ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІІМ Б.БЕЙСЕНОВ АТЫНДАҒЫ ҚАРАҒАНДЫ АКАДЕМИЯСЫ

НҰРМАХАНОВ ЖАНБОЛАТ СӘКЕНҰЛЫ

«Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарға қылмыстық құқықтық қарсы іс қимыл»

6М030300 – Құқық қорғау қызметі

Заң ғылымдарының магистрі
дәрежесін алу үшін дайындалған диссертация

Ғылыми жетекші:
PhD докторы, С.Күмісбеков

Қазақстан Республикасы
Қарағанды, 2021

МАЗМҰНЫ

АНЫҚТАМАЛАР, ҚЫСҚАРТУЛАР МЕН БЕЛГІЛЕУЛЕР

Интернет – халықаралық жаһандық байланыс желісі
«К» басқармасы – компьютерлік қылмыстармен шұғылданатын тергеу бөлімі
Әлеуметтік желілер - ермектері бірдей адамдардың Интернетте бірігетін қоғамдастық сайттары
Интернет-банкинг - несие ұйымының интернет арқылы алыстан банк қызметін көрсетуі. Электрондық сандық қол қою және кодтау жүйесі қауіпсіздікті қамтамасыз етеді.
Бот немесе веб робот - желілік мекен-жайлардың блоктарын автоматты түрде қарап шығатын және осал компьютерлерге жұғатын автоматтандырылған зиянкес бағдарлама
Компьютер вирусы — компьютеріңіздегі бар файлдарға алдын ала үстелетін немесе қосылатын зиянды код бөлігі
Компьютер құрты — басты компьютерлерді шабуылдап, желі арқылы тарайтын зиянды коды бар бағдарлама
Руткиттер – интернет шабуылдаушыларына бар екенін жасырып, жүйеге шектеусіз қатынас беретін зиянды бағдарламалар
DoS шабуылдар – компьютерді немесе желіні мақсатты пайдаланушылар үшін қол жетімді емес ету әрекеті. Зиянға ұшыраған пайдаланушылардың арасындағы байланыс кедергіге ұшырап, жұмысын бұдан әрі дұрыс жалғастыра алмайды. Әдетте тиісті дұрыс жұмыс істеуі үшін DoS шабуылдарына ұшыраған компьютерлер әдетте өшіріліп, қайта іске қосу қажет.
Бопсалаушы бағдарламалар (әрі файл кодтаушы ретінде белгілі) — құрылғыны құлыптайтын немесе құрылғыдағы мазмұнды шифрлайтын және мазмұнға қатынасты қалпына келтіру үшін сізден ақша сұрайтын зиянды бағдарлама түрі. Сондай-ақ, осы зиянды бағдарлама түрінде орындалуы керек алдын ала бағдарламаланған төлем мерзімі бар кірістірілген таймері болуы мүмкін
Фишинг - әлеуметтік жобалаудың тәсілдерін (құпия ақпарат алу үшін пайдаланушыларды қолдан жасау) пайдаланатын қылмыстық әрекетті анықтайды. Оның мақсаты банктегі есепшот нөмірлері, PIN кодтары, т.б. сияқты құпия ақпаратқа қол жеткізу болып табылады.
Жалған ескерту - зиянды бағдарлама немесе ықтимал қауіпті бағдарлама ретінде қате жіктелген таза файл/қолданба
Электрондық пошта - артықшылықтары көп байланыс үлгісі
e-gov – электронды үкімет
АКТ – ақпараттық-коммуникациялық технологиялар
БАҚ – бұқаралық ақпарат құралдары
ДОС (DOS) – операциялық жүйе
ТМД – тәуелсіз мемлекеттер достастығы
ББҰ – біріккен ұлттар ұйымы
ЭЕМ – электронды есептеу машинасы

ҚК – қылмыстық кодекс
ІІМ – ішкі істер министрлігі
Хакер (ағылш. *Hack* деген сөзінен) деп, әлемдегі ең ірі әрі күрделі саналатын компьютерлік желілерге кіруге қол жеткізген, өзінің электрондық саладағы білімін жаңа идеялар енгізу арқылы дәлелдейтін және де технологияның даму мәдениетін егжей-тегжейлі білетін адамды айтады
ҚХР – Қытай Халық Республикасы
АҚШ – Америка құрама штаттары
БАЭ – Біріккен Араб Әмірліктері
ЕК – Еуропалық Кеңес
IP-адрес *(Internet Protocol Address)* интернетке шыққан компьютердің адресі (мекенжайы). Провайдер (Интернетті пайдалануға рұқсат беретін ұйым) әр интернет қолданушыға қайталанбас IP адресін береді.

Кіріспе

Диссертацияның ғылыми жаңалығы. Ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар қоғамға аса қауіпті қылмыстық-құқықтық мәселелерді зерттеудің ғылыми қолданбалы-теориялық әдістемесімен ерекшеленеді. Алғаш рет қылмыстық-құқықтық доктринада телекоммуникациялық желілерді пайдалану арқылы жасалған қылмыстық құқық бұзушылықтарды криминализациялаудың ғылыми идеясы ұсынылады. Сонымен қатар «ақпараттық-телекоммуникациялық желі», «ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар» терминдеріне ғылыми тұрғыда тұжырымдар мен ұсыныстар жасалған. Аталған технологиялар арқылы жасалған қылмыстық құқық бұзушылықтардың негізгі белгілері анықталып, бекітіледі.

Диссертациялық зерттеудің теориялық мағыздылығы - ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарға қарсы қылмыстық-құқықтық әрекет етудегі отандық, шетелдік және халықаралық заңнамаға ғылыми қолданбалы-теориялық әдістемесі арқылы ұсыныстар мен тұжырымдар дайындау болып табылады. Ғылыми жұмыс ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарға қарсы тиімді түрде күрес жүргізуге бағытталған.

Ғылыми жұмыстың тәжірибелік мыңызы - ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың алдын алуға бағытталған заңнаманы жетілдіруге бағытталған ұсыныстардан тұрады.

Зерттеу жұмысының қорытынды бөлігіндегі тұжырымдар болашақта мынадай салаларда қолданылуы мүмкін:

- ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың алдын алуға бағытталған отандық заңнаманы жетілдіруде;
- Жоғары соттың интерпретациялық түсініктеме беруге дайындық кезінде;
- ведомстволық нормативтік-құқықтық базаны дайындауда;
- телекоммуникациялық желілерді пайдаланумен күресетін құқық қорғау органдарының қызметін жетілдіруде;
- ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар үшін жауапкершілікті бекітетін қылмыстық заңнаманы зерттейтін ғылыми және педагогикалық салада.

Ғылыми зерттеудің әдістемелік негіздерін философиялық, әлеуметтік, психологиялық, педагогикалық, қылмыстық құқық және криминологиялық жалпы танымдық тұжырымдар құрады, сонымен қатар криминологияда қолданылатын дидактикалық-материалистік ілім және осыған негізделген ғылыми әдістер: тарихи, формалды-логикалық, салыстырмалы, статистикалық, бақылау, жүйелік талдау, болжау және т.б. қолданылды. Жұмыста жеке әдіснаманың кешені пайлаланылды:

демографиялық, экономикалық, әлеуметтік және қылмыстық статистикаға талдау жасау; сауалнама алу, қылмыстық істерді зерттеу, сұхбат алу, әңгімелесу, халықаралық-құқықтық құжаттарға және ұлттық заңнамадағы нормативтік құқықтық актілерге талдау және салыстырмалы-құқықтық әдіс қарастырылған.

Зерттеудің нормативтік негізі болып зерттеу тақырыбына қатысы бар халықаралық, отандық және шетелдік заңнамалар жатады. Диссертацияны жазу барысында автор Киберқауіпсіздік тұжырымдамасына («Қазақстанның киберқалқаны»), Қазақстан Республикасы Конституциясының қағидалары, Қазақстан Республикасының конституциялық және басқа да заңдарына, Қазақстан Республикасының Президентінің жарлықтарына және Қазақстан Республикасы Үкіметінің қаулыларына, сонымен қатар ІІМ нормативтік актілеріне және қылмыстылықпен күресудің бағдарламаларына сүйене отырып дайындады.

Ақпараттық-телекоммуникациялық желілер Қазақстан Республикасының сандық экономикасын қалыптастыратын негізгі аспект болып табылады. Ол туралы Елбасы бірнеше отырыстарда атап өткен болатын. Бұл тақырып 2017 жылғы Елбасының «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Қазақстан халқына Жолдауында «Қазақстанның киберқалқаны» Киберқауіпсіздік тұжырымдамасын бекітуде атап өтіледі [1].

Ақпараттық-телекоммуникациялық желілер экономиканың тиімді дамуына және оның белсенді түрде өсуіне септігін тиігізіп, ұлттық байлығымыздың незгін құрауға көмектеседі. Мемлекеттің әлеуметтік өмірінің жүйелі факторына айналды және Қазақстан Республикасының экономикалық, әлеуметтік, саяси, әскери және т.б. қауіпсіздігін қамтамасыз етеді.

Телекоммуникациялық желілердің қарқынды түрде дамығаны бізге көптеген тиімді тұстарымен қатар, өкінішке орай жағымсыз тұстарында алып келді. Технологиялардың тез қарқынмен өсуіне байланысты осы қоғамдық өмірдің саласында қылмыстық құқық бұзушылықтың жылдам деңгейде өсуі байқалды.

Ақпараттық және телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жоғары деңгейдегі қоғамға қауіп төндіруде. Өйткені желілік жүйені дұрыс қолдану тәртібіне зиянын тигізіп қана қоймай, тұлғалардың құқықтары мен заңды мүдделеріне және мемлекеттік биліктің қызметіне, ұлттық қауіпсіздікке қауіп төндіріп, үлкен зардаптар алып келеді.

Заң шығарушы бұл қауіпті құқықтық құралдарды пайдалану арқылы заң аясында жұмыс атқарып келеді. Қазақстан Республикасының Бас прокуратурасы Құқықтық статистика және арнайы есепке алу жөніндегі комитеті есебіне сәйкес, интернет-алаяқтық бойынша 2018 жылы – 535; 2019 жылы – 8210; 2020 жылдың 7 айында – 7027 қылмыстық құқық бұзушылық тіркелген [2].

Қазіргі уақытта қылмыстық-құқық ғылымындағы ақпараттық және телекоммуникациялық желілерді пайдалану арқылы жасалған қылмыстық құқық бұзушылықтар туралы зерттеулердің көп болғанымен бұл мәселе соңына дейін зерделенбеген. Бұл мәселені зерттеу арқылы біз оның жүйесі мен белгілерін анықтаймыз және теориялық және практикалық шешімдерін табамыз.

Тақырыптың ғылыми зерттелу деңгейі. Айта кететін жайт, ақпараттық және телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстардың қылмыстық-құқықтық бағыты қылмыстық құқық доктринасында толық негізде зерттелмеген. Ақпараттық және телекоммуникациялық желілерді қолдану арқылы жасалатын қылмыстық құқық бұзушылықтың қылмыстық-құқықтық және криминологиялық аспектілерін зерттеген ғалымдар: В.Б. Вехов, В.Д. Курушин, П.Б. Гудков, В.Д. Ларичев, Н.А. Селиванов, Б.Х. Толеубекова, Аратұлы Қ. Д.В.Добровольский, А.П.Кузнецов, Маликова Ш.Б., А.В.Петрянин, Г.И.Узембаева, В:В:Хилюта және т.б.

Диссертациялық зерттеудің объектісіне ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар саласындағы құқықтық қатынасар жатады.

Диссертациялық зерттеудің пәніне жатады:

ақпараттық - телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарға қылмыстық жауапкершілікті реттейтін отандық қылмыстық заңнама;

телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық бағытын реттейтін шетелдік және халықаралық заңнама;

зерттелетін мәселе бойынша басқада криминологиялық және қылмыстық-құқықтық сипаттағы аспектілердің доктриналды және нормативтік қайнаркөздері;

ақпараттық - телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың статистикалық мәліметтері мен сот шешімдері.

Диссертациялық зерттеудің мақсаты ақпараттық - телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылыққа қарсы отандық заңнаманы жетілдіретін ұсыныстар мен тұжырымдар дайындау болып табылады.

Қойылған мақсатқа жету үшін мынадай міндеттер атқарылды:

- отандық заңнамадағы ақпараттық - телекоммуникациялық желілерідің белгілері, түсінігі және маңызы зерттелді;

- ақпараттық - телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың түсінігі мен белгілері қарастырылды;

- ақпараттық - телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылыққа қарсы әрекет ететін шетелдік және халықаралық заңнамаға ғылыми баға берілді;

- ақпараттық - телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылыққа қарсы әрекет ететін отандық заңнаманы жетілдіру бойынша ұсыныстар дайындалды.

Диссертацияның ғылыми жаңалығы. Ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар қоғамға аса қауіпті қылмыстық-құқықтық мәселелерді зерттеудің ғылыми қолданбалы-теориялық әдістемесімен ерекшеленеді. Алғаш рет қылмыстық-құқықтық доктринада телекоммуникациялық желілерді пайдалану арқылы жасалған қылмыстық құқық бұзушылықтарды криминализациялаудың ғылыми идеясы ұсынылады. Сонымен қатар «ақпараттық-телекоммуникациялық желі», «ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар» терминдеріне ғылыми тұрғыда тұжырымдар мен ұсыныстар жасалған. Аталған технологиялар арқылы жасалған қылмыстық құқық бұзушылықтардың негізгі белгілері анықталып, бекітіледі.

Диссертациялық зерттеудің теориялық мағыздылығы - ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарға қарсы қылмыстық-құқықтық әрекет етудегі отандық, шетелдік және халықаралық заңнамаға ғылыми қолданбалы-теориялық әдістемесі арқылы ұсыныстар мен тұжырымдар дайындау болып табылады. Ғылыми жұмыс ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарға қарсы тиімді түрде күрес жүргізуге бағытталған.

Ғылыми жұмыстың тәжірибелік мыңызы - ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың алдын алуға бағытталған заңнаманы жетілдіруге бағытталған ұсыныстардан тұрады:

1. Ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың авторлық анықтамасы беріледі: «Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар» түсінігіне ақпараттық-телекоммуникациялық желілерді пайдалану арқылы заңмен қорғалатын ақпаратпен байланысты қоғамдық қатынастарға (адамның жеке құқығына, қоғамның және мемлекеттің өміріне) залал келтіретін қоғамға қауіпті әрекет болып табылады.

2. Біздің еліміздің қылмыстық заңнамасы бойынша ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасағаны үшін қылмыстық жауаптылыққа 16 жасқа толған жеке тұлға тартылады. Ал шет мемлекеттердің қылмыстық заңнамасы бойынша Латвия ҚК (11-бап) –

14 жастан бастап, Дания ҚК (§15) - 15 жастан бастап, ҚХР ҚК (17 – бап) - 14-тен 16-ы жастан бастап қылмыстық жауаптылыққа тартылады.

Жоғарыдағы айтылғандарды талдай келе, автор ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар саласындағы жеке тұлғаларды қылмыстық жауаптылыққа тарту жасын, егер аса ауыр зардаптарға әкеліп соғатын болса, 16 жастан 14 жасқа дейін төмендетуді ұсынады. Өйткені ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарды жасайтын қылмыскерлер өз әрекеттері арқылы өте ауыр экономикалық зартаптарға әкеледі. Сонымен қатар он төрт жасқа толған жасөспірім қоғам мен ұжым алдындағы жауапкершілігін сезіне алатын, өзінің ойлау қабілетіне баға бере алатын дәрежеде бола алады.

3. Ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарды жасайтын қылмыскердің криминологиялық «портреттері» жасалған.

Зерттеу жұмысының қорытынды бөлігіндегі тұжырымдар болашақта мынадай салаларда қолданылуы мүмкін:

- ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың алдын алуға бағытталған отандық заңнаманы жетілдіруде;
- Жоғары соттың интерпретациялық түсініктеме беруге дайындық кезінде;
- ведомстволық нормативтік-құқықтық базаны дайындауда;
- телекоммуникациялық желілерді пайдаланумен күресетін құқық қорғау органдарының қызметін жетілдіруде;
- ақпараттық – телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар үшін жауапкершілікті бекітетін қылмыстық заңнаманы зерттейтін ғылыми және педагогикалық салада.

Ғылыми зерттеудің әдістемелік негіздерін философиялық, әлеуметтік, психологиялық, педагогикалық, қылмыстық құқық және криминологиялық жалпы танымдық тұжырымдар құрады, сонымен қатар криминологияда қолданылатын дидактикалық-материалистік ілім және осыған негізделген ғылыми әдістер: тарихи, формалды-логикалық, салыстырмалы, статистикалық, бақылау, жүйелік талдау, болжау және т.б. қолданылды. Жұмыста жеке әдіснаманың кешені пайлаланылды: демографиялық, экономикалық, әлеуметтік және қылмыстық статистикаға талдау жасау; сауалнама алу, қылмыстық істерді зерттеу, сұхбат алу, әңгімелесу, халықаралық-құқықтық құжаттарға және ұлттық заңнамадағы нормативтік құқықтық актілерге талдау және салыстырмалы-құқықтық әдіс қарастырылған.

Зерттеудің нормативтік негізі болып зерттеу тақырыбына қатысы бар халықаралық, отандық және шетелдік заңнамалар жатады. Диссертацияны

жазу барысында автор Киберқауіпсіздік тұжырымдамасына («Қазақстанның киберқалқаны»), Қазақстан Республикасы Конституциясының қағидалары, Қазақстан Республикасының конституциялық және басқа да заңдарына, Қазақстан Республикасының Президентінің жарлықтарына және Қазақстан Республикасы Үкіметінің қаулыларына, сонымен қатар ІІМ нормативтік актілеріне және қылмыстылықпен күресудің бағдарламаларына сүйене отырып дайындады.

1 Ақпараттық-телекоммуникациялық желілерді пайдалана отырып арқылы жасалатын қылмыстық құқық бұзушылықтың жалпы түсінігі

1.1 Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтың құрылымы мен түсінігі

Қазіргі технократиялық қоғамдағы әлеуметтік мәселелердің бірі ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың пайда болуы. Бұл қылмыстық құқық бұзушылықтар қоғамдағы ақпарттық салаға орасан зор шығын алып келуде. Азаматтар компьютерлік құрылғыларды пайдалану кезінде өздерінің жеке, жұмыс және қызмет барысындағы мәліметтерін жүктеу арқылы ақпараттарды сақтаудағы, өңдеудегі бағдарламаларды дұрыс пайдаланбау нәтижесінде компьютерлік қылмыскерлердің құрығына түсіп қалады. Сондықтанда жеке және заңды тұлғалардың ақпараттық қауіпсіздік мәселесі өте өзекті болып отыр.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың ғылымда нақты анықтамасы қалыптаспаған. Бұл мәселенің заңдық түсінігі ғылымда әлі күнге дейін дискуссиялық сипат алып келеді. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар компьютерлік құрылғыларды пайдалану арқылы жасалатын болғандықтан компьютерлік қылмыстардың аясында шектеледі [3, 15 б.].

Кейбір авторлар ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың заты компьютерлік ақпарат болып табылады және олар компьютерлік ақпарат саласындағы қылмыстарға жатады деп пайымдайды [4, 9 б.].

Т.М.Лопатинаның ойынша, компьютерлік қылмыстарға белгілі бір территорияда нақты қылмыс жасалған кезеңде компьютерлік ақпаратты жинау, өңдеу, сақтауды және материалдық пайда табу мақсатында компьютерді қолдануды болып табылады [5, 39 б.].

Д.В. Добровольский компьютерлік ақпараттың заты болып табылатын қоғамға қауіпті әрекеттер ғана емес, барлық ақпараттық технологиялар саласындағы жасалған барлық қылмыстық құқық бұзушылықтарды жатқызады [6, 45 б.].

А.А.Жмыховтың пайымдауынша копьютерлік жүйелерді немесе желілерді пайдалана отырып жасалатын барлық қылмыстық құқық бұзушылықтар. Сөйтіп ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстарға компьютерлік ақпарат саласындағы қылмыстардан басқа, есептеу техникасының көмегімен жасалатын ұрлық, алаяқтық және т.б. қылмыстық құқық бұзушылықтарды жатқызады [7, 19 б.].

Көптеген ғылыми еңбектерде киберқылмыстылық туралы заңнамалық түсініктер беріледі. Бұл түсініктер отандық және шетелдік еңбектерде кең

мағынада пайдаланылып жүр. Авторлардың көзқарасы бойынша бұл қылмысқа компьютерлік ақпараттық саласында жасалатын, яғни компьютерлік құрылғының, ақпараттық-телекоммуникациялық желілердің және ақпараттық технологиялардың көмегімен жасалатын қылмыстық құқық бұзушылықтар жатады [8. 5 б.]. Осыдан шығатын қорытынды ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар киберқылмыстылықтың бір бөлігі болып табылады.

И.М. Рассолов өзінің еңбегінде Интернетте жасалатын қылмыстық құқық бұзушылықтар, киберқылмыстылық және компьютерлік қылмыстылық түсінігі ортақ деген тұжырымға келеді [9, 253 б.].

Р.И.Дремлюганың көзқарасы бойынша интернет-қылмыстылық пен компьютерлік қылмыстылық түсінгі пареллелді болып табылады. Оның ойынша компьютерлік ақпарат саласындағы кез келген құқық бұзушылық интернет-қылмыстылық болып табылмайды. Өйткені Интернет желісі арқылы жасалған алаяқтық, ұрлық, бопсалау және т.б. – бұл интернет-қылмыстылық болып табылады. Сонымен қатар олардан келетін әсерлер Интернет желісінде болу міндетті емес деп есептейді [10, 45 б.].

Жоғарыда баяндалған ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың түсінігіне тар және кең мағынада түсінік беруге болады.

Авторлардың пайымдауынша ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың тар мағынасына негізгі объектісіне компьютерлік ақпаратты өңдеу мен сақтауды қорғайтын қоғамдық қатынастар жатса, затына ақпараттық-телекоммуникациялық желілердегі компьютерлік ақпараттар жатады.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың кең мағынасына ақпараттық технологиялар мен компьютерлік ақпараттың қауіпсіздігі саласындағы кез-келген қоғамдық қатынастар жатады. Мұндағы компьютерлік ақпаратты құру, сақтау, өңдеу және тарату (компьютерлер, смартфондар, кассалық аппараттар, банкоматтар, төлеу терминалдары және басқа да компьютерлік құрылғылар) қылмыстық әрекеттің заты болып табылады және қылмыс жасаудың құрылғысы ретінде танылады.

Сөйтіп ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың тар мағынасына Қазақстан Республикасының Қылмыстық кодексіндегі 7 тарауында қылмыстық жауаптылық қарастырылған компьютерлік ақпарат саласындағы қылмыстық құқық бұзушылықтарды қамтиды.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың кең мағынасына киберқылмыстылық, интернет-қылмыстылық, ақпараттық технологиялар саласындағы қылмыстардың түсінігін жатқызамыз. Біз осындай түсінікті қалыптастыру арқылы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың көп салалығын ғылыми тұрғыдан бөліп алуға көмектеседі.

Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашадағы «Қазақстан Республикасы ақпараттық қауіпсіздігінің 2016 жылға дейінгі тұжырымдамасы турады» Жарлығына сәйкес, ақпараттық қауіпсіздікті қамтамасыз етудің ағымдағы мынадай қатерлермен сипатталады:

1) аса маңызды ақпараттандыру объектілердің ақпараттық қауіпсіздігін қамтамасыз ету жүйесінің жетілмеуі және жұмысының бұзылуы;

2) заманауи ақпараттық-коммуникациялық технологияларды жасаудың, енгізу мен пайдаланудың қоғамның объективті қажеттілігіне жауап бермейтін төменгі деңгейі;

3) Қазақстан Республикасының ақпараттық технологиялар, ақпараттандыру және ақпаратты қорғау құралдары импортына тәуелді болуы, оларды пайдалану елдің ұлттық мүдделеріне зиян келтіруі мүмкін;

4) әлемдік жетекші күш орталықтары арасындағы ақпараттық, қарсы тұрудың үдей түсуі, ақпараттық кеңістікте шет мемлекеттердің күреске дайындалуы және жүргізуі;

5) жаһандық ақпараттық мониторинг саласындағы шет мемлекеттердің дәйексіз саясаты, ақпараттар мен жаңа ақпараттық технологиялардың таралуы;

6) ақпаратпен айлы-шарғылар жасау технологиясының дамуы;

7) елдің ұлттық мүдделеріне нұқсан келтіретін, қоғамдық сана мен мемлекеттік институттарға арандатушы ақпараттық әсер ету мүмкіндіктері;

8) Қазақстан Республикасының ұлттық мүдделеріне зиян келтіруге қабілетті сенімсіз және қасақана бұрмаланған ақпарат тарату;

9) ұлттық ақпараттық кеңістіктің ашықтығы және сыртқы әсерлерге осалдығы;

10) мемлекеттік саясатты ақпараттық қамтамасыз ету тиімділігінің жеткіліксіздігі;

11) ұлттық ақпараттық кеңістіктің әлсіз қорғалуы мен бәсекеге қабілеттілігінің төмендігі;

12) ұлттық контент сапасының қазақстандық қоғамның объективті қажеттіліктеріне және әлемдік деңгейге сәйкес келмеуі;

13) ақпараттық-коммуникациялық технологияларды пайдаланатын қылмыстың, оның ішінде трансұлттық қылмыстың, сондай-ақ экстремистік, террористік әрекеттің көбеюі;

14) Қазақстан Республикасының ақпараттық ресурстарына оның ұлттық мүдделеріне зиян келтіруге әкелетін, сырттан рұқсат етілмеген қол жеткізуге әрекет жасау;

15) шетелдік барлау және арнайы қызметтерінің, сондай-ақ шетелдік саяси және экономикалық құрылымдардың Қазақстан Республикасының мүдделеріне қарсы бағытталған қызметі;

16) Қазақстан Республикасының мемлекеттік құпияларын құрайтын мәліметтермен жұмыс істеу кезінде құпиялылық режимінің бұзылуы, сондай-ақ қолжетімділігі шектелген ақпаратпен жұмыс істеу кезінде

қасақана құқыққа қайшы әрекет пен абайсызда жасалған қателер мен жолсыздықтар;

17) ақпараттық саланы құқықтық реттеу жүйесінің жеткіліксіз дамуы;

18) дүлей зілзалалар мен апаттар;

19) жеке және заңды тұлғалардың, мемлекеттің ақпараттық саладағы заңды құқықтары мен мүдделерін бұзуға әкелетін мемлекеттік құрылымдардың құқыққа қайшы әрекеті [11].

2001 жылдың 23 қарашада Будапештте «Компьютерлік қылмыстар туралы Конвенцияға» қабылданды және оған Еуропа Кеңесінің 50 шақты мемлекеті ратификация жасаған болатын. Конвенцияға сәйкес компьютерлік ақпарат саласындағы қылмыстарды бес негізгі топқа бөледі: компьютерлік жүйе мен мәліметтерге кіру мен толықтығының құпиялығына қарсы қылмыстар; компьютерлік құрылғыларды пайдалану арқылы жасалатын қылмыстар; компьютерлік мәліметтердің мазмұнымен байланысты құқық бұзушылықтар; авторлық құқықтың бұзылуымен байланысты құқық бұзушылықтар; компьютерлік желілер арқылы расизм және ксенофобия актілерін жасау [12].

Қазақстан Республикасы саяси және заңнамалық себептерге сәйкес, жоғарыдағы Еуропа Кеңесінің конвенциясын ратификациялаған жоқ. Бірақта Қазақстан Республикасының ІІМ компьютерлік қылмыстарды тергеу және ашу барысында осы саладағы қылмыстарды саралауда оған сүйене алады.

Бірақта қазақстандық заң шығарушы ҚР қылмыстық кодексіндегі (205, 206, 207, 208 баптар) бірнеше баптарда ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды саралайтын белгілерін жатқызады.

Ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды саралау мәселесі әлі нақты қалыптасып болмады. Ресейлік киберқылмыстылықты тергейтін және алдын алумен шұғылданатын Group-IB халықаралық сараптама жүргізетін компаниясы мынадай негізгі қылмыстық құқық бұзушылықтарды бөліп көрсетеді:

- интернет-банкинг жүйесіндегі алаяқтық;
- фишинг;
- электронды ақшаларды жымқыру;
- әртүрлі заңсыз табыстарды қолма-қол ақшаға ауыстыру;
- спам (әртүрлі контрафактілі тауарларды және дәрі-дәрмекті заңға қайшы жарнамалау, жалған бағдарламалар тарату және т.б.);
- трафик сату;
- эксплойттар сату;
- анонимизация;
- DDoS-шабуылдар [13].

Өз кезегінде ресейдегі және дүние жүзіндегі киберқылмыстылықтың жыл сайынғы жағдайына сараптама жүргізетін «Касперский Лабораториясының» мамандары компьютерлік қауіптерге мыналарды жатқызады:

- мақсатты түрдегі кибершабуылдар;
- кибертыңшылық;
- хактивизм;
- құпия мәліметтерді ұрлау;
- кибербопсалау;
- жалдамалы кибершабуылдар;
- ұялы құрылғылар үшін зиян келтіретін бағдарламаларды пайдалану;
- бағытты фишинг;
- жеке өмірдің құпиялығын бұзу;
- ботнеттерді пайдалану [14].

Вирусқа қарсы бағдарлама дайындайтын Panda халықаралық компаниясының құрамына енген PandaLabs лабораториясының мамандарының көзқарасы бойынша компьютерлік қылмыстылықты қалыптастыратын құқық бұзушылықтарды атады:

- кибершантаж (мысалы, CryptoLocker зиян келтіретін бағдарлама компьютердегі барлық құжаттарды (электронды кестелер, құжаттар, фотографиялар және т.б.) оқи алады және жояды, кейін киберқылмыскерлер өзінің құрбандарына файлдарды қалпына келтіру үшін сыйақы сұрайды);

- ұйымның, мекеменің, компанияның ақпараттық ресурстарына бағытталған кибершабуылдар;

- клиенттердің банктік карталарынан мәліметтерді ұрлау үшін төлем терминалдарына кибершабуылдар;

- APT-шабуылдар (APT — Advanced Persistent Threats) – ipi компаниялардың және стратегиялық маңызды институттардың ақпараттарына бағытталған жиі шабуылдар;

- Интернетке қосылатын құрылғыларды бұзу – IP-камерадан бастап принтерге дейін;

- смартфондарға және басқа да ұялы байланыс құралдарына қолданушының мәліметтері мен парольдерін ұрлау мақсатындағы шабуылдар [15, 326 б.].

Қарастырылып отырған тақырып бойынша ғылыми әдебиеттер компьютерлік қылмыстық құқық бұзушылықтардың әртүрлі көзқарастарда екендігіне көзіміз жетеді. Мысалы, Д.К. Чирков и А.Ж. Саркисян ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарға компьютерлік ақпарат пен телекоммуникация саласында жасалатын қылмысарды ғана жатқызуды ұсынады [16, 220 б.].

Ал М.Б. Эмиров, А.Д. Саидов, Д.А. Рагимхановтың пайымдауынша, компьютерлік желілерде кең тараған бопсалау, арандату, вандализм, спуфинг (парольдерді бұзу), алаяқтық сияқты құқық бұзушылықтарды жатқызады [17, 65 б.].

