ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БАС ПРОКУРАТУРАСЫНЫҢ
ЖАНЫНДАҒЫҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫ АКАДЕМИЯСЫ

АХМЕТБЕК ЖАННҰР АСҚАРБЕКҰЛЫ

Қазақстан Республикасы ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметінің ұйымдық-құқықтық аспектілері

7М12301 «Құқық қорғау қызметі» (бейінді бағыт)
білім беру бағдарламасы бойынша
ұлттық қауіпсіздік және әскери іс магистрі
дәрежесін алуға магистрлік жоба

Ғылыми жетекші:
Жоғары оқу орнынан кейінгі
білім беру институтының
Арнайы заң пәндері
кафедрасыныңмеңгерушісі,
Н.Ш.Жемпиисов,
заң ғылымдарының кандидаты,
әділет аға кеңесшісі

_____

Қосшы қ., 2023ж.

ТҮЙІНДЕМЕ

Магистрлік жобада елімізде соңғы жылдары кең таралып отырған интернет-алаяқтықпен байланысты қылмыстарға қарсы іс-қимылдың өзекті мәселелері қарастырылады.

Мұндай қылмыстардың басым көпшілігін ашу және тергеу Қазақстан Республикасының ішкі істер органдарының құзыретіне жататындықтан, олардың осы бағыттағы қызметіндегі негізгі проблемаларды анықтау, оларды шешу жолдарын қарастыру, тиімді тәсілдер мен заңнамаға өзгерістер және толықтырулар енгізу жөнінде ұсыныстар әзірлеу жайында болмақ.

РЕЗЮМЕ

В магистерском проекте будут рассмотрены актуальные вопросы противодействия широко распространяемых встране в последние годы преступлений, связанных с интернет-мошенничеством.

Учитывая, что раскрытие и расследование подавляющего большинства таких преступлений относится к компетенции органов внутренних дел Республики Казахстан, речь пойдет о выявлении основных проблемв их деятельности в данном направлении, рассмотрении путей их разрешения, выработке эффективных способов и предложений о внесении изменений и дополнений в законодательство.

SUMMARY

Themaster's project will consider topical issues of combatting widespread in the country in recent years crimes related to Internet fraud.

Given that the disclosure and the investigation of the vast majority of such crimes falls within the competence of the internal affairs bodies of the Republic of Kazakhstan, it is about identifying the main problems in their activities in this direction, consideration of ways to solve them to develop effective ways and proposals to amend amendments to the legislation.

МАЗМҰНЫ

АНЫҚТАМАЛАР 4
КІРІСПЕ 6

1. ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА ИНТЕРНЕТ-АЛАЯҚТЫҚҚА ҚАРСЫ ІС-ҚИМЫЛДЫҢ АҒЫМДАҒЫ ЖАЙ-КҮЙІ 13
1.1 Интернет-алаяқтық қылмыстардың қылмыстық-құқықтықсипаттамасы, статистикалық деректердің динамикалық көрсеткіштері 13
1.2 Интернет-алаяқтық қылмыстардың негізгі түрлері мен тәсілдері, жедел-іздестіру және тергеу іс-шараларының тактикалық ерекшеліктері 18

2. ИНТЕРНЕТ-АЛАЯҚТЫҚҚА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕ 23
2.1 Интернет-алаяқтыққа қарсы іс-қимыл мәселелерін регламенттейтін негізгі халықаралық актілер 23
2.2 Шетел мемлекеттерінің құқық қорғау органдарының интернет-алаяқтық қылмыстарды ашу және тергеу қызметінің ұйымдық-құқықтық аспектілері..... 29

3. ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ІШКІ ІСТЕР ОРГАНДАРЫНЫҢ АЛАЯҚТЫҚҚА ҚАРСЫ ІС-ҚИМЫЛ ЖӨНІНДЕГІ ҚЫЗМЕТІН ЖЕТІЛДІРУДІҢ НЕГІЗГІ БАҒЫТТАРЫ 31
3.1 Ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметінің қазіргі жай-күйі мен құқықтық регламенттелуі 31
3.2 Ішкі істер органдарында интернет-алаяқтық қылмыстарды ашу және тергеу процесін оңтайландыружөніндегі ұсынымдар 35

ҚОРЫТЫНДЫ…..……..... 40

ҚОЛДАНЫЛҒАН ДЕРЕККӨЗДЕРДІҢ ТІЗІМІ……..... 41

ҚОСЫМША 1. Енгізу актісі .....…….... 44

АНЫҚТАМАЛАР

Осы магистрлік жобада сәйкесінше анықтамалары бар келесі терминдер қолданылған:

Интернет – электрондық ақпараттық ресурстарды жіберуге арналған телекоммуникациялардың біріктірілген желілерінің және есептеу ресурстарының дүниежүзілік жүйесі;

ақпараттық-коммуникациялық технологиялар – электрондық ақпараттық ресурстармен жұмыс істеу әдістерінің және аппараттық-бағдарламалық кешен мен телекоммуникациялар желілерін қолдана отырып жүзеге асырылатын ақпараттық өзара іс-қимыл әдістерінің жиынтығы;

ақпараттық жүйе – ақпараттық өзара іс-қимыл арқылы белгілі бір технологиялық әрекеттерді іске асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсетуші персоналдың және техникалық құжаттаманың ұйымдастырылып ретке келтірілген жиынтығы;

онлайн-платформа – қаржылық көрсетілетін қызметтерді ұсынуға және электрондық коммерцияға арналған интернет-ресурсты және (немесе) лездік хабарлар алмасу сервисін қоспағанда, белгілерді және (немесе) сигналдарды және (немесе) дауыстық ақпаратты және (немесе) жазбаша мәтінді және (немесе) кескінді және (немесе) дыбыстарды және (немесе) хабарларды орналастыру, қабылдау және (немесе) нақты айқындалған немесе айқындалмаған тұлғалар тобына беру арқылы пайдаланушының өзі жасаған дербес парақшасы арқылы ақпарат таратуына арналған интернет-ресурс және (немесе) лездік хабарлар алмасу сервисі;

онлайн-платформаны пайдаланушы – өзінің дербес деректерін тіркеген және ұсынған, сондай-ақ қазіргі бар онлайн-платформалардың бірінде сәйкестендіруден өткен жеке және (немесе) заңды тұлға;

цифрлық сауаттылық – адамның ақпараттық-коммуникациялық технологияларды білуі және оларды күнделікті әрі кәсіптік қызметінде пайдалана білуі;

байланыс операторы – байланыс қызметтерін көрсететін және (немесе) байланыс желілерін пайдаланатын, Қазақстан Республикасының аумағында тіркелген жеке немесе заңды тұлға;

интернет-трафик – белгілі бір уақыт кезеңінде Интернетке жалғау арқылы берілетін және қабылданатын ақпараттың көлемі;

ұялы байланыс операторы - Қазақстан Республикасының заңнамасына сәйкес ұялы байланыс қызметтерін көрсететін байланыс операторы;

банктік шот – клиенттің банктегі немесе банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдағы ақшасының қозғалысын, сондай-ақ клиентке банк қызметін көрсету бойынша клиент пен банк немесе банк операцияларының жекелеген түрлерін жүзеге асыратын ұйым арасындағы шарттық қатынастарды көрсету және есепке алу тәсілі;

төлем карточкасы – ұстаушысына электрондық терминалдар немесе басқа байланыс арналары арқылы төлемдерді және (немесе) ақша аударымдарын

жүзеге асыруға не қолма-қол ақша алуға не валюталарды айырбастауды және төлем карточкасының эмитенті айқындаған және оның шарттарымен басқа да операцияларды жүргізуге мүмкіндік беретін ақпарат қамтылған электрондық төлем құралы;

микроқаржылық қызметті жүзеге асыратын ұйым – микрокредиттер беру жөніндегі қызметті жүзеге асыратын микроқаржы ұйымы, кредиттік серіктестік, ломбард;

микрокредит – микроқаржылық қызметті жүзеге асыратын ұйым қарыз алушыға осы Заңда айқындалған мөлшерде және тәртіппен ақылылық, мерзімділік және қайтарымдылық шарттарымен Қазақстан Республикасының ұлттық валютасында беретін ақша;

ақша аударымдары жүйесі – банк немесе банк операцияларының жекелеген түрлерін жүзеге асыратын ұйым төлемдерді және (немесе) ақша аударымдарын жүзеге асыру үшін келісім жасасқан төлем жүйесі операторының бағдарламалық қамтамасыз етуі пайдаланыла отырып, ақша аударымдары жүзеге асырылатын төлем жүйесі;

электрондық ақша – электрондық нысанда сақталатын және электрондық ақша жүйесінде жүйеге басқа да қатысушылар төлем құралы ретінде қабылдайтын электрондық ақша эмитентінің шартсыз және кері қайтарып алынбайтын ақшалай міндеттемелері;

SMS (ағылшын тіліндегі Shot Messaging Service) - ұялы байланыс құралының көмегімен қысқа мәтінді хабарламалар жіберуге және қабылдауға мүмкіндік беретін технология.

КІРІСПЕ

Зерттеудің өзектілігі. Интернеттің дамуы тұлғааралық қатынастарды, тауарлар қозғалысы мен логистикалық ағынды, ақпарат алмасуды және жалпы тіршіліктің барлық аспектілерін қозғай отырып, әлемді терең және белсенді түрде трансформацияға ұшыратуда. Ғаламтордың жекелеген тұтынушыларға да, ірі экономикалық жүйелерге де әсері уақыт өткен сайын айқын және әрқилы сипат алып келеді.

2022 жылдың басында барша әлемде интернет пайдаланушылардың саны 4,9 млрд. адамды құраған - бұл планетадағы адамдардың 2/3 интернетке қосылғанын білдіреді. Тек соңғы 10 жылдың өзінде пайдаланушылар саны 2,2 есеге ұлғайған. Елдер бөлігінде Қазақстан мобилді интернет-трафикті тұтыну көлемінің көптігі бойынша ТОП-15-ке кіреді. 2021 жылдың 4-тоқсанының қорытындысы бойынша Қазақстанда бір пайдаланушының мобилді интернет-трафигін тұтынуы 14,4 ГБ құраған, бұл орташа көрсеткіштен 46% артық [1].

Қазақстанда цифрландыру кең белең алып келеді - қазір елімізде интернеттің ену көрсеткіші 90,1% құрайды[2].

Алайда интернеттің қарқынды дамуымен және оның мүмкіндіктерінің кеңеюімен, оның адамдар мен қоғамның күнделікті тіршілігіне жан-жақты енуімен бірге қылмыскерлер де белсенділігін күшейтті. Мыңдаған аңқау азаматтар алаяқтардың құрбаны болып, ауқымды қаражаттарынан айырылып қалып жатыр. Қылмыскерлер күн сайын алдаудың түрлі жолдары мен схемаларын ойлап тауып, онлайн-платформалар арқылы жарнамалап, арам пиғылдарын жемісті іске асыруда.

Қазақстан Республикасы Баспрокуратурасы жанындағы Құқықтық статистика және арнайы есепке алу комитетінің статистикалық мәліметтеріне ("Тіркелген қылмыстық құқық бұзушылықтар туралы" № 1-М нысанды есеп) сәйкес елімізде алаяқтық, оның ішінде ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен жасалатын алаяқтық қылмыстар (бұдан әрі - интернет-алаяқтық) жылдан жылға өсіп келеді. Дәлірек айтқанда, соңғы 3 жылда, яғни 2020-2022 жылдар аралығында Республика аумағында алаяқтық қылмыстар саны 29,5%-ға (2020жылы 29282 қылмыс тіркелсе, 2022жылы 43 499 қылмыс тіркелген) ұлғайса, оның ішінде интернет-алаяқтық қылмыстар саны тіпті 44,6%-ға (2020 жылы 14 220 қылмыс тіркелсе, 2022жылы – 20 569 қылмыс тіркелген) өсіп кеткен [3].

Интернет-алаяқтық қылмыстардың кең таралған түрлері – алдау немесе сенімді теріс пайдалану жолымен хабарландырулар бойынша тауар немесе қызмет үшін алдын-ала төлем алу, жеке тұлғалардың дербес деректеріне қол жеткізіп, микрокредиттік ұйымдардан несие рәсімдеу немесе банктік шоттарынан ақша қаражатын жымқыру. Көптеген жағдайда алаяқтар өздерінбанк немесе құқық қорғау органдары қызметкерлері ретінде таныстырады, ауысымдық абоненттік нөмірлерден қоңырау шалады және жалған немесе басқа тұлғаларға ресімделген төлем карточкаларын пайдаланады.

Елімізде Қазақстан Республикасының Қылмыстық-процестік кодексінің (бұдан әрі - ҚПК) 187-бабының 4-1-бабында белгіленген құзыреттеріне сәйкес интернет-алаяқтық қылмыстардың басым көпшілігін ашу және тергеумен ішкі істер органдары айналысады [4].

Қазақстан Республикасы Ішкі істер министрлігі (бұдан әрі - ІІМ) мен басқа да мүдделі мемлекеттік органдар соңғы жылдары интернет-алаяқтыққа қарсы іс-қимылдың тиімділігін арттыру үшін бір қатар заңнамалық, ұйымдық-практикалық және профилактикалық шаралар қабылдады: шет мемлекеттердің құқық қорғау органдарының киберкеңістіктегі қылмыстарды ашу және тергеудің тактикалары, заманауи ақпараттық технологияларды пайдалану тәжірибесі зерделенуде, киберқылмыстарға және интернет-алаяқтыққа қарсы іс-қимыл жөніндегі бағдарламалар әзірленіп іске асырылуда, халық арасында кеңінен ақпараттық-құқықтық түсіндіру жұмыстары жүргізілуде, өңірлік полиция департаменттерінде оларды тергеу жөніндегі арнайы жедел-тергеу топтары құрылды, сондай-ақ микроқаржылық қызметті жүзеге асыратын ұйымдар арқылы онлайн-режимде микрокредит рәсімдеу кезінде клиенттердің жеке басын куәландыру тәртібі қатаңдатылды.

Дегенмен жоғарыда көрсетілген статистикалық мәліметтер интернет-алаяқтықпен байланысты ахуалдың жақсармай отырғанын куәландырады, бұл, сәйкесінше, мемлекеттік органдардың, оның ішінде ішкі істер органдары қабылдап жатырған шаралардың жеткіліксіз және тиімсіз екендігін білдіреді.

Бұл дегеніміз, азаматтарымыздың Қазақстан Республикасының Конституциясымен кепілдік берілген меншік құқығы тиісті деңгейде қорғалмай отырғанын білдіреді. Ал Конституцияның 26-бабында Қазақстан Республикасының азаматтары заңды түрде алған қандай да болсын мүлкін жеке меншігінде ұстай алатыны көрсетілген. Соттың шешімінсіз ешкімді де өз мүлкінен айыруға болмайды. Заңмен көзделген ерекше жағдайларда мемлекет мұқтажы үшін мүліктен күштеп айыру оның құны тең бағамен өтелген кезде жүргізілуі мүмкін [5].

Практикалық міндеттің қазіргі уақыттағы жағдайы. Интернет-алаяқтыққа қарсы іс-қимыл мәселесін заңнамалық реттеу ақпараттық-коммуникациялық технологиялардың даму қарқынынан әлдеқайда артта қалып келеді деуге негіз бар. Нақтырақ, қылмыстық және қылмыстық-процестік заңнаманың адамзаттың ақпараттық даму процесіндегі жаһандық өзгерістерді ескермеуі салдарынан дәл қазір ішкі істер органдарының қорғау және алдын алу функциялары тиісті деңгейде іске асырылмай отыр.

Қазақстан Республикасы Парламентінің Мәжіліс депутаты Юрий Ли Қазақстан Республикасы Бас Прокуроры мен Ішкі істер министрінің атына жасаған депутаттық сауалында Қазақстанда интернет-қылмыстарды ашу өте төмен деңгейде екенін көрсетіп, 10 интернет-алаяқтың 8 табылмағанын айтты. Оның сөзінше, бұл құқық қорғау органдары қызметкерлерінің интернет-алаяқтықпен байланысты қылмыстық істерді тергеу кезінде әрекетсіздігі туралы шағымдардың көбеюіне әкеп соғуда. 2022 жылдың 11 айында елімізде

17 500 интернет-алаяқтық тіркелген және олардан азаматтарға 15 млрд. теңгеден астам залал келтірілген [6].

