі. Құқық қорғау органдарына жасалған барлық экономикалық киберқылмыстардың бестен бір бөлігі ғана белгілі болады.

5. Зерттеу нәтижелері негізінде диссертация қылмыстық-құқықтық сипаттағы (қылмыстық заңнамаға өзгерістер мен толықтырулар енгізу туралы ережелер) және криминологиялық сипаттағы (ұйымдастырушылық және техникалық шаралар) шараларды қамтитын киберкеңістікте жасалатын экономикалық қылмыстарға қарсы іс-қимыл шараларының кешенін әзірледі. Құқықтық шараларды Қазақстан Республикасы Қылмыстық кодексінің Ерекше және жалпы бөлігінің нормаларын жетілдіруге бағыттау қажет.

Қазақстанның қылмыстық заңнамасында ақпараттық қауіпсіздік саласындағы қатынастар "ақпараттық алаяқтық", "спам тарату", "ақпараттық жалғандық", "адамдарды терроризм мен экстремизмге насихаттайтын және оқытатын ақпараттық материал жасау және тарату", "компьютерлік диверсия" және т.б. қоғамға қауіпті бірқатар іс-әрекеттерді криминализациялау

6. Жоғарыда айтылғандарды ескере отырып, құқықтық реттеу, ұйымдастырушылық және ұйымдастырушылық-техникалық шаралар экономикалық киберқылмысқа қарсы іс-қимылдың негізгі бағыттары болуға тиіс.

Еуропалық киберқылмыс туралы конвенцияның ұсынымдарына сәйкес (күрестің мамандануы, қылмыстарды ашу және тергеу процесінің тікелей және үздіксіздігі қамтамасыз етіледі) тәулік бойы - 24/7 жұмыс істейтін тергеу және жедел топтарды қамтитын киберқылмыспен күрес жөніндегі бөлімшелерді ұйымдастыру қажет.

Құқық қорғау және арнайы органдарда кадрларды іріктеудің ерекше жүйесін қайта қарап, енгізу қажет. Біз, әдетте, техникалық білімі бар адамдарды заңгерлік дайындық курстарынан өтіп, жедел қызметкерлер мен мамандарды жұмысқа тартатын шет елдердің оң тәжірибесін қолдануға болады деп санаймыз. Бастапқы кезеңде мұндай талапты жедел қызметкерлерге орнатуға болады.

Тергеуді әдістемелік қамтамасыз ету. Қылмыстық әрекетті имитациялау және құқық қорғау органдары қызметкерлерінің енгізу әдістерін белсенді пайдалану, сондай-ақ посткеңестік кеңістік елдерінің аумағында киберқылмыстарды тергеу тәжірибесі, қылмыскерлер, бұғатталған сайттар туралы мәліметтер және т. б. бар бірыңғай құқықтық платформа құруға бастамашылық жасау.

Тиісті халықаралық құқықтық ынтымақтастық. Қазақстан Республикасының киберқылмыс туралы Еуропалық конвенцияға қосылуы туралы мәселенің оң шешілуі қажетті мәліметтер мен дәлелдемелерді жедел алуға мүмкіндік береді.

Пайдаланылған әдебиеттер тізімі

1 Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Жаңа жағдайдағы Қазақстан: іс-қимыл кезеңі» атты 2020 жылғы 1 қыркүйектегі Қазақстан халқына Жолдауы//https://www.akorda.kz/kz/addresses/addresses_of_president/memleket-basshysy-kasym-zhomart-tokaevtyn-kazakstan-halkyna-zholdauy-2020-zhylgy-1-kyrkuiek

2 Қазақстан Республикасының 2025 жылға дейінгі Ұлттық даму жоспарын бекіту және Қазақстан Республикасы Президентінің кейбір жарлықтарының күші жойылды деп тану туралы Қазақстан Республикасы Президентінің 2018 жылғы 15 ақпандағы № 636 Жарлығы// https://adilet.zan.kz/kaz/docs/U1800000636

3 А.Алехова./ Почему Казахстан так привлекателен для хакеров и киберпреступников?/ https://365info.kz/2020/10/pochemu-kazahstan-tak-privlekatelen-dlya-hakerov-i-kiberprestupnikov

4 Қазақстанда киберқылмыс жасау жағдайлары жиілеп кетті// https://forbes.kz/news/2021/02/15/newsid_243941

5 В Казахстане за год выявлено более 21 тыс. кибератак 31.01.2020 23356 Алматы. 31 января. Kazakhstan Today/ https://www.kt.kz/rus/science/v_kazahstane_za_god_vyyavleno_bolee_21_tys_kiberatak_1377893834.html

6 «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік»: Мемлекет басшысы Н.Назарбаевтың Қазақстан халқына Жолдауы. 2017 жылғы 31 қаңтар. // http://adilet.zan.kz/rus/docs/ K1700002017.