Басқа авторлар ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың құрылымының күрделілігіне байланысты, оның объектісіне, қол сұғушылық пәніне және жасалу тәсіліне сәйке қарастыруды ұсынады [18, 48 б.]. Мысалы, қол

сұғушылық объектісіне байланысты келесідей компьютерлік қылмыстардың тобына бөледі: компьютерлік желінің және компьютерлік мәліметтердің толықтығына, қол жетімдігіне, құпиялығына қарсы қылмыстар; экономикалық компьютерлік қылмыстар; адамның жеке өміріне қарсы компьютерлік қылмыстар; қоғамдық және мемлекеттің мүддесіне қарсы компьютерлік қылмыстар.

Қазақстан Республикасының Бас прокуратурасы Құқықтық статистика және арнайы есепке алу жөніндегі комитеті есебіне сәйкес, интернет-алаяқтық бойынша 2018 жылы – 535; 2019 жылы – 8210; 2020 жылдың 7 айында – 7027 қылмыстық құқық бұзушылық тіркелген.

Сөйтіп ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың көпшілігі компьютерлік ақпарат саласындағы интернет-алаяқтық қылмыстары болып отыр. Бұл қылмыстық құқық бұзушылықтың соңғы жылдарда артуына Дүниежүзілік денсаулық сақтау ұйымы Covid-19 коронавирусына байланысты пандемия жариялауына байланысты да болуында.

Қазақстан Республикасындағы ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды қарастыра келе, мынадай қорытынды жасауға болады:

- Қазақстандағы қылмыстылықтың бір түрі болып табылады, ол экономикалық, зорлық-зомбылық, сыбайлас жемқорлық, экологиялық және басқа да құқық бұзушылықтармен қатар жүреді;

- басқа да қылмыстық құқық бұзушылықтармен тығыз байланысты, өйткені компьютерлік ақпарат саласындағы құқық бұзушылықтар басқа да құқық бұзушылықтардың тәсілі болып табылады (ұрлық, бопсалау, банктік, коммерциялық және мемлекеттік құпияларды заңсыз жолмен алу);

- жоғары технологиялық сипаттағы IT-технологияны қолдану арқылы жасалатын қылмыс құралы немесе құрылғысы;

- өте жоғары латентті – компьютерлік қылмыстың құрбандары құқық қорғау органдарына жиі хабарласпайды, виртуалды ортада жасалатындықтан көптеген азаматтарға көрінбейді; арнайы құқық қорғау органдарында осы қылмысты ашумен айналысатын мамандардың тапшылығымен байланысты;

- өте жоғары деңгейде ұйымдастырылуымен және ұйымдасқан қылмыстылықпен тығыз байланысты, өйткені көптеген компьютерлік қылмыстар (DdoS-шабуылдар, банкинг, фишинг, ботнеттер құру және т.б.) ұйымдасқан қылмыстық топтармен жасалады;

- өте «кәсіби» сипатқа ие болады, IT-технология саласында қажетті білімі, тәжрибесі бар; қылмыстық жолмен әрекет жасау арқылы «табысқа» кенеледі; өзі сияқты қылмыскерлермен тәжірибесімен алмасып отырады;

- шекараның жоқтығымен сипатталады, яғни киберкеңістікте мемлекеттік шекараның болмауы қылмыскерлерге басқа мемлекеттің территориясында отырып, басқа мемлекеттегі тұлғаға қарсы қылмыс жасай алады;

- трансұлттық сипатқа ие; компьютерлік қылмыскерлер қылмыстық жолмен табыс табу мақсатында өздерінің жолын жеңілдету үшін екі және

оданда көп мемлекеттерде ұлтына, дініне қарамастан халықаралық топтарға біріге алады; ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың, оның ішінде ұйымдасқан трансұлттық қылмыстық топтар қызметінің таралуы айтарлықтай проблеманы құрайды. Киберқылмыстардың ерекшелігі олардың аса жасырын болуы. Осының салдарынан, қазіргі заманғы ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалған ресми тіркелген қылмыстар нақты жасалған қылмыстың азғана көбею үстінде. Ақпараттық қылмысқа қарсы күрес құқық қорғау органдарынан және арнайы қызметтерден шет елдердің арнайы қызметтері мен құқық қорғау органдарымен бірігіп, үйлестірілген іс-қимыл жасау жолымен барабар жедел әрекет етуді талап етеді;

- әрқашан динамикалық даму үстінде болады; азаматтар мен ұйымдардың, мекемелердің электронды құжат айналымына көшу, Интернет қолданушылардың көбеюі, ұялы байланыс құралдарының дамуы, жаңа IT-технологиялардың шығуы мен жетілуіне байланысты киберкеңістікте жаңадан қылмыс жасаушылар қосылып отырады;

- экономикалық қылмыстылықпен тығыз байланысты, өйткені компьютерлік қылмыскерлердің негізгі мақсаты жаңа табыс көздерін іздеуде және олар қаржылық-банктік немесе корпоративтік секторларда (интернет-банкинг, банктік фишинг, кибербопсалау және т.б.) жасалады;

- шетелдік мемлекеттердегі халықаралық эктремистік және террористік ұйымдардың (Интернеттегі экстремистік және террористік сипаттағы вербовкамен байланысты) шабуылдарымен байланысты болады. Экстремистік және террористік ұйымдар мен топтар өз идеологияларын насихаттау, пікірлестерін тарту мен оқыту, әртүрлі террористік топтармен байланыста болу және қаржыландыру үшін жаһандық ақпараттық-коммуникациялық желілер мүмкіндіктерін барынша белсенді пайдалануда. Қазақстан жастары арасында әртүрлі пайымдағы радикалды идеяларды тарату алаңдаушылық туғызады. Қазақстан азаматтары мақсатты насихаттың әсерімен, оның ішінде Интернет желісі арқылы әлемнің түрлі өңірлеріндегі заңсыз акцияларға қатысу жағдайлары байқалуда. Террористік қызметті жүзеге асыру әдісі сияқты мемлекеттің ақпараттық жүйелеріне компьютерлік шабуылдарды пайдалану қаупі өсуде. Мұндай шабуылдар көптеген елдерде бірнеше рет тіркелді [11].

Біз жүргізген ғылыми зерттеулердің нәтижесінде ақпараттық-телекоммуникациялық желілерді белсенді түрде қолданатын салалар анықталды. Шамамен оларды он негізгі салаларға бөлуге болады:

- ұйымдастырушылық-басқарушылық саласы;
- технологиялық басқару және өндірістік процесс саласы;
- автоматтандыру және моделдеу саласы;
- қашықтықтан оқыту және білім техногиялары;
- телемедицина;
- ақпараттық қамтамасыз ету, оның ішінде мемлекеттік және әкімшілік қызмет;

- ақпараттық-телекоммуникациялар өндірісі;
- коммуникация;
- қаржылық сала.

Айта кететін бір жайт, қаржылық саладағы электрондық жүйе мен коммуникацияның тез қарқынмен дамуы, осы салада жасалатын қылмыстық құқық бұзушылықтардың көбеюіне алып келді.

Зерттеудің пәні ретінде ақпаратық-телекоммуникацциялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың түсініігін анықтап алу қажет. Оның ішінде IT-технологияларды пайдалану арқылы жасалатын қылмыстардың түсінігі керек болып отыр.

Қазіргі уақытта отандық заңнамада ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың ортақ түсінігі жоқ. Халықаралық және отандық заңнаманың қайнар көздерінде ақпаратық-телекоммуникацциялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарға қатысты қоланылатын ортақ терминология қалыптаспаған.

Кейбір авторлар «ақпаратық-телекоммуникацциялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылық» терминін «киберқылмыстылық» терминімен тығыз байланыстырады [19, 46 б.], кейбіреулері «компьютерлік ақпарат саласындағы қылмыс» терминін пайдалануды ұсынады [20].

Оксфордтың талдама сөздігінде «киберқылмыстылық» (ағыл. «cybercrime») – «компьютерлер немесе Интернетті пайдалану арқылы жасалатын қылмыстық қызмет» деп атайды [21].

Ал М.Макмиллан сөзігінде «киберқылмыстылық» дегеніміз «Интернетті қолдану арқылы жасалған қылмыстар», мысалы жеке ақпараттарды ұрлау немесе бөтен біреудің компьютеріне зиянды бағдарламаларды енгізу [22].

«Википедия» энциклопедиясында «киберқылмыстылық» - «ақпараттық технологиялар саласында жасалатын қылмыстар» деген анықтама береді [23].

Біз зерттеп отырған термин туралы ғылымда нақты жауап жоқ болып отыр. Т.Л.Тропинаның ойынша, «компьютер жұмысына, компьютерлік бағдарламаларға, компьютерлік желілерге әсер ету арқылы қылмыстық жауапкершілікке алып келетін аса қауіпті қоғамдық құбылыс» [24, 64 б.].

И.Г.Чекуновтың пайымдауынша, «жеке қылмыс түріне жатады және оны қылмыс ретінде танудың объективті үш белгісі болады, яғни қылмыс құралы (зиянды бағдарламалар), бағдарламалық-техникалық құрал және компьютер желісіне немесе ұялы оператор желісіне қосылуы жатады» [25, 7 б.].

А.Ю.Чупрованың көзқарасы бойынша ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар «электронды коммерция» түсінігімен анықталады, яғни «отандық және халықаралық заңнамаға сәйкес, экономикалық қызметтен табыс алуға бағытталған ұйымдар мен жеке тұлғалар арасындағы

электронды коммуникациялық өзара байланыс» деп есептейді [26, 27 б.]. Біздің көзқарасымыз бойынша бұл анықтама ақпарат саласындағы барлық қылмыстарды қамти алмайды. Өйткені бопсалау, кәмелетке толмағандарға порнографиялық материалдар мен заттарды дайындауға итермелеу қылмыстары бойынша даулы болып табылады.

Шетелдік зерттеушілердің ойынша, «киберқылмыстылықтың» криминологиялық түсінігі «компьютерлік қылмыс» түсінігіне кең болып келеді және олар IT саласындағы барлық қылмыстарды жатқызады [27]. Бұл түсінікті біз жалпыдан жекеге өту арқылы анықтауымызға болады: киберқылмыстыққа ақпараттық кеңістікте ақпараттық-телекоммуникацияларды, құрылғыларды және Интернет желісін пайдалану арқылы жасалған барлық қылмыстарды жатқызамыз.

«Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар» түсінігі – криминологиялық түсінік және ол IT саласындағы әлеуметтік-құқықтық қылмыстық құбылысын бөліп көрсетеді.

Т.Н.Богданова қылмыстық заңнамада нақты бір техникалық құралдың қылмыс құралы болып табылатындығы қазіргі кезде ескірген деп есептеу қажет дейді [28, 64 б.].

А.Фоменко ақпараттық-телекоммуникациялық технологиялар арқылы жасалатын қылмыстық құқық бұзушылықтардың мынадай ерекшеліктерін атап көрсетеді: қылмыс құралы ретінде көп қырлы және жоғары технологияның қылмыс құралына айналуы [29, 45 б.].

IT-технологиясы саласындағы қылмыстарға сипаттама берген кезде «ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстар» деген терминді пайдалану ақпараттық қауіпсіздік саласындағы қылмыстық-құқықтық шаралардың тиімділігін арттыра түседі. Мұндай көзқарасты осы саланы зерттеп жүрген басқа да ғалымдар қолдап отыр [30, 7 б.]. Ұсынылған тұжырымдамамен сауалнама алған респонденттердің 60 пайызы қолдаған болатын.

Қарастырылып отырған саладағы заңнаманы зерттей келе, біз «ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстарға» ақпараттық-телекоммуникациялық желілерді пайдалану арқылы заңмен қорғалатын ақпаратқа қауіп төндіретін қоғамға аса қауіпті қоғамдық әрекет деген тұжырымға келдік.

IT технологиясы саласындағы қылмыстарды зерттеп жүрген шетелдік ғалым Д.Уолл төмендегідей саралауды ұсынады:

- компьютер жұмысына кедергі келтіретін қылмыстар, оған компьютердегі ақпаратты модификациялау және бұғаттау, бұзу;
- желілік ресурстардың мазмұнымен байланысты қылмыстар, яғни порнографиялық материалдарды, экстремистік және террористік сипаттағы материалдарды жүктеу;
- қаржылық алаяқтық жобаларды жүзеге асыру үшін компьютерлерді пайдалану арқылы жасалатын қылмыстар [31].

Дәл осындай көзқарас халықаралық заңнамада да қалыптасқан. Яғни, киберқылмыстылықпен күрес бойынша Еуропалық Конвенцияда қылмыстың негізгі түрлерін бөліп көрсетіледі: компьютерлік мәліметтер мен жүйеге қарсы қылмыстар; компьютерлік құрылғыларды пайдаланумен байланысты қылмыстар; мәліметтердің мазмұнымен байланысты қылмыстар; нәсілдік, діндік дискримиминацияға алып келетін ақпараттарды таратумен байланысты қылмыстар [12].

Ресейлік ғалымдар В.В.Хилюта [32] мен Е.В.Громов [33] ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды мынадай топтарға бөледі: компьютерлік техниканы және ақпаратты тасымалдаушы құрылғыны жоюға немесе зақым келтіруге бағытталған қылмыстық құқық бұзушылықтар; компьютердегі ақпаратты заңсыз алуға бағытталған қылмыстық құқық бұзушылықтар.

В.С.Карпов ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды екі топқа бөледі: біріншісі, компьютерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар, оның ішінде компьютерлік алаяқтық, компьютерлік ақпаратты заңсыз иемдену, зиян келтіретін бағдарламаларды дайындау, пайдалану және тарату, екіншісі компьютерлік қылмыстармен жапсарлас қылмыстық құқық бұзушылықтар [34].

А.Л.Осипенко «желілік қылмыстарға» төмендегідей анықтама бере кетеді: «жаһандық компьютерлік желілерге құқыққа қарсы сипаттағы материалдарды орналастыру» [35, 160 б.].

Біздің ойымызша жоғарыда талдау жасалған көзқарастардың ешқайсысы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың нақты анықтамасын бере алмайды. Біздің көзқарасымызша компьютерлік ақпарат саласындағы қоғамдық қатынастарды қорғауға бағытталуы қажет.

Ақпараттық-телекоммуникациялық желілер арқылы жасалатын қылмыстық құқық бұзушылықтар «желілік құқық бұзушылықтар» деп аталады. Өйткені ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар үшін жауапкершілік қарастырылған нормаларға талдау жасау арқылы Қылмыстық заңнамадағы кейбір нормаларды кездестіре аламыз. Атап айтсақ, «ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу»; «ақпараттық жүйенің немесе телекоммуникациялар желісінің жұмысын бұзу»; «құқыққа қайшы мақсаттарды көздейтін интернет-ресурстарды орналастыру үшін қызметтер ұсыну» сияқты сараптайтын белгілері кездеседі.

Ақпараттық-телекоммуникациялық технологияларды пайдалану арқылы жасалуы мүмкін басқа да құқық бұзушылықтарды атап көрсетуге болады: қаржылық (инвестициялық) пирамиданы құру және оған басшылық ету (217 бап), қылмыстық жолмен алынған ақшаны және (немесе)өзге мүлікті заңдастыру (жылыстату) (218 бап), кредитті заңсыз алу немесе бюджеттік кредитті мақсатсыз пайдалану (219 бап), жалған төлем карточкалары мен

өзге де төлем және есеп айырысу құжаттарын жасау немесе өткізу (232 бап), авторлық және (немесе) сабақтас құқықтарды бұзу (198 бап), адам саудасы (128 бап), хат жазысу, телефонмен сөйлесу, пошта, телеграф хабарлары немесе өзге де хабарлар құпиясын заңсыз бұзу (148 бап), алаяқтық (190 бап) [36].

Айта кететін жайт, ақпараттық-телекомуникациялық технологияларды пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың саны қоғамның ақпараттануына байланысты жыл сайын өсіп келеді. Біздің ойымызша, болашақта медицина немесе білім беру саласындағы ақпараттық-телекоммуникациялық технологияларды пайдалану арқылы жасалатын құқық бұзушылықтарды қарастыруымыз мүмкін.

Осы тармақшаны қорытындылай келе мынадай тұжырымдама жасаймыз:

- «Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар» түсінігіне ақпараттық-телекоммуникациялық желілерді пайдалану арқылы заңмен қорғалатын ақпаратпен байланысты қоғамдық қатынастарға (адамның жеке құқығына, қоғамның және мемлекеттің өміріне) залал келтіретін қоғамға қауіпті әрекет болып табылады;

- Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жүргізілген зерттеулердің нәтижесінде келесідей түрлерге бөлуге болады:

1) «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар», яғни қылмыстық кодекстегі 205-213 баптар, олар компьютерлік ақпарат саласындағы қоғамдық қатынастардың қорғалуына бағытталған;

2) «желілік құқық бұзушылықтар», яғни ақпараттық-телекоммуникациялық желілер бұл саладағы қылмыстық құқық бұзушылықты жасаудың құралы болып табылады (Қылмыстық кодекстің 128, 148, 190, 198, 217, 218, 219, 232 баптар).

2.1 Ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылық саласындағы шетелдік заңнамаға салыстырмалы-құқықтық талдау

Қазіргі уақытта ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстардың болуы Қазақстан экономикасына орасан зиян келтіруде. Сонымен қатар мемлекет пен қоғамның ақпараттық қауіпсіздігіне де қауіп төндіреді.

Сондықтан қазақстандық құқық қорғау органдарының және ғылыми қауымдастықтың алдында тұрған өзекті мәселелердің бірі – ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарға қарсы іс-қимыл жасау және оған қарсы қылмыстық-құқықтық заңнаманы жетілдіру.

Ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін жауапкершілікті реттейтін отандық қылмыстық құқықтың тиімді әдістерін жетілдіру үшін шетелдік заңнамаларына талдау жасау қажет және осы салада күрес жүргізіп келе жатқан мемлекеттердің озық тәжірибелерін зерттеу керек деп ойлаймыз.

Киберқылмысты ескертудің бұл тобына бәрінен бұрын компьютерлік саладағы заңға қарсы әрекеттерге қылмыстық жауапкершілік орнықтыратын заң нормалары жатады. Егер тарихқа жүгінсек, осындай типті бірінші нормативтік-құқықтық акт американ штаттары Флорида мен Аризонда 1978 жылы қабылданғанын көреміз. Бұл заң «Computer crime act of 1978» деп аталды. Сонан кейін Американың барлық штаттарында осындай заң қабылданды. Бұл құқықтық акттар заңның ары қарай компьютерлік қылмысты ескерту шараларын жүзеге асырудағы түбегейлі негізі болды [37, 179 б.].

Ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстар саласындағы жауаптылықты реттейтін Ресей, АҚШ, Франция, Германия, Швеция және т.б. дамыған мемлекеттердің заңнамасындағы қылмыстық-құқықтық нормаларына талдау жасаймыз.

Англо-американдық құқықтық отбасы. Америка Құрама Штаттары басқа мемлекеттерге қарағанда компьютерлік қылмыс ертерек пайда болған ел және оған қарсы қылмыстық жауапкершілікті бойынша шаралар қабылдаған әлемдегі алғашқы мемлекеттердің бірі болды.

1977 жылы АҚШ-та федералды деңгейде федералды компьютер жүйесін қорғау туралы заңның жобасы жасалған болатын. Онда мынадай құқық бұзушылықтарға қылмыстық жауапкершілік қарастырылды: компьютерлік жүйеге жалған ақпараттарды қасақана енгізу, компьютерлік құрылғыны заңсыз пайдалану, ақпараттарды өңдеу процесіне өзгерістер енгізу немесе бұл процестерді бұзу, компьютерлік технология мүмкіндіктерін пайдалана отырып ақшаны, бағалы қағаздарды, мүлікті, қызметті, бағалы ақпаратты жымқыру. Осы заң жобасының негізінде 1984 жылдың қазан айында «Компьютерді теріс пайдалану және алаяқтық туралы» заң қабылданды. Бұл нормативтік-құқықтық акт – компьютерлік ақпаратқа заңсыз иелік етуге қылмыстық жауапкершілікті қарастырады [38, 88 б.].

Біздің зерттеуіміз компьютерлік қылмыстылыққа арналғанына байланысты АҚШ заңдарының § 1029 жауапкершілікке тоқтала кеткенді жөн көрдік, яғни:

- жалған құрылғыны пайдалану және сату;
- 1000 доллардан асатын сомаға заңсыз түрде материалдық игіліктерді алу мақсатында құрылғыны пайдалану;
- 15 және оданда көп жалған немесе рұқсат етілмеген құрылғыларды пайдалану;
- жалған құрылғыларды жасау арқылы сату немесе иелік ету;
- басқа тұлға арналған құрылғы көмегімен мәміле жасау.

АҚШ заңдар жиынтығының § 1030 «а» тармақшасында зиянды компьютерлік бағдарламаларды пайдалану және тарату бойынша жеті қылмыс құрамына жауапкершілікке қарастырылған.

1. Компьютерлік шпионаж - мемлекеттік қауіпсіздік,халықаралық қатынастар және атом энергетикасы мәселелері бойынша заңсыз ақпаратқа иелік ету;

2. АҚШ-тың үкіметтік ведомствалық ақпаратына заңсыз ену немесе белгіленген нормадан асып кетуі;

3. Компьютерді қолдану арқылы алаяқтық – компьютерді алаяқтық мақсатта пайдалана отырып, алаяқтық пиғылын іске асыру үшін желіге қосылу;

4. Қорғалған компьютерлерді қасақана немесе абайызда істен шығару;

5. АҚШ үкіметі қолданатын компьютерлеріне заңсыз қосылуға мүмкіндік беретін компьютерлік парольдерді немесе ақпараттарды сату арқылы алаяқтық;

6. Компьютерлік технологияларды пайдалану арқылы бопсалау, қорқыту және басқа да құқыққа қайшы әрекеттер.

§ 1030 «а» тармақшасындағы қылмыстық әрекеттер үшін санкция өте қатал болып келеді. Жоғарыда аталған барлық тармақтар үшін 10 жылға дейін түрмеге қамау қарастырылған, ал құпия ақпарат алу немесе рецидив болған жағдайда 20 жылға дейін бас бостандығынан айыру көзделген [39].

Сөйтіп АҚШ заңнамасына қорытынды жасайтын болсақ, ақпарттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін жауапкершілік реттелген және қылмыстың барлық сатысында (дайындалу, оқталу, аяқталған) қатаң санкция қарастырылған.

Скандинавтық құқықтық отбасы. Шетелдік заңнамаға талдау жасай отырып, компьютерлік ақпараттарды қорғау бойынша алғашқы қадамды АҚШ емес, Швецияда 1973 жылы 4 сәуірде қабылданған «Мәліметтер туралы заңы» болды. Онда «компьютер көмегімен қастандық жасау» термині енгізілген болатын.

Қазіргі уақытта Швеция королдігінің Қылмыстық кодексінде компьютерлік қылмыстар туралы арнайы тарау белгіленбеген. Бұл қылмыстың түрлері мен жауаптылығы қылмыстық кодекстегі әртүрлі баптарда көрініс тапқан. Мысалы, Швеция ҚК-нің 4 тарауы, 9 бабында «автоматты мәліметтер жүйесіне заңсыз енсе немесе заңсыз түрде өзгертсе, жойса айыппұл төлейді немесе екі жылға дейін түрмеге қамалады» [40].

Данияның Қылмыстық кодексінде де компьютерлік қылмыстар үшін жауаптылықты қарастыратын арнайы тарау және баптар жоқ, бірақ кінәлілер осындай құқық бұзушылықтар жасаған жағдайда жауаптылыққа тартылады. Мысалы, Дания ҚК-нің § 193 сәйкес, байланыс құралдарының қызметіне, телефон және телеграф қызметіне, мәліметтерді өңдеу базасына заңсыз кедергі келтірсе, төрт жылға дейін түрмеге қамалады, ал жеңілдететін жағдайлар болған кезде айыппұл төлейді [41].

Роман-германдық құқықтық отбасы. 1989 жылы 13 қыркүйекте Еуропалық Кеңесі министрлер Кеңесінің отырысында компьютерлік құқық бұзушылықтардың тізімі анықталды. Осының негізінде «Құқық бұзушылықтың минимальді тізімі» атты заңнама қабылданды, оған төмендегідей компьютерлік қылмыс түрлері енді: компьютерлік алаяқтық, жалған компьютерлік ақпарат, ЭВМ бағдарламалары мен мәліметтерді бұзу, компьютерлік саботаж; заңсыз түрде қосылу; заңсыз түрде мәліметтерді қабылдау; қорғалған компьютерлік бағдарламаларды заңсыз түрде пайдалану.

1995 жылға дейін Франция, ГФР, Австрия, Нидерланды, Португалия сияқты еуропалық мемлекеттердекомпьютерлік ақпарат саласындағы қылмыстық жауаптылықты бекітетін заңдар қабылданды.

Мысалы, 1994 жылы Герман Федеративті Республикасында «Ақпараттарды қорғау туралы» федеративті заң қабылданды, ал ГФР Қылмыстық кодексіне мынадай компьютерлік қылмыстардың құрамы енгізілді:

- электронды, магнитті және басқа жолмен берілетін мәліметтерді өзі немесе басқа тұлға үшін заңсыз алу (§ 202а);
- дәлелдемелік маңызы бар мәліметтерді қолдан жасау (§ 269);
- техникалық жазбаларды өзгертетін және жоятын (§ 274) ;
- мәліметтерді заңсыз өзгертетін, жоятын және жарамсыз қылатын (§303а) [42].

ГФР Қылмыстық кодексінің 22 тарауында (Алаяқтық және сенімге заңсыз ену) § 263а «Компьютерлік алаяқтық» мазмұндалады, яғни заңсыз бағдарламаларды пайдалану арқылы өзіне немесе үшінші тұлғаларға мүліктік пайда табу мақсатында жасалытын қасақана әрекет болып табылады.

Ал Францияның Қылмыстық кодексінің №6 тарауы №2 томында төмендегідей қылмыстық жауаптылық көзделген:

- компьютерлік мәліметтерді пайдалану арқылы адам құқықтарын бұзу – 1 жыл бас бостандығынан айыру;
- жеке тұлға туралы жеке мәліметтерді заңмен тыйым салынған немесе алдау түрінде жинау – 5 жыл бас бостандығынан айыру;
- ақпарат саласындағы террористік актілер – отыз жылға дейін бас бостандығынан айыру [43].

Франция ҚК-нің тағы бір ерекшелігі, ол компьютерлік қылмыстарға жеке тұлғалармен қатар заңды тұлғалардыңда тартылатындығы.

Социалистік құқық отбасы. Шет елдердің қылмыстық заңнамасын зерттей отырып, Қытай Халық Республикасының заңнамасынағы компьютерлік қылмыстылық пен оларды жасаудағы жауапкершілікке жеке тоқталып кеткенді жөн көрдік.

Қытай зиянды компьютерлік бағдарламаларды құрастыру, пайдалану және тарату бойынша әлемде бірінші орынды иеленіп келді.

Алайда, ҚХР Үкіметінің ақпаратты қорғау және оған қарсы күрес саласындағы қатаң және сауатты саясатының арқасында соңғы жылдары компьютерлік қылмыстар мен қылмыстық әрекеттердің санын айтарлықтай

төмендеді. Компьютерлік қылмысқа қарсы Қытайдың ұлттық заңнамасында өте қатал санкциялар қарастырылған.

Атап айтқанда, ҚХР ҚК компьютерлік ақпарат саласындағы қылмыстар және оларды жасағаны үшін төмендегідей санкциялар қарастырылған:

285-бап. Мемлекеттік істер және мемлекеттік жүйені қалыптастыруға және дайындауға жаңа ғылыми-техникалық әдістерге қатысы бар компьютерлік ақпараттық жүйеге заңсыз араласу – 3 жылға дейін бас бостандығынан айыруға немесе қамауға алу арқылы жазаланады.

286-бап. Компьютерлік ақпарат жүйесімен мынадай заңсыз әрекеттер жасалса, яғни компьютерлік ақпарат жүйесінің тұрақты жұмыс жасауына кедергі келтіру, мәтінді қысқарту (алып тастау), толықтыру жасалса, егер бұл әрекеттер елеулі салдарларға әкеп соқса - 5 жылға дейінгі бас бостандығынан айырумен немесе қамауға алумен жазаланады;

дәл осы әрекет аса ауыр зардаптарға әкеліп соқтыратын болса - 5 жылдан астам мерзімге бас бостандығынан айыруға жазаланады.

Компьютерлік ақпарат жүйесіндегі сақталған мәліметтерді заңсыз түрде түзету, қысқарту, толықтыру елеулі салдарға әкеліп соқса – осы баптың бірінші бөлігіне сәйкес жазаланады.

Компьютерлік ақпарат жүйесінің дұрыс жұмыс жасауына кедергі келтіретін компьютерлік вирустарды және деструктивті сипаттағы өзге де бағдарламаларды қасақана жасау және тарату елеулі салдарға әкеліп соқса – осы баптың екінші бөлігіне сәйкес жазаланады.

287-бап. Алаяқтық жолмен ақшаны иелену, пара беру мен қоғамдық қаржыны мақсатсыз пайдалану, мемлекеттік құпияны ұрлау және басқа да қылмыстық құқық бұзушылықтарды жасау үшін компьютерді пайдалану - осы Кодекстің тиісті баптарына сәйкес жазаланады (5 жылдан өмір бойы бас бостандығынан айыру) [44].

Қытайдың қылмыстық заңнамасының ерекшелігі компьютерлік қылмыскерлерге негізгі (мемлекеттік қауіпсіздікке қарсы қылмыстар) немесе қосымша жазаны (қоғамдық тәртіпке қарсы қылмыстар) қолдануға мүмкіндік беріледі – саяси құқықтардан айыру (сайлау және сайлану құқығынан; сөз және баспасөз бостандығынан, жиналыстар, одақтар, көшеде шерулер мен демонстрациялар өткізу құқығынан; мемлекеттік органдарда лауазымды қызмет атқару құқығынан, мемлекеттік компаниялардағы, кәсіпорындардағы, өндірістік емес бірліктердегі басшылық лауазымдарды атқару құқығынан) бір жылдан бес жылға дейін немесе өлім жазасына кесілген жағдайда өмір бойы бас бостандығынан айыруға сотталады (ҚХР ҚК 54 – 57 баптар).

Ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін қылмыстық жауаптылық қарастырылған шетелдік заңнамаларға салыстырмалы-құқықтық талдау жүргізе отырып, 2001 жылдың 23 қарашасында Будапешт қаласында қабылданған компьютерлік ақпарат саласындағы қылмыстар туралы Еуропа Кеңесінің Конвенциясына тоқтала кеткен жөн деп есептейміз. Қазіргі уақытқа дейін АҚШ, Канада, Оңтүстік-Африка Республикасы, Жапония және

басқа да еуропа мемлекеттерінен құралатын 47 мемлекет Конвенцияны ратификациялады [45].

Ресей бірнеше саяси және заңды себептерге байланысты, (мысалы, Конвенцияға қатысушы басқа да мемлекет-мүшелеріне, әсіресе АҚШ және НАТО мемлекеттеріне ақпараттық ресурстарға еркін қол жеткізуді ұсыну туралы мәлімдемесіне байланысты) аталған халықаралық-құқықтық актіне ратификациялаған жоқ.

Бірақта Конвенция, компьютерлік қылмыстар үшін жауапкершілікті көздейтін Ресейдің қылмыстық заңнамасын одан әрі дамытуға үлкен әсер еткені жасырын емес.

Алайда, Ресейлік заң шығарушы еуропалық, американдық немесе қытайлық заңнамаға қарағанда Қылмыстық кодексінде арнайы 28 тарау «Компьютерлік ақпарат саласындағы қылмыстар» қарастырылып, төрт бапты бапты қамтиды.