ІІМ-нің өзі интернет-алаяқтықты тергеу мен ашудың күрделілігін мойындап отыр [7]. Ал "Қазақстан Республикасының ішкі істер органдары туралы" Қазақстан Республикасы Заңның (бұдан әрі - Заң) 1-бабына сәйкес Қазақстан Республикасының ішкі істер органдары адамның және азаматтың өмірін, денсаулығын, құқықтары мен бостандықтарын, қоғамның және мемлекеттің мүдделерін құқыққа қарсы қолсұғушылықтан қорғауға, қоғамдық тәртіпті сақтауға және қоғамдық қауіпсіздікті қамтамасыз етуге арналған құқық қорғау органы болып табылады [8]. Осы тақырыптағы ғылыми жұмыстарда авторлардың көпшілігі құқық қорғаушыларға мұндай қылмыстарды ашу қиындап бара жатқаны туралы ортақ пікір білдіреді.Олардың ішінде Л.К.Еськованы [9], О.И.Денисенконы [10], Л.В.Готчинаны [11] атап өтуге болады.

Жедел уәкілдер мен тергеушілер интернет-алаяқтық қылмыстарды ашу және тергеу барысында көптеген күрделі мәселелерге тап болуда, себебі олар көбінесе заманауи ақпараттық-коммуникациялық технологияларды пайдаланатын және қылмыс тәсілдерін үнемі өзгертіп отыратын кәсіби алаяқтарға қарсы тұруға мәжбүр.

Интернет-қылмыстарды ашу және тергеу біршама қиындықтарға әкеп соғуда, өйткені олар көбінесе аумақаралық, тіпті кейде трансшекаралық сипатта болады, яғни жәбірленуші бір аймақта, ал қылмыскер басқа аймақта болады. Көптеген ақша аударымдары жүйелері мен онлайн-платформалардың пайда болуы қылмыскерлерге қашықтан, тіпті шет елдерден әрекет етуге мүмкіндік жасайды. Қылмыскерлер үшінші тұлғаларға рәсімделген банктік төлем карточкалар мен абоненттік нөмірлерді қолданады, электрондық ақшаны қолма-қол ақшаға ауыстыру үшін бөгде адамдарды тартады.

Осылайша қылмыскерлер полиция қызметкерлеріне қарағанда бірнеше қадам ілгері әрекет етіп келеді, ал полиция қызметкерлері интернет-алаяқтық қылмыстарды ашу және тергеуді басқа қылмыстармен бірдей жүзеге асырып, консервативті жедел-тергеу тәсілдерін қолданып келеді.

Сондықтан бүгінгі күнде интернет-алаяқтыққа және ішкі істер органдарының құзыретіне жататын киберкеңістіктегі басқа да қауіптерге қарсы тиімді әрекет ету үшін ішкі істер органдарының жұмыс тәсілдерін түбегейлі қайта қарастыру қажеттігі туындап отыр. Ол үшін ішкі істер органдарының басқа мүдделі органдар және ұйымдармен ақпарат алмасу рәсімін оңтайландыру, артық қағазбастылықты жою және заманауи ақпараттық-коммуникациялық технологияларды кеңінен ендіру арқылы интернет-алаяқтық қылмыстарды ашу және тергеудің жеделдігін мейлінше арттыру қажет.

Қазіргі уақытта қалыптасқан тәжірибе бойынша интернет-алаяқтық қылмыстардың барлығын дерлік тергеу барысында жедел уәкілдер мен тергеушілер басқа ұйымдардан (банктер, микроқаржылық қызметті жүзеге асыратын ұйымдар, байланыс операторлары) мәліметтерді жинақтайды және олармен ақпарат алмасу негізінен қағаз түрінде жүзеге асырылады.

Сонымен бірге қылмыскерлер қашықтан әрекет жасайтындықтан басқа өңірлердің ішкі істер бөлімшелеріне анықталған адамдарды табу және олардан істің мән-жайлары туралы жауап алу туралы жеке тапсырмалар жолданады. Басқа өңірдің ішкі істер бөлімшелерінде ведомстволық қызығушылық болмағандықтан немесе орындаушылық тәртіптің сақталмауынан мұндай жеке тапсырмалар ұзақ уақыт орындалады, тіпті кейбірі мүлдем орындалмайды.

Бұл ретте кейбір жағдайда қылмыскерлер көпдеңгейлі қылмыс схемаларын қолданатындықтан жоғарыда аталған жедел-тергеу әрекеттері бірнеше рет қайталап жүргізіледі.

Кейбір жағдайда тіпті шет мемлекеттердің құқық қорғау органдарына тапсырма жолдау қажеттігі туындайды. Ал шет мемлекеттердің құқық қорғау органдары тарапынан құқықтық көмек көрсету туралы сұрау хаттарды орындау тәртібі халықаралық шарттармен реттеледі және оған ұзақ уақыт кетеді.

Осының салдарынан барлық деңгейдегі жергілікті ішкі істер органдары қызметкерлерінің жұмыс уақыты мен күші тиімсіз пайдаланылады, тергеу барысы созбалаңдыққа салынып, көптеген қылмыстар ашылмайды.

Әсіресе, интернет-алаяқтық қылмыстарды тергеу барысында ақша қаражаты айналымы негізгі дәлелдеме болып табылатындықтан банктік шоттарды және олардағы ақша қаражатының қозғалысын анықтауға бағытталған тергеу әрекеттерін шұғыл жүргізу аса маңызды.

Бұдан бөлек, интернет-алаяқтық қылмыстардың алдын-алу, ашу және тергеу саласындағы ведомствоаралық үйлестіру және мүдделі мемлекеттік органдардың өзара іс-қимылын күшейту, сондай-ақ ішкі істер органдарында интернет-алаяқтық қылмыстарды ашу және тергеу процесін орталықтандыру мәселесін қарастыру бүгінгі күн тәртібіндегі аса өзекті мәселелер қатарында.

Зерттеу мақсаты, міндеттері, объектісі мен тақырыбы.

Зерттеудің мақсаты:

Қазақстан Республикасы ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметінің ұйымдық-құқықтық аспектілерін кешенді зерттеу, өзекті проблемаларды анықтау және оларды шешу бойынша құқықтық және практикалық ұсыныстар әзірлеу болып табылады.

Зерттеудің міндеттері:

1) интернет-алаяқтық қылмыстар бойынша статистикалық деректердің динамикалық көрсеткіштерін терең талдау арқылы интернет-алаяқтыққа қарсы іс-қимылдың тетігі мен тәсілдерін түбегейлі қайта қарап күшейтудің аса маңыздылығын негіздеу;

2) интернет-алаяқтық қылмыстардың негізгі түрлері мен тәсілдерін, жедел-іздестіру және тергеу іс-шараларының тактикалық ерекшеліктерін қарастыру арқылы кемшіліктер мен проблемаларды көрсету;

3) интернет-алаяқтыққа қарсы іс-қимыл саласындағы халықаралық тәжірибені зерттей отырып, тиімді ұйымдық-құқықтық аспектілерін, озық әдістері мен тәсілдерін белгілеу;

4) Қазақстан Республикасы ішкі істер органдарының интернет-алаяқтықты ашу және тергеу жөніндегі қызметінің қазіргі жай-күйі мен негізгі проблемаларын айқындау;

5) ішкі істер органдарында интернет-алаяқтық қылмыстарды ашу және тергеу процесін жетілдіру және оңтайландыру жөніндегі ұсынымдарды қалыптастыру және негіздеу.

Зерттеу объектісі.

Қазақстан Республикасы ішкі істер органдарының интернет-алаяқтыққа қарсы қимыл жөніндегі қызметі.

Зерттеу тақырыбы.

Қазақстан Республикасы ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметінің ұйымдық-құқықтық аспектілері.

Зерттеудің әдістері мен әдістемелік негіздері.

Зерттеу барысында жалпыға ортақ негізгі ережелер қолданылды, теория мен практиканың өзара байланысын көрсетуге мүмкіндік беретін таным әдістері, зерттеу пәнінің нысандары мен мазмұны, даму процестері және қарастырылатын әлеуметтік-экономикалық және құқықтық құбылыстар, сондай-ақ абстрактіден нақтыға көтерілу, дедукция, талдау, синтез, салыстыру, динамикалық және статистикалық әдістер және т.б. сияқты зерттеудіңжалпығылыми әдістерінің жиынтығы.

Ғылыми жаңалықтың негіздемесі.

Жалпы киберқылмысқа, ақпараттық-коммуникациялық технологияларды пайдаланып жасалатын қылмыстарғағалымдар мен зерттеушілердің көптеген ғылыми жұмыстары арналған (диссертациялар, монографиялар, ғылыми мақалалар, оқу әдістемелері және т.б.). Олардың ішінде танымалдары - Ю.М.Батурин, А.М.Жодзишский, А.Б.Агапов, А.В.Черных,Г.Б.Кочетков, Н.Д.Литвинов, А.Н.Федоров, Е.А.Суханов, В.Н.Черкасов. Интернет желісіндегі ақша қаражатын жымқырумен байланысты туындайтын проблемаларды зерттеумен заң ғылымында Р.М.Букалерова, Б.В.Вехов, М.М.Милованова, В.В.Рябчиков, Л.К.Еськова, О.И. Денисенко, Л.В. Готчина, С.В.Ардабьева және т.б. ғалымдар мен заңгерлер айналысқан. Оларда негізінен аталған санаттағы қылмыстардың қылмыстық-құқықтық және криминологиялық аспектілері, тергеу тактикалары мен әдістері көтерілген.

Компьютерлік қылмыстардың криминалистикалық аспектілері ішінара В.Н.Белов, А.Н.Караханьян, В.Д.Ларичев, Н.С.Полевой, Н.А.Селиванов, П.Б.Гудков, А.Н.Федоровтың жұмыстарында қамтылған.

Сөзсіз, зерттеушілер мен заңгерлердің жұмыстары қылмыстық құқық пен заңнаманы жетілдіруге елеулі үлес қосты.

Дегенмен осы кезге дейін нақты Қазақстан Республикасында интернет-алаяқтық қарсы іс-қимылға тікелей жауапты ведомство - ішкі істер органдары қызметінің ұйымдық-құқықтық аспектілері ғылыми тұрғыда қарастырылмаған. Жоғарыда аталған авторлардың жұмыстарында Қазақстан Республикасында интернет-алаяқтық қарсы іс-қимылдың соңғы жылдардағы өзекті жай-күйі, еліміздің ішкі істер органдарының қызметі зерттелмеген, олардың мұндай

қылмыстарды ашу және тергеу барысында кездесетін проблемалары айқын ашып көрсетілмеген. Дәл қазіргі уақыттағы жедел-тергеу практикасының қажеттіліктерін ескере отырып, нақты интернет-алаяқтық қылмыстардың криминалистикалық сипаттамасының, оларды ашу және тергеу практикасын жетілдірудің проблемалары жеткіліксіз зерделенгенін мойындау керек. Сондықтан ғалым-заңгерлердің бұған дейінгі жарық көрген еңбектерін талдай отырып және олардың ықпалы мен рөлін мойындай отырып, нақты осы таңдап алған тақырыпта зерттеу жүргізуді мақсатқа сай деп санадық.

Осылайша, таңдалған тақырыптың жаңалығы - бұл жұмыста елімізде адам мен азаматтардың құқықтарын қылмыстық қол сұғушылықтар мен қауіп-қатерлерден қорғау жағынан алғанда қылмыстық құқық бұзушылықтарға қарсы тұратын негізгі қылмыстық қудалау органының қазіргі жағдайдағы интернет-алаяқтыққа қарсы іс-қимылды жүзеге асыру қызметінің ұйымдық және құқықтық реттелуі мен құқық қолдану тәжірибесін жан-жақты, егжей-тегжейлі зерттеуге, ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі жұмысының ұйымдық-құқықтық аспектілерін жетілдіруге және тиімділігін арттыруға бағытталған заңнамалық, ұйымдық және практикалық ұсынымдар әзірлеуге талпыныс жасалған.

Жұмыстың нәтижесі кейбір ұсынымдарды одан әрі тәжірибеде іске асыру арқылы қолданбалы сипатта болады деп күтіледі.

Қорғауға шығарылатын практикалық ұсынымдар:

1. 2001 жылғы 23 қарашада Будапешт қаласында қабылданған Компьютерлік қылмыстар туралы Еуропалық конвенцияға (киберқылмыстар туралы) қосылу туралы заң жобасын әзірлеу және Қазақстан Республикасы Парламентінің қарауына енгізу.

2. «Қазақстан Республикасындағы банктер және банк қызметі туралы» Заңның 50-бабы 7-тармағының б)-тармақшасында жеке тұлғаның банк шоттарының бар-жоғы және нөмірлері туралы, осы шоттардағы ақша қалдықтары мен ақша қозғалысы туралы анықтамаларды айрықша электронды форматта беруді (қылмыстық қудалау органының бірінші басшысы немесе тергеушінің қолтаңбасымен куәландырылған электрондық нысандағы сұрау салу, прокурордың электрондық нысанда салынған санкциясы негізінде) міндеттейтін өзгерістер мен толықтырулар енгізу [12].

3. ІІМ жанында өз бетімен тергеу-жедел функциясын жүзеге асыру құзыреті бар комитет немесе департамент деңгейінен төмен емес нысанда киберқылмысқа қарсы іс-қимыл жөніндегі толыққанды жеке құрылымдық бөлімше (Киберпол) құру, сәйкесінше, облыстық полиция департаменттері жанында ұқсас киберқылмысқа қарсы іс-қимыл басқармаларын құру туралы Ішкі істер министрінің бұйрығын шығару.

4. Интернет-алаяқтыққа қарсы іс-қимылдың тиімділігін айтарлықтай көтеру үшін осы саладағы ведомствоаралық үйлестіруді көздейтін орталық мемлекеттік және құқық қорғау органдары басшыларының бірлескен бұйрығын шығару, онда:

- ІІМ-не (киберқылмысқа қарсы іс-қимыл жөніндегі бөлімше) киберқылмыстар мен интернет-алаяқтықтардың алдын алу, анықтау, ашу және тергеу саласында ведомствоаралық үйлестіру функциясын жүктеуді;

- киберқылмысқа қарсы іс-қимыл жөніндегі бөлімшелердің жанында құрамына ішкі істер органдары және мүдделі мемлекеттік органдар мен басқа ұйымдардың (банктер, ұялы байланыс операторлары) қызметкерлері, жоғары білікті IT-мамандар кіретін арнайы штаб құру жолымен интернет-алаяқтықтарды анықтау, ашу және тергеу процесін орталықтандыру және оған келесі міндеттерді жүктеуді қарастыру:

а) ақпараттық-коммуникациялық жүйелер мен дереккөздерді қолдана отырып, жергілікті ішкі істер органдарын барша республика аумағында орын алған интернет-алаяқтықтарды жылдам ашу және тергеу үшін барлық қажетті мәліметтермен жедел және онлайн режимде қамтамасыз етуді;

б) интернет-алаяқтықтарды ашу және тергеу мәселелері бойынша әртүрлі өңірлердің ішкі істер органдары арасында жедел өзара іс-қимылды қамтамасыз етуді;

в) көпэпизодты интернет-алаяқтықтарды ашу және тергеу.

Апробация және нәтижелерін енгізу.

Магистрлік жобада қамтылған негізгі ережелер мен түйіндер "Академик" халықаралық ғылыми журналында жарияланған 1 мақалада көрініс тапты, сондай-ақ Түркістан облысының полиция департаментінің практикалық қызметінде пайдалану және қолданыстағы заңнама мен жедел-тергеу практикасын жетілдіруге ұсынылды, енгізу актісі бар.

1. ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА ИНТЕРНЕТ-АЛАЯҚТЫҚҚА ҚАРСЫ ІС-ҚИМЫЛДЫҢ АҒЫМДАҒЫ ЖАЙ-КҮЙІ

1.1 Интернет-алаяқтық қылмыстардың қылмыстық-құқықтық сипаттамасы, статистикалық деректердің динамикалық көрсеткіштері

Қазақстан Республикасының қылмыстық және қылмыстық-процестік заңнамасында нақты интернет-алаяқтық ұғымы қолданылмайды, тиісінше оның ұғым ретінде түсінігі де, қылмыстық заңнаманың термині ретінде мағынасы да берілмеген. Интернет-алаяқтық ұғымы Қазақстан Республикасы Жоғарғы Сотының "Алаяқтық туралы істер бойынша сот практикасы туралы" 2017 жылғы 29 маусымдағы № 6 нормативтік қаулысында да қамтылмаған[13].