7 Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.// https://adilet.zan.kz/kaz/docs/P1700000407/ history

8 Қазақстан Президенті ШЫҰ-ның ақпараттық қауіпсіздік жөніндегі орталығын құруды ұсынды. https://www.kazpravda.kz/news/prezident2/ prezident-kazahstana-predlozhil-sozdat-tsentr-shos-po-informatsionnoi-bezopasnosti

9 Как развивается кибербезопасность Казахстана/ https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/

10 Банки Казахстана будут сами раскрывать киберпреступления//https://liter.kz/banki-kazahstana-sozdadut-speczialnye-sluzhby-reagirovaniya-na-kiberprestupnikov/

11 Дремлюга Р.И. Интернет-преступность: Монография. Владивосток, Изд. Дальневосточного университета.2008.

12 Простосердов, М.А. Проблемы квалификации компьютерных преступлений / М.А. Простосердов // Российское правосудие. – 2012. –№ 6 (74).

13 Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием компьютерной техники: автореф. дис. … канд. юрид. Наук. Волгоград, 1995.

14 Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток. 2005.

15 Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы). автореф. дис. … канд. юрид. наук. М., 2008.

16 Коменский Н.А. Компьютерная информация и информационные технологии как средство совершения преступления. // Преступления в информационной сфере: проблемы расследования, квалификации, реализации ответственности и предупреждения: материалы международной научно-практической конференции 14-15 февраля 2013 г. / М-во обр. и науки РФ, ФГБОУ ВПО «Тамб.гос. ун-т им. Г.Р. Державина»; ред. кол.: А.В. Шуняева, Е.А. Попова, С.А. Пучнина. − Тамбов: Издательский дом ТГУ имени Г. Р. Державина, 2013.

17 Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. − 2013. − №5(10).

18 В Казахстане выявили более 21 тысячи инцидентов по нарушению информационной безопасности// https://liter.kz/v-kazahstane-za-2019-god-bylo-vyyavleno-bolee-21-tysyachi-inczidentov-po-narusheniyu-informaczionnoj-bezopasnosti/

19 Простосердов, М.А. К вопросу об оценке общественной опасности преступлений, совершаемых в сети Интернет / М.А. Простосердов // Актуальные проблемы уголовного права и криминологии: сборник научных трудов кафедры уголовного права. Вып. 3 / Под ред. Ю.Е. Пудовочкина и А.В. Бриллиантова. − М.: РАП, 2013.

20 Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: Монография. / Дворецкий М.Ю., Копырюлин А.Н. Тамбов, ТГУ им. Г.Р. Державина. 2006.

21 Степанов-Егиянц В.Г. Преступления сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. …канд. юрид. наук. М., 2005.

22 Простосердов, М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им / М.А. Простосердов // Судебные известия. Информационный бюллетень Управления судебного департамента в Тамбовской области. – 2014. − №15(2).

23 Информационный ресурс «Улфек». Компьютерная преступность. [Электронный ресурс] // URL: http://ulfek.ru/osnovy-bezopasnosti-informatsionnykh-tekhnologij/3469-kompyuternaya-prestupnost.html

24 Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., Юрлитинформ, 2001.

25 Сухомлинов В.В. Вопрос - Ответ // Юный техник. 1989. №5.

26 Крылов В.В. «Расследование преступлений в сфере информации» Глава 1, § 3 «Информация как элемент преступной деятельности».

27 Ахметов Е. «Киберпреступность в Казахстане» // Журнал «Законность

и правовая статистика» 2009, № 2 (11).

28 Голубев В. «Стратегия и тактика борьбы с киберпреступностью в странах СНГ» 20 июня 2005 года. //crime-research.ru

29 «Европейская Конвенция по преступлениям в киберпространстве» // Будапешт, 23 ноября 2001 года (перевод: Институт проблем информационного права).

30 https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/

31 https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/

32 Хуторной С.Н. Киберпространство и становление сетевого общества: дис… канд. фил. наук. Воронеж,2013.

33 Вылков Р. И. Киберпространство как социокультурный феномен, продукт технологического творчества и проективная идея: дис. …канд. фил. наук. Екатеринбург, 2009.

34 Барышев Р. А. Киберпространство и проблема отчуждения: дис. …канд. фил. наук. Красноярск, 2009.

35 Информационный ресурс «Ciec.org». Reno vs. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932-53). [Электронный ресурс] // URL:http//ciec.org/SC_appeal/opinion.shtml.

36 Уголовный кодекс Федеративной Республики Германия от 15.05.1871. Особенная часть. – СПб.: Юридический центр «Пресс», 2003.

37 Уголовный кодекс Швеции от 01.01.1962 / Под ред. Беляева С.С., Кузнецовой Н.Ф. – СПб.: Юридический центр «Пресс», 2001.