Қазақстан Республикасының 2014 жылғы 3 шілдедегі Қылмыстық кодексінде компьютерлік қылмыстық құқық бұзушылық бойынша жауаптылықты қарастыратын арнайы «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» тарау қарастырылған және ол 9 бапты қамтиды, яғни:

205 бап - Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу;

206 бап - Ақпараттық құқыққа сыйымсыз жою немесе түрлендіру;

207 бап - Ақпараттық жүйенің немесе телекоммуникациялар желісінің жұмысын бұзу;

208 бап - Ақпараттық құқыққа сыйымсыз иеленіп алу;

209 бап - Ақпаратты беруге мәжбүрлеу;

210 бап - Зиян келтіретін компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату;

211 бап - Қолжетімділігі шектелген электрондық ақпараттық ресурстарды құқыққа сыйымсыз тарату;

212 бап - Құқыққа қайшы мақсаттарды көздейтін интернет-ресурстарды орналастыру үшін қызметтер ұсыну;

213 бап - Ұялы байланыстың абоненттік құрылғысының сәйкестендіру кодын, абонентті сәйкестендіру құрылғысын құқыққа сыйымсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгертуге арналған бағдарламаларды жасау, пайдалану, тарату [36].

1996 жылы 17 ақпанда ТМД-ға қатысушы-мемлекеттердің Парламентаралық ассамблеясының VII пленарлық отырысында «Модельді Қылмыстық кодекс» қабылданып, оның XII тарауы «Ақпараттық қауіпсіздікке қарсы қылмыстарға» арналды. Онда ТМД мемлекеттерінің заңнамасына бекітілуі қажетті бірнеше баптар көрсетілген. Мысалы, 243-бап «Компьютерлік техниканы пайдалану арқылы ұрлау», 286-бап «Компьютерлік ақпаратқа құқыққа сыйымсыз қол жеткізу»; 287-бап «Компьютерлік ақпаратты түрлендіру»; 288-бап «Компьютерлік іріткі салу»; 289-бап «Компьютерлік ақпарат заңсыз иелену» [46].

Жоғарыда көрсетілген «Модельді Қылмыстық кодексте» компьютерлік қылмыстарға қарсы қылмыстық-құқықтық әсер етуінің бірнеше нұсқалары берілгендігін байқаймыз. Бірақта ТМД мемлекеттері осы кодекстің дайындалуына ат салысқан заң ғылымдарының еңбектеріне жүгіне қоймады. ТМД мемлекеттерінің ішінде тек Белорусь республикасы (ішінара Қазақстан, Ресей, Әзербайжан, Украина, Грузия) ғана заң шығаруда өзінің ұлттық қылмыстық заңнамасының ережелерін алды.

Ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін жауапкершілікті реттейтін шетелдік мемлекеттердің және қазақстандық заңнамаға салыстырмалы-құқықтық талдау жасай отырып, мынадай қорытындыларға келеміз.

Біріншіден ағылшын-американдық, скандинавтік, романо-герман және социалистік құқықтық отбасылардың қылмыстық-құқықтық жүйелерінде ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін заңнамалық актілерде (қылмыстық кодекстер немесе арнаулы заңдарда) қылмыстық жауапкершілікті нығайтуға жалпы тенденция байқалады.

Екіншіден, шетелдік қылмыстық заңнамалардың Қазақстан Республикасы Қылмыстық кодексінен айырмашылығы, ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар басқа қылмыс құрамдарында саралау белгісі ретінде немесе басқа қылмыстық әрекетті жасау тәсілі ретінде болуы мүмкін (мысалы, 9-бап 4-тарауы, 1-бап 9-тарауы Швеция ҚК; §206, §317, §263а ГФР ҚК; 226-18, 226-19 – баптары Франция ҚК).

Үшіншіден, қазақстандық заңнама заңдық техника тәртібі тұрғысынан ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар Қылмыстық кодекстің (7 тарау «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар») бір тарауына біріктірілген. Ал шетелдік қылмыстық заңнамада бұл қылмыстардың құрамы қылмыстық кодекстердің әртүрлі бөлімдерінде, тарауларында, бөлімшелерінде (кіші бөлімдерінде) немесе заңдар орналастырылған (Швеция ҚК, Дания ҚК, ГФР ҚК, Франция ҚК, ҚХР ҚК, Ұлыбритания қылмыстық заңнамасы).

Төртіншіден, қазақстандық қылмыстық кодексте ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтың субъектісі ретінде тек жеке тұлға танылады. Өз кезегінде скандинавтік және роман-германдық құқықтық отбасыларындағы қылмыстық заңнамада кінәлі ретінде заңды тұлғада бола алады (Швеция ҚК, Дания ҚК, Франция ҚК және т.б.).

Бесіншіден, біздің еліміздің қылмыстық заңнамасы бойынша ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасағаны үшін қылмыстық жауаптылыққа 16 жасқа толған жеке тұлға тартылады. Ал шет мемлекеттердің қылмыстық заңнамасы бойынша Латвия

ҚК (11-бап) – 14 жастан бастап, Дания ҚК (§15) - 15 жастан бастап, ҚХР ҚК (17 – бап) - 14-тен 16-ы жастан бастап қылмыстық жауаптылыққа тартылады.

Жоғарыдағы айтылғандарды талдай келе, автор ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар саласындағы жеке тұлғаларды қылмыстық жауаптылыққа тарту жасын, егер аса ауыр зардаптарға әкеліп соғатын болса, 16 жастан 14 жасқа дейін төмендетуді ұсынады. Өйткені ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарды жасайтын қылмыскерлер өз әрекеттері арқылы өте ауыр экономикалық зардаптарға әкеледі. Сонымен қатар он төрт жасқа толған жасөспірім қоғам мен ұжым алдындағы жауапкершілігін сезіне алатын, өзінің ойлау қабілетіне баға бере алатын дәрежеде бола алады.

Сондықтан автордың көзқарасы бойынша ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар үшін қылмыстық жауаптылықты қатаңдатуды ұсынады және компьютерлік қылмыстардың алдын алу үшін құқық қорғау органдары азаматтық қоғам институттарымен (бұқаралық ақпарат құралдарымен, білім беру мен ғылыми ұйымдармен, қоғамдық қозғалыстармен, саяси партиялармен, қоғамдық бірлестіктермен және т.б.) белсенді түрде жұмыс жасау қажет деп есептейді.

1991 жылдың 8 желтоқсанында Тәуелсіз Мемлекеттер Достастығы (ТМД) құрылды. Посткеңестік кеңістіктегі қатысушы-мемлекеттер компьютерлік ақпарат саласындағы қылмыстармен күрес бойынша өзара байланыстың тиімділігін ұмыт қалдырған жоқ. «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің компьютерлік ақпараттық саласындағы қылмыстармен күрестегі ынтымақтасығы туралы келісімі» (2001 жылдың 1 маусымы, Минск қаласы) қабылданса, кейін 2018 жылғы 28 қыркүйегінде Душанбеде жасалған «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісім» жасалды.

«Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтасығы туралы келісімді ратификациялау туралы» Қазақстан Республикасының 2019 жылғы 9 желтоқсандағы заңына сәйкес, қылмыстық жазаланатын әрекеттерге мыналар жатады:

1. Тараптар ұлттық заңнамаға сәйкес ақпараттық технологиялар саласындағы мынадай әрекеттерді, егер олар қасақана жасалса:

а) заңмен қорғалатын компьютерлік ақпаратқа санкциясыз қол жеткізу арқылы ақпаратты жоюды, бұғаттауды, түрлендіруді не көшіруді, ақпараттық (компьютерлік) жүйенің жұмысын бұзуды;

б) зиянды бағдарламаларды жасауды, пайдалануды немесе таратуды;

в) компьютерлік жүйені пайдалану қағидаларын оған қолжетімділігі бар адамның заңмен қорғалатын компьютерлік ақпаратты жоюға, бұғаттауға

немесе түрлендіруге әкеп соққан бұзуын, егер бұл іс-әрекет айтарлықтай зиян келтірсе немесе ауыр салдарға әкеп соқса;

г) компьютерлік жүйеде өңделетін, машиналық тасымалдағыштарда сақталатын немесе деректерді беру желілері арқылы берілетін ақпаратты өзгерту арқылы не компьютерлік жүйеге жалған ақпаратты енгізу арқылы не заңмен қорғалатын компьютерлік ақпаратқа санкциясыз қол жеткізе отырып, мүлікті жымқыруды;

д) «Интернет» ақпараттық-телекоммуникациялық желісін немесе электр байланысының өзге де арналарын пайдалана отырып, порнографиялық материалдарды немесе кәмелетке толмағанның бейнесі бар порнографиялық сипаттағы заттарды таратуды;

е) қорғалған компьютерлік жүйеге немесе желіге санкциясыз қол жеткізудің арнайы бағдарламалық немесе аппараттық құралдарын өткізу мақсатында дайындауды не өткізуді;

ж) компьютерлік жүйелерге арналған бағдарламаларды және авторлық құқық объектілері болып табылатын деректер қорын заңсыз пайдалануды, сол сияқты авторлықты иемденуі, егер бұл іс-әрекет айтарлықтай залал келтірсе;

з) ақпараттық-телекоммуникациялық «Интернет» желісін немесе электр байланысының өзге де арналарын пайдалана отырып, белгіленген тәртіппен экстремистік деп танылған немесе террористік әрекетті жүзеге асыруға немесе терроризмді ақтауға шақыруды қамтитын материалдарды таратуды қылмыстық жазаланатын әрекеттер ретінде таниды.

2. «Айтарлықтай зиян», «ауыр салдар» және «айтарлықтай залал» деген ұғымдарды анықтау тараптардың құзыретіне жатады [47].

Осы заңға сай, компьютерлік ақпарат - компьютерлік жүйенің жадында, компьютерлік жүйенің қабылдауына қолжетімді нысанда машиналық немесе өзге де тасымалдағыштардағы немесе байланыс арналары арқылы берілетін ақпарат деген талдама беріледі.

Бұл заңнамаға қатысушы мемлекеттердің заңнамасындағы нормаларда өзіндік көрініс тапқан болатын. Мысалы, Ресей Федерациясының Қылмысық кодексінде - 28 тарау (272-274 баптар), IX бөлігінде «Қоғамдық қауіпсіздікке және қоғамдық тәртіпке қарсы қылмыстар»; Арменияда – 24 тарау «Компьютерлік ақпарат қауіпсіздігіне қарсы қылмыстар», 9 бөлік «Қоғамдық қауіпсіздікке, компьютерлік ақпарат қауіпсіздігіне, қоғамдық тәртіпке және халықтың денсаулығына қарсы қылмыстар»; Әжірбайжанда – 30 тарау «Киберқылмыстар», X бөлік «Қоғамдық қауіпсіздік және қоғамдық тәртіпке қарсы қылмыстар»; Украинада – XVI бөлік «Электронды-есептегіш машиналар (компьютерлер), компьютерлік желілер саласындағы қылмыстар»; Молодовада – XI тарау «Электрлік байланыс саласындағы қылмыстар және ақпараттық қылмыстар»; Грузияда – XXXV тарау «Компьютерлік қылмыстар», 9 бөлік «Қоғамдық қауіпсіздік және қоғамдық тәртіпке қарсы қылмыстар»; Түркменстанда – 33 тарау, XIII бөлік «Компьютерлік ақпарат саласындағы қылмыстар».

Ақпаратты алу және тарату туралы адамның құқықтары «Адам құқықтарының жалпыға бірдей декларациясының» [48] 19 бабында және «Мемлекеттік құқықтар туралы халықаралық пакттің» 19 бабында бекітілген. 2011 жылы «Интернет» Біріккен Ұлттар Ұйымының деңгейінде бұл құқықты жүзеге асыратын негізгі құрал ретінде танылды. Сөйтіп ақпараттық-телекоммуникациялық желілерге («Интернет» желісін қоса алғанда) қол жетімділік адам құқығының бір белгісі болып табылады.

БҰҰ-ның құрамында «Интернет» ақпараттық-телекоммуникациялар технологиялар мәселелерімен белсенді түрде айналысатын Халықаралық Электрлібайланыс Бірлестігі (ХЭБ) жұмыс жасайды. ХЭБ-нің мәліметі бойынша «Интернет» ақпараттық-телекоммуникация желісін пайдаланушылар 1985 жылы 20 мың адам болса, 2005 жылы – 1 миллиардтан астам өскен [49]. 2000 жылдан 2015 жыл аралығында «Интернет» ақпараттық-телекоммуникациялық желісін пайдаланушылау 7 есеге өскен. Ал 2020 жылдың басында 4,5 миллиард адам «Интернет» желісін пайдаланған, яғни жер бетіндегі халықтардың 60 % құрайды [50].

Ақпараттық-телекоммуникациялық желілер – трансұлттық институт және оның шекарасы болмайды. Осы фактор халықаралық қауымдастықтың, экономиканың және әлеуметтенудің одан ары дами түсуіне септіген тигізеді. Телекоммуникациядағы желілердің дамуымен қатар жағымсыз жақтары да пайда бола бастады. Қылмыскерлер телекоммуникация желісін пайдалана отырып, басқа мемлекетте бола тұра, өзінің қылмыстарын жасай алатын болды.

Сондықтан да телекоммуникация желісін пайдалана отырып жасалатын құқық бұзушылықтардың алдын алу үшін халықаралық және отындық заңнамаларды жетілдіру қажет болып отыр.

1998 жылы БҰҰ Бас Ассамблеясының 53-ші сессиясында телекоммуникация және ақпараттану саласындағы жетістіктер туралы резолюция қабылданды [51], яғни онда қатысушы-мемлекеттер ақпараттық-телекоммуникациялық желілер құқыққа қайшы мақсаттар пайдалануы мүмкін деген шешімге келді. Ақпараттық-телекоммуникациялық желі саласындағы қауіпсіздікті қамтамасыз ететін халықаралық принциптер дайындау қажеттігі атап өтілді.

2001 жылдың 19 желтоқсанында БҰҰ Бас Ассамблеясының A/RES/56/121 резолюциясында қатысушы-мемлекеттердің ақпарттық-телекоммуникациялық желілерді пайдалана отырып жасалатын құқық бұзушылықтармен күресу үшін қылмыстық саясатты дайындау қажеттігі айтылған болатын [52].

БҰҰ-нан басқа осы мәселе бойынша басқада халықаралық ұйымдар айналаса бастаған болатын. 1989 жылы 13 қыркүйекте Еуропа Кеңесі ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстарға қарсы тұруға бағытталған құжат дайындаған болатын [53]. Бұл құжатқа сәйкес, қылмыстың екі түрі бөліп көрсетіледі:

1) ұлттық қылмыстық заңнамада компьютерлік ақпарат саласындағы алаяқтық, компьютерлік мәліметтерді заңсыз алу, өзгерту және т.б. міндетті түрде көрсету;

2) ақпараттық-телекоммуникациялық желілерді пайдалану арқылы түрлі қылмыстарды жасаудың құрамын көрсету.

Конвенция «ақпараттық-телекоммуникация желісіне» «екі немесе одан да көп компьютерлер арасындағы байланыс» деген түсінік береді. Қарастырылып отырған құжат киберқылмыстылықты екі санатқа бөліп қарастырады. Бірінші топқа, компьютерлік ақпарат, компьютерлік құрылғы және желімен байланысты:

1) компьютерлік ақпаратты алу мақсатында қасақана заңсыз алып қою;

2) компьютерлік ақпараттарды заңсыз алу.

Конвенция екінші топқа ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалану жасалған қылмыстың құралы ретінде қарастырылады.

Тәуелсіз Мемлекеттер Достастығы ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстармен күресуде үлкен жұмыстар атқаруда. Бұрындары тек компьютерлік ақпарат саласындағы құқық бұзушылықтарға ғана көңіл бөлініп келсе, 2013 жылдан бастап ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстармен күресуге халықаралық деңгейде көңіл бөлініп отыр.

2013 жылдың 20 қарашасында Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастығы туралы келісім [54] қабылданып, біз зеттеп отырған құқық бұзушылыққа қарсы әдістемелік негіз бола білді. Біздің еліміз бұл келісімді 2018 жылдың 3 мамырында ратификациялады [55]. Осы заңда «ақпараттық қылмыстылық» түсінігі беріледі, яғни ақпараттық қауіпсіздік - жеке адамның, қоғам мен мемлекеттің және олардың мүдделерінің ақпараттық кеңістікте қауіп-қатерлерден, бұзушы және өзге де теріс ықпал етуден қорғалуының жай-күйі болып табылады.

Бұл келісімге сай, қатысушы мемлекеттер мынадай негізгі бағыттар бойынша жұмыс атқарады:

- мемлекеттердің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы қатынастарды регламенттейтін нормативтік құқықтық актілерін және нормативтік-әдістемелік құжаттарын жақындастыру;

- мемлекеттерде ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған, ақпараттық кеңістікте бірлескен үйлестірілген іс-шаралар жүргізу үшін нормативтік құқықтық актілерді әзірлеу;

- ақпараттық қауіпсіздікті қамтамасыз ету мәселелерін реттейтін нормативтік құжаттарды әзірлеу және пайдаланушыларға жеткізу;

- бағдарламалық-техникалық құралдар мен ақпаратты қорғау құралдарының жасап шығарылуын дамытуды нормативтік құқықтық қамтамасыз ету;

- ақпараттық қауіпсіздік саласында халықаралық стандарттарға үйлесімді мемлекетаралық стандарттарды әзірлеу;

- әртүрлі қолданбалы мақсаттағы қорғалған ақпараттық жүйелерді құру; ақпаратты трансшекаралық беруді ұйымдастыру;

- ақпараттық жүйелер мен ресурстарды ықтимал және нақты қатерлерден қорғау технологиясын жетілдіру;

- ақпараттық жүйелердің ақпараттық қауіпсіздігіне қатерлерді талдау және бағалау;

- ақпараттық жүйелердің жұмыс істеуіне қауіп төндіретін құрылғылар мен бағдарламаларды анықтау және бейтараптандыру саласындағы қызметті жетілдіру;

- ақпараттық жүйелерде орналасқан ақпаратқа санкцияланбаған қол жеткізуді және техникалық арналар бойынша оның жария болуын жол болғызбауға бағытталған келісілген іс-шараларды іске асыру;

- қорғалу сыныптары әртүрлі ақпараттық жүйелердің өзара іс-қимылы кезінде қолжетімділігі шектеулі ақпарат пен ақпараттық технологияларды қорғауды қамтамасыз ету;

- мемлекеттерге тиесілі мемлекетаралық ақпараттық жүйелер сегменттерін және оларды бағдарламалық қамтамасыз етуді жаңғырту;

- ақпаратты қорғау құралдарын сертификаттаудың және сертификаттау нәтижелерін өзара танудың келісілген тәртібін белгілеу;

- ақпараттық қауіпсіздік саласындағы перспективалы ақпараттық технологияларды әзірлеу;

- ақпараттық қауіпсіздік саласындағы ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарға, ғылыми-техникалық өнімге сараптама жүргізу;

- ақпараттық қауіпсіздікті қамтамасыз ету саласындағы кадрларды кәсіптік қайта даярлау және олардың біліктілігін арттыру;

- озық тәжірибелерді қорыту, тарату және енгізуді ұйымдастырады [55].

Сөйтіп халықаралық-құқықтық салада ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстың жеке тобын бөліп көрсету қажет. Біз осы топқа жататын қылмыстық құқық бұзушылықты бөліп алып, жеке классификатор беруді ұсынамыз. Бірақта халықаралық құқықта ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстың ортақ түсінігінің және оның белгілерін болмауы жүйелеуге кедергі келтіріп отыр.

Қазақстандық қылмыстық заңнама жалпы халықаралық заңнамаға сәйкес келеді. Бірақта ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстың құрамы жүйеленбеген. Сонымен қатар, ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстардың көп бөлігі заңнама назарынан тыс қалуда.

Франция мемлекетінің ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылыққа қарсы қылмыстық саясаты бізді қызықтырады. Франция Қылмыстық кодексінің

222-24 бабындағы біз зерттеп отырған белгісі аса қауіпті қоғамдық әрекетке жатқызылады. Ақпараттық-телекоммуникациялық желілерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар нормасы қылмысқа дайындалу кезеңінде пайдалануы мүмкін. Ол әсіресе Франция ҚК-де төмендегідей баптарда көрініс береді:

1) зорлау болып табылмайтын сексуалды агрессия (222-27 бап Франция ҚК);

2) жеңгетайлық (222-25 бап Франция ҚК);

3) кәмелетке толмаған тұлғаны азғындық жасауға тарту (227-22 бап Франция ҚК);

4) кәмелетке толмаған тұлғаның порнографиялық сипаттағы бейнелерін немесе суреттерін тарату (227-23 бап Франция ҚК)

Зерттеуден байқағанымыздай ақпараттық-телекоммуникациялық желілерді пайдалану Франция Қылмыстық кодексі бойынша кінәні ауырлататын жағдайларға жатады [56].

Македония және Исландия қылмыстық кодекстерінде телекоммуникациялық желілерді тұлғаның жыныстық қылмыстық жауаптылық қарастырылған.

Македония ҚК-нің 193 бабында «Он төрт жасқа толмаған тұғаға қарсы компьютерлік құрылғыны пайдалану арқылы сексуалдық әрекет жасау» белгісі қарастырылған.

Телекоммуникация желілерін пайдалана отырып балалар порнографиясын тарату бабы екі бөліктен тұрады:

- балалар порнографиясын дайындау (Македония ҚК 193 бабының 1 бөлігі) – бес жылға бас бостандығынан айырумен жазаланады;

- кәмелетке толмағандармен байланысты порнографиялық материалдарды сақтау - (Македония ҚК 193 бабының 2 бөлігі) – бес жылдан сегіз жылға дейін бас бостандығынан айырумен жазаланады.

Исландияның қылмыстық-құқықтық заңнамасында ақпараттық-телекоммуникациялық желілер жасалған қылмыстық құқық бұзушылықтың құралы ретінде қарастырылады. «Сексуалдық сипаттағы қылмыстар» заңының 22 тарауында бұл норма көрініс береді.

Мысалы, Исландия ҚК-нің 202 бабында он бес жасқа толмаған тұлғамен «Интернет» желісін және басқада телекоммуникациялық технологияларды пайдалана отырып, жыныстық қатынасқа түсу мақсатында кездесуді ұйымдастыру үшін жауаптылық қарастырылған.

Эстонияның қылмыстық заңнамасында («Компьютерлік мәліметтерге араласу» ЭР ҚК 206 бабы; «Компьютерлік алаяқтық» 213 бабы) қылмыстың заты ретінде ақпараттық-телекоммуникациялық желілер жатады. Бұл қылмыстық-құқықтық нормалар негізінен меншік саласындағы қоғамдық қатнастарға бағытталған.

2 Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың детерминанттары

2.1 Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың себептері мен жағдайлары

Криминологияда қылмыстық мінез-құлықтың детерминанттары әр түрлі критерийлер бойынша жіктеледі: объективті және субъективті себептер [57], толық және нақты себептер [58], қоғамдық өмірдің әр түрлі деңгейлерінің себептері. Осы саралаудың әрқайсысы қылмыстардың жасалуының белгілі бір жақтарын бөліп көрсетуге мүмкіндік береді. Криминогендік факторлардың деңгейлік жіктелуіне жатады:

- бірінші деңгей - бұл әлеуметтік орта (макроорта);
- екінші деңгей - тұлғаны қалыптастырудың тікелей факторлары (микроорта);
- үшінші деңгей - нақты өмірлік жағдаймен өзара әрекеттесетін тұлғаның өзі [59, 95 б.].

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар - бұл жалпы қылмыстың құрамдас бөлігі, ол оның басқа себептермен, жалпы себептермен жасалатынын білдіреді. Компьютерлердің заңмен қорғалатын ақпараттарына нұқсан келтіретін заңсыз қылықтар әлеуметтік қайшылықтардың ғана емес, ұлттық қайшылықтар аясында ақпараттық ортадағы қайшылықтардың нақты нәтижесі болып табылады.

Ақпараттық орта дегеніміз - қоғамның барлық өмір салаларына енетін, ақпаратты құрумен, түрлендірумен және тұтынумен байланысты субъектілердің қызмет саласы. Сондықтан, ғалымдар қоршаған ортаның заңға қарсы мінез-құлыққа әсері жеке тұлғаның әлеуметтік ортасының кеңеюін анықтайтын ғылыми-техникалық прогресс жағдайында ерекше өзектілікке ие болатынын дұрыс атап өтті [60, 187 б.].

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың себептерін, оның өмір сүру салаларында болуы мен өсуін бөліп көрсетейік.

1. Экономикалық себептер. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың жалпы себептерін экономикалық саясат пен экономикалық қатынастардың кемшіліктерінен іздеу керек. Қатаң бәсекелестік пен жұмыссыздық жағдайында экономика адамдардың бойында қаржылық байлыққа деген құштарлықты оятады.

Қоғам өміріндегі экономикалық және саяси жағдайлардың тұрақсыздығы біздің елде маңызды рөл атқарады. Осындай экономикалық жағдайда билікке деген жаппай наразылық пен ашуды туғызатын жағдай пайда болады және соның салдарынан қоғамда қылмыстық құрылымдардың белсенділігінің артуына себеп болды. Сондықтан нақты табыс деңгейі мен

нақты өмір деңгейі арасындағы сәйкессіздіктің пайда болуы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың негізгі себептерінің бірі болып табылады.

Сарапшылар бай азаматтардың әлеуметтік табының тұрақты қалыптастырумен қатар, кедейлердің де тұрақты табы қалыптасып келе жатқанын атап өтеді. Мұндай экономикалық жағдайы азаматтардың көпшілігінде бірінші кезекте өзімшілдік ниетпен ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасауға ықпал етеді. Қылмыскерлерге компьютерлерді, компьютерлік жүйелерді немесе олардың желісін пайдаланатына отырып, өздерінің заңсыз әрекеттері үшін елеулі экономикалық пайда алуға нақты мүмкіндік беріледі. Зерттеушілердің көпшілігі ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардағы жеке қызығушылық пен басқа мотивтердің арақатынасының 60-66% құрайды деп атап өтеді.

Бұл мотивацияның үстемдігіне жұмыссыздардың көп болуы да ықпал етеді. Сұраныс ұсынысты тудырады, сондықтан мемлекеттегі қалыптасқан экономикалық жағдай екі жақты жағдай туғызады. Бір жағынан, ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасау қылмыскерлерге айтарлықтай пайда әкеледі. Екінші жағынан, ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскерлерге өздерінің интеллектуалды заңсыз еңбегінің өнімін басқа да артықшылықтар үшін жүзеге асыруға мүмкіндік бар.

Экономикалық жағдай келесі проблеманың туындауына себеп болды, яғни құқық қорғау органдарының кәсіби деңгейінің компьютерлендірудің жалпы деңгейінен артта қалуы. Құқық қорғау органдарының жеткіліксіз қаржыландырылуы және оларды соңғы ақпараттық жүйелер мен технологиялармен қамтамасыз етілмеуі негізгі экономикалық себептердің бірі болып табылады. Қаржының жеткіліксіздігі органдардың материалдық-техникалық жабдықталуына әсер етеді, оны заманауи компьютерлік технологиялардың қол жетімділігінсіз іске асыру мүмкін емес. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды тергеу компьютердің қыр-сырын түсіну дағдыларын және жедел-іздестіру қызметінің ақпараттық қауіпсіздігін талап етеді.

2. Жалпы әлеуметтік себептер. Экономикалық қатынастарға ұқсас әлеуметтік қатынастар әр түрлі болып келеді және олар микро және макродеңгейлерге бөлінеді. Макродеңгей адамның қоғам мен мемлекеттің қарым-қатынасын (мысалы, өндірістік қатынастар, білім беру, әлеуметтік қызмет және т.б.) және оның тұлға ретіндегі жағдайы (адам құқықтарын білдіреді) сипаттайды. Әлеуметтік себептер әлеуметтік-экономикалық қатынастардың жетілмегендігімен байланысты және олар қоғамдағы мақсаттарға әсер ететін (қаржылық жетістікке жету) мен оларды жүзеге асырудың қол жетімді заңды құралдары арасындағы қарама-қайшылықтарда көрініс табады.

Әлеуметтік себептер кешені ақпараттандыру және компьютерлендіру процестерінің ерекшеліктерімен байланысты. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар саласындағы қылмыстардың жасырын сипаты болады, моральдық нормаларды ұмытуға тез және эгоцентрлік түрде беруге мүмкіндік беретін қатаң регламенттің болмауынан тұрады.

Ақпараттық саладағы қатынастардың криминалдануына ықпал ететін әлеуметтік факторлардың жиынтығының қалыптасқан өзара байланысы мен шарттылығы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың әлеуметтік себептерінің бірі ретінде танылады қоғамдағы әлеуметтік теңдіктің жоқтығы және тәрбиелік жүйенің бұзылуы да әсер етеді. Қазіргі кезде елде әлеуметтік тұрақталықтың болмауының салдарынан қоғамда шиеленіс жағдай туындайды, екінші жағынан, заңсыз өмір салтына бағытталған әлеуметтік топтардың болуымен сипатталады.

Әлеуметтік әділеттілік қағидасының толық сақталмауы және адамдардың қалыпты заңға бағынушылығының қамтамасыз етілмеуі адамдардың арасындағы тұрақсыздыққа, жанжалды жағдайға әкеліп соқтырады және сөзсіз қылмысқа итермелейді. Сарапшылардың пікірінше, халықтың 98% -ы заңсыз өмір салтын қолайлы деп санайды, ал 85% -ы қандай да бір заңсыз әрекеттерді жасайды. Халықтың құндылықтар жүйесінде вулгарлық нарықтық қатынастар қалыптастырады, сонымен қатар оларда әлеуметтік және құқықтық компонентті елеу байқалмайды. Әлеуметтік-құқықтық қорғаудың кепілдіктерінің болмауы мемлекеттің заңды қорғау бойынша дәрменсіздігін тудырады.

Қазіргі таңда «саяси мотивация» терроризмді, соның ішінде халықаралық терроризмді тудырады. Мұндай терроризм бүкіл дүниежүзілік қауымдастықтың немесе дамыған елдердің ақпарат алмасу инфрақұрылымының дағдарысын тудыруы мүмкін. Оның орындалу мүмкіндігі арта түседі, өйткені заманауи өркениет ақпарат алмасудың жоғары технологиялары негізінде құрылады. Олар ақпаратты өңдеу және сақтау арқылы жүзеге асырылады: компьютерлер және олардың негізінде құрылған жүйелер; банктік, биржалық, ғылыми-зерттеу, басқарушылық, сонымен қатар спутниктік теледидардан бастап ұялы байланыс құралдарына дейін.

3. Құқықтық сипаттағы себептер. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың негізгі себептерінің бірі – барлық деңгейдегі ақпараттық саладағы қоғамдық қатынастарды құқықтық реттеудің жеткіліксіздігі. Заңнамаға талдаулар көрсеткендей, бірқатар мәселелер құқықтық реттеу саласынан тыс қалап жатса, кейбір заң жобалары тек әзірлену сатысында қалып қойып жатыр. Бұрын қабылданған нормативтік актілерге қазіргі қоғам мен мемлекеттің даму жағдайын, сондай-ақ ғылым мен техниканың жетістіктерін ескере отырып өзгертулер мен толықтырулар енгізу қажет.