Жалпы әлемдік қоғамдастықта қалыптасқан түсінік бойынша интернетті, бірінші кезекте, басты мақсаты ақпараттарды сақтау және трансляциялау болып табылатын компьютерлік желілердің өзара байланысқан жүйесі деп білеміз.

Оған отандық заңнамамызда ресми белгіленген интернет ұғымының мағынасы да өте жақын. Яғни, "Ақпараттандыру туралы" Қазақстан Республикасы Заңында интернет – электрондық ақпараттық ресурстарды жіберуге арналған телекоммуникациялардың біріктірілген желілерінің және есептеу ресурстарының дүниежүзілік жүйесі деп танылған [14].

Қазақ тілді әдебиетте интернетті "Ғаламтор" деп те атайды, орыс тілінде "Всемирная сеть", "Глобальная сеть" ұғымдары жиі пайдаланылады, ал ауызекі тілде "Всемирная паутина" тіркесі жиі кездеседі.

Қазақстан халқының басым бөлігі ақпараттық-коммуникациялық технологияларды кеңінен тек соңғы жылдары қолдана бастағандықтан интернет-алаяқтық қылмыстар бойынша толыққанды әрі тиімді жедел-іздестіру және сот-тергеу практикасы қалыптаспаған десе болады.

Бүгінгі күнге қалыптасқан сот-тергеу практикасы бойынша интернет-алаяқтық қылмыстарға Қазақстан Республикасының Қылмыстық кодексінің (бұдан әрі - ҚК) 190-бабы 2-бөлігінің 4) тармағымен сараланатын қылмыстар жатады деп түсініледі.

ҚК 190-бабының 1-бөлігіне сүйенсек, алаяқтық ұғымы алдау немесе сенімді теріс пайдалану жолымен бөтеннің мүлкін жымқыру немесе бөтен мүлікке құқықты иемденуді білдіреді. Ал осы баптың 2-бөлігінің 4) тармағы "ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен" саралау белгісін қамтиды [15].

Осылайша отандық заңнама интернет-алаяқтықтың диспозициясын "ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен бөтеннің мүлкін жымқыру немесе бөтен мүлікке құқықты иемдену" деп айқындаған.

Қазақстан Республикасы Жоғарғы Сотының "Алаяқтық туралы істер бойынша сот практикасы туралы" 2017 жылғы 29 маусымдағы № 6 нормативтік қаулысында ақпараттық жүйені пайдаланушыны алдау немесе оның сенімін

теріс пайдалану жолымен жасалған алаяқтық деп ақпараттық жүйені пайдаланушыны Qiwi-кошелек, интернет-банкинг және т.б. арқылы алдап өзінің қылмыстық пиғылын іске асыру мақсатында ақпараттық жүйеде көрінеу жалған мәліметтерді немесе бағдарламаларды орналастыру жолымен ақпараттық технологиялар (компьютер, компьютерлік бағдарламалар, интернет, ұялы телефон және т.б.) арқылы жасалған, ақпараттық жүйені пайдаланушының мүлкін немесе мүлікке құқығын иеленуге бағытталған кінәлінің әрекеттерін тану қажет деп көрсетілген [13].

Қылмыстық заңның өзі мен ҚК 6-тарауының атауын (Меншікке қарсы қылмыстық құқық бұзушылықтар) сөзбе сөз түсінсек, интернет-алаяқтықтың объектісіне бөтеннің мүлкі және оған меншік құқығы жатқызылады. Зерттеліп отырған қылмыс түрінің субъектісі жалпыға бірдей, яғни қылмыстық құқық бұзушылық жасаған уақытта он алты жасқа толған есі дұрыс жеке тұлға қылмыстық жауаптылыққа жатады.

Қылмыстың объективті жағы алдау және сенімді теріс пайдаланумен сипатталса, субъективті жағы тікелей пиғылмен және пайдакүнемдік мақсатпен сипатталады.

Мұндай қылмыс үшін мүлкі тәркіленіп, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз, төрт мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір мың сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не төрт жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазалау көзделген [15].

Осындай қылмыс ірі мөлшерде, мемлекеттік функцияларды орындауға уәкілеттік берілген адам не оған теңестірілген адам не лауазымды адам не жауапты мемлекеттік лауазымды атқаратын адам жасаған алаяқтық, егер ол өзінің қызмет бабын пайдалануымен ұштасса, екі немесе одан да көп адамға қатысты, сондай-ақ бірнеше рет жасалса мүлкі тәркіленіп, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан алты жылға дейінгі мерзімге айыра отырып немесе онсыз, үш жылдан жеті жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға, ал 2) тармақта көзделген жағдайларда мүлкі тәркіленіп, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан өмір бойына айыра отырып, жымқырылған мүліктің он еселенгеннен жиырма еселенгенге дейінгі мөлшерінде айыппұл салуға не үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыруға жазаланады [15].

Ал егер қылмыстық топпен немесе аса ірі мөлшерде жасалса мүлкі тәркіленіп, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан он жылға дейінгі мерзімге айыра отырып немесе онсыз, ал осы баптың үшінші бөлігінің 2) тармағында көзделген жағдайларда белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан өмір бойына айыра отырып, бес жылдан он жылға дейінгі мерзімге бас бостандығынан айыруға жазалануы мүмкін [15].

Интернеттің қарқынды дамуы және оның мүмкіндіктерінің кеңеюі, адамдар мен қоғамның күнделікті тіршілігіне жан-жақты енуі қылмыскерлердің де белсенділігінің күшеюіне алып келуде, бұл ретте олар үнемі алдаудың түрлі жолдары мен схемаларын ойлап табуда.

Интернет-қылмыстарды ашу өте қиын, себебі олар көбінесе өңіраралық, тіпті кейде трансшекаралық сипатта болады, яғни жәбірленуші бір аймақта, ал қылмыскер басқа аймақта болады. Төлем жүйелері мен онлайн-платформалардың тез дамуы қылмыскерлерге қашықтан, тіпті шет елдерден әрекет етуге жағдай жасап отыр. Қылмыскерлер үшінші тұлғаларға рәсімделген банктік төлем карточкалар мен абоненттік нөмірлерді қолданады, электрондық ақшаны қолма-қол ақшаға ауыстыру үшін бөгде адамдарды тартады.

Зерттеу барысында Қазақстан Республикасы Бас прокуратурасы жанындағы Құқықтық статистика және арнайы есепке алу комитетінің статистикалық мәліметтерін пайдалана отырып, Республика аумағында және Түркістан облысы бойынша жалпы алаяқтық қылмыстардың, оның ішінде интернетпен байланысты алаяқтық қылмыстардың сандық көрсеткіштеріне динамикалық тұрғыда салыстырмалы талдау жасалды және талдау нәтижесі олардың саны жылдан жылға тұрақты түрде өсіп келе жатқанын куәландырады [3].

Есептік кезең	Республика бойынша		
	Жалпы тіркелген қылмыс саны	Алаяқтық қылмыстар саны	Интернет-алаяқтық қылмыстар саны
2018 жыл	292 286	29 282	
2019 жыл	243 462	32 286	
2020 жыл	163 226	33 653	14 220
2021 жыл	157 884	41 083	21 405
2022 жыл	157 473	43 499	20 569

Жоғарыдағы кестеден байқағандай, Республика бойынша алаяқтық қылмыстар саны соңғы 5 жылда, яғни 2018-2022 жылдар аралығында үздіксіз тек ұлғайып келеді және 2018 жылмен салыстырғанда 2022 жылы 48,5%-ға өскен.

Интернет-алаяқтық бойынша жағдай да өсу қарқынымен сипатталады, бұл ретте статистикалық есепке интернет-алаяқтық бойынша деректер ресми түрде тек 2020 жылдан бері енгізіліп қалыптастырылатынын атап өткен жөн.

Кестеден Республика бойынша соңғы 3 жылда, яғни 2020-2022 жылдар аралығында Республика аумағында интернет-алаяқтық қылмыстар саны 44,6%-ға (2020 жылы 14 220 қылмыс тіркелсе, 2022 жылы – 20 569 қылмыс тіркелген) өскені көрінеді.

Сонымен бірге алаяқтық пен интернет-алаяқтықтардың жалпы қылмыстық құқық бұзушылықтардың ішіндегі үлесі жылдан жылға ұдайы өсіп келеді. Мысалы, 2018 жылы алаяқтық барлық тіркелген қылмыстық құқық бұзушылықтардың небәрі 10% құраған болса, соңғы 2 жылда алаяқтықтың

үлесі 4/1 (2021ж. - 26%, 2022ж. - 27,6%) асып отыр. Ал интернет-алаяқтық қылмыстардың үлесі 2020 жылы небәрі 8,7% құраған болса, 2021-2022 жылдары 13%-дан асқан.

Есептік кезең	Түркістан облысы бойынша		
	Жалпы тіркелген қылмыс саны	Алаяқтық қылмыстар саны	Интернет-алаяқтық қылмыстар саны
2018 жыл	11 031	984	68
2019 жыл	8 309	800	59
2020 жыл	6 004	1 029	226
2021 жыл	5 842	1 474	475
2022 жыл	5 929	1 570	530

Түркістан облысы бойынша жағдайға қатысты статистикалық көрсеткіштердің де ұқсас динамикасы байқалады. Атап айтқанда, тек соңғы 3 жылдың өзінде облыс бойынша интернет-алаяқтық саны екі есе өскен.

Бұдан Республиканың барлық өңірлерінде дерлік алаяқтық бойынша көрсеткіштер мағыналас жағымсыз сипатта екенін болжауға болады.

Қазақстан Республикасында интернетті пайдалану арқылы жасалатын алаяқтық қылмыстардың басым көпшілігін ашу және тергеумен ішкі істер органдары айналысады. Нақтырақ, ҚПК-нің 187-бабының 4-1-бөлігіне сәйкес ҚК-нің 190-бабында (екінші бөлігінде, үшінші бөлігінің 1), 3) және 4) тармақтарында, төртінші бөлігінде) көзделген қылмыстық құқық бұзушылықтар туралы істер бойынша алдын ала тергеуді ішкі істер органдары, ал мемлекетке залал келтірілген жағдайда – экономикалық тергеу қызметі жүргізетіні көрсетілген [4].

Алайда ішкі істер органдарында интернет-алаяқтықты ашу бойынша тиімді тетіктердің болмауы, мүдделі мемлекеттік және мемлекеттік емес ұйымдар арасында өзара іс-қимылдың осалдығы, барлық деңгейдегі жергілікті ішкі істер органдары қызметкерлерінің жұмыс уақыты мен күшінің тиімсіз пайдаланылуы салдарынан интернет-алаяқтық қылмыстардың басым көпшілігі ашылмайды, тергеу барысы созбалаңдыққа салынады.

Есепті кезең	Республика бойынша	
	Алаяқтық бойынша ашу көрсеткіші	Интернет-алаяқтық бойынша ашу көрсеткіші
2020	43,2%	18,1%
2021	35,7%	17,7%
2022	35,5%	20,1%

Жоғарыдағы кестеден интернет-алаяқтықты ашу көрсеткіші 20%-дан аспайтынын және жалпы алаяқтық қылмыстарды ашу деңгейінен екі есе аз екенін көруге болады. Яғни интернет-алаяқтықтарды ашу деңгейі барлық қылмыс түрлерінің ішінде ең төмен көрсеткіш.

Интернет-алаяқтықтар туралы қылмыстық істердің басым көпшілігі ашылмауына байланысты сотқа істер сирек жіберіледі.

Сәйкесінше, жәбірленушілерге келтірілген залал негізінен өтелмейді, ал қылмыскерлер жауаптылықтан жалтарады. Бұл, өз кезегінде, халықтың жалпы құқық қорғау органдарына сенімсіздігін тудырып, беделін төмендетеді.

Мысалы, Түркістан қаласының прокуратурасы Түркістан қалалық полиция басқармасының (бұдан әрі - Басқарма) алаяқтық қылмыстарды ашу және тергеу жұмысының заңдылығы мен тиімділігіне талдау жүргізу нәтижесі бойынша Түркістан облысының полиция департаментіне (бұдан әрі - Департамент) енгізген ұсынуда (14.02.2023ж. №2-12-23-00462) соңғы жылдары алаяқтық қылмыстарын ашу деңгейі жылдан жылға төмендеп келе жатқаны көрсетілген.

Атап айтқанда, 2022 жылы 76 қылмыстық іс (2021ж. - 46, 2020ж. - 37, 2019ж. - 15) бойынша күдікті тұлғалар анықталмай, сотқа дейінгі тергеп-тексерудің мерзімі ҚПК-нің 45-бабы 7-бөлігінің 1-тармағымен үзілген. Алаяқтардың әрекеттерінен тек 2022 жылы 112 адамға 59,3 млн. теңге материалдық залал келтірілсе, оның тек 8,1 млн. теңгесі нақты өндірілген [16].

Мысалы, Басқармаға Түркістан қаласының тұрғыны Д.С. деген азаматша арызданып, 18.05-29.05.2022 күндері аралығында өздерін "Ұлттық банк" қызметкерімін деп таныстырған бейтаныс адамдар ұялы телефон арқылы хабарласып, сеніміне кіріп, бірнеше банктен несие алдыртып, жалпы сомасы 16 552 000 теңге материалдық шығын келгенін көрсеткен. Аталған факт бойынша 04.06.2022ж. ҚК 190-бабы 4-бабының 2-бөлігімен сотқа дейінгі тергеп-тексеру басталған. Қылмысты ашу мақсатында Басқарма Департаменттің Криминалдық полиция басқармасының «К» тобының қызметкерлерімен бірлесіп жедел-тергеу тобы құрылған.

Тексеру барысында жәбірленушінің ұялы телефонына хабарласқан 4 қазақстандық абоненттік нөмірлер тексеріліп, алайда қылмыстық іске маңызы бар ақпарат алынбаған. Банктерге сұрау хаттар жіберу арқылы жәбірленуші Д.С. ақша қаражатын келесі есепшоттарға аударғаны анықталған:

- Атырау облысы, Атырау қаласы, Сарықамыс 2 м.а., 8/2 үй тұрғыны 01.01.1957 ж.т. Мусиева Насипа Тулегеновағa тиесілі «ForteBank» №4042 4386 0987 8024 есепшотына – 2 500 000 теңге аударылған.
- Жетысу облысы, Ескелді ауданы, Жалғызағаш ауылы, Бақтыбай көшесі №27 үй тұрғыны 09.06.2000 ж.т. Маратұлы Рахатқа тиесілі «ForteBank» №4042 4389 0362 2451 есепшотына - 2 500 000 теңге аударылған.
- СҚО, Темирязев ауданы, Белоградовка ауылы, Строительная көшесі № 6 үй тұрғыны 22.07.2003 ж.т. Бубнов Максим Викторовичке тиесілі «ForteBank» №4042 4386 0427 5911 есепшотына – 5 827 000 теңге аударылған.
- Астана қаласы, Алматы ауданы, 1 м.а., 14/30 үй тұрғыны 07.01.1988 ж.т. Тасеменов Мирболат Жоламановичке тиесілі «ForteBank» №4042 4387 0002 4114 есепшотына - 700 000 теңге аударылған.

- Жетысу облысы, Талдықорған қаласы, Жастар 28/27 үй тұрғыны 01.02.1998 ж.т. Белгиев Абылай Берікұлына тиесілі «ForteBank» №4042 4386 0514 7358 есепшотына - 1 822 000 теңге аударылған.
- Жетысу облысы, Талдықорған қаласы, Қожабергенова №6 үй тұрғыны 16.07.2002 ж.т. Құрманғали Марлен Берікұлына тиесілі «ForteBank» №4042 4386 0981 2858 есепшотына - 1 000 000 теңге аударылған.
- Астана қаласы, Есіл ауданы, Күлтегін көшесі №14/253 үй тұрғыны 26.04.1971 ж.т. Турсынбеков Марат Бековичке тиесілі «HalykBank» №4405 6398 1049 7824 есепшотына - 1 900 000 теңге аударылған.