38 Уголовный кодекс Австрии от 29.01.1974. – СПб.: Юридический центр «Пресс», 2004.

39 Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. – 2016. – № 9.

40 Recommendation № R (89) 9 of the Committee of Ministers of the Council of Europe to member States for the Computer-Related Crime and Final Report of the European Commitee on Crime Problems (adopted by the Com- mittee of Ministers on 13 September 1989 at the 428 th meeting of the Ministers' Deputies). – Strasbourg, 1990

41 Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activity report. – Pre- pared by Committee of Experts on Crime in Cyber-Space (PC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50 th plenary session (18 – 22 June 2001). – Secretariat Memorandym prepared by the Di- rectorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev 2. – Strasbourg, 20 June 2001.

42 Recommendation № R (90) 19 of the Committee of Ministers of the Council of Europe to member States for the protection of personal data used for payment and other related operations. – Strasbourg, 1990.

43 Recommendation № R (91) 10 of the Committee of Ministers of the

Council of Europe to member States for the communication to third parties of personal data by public bodies. – Strasbourg, 1991.

44 Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. // Диссертация на соискание учёной степени к.ю.н. - Москва, 2007.

45 1997 жылғы 16 шілдедегі ҚР Қылмыстық кодексі. Алматы, 2012.

46 Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: Учебное пособие. // Алматы: Данекер, 1999.

47 Батурин Ю. М. Компьютерные преступления и компьютерная безопасность. // Москва: Юридическая литература, 1991.

48 Указ Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан» от 10 октября 2006 года, № 199.// https://adilet.zan.kz/rus/docs/U060000199_/history

49 Голубев В.А., Головин А.Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий //crime-research.org / articles.

50 computerra.ru/news/31134025

51 conventions.coe.int/Treaty/en/Treaties/Html/185.htm 30

52 Қазақстан Республикасының Қылмыстық кодексі. 2014 жылғы 3 шілдедегі №226-V ҚРЗ// https://adilet.zan.kz/kaz/docs/K1400000226

53 Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года № 2012-XII. –www.online.zakon.kz

54 Сборник УК стран СНГ. – www.twirpx.com/law/criminal/foreign/ codes/

55 World Internet Usage. URL: http://www. intemetworldstats.com/stats.htm

56 Отчет ФАТФ Виртуальные валюты, ключевые определения и потенциальные риски в сфере ПОД/ФТ. – 2014.

57 Волеводз, А. Г. Конвенция о киберпреступности: новации правового регулирования / А. Г. Волеводз // Правовые вопросы связи. – М. : Юрист, 2007. – № 2.

58 Балановская, А. В. Современное состояние и перспективы развития информационной безопасности Республики Казахстан / А. В. Балановская, В.А.Сейткереев // Вестник Самарского муниципального института управления. – 2014. – № 29.

59 Айвазова, О. В. Междисциплинарный характер категории «способ преступления»: проблема соотношения уголовно-правовых, уголовно-процессуальных и криминалистических аспектов / О. В. Айвазова, С. И. Коновалов // Юристъ-Правоведъ. – 2007. – № 4.

60 Бондаренко С.В. Виртуальные сетевые сообщества девиантного поведения. URL: http: // www.cyberpolitics.ru/ content/view/ 256/34/

61 Giddens A. 1991. Modernity and Self-Identity. Self and Society in the Late Modern Age. Stanford University Press

62 Цифровая компетентность подростков и родителей (под ред. Г.У. Солдатовой, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова). 2013. М.: Фонд развития Интернет

63 Джансараева Р.Е., Аратулы К. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ // Криминологический журнал Байкальского государственного университета экономики и права. - 2012. - №3(21)

64 https://liter.kz/v-kazahstane-za-2019-god-bylo-vyyavleno-bolee-21-tysyachi-inczidentov-po-narusheniyu-informaczionnoj-bezopasnosti/

65 «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік»// Мемлеке басшысы Н.Назарбаевтың Қазақстан халқына Жолдауы. – 2017 жылғы 31 қаңтар// http://www.akorda.kz/kz/addresses/ addresses_of_president /Memleket - basshysy-nnazarbaevtyn-kazakstan-halkyna-zholdauy-2017-zhylgy-31-kantar

66 Информационный сервис Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан http://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat (дата обращения: 16.02.2019)

67 https://www.inform.kz/ru/155-kiberprestupleniy-vyyavili-v-kazahstane_a3716257

68 https://inbusiness.kz/ru/news/kiberprestupnost-vse-pod-pricelom

69 Материалы регионального симпозиума для Центральной Азии «Борьба с киберпреступностью и обеспечение целостности и безопасности информации», г.Тбилиси (Грузия), 15-17 октября 2018 г.