Ақпарат саласындағы құқық бұзушылықтарға қатысты құқық қолдану тәжірибесін дұрыс қолданбау компьютерлік қылмыстың себептерінің бірі болып табылады. Әлемдегі экономикалық қатынастардың дамуына компьютерлік технологияны енгізу процестері әсер етуде. Бүгінгі күні біздің елде Интернетте өздерінің өнімдерін және қызметтерін жарнамалауға және электронды құжат айналымын пайдалануда көптеген тұтынушыларды тартуға мүдделі болып отыр. Сонымен қатар, еліміздегі қолданыстағы қылмыстық заңнамасы электронды сауда саласында жасалған қылмыстарды басқа экономикалық қылмыстардан және меншікке қарсы қылмыстардан бөлмейді, бұл құқық қорғау органдары қызметкерлерінің іс-әрекеттерде қылмыс құрамының болуын нақты анықтау мүмкіндігін әлсіретеді.

Нәтижесінде мемлекетімізде осы саладағы қылмыстық құқық бұзушылықтар үшін қылмыстық қудалау фактілері іс жүзінде жоқ. Бұл дегеніміз ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың одан әрі кең қанат жаюына, оның одан әрі өсуіне себеп болады және қоғамда үйреншікті дағдыға айналады айналады.

Жоғарыда айтылғандарды қорытындылай келе, кейбір нәтижелерді қорытындылайық:

1. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың себептері қазіргі уақытта анықталуда. Бұл көбіне ақпараттық қатынастардың қалыптасуының бастапқы кезеңімен және қоғамды әлі де болса компьютерлендірумен байланысты және осыған байланысты отандық криминология қылмыстың осы түріне жеткіліксіз назар аударуда.

2. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жалпы қылмыстың ажырамас бөлігі болып табылады, сондықтан ол ақпараттық саладағы жалпы әлеуметтік және нақты қайшылықтардан туындайды. Ақпараттық сала өз кезегінде қоғамның барлық өмір салаларына еніп, адамның әлеуметтік ортасының шеңберін кеңейтіп, жалпы әлеуметтік себеп-салдарлық қарама-қайшылықтардан бас тартып өмір сүреді. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың жасалуына тікелей әсер ететін құқықтық, экономикалық, әлеуметтік себептердің топтары ажыратылады.

Қазіргі заманғы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың әлеуметтік себептеріне мыналарды жатқызу керек:

1. Қоғамын жалпы компьютерлендіру (компьютерлік технологиялардың тез қарқынмен дамуы, ақпараттық және телекоммуникацияны желілер, ақпараттық қызметтер, электрондық құжат айналымы және т.б.) киберқылмыскерлердің қызметі үшін қажетті жағдай жасайды.

Біз профессор Т.М. Лопатинаның компьютерлендіру жалпы жағымды құбылыс, бірақ жоғары технологиялардың мүмкіндіктерін қолдану арқылы

жасалатын қылмыс құбылысымен тығыз байланысты болады деген пікірімен келісеміз.

Ақпарат алмасудың дамуы және компьютерлік технологиялардың дамуы қылмыскерлердің жаңа «тапқырлығын» ойлап табуда. Жаңа техникалық құралдарға қол жеткізу арқылы заңсыз түрде ірі мөлшерде ақша жымқыру, салық төлеуден жалтару, қылмыстық жолмен алынған кірістерді жылыстатуды жүзеге асырады. Ақпаратты сақтау және беру саласындағы техникалық жетістіктердің қарқынды өсуі, компьютерлік желінің бөлшектенуі (орталықтан файлдық процессорларға өтуіне байланысты), компьютерлік қылмыстардың пайда болуы мен өсуіне негіз болатын қауіпсіздік шараларының компьютерлік технологияның даму деңгейінен артта қалуы криминогендік факторлар болып табылады.

2. Халықтың ақпараттық қызметтерге, бағдарламалық өнімдерге деген нақты қажеттіліктері мен оларды өмір сүру деңгейінің төмен болуына байланысты заңды жолдармен қанағаттандыру мүмкіндігі арасындағы қайшылықтар.

2020 жылы ең төменгі жалақы 42 500 теңге болды, яғни бұл шамамен 98 долларды құрайды. Ең төменгі жалақының ең үлкен мөлшері келесі елдерде байқалады: Люксембург (1989 АҚШ доллары), Австралия (1923 доллар), Ирландия (1743 доллар). Үздік ондыққа Нидерланды, Ұлыбритания, Оңтүстік Корея, Канада, Бельгия, Германия және Франция кіреді. Салыстырып қарайтын болсақ, еі төменгі жалақы мөлшері бірнеше есе төмен.

Сондықтанда біздің елдің азаматтарының өмір сапасы Солтүстік Америка, Еуропа, кейбір Азия елдері (Жапония, Оңтүстік Корея, Тайвань), Таяу Шығыс (Біріккен Араб Әмірліктері, Сауд Арабиясы, Катар, Кувейт) елдерінен әлі де төмен болып отыр. Алайда, әділеттілік үшін айта кету керек, соңғы жылдары мемлекеттік секторда жалақының өсуі және жалпы алғанда, халықтың өмір сүру деңгейінің жақсаруы байқалады. Бірақ ол баяу қарқынмен жүзеге асуда. Үкімет жүргізетін әлеуметтік реформаларға аймақтық және облыстық деңгейлердегі тиімсіз менеджмент (бюрократия мен сыбайлас жемқорлықтың салдарынан), жоғары инфляция және энергетика мен шикізатқа бағытталған орта кедергі келтіреді. Сарапшылардың пікірінше, кедейлік барлық пайдакүнемдік қылмыстардың 20-30%-ын құрайды, яғни, табысы төмен халықтың санаты ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасайды.

Жоғарыда айтыған тезисті дәлелдеу үшін Түркістан облысының Жетысай аудандық сотының үкімінен үзінді келтіре кетейік. Сотталушы Д.Н.Серикбеков 2017 жылдың маусым айының 06-шы жұлдызында, сағат 13:00-дер шамасында, алаяқтық, яғни бөтеннің мүлкін, ақпараттық жүйені пайдаланушының сеніміне кіріп, алдап, теріс пайдалану жолымен бөтен мүлікке құқықты бірнеше рет иемдену мақсатында, өзінің танысы Т.Төремұратовқа жолығып оған «банкомат карточкаңды бере тұршы, бір кісілер қаражат аударатын еді, саған қазір керек емес қой, кейін өзіңе карточкаңды қайтарып беремін» - деп оны алдап, Т.Төремұратовтың атына

«Halyk Bank» акционерлік қоғамынан (бұдан әрі – «Halyk Bank» АҚ) берілген карточкасын құпия сөзін біліп, маусым айының 07-ші жұлдызында, сағат 10:00-дер шамасында, өзінің ұялы телефоны арқылы «Google Chrome» программасына заңсыз еніп, Т.Төремұратовтың атынан шағын несие беретін бірнеше жауапкершілігі шектелген серіктестіктеріне (бұдан әрі - серіктестік) жәбірленушінің жеке бас деректерін толтырып, несие алуға тапсырыстар беріп, «ALTENGE» серіктестігімен №201706070104 санды қарыз беру шартын түзіп, 20 000 теңгені Т.Төремұратовтың шотына аударып, Т.Төремұратовқа «менің танысым сенің шотыңа ақша салып жіберген еді, соны алып берші» - деп алдап, Т.Төремұратов өзінің шотына түскен 20 000 теңгені алып, Д.Серикбековке берген, ал Д.Серикбеков ол ақшаны өзінің жеке бас пайдасына жаратып жіберген.

3. Біздің қоғамымыз компьютерлік қылмысқа жеңіл-желпі көзқараспен қарауда. Біздің елімізде соңғы 30 жылда болған оқиғалар (КСРО-ның ыдырауы, көппартиялы саяси жүйеге көшу және нарықтық экономика, саяси режимнің өзгеруі, өнеркәсіп өндірісі мен ауыл шаруашылығының құлдырауы, қаржылық дефолт) әлеуметтік дағдарысқа және азаматтарымыздың өмір деңгейінің күрт төмендеуіне әкелді.

Еліміздегі компьютерлік қылмыстың экономикалық себептері:

4. Қылмыскерлерді жылдам және салыстырмалы түрде қауіпсіз байыту. Компьютерлік қылмыстар қылмыскерлердің заңсыз баюдың тәсіліне айналды.

Сотталушы Аукалиев Д.Т., 02.01.2019 жылы еш жерде жұмыс істемей, қаражатқа мұқтаж болғандықтан алаяқтық, яғни адамдарды алдау және сенімді теріс пайдалану арқылы бөтеннің мүлкін жымқыру қылмыстық құқық бұзушылық пиғылымен алдын ала жоспар құрып, құрған жоспары бойынша «Крыша» ғаламтор парақшасы арқылы Алматы қаласында тәулікке жалға берілетін пәтерлерді тауып алып, сол пәтерді тәулікке жалға алғаннан кейін, қайтадан «Крыша» ғаламтор парақшасы арқылы тәуліктік жалға алған пәтерді ұзақ мерзімге жалға беремін деп адамдарды алдап, ақшаларын заңсыз иемденіп, оқиға болған жерден бой тасалап қашып кету болған. Сол күні, ол қылмыстық пиғылын жүзеге асыру мақсатында Алматы қаласы, Тимирязев көшесінің бойында орналасқан компьтерлік клубқа келіп, сол жерде «Крыша» ғаламтор желісі арқылы Алматы қаласында тәуліктік жалға беретін пәтерлерді қарап отырып, Алматы қаласы, Ғабдуллин көшесі № 175 «А» үй, 26-пәтердің жалға берілетінін көріп, пәтер иесі Н.И.Лоншаковпен ұялы телефон арқылы хабарласып, көрсетілген пәтерді жалға алатын болып келісіп, сағат 20-00 шамасында аталған пәтердің иесі Н.И.Лоншаковпен кездесіп, көрсетілген пәтерді бір тәулікке жалға аламын алдап, соңғының қолына 5000 тенге беріп, одан пәтердің кілтін алып қалған. Сосын, Д.Т.Аукалиев өзінің алаяқтық жоспарын аяғына дейін жеткізу мақсатында, қайтадан Алматы қаласы, Тимирязев көшесінің бойында орналасқан компьтерлік клубқа келіп, сол жерде «Крыша» ғаламтор желісі арқылы Алматы қаласы, Ғабдуллин көшесі № 175 «А» үй, 26 пәтердің ұзақ мерзімге жалға берілетінін туралы жарнамалаған. Сол күні, сағат 21-20 шамасында

Д.Т.Аукалиевтің алдын ала қылмыстық ісін жасыруға арнап сатып алған ұялы телефонына Скатова Надежда Александровна телефон шалып, «Крыша» ғаламтор желісіндегі жарнама арқылы хабарласып тұрғанын айтып, екеуі Алматы қаласы, Ғабдуллин көшесі № 175 «А» үй, 26 пәтерде кездесетін болып келісіп, Н.А.Скатова келісім бойынша жоғарыда көрсетілген пәтерге келіп, сол жерде Д.Т.Аукалиевпен кездескен. Кездесу барысында Д.Т.Аукалиев алаяқтық, яғни адамдарды алдау және сенімді теріс пайдалану арқылы бөтеннің мүлкін жымқыру қылмыстық құқық бұзушылық пиғылын жалғастыра отырып, пәтерді өзінікі және бір айға жалға беретінін айтып, айлық жалға беру 75 000 тенге екенін айтып Н.А.Скатованы сеніміне қиянат жасап оның 75 000 тенгесін алдап алып қылмыстық құқық бұзушылығын аяғына дейін жеткізіп, оқиға болған жерден бой тасалап кетіп, өзінің қылмыстық құқық бұзушылық әрекетімен жәбірленуші Н.А.Скатоваға 75 000 тенгеде материалдық залал келтірген. Сөйтіп, Аукалиев Д.Т. алаяқтық, яғни алдау және сенімді теріс пайдалану арқылы бөтеннің мүлкін жымқыру қылмыстық құқық бұзушылық әрекетін жасаған.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың барлық факторларын үш санатқа бөлуге болады:

- ақпаратқа, ақпараттық ортаға және оның инфрақұрылымына байланысты;

- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың өзіндік ерекшеліктеріне байланысты;

- ақпараттық қауіпсіздікті қамтамасыз ету кезінде туындайтын қоғамдық қатынастардың қатысушылары ретінде адамдарға, қоғамға және мемлекетке қатысты.

1. Ақпаратқа, ақпараттық ортаға және оның инфрақұрылымына байланысты қылмыстың факторлары.

Әлемде және елде ақпарат алмасудың ұлғаюы байқалады, бірақ бұл өсу ақпараттық қорғаудың тиісті деңгейін қамтамасыз етпейді және бұл қылмыстарға «сыртқы» және «ішкі» ықпал ету арқылы жасауға қолайлы мүмкіндіктер жасайды. Әлеуметтік маңыздылығына байланысты ақпаратты қорғау жүзеге асырылмайды. Компьютерлік ақпаратты өңдеу кезінде ақпаратты өңдеудің технологиялық режимдерінен ауытқу жиі кездеседі. Заңмен қорғалатын ақпаратпен жұмыс істеу ережелері бұзылған.

Ақпараттық ортаға байланысты компьютерлік қылмыстың факторларына мыналар жатады:

- бүкіл әлемде және мемлекетімізде бағдарламалық және ақпараттық құралдарды пайдаланушылар санының өсуі; инфрақұрылымды, желілерді, бағдарламаларды, жабдықтарды жаппай пайдалану;

- компьютерлік технологияның қол жетімділігі;

- заманауи технологиялардың компьютерлік жүйелер мен телекоммуникация құралдарына тәуелділігінің артуы;

- шетелдік бағдарламалық қамтамасыздандыруды, операциялық жүйелерді, сондай-ақ техникалық компоненттерді кеңінен қолдану.

Ақпараттық инфрақұрылым - бұл мемлекеттің аумағында орналасқан ақпараттандыру объектілерінің, Интернеттегі және байланыс желілеріндегі сайттардың, ақпараттық жүйелердің жиынтығы.

Ақпараттық инфрақұрылымға байланысты компьютерлік қылмыстың факторларына мыналар жатады:

- компьютерлік ақпаратты өңдеумен айналысатын қызметкерлердің қызметіне әкімшілік тарапынан тиісті бақылаудың болмауы;

- бұқаралық ақпарат құралдары мен Интернеттің қазақстандық сегментіне мемлекет тарапынан тиісті бақылаудың болмауы;

- жабық анонимді ақпараттық және телекоммуникациялық желілердің болуы және олар арқылы әртүрлі қылмыстардың жасалуы.

2. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың белгілеріне қатысты факторлар:

- жасырын болу, инфрақұрылымның шалғайлығына және күрделілігіне, жәбірленушілерді білмеуіне байланысты қылмыстардың құпиялылық сипаты;

- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың жаһандық және трансшекаралық сипаты. Қылмыскер осы мемлекетте болып, басқа мемлекетте қылмыс жасауы мүмкін, ал қылмыстың салдарын үшінші бір тұлға тартуы мүмкін, бұл бір мемлекеттің қылмысқа қарсы тұруын қиындатады;

- бұл қылмыстардың бір уақытта және әр түрлі елдерде орналасқан жүздеген және мыңдаған компьютерлерге бір уақытта шабуыл жасау мүмкіндігі;

- осындай қылмыстар жасаудың әр түрлі тәсілдері;

- қарапайым дәстүрлі әдістермен ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың алдын алу мен жолын кесудің мүмкін еместігі;

- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар, оның жағдайы, құрылымы мен динамикасы туралы сенімді статистиканың болмауы;

- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың өте кең таралуы және әр түрлі себептерге байланысты бұл қылмыстардың өте жоғары латенттік сипаты;

- осындай қылмыстарды ашу, тергеу және саралау бойынша ғылыми негізделген әдістемелік ұсыныстардың болмауы.

3. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың адамдарға, қоғамға және мемлекетке қатысты факторлары.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың мемлекет қызметіне және қоғамның қызмет етуіне байланысты факторлары:

- компьютерлік технологиялар, телекоммуникация және ақпараттық қауіпсіздік саласындағы халықаралық стандарттар жүйесінің уақыт талабына сәйкес келмеуі;
- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарға қарсы іс-қимыл саласындағы тиісті халықаралық-құқықтық ынтымақтастықтың болмауы;
- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарға қарсы бағытталған мемлекеттік кешенді шаралардың болмауы;
- қолданыстағы ақпараттық заңнаманың жүйелі және жоспарлы даму мен заңнамалық реттеудің болмауынан зардап шегетін кемшіліктері;
- ақпарат саласындағы қалыптасқан қоғамдық қауіпті құбылыстарға сәйкес келмейтін қылмыстық заңнаманың кемшіліктері;
- қолданыстағы қылмыстық заңнаманың жетілмегендігі;
- телекоммуникациялық технологиялардың даму деңгейінен едәуір артта қалған әлеуметтік, құқықтық және саяси құрылымдардың жетілмегендігі;
- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарға құқықтық, ғылыми, ұйымдастырушылық-техникалық құқық қолданудың жеткіліксіздігі;
- компьютерлік жүйелердің осалдығы және қауіпсіздіктің тиімді шараларын пайдалану бойынша қарапайым халықтың хабардар болмауы;
- ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарға және компьютерлік қылмыскерлерге қоғамның адекватты емес қатынасы;
- халықтың, әсіресе жас ұрпақтың құқықтық білімінің жеткіліксіздігі.

Қылмыскерлер аз уақыттың ішінде үлкен пайда табуға ұмтылады. Мысалы, АҚШ-та бір топ қылмыскерлер Интернет арқылы миллионнан астам банктік карточкалардың нөмірлеріне иелік етіп, 30 минут ішінде 9 миллион долларға жуық «пайда» тапқан.

Интернет-алаяқтық - бұл нақты әлемнен виртуалды әлемге енген құбылыс. Интернет-алаяқтық анықтамасы бойынша шынайы әлемдегі алаяқтыққа ұқсас: бұл бөтеннің мүлкін ұрлау немесе алдау арқылы біреудің мүлкін иемдену немесе сенімге қиянат жасау арқылы алу. Алайда, Интернеттегі алаяқтық виртуалды кеңістіктің заңдарына, «Интернет-уақыт» режиміне, пайдаланушылардың бір-бірінен физикалық арақашықтығына және Интернеттегі қолданушылардың жасырын болуына бағынады. Осы себептерге байланысты алаяқтарды жауапкершілікке тарту өте қиын.

Интернет-алаяқтар өздерінің құрбандарын табу үшін Интернеттегі барлық мүмкін байланыс арналарын пайдаланады. Алаяқтардың

хабарламаларының өзі олар мен Интернет қолданушылары арасындағы байланыс нысандары болып табылады.

Зерттелген құбылыс - алаяқтық, экономикалық пайданы заңсыз алу мақсатында Интернетті қолданумен байланысты шындықты көрсетеді. Құқық бұзушы өздігінен немесе үшінші тұлғалар үшін пайда табатындай етіп компьютердің мәліметтерді өңдеуінің дұрыс жұмысына кедергі келтіреді.

Интернет - өзін-өзі реттеу, дербестік және өзін-өзі қамтамасыз ету қағидатына негізделген ғаламдық компьютерлік желі. Егер ғаламдық ақпараттық технологиялар алаяққа өзінің қылмыстық жоспарларын жүзеге асыру үшін беретін мүмкіндіктерді бағалайтын болсақ, онда келесі жағдайларды ажыратуға болады:

Анонимдік - негізінен ғаламдық желідегі қолданушы байланысының ерекшеліктерін анықтайды. Адамдардың бір-бірімен бетпе-бет кездеспеуі психологиялық кедергілерді жояды және олардың ашыла түсуіне көмектеседі.

Виртуалды кеңістікте елеусіз қалғысы келетін адамның жеке басын анықтау мүмкін емес, өйткені нақты IP - жеке компьютердің орналасқан жерін анықтауға болатын адресті жасыратын бағдарламалар бар.Мобильді Интернет технологиялары жағдайды ушықтырып отыр, өйткені қылмыскер әр түрлі қол жеткізу нүктелерін пайдаланып кеңістікте еркін қозғалады. Барлығы дерлік Интернетке қол жетімділікті салыстырмалы түрде аз ақшаға пайдалануға мүмкіндігі бар.

Тағы бір ерекшелігі - Интернетте «нақты уақыт режимінде» орындалатын іс-әрекеттердің тиімділігі. Кез-келген операцияның тиімділігі елдер мен континенттерді қамтитын бүкіл Интернет кеңістігіне тарайды. Интернет әлемнің әр түкпіріндегі адамдармен байланыс орнатуға мүмкіндік берді.

Жаңа технологияларды қолдану тапсырманы едәуір жеңілдетті. Кәдімгі поштаны пайдаланып хаттарды көбейту және жіберу кезінде олар почта төлемдеріне көп ақша жұмсауы керек. Заманауи желілік технологиялар алаяқтық жасауды жеңілдетіп қана қоймай, оның құнын төмендетеді.

Фишинг (парольдерді аулау) - Интернеттегі алаяқтықтың ең көп таралған түрі. Пайдаланушының сәйкестендірілуін болжап, банктің сайтына визуалды түрде имитация жасайтын жалған сайт. Олар келесі тәсілдерді қолданады:

- спам - қолданушыдан белгілі бір әрекеттерді орындауға рұқсат беруді талап ететін кейбір проблемалармен қорқыту үшін (есептік жазбаны бұғаттан шығару және т.б.). Хатта жалған сайтқа сілтеме бар, және визуалды түрде оны шынымен ажырату мүмкін емес. Қарапайым нысаны - бұл банктің немесе белгілі бір қызмет көрсетушінің атынан шот жіберу, логин / пароль және басқа жеке деректерді оған жіберу арқылы нақтылау туралы өтінішпен хаттар жіберу;

- интернет-дүкеннен сатып алуға болатын тауарлардың немесе қызметтердің жарнамасы.

- фишингтің жаңа түрі - пайдаланушыдан оның құжаттарының сканерленген көшірмелерін алу, мысалы, сіз лотереяда жеңіске жеттіңіз деген хабарлама жіберу арқылы жүргізіледі.

- ақшаны өте қолайлы шарттармен салуды ұсынатын Интернет-банктер, пирамидалар, жалған электрондық ақша айырбастаушылар мен әртүрлі қызметтер. Соңында тұтынушы ешқандай ақша немесе пайыздар алмайды;

- аз ақшаға беделді жұмыс табуды ұсынатын жалған еңбек биржалары құрылады. «Құжаттарды рәсімдеу» үшін ақша талап етіледі.

- Интернет лотереялары, казино және басқа да ойын түрлері. Жалған ұтыстар электрондық пошта мекен-жайлары немесе телефон нөмірлері арасында жіберіледі. Хатта ұтыстың фотосуреті және лотереяның «түпнұсқалық белгілері» - билеттің нөмірі, лицензия туралы куәлік және басқа жалған мәліметтер бар. Жүлде алу үшін ақша төлеу ұсынылады;

- қайыр сұрау - (пошта арқылы және әр түрлі форумдарда) балаға операция жасау, шіркеуді қалпына келтіру, балалар үйіне көмек және басқа да осыған ұқсас заттарға ақша аудару туралы өтінішпен шығады;

- скамерлік «scam» - алаяқтық. Ақшаны жымқыру үшін Интернетте танысу. Алаяқтар танысу сайттарында тіркеледі, олар әдетте шетелдік азаматтармен виртуалды қарым-қатынас орнатады. Ол интернетте романтикасын жүргізеді және тезірек бірге болу үшін белгілі бір ақша аударуды сұрайды.

Сайттарды бұзу және DDoS шабуылдары. Шабуылшылар шабуылды тоқтату үшін немесе сайтты белгілі бір уақыт ішінде бұзбайтындығына кепілдік беру үшін ақша бопсалаумен интернет-ресурстың жұмысын бұзады.

Профилактика

Интернеттегі алаяқтықтың алдын-алу бойынша ұсыныстар әзірледік: теледидар және әлеуметтік желілер арқылы халықты алдаудың жаңа тәсілдері туралы үнемі хабардар ету; мектептерде, орта және жоғары оқу орындарында дәрістер мен семинарлар өткізу арқылы азаматтардың құқықтық мәдениетінің деңгейін көтеру; құқық қорғау органдарының беделін нығайту.

Қылмысқа қарсы күрестегі халықаралық ынтымақтастық туындайтын жаһандық қауіп-қатерлерге тез арада ден қоюға мүмкіндік беріп, принципиалды жаңа тактикалық деңгейде ұйымдастырылуы керек.

Жаһандық желінінің криминализациялануына байланысты және осы жағдайдан шығудың екі жолмен мүмкін екендігі айқын болады: біріншісі, Дүниежүзілік Интернет желісіндегі қылмысқа бақылау жасау үшін әлемдік қауымдастықтың күш-жігерін біріктіру немесе жаһандық деңгейде оның жұмысын тоқтату арқылы, яғни жекелеген мемлекеттердің юрисдикциясындағы қылмысқа тиімді әрекет етуді ұйымдастыру мақсатында ұлттық сегменттерді оқшаулау қажет.

Біз алаяқтық жасауға ықпал ететін факторларды және алаяқтық жасауға ықпал ететін себептерді біле алдық. Интернетте алаяқтықтың кеңінен таралуының басты себебін анықтадық - бұл алаяқтардың жазасыз қалуы. Өз

кезегінде алаяқтардың құрбандары оны пайдасыз деп санап, құқық қорғау органдарына жүгінбейді. Электронды төлемдерді іздеу қиынға соғуы және келтірілген зияннның елеусіздігі көбіне қылмыстық іс қозғауға кедергі келтіреді, мәселе күрделене түседі. Бұл жағдай өзгермейінше, желідегі алаяқтық жағдайды түзету қиын болады.

Алаяқтықтың ең көп таралған тәсілі әлеуметтік инженерия – ақша қаражатын тонау мақсатымен клиенттерді алдау әдістері және жаңылыстыру. Алаяқтар әдетте банктің клиенттеріне «банктің қауіпсіздік қызметінен» немесе «қаржылық мониторинг қызметінен» хабарласып тұрмын деп қоңырау шалады және картада күдікті операция жүргізді деп хабарлайды. Олар ақша қаражатын сақтаймын деген желеумен клиентті оның шотына ақша ұрлау үшін бірқатар іс-әрекетті жасауға мәжбүрлейді. Сондай-ақ сенімді болуы үшін олар банктердің және басқа құрылымдардың ауыстырылатын нөмірлерінен қоңырау шалуы мүмкін. Алаяқтықтың схемасы одан әрі бірнеше сценарий бойынша дамиды. [https://kursiv.kz/kz/news/kogam/2021-02/pandemiya-kezinde-kazakstanda-internet-alayaktar-kobeyip-ketti].

Алаяқтар картаның төлем деректерін (16 таңбалы нөмір, иесінің аты-жөні, қолданыс мерзімі және артқы жағындағы үш таңбалы код, сондай-ақ банктен SMS-хабарлама алған код) білуге тырысады немесе жеке кабинетке кіру үшін деректерді алдап біліп алады. Сондай-ақ, қоңырау соғу кезінде алаяқтар өз құрбандарын банкоматтан ақшаны шешіп алуға және оларды «қаражатты құтқару» үшін арнайы шотқа аударуға көндіреді. Кейбір зиянкестер тіпті клиентке «қамқорлық көрсетіп» өз құрбандарына ең жақын банкоматқа дейін таксиге тапсырыс берген. [Пандемия кезінде Қазақстанда интернет-алаяқтар көбейіп кетті...https://kursiv.kz/kz/news/kogam/2021-02/pandemiya-kezinde-kazakstanda-internet-alayaktar-kobeyip-ketti].

Алаяқтар көбіне өздерін банк қызметкері ретінде таныстырып, клиент есепшотынан ақша ұрланғанын айтып, сақтандыру агентіне немесе "балама шотқа" ақша аударуды ұсынады. Пошта немесе мессенжер арқылы да қайырымдылық акциялары, ерекше қаржы қызметі, сыйлық ұтып алу сияқты түрлі шаралар туралы ақпарат жібереді.

Біріншісі – алдын ала төлем жасау немесе интернеттегі тауар үшін толық төлем алуға үгіттеу; Екіншісі – азаматтарға микронесие беретін ұйымдардың сайты арқылы онлайн несие рәсімдеу; үшіншісі – банк қызметкері болып хабарласып, тұрғындарды алдау; Сондай-ақ жиһаз, пластик терезелер дайындау, пәтерлерді жалға беру үшін алдын ала төлем немесе толық төлем алу; түрлі жобаға ақша салуға үгіттеу; картаның дербес деректерін білу арқылы ақша ұрлау.

Алматы полициясы күдіктінің жұмыс схемасын да жариялады. Мысалы, азаматвелосипед сату үшін OLX сайтына хабарлама жібереді. Аздан кейін WhatsApp нөміріңізге бұрын бейтаныс адам жазып, тауарды сатып алатынын айтады. Алайда өзінің басқа қала тұрғыны екенін алға тартып, келе алмайтынын жеткізеді. Оның орнына OLX жеткізу қызметінің бар екендігі туралы айтып, сол қызметті ұсынады. Алайда бұл сайт ондай

қызметті ұсынбайды. Ал оны білмейтін азаматтар қажетті мәліметтерді көрсететін нысанды толтыру үшін сілтеме жібереді. Содан кейін төлем түсетінін айтады.

Сілтемені басу арқылы адам фишинг деп аталатын сайтқа түседі. Сонымен қатар, оның дизайны өнімді сату туралы хабарландыру орналастырылған сайттың дизайнына сәйкес келеді: айырмашылықтарды оны мұқият зерделеу арқылы ғана байқауға болады.

Сондықтан жәбірленушілер өз деректемелерін ойланбастан енгізді: карта нөмірі, оның жарамдылық мерзімі және CVV коды. Осы сәттен бастап шабуылдаушы банк карталарына шексіз қол жеткізеді. Содан кейін алаяқ шот бойынша кез келген операцияны жүзеге асыра алады.

Интернет алаяқтықтықтың тағы бір жолы – әлеуметтік желі арқылы сауда жасау. Жуырда Петропавл қаласының полиция басқармасына тұрғындардан интернет-алаяқтық фактілері туралы бірқатар арыз түскен. Барлық жағдайларда жәбірленушілер өздерін интернет-дүкен ретінде көрсеткен Instagram парақшасында алаяқтың құрбаны болғанын хабарлады. Парақша иесі әйелдерге арналған киімдерді сатылымға шығарған. Алдын ала төлем жасауды талап етіп, содан кейін байланысқа шықпаған.

2.2 Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасаушы қылмыскер тұлғасы

Криминологтар объективті және субъективті факторлар мен өзара әрекеттесетін құбылыстардың жекелеген бөліктері - жеке тұлға мен қоршаған орта арасындағы күрделі тоғысу қылмыстың тікелей себебі ретінде әрекет ететіндігін мойындады. Тұлға өзінің барлық әлеуметтік, моральдық-психологиялық қасиеттері мен сипаттамаларының бірлігінде әрекет ете отырып, адамның өмірі мен қызметі процесінде қалыптасады. Тұлғаның қалыптасуы - бұл күрделі және «спиральды бойынша» даму процесі, және ол өзінің кейінгі дамуына жағдай дайындайды. Сондықтан ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың жасалу себептері туралы айта келіп, оның жекелік деңгейіне да тоқтала кету керек.