Қылмысты ашу мақсатында жоғарыда аталған тұлғаларға қатысты екінші деңгейлі банктерге сұрау хаты жолданып, мәліметтері қылмыстық іске біріктірілді. Әрі қарай қызметкерлер іс-сапарға жолданып, жоғары аталған тұлғаларды полицияға жеткізіп, іс бойынша жауап алынды.

Нәтижесінде жоғарыда аталған әрбір тұлға жеңіл әрі оңай ақша табу мақсатында интернет жүйесімен «Telegram» мессенджері арқылы белгісіз тұлғаға *(ID:5014785358 - @plystoketpo)* өздерінің жеке банктік есепшоттарын белгіленген сомаға сатып жібергендігі анықталды.

«Telegram» мессенджерінде ID:5014785358 - @plystoketродеректерімен тіркелген белгісіз тұлғаны, яғни аккаунт иесін анықтау мүмкін болмады.

Екінші деңгейлі банктердің мәліметіне сәйкес жәбірленушінің қаражаты - 16 552 000 теңге BINANCE – цифрлық валютаны айырбастыру (аудару) онлайн-сервисы арқылы Ресей Федерациясының азаматы 1999ж.т. К.Н.Головатюкке жолданғаны анықталған.

Нәтижесінде 04.08.2022ж. ҚПК 45-бабы 7-бөлігінің 1-тармағы негізінде сотқа дейінгі тергеп-тексеру мерзімін үзу туралы шешім қабылданған.

1.2 Интернет-алаяқтық қылмыстардың негізгі түрлері мен тәсілдері, жедел-іздестіру және тергеу іс-шараларының тактикалық ерекшеліктері

Қазіргі заманның үрдісіне байланысты барлық онлайн-платформалар мен ақпараттық жүйелер мобилді форматқа ауысқандықтан соңғы жылдары интернет-алаяқтық жасау үшін қылмыскерлер бұрынғыдай компьютер емес, негізінен мобилді телефондар пайдаланады.

Интернет-алаяқтық фактілері бойынша жедел-тергеу практикасы мен қылмыстық істердің материалдарын зерделеу нәтижесінде ақша қаражатын жымқыру тәсілі бойынша тергеудің бастапқы сатыларында жиі қалыптасатын мынадай жағдайлар айқындалды:

1) ақша қаражаты алаяқтың талабы бойынша жәбірленуші оған өзінің дербес деректерін ұсынғаннан кейін жәбірленушінің есепшотынан шешіледі;

2) ақша қаражаты алаяқтың талабы бойынша нақты бір жеке тұлғаның атына тіркелген банктік есепшотқа немесе басқа онлайн төлем жасау жүйелері (QIWI, Каспи) арқылы белгілі бір мобилді телефон нөміріне аударылады;

3) ақша қаражатын жәбірленуші курьер немесе басқа да бір адам арқылы беріп жібереді;

4) алаяқ жәбірленушінің дербес деректерін пайдалану арқылы микроқаржы ұйымдарында микрокредит рәсімдейді;

5) алаяқ ұялы телефон арқылы жәбірленушінің ұялы телефонына қоңырау шалады немесе SMS жібереді, содан банк, коммерциялық ұйым немесе жарнама компаниясының қызметкері ретінде танысып, жәбірленушіге оның атына ірі "ұтыс" (автокөлік, тұрмыстық техника, туристік жолдама және т.б.) шыққанын хабарлайды және жәбірленушіге сыйлықты алу немесе жеткізу үшін белгілі бір көлемде ақша қаражатын (салық, аванс, жеткізу төлемі және т.б. ретінде) өзі көрсеткен есепшотқа аударуды ұсынады;

6) алаяқ ұялы телефон арқылы жәбірленушінің ұялы телефонына қоңырау шалу немесе SMS жіберу арқылы жәбірленушіге оның банктік есепшоты немесе мобилді телефон нөмірінің шоты бұғатталғаны жөнінде хабарлайды және өзін банк немесе ұялы байланыс операторының қызметкері ретінде таныстырып, оны шешу үшін банкоматта немесе төлем терминалында не мобилдік қосымшада (Kaspi, Homebank және т.б.) белгілі бір комбинацияны теруді ұсынады.

Осындай қарапайым әрекеттердің нәтижесінде ақша алаяқтың немесе оның таныстарының шотына аударылады.

Сонымен қатар негізінен қылмыс субъектілерінің сипаттамасы бойынша интернет-алаяқтықтың бірнеше түрін атап өтуге болады:

1) бостандықта жүрген қылмыскерлер жасаған;

2) бас бостандығынан айыру орындарына жазасын өтеп жатқан қылмыскерлер жасаған.

«Телефон алаяқтығын» ұйымдастыруда бірнеше қылмыскер қатысады және осындай топтарға Қылмыстық-атқару жүйесі комитетінің (бұдан әрі - ҚАЖК) мекемелерінде жазасын өтеуші адамдар кіреді. Олар негізінен заңсыз алынған SIM-карталарды пайдалана отырып, құрбандарымен хабарласу үшін телефон шалады немесе қысқа мәтінді хабарлама (SMS) жібереді, бұл ретте қылмыскерлер әртүрлі өңірлерден, тіпті шет елдерден де хабарласады.

Бастапқы кезеңде осы санаттағы қылмыскер туралы деректерді анықтау өте қиын. Әдетте, алаяқтарды қарым-қатынас тәсілі және жеке мәліметтерге, төлем карталарының деректеріне қызығушылық танытуынан білуге болады. Мұның барлығы алдау әдісіне байланысты.

ҚАЖК мекемелерінің лауазымдары тұлғаларының әрекетсіздігі салдарынан осы мекемелерде қылмыстық жазасын өтеуші адамдардан тұратын интернет және телефон алаяқтығын жүйелі жолға қойған қылмыстық топтар әрекет етуде. ҚАЖК мекемелері қауқарсыз, толық тосқауыл қоюға мүдделік танытпауда. ҚАЖК 2012 жылдан бері қайтадан ІІМ құрамына қосылғанына қарамастан мәселе толық шешілмеуде. Мобилді телефондар өткізуге жол бермеу үшін біршама шаралар атқарылғанымен мәселе толық шешілмеген

Жалпы алғанда, көп жағдайда зиянкестердің екі тобы басты назар аударады:

- ұзақ мерзімді жұмысы мен тұрғылықты жерінен айырылған адамдар, алаяқтық немесе басқа да мүлікке қарсы құқық бұзушылықтар үшін бірнеше рет сотталғандар;

- кішігірім алаяқтық жасайтын алаяқ-рецидивистер, негізінен олардың құрбандары таныс адамдары болып келеді.

Құқық бұзушылық жасау мотивіне қарай интернет-алаяқтың жеке басын классификациялауың/жіктеудің бірнеше тәсілдері бар. В.Б.Вехов ұсынған жіктеуде интернет-алаяқтың жеке басы келесідей бөлінеді:

1) ақпараттық технологиялар мен бағдарламалау саласындағы жақсы білім мен дағдыларды біріктіретін, сондай-ақ мамандыққа деген адалдық пен жаңа схемаларды ойлап табуға бейімділікті көрсететін кәсібилігі және құзыреттілігімен ерекшеленетін субъектілер. Оларда қоғамға қарсы ниеттердің нақты көрінісі жоқ, оларды көбінесе бастапқы кезеңде зиянкестер пайдалануы мүмкін;

2) интернетке тәуелділігі бар тұлғалар;

3) интернет-алаяқтықпен мақсатты түрде айналысатын, айқын пайдакүнемдік пиғылы бар хакерлер. Олар қылмыстық құқық бұзушылықтарды қайталап жасаумен ерекшеленеді, айтарлықтай сендіру және көндіру, сондай-ақ қылмыстардың іздерін жасыру дағдыларына ие;

4) технология саласында елеулі кәсіби біліктілігі жоқ, тек әлеуметтік желілер мен интернетте тұтынушылық сипатта игерген қарапайым адамдар [17].

Алаяқтық жолмен жымқырылған ақша қаражаты әртүрлі тәсілмен алынады.

Интернет-алаяқтық жасау тәсілдері көп және әр алуан болып келеді. Бұл, бірінші кезекте, ақпараттық технологиялар саласында көрсетілетін қызметтер санының жылдам өсуі және сапасының ұдайы дамуымен байланысты.

Интернет-алаяқтық қылмыстарды жасаудың ең кең тараған танымал тәсілдеріне фишинг, вишинг, киберсквоттинг, тайпсквоттинг жатады.

Бұл ретте Интернет желісіндегі қылмыстың нысанасы қолма-қол ақша қаражаты емес, виртуалды, яғни банктік карточкалардың, шоттардың деректері, төлем жүйелері арқылы ақша қаражатын аударымдар. Ақша қаражаты аударылған жағдайда аляқтар жәбірленушімен тікелей жанаспайтындықтан қылмыскерді анықтап табу ықтималдығы аз.

Қолда бар интернет-алаяқтықтарды тергеу әдістемелері бұрын қылмыскерлерді әшкерелеуге мүмкіндік беретін. Алайда қазіргі уақытта олар тиімсіз болып отыр, себебі қылмыстың осы түрлерінің қылмыстық-құқықтық, криминалистикалық және криминологиялық сипаттамалары айтарлықтай өзгерген.

Алғашқы жедел-іздестіру іс-шаралары мен тергеу әрекеттері, оларды жүргізу тәртібі қылмыстың із суытпай ашылу-ашылмауына, алаяқтың анықталып ұсталу-ұсталмауына қарай қарастырылады. Көп жағдайларда интернет-алаяқтық оқиғасы туралы қылмыстық қудалау органына біршама

уақыт өткеннен кейін хабарланады және арыз түскен кезде интернет-алаяқтықты кім жасағаны мүлдем белгісіз болады.

Қылмыстың осы түрін тергеу сапасын көтеру үшін процестік және процестік емес әрекеттерді бірлесіп жоспарлау қажет.

1. Интернет-алаяқтық туралы арыз немесе хабарлама түскен кезде арызданушыдан егжей-тегжейлі жауап алу, жауап алу кезінде қылмыскердің қай уақытта, қандай абоненттік нөмірден қоңырау шалғанын, қанша рет қоңырау шалғанын, өзін кім болып таныстырғанын, не айтқанын, қандай әрекеттер жасауды ұсынғанын, оған қандай сомада ақша қаражатын және қандай қызметтер үшін аударуды сұрағанын, ақша қаражатын жіберу тәсілін (блиц-аударым, қолма-қол, мобилді телефон нөміріне аудару және т.б.), қылмыскерді дауысынан таныған-танымағанын, дауысын сипаттап беру мүмкіндігін анықтау. Егер ақша қаражаты делдал арқылы қолма-қол берілген жағдайда оның сыртқы келбетін сипаттап беруді ұсынып, кейін оның көмегімен фотопортретін жасау;

2. Шұғыл ішкі істер органының барлық сыртқы қызметтерін жұмылдыру;

3. "Телефон алаяқтығы" туралы хабарлама түскен жағдайда тергеуші немесе жедел қызметкер дереу абоненттік нөмірдің қай ұялы байланыс операторға тіркелгенін, иесін, қай жерде орналасқанын анықтау;

4. Осы абоненттік нөмірден шығыс-кіріс қоңыраулардың биллингін жасау, тиісті абоненттердің иелерінің аты-жөндері мен жеке басы туралы мәліметтерді анықтап, оларды жеткізу және жауап алу;

5. Қылмыстық іс бойынша қызықтыратын абонент туралы қосымша деректер алу мақсатында тергеуші абонент туралы, ал қажет болған жағдайда, телефонмен сөйлесулер туралы ақпарат алу немесе телефонмен сөйлесулерді бақылау және жазу жүргізу жөнінде қаулы шығарады. Ұялы байланыс операторынан алынған ақпараттарды талдау тергеуге белгісіз қылмысқа қатыстылығы бар адамдарды, жәбірленушілер мен куәлерді анықтауға мүмкіндік береді. Ол адамдардан жауап алу.

6. Егер ақша Қазақстан Республикасының екінші деңгейлі банктері арқылы аударылған болса:

- қандай жағдайда аударым жасалғанын, жәбірленушінің қылмыскерге қандай дербес деректерді хабарлағанын анықтау. Жәбірленушіден жасалған аударымға қатысты құжаттардың бар-жоғын сұрату, оларға алу және қарау жүргізу, дәлелдеме ретінде танып іс материалдарына тіркеу;

- банктерден қылмыстық іс бойынша фигурантқа түскен ақша аударымдары, олардың әрі қарай қозғалысы, егер қолма-қол шешіп алған болса банк бөлімшесінің немесе банкоматтың атауы мен мекенжайы туралы ақпарат алу, сондай-ақ бейнебақылау камераларынан жазбаларды алу;

- ақша қаражатын алушы адам анықталған жағдайда оның соттылығы туралы мәліметтерді тексеру, сипаттаушы материалдар жинақтау, бейнетүсірілім жүргізу арқылы ақша қаражатын алудың мән-жайлары бойынша жауап алу, дауыс үлгілерін алу және оны жәбірленушіге тану үшін ұсыну, қажет болған жағдайда сараптама тағайындау; туысқандары мен қарым-

қатынастағы басқа жақын адамдарды анықтау, олардың ішінде ұқсас қылмыстар үшін соттылығы бар немесе жазасын өтеп жатқандардың бар-жоғын тексеру; анықталған адамдардың бұрын жасалған басқа қылмыстарға қатыстылығын тексеру;

7. Ұялы байланыс операторынан ақпараттар алынғаннан кейін:

- жәбірленушіге қоңырау шалынған мобилді нөмір тіркелген адамды анықтап жауап алу, телефонына қарау жүргізу, қажет болған жағдайда алу жүргізу, дауыс үлгілерін алу және оны жәбірленушіге тану үшін ұсыну, қажет болған жағдайда психофизиологиялық зерттеу тағайындау;

- егер мобилді нөмір тіркелген адам ол нөмірді өз атына рәсімдемегенін көрсетсе, ұялы байланыс операторынан тиісті құжаттарды алдырып, қолтаңба сараптамасын тағайындау;

- туысқандары мен қарым-қатынастағы басқа жақын адамдарды анықтау, олардың ішінде ұқсас қылмыстар үшін соттылығы бар немесе жазасын өтеп жатқандардың бар-жоғын тексеру; анықталған адамдардың бұрын жасалған басқа қылмыстарға қатыстылығын тексеру;

8. Егер ақша қаражаты мобилді нөмірге немесе электронды әмиянға (Каспи, Web Money, Яндекс деньги, QIWI) жіберілген болса:

- электронды әмиянды әкімшілендіруді жүзеге асыратын ұйымға иесінің тіркеу мәліметтерін, жүйеге кіру және транзакциялар журналдарынан үзінділер, жүйеге кіру жүзеге асырылған IP-мекенжайы жөнінде деректер беру туралы сұрау хат жолдау;

- электронды әмиян тіркелген адамды анықтап жауап алу, дауыс үлгілерін алу және оны жәбірленушіге тану үшін ұсыну, қажет болған жағдайда психофизиологиялық зерттеу тағайындау;

-туысқандары мен қарым-қатынастағы басқа жақын адамдарды анықтау, олардың ішінде ұқсас қылмыстар үшін соттылығы бар немесе жазасын өтеп жатқандардың бар-жоғын тексеру; анықталған адамдардың бұрын жасалған басқа қылмыстарға қатыстылығын тексеру;

9. Егер ақша қаражаты қолма-қол берілген жағдайда:

- арызданушының қатысуымен ақша берілген адамның субъективті портретін құрастыру;

- ақша берілген орында сыртқы бақылау камераларының бар-жоғын, бар болса бейнежазбаларды қарау және алу, қажет болған жағдайда дәлелдеме ретінде тану және іс материалдарын тіркеу;

10. Сотқа дейінгі тергеп-тексеру барысында алынған барлық құжаттар мен заттарды ҚПК талаптарын сақтай отырып іс материалдарына тіркеу.

2. ИНТЕРНЕТ-АЛАЯҚТЫҚҚА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕ

2.1 Интернет-алаяқтыққа қарсы іс-қимыл мәселелерін регламенттейтін негізгі халықаралық актілер

Интернет-алаяқтық қылмыстарына тиімді қарсы іс-қимыл проблемасын тек бір мемлекеттің күшімен шешу мүмкін емес, себебі интернет-қылмыскерлерде шекаралық шектеу болмайды, олар қылмысты қандай да бір мемлекеттен тыс жерде отырып жасай береді.

Біріккен Ұлттар Ұйымы (бұдан әрі - БҰҰ) интернеттің көмегімен жасалатын ақпараттық-техникалық құқық бұзушылықтарды жаһандық және халықаралық деңгейдегі проблема деп танып отыр.

Ақпараттық-коммуникациялық технологиялар саласындағы қылмыстар ғаламдық және трансұлттық сипатта болуы халықаралық ынтымақтастықты оларға қарсы іс-қимылдың тиімді шараларын қабылдаудың басты факторы ретінде айқындайды [18].

Сондықтан Е.М.Якимова мен С.В.Нарутто атап өткендей, трансшекаралық қылмыстармен күресте - оларға киберқылмыстардың басым бөлігін жатқызуға болады - мемлекет ерекше рөл атқарады және әртүрлі елдердің құқық қорғау органдарының тек дұрыс үйлесімді жұмысы бұл саладағы қылмыстардың санын азайтуға мүмкіндік береді [19].

Мысалы, ақпараттық технологияларды пайдалану арқылы жасалатын қылмыстарды тергеу практикасы онлайн-платформалар мен әлеуметтік желілердің (Telegram, Facebook, Instagram, Whatsapp және т.б.) ресми өкілдерімен өзара іс-қимылдың болмауы өзекті проблемалардың бірі екенін көрсетеді. Қазақстандық құқық қорғау органдары тергеу барысында IP-мекенжайлар мен әлеуметтік желілердің қолданушылары туралы мәлімет алу кезінде қиыншылықтарға тап болуда. Мұндай компаниялардың бас офистері АҚШ, Ресей сияқты шет мемлекеттердің аумағында орналасқандықтан дәлелдемелерді алу тек халықаралық тапсырма жолдау арқылы мүмкін болады.

Жалпы әлемдік қауымдастық осы саладағы қылмыстарға қарсы іс-қимылдың тиімді тетіктерін әзірлеген және кеңінен қолданып келеді деуге негіз бар, дегенмен оларды тұрақты түрде жаңартып дамыту жұмыстары жүргізілуде.

Осы саладағы халықаралық ынтымақтастықтың негізгі мақсаттары:

- тиісті саладағы халықаралық-құқықтық реттеуді жетілдіру;
- халықаралық нормалар мен ұсынымдар негізінде ұлттық заңнаманы үйлестіру;
- мемлекеттердің мүдделерін білдіретін құқық қорғау органдарының қылмыстарды анықтау, тергеу және алдын алу кезіндегі әрекеттерінің бірлігіне қол жеткізу.

Басқа салалардағыдай, мемлекеттердің осы саладағы ынтымақтастығы да конвенциялық (шарттық-құқықтық) және институционалдық (халықаралық ұйымдар шеңберінде) тетіктерге негізделеді [18].

Бүгінгі күні осы салада халықаралық өзара іс-қимылды қамтамасыз ететін басты әмбебап құжатқа Еуропа Одағына қатысушы-мемлекеттер арасында 2001 жылғы 23 қарашада Будапешт қаласында қабылданған Компьютерлік қылмыстар туралы Еуропалық конвенцияны (киберқылмыстар туралы) (бұдан әрі - Будапешт конвенциясы) жатқызуға болады. Будапешт конвенциясы алғашында өңірлік Еуропалық құжат ретінде қабылданғанымен, оның халықаралық ынтымақтастықтың көптеген проблемаларын шешетін ең ауқымды халықаралық актілердің біріне айналуына байланысты оған Еуропа елдерінен бөлек АҚШ, Жапония, ОАР, Грузия, Канада, Аргентина, Израиль, Австралия және т.б. дамыған мемлекеттер қосылған. Жалпы Будапешт конвенциясын 65 мемлекет ратификациялаған [20].

Будапешт конвенциясы құқықтың түрлі салаларына (қылмыстық, қылмыстық-процестік, авторлық, азаматтық, ақпараттық) елеулі ықпал етуге бағытталған нормаларды қамтитын және халықаралық құқықтың негізгі қағидаттарына (адам құқығын құрметтеу, ынтымақтастық және міндеттемелерді адал орындау) негізделген кешенді құжат болып табылады. Оның нормалары негізгі 3 мәселелер жиынтығынреттеуге бағытталған:

- компьютерлік ақпарат саласындағы қылмыстарды қылмыстық-құқықтық баға беруді жақындату;
- осындай қылмыстарды тергеу барысында дәлеледемелердің жинақталуын қамтамасыз ететін ұлттық қылмыстық-процестік шараларды жақындату;
- осындай қылмыстардың шет елдерде жасалуының дәлелдемелерін жинқаталуын қамтамасыз ететін қылмыстық-процестік қызмет саласындағы халықаралық ынтымақтастық [21].

Бұл ретте Будапешт конвенциясы зерттеуіміздің мәні болып табылатын компьютерлік технологияларды пайдалану арқылы жасалатын алаяқтықтарды компьютерлік қылмыстар қатарына жатқызатынын атап өту қажет [20, 25-б].

Будапешт конвенциясы шеңберінде қатысушы-мемлекеттердің аумақтарында құқық қорғау органдарының өзара құқықтық жәрдем көрсету кезінде жалпы тәртіптегі қатынастардан тысжедел байланыс құралдары, оның ішінде факсимилді хабарламалар және электронды пошталар арқылы оңтайлатылған ақпарат алмасу тетігі көзделген [20, 25-б].

Сонымен бірге Будапешт конвенциясы бұрын соңды халықаралық-құқықтық құжаттармен реттелмеген қатынастар тәртібін енгізуді - күнделікті тәулік бойы қолжетімді желі (халықаралық атауы "24/7 Network") құруды ұсынады. Желінің байланыс пункттерінің басты міндеті - осы конвенцияда көзделген құқықтық көмек беру жөніндегі функциялардың өзара жылдам атқарылуын қамтамасыз ету [20, 35-б].

Қазақстан бүгінгі уақытқа дейін Будапешт конвенциясын ратификацияламаған. Дегенмен ІІМ мәліметінше Қазақстанның мүдделі мемлекеттік органдары шетелдік киберқылмысқа қарсы іс-қимыл жөніндегі құқық қорғау органдарымен 2018 жылдан бастап Будаешт конвенциясына Қазақстанның қосылуы жөнінде іс-шараларды талқылау процесінде [22]. Осы

кезге дейін пікіртілас пен келіспеушілік тудырып келген негізгі мәселе - Конвенцияның 32-бабының талабы. Ол кез келген Тараптың өзге Тараптың келісімінсіз компьютерлік жүйенің көмегімен өз аумағынан өзге Тараптың аумағында орналасқан компьютерлік деректерге қол жеткізу құқығын көздейді [20, 32-б].

Будапешт конвенциясына қосылу еліміздің құзырлы органдарының оған қатысушы-мемлекеттік органдардың құзырлы органдарымен өзара іс-қимыл тәртібіне оң ықпал етіп, олармен қажетті мәліметтер және дәлелдемелерді жедел түрде алмасуға мүмкіндік беретіні, сәйкесінше барлық киберқылмыстар мен интернет-жымқыруларға қарсы іс-қимылдың тиімділігі артатыны анық, сондықтан Қазақстанның Будапешт конвенциясын ратификациялауы күн тәртібіндегі өзекті мәселелердің қатарында тұр. Бұл ретте Будапешт конвенциясына қосылу ұлттық заңнамаға қайшы келетін кейбір ережелер мен нормаларды қолданбау жөнінде ескертпе жасау арқылы жүзеге асырылуы мүмкін.

Бұдан бөлек, мағыналас жоғарыдағы себеппен Будапешт конвенциясына қосылмаған Ресей Федерациясы 2021 жылы БҰҰ-ға ақпараттық-коммуникациялық технологиялардың көмегімен жасалатын қылмыстарға қарсы күрес жөніндегі басқа конвенция жобасын әзірлеп ұсынған. Бұл ретте Будапешт конвенциясыныңбіршама ережелері осы жобаны әзірлеу барысында пайдаланылған.

Жобаны әзірлеушілердің айтуынша, бұл құжат ақпараттық-коммуникациялық технологияларды пайдалану саласындағы қылмыстарға қарсы іс-қимылдың тиімді әмбебап тетігі ретінде қарастырылады. Онда Будапешт конвенциясымен салыстырғанда киберқылмыстар құрамын 9-дан 23-ке ұлғайту ұсынылған. Жобаға трансшекаралық сипаттағы және кезек күттірмейтін шұғыл әрекеттерді қажет ететін қылмыстарды тергеу кезінде құқық қорғау органдары жұмысының жылдамдығы мен тиімділігін арттыратын халықаралық ынтымақтастықтың өз тиімділігін растаған тәсілдері мен қазіргі кезде аса өзекті өзара іс-қимылдың шұғыл тетіктері енгізілген. Бұл ретте дербес деректерін қорғау, мемлекеттік егемендік пен адам құқығын құрметтеу мәселелерінде тепе-теңдік сақталған. Куәлерді қорғау, заманауи ақпараттық-коммуникациялық технологияларды, соның ішінде айғақ алу және т.б. процестік әрекеттерді жүргізу үшін видео-конференц байланыс немесе телефондық конференция жүйелерін қолдану бойынша шаралар кешені іске асырылған. Мұндай конвенцияның қабылдануы БҰҰ-ға қатысушы мемлекеттердің адамдарды, қоғамды және бизнесті қорғау бағытында мықты заңнамалық база қалыптастыруға және техникалық әлеуетін арттыруға үлкен серпін береді [23].

Бұлардан басқа, Еуропа Кеңесінің ақпараттық техникалық құқық бұзушылықтар туралы конвенциясы, Жаһандық ақпараттық қауымдастық туралы Окинава хартиясы, Бангкок декларациясы сияқты халықаралық актілер қабылданған.

Тәуелсіз мемлекеттер достастығы (бұдан әрі - ТМД) шеңберінде шарттық-құқықтық ынтымақтастық 2001 жылғы 1 маусымда Минскте қабылданған ТМД-ға қатысушы-мемлекеттердің компьютерлік ақпарат саласындағы қылмыстарға қарсы күрестегі ынтымақтастығы туралы келісімге негізделеді. Келісімге қатысушы мемлекеттер - Әзірбайжан, Армения, Беларусь, Қазақстан, Қырғызстан, Молдова, Ресей, Тәжікстан, Өзбекстан, Украина [18].

Қазақстанда Келісім Қазақстан Республикасы Президентінің 2002 жылғы 25 маусымдағы N 897 Жарлығына сәйкес бекітілген [24].

Осы Келісімнің жалғасы ретінде ақпараттық технологиялар саласындағы қылмыстармен тиімді күресті қамтамасыз ету мақсатында 2018 жылғы 28 қыркүйекте Душанбе қаласында ТМД-ға қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісім (бұдан әрі - Келісім) қабылданып, оған жоғарыда аталған мемлекеттерден басқа Түрікменстан қосылды. Келісім елімізде Қазақстан Республикасының 2019 жылғы 9 желтоқсандағы № 277-VI ҚРЗ Заңымен ратификацияланды [25].

Келісім ақпараттық технологиялар саласындағы қылмыстармен күресте қатысушы мемлекеттердің құқық қорғау орғандары ынтымақтастығының құқықтық негізін құруға ұмтылысын білдіреді [25, 2-б].

Келісімге сәйкес қатысушы мемлекеттер 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 [25, 3-б].

Тараптардың құзыретті органдары осы Келісім шеңберінде ынтымақтастықты мынадай:

а) ақпарат алмасу, оның ішінде:

ақпараттық технологиялар саласында дайындалып жатқан немесе жасалған қылмыстар және оларға қатысы бар жеке және заңды тұлғалар туралы;

көрсетілген саладағы қылмыстардың алдын алу, анықтау, жолын кесу, ашу және тергеп-тексеру нысандары мен әдістері туралы;

ақпараттық технологиялар саласында қылмыстарды жасау тәсілдері туралы;

Тараптардың ақпараттық технологиялар саласындағы қылмыстардың алдын алу, анықтау, жолын кесу, ашу және тергеп-тексеру мәселелерін реттейтін ұлттық заңнамасы мен халықаралық шарттары туралы ақпарат алмасу;

б) сұрау салушы Тараптың азаматына қатысты не сұрау салушы Тараптың аумағында жасалған қылмыстардың алдын алуға, анықтауға, жолын кесуге, ашуға және тергеп-тексеруге ықпал етуі мүмкін ақпаратты алуға жәрдем көрсету, жедел-іздестіру іс-шараларын жүргізу туралы сұрау салуларды орындау;

в) ақпараттық технологиялар саласындағы қылмыстардың алдын алу, анықтау, жолын кесу, ашу және тергеп-тексеру бойынша үйлестірілген іс-шаралар мен операцияларды жоспарлау және жүргізу;

г) кадрларды даярлауға және олардың біліктілігін арттыруға, оның ішінде мамандарды тағылымдамадан өткізу, конференциялар, семинарлар және оқу курстарын ұйымдастыру арқылы жәрдем көрсету;

д) ақпараттық технологиялар саласындағы қылмыстардың алдын алу, анықтау, жолын кесу, ашу және тергеп-тексеру жөніндегі міндеттерді орындауды қамтамасыз ететін ақпараттық жүйелер мен бағдарламалық өнімдер жасау;

е) ғылыми зерттеулер жарияланымдарымен және нәтижелерімен алмасу, сондай-ақ өзара қызығушылық туғызатын ақпараттық технологиялар саласындағы қылмыстармен күрес проблемалары бойынша бірлескен ғылыми зерттеулер жүргізу;

ж) ақпараттық технологиялар саласындағы қылмыстармен күрес жөніндегі нормативтік құқықтық актілермен, ғылыми-техникалық әдебиетпен алмасу;

з) өзара іс-қимыл жасау және тәжірибе алмасу шеңберінде ақпараттық технологиялар саласындағы қылмыстардың алдын алуда, анықтауда, жолын

кесуде, ашуда және тергеп-тексеруде пайдаланылатын бағдарламалық өнімдермен және шешімдермен алмасу;

и) компьютерлік жүйелерде сақталатын деректердің сақталуын шұғыл қамтамасыз ету туралы сұрау салуды орындау нысандарында;

к) басқа да өзара қолайлы нысандарда жүзеге асырады [25, 5-б].

Бұл ретте Келісім шеңберіндегі ынтымақтастық құзыретті органдардың жәрдем көрсету туралы сұрау салулары негізінде жүзеге асырылады. Егер ақпарат көрсетілген құзыретті органның мүддесін білдіреді деп пайымдауға негіздер болса, ол екінші тараптың құзыретті органына сұрау салусыз берілуі мүмкін [25, 6-б].

Сонымен бірге институционалды деңгейде БҰҰ, Еуропа Кеңесі, Экономикалық ынтымақтастық және даму ұйымы (ЭЫДҰ), Интерпол, Европол, Евроюст сияқты халықаралық ұйымдар осы саладағы қылмыстармен күресте бірыңғай тәсілдерді қалыптастыруда және халықаралық іс-әрекеттерді үйлестіруде маңызды рөл атқарады. Мысалы, ЭЫДҰ халықаралық масштабта алғаш рет киберқылмыстылық проблемалары мен оған қарсы күрестің қылмыстық-құқықтық шараларын жан-жақты зерттеуді жүргізіп, онда киберқылмыстар үшін қылмыстық жауаптылықты көздейтін нормаларды үйлестіру мүмкіндігін талдаған және компьютерлік қылмыстың криминологиялық анықтамасын жасаған. Ал Интерпол жұмыс айналымына компьютерлік қылмыстардың және оларды жасау әдістерінің кодификаторын енгізді [18].

Бұдан басқа, 2004 жылы Қазақстан экономикалық қауіпсіздікті қамтамасыз ету және қаржылық тұрақтылық қатерлеріне жол бермеу мақсатында Ақшаны жылыстатуға қарсы күрестің қаржылық шараларын әзірлеу тобының (бұдан әрі - ФАТФ)өңірлік тобы - Қылмыстық кірістерді заңдастыруға және терроризмді қаржыландыруға қарсы іс-қимыл жөніндегі еуразиялық топтың (бұдан әрі - ЕАТ) құрылтайшыларының бірі болды [26].