Авторлар құқық бұзушының жеке тұлғасын анықтауда әр түрлі көзқарастар айтады. Кейбіреулер қылмыскердің жеке тұлғасы дегеніміз - бұл қылмыстың жасалуын анықтайтын оның қоғамдық қауіптілігін қалыптастыратын әлеуметтік және психикалық қасиеттер жүйесі деп көрсетеді. Екіншілері, барлық қылмыс жасаған тұлаларды бір жалпы әлеуметтік типке жатқызады [61]. Үшіншілері, басқа адамдармен әр түрлі және жүйелі өзара әрекеттесу процесінде қалыптасқан әлеуметтік жағымсыз қасиеттер жиынтығы ұсынады [62, 61 б.].

Жалпы, қылмыскердің жеке тұлғасына тән қажеттіліктерін қанағаттандыру үшін әлеуметтік қауіпті жолды таңдаған биологиялық,

психологиялық және әлеуметтік сипаттамалардың, қоғамға қарсы көзқарастардың және моральдық нұсқаулардың жиынтығы немесе қажетті әлеуметтік қызметті көрсете алмау ретінде анықтауға болады. Бұл анықтама қасақана қылмыс жасағандарды және қылмыстық абайсызда кінәлі адамдарды қамтиды. Сонымен қатар, ол криминологиялық зерттеудің объектісі болып табылатын белгілер тізімін қамтиды:

1) әлеуметтік мәртебе қылмыскердің қоғамдық қатынастар жүйесіндегі орнын көрсететін белгілер жиынтығы ретінде;

2) қылмыскер тұлғасының оның іс-әрекетінің негізгі бағыттарындағы (кәсіптік және еңбек, әлеуметтік-мәдени, әлеуметтік) нақты көріністерінің индикаторлары арқылы көрінетін әлеуметтік функциялар;

3) құқық бұзушының азаматтық-құқықтық міндеттемелерге, мемлекеттік органдарға, заңға, тәртіпке, отбасына, басқа мәдени құндылықтарға, өзіне және қоршаған әлемге қатынасын көрсететін моральдық-психологиялық қатынастар.

Қылмыскердің жеке басын криминологиялық зерттеуде екі негізгі тәсіл бар. Бірінші тәсіл нақты қылмыскердің жеке басын зерттеуді қамтиды. Бұл жағдайда қылмыскердің жеке басы туралы нақты қылмыстың субъектісіне қатысты ғана талқылауға болады. Іс-әрекетте белгілі бір қылмыс құрамы бар-жоғын және қылмыстық жауаптылықтың мүмкін екендігін анықтау үшін нақты адамды және оның қылмыстық заңда белгіленген белгілердің барлық жиынтығына ие екендігін анықтау қажет.

Екінші тәсіл қылмыс жасайтын адамдар тобының жалпы қасиеттері туралы түсінік береді. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарға қатысты мұндай адамдардың ауқымы кең: компьютерлерімен манипуляция жасайтын жасөспірімдерден бастап, ұйымдасқан, мобильді және техникалық жабдықталған қылмыстық топтардың мүшелері болып табылатын өте қауіпті қылмыскерлерге дейін жатады. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жасайтын қылмыскерлердің анықталған түрлеріне сүйене отырып, біз олардың компьютерлік ақпарат саласында қылмыстық құқық бұзушылықтар жасауға себеп болуы мүмкін әлеуметтік-психологиялық сипаттамалары мен деформацияларын сипаттаймыз және олардың негізінде компьютерлік қылмыстың жеке-жеке себебін тұжырымдаймыз.

Бірінші топқа мақсаты айқын, кәсіби компьютерлік дайындық деңгейімен ерекшеленетін, әлеуметтік, қызметтік (немесе қызметтік) жағдайдағы, беделді, компьютерлік технологиялардың мүмкіндіктерін пайдалана отырып, қылмыс жасауға бағыттылығы бар адамдар кіреді.

Олар жүйенің ішінде орналасуы мүмкін - бұл банк қызметкерлері, қаржылық ресурстарға қол жеткізетін фирмалар мен мекемелердің қызметкерлері болуы мүмкін. Олар өздерінің арнайы білімдерін пайдалана отырып, саяси себептер мен кек алу немесе басқа да жеке мүдделер үшін жалдамалы және басқа материалистік себептерді басшылыққа ала отырып, қылмыс жасайды. Бұл қылмыскерлер коммерциялық, банктік, кәсіптік

құпияларды және жеке өмірді құрайтын ақпараттар еніп, өндірістік, мемлекеттік, экономикалық және өзге де қауіпсіздік саласындағы тыңшылыққа байланысты әртүрлі ерекше қауіпті қол сұғушылықтардың, қылмыстық құқық бұзушылықтардың максималды санын құрайды.

Бұл топқа техникалық деңгейі зиянды компьютерлік бағдарламалар жасауға немесе оларды өзгертуге мүмкіндік беретін «тар мамандар» кіреді. Мұндай бағдарламаны құру - бұл ақпаратты жою, бұғаттау, өзгерту немесе көшіру процестерін басқаруға арналған бастапқы мәліметтерді дайындаудан тұратын кешен [63, 93 б.]. Мұндай жұмысты тек жоғары білікті мамандар ғана орындай алады: кәсіби дайындалған бағдарламашылар; бағдарламаны зиянды ету үшін өзгерту мүмкіндігі бар адамдар. Олар сондай-ақ зиянды бағдарламалармен немесе осындай бағдарламалармен компьютерлік ақпарат құралдарымен заңсыз жұмыс істеуге қатысатындарды қамтиды.

Осы топқа тән ерекшеліктер: арнайы компьютерлік оқытудың болуы; компьютерге, компьютерлік жүйеге немесе компьютерлік желіге кіру; қылмыс жасауға мақсатты, ойластырылған дайындықтың болуы; алдын-ала қалыптасқан мотив үшін қылмыс жасау; қылмыс іздерін жасыру үшін ойластырылған шаралар жүйесін қолдану; өмірлік қаржылық мәселелерді шешу үшін, әдетте, қылмыс жасау; қылмыстарды жасыруға бағытталған әрекеттерді міндетті түрде қолданумен бірнеше рет жасау; тұрақты қылмыстық дағдыларды меңгеру.

Екінші топты ерекше ерекшелігі компьютерлік технологиялар мен бағдарламалау саласындағы кәсіпқойлықтың фанатизм мен тапқырлықтың элементтерімен тұрақты үйлесуі болып табылатын адамдар құрайды.

Зерттеушілер бұл топқа хакерлер мен крекерлер жатқызады. «Хакер» дегеніміз - компьютерлерге, компьютерлік жүйелерге немесе олардың желілеріне енудің заңсыз тәсілдерін іздейтін және дамытатын компьютер қолданушысы. Хакерлік орта дегеніміз - computer undergraund ортадағы әлемдік деңгейдегі өкілдер - 0,1%, кәсіпқойлар - 9,9%, әуесқойлар - 90% құрайды.

«Хакерлер» мен «крекерлер» арасындағы шекара өте жұқа және іс-әрекет мақсаттарына сәйкес сызылады. Біріншісі, танымдық және зерттеу мақсаттары үшін қорғаныс жүйесінің әлсіз жақтарына іздеу жүргізеді. Екіншісі - қауіпсіздік жүйелерін бұзып, компьютерлік желіге заңсыз еніп, ұрлау, алмастыру немесе басқа мақсаттарда компьютерлік ақпаратты қылмыстық мақсатта рұқсат етілмеген түрде қолданатын қарапайым ұрылар.

Біздің ойымызша, хакерлердің кіші типі ретінде фрикерлер(freak) - қолданушылар теледидарлық және басқа байланыс қызметтері үшін төлемнің баламалы нұсқаларын қалайды.

Үшінші топ - психиканың бұзылуының жаңа түрімен - ақпараттық аурулармен немесе компьютерлік фобиялармен ауыратын адамдар, компьютерлік техниканы үнемі қолданумен психикасы деформацияланады.

Қазіргі қоғамды қамтитын әмбебап компьютерлендіру, жұмыс орындарын дербес компьютерлермен жабдықтау, оларды күнделікті өмірге

енгізу үрдісіне байланысты көптеген адамдар мынадай жағдайларға тап болады:

- техностресс - адам ақпараттық және компьютерлік технологияларға барабар жауап бере алмайтын бейімделу аурулары;

- әлеуметтік оқшаулану - адамның бойындағы индивидуализм психологиясының күшеюімен, адамның қоршаған ортадан және қарым-қатынастан абстракциялануымен байланысты жағдай. Жаңа тәжірибеге деген қажеттілік танысу, дәстүрлі спорт немесе саяхат арқылы емес, Интернетті шарлау арқылы қанағаттандырылады.

Зерттеушілер компьютерлік қолданушыларды адамзат қоғамынан бөлетін рухани өмірді «виртуалдандыру» фактісін айтады. Баспа, радио, теледидар және қазіргі кездегі компьютерлік желілер (мысалы, Интернет) көптеген адамдармен ғана емес, миллиондаған адамдарға әсер ете отыр және психологиялық әсер етудің қуатты құралына айналды. Бірінші кезекте Интернетті қамтитын ақпаратты қабылдау мен берудің заманауи құралдары көптеген адамдар үшін көптеген құбылыстар, түсініктер мен мінез-құлық стереотиптері туралы идеяларды қалыптастырудың бірден-бір көзі болды. Сондықтан бұл топқа компьютерлік тәуелділіктен зардап шегетін, психикалық ауытқушылықпен байланысты емес адамдар кіруі керек.

Қылмыстық істерді, сондай-ақ арнайы әдебиеттерді талдау арқылы осындай қылмыстарды көбінесе ер адамдар жасайтынын айтуға мүмкіндік береді. Алайда әлемдік тәжірибедегі тенденцияларды ескере отырып, қылмыстың бұл түріндегі әйелдердің үлесі жақында артады деп болжауға болады.

Қылмыс жасайтын тұлғаларды зерттеу қылмыстық іс-әрекеттің белгілі бір түріне қарсы күресті дұрыс ұйымдастырудың маңызды шарты болып табылады. Ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскердің жеке басын зерттеу ерекше өзекті болып табылады, өйткені бұл жағдайда жақын уақытқа дейін құқық қорғау органдарының көзқарасына кірмеген субъектілермен жұмыс жасау қажет болады.

Заң ғылымдары туралы білімнің конвергенциясы негізінде ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскерге мынадай жалпы сипаттама және жіктеу беруге болады:

1. Жасы. Ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскер, негізінен, 18 жастан 24 жасқа дейінгі жастар (зерттелген қылмыстық істердің 55%) құрайды. Яғни студенттер немесе университетті бітіргендер, бірақ әлі үйленбегендер. Басқаша айтқанда, бұл қоғамдағы әлеуметтенудің ең маңызды кезеңін басынын өткізіп жатқан тұлғалар. Дәл осы жаста мұндай адамдарда өзін-өзі дамыту қажеттілігі туындайды. Қазіргі уақытта ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана

отырып жасалатын қылмыстық құқық бұзушылықтар жасарып келеді, өйткені қазіргі кезде балалар мен жасөспірімдер компьютерлік техникамен және желілік ақпараттық технологияларды тез меңгеруімен байланысты болып отыр [64, 251 б.].

2. Жынысы. Көптеген ғалымдар осы санаттағы қылмыстардың жасалуы ер адамдарға тән екендігімен келіседі [65, 100 б.]. Алайда, кейінгі кезде осы қылмыстарды жасайтын әйелдер санының өсу тенденциясы байқалады [66, 130 б.]. Бұл жағдайда әйелдер, әдетте, ер адамдармен бірге қылмысқа серіктес ретінде қатысады.

3. Білімі. Біздің ойымызша, осы түрдегі аса қауіпті қылмыстарды орта білімі бар және өзінің заңсыз әрекеттері ешқашан әшкереленбейді, тіпті өзін жазадан қашып құтылам деп ойлайтын адамдар жасайды. Ашылған қылмыстардың негізгі бөлігін біліктілігі төмен адамдар жасайды, олардың білімі жасаған қылмыс іздерін жасыруға жеткіліксіз болып келеді.

4. Тұлғаның психологиялық аспектілері. Криминологиялық әдебиеттерді зерттеу әдеттегі киберқылмыскердің келесі ұжымдық портретін қалыптастыруға мүмкіндік берді.

Әдетте, бұл қылмыстарды «виртуалды әлемде өзін-өзі тануға ұмтылатын, құрдастарымен қарым-қатынаста қиындықтары бар адам, электрондық цифрлық ақпаратты бағдарламалау мен қолдануда белгілі бір кәсіби биіктерге жетуге» ұмтылатын тұлғалар жасайды [67, 88 б.]. Сонымен қатар «өзін-өзі бекітуге ұмтылған, атақ-даңққа ие болуға тырысатын, өз шеңберінде беделге ие болуға» ұмтылатын адамдарда кіреді [68, 152 б.].

Киберқылмыскерлердің типтік бейнесі туралы келтірілген деректерге қарамастан, біз олардың өзгеріп тұрады деп санаймыз. Қазіргі кезде киберқылмыскер болу, ең алдымен, оның материалдық тұрғыдан тиімді екендігімен байланысты. Нәтижесінде, бастамашыл, авантюрист және тіпті харизматикалық адамдар қылмыстық жауапкершіліктен жалтару ықтималдығы жоғары болатын және үлкен мөлшерде қылмыстық табыстар әкелетін қылмыстық құқық бұзушылықтар жасайды.

Д.Айков осы санаттағы қылмыскерлерді қылмыстың себептеріне қарай үш санатқа бөледі: хакерлер (басты мақсаты - жүйеге ену), қылмыскерлер (басты мақсаты - пайда табу), бұзақылар (басты мақсаты - зиян келтіру) [69, 90 б.].

Көптеген батыстық құқық қорғау органдарының қызметкерлерінің айтуы бойынша, ақпараттық технологиялар саласында жеткілікті дәрежеде дайындалған және жұмысының сипаты бойынша компьютерлік жүйелерге белгілі бір кіру құқықтары бар, наразылық білдірген қызметкерлер және жақында жұмыстан шығарылған қызметкерлер киберқылмыскерлердің пайыздық құрамы бойынша ең маңызды топты құрайды.

Тергеу барысында киберқылмыскер әдетте қылмыс жасағандағы кінәсін мойындайды, өкінеді, зиянды жоюға тырысады және тергеуге белсенді үлес қосады. Кейбір зерттеулер киберқылмыскерлердің психикалық ауруға шалдығуы сирек кезесетінін айтады. Мысалы, хакерлерде аутистикалық бұзылулар бар, Аспергер синдромы, оларда әлеуметтік өзара

әрекеттесудің елеулі қиындықтарымен байланысты дамудың бұзылуы, сонымен қатар қызығушылықтар мен кәсіптердің шектеулі, стереотипті, қайталанатын жиынтығы бар.

Ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскер киберқылмыс түріне және компьютерде жұмыс істеу деңгейіне байланысты былайша бөлінеді:

- арнайы киберқылмыстарды жасауға мамандандырылған осы саладағы жоғары білімі бар адамдар. Арнайы білімнің болуы мұндай қылмыскер хакерлердің (крекерлердің) субмәдениетіне жататындығын білдіреді;

- қылмыстық іс-әрекеттерді жасаудың дайын алгоритмі бар, ақпараттық жүйелерде болатын мәліметтер мен процестерді нашар білетін, киберкеңістік әрекеттері үшін «спецификалық емес» электрондық құрылғылардың көмегімен (алаяқтық, ұрлық, ақшаны жылыстату, заңсыз) порнографиялық материалдарды тарату және т.б.) әрекет жасайтындар;

- бұрын қылмыс жасаған, киберқылмыскерлерге «қайта оқытылған», кибер кеңістігінің кең мүмкіндіктерін пайдаланатын адамдар, сондай-ақ қылмысты жасау үшін арнайы білімдері бар адамдарды біріктіруге қабілетті ұйымдасқан қылмыскерлердің өкілдері, негізгі күш-жігерді пайда алуға бағыттайды.

Ақпараттық қауіпсіздік саласындағы қылмыстық жауапкершілікке тартылған тұлғалардың санаттарын зерттей келе, «К бөлімінің» қызметкерлері осы саладағы көптеген қылмыстарды 18-29 жас аралығындағы жастар (60,8%) жасайтындығын атап өтті. Екінші орынды 30 және одан асқан азаматтар (33, 2%) алады. Ал кәмелете толмағандар жалпы жасалған қылмыстардың 7% құрайды екен. Бірақта соңғы уақытта жоғары технологиялар саласында жасалатын қылмыстардың ішінде кәмелетке толмағандардың үлес салмағы жыл сайын артып келеді. Мысалы, 2008 жылы Алматыдағы жоғары оқу орындарының 17 жасар студенті Нұрсұлтан қаласындағы ІІМ-ның серверін бұзған. Ол Интернеттен тауып алған нұсқаманы іске асырып көру мақсатында бұл қылмысқа барған. Бұл азаматтың қылмысқа қасақана бармағаны анықталып, қылмыстық іс тоқтатылған болатын [Пять лет назад специальным указом министра МВД РК был создан секретный отдел по борьбе с информационными преступлениями // https://www.zakon.kz/139027-pjat-let-nazad-specialnym-ukazom.html].

Криминологияда қылмыскер тұлғасын зерттеу кезінде мынадай мәліметтер жинақталады: жынысы, жасы, азаматтығы, білімі, әлеуметтік жағдайы, соттылығы, қылмыстық әрекетінің мақсаты мен мотиві және басқа да қылмыскердің белгілері зерттеленеді.

Ақпараттық қылмыстар саласында қылмыс жасайтын тұлғалардың аумағы өте кең. Арнайы зерттеулердің нәтижесі бойынша бұл саладағы қылмыстарды жоғары санатты мамандардан бастап қарапайым дилетанттарға дейін жасайды және әлеуметтік мәртебесі мен білімдері де әртүрлі болып келеді.

Осы категория бойынша қылмыс жасаған тұлғалардың білім деңгейі қылмыскерлердің интеллектуалдық даңгейінің негізгі көрсеткіш болып табылады. Зерттеліп отырған қылмыстың категориясы бойынша қылмыс жасағандардың 50%-дан 69%-ның орташа білімі; 7%-дан 21%-ның орташа арнайы білімі; 17%-дан 20,1%-ның жоғары білімдері болған [295 б. Омарова А.Б., Маликова Ш.Б. К понятию личности преступника преступлений в сфере компьютерной информации // Вестник КазНУ. Серия юридическая. №3 (79). 2016. С.293-297.].

Қылмыскерлердің «компьютерлік сауаттылығының» жоғары болуы бұл қылмыс түрінің латенттігінің жоғары болуына септігін тигізеді.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалған қылмыстарды жасаған тұлғаларға талдау жасай отырып, біз қылмыскер тұлғасының сипаттамасын жасауға мүмкіндік аламыз. Яғни, бұл – 18-24 жас мөлшеріндегі, орта (арнайы) білімі бар, жас адам. Құқыққа қарсы әрекетін көбінесе жалғыз жасайды, бұрын заң бұзушылық жасаумен көзге түспеген тұлға. Компьютерлік техникамен, ақпараттық технологиялармен және бағдарламалық қамтамасыз етумен қызығады. Мінезі – тұйық және оқшауланып жүреді.

2.3 Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың виктимологиялық маңыздылығы

Виктимология қазіргі криминологиядағы қылмыстық құқық бұзушылық жәбірленушісінің тұлғасын, мінез-құлығын және жүріс-тұрысын, қылмыстық құқық бұзушылықтың пайда болуына алып келетін негізгі себептерді және жағдайларды, қылмыстық құқық бұзушылықтың жәбірленушісі мен қылмыстық құқық бұзушының ара-қатынасын зерттеп, қылмыстық құқық бұзушылықтың орын алуына түрткі болған жағдайларда қылмыстық құқық бұзушылықтың жәбірленушілеріне қандай іс-қимыл жасау қажеттігін оқытатын ілім. Сонымен қатар, виктимология адамдардың виктимділігін азайтуға бағытталған іс-шараларды құрайды.

Виктимологиялық профилактика қылмыстық құқық бұзушылықтың алдын алудың бір бағыты және оның негізгі мақсаты - қылмыстық құқық бұзушылықтың жәбірленушілерінің қылмыстық құқық бұзушылықтың орын алуына түрткі болатын себептер мен жағдайлардың қатарына жатқызылатын оның жүріс-тұрысы мен мінез-құлқын айқындау болып отыр. Қазіргі уақытта осы қылмыстық құқық бұзушылықтардың алдын алудағы елімізбен қабылданып, қолданысқа енгізіліп жатқан нормативтік құқықтық актілерде «профилактитка» термині кеңінен қолданылуда десек болады. Сонда да болса, осы «профилактика» ұғымымен байланысты ілімдердің бірі «виктимология» ұғымы нормативтік құқықтық актілермен қарастырлып бекітілмегендігі сұрақ ретінде қалып отыр.

Виктимділік пен виктимогендік бойынша көзқарасымен бөлісіп жүрген И. Құрбанованың ойынша: «Виктимділік пен виктимогендік – бұл адамдарда

пайда болатын қылмыстың құрбанына айналуға бейімділіктің физикалық, психикалық және әлеуметтік қасиет нышандары. Виктимизация – виктимділіктің пайда болу процесі» [70, 22 б.]. Біз оның келтірілген пікірінен виктимділік пен виктимогендіктің белгілері үшке бөлінетіндігін және олардың адамдардың физикалық, психикалық және әлеуметтік қасиетінен тұратындығын байқаймыз. Осыған байланысты, қылмыстық құқық бұзушылықтардың жәбірленушілерінің, яғни адамдардың бойындағы өзіне тән физикалық, психикалық, әлеуметтік қасиетін жағымды және жағымсыз жақтарға бөледі. Жағымсыз физикалық, психикалық және әлеуметтік қасиеттері олардың қылмыстық құқық бұзушылықтың жәбірленушісіне айналдыратын жақтарын құрайды. Сондықтан кез келген адам қандайда бір құқық бұзушылықтан өзін сақтау немесе алдын алу мақсатында өзінің жағымсыз физикалық, психикалық және әлеуметтік қаситеттерінен айырылуы, болмаған жағдайда уақытша болса да олардан арылуы тиістігі туындайды.

Бір топ авторлар қылмыстылықтың алдын алуда жеке адамдарға қарсы қылмыстық құқық бұзушылықтардың жасалу механизімі бойынша бірінші кезекте қылмыстық құқық бұзушылық жәбірленушілерінің рөлі маңызды екендігін атап өтеді [71, 17 б.]. Осы бірқатар авторлардың пікірімен келісе отырып, жеке адамдарға қарсы қылмыстық құқық бұзушылықтардың орын алуына қылмыстық құқық бұзушылық жәбірленушілерінің өздерінің әсер етуі анықталады.

Виктимолог ғалымдар қылмыстық құқық бұзушылық жәбірленушілерінің алдын алудағы келесі бағыттағы шараларды ұсынады:

- әлеуметтік топтардың қылмыстық құқық бұзушылықтың виктимологиялық әрекеттерін анықтау мен жоюға бағытталған жалпы виктимологиялық алдын алу шаралары;

- қылмыстық құқық бұзушылықтан жәбір көрген құрбандарды анықтау, оларды қылмыстық құқық бұзушылықтан қорғануға оқытып үйрету және олардың жүріс-тұрысы мен мінез-құлқын заңға, әдет-ғұрып нормаларына сәйкес болуға бағытталған жеке виктимологиялық алдын алу шаралары;

- қылмыстық құқық бұзушылықтың виктимологиялық мәліметін, сонымен қатар, жәбірленушіні тану ерекшеліктерін ескере отырып, қылмыстық құқық бұзушылықтардың жекелеген түрлерінің жолын кесуге мүмкіндік беретін амал-тәсілдерді, ережелерді қолдана отырып, қылмыстылықтың алдын алу шаралары [72, 95 б.]. Д.В. Ривман мен виктимолог ғалымдар атап отырғанындай қылмыстық құқық бұзушылықпен күрестегі басты бағыттарды қылмыстық құқық бұзушылықтың жәбірленушілеріне аудару керектігі анықталады. Осының негізінде виктимологияның қылмыстық құқық бұзушылықтың алдын алудағы басты бағыты болу қажеттігі туындап отыр деуге негіз бар.

Қылмыстық құқық бұзушылықтың құрбанына қатысты виктимологиялық профилактика қылмыстық құқық бұзушылықтарды ескертудің криминологиялық теориясының құрамдас бөлігі болып табылатындығын көрсеткен А.Ш. Ещанов, виктимологиялық профилактика -

бұл виктимогенді жағдайға себеп болатын себептер мен жағдайларды болдырмау, оларды жоюға бағытталған ерекше процесс болып табылады. Сонымен қатар, қылмыстық құқық бұзушылықтарды ескертудің бұл нысаны адамның қылмыстық құқық бұзушылықтың жәбірленушісіне айналуына әсер еткен себептер мен жағдайларды анықтау мен оларды бейтараптандыру мақсатында жүзеге асырылатын іс-әрекеттер кешені болып табылатындығы жөніндегі пікірлерімен бөліседі [73, 43]. Қылмыстық құқық бұзушылықтардың виктимологиялық профилактикасын қарастыра отырып, осындай қылмыстық құқық бұзушылықтардың себеп салдарын анықтай келе, олардың жасалуына себептер мен жағдайларды анықтау қажеттігі туындайды. Себебі, қылмыстық құқық бұзушылықтардың орын алуына осы қылмыстық құқық бұзушылықтардың жәбірленушілері әсерінің бар екендігін атап өткен жөн.

Е.О. Алауханов қылмыстық құқық бұзушылықтың алдын алудағы виктимологиялық аспектілерге назар аудара келе, виктимологиялық алдын алу – бұл халықтың, кейбір азаматтардың қылмыстық қол сұғушылық жәбірленушілері болу қаупін азайту жолымен қылмыстылықтың алдын алуға бағытталған мемлекеттік және қоғамдық шаралардың жиынтығы деген түсінігін береді [74, 189 б.]. Е.О. Алаухановтың виктимологиялық алдын алуды халықтың, кейбір азаматтардың қылмыстық қол сұғушылық құрбандары болу қаупін азайту жолымен қылмыстылықтың алдын алуға бағытталған мемлекеттік және қоғамдық шаралардың жиынтығымен байланыстыруынан виктимологиялық алдын алу мемлекет пен қоғамдық шаралар екендігін анықтаймыз. Сонда да болса осы виктимологиялық алдын алу шаралары осы құқық бұзушылық профилактикасын жүзеге асыратын субъектілер тарапынан жан-жақты және толық жүргізіліп жатқандығына күдік көп.

И.И. Карпец виктимологияның дамуы виктимизация терминінің туындауына алып келді. Оны криминология курсының авторлары былайша түсіндіреді: виктимизация – белгілі бір тұлғаның, сонымен қатар белгілі бір адамдар қауымының қылмыстың құрбанына айналу процесі. Виктимизация қылмыстылықтан өзін қылмыс құрбандарына айналу процесінің жиынтығы ретінде ұсынылатындығымен ажыратылатындығын қарастырады [75, 45 б.].

Б.Т. Абулкаированың виктимологиялық алдын алуға берген авторлық түсінігі бойынша виктимологиялық алдын алудың белгілеріне мыналар жатады:

- жоғары виктимділік деңгейі бар нақты топтар немесе виктимділік мінез-құлқын құрайтын жағдайлар мен факторларды, уақиғаларды бейтараптандыруға, жоюға, анықтауға бағытталған әлеуметтік институттардың қызметі;

- азаматтарды қылмыстық құқық бұзушылықтан сақтандыруға және қызметті жүзеге асыратын арнайы қорғау құралдарын жетілдіруге бағытталған әлеуметтік институттардың қызметі. [76, 48 б.].

Қылмыстық құқық бұзушылықтың виктимологиялық алдын алу қоғам мен мемлекеттің қауіпсіздігін қамтамасыз ету алдында жүзеге асырылатын

маңызы зор шаралардың жүйесін құрайды. Қылмыстық құқық бұзушылық профилактикасы саласындағы виктимологиялық саясатты жүзеге асыру өз кезегінде халықтың құқықтары мен бостандықтарын, өмірі мен денсаулығын қылмыстық құқық бұзушылықтан қорғауға ықпал ететіндігі белгілі. Мемлекет қылмыстық құқық бұзушылық виктимологиясы бойынша нормативтік құқықтық актілерді қарастырып, оларды жүзеге асыру арқылы қоғамды виктимизацияланудан сақтауға мүмкіндік береді.

Виктимологиялық алдын алу келесі қызметтерден тұрады:

- қылмыстық құқық бұзушылық жағдайға ықпал ететін белгілері бар адамдар мен топтарды анықтау және жою;

- қылмыстық құқық бұзушылықтың жәбірленушілеріне эмоционалды және психологиялық қолдауды ұйымдастыру шаралар кешенін жүзеге асыру;

- виктимділіктің алдын алуда тиісті мемлекеттік органдарды міндеттеу.

Қылмыстық құқық бұзушылықтардың алдын алу құқық қорғау органдарының ішіндегі ішкі істер органдарына ғана жүктеліп қоймай, сонымен қатар, басқа да мемлекеттік және қоғамдық институттарға, азаматтарға да жүктелген. Өкінішке орай, Қазақстанда қылмыстық құқық бұзушылықтың алдын алу шараларымен тек ішкі істер органдары ғана айналысатындығы көрініп тұр. Қылмыстық құқық бұзушылықтың профилактикасымен айналысатын профилактиканы жүзеге асыратын субъектілер қатарындағы мемлекеттік билік органдары, жергілікті өкілді органдар, үкіметтік емес ұйымдар тарапынан жүргізіліп жатқан шаралар жоқтың қасы екендігін айта кетуіміз керек.

Криминологияның бір бағыты болып саналатын виктимологияның негізгі мақсаты - қылмыстық құқық бұзушылықтардың орын алуына түрткі болатын себептер мен жағдайларды анықтап, зерделеп, жою арқылы виктимділіктің алдын алу болып табылады. Кез-келген адам виктимділікке бейім болатындығын атап кеткеніміз дұрыс. Барлық адам қылмыстық құқық бұзушылықтың жәбірленушісі болудан сақтандырылмаған. Осыған байланысты, кез-келген тұлғаның виктимологиялық қауіпсіздігін қамтамасыз ететін арнайы алдын алу шараларының жүргізілуі келесі бағытта болуы қажет:

1) отандық нормативтік құқықтық актілерді жетілдіру;

2) қолданыстағы нормативтік құқықтық актілерге қылмыстық құқық бұзушылық жәбірленушілеріне жүргізілетін шаралар туралы өзгертулер мен толықтырулар енгізу;

3) қылмыстық құқық бұзушылық жәбірленушілерінің алдын алу мақсатында олармен жұмыс жүргізетін орталықтарды құру;

4) қылмыстық құқық бұзушылық жәбірленушілерінің қылмыстық құқық бұзушылықтың орын алуына түрткі болған себептері мен жағдайларды арнайы есепке алу.

Т.В. Варчук қылмыстық құқық бұзушылық құрбандарына қатысты өзінің пікірлерімен бөлісе отырып, қылмыстық құқық бұзушылық құрбандарын оқып білудің стратегиялық мақсаты, тұтастай алғанда, жәбірленушіге кең көлемдегі құқықтық тәрбие арқылы нақты бір қылмыстық

құқық бұзушылық пен қылмыстылықтың алдын ала ескертудің тиімділігін жетілдіруден тұратындығын атап өтеді [77, 39 б.]. Біз Т.В. Варчуктың алға қойып отырған пікіріне назар сала отырып, негізінен қылмыстық құқық бұзушылықпен күрестегі тиімді жолдың бірі ретінде қылмыстық құқық бұзушылық құрбандарын тереңінен оқып үйрену арқылы, оларға құқықтық тәрбие беру болып отыр. Қандай да болмасын, қылмыстық құқық бұзушылықтардың орын алуына қылмыстық құқық бұзушылық құрбандарының өздері себепкер болып жатады. Сонда да болса, олар еш жауаптылыққа тартылмай, оларға қатысты алдын алу шаралары қарастырылмаған.

Қылмыстық құқық бұзушылықты ескерту сияқты виктимологиялық профилактиканың күрделі құрылымы бар, ол түрлі субъектілермен түрлі нысанда жүзеге асырылады және өзіндік ерекшеліктерге ие. Осындай ерекшелікке виктимологиялық профилактиканың мақсаттарын да жатқызуға болады. Олар:

- қоғамдық қауіпсіздікті қамтамасыз ету;
- жеке тұлғаның құқықтарын, бостандықтары мен заңды мүдделерін қорғау;
- халықты виктимизациядан қорғау мақсатында әлеуметтік қорғау жүйесін құру;
- қылмыс құрбандарына әлеуметтік көмек көрсету болып табылады.

Қоғамдық қауіпсіздікті қамтамасыз етудегі профилактика негізінен тек қана ішкі істер органдарының қызметтік міндеттерімен қамтылған болып отыр деуге болады. Сонда да болса, осы бағыттағы құқық қорғау органдарынан басқа қандай да бір шараларды өз беттерімен атқаратын қандай да болсын мемлекеттік немесе мемлекеттік емес мекемелер, ұйымдар жоқтың қасы деуге болады. Осыған байланысты қылмыстық құқық бұзушылықтың алдын алудағы қоғамдық қауіпсіздікті қамтамасыз ету міндеттілігін қоғамдық бірлестіктерге, мемлекеттік емес ұйымдарға жүктеу қажеттілігі туындап отыр. Осы бағыттардың бірі ретінде қандай да болсын мемлекеттік емес ұйымдар, мекеме, кәсіпорын, қоғамдық бірлестіктер өздерінің басшылыққа алатын қызметтік ережелеріне қоғамдық қауіпсіздікті қандай да болсын құқық бұзушылықтан қорғау бағытындағы міндеттемелер енгізе отырып, олар құқық қорғау органдарымен тікелей байланыста жұмыс жасауы керек.

Осы аталғандардың негізінде қылмыстық құқық бұзушылықтың алдын алуда арнайы жоспарлар мен бағдарламалардың болуы шарт. Қылмыстық құқық бұзушылықтың алдын алудағы жүргізілетін іс-шаралардың белгіленуі мен олардың орындалу мерзімдері мен орнын белгіленетін жоспардың жасалуы қылмыстық құқық бұзушылықтың алдын алудағы профилактиканың негізгі мақсатына жетуге мүмкіндік береді. Өйткені, қылмыстық құқық бұзушылықтың алдын алудағы жоспарда қылмыстық құқық бұзушылықтың орын алу себептері мен оған мүмкіндік беретін жағдайлар ескеріле отырып, олар бойынша қандай іс-шаралардың атқарылатындығы белгіленеді.

И. Құрбанова қылмыстылықтағы виктимологиялық мәселелерді қарастыра келе, жәбірленушінің субъективті және объективті мінездемелерін ескере отырып, оны былайша жіктейді:

1. Жәбірленушіні жынысы бойынша жіктеу;
2. Жәбірленушінің жасы бойынша жіктеу;
3. Жәбірленушіні олардың рөлдік статусы бойынша жіктеу;
4. Жәбірленушіні қылмыскерге қатынасына байланысты жіктеу;
5. Жәбірленушіні адамгершілік-психологиялық белгілері бойынша жіктеу;
6. Жәбірленушіні қылмыстың ауырлығына байланысты жіктеу [70, 17 б.]. И. Құрбанованың ұсынысына назар аудара отырып, біздің пікірімізше, қылмыстық құқық бұзушылықтардың жәбірленушілерін автордың көрсетіп отырғанындай жіктей отырып, оларға шолу жасау арқылы қашан, қандай жағдайда және кімге қатысты қылмыстық құқық бұзушылықтың алдағы уақытта болу мүмкіндігін анықтауға болады. Осыған байланысты, орын алған қылмыстық құқық бұзушылықтың алдын алу ғана емес оның алдағы уақытта ашылуы, яғни қылмыстық құқық бұзушылық жасаған адамды анықтауда қылмыстық құқық бұзушылық жәбірленушісінің көмегі мол дегіміз келеді.

Жалпы виктимологиялық ескерту шаралары жағымсыз экономикалық факторларға, қоғамның әлеуметтік және саяси тұрғыдан тұрақтануына әсер етуге, адамдар арасындағы адамгершілік - психологиялық қарым-қатынастарды нығайтуға бағытталған. Тәжірибе көрсеткендей кейбір қылмыстық құқық бұзушылық жәбірленушілердің құқықтық сауатсыздығына байланысты орын алып жатады. Сондықтан, жалпы ескерту шаралардың ішінен халыққа құқықтық тәрбие беру, түсіндіру жұмыстарын жүргізу, яғни бұқаралық ақпарат көздерін пайдалана отырып, халықтың құқықтық сауаттылығын арттыру, адамдарды абай болуға, қауіпсіздік шараларын сақтауға үгіттеу шаралары тиімді болып табылады.

Жоғарыда қарастырылғандарды қорытындылай отырып, қоғамдық қауіпсіздікті қамтамасыз етудегі профилактика негізінен тек қана ішкі істер органдарының қызметтік міндеттерімен қамтылған болып отыр деуге болады. Сонда да болса, осы бағыттағы құқық қорғау органдарынан басқа қандай да бір шараларды өз беттерімен атқаратын қандай да болсын мемлекеттік немесе мемлекеттік емес мекемелер, ұйымдар жоқтың қасы деуге болады. Осыған байланысты қылмыстық құқық бұзушылықтың алдын алудағы қоғамдық қауіпсіздікті қамтамасыз ету міндеттілігін қоғамдық бірлестіктерге, мемлекеттік емес ұйымдарға жүктеу қажеттілігі туындап отырғандығын айта кету керек. Осы бағыттардың бірі ретінде қандай да болсын мемлекеттік емес ұйымдар, мекемелер, кәсіпорындар, қоғамдық бірлестіктер өздерінің басшылыққа алатын қызметтік ережелеріне қоғамдық қауіпсіздікті қандай да болсын құқық бұзушылықтан қорғау бағытындағы міндеттемелер енгізе отырып, олар құқық қорғау органдарымен тікелей байланыста жұмыс жасауы керек.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың құрбандары жеке адамдар да, белгілі бір әлеуметтік топтар да болуы мүмкін.

Криминологиялық әдебиеттерде зерттеушілердің пікірінше қылмыстың жасалуына әсер ететін көптеген факторлар қарастырылды. Криминологиялық әдебиеттерде келтірілген ғылыми тәсілдерге сүйене отырып және ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жасаудың ерекшеліктерін ескере отырып, ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың жасалуына әсер ететін виктимологиялық факторлар, олардың мазмұнына сәйкес жеке-жеке болып бөлінеді: жеке, әлеуметтік және мінез-құлық. Виктимологиялық факторларға жеке адамдардың немесе адамдардың қауымдастығының оларды қылмыстық қол сұғушылық объектісіне айналдыратын типтік қасиеттері де, олардың қорғалуын өз бетінше қамтамасыз ету қабілетін төмендететін типтік қасиеттері де кіруі мүмкін. Яғни, алдымен адам қылмыскерлердің назарын аударады, содан кейін, егер ол өзін тиісті қорғаныспен қамтамасыз етпесе, ол қол сұғушылықтың құрбаны болады. Егер адам олардың қауіпсіздігіне қамқорлық жасаса, онда бұл құрбан болмас еді.

Сонымен, жеке тұлға ретінде ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың құрбаны түсінігінің мазмұны оның мәртебесімен белгілі бір қылмыстың қылмыстық механизміндегі мінез-құлықпен және рөлмен байланысты.

Виктимологиялық факторлардың әсерінен адам потенциалды немесе қылмыстың құрбаны болады. Жеке тұлғаға қатысты бұл жеке тұлғаның әлеуметтенуінің ерекшеліктерімен байланысты жеке-жеке (әлеуметтік-психологиялық) қасиеттер жиынтығы. Нақты жеке тұлғаның жәбірленуі - бұл оның жеке қасиеттерінің сыртқы факторлармен теріс әсер етуі нәтижесінде оның қылмыстың құрбанына айналу мүмкіндігі. Әдетте қылмыскер қылмыстың құрбанны туралы жақсы біледі. Ешқандай ақпарат оның назарынан тыс қалмайды: қылмыс механизмінде жәбірленушінің жынысы, жасы, кәсібі, мамандығы, қызметтік және отбасылық жағдайы жиі маңызды рөл атқарады.

В.Устинов пен Д.Ривман берген жәбірленушілердің жіктеуіне сәйкес келесілер ажыратылады:

«Бейтарап» тип - осы түрдегі жәбірленушілердің мінез-құлқы барлық жағынан мінсіз және ешқандай жолмен қылмыстық іс-әрекеттерді тудырмайды; өз мүмкіндіктері шегінде бұл құрбандар жағдайды сыни тұрғыдан қарастыра алады;

«Критикалық емес» тип - осы типтегі жәбірленушілердің мінез-құлқы абайсыздығымен, өмірлік жағдайларды дұрыс бағалай алмауымен, сенімділігі мен сенімділігімен ерекшеленеді. Егер олар жағдайдың айқын қаупін көрмесе, онда олардың мінез-құлқы заңдылықтан асып түсетінін мойындайды.

Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылыққа қатысты бірінші типке ұялы байланыс пайдаланушыларының құрбандары жатады. Бұл әр түрлі ұялы байланыс компанияларының абоненттері, олар техникалық дағдылары мен қаржылық шектеулеріне байланысты әлсіз қорғалған Интернет қосылыстарын пайдаланады және пайдаланушылардың теңгерімінен қаражаттарды рұқсатсыз «алып тастайтын» вирустық бағдарламалардың құрбаны болады. Оларға жарақат алған телефон қолданушылары - телефон «қарақшыларының» құрбанына айналған абоненттер қосылады. Екінші түріне компьютерлік қарақшылардың құрбандары жатады. Бұл лицензияланған бағдарламалық өнімдердің қымбаттығына байланысты оның жалған көшірмелерін қолданатын және сол арқылы әлеуетті құрбанға айналатын қарапайым пайдаланушылар.

Потенциалды құрбандардың құрбандық қасиеттері сыртқы - әлеуметтік қана емес, сонымен қатар ішкі - психологиялық белгілердің әсерінен қалыптасады, сондықтан ақпараттық – телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың құрбандарына қатысты «патологиялық» басқа түрін ажыратуға болады. Бұл типке әлеуметтік желілерге тәуелділік, компьютерлік ойындарға тәуелділіктің түрлері немесе Интернетте сағаттап отыратын құрбандар кіруі мүмкін.

Осы типтегі құрбандардың мінез-құлқы «виртуалды» өмір салтына дағдылануымен, виртуалды байланыс орнатудағы жүйелілікпен, виртуалды серіктестермен қарым-қатынас кезінде жеңілдік пен жеңілдікпен сипатталады. Мұндай құрбандардың жеке басының психологиялық сипаттамалары, ең алдымен, осы белгілер олардың жасалуын анықтайтын ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар санаты жатады. Мысалы, виртуалды биржаларда алаяқтық құрбандары бірінші кезекте виртуалды биржаларда маникальды тәуелділікпен жүйелі түрде ойнайтын, осылайша өздерінің қаржылық мәселелерін шешуге тырысатын қатысушылар болуы мүмкін. Құрбандар жағдайдың айқын қауіптілігін көрмейді, сондықтан ішкі жеке қасиеттерінің сыртқы факторлармен өзара әрекеттесуі нәтижесінде қылмыс құрбаны рөлінде болуы мүмкін.

Егер киберқылмыс нәтижесінде белгілі бір қоғамдастыққа зиян келтірілсе, онда виктимологиялық факторлар дегеніміз - бұл белгілі бір қылмыстың қатынастардың күрделі жүйесі арқылы жасалуына ықпал ететін әлеуметтік факторлар. Әлеуметтік сипаттағы факторларға, атап айтқанда, қылмыстың құрбаны болуы мүмкін қоғамның әлеуметтік иерархиясындағы жағдайы жатады. Ұйымды жоспарланған кибершабуылдың құрбаны ретінде таңдау туралы сөз болғанда, оның өндірістік және қаржылық ортадағы беделі шешуші болады. Әрине, қылмыскер ұсақ көтерме өнімді сататын кез-келген фирмадан гөрі банкті, өркендеген компанияны, ауқатты холдингті мақсатты етіп таңдайды.

Құрбандық жағынан маңызды факторларға ақпараттық – телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылық жасауды алдын-ала анықтайтын мінез-құлық (белсенділік) факторлары жатады. Адам қылмыстың потенциалды құрбанына айналатын (немесе болуы мүмкін) мінез-құлық факторлары болу ортасы мен жеке әлеуметтік-психологиялық қасиеттерінің өзара әрекеттесуінің нәтижесі болып табылады. Сонымен қатар, мұндай өзара әрекеттесу әртүрлі нәтижелерге әкелуі мүмкін. Нақты өмірлік жағдай - бұл адам өзінің субъективті позицияларынан қабылдайтын объективті фактор. Сондықтан, ақпараттық – телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылық саласындағы қылмыстар құрбандарының мінез-құлқы, басқа қылмыстық мінез-құлық түрлері сияқты, заңды, заңсыз немесе бейтарап (заң тұрғысынан немқұрайлы) болуы мүмкін.

Жәбірленушілер төмендегі факторлардың нәтижесінде қылмыскерлердің қақпанына түсіп қалуда:

- ақпараттық қауіпсіздік мәселесіне қажетті түрде көңіл бөлмеу;
- қаржы институттары тұтынушыларын жоғалтпау үшін оларға жасалған қылмыстар туралы құқық қорғау органдарына хабарлама жіберуге құлықсыздығы;
- Интернет пайдаланушылардың құқықтық және компьютерлік сауатсыздығы;
- Интернет қызметтерін және электронды төлем құралдарын белсенді қолданудың нәтижесіндегі жоғары виктимділік. Бүгінгі таңда пайдаланушылардың ешқайсысы толық ақпараттық қауіпсіздікті сезіне алмай келеді.

3.1 Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың алдын алу мәселелері

Мемлекет және қоғам бір-бірімен тығыз байланысып, әрқашан даму үстінде болады. Ақпараттық технологияларда әрқашан жетілу және даму кезеңдерін бастан кешіріп отырады. Бұл құбылыс алғашында қоғамды алға ұмтылуға жетелесе, кейнгі жылдары бұл салада заңға бағынушы азаматтарға қарсы құқыққа қайшы әрекеттер жасалуда. Ақпараттық телекоммуникациялар желілердің шексіз шексіз мүмкіндіктері ақпараттық саладағы көптеген қылмыстық құқық бұзушылықтарға жол ашты. Қылмыскерлер бет перде кимей, қолына қару-жарақ ұстамай, адам өлтірмей-ақ банктерді тонап, кәсіпорындардың қорындағы ақшаларды қас пен көздің арасында қолды ететін қылмыскерлер пайда болды.

Жоғары технологиялық қылмыс біздің мемлекетімізде алғаш рет 2003 жылы Лисаков қаласындағы «Гол+Пас» букмекерлік кеңсесінде жасалған болатын. Компьютерлік желі арқылы 3 миллион 500 мың теңгені оп-оңай жымқырған К. деген азамат сот сараптамасынан соң жасаған қылмысы үшін 5 жылға сотталды [78].

Мемлекет біздің және шетелдік мемлекеттердің компьютерлік ақпарат және телекоммуникация саласындағы криминогенді жағдайларға талдамалар жасау арқылы бірнеше нормативтік-құқықтық актілер қабылдаған болатын. Қазақстан Республикасының 1997 жылғы 16 шілдеде күшіне енген Қылмыстық кодексінде компьютерлік қылмыстың қылмыстық жауапкершілігі алғаш қаралды. Ал 2016 жылдың 01 қаңтарынан бастап күшіне енген қолданыстағы Қылмыстық кодексте ақпараттық технологиялардың қауіпсіздігіне қарсы қылмыстық құқық бұзушылықтарға жауапкершілік қарастырылған. 2004 жылы Ішкі істер министрінің бұйрығымен ақпараттық қылмыстармен күрес бойынша арнаулы бағытта жұмыс жасайтын кәсібилендірілген «К» құпия бөлімі ашылды.

Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтардың негізгі бір ерекшелігі – халықаралық байланыс желілері арқылы мемлекеттер арасындағы шекараны елемейтіндігінде болып отыр. Сонымен қатар бұл салада қылмысқа барар алдында олар өздері туралы мәліметтерді өзгертіп, жан-жақты жетілдірілген арнайы бағдарламаларды пайдаланады. Ақпарат саласындағы жеке дара қылмыс жасайтын тұлғалардың орнына сапалы ұйымдасқан қылмыстық топтар келе бастады.

Аз уақыттың ішінде жоғары технологиялар саласындағы қылмыстардың ауқымы тез қарқынмен кеңейе бастады. Мысалы, олар алғашында тек экономикалық салада ғана жасалатын болса, уақыт өте келе мемлекеттік маңызы бар интернет-ресурстарға хакерлік «шабуылдар» жасау жиілеп кетті.

IT-саласындағы қылмыстық құқық бұзушылықтардың алдын алудың тиімділігін арттыру үшін ақпараттық технологияларды тұтынушылардың өздерінің қауіпсіздік шараларын ұмытпағаны дұрыс. Осы саладағы қылмыстардың құрбанына айналмас бұрын қарапайым сақтық ережелерін сақтау қажет және ол өз кезегінде осы саладағы қылмыстардың санын азайтуға көмеген тигізеді.

Қарапайым сақтық шараларына мыналар жатады:

1 Таныс емес адамдар үшін SIM-карта сатып алу кезінде өзінің жеке куәлігіндегі мәліметтермен бөлісуге келісімін бермеу;

2 Таныс емес адамдармен Сіздің SIM-картаңызға келген құпия мәліметтермен бөліспеу;

3. Сіздің ұялы телефоныңызға таныс емес абоненттен келген СМС-хабарламалардың сілтемелеріне көшпеңіз және суреттерді жүктемеңіз;

4. Ешқашан ІІО интернет немесе ұялы байланыс арқылы электронды айыппұл төлеу туралы хабарлама жібермейтінін есте сақтаңыз;

5. Әлеуметтік желілер немесе электронды пошта арқылы таныс емес адамдармен араласпаңыз, өйткені бұл тәсіл соңғы кездері террористік ұйымдарға тарту үшін жиі пайдалануда.

Теорияда қылмысқа мемлекеттік-құқықтық әсер етудің мәнін тұжырымдамалық тұрғыдан анықтауға арналған көптеген терминдер қолданылады.

Дәстүрлі «қылмысқа қарсы күрес» және «қылмыстың алдын-алу» [79] ұғымдары біртіндеп басқаларымен ауыстырылады: «қылмысқа қарсы соғыс», «қылмысқа қарсы күрес», «қылмысқа бақылау» [80] және т.б.

Қоғамдағы әлеуметтік тыныштықты қамтамасыз ету тұрғысынан мемлекеттің профилактикалық қызметі қылмысқа дайындық немесе жасамақ болған адамдардың іс-әрекеттерін тоқтатуға бағытталған шаралар қабылдау арқылы қылмыстардың *жолын кесуді* көздейді; нақты қылмыстарды жоспарлап отырғандарды анықтау арқылы қылмыстың *алдын алу*; қылмыстарға *қарсы тұру*, олардың жасалуына ықпал ететін себептер мен жағдайларды анықтау және жою, тиісті шаралар кешенін қолдану.

Әлеуметтік тұрғыдан алғанда, қылмыстың алдын алудың жоғарыда аталған үш аспектілері арасында қарсы тұру қылмыстардың жасалуына ықпал ететін себептер мен жағдайларды білу негізінде тұжырымдалған шаралардың кешенді жүйесі ретінде үлкен қызығушылық тудырады (немесе қылмыстардың жекелеген түрлері) және олардың іс-әрекетін болжауға бағытталған. Бұл қарсы шаралар бұлтартпау мен алдын-алу шараларынан түбегейлі ерекшеленеді.

Компьютерлік қылмысқа қарсы күрес мемлекеттің, қоғамның және жекелеген пайдаланушылардың ақпараттық саладағы заңсыз мінез-құлықты ілеспе факторлар бойынша өзара іс-қимылына негізделген.

Мұндай мақсатты жүзеге асыру әр түрлі құқық салаларының әдістері мен құралдарын біріктіру арқылы мүмкін болады. Қылмыстық циклдің мүмкіндіктері (қылмыстық, қылмыстық іс жүргізу, қылмыстық-атқару заңнамасы) азаматтық құқықтың нормаларымен үйлесуі керек. Адамзат

қылмыстық қуғын-сүргіннің алуан түрін бастан кешірді, ал қазір ғалымдар «жаза дағдарысы» мен бүкіл қылмыстық сот жүйесінің дағдарысы туралы көбірек айта бастады [81]. Осыдан - қылмыстық құқық бұзушылыққа тосқауылдың бір түрі ретінде нақты әлеуметтік қатынастарды барынша толық, жан-жақты реттеу арқылы жүзеге асырылуы тиіс.

Тиісті нормативтік-құқықтық базасыз (негізгі заң және осы саладағы басқа заңдар мен ережелерді жүйелеу) компьютерлік қылмысқа қарсы әрекет тиімді болмауы мүмкін. Қазақстанда қажетті криминологиялық заңнама бар. Оны екі негізгі бөлікке бөлуге болады. Бірінші бөлім - өзінің кең мағынадағы қылмыстық заңнамасы, оған материалдық құқық нормаларымен қатар, қылмыстық іс жүргізу және қылмыстық құқық нормалары кіреді. Екінші бөлім - қылмыстың жасалуына жол бермейтін қылмыстық емес репрессиялық қызметті реттейтін криминологиялық заңнама. Бұл заңнама мемлекеттің криминологиялық саясатын реттейтін нормативтік құқықтық актілерден тұрады; халықтың криминогендік контингенттерін қайта әлеуметтендіру; қаржылық қызметті, сондай-ақ есірткінің, күшті заттардың, қару-жарақтың және оқ-дәрілердің, мәдени-тарихи құндылықтардың, валютаның және басқалардың айналымын бақылау, кәмелетке толмағандардың ұсақ құқық бұзушылықтары мен әдепсіз әрекеттерінің алдын алу; виктимологиялық қылмыстың алдын алу; қылмысты әлеуметтік бақылау субъектілерінің өздері қызметі және т.б.

Заңмен реттелетін қоғамдық қатынастардың сипатымен функционалды түрде алдын-ала анықталған құралдар мен әдістерге байланысты қылмысқа екі түрге бөлінетін құқықтық бақылау орнату арқылы қарсы тұруға болады: оң және репрессивті.

Қылмысқа оң құқықтық бақылау салалық тәртіпте тиісті құқықтық қатынастарды реттейтін құқықтық нормалардың жиынтығын қамтиды. Позитивті құқықтық бақылаудың тиімділік дәрежесі позитивті қоғамдық қатынастарды құқықтық реттеу механизмінің тереңдігі мен айқындылығына, заңдық нұсқамалардың негізділігіне, олардың қоғамдық пайдалылығы мен заңды мағынадағы тиімділігіне тікелей байланысты.

Бұл критерийлер компьютерлік қылмыстарды оң бақылауға қатысты қолданыстағы заңдылық жағдайын талдауға мүмкіндік береді.

Компьютерлік ақпарат саласындағы қылмыстардың қылмыстық-құқықтық сипаттамасы

Компьютерлер адамның өміріне салыстырмалы түрде жақында енді. Оларды адамның өміріне байланысты құру жұмыстары 1940-шы жылдары КРСО-да, АҚШ-та және Ұлыбританияда бір уақытта басталды. КСРО-да алғашқы компьютер 1950 жылы жасала бастады, ал 1950 жылдардың аяғында Кеңес Одағында «Орал», «Минск», «Ереван» атты компьютерлер жасалып шығарылды. 1990 жылдардың ортасынан бастап компьютерлер бүкіл әлемде кең тарай бастады.

Алғашында компьютер математикалық есептеу құралы ретінде ойластырылып шығарылды. Қазіргі уақытта компьютер адам өмірінің барлық саласында қолданылады және ол ақпаратты іздеуге, қабылдауға, беруге, өндіруге және таратуға арналған әмбебап құрылғыға айналды.

Болжамдарға сүйенетін болсақ, жақын болашақта дүние жүзіндегі әрбір адам ғаламдық компьютерлік желілерге қол жеткізе алады. Ал компьютерлік технологиялар әрбір отбасыға, кеңсеге, технологияға немесе өндіріске ғана емес, сонымен қатар адамзат пайдаланатын құрылғылар мен құралдардың көпшілігіне енеді.

Алғашқы компьютерлік желі 1960 жылдары АҚШ қорғаныс министрлігінде пайда болды. АҚШ университеттері әскери зерттеушілер құрған желіге қосылды. Шамамен 1980 жылдардың ортасынан бастап АҚШ әскерилері желінің бір бөлігін тек өз мақсаттары үшін қолдана бастады, ал желінің қалған сегменті біртіндеп қоғамдық байланыс арнасына айналды. Қазір бұл бүкіләлемдік желі «Интернет» (Internet) деген атпен белгілі.

Компьютерлік технологиялардың дамуы бұрын қылмыстық заңнамаға белгісіз құбылыстармен бетпе-бет келуіне әкелді және қоғамның дамуына айтарлықтай қауіп төндіре бастады. Атап айтқанда, компьютерлерге жалған ақпараттар енгізу, компьютерлерді заңсыз пайдалану, ақпаратты өңдеуді бұзу, ақпаратты ұрлау және т.б.

Көптеген мемлекеттер компьютерлердің көбеюіне басқа адамдарға және ұйымдарға зиян келтіру үшін арнайы қылмыстық заңдар қабылдау арқылы жауап беруге мәжбүр болды. Компьютерлік қылмысқа қарсы тұруға бағытталған әлемдегі алғашқы заң АҚШ-та 1984 жылы қабылданған заң болды.

Кеңес Одағының аумағында алғашқы ресми тіркелген компьютерлік қылмыс 1979 жылы Вильнюста компьютермен ақша ұрлау арқылы бөтеннің мүлкіне қарсы қылмыс болып табылады [82, 126 б.].

Біз ақпараттық және телекоммуникациялық желілер (технологиялар) кеңінен тараған ақпараттық қоғамда өмір сүреміз. Әлемдегі дербес компьютерлердің санын есепке алу мүмкін болмай отыр. Тек бір ғана Microsoft 2018 жылы Windiws бағдарламасын қолданушылар санын 10 миллиард құрылғыға жеткізуді жоспарлап отыр [83].

Интернетті пайдаланушылар саны қол жетімді смартфондардың пайда болуына және салыстырмалы төмен тарифтеріне байланысты жоғары жылдамдықты мобильді интернетті пайдалану қызметтері тез қарқынмен өсуде. Бүгінгі күні смартфон пайдаланушыларының саны 3,2 миллиардтан асты, бұл әлем халқының шамамен 41% құрайды [84]. Олардың көпшілігі әлеуметтік желілерді үнемі тұтынушылар болып отыр. Әлемде әр секунд сайын әлеуметтік желіні пайдаланушылар саны 11 адамға көбейіп келеді, ал планетадағы 7,6 миллиард адамның үштен екісі ұялы телефонға ие болады. Жалпы алғанда Қазақстанда Интернетті пайдалану жыл сайын артып келеді. 2019 жылдың жазында 2,5 миллион абонент болса, бір жылдың ішінде олардың саны 1,2 % өсті. Республикада телефондағы интернет желісін

қолданатын азаматтардың саны 15,1 млн абонентті құрады. Бұл өткен жылғы көрсеткіштерден (13,9 млн) 8,5% артық.

Интернет, әлеуметтік желілер, ақпараттық және телекоммуникациялық технологиялар қоғамның ажырамас бөлігіне айналды десек артық айтқандық емес болар еді.

Алайда компьютерлендіру процесінің жағымды да, жағымсыз да жақтары да бар екені бәрімізге мәлім. Ақпараттық және телекоммуникациялық желілерді қарапайым қолданушылар ғана емес, қылмыскерлер де пайдалануды тез қарқынмен үйрене бастады.

Қылмыстық-құқықтық әдебиеттерде «компьютерлік ақпарат саласындағы қылмыстар», «компьютерлік қылмыстар», «киберқылмыстар», «интернет-қылмыстар» «ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылық» және т.б. атаумен белгілі қылмыстық құқық бұзушылықтардың жаңа санаттары пайда бола бастады.

Компьютерлік ақпарат саласындағы қылмыстар - бұл Қазақстан Республикаының Қылмыстық кодексінің 7-тарауында көзделген қылмыстардың заңнамалық анықтамасы.

«Компьютерлік қылмыстар» түсінігі жан-жақты және оның нақты анықтамасы жоқ болып отыр. Оны мынадай жағдайларда қолдануға болады: 1) «компьютерлік ақпарат саласындағы қылмыстар» ұғымының синонимі ретінде; 2) ақпараттық-телекоммуникациялық салада жасалған қылмыстардың анықтамасы ретінде (ақпараттық қылмыстар); 3) компьютерлік жүйені немесе желіні, компьютерлік жүйені немесе желіні қолданып, компьютерлік жүйеге немесе желіге (киберқылмысқа) қарсы жасалуы мүмкін қылмыстардың анықтамасы ретінде.

Сөйтіп қылмыстық құқық доктринасында компьютерлік қылмыстарды мынадай жағдайларда қолдануға болады:

- компьютерлік ақпарат саласындағы қылмыстар ретінде;
- ақпараттық компьютерлік қылмыстар;
- киберқылмыстар (интернет қылмыстары).

Ақпараттық компьютерлік қылмыстар шеңбері ақпараттық және телекоммуникациялық (компьютерлік) технологияларды пайдалану кезінде жасалған қылмыстардан қалыптасады. Бұл санатқа компьютерлік ақпарат саласындағы қылмыстар, сондай-ақ ақпараттық және телекоммуникациялық желілерді пайдалану саласындағы басқа да қылмыстар жатады.

БҰҰ-ның X конгрессінің ұсынымдарына сәйкес киберқылмыстарға компьютер, ақпараттық және телекоммуникациялық технологиялар немесе желілер қылмыстың субъектісі, құралы немесе құралы болып табылатын барлық қылмыстар жатады [85].

Бұл қылмыстар тобына ақпараттық компьютерлік қылмыстардан басқа, компьютерлерді, ақпараттық және телекоммуникациялық технологияларды немесе желілерді пайдаланумен байланысты жаалатын қандай да бір басқа қылмыстар жатады. Мысалы, ақпараттық және телекоммуникациялық

технологияларды қолдану арқылы жасалған кісі өлтіру киберқылмыс болып табылады.

Сонымен бірге 1990 жылдардың басында құрылған автоматтандырылған ақпараттық-іздеу жүйесінің негізінде құралған Интерпол кодификаторы 30-дан астам қоғамдық қауіпті әрекеттерді топтарға бөледі:

QA - рұқсат етілмеген кіру және ұстап алу:

QAH – компьютерлік абордаж (рұқсатсыз кіру);

QAI - арнайы техникалық құралдарды қолдану арқылы ұстап алу;

QAT - уақытты ұрлау (ААЖ қолданғаны үшін төлемдерден жалтару);

QAZ - рұқсат етілмеген кірудің және ұстап алудың басқа түрлері.