Оның негізгі қызмет бағыттары өңірлік деңгейдегі тиімді өзара іс-қимыл мен ынтымақтастықты қамтамасыз ету, сондай-ақ ЕАТ-қа мүше мемлекеттер деңгейінде халықаралық ылмыстық жолмен алынған қаражатты заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл (бұдан әрі - КЖ/ТҚҚІ) жүйесіне интеграциялану болып табылады.

Халықаралық сапа және қауіпсіздік стандарттарына жауап беретін қаржылық мониторинг субъектілерінің деректерін жинау мен өңдеудің бірегей ақпараттық жүйесі құрылды.

2011 жылы Қазақстан "Эгмонт" қаржылық барлау бөлімшелері тобының толыққанды мүшесі болды, бұл шет мемлекеттердің қаржылық барлау бөлімшелерімен өзара іс-қимылдың тиімділігін арттырды. Әлемнің 100-ден астам қаржылық барлау бөлімшелерімен белсенді ақпарат алмасу басталды.

2.2 Шетел мемлекеттерінің құқық қорғау органдарының интернет-алаяқтық қылмыстарды ашу және тергеу қызметінің ұйымдық-құқықтық аспектілері

Көптеген дамыған мемлекеттер киберқауіпсіздік проблемасына, соның ішінде ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатын жымқыруларды тергеп-тексеруге баса мән береді.

Киберқылмыстармен күрес саласында дамыған шетел мемлекеттерінің ішінде Корея Республикасының озық тәжірибесі өте қызықтырады. Мұнда Корея Республикасы Бас прокуратурасының құрамында 2012 жылы құрылған Киберқауіпсіздік орталығы (Prosecutor's Cybersecurity Center) бар. Прокуратура құрамында киберқауіпсіздік қызметін ұйымдастыру тәсілі іс жүзінде өзінің тиімділігін көрсеткен, себебі осы орталық құрылғаннан бері киберқауіпсіздікке нұқсан келтіретін елеулі оқиғалар орын алмаған. Орталық - бұл ақпараттық жүйелер мен киберқауіпсіздік жүйелерін мониторингілеу орталығы (электронды журналдарды талдау және оқиғаларды байланыстыру, вирустық белсенділікті, ақпараттың таралып кетуін болдырмау құралдарын және басқа да оқиға көздерін талдау) [27].

Израилде Жалпы қауіпсіздік қызметінің (ШАБАК) жанынан ақпараттық қауіпсіздік бөлімі құрылған, ал 2011 жылы Ұлттық Киберқауіпсіздік бюросы құрылған.

Қытай Халық Республикасында телекоммуникациялық алаяқтықтың өсіп кетуіне байланысты 2015 жылы ҚХР Қоғамдық қауіпсіздік министрлігінің құрылымында Телекоммуникация саласында алаяқтыққа қарсы орталықтар құрылған. Алаяқтықтың мұндай түрлері бойынша тар мамандану оларды ашуға және тергеуге баса назар аударып, алаяқтықтың нақты түрлері бойынша практика (қарсы іс-қимылдың әдістері, тәсілдері мен нысандары) жинақтап қалыптастыруға және халықтың виктимизациялану деңгейін азайту үшін ақпараттық-түсіндіру және басқа да профилактикалық іс-шараларды дұрыс ұйымдастыруға мүмкіндік береді.

Ұқсас ұлттық киберқауіпсіздік орталықтары Германия (NCAZ), АҚШ (NCSC), Ұлыбритания (NISCC) сияқты тағы басқа елдерде бар.

Будапешт конвенциясының талаптарын орындау мақсатында Грузияда 2012 жылы Криминалдық полиция департаментінде киберқылмысқа қарсы іс-қимыл ететін арнайы бөлімше құрылған, оның құрамында техникалық бөлім мен тергеу бөлімі бар. Техникалық бөлім қызметкерлері білімі бойынша ақпараттық-техникалық саланың мамандары болып табылады, олар қылмыстарды әшкерелеу және ашумен, сондай-ақ тергеу бөлімінің тергеушілеріне әдістемелік тұрғыда жәрдемдесумен айналысады. Ал тергеу бөлімі әрекеттердің құқықтық саралауын жүзеге асырады. Бөлімшелердің жұмыс режимі - 24/7 (Contact point - Будапешт конвенциясының ұсынымы).

Чехия Республикасында Кибеқылмыстарды тергеу саласында құқық қорғау органдарының әлеуетін дамыту тұжырымдамасы әзірленіп, Ұлттық қауіпсіздік кеңесімен бекітілген. 2016 жылы Ұйымдасқан қылмыспен күрес агенттігі құрылып, оның құрамына Киберқылмысқа қарсы іс-қимыл тобы енген. Топтың функциясына үйлестіру және тәулік бойы техникалық қолдау көрсету

(24/7 Contact point), қылмыстарды әшкерелеу және тергеу, осы салада халықаралық өзара іс-қимыл мен ғылыми-білім беру қызметін жүзеге асыру кіреді. Құрамына 250 полицейлер (тергеушілер) мен IT-мамандар кіреді. Агенттіктің 14 өңірлік басқармалары бар, олардың құрамына киберқылмыстарға қарсы іс-қимыл бөлімдері кіреді.

Осылайша, жоғары көрсетілген мысалдардан халықаралық тәжірибеде киберқауіпсіздік және кибержымқыруларға қарсы іс-қимыл бағытында құқық қорғау қызметін мамандандыру үрдісіне басымдық беріліп отырғанын анық байқауға болады.

Соынмен қатар интернет-алаяқтыққа қарсы іс-қимылдың тиімділігін арттыруда қаржылық барлау жүйесіндегі халықаралық және отандық озық тәжірибелерді зерттеу және тәжірибеге енгізу маңызды.

Қаржылық барлау бөлімшесінің талдамалық материалдарының жоғары сапасы КЖ/ТҚҚІ жүйесі тиімділігінің негізгі факторы болып табылады.

Ұлыбритания, Германия, Грецияның қаржылық барлау бөлімшелері өз функцияларын орындау үшін құқық қорғау, салық органдарының, қаржы ұйымдарының дерекқорларына, оған қоса жылжымайтын мүлік объектілерінің, көлік құралдарының, жер учаскелерінің және т.б. тізілімдеріне қол жеткізе алады. Бұдан басқа, Еурополдың, Интерполдың, Еуроәділеттің мәліметтеріне, сондай-ақ коммерциялық дерекқорларға (World Check, Dow Jones) қол жеткізе алады [26].

КЖ/ТҚ тәуекелдерін талдау сапасын арттыруға IT-құралдарын пайдалану да ықпал етеді. ФАТФ-ның КЖ/ТҚҚІ стандарттарына сәйкестікті қамтамасыз ету кезінде жаңа технологияларды енгізу жөніндегі зерттеуінің нәтижелері жасанды интеллекттің, қолданбалы бағдарламалау интерфейстерінің және субъектілер клиенттерді тиісінше тексеру мақсаттары үшін пайдаланатын құралдардың ең жоғары әлеуеті бар екенін көрсетті. Бразилияның Орталық банкі реттеушілік қызметтің тиімділігін арттыру үшін табиғи тілді өңдеу жобасын мақұлдады. Жобада КЖ/ТҚ туралы күдікке байланысты ақпаратты алу мақсатында әлеуметтік желілер мен өзге де жалпыға бірдей қолжетімді деректерді сканерлеу мен талдауға арналған құралдарды әзірлеу көзделеді [26].

Өз кезегінде, мұндай практикаларды Қазақстанның тек қана қаржылық барлау емес, ішкі істер органдарының қызметінде қолдану талдамалық жұмыстың тиімділігін айтарлықтай арттыруға мүмкіндік беретіні сөзсіз.

3. ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ІШКІ ІСТЕР ОРГАНДАРЫНЫҢ ИНТЕРНЕТ-АЛАЯҚТЫҚҚА ҚАРСЫ ІС-ҚИМЫЛ ЖӨНІНДЕГІ ҚЫЗМЕТІН ЖЕТІЛДІРУДІҢ НЕГІЗГІ БАҒЫТТАРЫ

3.1 Ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметінің қазіргі жай-күйі мен құқықтық регламенттелуі

Қазақстан Республикасының ішкі істер органдары адамның және азаматтың өмірін, денсаулығын, құқықтары мен бостандықтарын, қоғамның және мемлекеттің мүдделерін құқыққа қарсы қолсұғушылықтан қорғауға, қоғамдық тәртіпті сақтауға және қоғамдық қауіпсіздікті қамтамасыз етуге арналған құқық қорғау органы болып табылады [8].

Заңның 4-бабында Қазақстан халқына қызмет етуге тиісті ішкі істер органдары қоғамдық қауіпсіздікті қамтамасыз ету мақсатында жүзеге асыруға тиіс міндеттердің бірі ретінде қылмыстылықпен күрес айқындалған [8].

Аталған заңнамалық міндеттерін жүзеге асыра отырып, ІІМ интернет-алаяқтыққа қарсы іс-қимыл бағытындағы жұмысын негізінен басқа құқық қорғау және мемлекеттік органдармен бірлесе отырып атқарады.

Интернет-алаяқтыққа қарсы іс-қимыл мәселелері Қазақстан Республикасы Бас Прокурорының төрағалығымен үнемі Заңдылықты, құқықтық тәртіпті және қылмысқа қарсы күресті қамтамасыз ету жөніндегі үйлестіру кеңесінде қаралып, осы саладағы жұмыстың тиімділігін арттыруға бағытталған ұсынымдар мен шешімдер қабылданады. Мүдделі мемлекеттік және құқық қорғау органдарының өкілдері құрамына кіретін ведомствоаралық жұмысшы топтар құрылған, іс-шаралар жоспарлары әзірленіп іске асырылуда, әдістемелік құралдар әзірленген.

Қаржы мониторингі агенттігі әлеуетті қаржы пирамидаларын ерте анықтау тетігін енгізді. Қаржы пирамида сайттарына 680 сілтеме бұғатталған. Банктер операциялардың күшейтілген мониторингіне және күдікті клиенттермен іскерлік қатынастарды бұзуға бағытталған. Осындай 149 тұлғамен іскерлік қатынастар орнатудан бас тартылды. Мысалы, «Kaspi Bank» АҚ 40 салымшыны тартып үлгерген «Қара қазандық» қаржы пирамидасының ұйымдастырушыларына қызмет көрсетуді тоқтатты (залал толығымен өтелді).

Қаржы нарығын реттеу және дамыту агенттігі ІІМ бастамасы бойынша микрокредиттерді электронды тәсілмен беру қағидаларына өзгерістер енгізді (аутентификациялаудың қосымша тәсілдері енгізілді).

Ақпарат және қоғамдық даму министрлігі «Metaplatforms» компанияларының өкілдерімен әлеуметтік желілерде бақылауды күшейту, күмәнді жарияланымдар анықталған кезде жедел өзара іс-қимыл жасау, оның ішінде осындай материалдарды жою жөнінде шаралар қабылдау бойынша жұмыс жолға қойылды. Осыған ұқсас жұмыс «Колеса КЗ» онлайн сатукомпаниясымен жүргізілуде.

Қазақстан Республикасының цифрлық даму министрлігі ұялы байланыс операторларымен заңсыз қызметтің жолын кесу жөніндегі ынтымақтастық туралы келісім жасасты (Антифрод бағдарламасы). Осылайша, 2022 жылы осы

жүйенің арқасында байланыс желілеріндегі ауысымдық нөмірлерден шамамен 18 млн. шетелдік қоңыраулар анықталып, бұғатталса, 2023 жылы 8,5 млн. қоңырау бұғатталды. Сонымен бірге ІІМ және байланыс операторларымен бірлесіп алаяқтық жағдайлары жиілеп кеткен қазақстандықтардың хабардарлығын арттыру бойынша жұмысты ұйымдастырды және ескерту сипатындағы SMS-хабарламалар жіберді.

Дегенмен интернет-алаяқтыққа қарсы іс-қимыл бойынша негізгі міндетті ішкі істер органдары атқарады, себебі Қазақстан Республикасының қылмыстық-процестік заңнамасы интернет-алаяқтық қылмыстардың басым көпшілігін ашу және тергеп-тексеруді ішкі істер органдарына жүктейді.

Дәлірек, ҚК-нің 190-бабында (екінші бөлігінде, үшінші бөлігінің 1), 3) және 4) тармақтарында, төртінші бөлігінде) көзделген қылмыстық құқық бұзушылықтар туралы істер бойынша алдын ала тергеуді ішкі істер органдары, ал мемлекетке залал келтірілген жағдайда – экономикалық тергеу қызметі жүргізеді [4, 187-б].

ІІМ шет мемлекеттердің құқық қорғау органдарының киберкеңістіктегі қылмыстарды ашу және тергеу тактикаларын, заманауи ақпараттық технологияларды пайдалану тәжірибесін зерделеуде, интернет-алаяқтыққа қарсы іс-қимыл жөніндегі бағдарламалар әзірлеп іске асыруда, өңірлік полиция департаменттерінде тұрақты түрде жұмыс істейтін киберқылмыстарды тергеу жөніндегі арнайы жедел-тергеу топтары құрылды. Криминалдық полиция бөлімшелері үшін интернет желісін мониторингілеуге, әлеуметтік желілер мен мессенджерлердің қазақстандық пайдаланушыларын (зиянкестерді) анықтауға арналған заманауи жабдықтар мен мамандандырылған бағдарламалар сатып алған. Сондай-ақ білікті мамандар даярлау мақсатында алаяқтық және қаржы пирамидалары туралы қылмыстық істерді тергеу тактикасы мен әдістемесі жөнінде арнайы оқу бағдарламалары әзірленді (біліктілікті арттырудың онлайн-курстары, оның ішінде шетелдік мамандарды шақырумен), олар ведомстволық жоғары оқу орындарының оқу бағдарламасына енгізілген.

Дей тұрғанмен, осы зерттеу барысында талданған және жоғарыда көрсетілген интернет-алаяқтықпен байланысты ахуалды сипаттайтын статистикалық мәліметтер бұл бағытта қылмыстылықпен күрес жағдайы қанағаттандырусыз күйде екенін куәландырады, бұл, сәйкесінше, мемлекеттік органдардың, әсіресе ішкі істер органдары қабылдап жатырған шаралардың жеткіліксіз және тиімсіз екендігін білдіреді.

Ішкі істер органдарының интернет-алаяқтық қылмыстарды ашу және тергеу жұмысы ақпараттық-коммуникациялық технологиялардың даму қарқынынанәлдеқайда артта қалуы салдарынан ішкі істер органдарыөздеріне жүктелген қорғау және алдын алу функцияларын тиісті деңгейде іске асыра алмауда. Жедел уәкілдер мен тергеушілер интернет-алаяқтық қылмыстарды ашу және тергеу барысында көптеген күрделі мәселелерге тап болуда, себебі олар көбінесе заманауи ақпараттық-коммуникациялық технологияларды пайдаланатын және қылмыс тәсілдерін үнемі өзгертіп отыратын кәсіби алаяқтарға қарсы тұрады.

Интернет зиянкестерге өздерін білдіртпей жасырын әрекет етуге және іздерін жеңіл жасыруға мүмкіндік береді. Сондықтан тергеудің аса күрделілігі және дәлелдемелердің материалдық базасының болмауы себепті дәлелдеудің қиындығы орын алуда. "Банктер және банк қызметі туралы" Заңға сәйкес банктік құпия саласындағы заңнамалық кедергілер де қылмыстарды жылдам ашуға, тергеудің жедел жүргізілуіне теріс әсер етуде. Интернет-қылмыстар көбінесе аумақаралық, тіпті кейде трансшекаралық сипатта болады. Көптеген ақша аударымдары жүйелері мен онлайн-платформалардың пайда болуы қылмыскерлерге қашықтан, тіпті шет елдерден әрекет етуге мүмкіндік жасайды. Қылмыскерлер үшінші тұлғаларға рәсімделген банктік төлем карточкалар мен абоненттік нөмірлерді қолданады, электрондық ақшаны қолма-қол ақшаға ауыстыру үшін бөгде адамдарды тартады.