QD - компьютерлік деректердің өзгеруі:

QDL - логикалық бомба;

QDT - трояндық ат;

QDV - компьютерлік вирус;

QDW - компьютерлік құрт;

QDZ - деректердің өзгеруінің басқа түрлері.

QF - компьютерлік алаяқтық:

QFC - банкоматтағы алаяқтық;

QFF - компьютерлік контрафактілік;

QFG - ойын автоматтарына қатысты алаяқтық;

QFM - енгізу-шығару бағдарламаларын манипуляциялау;

QFP - төлемдер бойынша алаяқтық;

QFT - телефондық алаяқтық;

QFZ - басқа компьютерлік алаяқтық.

QR - заңсыз көшіру:

QRG - компьютерлік ойындар;

QRS - басқа бағдарламалық жасақтама;

QRT - жартылай өткізгіш топологиясы;

QRZ - басқа заңсыз көшіру.

QS - компьютерлік диверсия:

QSH - аппараттық құралдармен (компьютердің ақаулығы);

QSS - бағдарламалық қамтамасыздандырумен (ақпаратты жою, бұғаттау);

QSZ - диверсияның басқа түрлері.

QZ - басқа компьютерлік қылмыстар:

QZB - компьютерлік хабарландыру тақталарын пайдалану;

QZE - коммерциялық құпияны құрайтын мәліметтерді ұрлау;

QZS - соттың қарауына жататын ақпаратты беру;

QZZ - басқа компьютерлік қылмыстар.

Жоғарыда аталған ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды саралауда кемшіліктердің бар екенін мойындау керек. Атап айтқанда, заңды және техникалық түсініктердің бірігіп кеткендігін байқауға болады. Алайда бұл қылмыстық заңнаманы одан әрі жетілдіруге жағдай жасайды.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың криминологиялық сипаттамасы

Криминологтардың айтуынша, ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар саны күн санап өсіп келеді. Алайда бұл әртүрлі себептерге байланысты ресми статистикада көрінбейді. Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар саласындағы қылмыстың толық көрінісі бізде жоқ деп біржақты пікір айтуға болады.

Қазақстанда 2019 жылы ақпараттық қауіпсіздікті бұзудың 21 мыңнан астам оқиғасы анықталды. Кибершабуылдардың ең көп таралғаны - ботнеттер (17,7 мың жағдай). Ботнет немесе зомби желісі - зиянкестермен зақымдалған компьютерлер желісі, бұл шабуылдаушыларға өз иелерінің білместен басқа адамдардың машиналарын қашықтықтан басқаруға мүмкіндік береді. Ботнеттер арқылы шабуылдаушылар спам жібере алады, вирустар тарата алады, компьютерлер мен серверлерге шабуыл жасай алады, сонымен қатар басқа да қылмыстар жасай алады. Одан кейін фишинг (883 оқиғамен) екінші орында тұр. Бұл компьютерлік алаяқтықтың басты мақсаты - жәбірленушіні шабуылдаушыға қажетті ақпаратты беру үшін алдау. Осындай ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар заңмен қудаланады және жауапкершілікке тартылады. Бүгінгі күні фишинг әлемдегі ең кең таралған киберқылмыс түрлерінің бірі болып табылады, олардың көмегімен шоттар мен банктік ақпарат жиі ұрланады.

Бүкіл әлемде хакерлік шабуылдар 2019 жылы әр 14 секунд сайын жасалған болса, Cybersecurity Ventures компаниясы 2021 жылға қарай олардың жиілігі әр 11 секундқа дейін өседі деп болжайды. Сонымен қатар әлемдік киберқылмыстардың зияны 2021 жылға қарай 6 триллион долларға жетеді деп болжануда [86].

Касперский зертханасы әлемде жылына 70 мыңнан астам зиянды бағдарламалар пайда болатынын жазады. Мемлекетте зиянды компьютерлік бағдарламалардан зардап шекпеген бірде-бір қолданушы жоқ екені белгілі. Бұл нені білдіреді? Компьютерлік ақпарат саласындағы қылмыстар іс жүзінде ресми статистикада көрініс таппайтындығында. Мұның бірнеше себептері бар.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар саласындағы қылмыстарға қарсы тұру үшін оның себептері мен қылмыстарды жасауға қолайлы жағдайларды нақты анықтап алу қажет.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтың себептері мен шарттары туралы мәселе әлемдік және отандық ғылымда ең күрделі және шешімін таппаған мәселелердің бірі болып табылады. Алайда бұл криминологияның

орталық мәселесіне жатады. Криминология ғылымы қылмыстың алдын алу мақсатында оған зерттеу жүргізетіні белгілі.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар, бір жағынан, жалпы қылмыстарға тән себептер мен жағдайлардан туындайды. Екінші жағынан, оның сипаттамаларына байланысты себептері мен шарттарының өзіндік ерекшеліктері болады.

Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың себептері мен жағдайларына қысқаша тоқтала кетейік. Криминологияда қылмыстың себептері деп қылмысты тудыратын жағдайлар түсініледі. Ал жағдайлары деп қылмысқа әкелетін шарттарды айтады. Олардың арасындағы айырмашылыққа тоқталатын болсақ, себептер қылмысты тікелей тудырады, ал жағдай - бұл қылмыстың көрініс беруі мүмкін жағдайлар. Олар қылмыстың пайда болуына және көрінуіне ықпал етеді. Дәл осы себептер мен жағдайлардың өзара әрекеттесуі салдарынан қылмыстың пайда болуына әкеп соқтырады. Қажетті жағдайлар болмаған кезде себеп өздігінен пайда болмайды. Кейде себептер мен жағдайлар бірігіп көрініс беруін қылмыстың факторлары деп те атайды.

Арнайы әдебиеттерді талдау көрсеткендей, қазіргі кезде криминологияда қылмыстың алдын алу саласында тәжірибе қажеттіліктерін қанағаттандыратын тұжырымдама жоқтың қасы.

Адамның мінез-құлқының себептеріне сыртқы жағдайлар, әлеуметтік орта, тұлғаның психологиялық немесе биологиялық ерекшеліктері жататынын анықтау қажет.

Біздің көзқарасымыз бойынша, қылмыстың себептерін жеке қылмыстық мінез-құлық себептерінен іздеу керек.

Н.Ф.Кузнецова теорияда және тәжірибеде нақты қылмыстардың детерминанттары туралы статистикалық жалпыланған мәліметтер жалпы қылмыстың себептері мен жағдайларын сипаттау үшін пайдаланылатындығына ерекше көңіл бөледі [87, 787 б.].

Біздің ойымызша, қылмыстың себептері мен жеке қылмыстардың себептерін қарсы қою мүмкін емес. әрбір қылмыстың жекелеген себептері болады. Қылмыстың себептері мен жеке қылмыстардың себептерін бір-бірінен бөлуге болмайды.

Сонымен, жеке қылмыстың себебіне адамның психологиялық, моральдық, діни, дүниетанымдық және басқа құндылықтары мен қатынастарына негізделген ерік білдіру жатады.

Көптеген ғылыми зерттеулер қылмыс пен қылмыстың басты себебі ретінде адам санасының қасиеттері туралы ойды растайды. Көптеген жағдайда қылмыстар адамның эгоистік мотивтеріне байланысты жасалады. Қасақана жасалған қылмыстардың мотивтеріне негізінен жеке бастың мүддесі, ашкөздік, билікке ұмтылу, нәпсіқұмарлықты қанағаттандыруға ұмтылу, кек алу, арсыздық және адам табиғатының басқа да негізгі көріністері болып табылады.

Қылмыстылықтың жағдайларына адамның өмірімен байланысты сыртқы жағдайлар жатады. Біз ондай сыртқы жағдайларға туралы айтатын болсақ, олар өздігінен қылмыс туғызбайды, бірақ онсыз қылмыс жасалмас еді. Мысалы, электрондық құрылғылар мен Интернеттің болуы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жасауға қолайлы жағдай туғызады. Алайда, гаджеттер мен әлемдік желілердің болуы фактісі бұл қылмыстардың жасалуына себеп бола алмайды.

Қолда бар ғылыми әдебиеттерге талдау жасау ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың детерминанттарына арналған арнайы монографиялық зерттеулер жоқ екенін көрсетті. Киберқылмыстың себептері мен жағдайлары туралы мәселе басқа мәселелермен қатар жиі қарастырылады. Сонымен ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасауға ықпал ететін жағдайларға мыналарды жатқызамыз:

- елімізде қолданыстағы компьютерлер санының артуы және соның әсерінен оларды пайдаланушылар санының өсуі, компьютерлерде сақталатын ақпараттың көбеюі;

- компьютерлерді және олардың жүйелерін қорғаудың жеткіліксіз шаралары, сондай-ақ басшылықтың ақпараттық қауіпсіздік пен ақпаратты қорғауды қамтамасыз ету мәселелеріне әрқашан бей-жай қарауы;

- бағдарламалардың қажетті деңгейде қорғалмауы;

- компьютерлік техниканы қорғаудың техникалық құралдарының жеткіліксіз қорғалуы;

- ақпаратмен алмасу, келісімшарттар жасау, төлемдер жасау және т.б. бойынша компьютерді қолданушылардың әлемдік ақпараттық желілерге ену мүмкіндігі;

- заманауи техникалық құралдарды қылмыстық әрекетте қолдану;

- электрондық пошта құралдарының жеткіліксіз қорғалуы;

- компьютер пайдаланушыларының жұмыстыры немқұрайлылықпен қарауы;

- жұмысқа алу және шығару мәселелері бойынша ойластырылмаған кадр саясаты;

- компьютерлік қылмыстардың алдын алуға, ашуға және тергеуге міндетті ішкі істер органдарының, оның ішінде ішкі істер органдарының лауазымды адамдарының арнайы даярлығының төмен деңгейі;

- ақпараттық қауіпсіздік саласындағы мемлекеттік және қоғамдық құрылымдардың жұмысындағы үйлесімділіктің болмауы;

- елімізге электрондық тыңшылықтан қорғалған компьютерлер мен желілік жабдықтарды әкелуге шектеулер.

А.Л. Осипенко ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың детерминанттарына мыналарды жатқызады:

- ашық ғаламдық желілердің технологиялық қорғалмағандығы;

- заманауи желілер инфрақұрылымының күрделілігі мен өзгергіштігі;
- қолданылатын бағдарламалардың жоғары деңгейі осалдығы;
- желіде жұмыс істеген кезде анонимді мүмкіндіктердің кең мүмкіндігі (оның ішінде заңсыз) [88, 135 б.].

Біздің зерттеу нәтижелері көрсеткендей, қазіргі уақытта жасалған қылмыстарға, оның ішінде ақпараттық және телекоммуникациялық желілерді пайдалану арқылы (Интернетті қоса) жасалған қылмыстарға қылмыстық-құқықтық ескерту жұмыстары өте төмен деңгейде жүзеге асырылып жатыр. Бұл жағдай күрестің бірыңғай тұжырымдамалық жүйесінің болмауына байланысты.

Компьютерлік қылмысқа қарсы күрес мемлекеттің, қоғамның және жекелеген қолданушылардың ақпараттық саладағы заңсыз мінез-құлықты факторлары бойынша өзара іс-қимылына негізделген. Мұндай мақсатты әсер етуді жүзеге асыру әр түрлі құқық салаларының әдістері мен құралдарын біріктіру арқылы мүмкін болады. Қылмыстық циклдің мүмкіндіктері (қылмыстық, қылмыстық іс жүргізу, қылмыстық-атқару заңнамасы) азаматтық құқықтың нормаларымен үйлесуі керек. Адамзат қылмыстық қуғын-сүргін құралдарының алуан түрін қолданып көрді, ал қазір ғалымдар «жазалау дағдарысы» мен бүкіл қылмыстық сот жүйесінің дағдарысы туралы көбірек айтады.

Тиісті нормативтік-құқықтық базасыз компьютерлік қылмысқа қарсы іс-қимылдың (негізгі заң және осы саладағы басқа заңдар мен ережелерді жүйелеу) тиімді болуы мүмкін емес.

Заңмен реттелетін қоғамдық қатынастардың сипатымен функционалды түрде алдын-ала анықталған құралдар мен әдістерге байланысты қылмысқа қарсы екі түрге бөлуге болатын құқықтық бақылау орнату арқылы қарсы тұруға болады: позитивті және репрессивті.

Қылмысқа позитивті құқықтық бақылау салалық тәртіпте тиісті құқықтық қатынастарды реттейтін құқықтық нормалардың жиынтығын қамтиды. Позитивті құқықтық бақылаудың тиімділік дәрежесі позитивті қоғамдық қатынастарды құқықтық реттеу механизмінің тереңдігі мен айқындылығына, заңдық нұсқамалардың негізділігіне, олардың қоғамдық пайдалылығы мен заңды мағынадағы тиімділігіне тікелей байланысты.

Бұл критерийлер компьютерлік қылмыстарды оң бақылауға қатысты қолданыстағы заңдылық жағдайын талдауға мүмкіндік береді. Осы тұрғыдан алғанда, бақылау тиісті құқық салаларында ақпараттық қатынастарды реттейтін және ақпараттық ресурстардың жұмыс істеу тәртібін белгілейтін, сондай-ақ қылмыстық өнімді әкетпейтін мақсаттар үшін ақпараттық өнімді пайдалану шарттарын белгілейтін құқықтық нормаларда көрінеді.

Әңгіме коммерциялық ортаға, компьютерлердің, компьютерлік жүйелердің немесе олардың желілерінің жалпы пайдаланушысына бағытталған ашық ақпаратты қорғау туралы болып отыр. Позитивті құқықтық бақылау арқылы қорғау конституциялық, халықаралық,

ақпараттық, азаматтық және әкімшілік құқық нормалары арқылы жүзеге асырылады.

Киберқылмыс - бұл жаһандық жауапкершілікті қажет ететін «жаңа» қылмыс түрі. Соңғы онжылдықтар ішінде есірткінің заңсыз айналымы және трансұлттық ұйымдасқан қылмыс сияқты проблемала халықаралық келісімдерді әзірлеу арқылы шешу қажеттігі туындады. Сонымен қатар, бүгінде киберқылмыс халықаралық ынтымақтастық үшін бірегей қиындықтар тудыратындығына ешкім күмән келтірмейді.

Компьютерлік технологияларды қолдана отырып жасалатын құқық бұзушылықтар әртүрлі мемлекеттердің заңнамасында және ғылым мен құқықтық құрылымдар үшін халықаралық деңгейде құқықтық кеңістікті біріздендіру проблемасын тудырады.

Бұл бағыттағы жұмыс мемлекетаралық және аймақтық құқықтық реттеу деңгейлерінде жүзеге асырылуда. Халықаралық шарттарға қатысушы-мемлекеттердің қол қоюының арқасында компьютерлік технологияларды қолдану арқылы мемлекеттердің қылмысқа қарсы күрес саласындағы халықаралық ынтымақтастық ережелері үшін юрисдикцияның бірыңғай негізі құрылды.

Киберқылмыс проблемасы Қазақстан Республикасында ерекше өзектілікке ие болуда. Мысалы, Қазақстан Республикасының Қылмыстық кодексінде компьютерлік ақпарат саласындағы қылмыстардың теориялық және оларды қолдану практикасында да айтарлықтай қайшылықтар пайда болды, яғни: кейбір қылмыстық-құқықтық терминдерді теориялық және практикалық түсіндірудегі қателіктер, құқық қорғау органдарының қоғамдық қатынастарды қорғаудағы зерттелген нормалардың мәні мен рөлі туралы қате түсініктері жатады. Сонымен қатар, әлі күнге дейін техникалық артта қалушылық және компьютерлік қылмыстармен жұмыс жасау кезінде құқық қорғау органдарының қызметкерлерінің психологиялық қорқынышы басым болып отыр.

Көрсетілген себептерге байланысты тергеушілер, прокурорлар мен соттардың қылмыстық істі тергеу, саралау және жаза тағайындау туралы шешімдер қабылдаудағы қателіктердің таралуы да байқалады. Сот-медициналық практикада компьютерлік ақпараттармен заңсыз әрекеттерді қылмыс әдісі ретінде компьютерлік құралдарды қолданып жасалған басқа қылмыстардан ажырату кезінде қателіктер жіберіледі. Құқық бұзушылыққа дұрыс емес баға берілуі жиі кездеседі, компьютерлік қылмыстың орнына ол қылмыстық заңның басқа баптары бойынша сараланууы, ал компьютерлік алаяқтыққа кінәлі адамдар қауіпті қылмыс жасағаны үшін жауапкершіліктен құтылып кетулері көп кездеседі. Ғылыми негізделген әдістердің жоқтығы, компьютерлік қылмыстармен күресудің әзірленген тактикасының болмауы, құқық қорғау органдарының осы қылмыстарды анықтау, алдын алу, жолын кесу және ашу бойынша қабылдаған шараларын тиімсіз етеді.

Қылмыстық іс жүргізу әрекеттерін реттейтін заңнамалық актілердің болмауымен және қажетті техникалық құралдардың жоқтығы, арнайы оқытылған адамдардың болмауына (ақпараттық-телекоммуникация саласындағы қылмыстарды анықтауға және ашуға мамандандырылған жедел-тергеу аппараты) байланысты, біздің алдымызда киберқылмыстардың техникалық және құқықтық мәселелеріне тап болдық.

Қазіргі кезеңде киберқылмыстардың өсу тенденциясы байқалады. Қылмыстық қол сұғушылықтың осы түріне қарсы күрестегі халықаралық ынтымақтастық құқықтық, ұйымдастырушылық, ғылыми және қаржылық қолдауды қажет етеді және осы факторлардың жиынтығын ескере отырып, халықаралық қауымдастық киберқылмыс проблемаларының барлық спектрін шұғыл шешуі керек.

Кибер кеңістігінде жасалған қылмыстар саны компьютерлік желілерді пайдаланушылар санына пропорционалды түрде өсуде және Интерполдың талдауы бойынша, ғаламдық Интернеттегі қылмыстың өсу қарқыны әлемдегі ең жылдам болып отыр. Мысалы, Naskeg-watch.org порталының мәліметтері бойынша әлемде апта сайын 55 миллионнан астам компьютерлік хакерлердің акциясы тіркеледі.

Компьютерлік вирустар мен Интернеттегі алаяқтықтар жыл сайын миллиондаған Интернет қолданушыларына әсер етеді, олардың жүйелерін қалпына келтіру және қалпына келтіру үшін жүздеген, тіпті мыңдаған долларлар кетеді. Американдық тұтынушыларды зерттеу ұйымы жүргізген сауалнамаларға сәйкес, соңғы екі жылда интернет пайдаланушылардың төртіншісінің компьютері вирус жұқтырған. Пайдаланушылардың 16% маңызды деректерді жоғалтады, ал 8% техникалық құралдарды өзгертеді [4, 126 б.]. Карнеги Меллон Университетінің компьютерлік авариялық-құтқару тобының компьютерлік қауіпсіздік бойынша сарапшылар тобы компьютерлік қауіпсіздік жүйелеріндегі жаңа проблема әр 82 минут сайын анықталады деп есептеді.

Киберқылмыс проблемасының ерекшелігі мынада: жеке мемлекет оған өзінің мемлекеттік билік механизмімен қарсы тұра алмайды, тек ынтымақтастық арқылы ғана халықаралық қауымдастық трансұлттық қауіптің осы факторына қарсы тұра алады.

Бұл сондай-ақ қоғамның қазіргі даму кезеңінде мемлекеттің ақпараттық ресурстарының басқа маңызды ресурстармен - табиғи, қиын, қаржылық және оның әлеуетін құрайтын басқа ресурстармен бір деңгейде болуымен байланысты. Ақпарат - қылмыстық қауымдастық өзінің шабуылына бағыттауға қабілетті мүлік, тауар ретінде қарастырылады.

Сонымен қатар, белгілі бір қоғамдық қауіпті құбылыстарды жасаудың басқа тәсілдерімен қатар, ақпараттық-коммуникациялық желілердің жоғары жылдамдығы, жасырын болуы, ауқымдылығы, трансұлттық сияқты әрекеттері қылмыскерлер үшін ең тартымды болып отыр.

Киберқылмыстың бүкіл әлем үшін де, Ресей Федерациясы мен Қазақстан Республикасы үшін де қауіптілігін құқық қорғау органдары мойындайды.

Сонымен, Ресейдің Ішкі істер министрлігі Арнайы техникалық шаралар бас басқармасының, сондай-ақ Қазақстан Республикасының Ақпараттық қауіпсіздік комитетінің соңғы мәліметтері бойынша, қазіргі кезде киберқылмыс (жоғары технологиялық қылмыс) ақпарат саласындағы Ресей мен Қазақстанның ұлттық қауіпсіздігіне ең үлкен қауіп-қатер алып келуде.

Киберқылмысқа қарсы күресте халықаралық ынтымақтастықтың қажеттілігі туралы көп айтылғаны соншалық, оны қайталаудың қажеті жоқ. Виртуалды кеңістіктегі шекаралардың болмауы, жасырындық, процестердің жоғары жылдамдығы - бұл факторлар кез-келген тергеуді айтарлықтай қиындатады. Бірақ олар ынтымақтастықты ынталандырады.

Кезінде ресейлік сарапшылар британдық әріптестерімен бірлесіп, Ұлыбританиядағы банктер мен букмекерлік компаниялардың серверлеріне DDOS шабуылдарын жасаған, содан кейін әр түрлі электрондық төлем жүйелерін қолдана отырып ірі ақша алып жатқан адамдар тобының бірлескен тергеуі мен ұсталуы туралы айтқан болатын. 2006 жылдың қазанында сот ұйымдасқан қылмыстық топ мүшелеріне 8 жыл бас бостандығынан айыру және ірі көлемде айыппұл түріндегі жаза белгіледі [90, 84 б.].

Шетелдік серіктестермен тәжірибе алмасу, ақпарат алмасу және бірлескен жұмыс туралы көптеген келісімдер бар. Мысалы, «Қазақстанның киберқалқаны» Тұжырымдамасын іске асыру шеңберінде жас IT-мамандар даярлайтын киберқауіпсіздік академиясын ашу жоспарлануда. Қазіргі уақытта академияны құрудың ұйымдастырушылық-құқықтық мәселелері зерттелуде. Осы жұмысқа түрік, израиль және ресей сияқты мықты компаниялар қатысады. Бұл академия мемлекеттік-жекеменшік серіктестік негізінде жұмыс жасауды жоспарлап отыр. Сонымен, 2018 жылы Транстелекоммен бірге Ұлттық Киберқауіпсіздік орталығы құрылды [91, 125 б.]. Оның басты мақсаты - стратегиялық маңызы бар нысандардың киберқауіпсіздігін қамтамасыз ету. Қазіргі уақытта мемлекеттік органдар мен квазимемлекеттік сектордың ақпараттық қауіпсіздігін қамтамасыз ету үшін нормативтік-құқықтық база құрылды.

Соңғы онжылдықта киберқылмысқа қарсы бағытталған халықаралық және аймақтық құжаттарды қабылдау бойынша айтарлықтай белсенділік байқалды. Олар міндетті және қосымша құжаттарды қамтиды. Жасалған құжаттарды қамтитын бес топты ажыратуға болады:

1. Еуропа Кеңесі немесе Еуропалық Одақ
2. Тәуелсіз Мемлекеттер Достастығы немесе Шанхай ынтымақтастық ұйымы
3. Африка үкіметаралық ұйымдары
4. Араб мемлекеттерінің лигасы
5. Біріккен Ұлттар Ұйымы.

Осы құжаттардың барлығы бір-бірін едәуір толықтырады, соның ішінде Еуропалық Кеңестің киберқылмыс туралы конвенциясында жасалған тұжырымдамалар мен тәсілдерге қатысты.

Әлемде 82 мемлекет міндетті киберқылмыс заңнамасына қол қойды және ратификациялады. Киберқылмыс бойынша көпжақты құралдар оларға ресми қатысуды және олардың орындалуын, жүзеге асырылуын қамтамасыз етіп қана қоймайды, сонымен бірге ұлттық заңнамаға жанама әсер етеді.

Киберқылмыс туралы көпжақты құжатқа қол қою ұлттық қылмыстық және процессуалдық заңнаманың жеткіліктілікті деңгейде екендігін көрсетеді, бұл осы салалардағы ережелері, әдетте, тиімді болып саналады. 40-тан астам есеп беруші ел Еуропа Кеңесінің киберқылмыс туралы конвенциясын киберқылмысқа қарсы іс-қимыл саласындағы заңнама ең көп қолданылатын көпжақты құрал деп санайды.

Осылайша, Еуропалық Кеңестің 2001 жылдың 23 қарашада Будапешт қаласында «Компьютерлік ақпарат саласындағы қылмыс туралы» атты конвенция компьютерлік қылмысқа қарсы күрестегі халықаралық ынтымақтастықты дамытуда маңызды рөл атқарды. Бұл құжат осы тақырыппен әлі байланысқа түспеген көптеген елдерге проблеманы түсінуге және заман талабына қарай шешуші қадамдар жасауға мүмкіндік берді.

«Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің компьютерлік ақпарат саласындағы қылмысқа қарсы күрестегі ынтымақтастығы туралы келісімді бекіту туралы» Қазақстан Республикасы Президентінің 2002 жылғы 25 маусымдағы N 897 Жарлығымен бекітілді.

Осы күнге дейін Ресей Конвенцияға қол қойған жоқ. Оған негізгі болып Конвенцияның 32-бабынан бас тарту табылады, яғни оның түсініксіз тұжырымдамасы басқа мемлекеттің ақпараттық желілеріне біреудің жеке рұқсаттарына сүйене отырып, оның хабарламасынсыз енуге мүмкіндік береді.

Сонымен бірге көптеген ғалымдардың тәжірибелеріне сүйене отырып айта аламыз: компьютерлік қылмысты заманауи тергеу дегеніміз - бұл жедел әрекет ету бөлімшелері мен мемлекеттік және мемлекеттік емес секторлардың әртүрлі құрылымдарының өзара байланысты шаралар кешені. Ал тергеу телекоммуникация желілерінің виртуалды кеңістігінде емес, белгілі бір елдің аумағында жүргізіледі.

Сондықтан 32-бапта мүлдем басқа мақсаттар тұрғандығы анық, ал компьютерлік қылмыстарды тергеу мақсаттары тұрмағаны анық. Сонымен бірге, бұл әлемде қабылданған егемендік пен адам құқығын құрметтеу нормаларына қайшы келеді. Көптеген ғалымдар Конвенция мәтінін қазіргі заманға және тәжірибеге сәйкес, мәселені орынынан жылжытатын түзетулер енгізуді ұсынады.

Конвенция нақты қылмыстық істер бойынша өзара ынтымақтастықты құру әдістерін толықтай қамтамасыз ете алатын және заңды тұрғыдан негіздейтін бірқатар ережелерді қамтиды. Бірнеше фактор өте маңызды: шетелдік серіктестен сұрау салуды қабылдау, мұндай сұрау салуды қабылдаған тараптың жедел немесе тергеу шараларын жүзеге асыруы,

нәтижені бастамашыға беру немесе алынған ақпаратты бірлесіп жүзеге асыру.

Еуропалық Кеңестің компьютерлік ақпарат саласындағы қылмыс туралы конвенциясы біздің елдің қылмыстық заңнамасында іс жүзінде енгізілген деген қорытынды жасауға болады. Еліміздің ұлттық заңнамасында 2001 жылы қабылданған конвенцияның құқықтық мәртебесін заңды түрде шоғырландырудан бас тарту, қазіргі кезде цифрлық кеңістіктің жедел қарқынмен дамып келе жатқандығы және жаңа технологиялардың енгізілуі өзектілігін тоқтатады.

Өзінің даму кезеңінде (1997-2001 жж.) ақпараттық қауіпсіздік саласындағы көптеген қауіп-қатерлер жаңаша сипатқа ие болды. Оның ішінде кейбір қылмыстық құқық бұзушылықтардың белгілері де болған жоқ немесе тиісті мән берілмеді. Ақпараттық технологиялар саласында қылмыстың жаңа түрлері пайда бола бастады, атап айтқанда, киберқылмыскерлердің «ботнеттер» деп аталатын түрлерін - зиянды бағдарламалармен зарарланған компьютерлер желісін қолдануы, бұл әр түрлі заңсыз әрекеттерді қашықтықтан жасауға мүмкіндік береді.

Бүгінгі таңда бізге ақпарат саласындағы қылмысқа қарсы күресте егемендікке және компьютерлік технологиялар арқылы мемлекеттердің ішкі істеріне араласпауға кепілдік беретін дүниежүзін қамтитын құжат қажет. Бұл құжат осы жас, бірақ онсыз да өте қауіпті құбылысқа халықаралық, аймақтық және ұлттық құқықтық реттеудің үш деңгейінде тиімді қарсы тұруға мүмкіндік береді.

XXI ғасыр жаһандану және ақпараттандыру ғасырымен белгіленді. Интернет адам іс-әрекетінің барлық салаларына еніп кетті, атап айтқанда медицина, көлік, білім беру, өндіріс, банк және т.б. Ақпараттық технологияларды қолдану осы саладағы қылмыстармен байланысты тәуекелдер мен қатерлерге ұшырайды.

Әрине, Қазақстан қазірдің өзінде жауап беруді қажет ететін қиындықтарға тап болды. Құқық қорғау органдарының мәліметтері бойынша, Қазақстанда киберқылмыс саны жыл сайын артып келеді. Азаматтардың жеке деректері, мемлекеттік органдардың құпия деректері, ұялы байланыс, банктік шоттар туралы мәліметтер және т.б. қылмыскерлердің назар аударатын объектісіне айналды.

Бағдарламалау тілін түсіну барлық азаматтар үшін қиындық туғызады. Басқа біреудің жүйесіне басып кіру мүмкіндігінің арқасында қылмыскерлер елдің ұлттық қауіпсіздігіне орасан зор зиян келтіруі мүмкін. Интернеттің мемлекетаралық шекарасы жоқ, көбіне қылмыскерлер жүздеген шақырым жерде болуы мүмкін және басқа мемлекетте тұрады. Бұл қылмыскерлерді тергеу және ұстау процесін қиындатады.

Мысалы, Алматыда «Интернет-банкинг» электрондық жүйесін қолданып кәсіпкерлердің есепшоттарынан ақша ұрлаумен айналысқан қылмыстық топ анықталды. Тергеу анықтағандай, қылмыскерлер Бас прокуратураның атынан ғана емес, сонымен қатар Салық комитетінен, Қаржы министрлігінен, Қазақстан Республикасы Қаржы министрлігінің

Мемлекеттік кірістер комитетінен және түрлі қызметтерден хаттар жіберген. Кәсіпкерлер зиянды бағдарламаны іске қосқаннан кейін оның белсенділігі іске қосылады. Содан кейін вирус жұққан компьютерлерге және құпия ақпаратқа қашықтан қол жеткізе отырып, қылмыскерлер екінші деңгейлі банктерде бұрын ашылған шоттарға ақша аударды.

Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ішкі заңнаманы және мемлекетаралық ынтымақтастықты жетілдіру қажеттігі туындап отыр. Халықаралық құқық қағидаттарына сәйкес осы саладағы халықаралық ынтымақтастықты одан әрі жетілдіру қажет.