Осылайша қылмыскерлер полиция қызметкерлеріне қарағанда бірнеше қадам ілгері әрекет етіп келеді, ал полиция қызметкерлері интернет-алаяқтық қылмыстарды ашу және тергеуді басқа қылмыстармен бірдей жүзеге асырып, консервативті жедел-тергеу тәсілдерін қолданып келеді.

Сондықтан бүгінгі күнде интернет-алаяқтыққа және ішкі істер органдарының құзыретіне жататын киберкеңістіктегі басқа да қауіптерге қарсы тиімді әрекет ету үшін ішкі істер органдарының жұмыс тәсілдерін түбегейлі қайта қарастыру қажеттігі туындап отыр. Ол үшін ішкі істер органдарының басқа мүдделі органдар және ұйымдармен ақпарат алмасу рәсімін оңтайландыру, артық қағазбастылықты жою және заманауи ақпараттық-коммуникациялық технологияларды кеңінен ендіру арқылы интернет-алаяқтық қылмыстарды ашу және тергеудің жеделдігін мейлінше арттыру қажет.

Қазіргі уақытта қалыптасқан тәжірибе бойынша интернет-алаяқтықты тергеу алгоритмі өте ұзақ уақытты қажет етеді. Интернет-алаяқтық қылмыстардың барлығын дерлік тергеу барысында жедел уәкілдер мен тергеушілер басқа ұйымдардан (банктер, микроқаржылық қызметті жүзеге асыратын ұйымдар, байланыс операторлары) мәліметтерді жинақтайды және олармен ақпарат алмасу негізінен қағаз түрінде жүзеге асырылады.

Сонымен бірге қылмыскерлер қашықтан әрекет жасайтындықтан басқа өңірлердің ішкі істер бөлімшелеріне анықталған адамдарды табу және олардан істің мән-жайлары туралы жауап алу туралы жеке тапсырмалар жолданады. Басқа өңірдің ішкі істер бөлімшелерінде ведомстволық қызығушылық болмағандықтан немесе орындаушылық тәртіптің сақталмауынан мұндай жеке тапсырмалар ұзақ уақыт орындалады, тіпті кейбірі мүлдем орындалмайды.

Бұл ретте кейбір жағдайда қылмыскерлер көпдеңгейлі қылмыс схемаларын қолданатындықтан жоғарыда аталған жедел-тергеу әрекеттері бірнеше рет қайталап жүргізіледі.

Қылмыстарды тергеу барысында ішкі істер органдарының тергеушілері шетелдік IP-мекенжайлардың, мобилді нөмірлер мен электронды әмияндардың нөмірлерінің кімге тиесілі екені туралы мәліметтер алумен байланысты проблемалы мәселелерге тап болады. Сондықтан кейбір жағдайда тіпті шет мемлекеттердің құқық қорғау органдарына тапсырма жолдау қажеттігі

туындайды. Ал шет мемлекеттердің құқық қорғау органдары тарапынан құқықтық көмек көрсету туралы сұрау хаттарды орындау тәртібі халықаралық шарттармен реттеледі және оған ұзақ уақыт кетеді.

Осының салдарынан барлық деңгейдегі жергілікті ішкі істер органдары қызметкерлерінің жұмыс уақыты мен күші тиімсіз пайдаланылады, тергеу барысы созбалаңдыққа салынып, көптеген қылмыстар ашылмайды.

Әсіресе, интернет-алаяқтық қылмыстарды тергеу барысында ақша қаражаты айналымы негізгі дәлелдеме болып табылатындықтан банктік шоттарды және олардағы ақша қаражатының қозғалысын анықтауға бағытталған тергеу әрекеттерін шұғыл жүргізу аса маңызды.

Бұдан бөлек, интернет-алаяқтық қылмыстардың алдын-алу, ашу және тергеу саласындағы ведомствоаралық үйлестіру және мүдделі мемлекеттік органдардың өзара іс-қимылын күшейту, сондай-ақ ішкі істер органдарында интернет-алаяқтық қылмыстарды ашу және тергеу процесін орталықтандыру мәселесін қарастыру бүгінгі күн тәртібіндегі аса өзекті мәселелер қатарында.

Алайда ішкі істер органдарында интернет-алаяқтықты ашу бойынша тиімді тетіктердің болмауы, мүдделі мемлекеттік және мемлекеттік емес ұйымдар арасында өзара іс-қимылдың осалдығы, барлық деңгейдегі жергілікті ішкі істер органдары қызметкерлерінің жұмыс уақыты мен күшінің тиімсіз пайдаланылуы салдарынан интернет-алаяқтық қылмыстардың басым көпшілігі ашылмайды, тергеу барысы созбалаңдыққа салынады.

Қазіргі уақытта заманауи технологияларсыз интернеттегі құқыққа қайшы әрекеттерге төтеп беру мүмкін емес екенін атап өткен О.П.Грибуновтың пікірімен келісеміз [28, 11 б].

Аталған проблемаларды шешу үшін интернет-алаяқтық қылмыстарға қарсы іс-қимыл жұмысын мамандандыру мақсатында Қазақстан Республикасы Ішкі істер министрінің 18.01.2021г. №27 өкімімен аумақтық полиция департаменттерінде интернет-алаяқтықтарды тергеу бойынша тергеу-жедел топтары (бұдан әрі - ТЖТ) құру тапсырылған. Қазақстан Республикасы Ішкі істер министрінің орынбасары Қ.Сөнтаевтың 02.02.2021ж. шығ.№1-3-6-41/309-И тапсырмасынегізінде облыстық полиция департаменттерінде ақпараттық технологиялар саласындағы қылмыстарды ашу және тергеу жөнінде тұрақты ТЖТ құрылған [29].

Дегенмен тәжірибеде бұл тәсіл интернет-алаяқтыққа тиімді қарсы тұру үшін жеткіліксіз екенін көрсетті. Құрылған ТЖТ штат саны шектеулі болғандықтан барлық қылмыстарды қамтумүмкін болмай, тек жекелеген істермен айналысуда, сондай-ақ ТЖТ жұмысы тек интернет-алаяқтықпен шектелмей, барлық ақпараттық технологиялар саласындағы қылмыстар (ҚК-нің 105, 131, 132, 134, 147, 148, 195, 274, 313 және т.б.) бойынша қылмыстық істерді қамтиды.

Сонымен қатар Қазақстан Республикасы Бас прокуратурасы қызметкерлері өңірлерге шығып тексеру арқылы Алматы қаласы, Түркістан, Маңғыстау, Павлодар және Солтүстік Қазақстан облыстарында ТЖТ формальды түрде жұмыс істейтінін анықтаған. Бірде-бір тексерілген ТЖТ

интернет-алаяқтықпен жүйелі түрде айналысатын қылмыстық топтарды анықтау бағытында жұмыс атқармаған, оған ашылған көпэпизодты қылмыстардың болмауы дәлел бола алады (тек Шымкент қаласында ТЖТ 2022 жылдың басынан бері 4 қылмыстық топты әшкерелеген) [30].

Бұл ретте бірнеше жылдан бері еліміздің барлық өңірлерінде интернет-алаяқтықтың қарқынды өсу үрдісі орын алуына байланысты облыстық полиция департаменттерінің "К" бөлімшелерінде білікті қызметкерлердің жетіспеушілігі байқалады. Бұл бөлімшелердің қазіргі уақыттағы штаттық бірліктерінің саны қылмыстардың осыншама көп тіркелуіне есептелмеген.

Киберқылмыстарды әшкерелеу және тергеумен біліктілік талаптарына сәйкес жоғары заң білімі бар жалпықылмыстық, оның ішінде сыбайлас жемқорлық және экономика саласындағы құқық бұзушылықтарды тергеуге машықтанған/маманданған қызметкерлер айналысады. Құқық қорғау органдарының тергеу қызметкерлерінде киберқылмыстар туралы қылмыстық істерді тергеу бойынша арнайы танымдардың болмауы, жедел қызметкерлердің жұмыс дағдыларының жеткіліксіз деңгейі қылмыстардың дер кезінде ашылуына, дәлелдемелерді жинақтауға және кінәлі адамдарды жауаптылыққа тартуға кедергі келтіреді.

"К" бөлімшелерінің қызметі IT-мамандардың жұмысымен тығыз байланысты, алайда жоғары білікті IT-мамандардың құқық қорғау органдарына қарағанда жеке секторда анағұрлым көбірек табыс табуға мүмкіндігі бар. Жеке секторда еңбек шарттары да олар үшін тартымды. Мұның бәрі оларды құқық қорғау органдарына қызметкер ретінде тартуға теріс ықпал етеді.

КПК (79,80-баптар) жоғары IT-білімі бар адамдарды қылмыстық процеске тек сарапшы немесе маман ретінде қорытынды беру немесе жекелеген процестік әрекеттерді техникалық сүйемелдеу үшін тартуға мүмкіндік береді [4], олар тергеу барысына араласа алмайды, тиісінше істің шешілуіне мүдделік танытпайды.

Аталған проблеманы шешу мақсатында осы санаттағы мамандар үшін еңбекақының ұлғайтылған сеткасын және қажетті еңбек шарттарын қарастыруға мақсатқа сай көрінеді.

3.2 Ішкі істер органдарында интернет-алаяқтық қылмыстарды ашу және тергеу процесін оңтайландыру жөніндегі ұсынымдар

Қазақстан Республикасының ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметін одан әрі жетілдіру және тиімділігін арттыру үшін келесі заңнамалық, ұйымдық және практикалық іс-шараларды жүзеге асыруды ұсынамыз:

1. Жоғарыда атап өткендей, Будапешт конвенциясы киберқылмыстарға қарсы күрес саласындағы халықаралық өзара іс-қимылды қамтамасыз ететін басты әмбебап кешенді құжат болып табылады және оған әлемнің дамыған

мемлекеттерінің басым көпшілігі қосылып, құқық қорғау органдары оның мүмкіндіктерін іс жүзінде пайдалануда.

Бұл ретте осы зерттеуіміздің мәні болып табылатын интернет-алаяқтықтар Будапешт конвенциясында компьютерлік қылмыстар қатарына жатқызылғандықтан, оның реттеуіне кіреді, сондықтан қатысушы-мемлекеттердің құқық қорғау органдары интернет-алаяқтық қылмыстар бойынша Будапешт конвенциясында қарастырылған оңтайлатылған тәртіпте өзара ақпарат алмасу тетіктерін, соның ішінде 24/7 желісінің байланыс пункттерінің мүмкіндіктерін пайдалана алады [20, 25-б].

Будапешт конвенциясына қосылу еліміздің құзырлы органдарының оған қатысушы-мемлекеттік органдардың құзырлы органдарымен өзара іс-қимыл тәртібіне оң ықпал етіп, олармен қажетті мәліметтер және дәлелдемелерді жедел түрде алмасуға мүмкіндік беретіні, сәйкесінше, онда көзделген тетіктер Қазақстан Республикасының ішкі істер органдарының интернет-алаяқтық қылмыстарды ашу және тергеу қызметінің жылдамдығы мен тиімділігін арттыруға айтарлықтай септігін тигізері анық.

Осыған байланысты Үкіметтің Будапешт конвенциясына қосылу туралы заң жобасын әзірлеуін және оны Қазақстан Республикасы Парламентінің қарауына енгізуін ұсынамыз.

2. Интернет-алаяқтық қылмыстарды тергеу барысында ақша қаражаты айналымы негізгі дәлелдеме болып табылатындықтан банктік есепшоттарды және олардағы ақша қаражатының қозғалысын анықтауға бағытталған тергеу әрекеттерін шұғыл жүргізу аса маңызды.

ҚПК-нің 34-бабының 5-бөлігіне сәйкес қылмыстық қудалау органының заңға сәйкес қойған талаптары барлық мемлекеттік органдардың, ұйымдардың, лауазымды адамдар мен азаматтардың орындауы үшін міндетті және олар белгілеген мерзімде, бірақ үш тәуліктен кешіктірілмей орындалуға тиіс [4].

Алайда іс жүзінде тергеушілердің банктерге есепшоттар мен олардағы ақша қаражатының қозғалысы туралы мәліметтерді ұсыну жөнінде сұрау хаттары уақтылы орындалмайды және ақпарат алмасу қағаз түрінде жүзеге асырылатындықтан қажетті мәліметтер тергеушіге бірнеше аптада жетеді. Ал көптеген банктердің филиалдары тек облыс орталықтарында орналасатындықтан аудандық және кейбір қалалық деңгейде қызметкерлер сұрау хаттарды оларға пошта арқылы жолдайды немесе өздері қолма-қол қағаз түрінде жеткізеді. Өз кезегінде,банктер де жауапты поштамен жолдайды немесе қағаз түрінде шығарып, қызметкерлердің қолма-қол алып кетуін күтеді.

Ақша қаражатының қозғалысын анықтау процесінің созбалаңға салынуы салдарынан алаяқтық жолмен жымқырылған ақша басқа есепшоттарға бірнеше рет аударылып, қылмыстардың ашылуы қиындатады.

«Қазақстан Республикасындағы банктер және банк қызметі туралы» Заңның 50-бабы 7-тармағының б)-тармақшасында жеке тұлғаның банк шоттарының бар-жоғы және нөмірлері туралы, осы шоттардағы ақша

қалдықтары мен ақша қозғалысы туралы анықтамаларды электронды форматта беру мүмкіндігі қарастырылғанмен тергеу мерзімін тиімді пайдалану үшін құқық қорғау органдары мен банктер арасында электронды форматта ақпарат алмасу іс жүзінде жолға қойылмаған және ақпарат алмасудың альтернативті тәсілдерінің қарастырылуы салдарынан банктер электронды түрде ақпарат алмасуға көшуге мүдделілік танытпайды.

Көрсетілгендердің негізінде «Қазақстан Республикасындағы банктер және банк қызметі туралы» Заңның 50-бабы 7-тармағының б)-тармақшасына жеке тұлғаның банк шоттарының бар-жоғы және нөмірлері туралы, осы шоттардағы ақша қалдықтары мен ақша қозғалысы туралы анықтамаларды айрықша электронды форматта беруді (қылмыстық қудалау органының бірінші басшысы немесе тергеушінің қолтаңбасымен куәландырылған электрондық нысандағы сұрау салу, прокурордың электрондық нысанда салынған санкциясы негізінде) міндеттейтін өзгерістер енгізуді ұсынамыз.

3. Сарапшылар болашақта интернет-алаяқтық қылмыстардан басқа террористік, экстремисттік, сыбайлас жемқорлық, экономикалық және т.б. қылмыстар одан әрі кеңінен ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатындығы туралы жиі айтуда. Ал мұндай қылмыстарды тергеу арнайы танымдарды талап ететіндігін назарға ала отырып, құқық қорғау органдарында киберқылмыстарды анықтау, жолын кесу, ашу және тергеуді жүзеге асыратын мамандандырылған бөлімшелер осы бастан құрып дамыту қажеттігі анық.

Бірқатар ғалымдар мен заңгерлер, оның ішінде Е.М. Якимова мен С.В. Нарутто мағыналас пікірді ұстанады [19, 371 б].

Құрамына тергеу және жедел топтар кіретін, тәулік бойы 24/7 режимде жұмыс істейтін киберқылмыстарға қарсы күрес бөлімшелер ұйымдастыру - Будапешт конвенциясының ұсынымдарының бірі (қылмыстарға қарсы іс-қимылдың мамандануы, қылмыстарды ашу және тергеу процесінің тікелей және үзіліссіз жүргізілуі қамтамасыз етіледі) болып табылады.

Қазақстанда бұл идеяны жүзеге асыру мәселесі кемінде он жылдан астам уақыт көтеріліп келе жатқанымен осы күнге дейін толыққанды іске асырылмаған.

2013 жылы Бас прокуратураның ресми сайтында жарияланған "Қазақстан Республикасының құқық қорғау жүйесін одан әрі жаңғыртудың 2014-2020 жылдарға арналған мемлекеттік бағдарламасының" жобасында "Киберқылмыстардың айтарлықтай өсуі байқалады. Бүгінгі күні ішкі істер органдары киберқылмысқа нақты қарсы іс-қимылға дайын емес - ол үшін барабар құрылым да, білікті кадрлар, да қажетті техникалық жабдықталу да жоқ. Осыған байланысты жалпы қылмыстық киберқылмыстардың алдын алу, ашу және тергеу саласында ведомствоаралық үйлестіру мәртебесін берумен бірге ІІМ құрылымында толыққанды Киберқылмысқа қарсы күрес орталығын құру қажет" деп атап өтілген болатын.