Біздің елде кибер қорғанысты ұйымдастыру үшін бірқатар құрылымдар құрылды, мысалы, Ішкі істер министрлігі Криминалдық полиция комитетінің «К» бөлімі, ҰҚК-де осындай мамандандырылған бөлім, Министрліктің мемлекеттік техникалық қызметі Ақпараттық және коммуникациялар, мемлекеттің ақпараттық қауіпсіздігін қамтамасыз етуге арналған органдар құрылды. Олар заңнаманы жетілдірумен, техникалық құралдарды зерделеумен және сертификаттаумен, мемлекеттік органдардың жүйелерін ақпараттық қорғаумен, қылмыстар мен анықталған кибершабуылдарды тергеумен, сондай-ақ олардың жолын кесу шараларын қабылдаумен айналысады.

Ақпараттандыру саласындағы қатынастарды реттеудің негіздері 2016 жылдың 1 қаңтарында күшіне енген «Ақпараттандыру туралы» Заңда қарастырылған. Осы заң ақпараттандыру объектілерін құру, дамыту және пайдалану кезінде, сондай-ақ ақпаратты дамытуды мемлекеттік қолдау кезінде Қазақстан Республикасының аумағында мемлекеттік органдар, жеке және заңды тұлғалар арасында туындайтын ақпараттандыру саласындағы қоғамдық қатынастарды реттейді.

Әрине, ақпараттық саланы реттейтін қазақстандық заңнамалар өзінің дамуының бастапқы кезеңін өткеруде. Азаматтық және қылмыстық заңнамада инновациялар қажет, өйткені қазіргі кезде бұл құқық салалары киберқылмыскерлер тудыратын қылмыстар мен қауіп-қатерлердің тізімін қарастырмайды. Отандық заң ғылымында бұл бағытта ғалымдардың зерттеулері бұрыннан бар, дегенмен ғылыми база әлі де дамып келеді және негізінен шетелдік ғалымдардың еңбектеріне негізделген.

Өткен жылы Қазақстанда ақпараттандыру туралы заңнамаға түзетулер қабылданды. Заңда отандық Интернетті пайдаланушыларға арналған қауіпсіздік сертификаты туралы норма қабылданды, оған сәйкес шетелдік интернет-ресурсқа ақпаратты шифрланған жіберу хаттамаларын қолдана отырып кірген уақытта кез-келген азамат қазақстандық қауіпсіздік сертификатын өз компьютерлеріне орнатқаннан кейін ғана қол жеткізе алады. Тиісінше, барлық байланыс операторлары шифрлауды қолдайтын протоколдарды қолдана отырып, халықаралық трафиктен осындай қауіпсіздік сертификатын қолданумен ғана өтуі керек болады.

Республика біздің ел мен Еуропалық Одақ және оған мүше мемлекеттер арасындағы кеңейтілген серіктестік пен ынтымақтастық туралы келісімді ратификациялады, онда тараптар ынтымақтастықты, оның ішінде

қарым-қатынасты пайдаланып жасалған қылмыстық әрекеттердің алдын алу және күресу мақсатындағы ынтымақтастығы, оның ішінде озық тәжірибелермен алмасу арқылы нығайтады делінген.

Қазіргі қолданыстағы Қазақстан Республикасының Қылмыстық кодексінде «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» деген тарау киберқылмыстарға арналған, ол осы саладағы құқықтық қатынастарды реттейтін және қылмыстық жауапкершілікті қарастыратын 9 баптан тұрады. Біздің ойымызша, қазіргі заманғы киберқылмыстар мәселесіне неғұрлым егжей-тегжейлі қарау керек және олар қарапайым ұсақ бұзушылықтардан бастап жаһандық шабуылдарға дейін көрініс беретін алуан түрлі қылмыстар көбейіп келеді.

Киберқылмысқа қарсы тұру үшін келесі шараларды қарастыру қажет: ұлттық ақпараттық кеңістікті қорғауды қамтамасыз ету жүйесі үшін қауіп-қатерлерді азайту, заңсыз ақпараттың таралуын болдырмау, қазақстандық пайдаланушыларды деструктивті және технологиялық әсерден қорғау; заңсыз интернет-ресурстарын және телекоммуникация желілерін байланыс операторларының заңсыз мақсаттары үшін пайдалануға бақылауды күшейту, телекоммуникация желілерін орталықтандырылған басқару жүйесін жетілдіру; кіріс ақпараттық ағындарды басқару процесін реттеу.

Жалпы алғанда меншікті ақпараттық кеңістікті қорғау, ықтимал қауіп-қатерлерді жоюға бағытталған әрекеттерді бағалау және дамыту кез-келген мемлекеттің бірінші кезектегі міндеті болып табылатындығын атап өткіміз келеді, өйткені ақпарат көбірек қоғамдық қатынастарға әсер етеді.

Қорытынды

Айта кететін жайт, ақпараттық-телекомуникациялық технологияларды пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың саны қоғамның ақпараттануына байланысты жыл сайын өсіп келеді. Біздің ойымызша, болашақта медицина немесе білім беру саласындағы ақпараттық-телекоммуникациялық технологияларды пайдалану арқылы жасалатын құқық бұзушылықтарды қарастыруымыз мүмкін.

Қарастырылып отырған саладағы заңнаманы зерттей келе, біз «ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстарға» ақпараттық-телекоммуникациялық желілерді пайдалану арқылы заңмен қорғалатын ақпаратқа қауіп төндіретін қоғамға аса қауіпті қоғамдық әрекет деген тұжырымға келдік.

Осы тармақшаны қорытындылай келе мынадай тұжырымдама жасаймыз:

- «Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар» түсінігіне ақпараттық-телекоммуникациялық желілерді пайдалану арқылы заңмен қорғалатын ақпаратпен байланысты қоғамдық қатынастарға (адамның жеке құқығына, қоғамның және мемлекеттің өміріне) залал келтіретін қоғамға қауіпті әрекет болып табылады;

- Ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтар жүргізілген зерттеулердің нәтижесінде келесідей түрлерге бөлуге болады:

1) «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар», яғни қылмыстық кодекстегі 205-213 баптар, олар компьютерлік ақпарат саласындағы қоғамдық қатынастардың қорғалуына бағытталған;

2) «желілік құқық бұзушылықтар», яғни ақпараттық-телекоммуникациялық желілер бұл саладағы қылмыстық құқық бұзушылықты жасаудың құралы болып табылады (Қылмыстық кодекстің 128, 148, 190, 198, 217, 218, 219, 232 баптар).

Ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін жауапкершілікті реттейтін шетелдік мемлекеттердің және қазақстандық заңнамаға салыстырмалы-құқықтық талдау жасай отырып, мынадай қорытындыларға келеміз.

Біріншіден ағылшын-американдық, скандинавтік, романо-герман және социалистік құқықтық отбасылардың қылмыстық-құқықтық жүйелерінде ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар үшін заңнамалық актілерде (қылмыстық кодекстер немесе арнаулы заңдарда) қылмыстық жауапкершілікті нығайтуға жалпы тенденция байқалады.

Екіншіден, шетелдік қылмыстық заңнамалардың Қазақстан Республикасы Қылмыстық кодексінен айырмашылығы, ақпараттық-

телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар басқа қылмыс құрамдарында саралау белгісі ретінде немесе басқа қылмыстық әрекетті жасау тәсілі ретінде болуы мүмкін (мысалы, 9-бап 4-тарауы, 1-бап 9-тарауы Швеция ҚК; §206, §317, §263а ГФР ҚК; 226-18, 226-19 – баптары Франция ҚК).

Үшіншіден, қазақстандық заңнама заңдық техника тәртібі тұрғысынан ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар Қылмыстық кодекстің (7 тарау «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар») бір тарауына біріктірілген. Ал шетелдік қылмыстық заңнамада бұл қылмыстардың құрамы қылмыстық кодекстердің әртүрлі бөлімдерінде, тарауларында, бөлімшелерінде (кіші бөлімдерінде) немесе заңдар орналастырылған (Швеция ҚК, Дания ҚК, ГФР ҚК, Франция ҚК, ҚХР ҚК, Ұлыбритания қылмыстық заңнамасы).

Төртіншіден, қазақстандық қылмыстық кодексте ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтың субъектісі ретінде тек жеке тұлға танылады. Өз кезегінде скандинавтік және роман-германдық құқықтық отбасыларындағы қылмыстық заңнамада кінәлі ретінде заңды тұлғада бола алады (Швеция ҚК, Дания ҚК, Франция ҚК және т.б.).

Бесіншіден, біздің еліміздің қылмыстық заңнамасы бойынша ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасағаны үшін қылмыстық жауаптылыққа 16 жасқа толған жеке тұлға тартылады. Ал шет мемлекеттердің қылмыстық заңнамасы бойынша Латвия ҚК (11-бап) – 14 жастан бастап, Дания ҚК (§15) - 15 жастан бастап, ҚХР ҚК (17 – бап) - 14-тен 16-ы жастан бастап қылмыстық жауаптылыққа тартылады.

Жоғарыдағы айтылғандарды талдай келе, автор ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстар саласындағы жеке тұлғаларды қылмыстық жауаптылыққа тарту жасын, егер аса ауыр зардаптарға әкеліп соғатын болса, 16 жастан 14 жасқа дейін төмендетуді ұсынады. Өйткені ақпараттық-телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстарды жасайтын қылмыскерлер өз әрекеттері арқылы өте ауыр экономикалық зартаптарға әкеледі. Сонымен қатар он төрт жасқа толған жасөспірім қоғам мен ұжым алдындағы жауапкершілігін сезіне алатын, өзінің ойлау қабілетіне баға бере алатын дәрежеде бола алады.

Қазіргі заманғы ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың әлеуметтік себептеріне мыналарды жатқызу керек:

1. Қоғамын жалпы компьютерлендіру (компьютерлік технологиялардың тез қарқынмен дамуы, ақпараттық және телекоммуникацияны желілер, ақпараттық қызметтер, электрондық құжат

айналымы және т.б.) киберқылмыскерлердің қызметі үшін қажетті жағдай жасайды.

2. Халықтың ақпараттық қызметтерге, бағдарламалық өнімдерге деген нақты қажеттіліктері мен оларды өмір сүру деңгейінің төмен болуына байланысты заңды жолдармен қанағаттандыру мүмкіндігі арасындағы қайшылықтар.

Заң ғылымдары туралы білімнің конвергенциясы негізінде ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскерге мынадай жалпы сипаттама және жіктеу беруге болады:

1. Жасы. Ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарды жасайтын қылмыскер, негізінен, 18 жастан 24 жасқа дейінгі жастар (зерттелген қылмыстық істердің 55%) құрайды. Яғни студенттер немесе университетті бітіргендер, бірақ әлі үйленбегендер. Басқаша айтқанда, бұл қоғамдағы әлеуметтенудің ең маңызды кезеңін басынын өткізіп жатқан тұлғалар. Дәл осы жаста мұндай адамдарда өзін-өзі дамыту қажеттілігі туындайды. Қазіргі уақытта ақпараттық-телекоммуникациялық желілерді («Инернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылықтар жасарып келеді, өйткені қазіргі кезде балалар мен жасөспірімдер компьютерлік техникамен және желілік ақпараттық технологияларды тез меңгеруімен байланысты болып отыр.

2. Жынысы. Көптеген ғалымдар осы санаттағы қылмыстардың жасалуы ер адамдарға тән екендігімен келіседі. Алайда, кейінгі кезде осы қылмыстарды жасайтын әйелдер санының өсу тенденциясы байқалады. Бұл жағдайда әйелдер, әдетте, ер адамдармен бірге қылмысқа серіктес ретінде қатысады.

3. Білімі. Біздің ойымызша, осы түрдегі аса қауіпті қылмыстарды орта білімі бар және өзінің заңсыз әрекеттері ешқашан әшкереленбейді, тіпті өзін жазадан қашып құтылам деп ойлайтын адамдар жасайды. Ашылған қылмыстардың негізгі бөлігін біліктілігі төмен адамдар жасайды, олардың білімі жасаған қылмыс іздерін жасыруға жеткіліксіз болып келеді.

4. Тұлғаның психологиялық аспектілері. Криминологиялық әдебиеттерді зерттеу әдеттегі киберқылмыскердің келесі ұжымдық портретін қалыптастыруға мүмкіндік берді.

Әдетте, бұл қылмыстарды «виртуалды әлемде өзін-өзі тануға ұмтылатын, құрдастарымен қарым-қатынаста қиындықтары бар адам, электрондық цифрлық ақпаратты бағдарламалау мен қолдануда белгілі бір кәсіби биіктерге жетуге» ұмтылатын тұлғалар жасайды Сонымен қатар «өзін-өзі бекітуге ұмтылған, атақ-даңққа ие болуға тырысатын, өз шеңберінде беделге ие болуға» ұмтылатын адамдарда кіреді.

Киберқылмыскерлердің типтік бейнесі туралы келтірілген деректерге қарамастан, біз олардың өзгеріп тұрады деп санаймыз. Қазіргі кезде киберқылмыскер болу, ең алдымен, оның материалдық тұрғыдан тиімді

екендігімен байланысты. Нәтижесінде, бастамашыл, авантюрист және тіпті харизматикалық адамдар қылмыстық жауапкершіліктен жалтару ықтималдығы жоғары болатын және үлкен мөлшерде қылмыстық табыстар әкелетін қылмыстық құқық бұзушылықтар жасайды.

Ақпараттық– телекоммуникациялық желілерді («Интернет» желісін қоса алғанда) пайдалана отырып жасалатын қылмыстық құқық бұзушылыққа қатысты бірінші типке ұялы байланыс пайдаланушыларының құрбандары жатады. Бұл әр түрлі ұялы байланыс компанияларының абоненттері, олар техникалық дағдылары мен қаржылық шектеулеріне байланысты әлсіз қорғалған Интернет қосылыстарын пайдаланады және пайдаланушылардың теңгерімінен қаражаттарды рұқсатсыз «алып тастайтын» вирустық бағдарламалардың құрбаны болады. Оларға жарақат алған телефон қолданушылары - телефон «қарақшыларының» құрбанына айналған абоненттер қосылады. Екінші түріне компьютерлік қарақшылардың құрбандары жатады. Бұл лицензияланған бағдарламалық өнімдердің қымбаттығына байланысты оның жалған көшірмелерін қолданатын және сол арқылы әлеуетті құрбанға айналатын қарапайым пайдаланушылар.

IT-саласындағы қылмыстық құқық бұзушылықтардың алдын алудың тиімділігін арттыру үшін ақпараттық технологияларды тұтынушылардың өздерінің қауіпсіздік шараларын ұмытпағаны дұрыс. Осы саладағы қылмыстардың құрбанына айналмас бұрын қарапайым сақтық ережелерін сақтау қажет және ол өз кезегінде осы саладағы қылмыстардың санын азайтуға көмеген тигізеді.

Қарапайым сақтық шараларына мыналар жатады:

1 Таныс емес адамдар үшін SIM-карта сатып алу кезінде өзінің жеке куәлігіндегі мәліметтермен бөлісуге келісімін бермеу;

2 Таныс емес адамдармен Сіздің SIM-картаңызға келген құпия мәліметтермен бөліспеу;

3. Сіздің ұялы телефоныңызға таныс емес абоненттен келген СМС-хабарламалардың сілтемелеріне көшпеңіз және суреттерді жүктемеңіз;

4. Ешқашан ІІО интернет немесе ұялы байланыс арқылы электронды айыппұл төлеу туралы хабарлама жібермейтінін есте сақтаңыз;

5. Әлеуметтік желілер немесе электронды пошта арқылы таныс емес адамдармен араласпаңыз, өйткені бұл тәсіл соңғы кездері террористік ұйымдарға тарту үшін жиі пайдалануда.

ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жасауға ықпал ететін жағдайларға мыналарды жатқызамыз:

- елімізде қолданыстағы компьютерлер санының артуы және соның әсерінен оларды пайдаланушылар санының өсуі, компьютерлерде сақталатын ақпараттың көбеюі;

- компьютерлерді және олардың жүйелерін қорғаудың жеткіліксіз шаралары, сондай-ақ басшылықтың ақпараттық қауіпсіздік пен ақпаратты қорғауды қамтамасыз ету мәселелеріне әрқашан бей-жай қарауы;

- бағдарламалардың қажетті деңгейде қорғалмауы;

- компьютерлік техниканы қорғаудың техникалық құралдарының жеткіліксіз қорғалуы;

- ақпаратмен алмасу, келісімшарттар жасау, төлемдер жасау және т.б. бойынша компьютерді қолданушылардың әлемдік ақпараттық желілерге ену мүмкіндігі;

- заманауи техникалық құралдарды қылмыстық әрекетте қолдану;

- электрондық пошта құралдарының жеткіліксіз қорғалуы;

- компьютер пайдаланушыларының жұмыстыры немқұрайлылықпен қарауы;

- жұмысқа алу және шығару мәселелері бойынша ойластырылмаған кадр саясаты;

- компьютерлік қылмыстардың алдын алуға, ашуға және тергеуге міндетті ішкі істер органдарының, оның ішінде ішкі істер органдарының лауазымды адамдарының арнайы даярлығының төмен деңгейі;

- ақпараттық қауіпсіздік саласындағы мемлекеттік және қоғамдық құрылымдардың жұмысындағы үйлесімділіктің болмауы;

- елімізге электрондық тыңшылықтан қорғалған компьютерлер мен желілік жабдықтарды әкелуге шектеулер.

А.Л. Осипенко ақпараттық-телекоммуникациялық желілерді пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтардың детерминанттарына мыналарды жатқызады:

- ашық ғаламдық желілердің технологиялық қорғалмағандығы;

- заманауи желілер инфрақұрылымының күрделілігі мен өзгергіштігі;

- қолданылатын бағдарламалардың жоғары деңгейі осалдығы;

- желіде жұмыс істеген кезде анонимді мүмкіндіктердің кең мүмкіндігі (оның ішінде заңсыз).

Пайдаланған әдебиеттер тізімі:

1 «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» Мемлекет басшысы Н.Назарбаевтың Қазақстан халқына жолдауы. 2017 жылығы 31 қаңтар http://adilet.zan.kz/kaz/docs/K1700002017

2 Қазақстан Республикасының Бас прокуратурасы Құқықтық статистика және арнайы есепке алу комитеті https://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat

3 Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М.А. Ефремова. — М. : Юрлитинформ, 2015. — 200 с.

4 Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации: (по материалам Республики Дагестан) : дис. ... канд. юрид. наук : 12.00.08 / М.С. Гаджиев. — Махачкала, 2004. — 168 с.

5 Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук : 12.00.08 / Т.М. Лопатина. — М., 2007. — 418 с.

6 Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью : дис. … канд. юрид. наук : 12.00.08 / Д.В. Добровольский. — М., 2005. — 218 с.

7 Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук : 12.00.08 / А.А. Жмыхов. — М., 2003. — 178 с.

8 Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : автореф. дис. … канд. юрид. наук : 12.00.08 / И.Г. Чекунов. — М., 2013. — 22 с.

9 Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. — М. : Норма, 2003. — 332 с.

10 Дремлюга Р.И. Интернет-преступность / Р.И. Дремлюга. — Владивосток : Изд-во Дальневост. ун-та, 2008. — 240 с.

11 «Қазақстан Республикасы ақпараттық қауіпсіздігінің 2016 жылға дейінгі тұжырымдамасы туралы» Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашадағы Жарлығы

12 Конвенция о преступности в сфере компьютерной информации (ETS N 185) : заключена в Будапеште 23 нояб. 2001 г. https://online.zakon.kz

13 Group-IB [Электронный ресурс] : офиц. сайт. URL : https://www.group-ib.ru/

14 **Kaspersky Security Bulletin 2014. Основная статистика за 2014 год https://securelist.ru/kaspersky-security-bulletin-2014-osnovnaya-statistika-za-2014-god/24580/**

15 С.В. Скляров, К.Н. Евдокимов Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10, № 2. С. 322–330

16 Чирков Д.К. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны / Д.К. Чирков, А.Ж. Саркисян // Актуальные проблемы экономики и права. — 2013. — № 3. — С. 219–226.
17 Эмиров М.Б. Борьба с преступлениями в глобальных компьютерных сетях / М.Б. Эмиров, А.Д. Саидов, Д.А. Рагимханов // Юридический вестник Дагестанского государственного университета. — 2011. — № 2. — С. 63–66.
18 Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 24. — С. 45–55.
19 Крылов В.В. Расследование преступлений в сфере информации. – М., 1998. – 264 с.
20 Завидов Б.Д. Сфера высоких технологий как мошенничество и как спорные объекты интеллектуальной собственности, находящиеся вне правового поля (фрикерство, хакерство и радиопиратство): подготовлено для системы «КонсультантПлюс». – Доступ из справ. правовой системы КонсультантПлюс.
21 Oxford dictionaries language matters. – URL: http://www.oxforddictionaries.com
22 Macmillan dictionary.URL: http://www.macmillandictionary.com
23 Википедия – свободная энциклопедия. – URL: https://ru.wikipedia.org
24 Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: понятие, состояние, уголовно-правовые меры борьбы: дис…. канд. юрид. наук. – Владивосток, 2005. – 234 с.
25 Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. … канд. юрид. наук. – М., 2013. – 23 с.
26 Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции. – Нижний Новгород: Нижегородский госуниверситет. – 2014. – 560 с.
27 Aghatise E. J. Cybercrime definition. Computer Crime Research Center. – URL: http:// www.crime-research.org/articles/joseph06
28 Богданова Т.Н. К вопросу об определении понятия «преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. – 2012. – № 37 (291). – С. 64–67.
29 Фоменко А.И. К вопросу об определении понятия «преступления в сфере высоких технологий» // Вестник Северо-Кавказского гуманитарного института. – 2013. – № 1 (5). – С. 43–50.
30 Добровольский Д.В. Актуальные проблемы борьбы с преступностью (уголовно-правовые и криминологические проблемы): дис. … канд. юрид. наук. – М., 2005. – С. 19; Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: автореф. дис. … канд. юрид. наук. – М., 2005. – С. 7
31 Wall D. Cybercrime: the transformation of crime in the information age. – N.-Y., Polity, 2007. – P. 49-50.

32 Хилюта В.В. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием компьютерной техники // Криминологический журнал Байкальского государственного университета экономики и права. – 2012. – № 1. – С. 26–31.
33 Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании и ФРГ, Нидерландах, Польше) // Вестник ТГПУ. – 2006. – № 11. – С. 31–32.
34 Карпов В. С. Уголовная ответственность за преступления в сфере компьютерной информации: автореф. дис. … канд. юрид. наук. – Красноярск, 2002. – 26 с.
35 Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы. – Омск, 2009. – 480 с.
36 Қазақстан Республикасының Қылмыстық кодексі 2014 жылғы 3 шілдедегі №226-V Заңы [Электронный ресурс] URL: http://adilet.zan.kz/rus/docs/K1400000226 (Дата обращения 10.01.2020).
37 Базилова А.А. Компьютерлік қылмыстардың алдын алу шаралары // ҚазҰУ хабаршысы. Заң сериясы = Вестник КазНУ. Серия: юридическая. – 2016.- № 3 (79).- 179-182 б.
38 Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества /А.Г. Волеводз. – М.:ООО Изд-во «Юрлитинформ», 2002. – 496 с.
39 Свод законодательства США Раздел 18, часть 1, глава 47, §1029, §1030 Computer Fraud and Abuse Act (CFAA) [Электронный ресурс] // URL: http://www.law.cornell.edu/uscode/text/18/1030 (Дата обращения: 20.01.2020)
40 Уголовный кодекс Швеции / Научные редакторы проф. Н. Ф. Кузнецова и канд. юрид. наук С. С. Беляев. Перевод на русский язык С. С. Беляева. — СПб.: Издательство «Юридический центр Пресс», 2001.- 320 с.
41 Уголовный кодекс Дании / Научное редактирование и предисловие С. С.Беляева, канд. юрид. наук (МГУ им. М. В. Ломоносова). Перевод с датского и английского канд. юрид. наук С. С. Беляева, А.Н. Рычевой. — СПб.: Издательство «Юридический центр Пресс», 2001. – 230 с.
42 Уголовный кодекс Германии с изменениями от 28 декабря 2003 года. [Электронный ресурс] URL: http://lexetius.com/StGB/263a (Дата обращения: 25.01.2020)
43 Зарубежные уголовные кодексы. Уголовный кодекс Франции [Электронный ресурс] - http://crimpravo.ru/codecs/france/2.doc (Дата обращения 14.01.2020).
44 Уголовный кодекс Китайской Народной Республики [Электронный ресурс]. – URL: http://www.asia-business.ru/law/law1/criminalcode/code/#6 (Дата обращения 09.12.2019).
45 «Конвенция о преступности в сфере компьютерной информации» (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 20.12.2019)

46 Модельный Уголовный кодекс /Приложение к информационному бюллетеню Межпарламентской ассамблеи СНГ// СПб., 1996. - № 10
47 «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтасығы туралы келісімді ратификациялау туралы» Қазақстан Республикасының 2019 жылғы 9 желтоқсандағы заңы
48 Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) // Российская газета. 1998. 10 декабря.
49 *КасеноваМ.Б.* Основы трансграничного управления Интернетом // Кибербезопасность и управление Интернетом: Документы и материалы для российских регуляторов и экспертов / отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. М.: Статут, 2013. С. 9.
50 Вся статистика Интернета на 2020 год – цифры и тренды в мире и в России https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/
51 Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: резолюция ООН A/RES/53/70 от 4.12.1998 [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf (дата обращения: 29.10.2020).
52 Борьба с преступным использованием информационных технологий: резолюция ООН A/RES/56/121 от 19.12.2001 [Электронный ресурс] URL: http://www.ifap.ru/ofdocs/un/56121.pdf (дата обращения: 30.10.2020)
53 О преступлениях, связанных с компьютерами: рекомендация Совета Европы № 89 (9) от 13.09.1989 [Электронный ресурс]. URL: https://wcd.coe.int (дата обращения: 27.10.2020)
54 Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года [Электронный ресурс]. URL: http://publication.pravo.gov.ru (дата обращения: 27.10.2020).
55 «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастығы туралы келісімді ратификациялау туралы» Қазақстан Республикасының 2018 жылғы 3 мамырдағы заңы
56 Уголовный кодекс Франции (ред. от 03.07.2016). [Электронный ресурс]. URL: https:// www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 15.07.20)
57 Криминология / под ред. В. К. Звирбуля, Н. Ф. Кузнецовой, Г. М. Миньковского. – М., 1979. – С. 118-201.
58 Кузнецова, Н.Ф. Проблемы криминологической детерминации / Н.Ф. Кузнецова – М., 1984. – С. 54 – 55.
59 Кудрявцев, В.Н. Причинность в криминологии / В.Н. Кудрявцев. – М., 1987. – 106 с.

60 Антонян, Ю. М. Социальная среда и формирование личности преступника / Ю.М. Антонян. – М., 1975. – 351 с.
61 Ведерников, Н.Т. Личность обвиняемого как объект изучения на предварительном следствии / Н.Т. Вердников // Актуальные вопросы борьбы с преступностью. – Томск: Томский университет, 1990. – С. 99.
62 Антонян, Ю.М. Преступник как предмет криминологического изучения / Ю.М. Антонян // Вопросы борьбы с преступностью. Вып. 34. – М., 1981. – С. 21.
63 Уголовное право Республики Казахстан. Особенная часть: учебник / под ред. И. Ш. Борчашвили и С. М. Рахметова: В 2-х ч. Часть 2. – Алматы: Институт Данекер, 2000. – С. 93.
64 250–255. Поляков В.В., Людкова Н.В. Характеристика личности киберпреступников // Теоретические и практические проблемы организации раскрытия и расследования преступлений : сб. матер. Всерос. науч.-практ. конф. 22 апреля. — Хабаровск, 2016 г.
65 Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) : дис. ... канд. юрид. наук. — Ростов, 2000.
66 Дьяков В.В. О личности преступника как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации // Бизнес в законе. — 2008. — № 2.
67 с. 86–90 Евдокимов К.Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. — 2011. — № 1.
68 Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. ... канд. юрид. наук. — Иркутск, 2006.
69 Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Перевод с англ. / Д. Айков, К. Сейгер, У. Фонсторх. М.: Мир, 1999. С. 90.
70 Құрбанова И. Виктимология және виктимділік // Жантану - 2008. -№4(4). – Б. 22-25.
71 Криминология. Учебно-методические материалы и альбом схем: учебное пособие / под редакцией С.Е. Вицина и В.А. Уткина. – М.: Издательство «Щит-М», 1999. – 242 с.
72 Ривман Д.В. Виктимологические факторы и профилактика преступлений. –Л., –1975. - 156 с.
73 Ещанов А.Ш. К вопросу о виктимологической профилактике в Республике Казахстан // Экономика и право Казахстана. – 2003. - № 20. – С. 41-44.
74 Алауханов Е.О. Профилактика престиуплений: учебник. – Алматы: Заң әдебиеті, 2008. – 376 с.
75 Криминология: учебник / под ред. акад. В.Н. Кудрявцева, проф. В.Е. Эминова. – М.: Юрист, 1995. – 512 с.

76 Абулкаирова Б.Т. Зорлық-пайдақорлық қылмыстардың виктимологиялық алдын алу: маг. дис. – Алматы, 2013. – 113 б.
77 Варчук Т.В. Виктимологическое моделирование в криминологи и практикуе предупреждения преступости: Серия «Научные издания для юристов». – М.: ЮНИТИДАНА: Закон и право, 2014. – 239 с.
78 Киберқылмыс және киберпол // egemen.kz: https://egemen.kz/article/33685-kiberqylmys-dgane-kiberpol
79 Лунеев, В.В. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями / В.В. Лунев // Государство и право. – 2000. – № 9
80 Криминология: преступность как свойство общества. Краткий курс. – СПб: ЛАНЬ, 2001.
81 Жилинский, С. Э. Правоохранительная деятельность / С.Э. Жилинский // Российская криминологическая энциклопедия. – М., 2000.
82 Батурин Ю. М. Проблемы компьютерного права. М., 1991. С. 126.
83 Цифры: количество устройств под управлением Windows 10 в мире https://vc.ru/flood/37606-cifry-kolichestvo-ustroystv-pod-upravleniem-windows-10-v-mire (дата обращения: 07.02.2021)
84 Рейтинг стран по доле обладателей смартфонов. Насколько продвинуты россияне, китайцы и американцы? https://zen.yandex.ru/media/id/5db5508979c26e00b268e04f/reiting-stran-po-dole-obladatelei-smartfonov-naskolko-prodvinuty-rossiiane-kitaicy-i-amerikancy-5e161b662b616900b17b9eb5 (дата обращения: 07.02.2021)
85 Организация Объединенных Наций : вебсайт ООН. URL: http://www.un.org/ru/documents/decl_conv/declarations/crime91.shtml (дата обращения: 10.02.2021)
86 Тысячи кибератак зафиксировали в Казахстане в 2019 году https://rus.azattyq-ruhy.kz/incidents/4834-tysiachi-kiberatak-zafiksirovali-v-kazakhstane-v-2019-godu
87 Кузнецова Н. Ф. Избранные труды / предисл. акад. В. Н. Кудрявцева. СПб., 2003. С. 788.
88 Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы : монография / А. Л. Осипенко. Омск, 2009. С. 135.
89 Дремлюга, Р.И. Интернет-преступность [Текст]: дис. ... канд. юрид. наук /Р.И. Дремлюга. - М.,2018. - 198 с.
90 Дашян М.С. Право информационных магистралей: вопрос правового регулирования в сети «Интернет [Текст] /М.С. Дашян. - М.: Волтерс Клувер, 2017. - 248 с.
91 Уваров В.Н. Международное сотрудничество в области борьбы с компьютерными правонарушениями / В.Н. Уваров // Казахстан в глобальных процессах - 2016. - № 8. - С. 123-126.
92