Қазақстан Республикасы Үкіметінің 01.04.2014ж. №292 қаулысымен бекітілген «Қазақстан Республикасының құқық қорғау жүйесін одан әрі жаңғыртудың 2014-2020 жылдарға арналған мемлекеттік бағдарламасын іске

асыру жөніндегі іс-шаралар жоспарының» 42-тармағына сәйкес ІІМ-нің құрылымында Киберқылмысқа қарсы күрес орталығы құру көзделіп, оған жалпы киберқылмыстардың алдын алу, ашу және тергеу саласындағы ведомствоаралық үйлестіру құзыретін беру жоспарланған [31].

Алайда аталған тармақ формальды түрде орындалып, тиісті орталық ІІМ-нің Криминалдық полиция департаментінің құрамында ғана ашылған, оның құзыреті заңнамалық деңгейде реттелмеген, ведомствоаралық үйлестіру функциясы айқындалмаған. Яғни, киберқылмыстарға қарсы іс-қимыл жасайтын толыққанды дербес орталық мәртебесінде құрылмаған болатын.

Осылайша, ІІМ жанында толыққанды Киберқылмысқа қарсы іс-қимыл орталығын жеке құрылымдық бөлімшенысанында құру мәселесі ашық қалған.

Өз кезегінде, жоғарыда жүргізілген халықаралық тәжірибені талдау нәтижесі де көптеген дамыған мемлекеттер киберқауіпсіздік проблемасына, соның ішінде ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатын жымқыруларды тергеп-тексеруге баса мән беретінін көрсетеді. Бұл ретте бұл саладағы қылмыстармен күрес жөніндегі қызметті барынша мамандандыру үрдісі байқалады.

Еліміздің басты қадағалау органы - Бас прокуратураның өзі осындай қылмыстарға тиімдірек қарсы іс-қимыл жасау үшін ІІМ жанында аумақтық бөлімшелер мен "К" бөлімшелеріне жеке тапсырмалар жолдай отырып олардың жедел мүмкіндіктерін пайдалану арқылы қылмыстық топтарға қатысты көпэпизодты интернет-алаяқтықтарды тергеуді тікелей жүзеге асыратын бөлек бөлімше (бас офис) құру қажет деп санайды. Бас прокуратурада бұл жаңалық интернет-алаяқтықтың эпизодтарын іздеуді және одан әрі негізгі іске біріктіруді айтарлықтай оңайлатады және тездетеді, сотқа дейінгі тергеп-тексеру материалдарын басқа өңірлерге негізсіз жіберуді болдырмайды, сондай-ақ тергеудің сапасын біршама көтереді деп есептейді [30].

Яғни, зерттеуде көтеріліп отырған мәселе құқық қорғау органдары жүйесінің қызметін үйлестіруші және жоғарғы заңдылықты қадағалаушы орган болып табылатын Бас прокуратураның күн тәртібінде тұрған маңызды мәселелердің қатарында екенін білдіреді және Бас прокуратураның ұсынысы да осы зерттеуіміздің нәтижесі бойынша әзірленген ұсынымдармен мағыналас.

Оның үстіне, соңғы кездері ІІМ бұқаралық ақпарат құралдарында жариялаған мәлімдемелерінен осындай тетіктерді пилоттық режимде іске асыруға шара қолданылып жатқанын байқауға болады. Дәлірек айтсақ, жуырда Ішкі істер министрі М.Ахметжанов елордада Киберполдың құрылғанын еске салып (ІІМ цифрлық технологиялар саласындағы қылмыспен күресу үшін қолға алған пилоттық жоба): «Біз оны заманауи құрал-жабдықтармен жабдықтап, интернеттегі қылмыстарды ашу мен тергеу тәсілдерін өзгерттік. Осындай фактілер бойынша азаматтардың өтініштері «бір терезе» қағидаты бойынша қабылданады. Нәтижелер бар. Небәрі 5 айда Есіл ауданында осындай 864 қылмыс тіркелген. Оның 308-і ашылды. Сондай-ақ Астана мен Қостанайда жоқ көліктерді ұтып алу үшін call-орталығын ұйымдастырған қылмыстық топтың 18 мүшесі ұсталды" деді [32].

Жоғарыда баяндалғандардың негізінде озық халықаралық тәжірибені ескере отырып, ІІМ жанында өз бетімен тергеу-жедел функциясын жүзеге асыру құзыреті бар комитет немесе департамент деңгейінен төмен емес нысанда киберқылмысқа қарсы іс-қимыл жөніндегі толыққанды жеке құрылымдық бөлімше (Киберпол) құру, сәйкесінше, облыстық полиция департаменттері жанында ұқсас киберқылмысқа қарсы іс-қимыл басқармаларын құру туралы Ішкі істер министрінің бұйрығын шығаруды ұсынамыз.

4. Ішкі істер органдарында интернет-алаяқтықты ашу бойынша тиімді тетіктердің болмауы, мүдделі мемлекеттік және мемлекеттік емес ұйымдар арасында өзара іс-қимылдың осалдығы, барлық деңгейдегі жергілікті ішкі істер органдары қызметкерлерінің жұмыс уақыты мен күшінің тиімсіз пайдаланылуы салдарынан интернет-алаяқтық қылмыстардың басым көпшілігі ашылмайды, тергеу барысы созбалаңдыққа салынады.

Нәтижесінде интернет-алаяқтықтар туралы қылмыстық істердің басым көпшілігі ашылмауына байланысты сотқа істер сирек жіберіледі. Сәйкесінше, жәбірленушілерге келтірілген залал негізінен өтелмейді, ал қылмыскерлер жауаптылықтан жалтарады. Бұл, өз кезегінде, халықтың жалпы құқық қорғау органдарына сенімсіздігін тудырып, беделін төмендетеді.

Сондықтан интернет-алаяқтық қылмыстардың алдын-алу, ашу және тергеу саласындағы ведомствоаралық үйлестіру және мүдделі мемлекеттік органдардың өзара іс-қимылын күшейту, сондай-ақ ішкі істер органдарында интернет-алаяқтық қылмыстарды ашу және тергеу процесін орталықтандыру мәселелерін қарастыру аса маңызды.

Осыған байланысты интернет-алаяқтыққа қарсы іс-қимылдың тиімділігін айтарлықтай көтеру үшін орталық мемлекеттік және құқық қорғау органдары басшыларының бірлескен бұйрығын шығару ұсынылады, онда:

- ІІМ-не (киберқылмысқа қарсы іс-қимыл жөніндегі бөлімше) киберқылмыстар мен интернет-алаяқтықтардың алдын алу, анықтау, ашу және тергеу саласында ведомствоаралық үйлестіру функциясын жүктеуді;

- киберқылмысқа қарсы іс-қимыл жөніндегі бөлімшелердің жанында құрамына ішкі істер органдары және мүдделі мемлекеттік органдар мен басқа ұйымдардың (банктер, ұялы байланыс операторлары) қызметкерлері, жоғары білікті IT-мамандар кіретін арнайы штаб құру жолымен интернет-алаяқтықтарды анықтау, ашу және тергеу процесін орталықтандыру және оған келесі міндеттерді жүктеуді ұсынамыз:

а) ақпараттық-коммуникациялық жүйелер мен дереккөздерді қолдана отырып, жергілікті ішкі істер органдарын барша республика аумағында орын алған интернет-алаяқтықтарды жылдам ашу және тергеу үшін барлық қажетті мәліметтермен жедел және онлайн режимде қамтамасыз ету;

б) интернет-алаяқтықтарды ашу және тергеу мәселелері бойынша әртүрлі өңірлердің ішкі істер органдары арасында жедел өзара іс-қимылды қамтамасыз ету;

в) көпэпизодты интернет-алаяқтықтарды ашу және тергеу.

ҚОРЫТЫНДЫ

Қорытындылай келе, кез-келген орнықты құқықтық мемлекетті қалыптастыру және дамытуда қылмыстылықпен күрес маңызды рөл атқаратыны белгілі. Құқық тәртібі мен заңдылықтың тиісті деңгейін сақтау - қазіргі заман қоғамының басты міндеттерінің бірі.

Қылмыстылықты талдау нәтижесі ақпараттық-телекоммуникациялық технологиялар бірте-бірте кез-келген саладағы қызметтің айырылмас бөлігі болып келе жатқанын көрсетеді және бұл ақпараттық қауіпсіздікке назар аударудың маңыздылығын арттыра түседі. Бұл ретте қылмыстың мұндай түрлері айрықша сипатқа ие, сондықтан істің оң шешілуі көбінесе тергеудің жеделдігі мен сапасына тікелей байланысты.

Интернет желісіндегі қылмыстар жыл сайын эволюционалады: жыл сайын жаңа алаяқтық топтар пайда болады, қылмыс схемалары қиындай түседі, қылмыскерлер техникалық инструменттері мен тәсілдерін жетілдіреді.

Әлемде цифрлық активтер нарығының серпінді өсуі байқалады. Ал қазақстандықтар интернет және онлайн-платформалардың өте белсенді қолданушылары болып табылады.

Қазақстанда цифрландыру кең белең алып келеді - қазір елімізде интернеттің ену көрсеткіші 90,1% құрайды [2].

DataReportal сайтының деректеріне сәйкес 2022 жылдың қаңтар айына Қазақстанда 16,4 млн. интернет-пайдаланушы тіркелген.

Яғни интернетті пайдаланушылар саны өсуде, бұл келешекте интернет-алаяқтықтың әлеуетті құрбандарының азаймайтынын білдіреді.

Интернет-алаяқтық және интернеттегі басқа да құқық бұзушылықтар саны жағынан да сапасы жағынан да ұлғая береді, бұл мемлекеттің заң шығарушы органдарынан да, құқық қорғау органдарынан да тиісті реакцияны талап етеді. Сондықтан интернет-алаяқтыққа қарсы іс-қимылдың жеке реттелуінің маңыздылығына баса назар аудару керек, себебі дұрыс және ыңғайлы заңнамалық регламенттеу ұлғайып келе жатқан қауіппен тиімді күресуге септігін тигізеді.

Интернет-қылмыстарға қарсы іс-қимыл экономикалық, қаржылық, ұйымдық-басқарушылық және заңнамалық шараларды қамтитын күрделі, көпжақты процесс. Дегенмен бұл зерттеуде Қазақстан Республикасының ішкі істер органдары қызметінің ұйымдық-құқықтық аспектілеріне баса назар аударылып, нақты ұйымдық-құқықтық, оның ішінде нақты заңнамалық ұсынымдар әзірленді.

Біздің пікірімізше, аталған ұсынымдардың іске асырылуы ішкі істер органдарының интернет-алаяқтық қылмыстарға қарсы іс-қимыл жөніндегі қызметінің тиімділігін арттыруға ықпал етеді. Сәйкесінше, түпкі мақсат - азаматтарымыздың Қазақстан Республикасының Конституциясымен кепілдік берілген меншік құқығының тиісті деңгейде қорғалуына септігін тигізеді.

ҚОЛДАНЫЛҒАН ДЕРЕККӨЗДЕРДІҢ ТІЗІМІ

1. Потребление интернет-трафика в РК выше среднемировых показателей на 46. [Электрондық деректер] // - Қол жеткізу режимі: https://forbes.kz/news/2022/06/16/newsid_278137 (жүгінген күн: 17.01.2023ж.)

2. Сколько казахстанцев в интернете и что они там делают — цифры из исследования digital-рынка. [Электрондық деректер] // - Қол жеткізу режимі: https://digitalbusiness.kz/2022-12-27/skolko-kazahstanczev-v-internete-i-chto-oni-tam-delayut-czifry-iz-issledovaniya-digital-rynka/ (жүгінген күн: 17.01.2023ж.)

3. Қазақстан Республикасы Бас прокуратурасы жанындағы Құқықтық статистика және арнайы есепке алу комитетінің "Қазақстан Республикасының құқық қорғау органдары қызметінің негізгі көрсеткіштері туралы мәліметтер" 2018-2022ж.ж. статистикалық есептері.

4. Қазақстан Республикасының Қылмыстық-процестік кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/K1400000231 (жүгінген күн: 26.01.2023ж.)

5. Қазақстан Республикасының Конституциясы. 1995 жылғы 30 тамызда республикалық референдумда қабылданған. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/ K950001000 (жүгінген күн: 26.01.2023ж.)

6. 8 из 10 интернет-мошенников не найдены в Казахстане – Юрий Ли. [Электрондық деректер] // - Қол жеткізу режимі: https://inbusiness.kz/ru/last/8-iz-10-internet-moshennikov-ne-najdeny-v-kazahstane-yurij-l (жүгінген күн: 15.03.2023ж.)

7. Интернет-мошенничество в Казахстане: тысячи таких дел остаются не раскрытыми. [Электрондық деректер] // - Қол жеткізу режимі: https://profit.kz/news/58861/Internet-moshennichestvo-v-Kazahstane-tisyachi-takih-del-ostautsya-ne-raskritimi/ (жүгінген күн: 17.01.2023ж.)

8. "Қазақстан Республикасының ішкі істер органдары туралы" Қазақстан Республикасының 2014 жылғы 23 сәуірдегі № 199-V ҚРЗ Заңы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet. zan.kz/kaz/docs/Z1400000199 (жүгінген күн: 26.01.2023ж.)

9. Еськова Л.К. "Новые преступные способы мошенничества в период пандемии коронавирусной инфекции" // Гуманитарные, социально-экономические и общественные науки. Владимир, 2021. № 4. 122-126 б.

10. Денисенко О.И. "Рост числа случаев мошенничества в период самоизоляции и организационно-правовые методы борьбы с мошенниками" // Вестник Самарского юридического института. 2021. №3. 125-130 б.

11. Готчина Л.В. "Коронавирус и изменения в структуре преступности" // Криминология: вчера, сегодня, завтра. – 2020. – №4 (32). – 40-44 б.

12. "Қазақстан Республикасындағы банктер және банк қызметі туралы" Қазақстан Республикасының 1995 жылғы 31 тамыздағы N 2444 Заңы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/Z950002444_ (жүгінген күн: 26.01.2023ж.)

13. "Алаяқтық туралы істер бойынша сот практикасы туралы" Қазақстан Республикасы Жоғарғы Сотының 2017 жылғы 29 маусымдағы № 6 нормативтік қаулысы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/P170000006S (жүгінген күн: 09.02.2023ж.)

14. "Ақпараттандыру туралы" Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/Z1500000418 (жүгінген күн: 09.02.2023ж.)

15. Қазақстан Республикасының Қылмыстық кодексі 2014 жылғы 3 шілдедегі №226-V ҚРЗ. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/K1400000226 (жүгінген күн: 09.02.2023ж.)

16. Түркістан қаласы прокуратурасының Түркістан облысының полиция департаментіне енгізген заңдылықты бұзушылықты жою туралы ұсынуы. - 14.02.2023ж. шығ.№2-12-23-00462. - 1 б.

17. Вехов В.Б. "Компьютерные преступления. Способы совершения и методика расследования". [Электрондық деректер] // - Қол жеткізу режимі: https://www.studmed.ru/view/vehov-vb-kompyuternye-prestupleniya-sposoby-soversheniya-i-metodika-rassledovaniya_781a155ddb1.html? page=3 (жүгінген күн: 02.03.2023ж.)

18. Архипова Е.А., Додонов В.Н. "Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации". [Электрондық деректер] // - Қол жеткізу режимі: https://www.mjil.ru/jour/article/viewFile/362/264 (жүгінген күн: 15.03.2023ж.)

19. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью. Криминологический журнал Байкальского государственного университета экономики и права. - 2016. - №2. Т.10. – 369-378 б.

20. Компьютерлік қылмыстар туралы Еуропалық конвенция (киберқылмыстар туралы. 2001 жылғы 23 қарашада Будапешт қаласында қабылданған. [Электрондық деректер] // - Қол жеткізу режимі: https://rm.coe.int/1680081580 (жүгінген күн: 15.03.2023ж.)

21. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования. [Электрондық деректер] // - Қол жеткізу режимі: https://mgimo.ru/upload/iblock/2f2/2f24a1dc778ca03f5a32a609d2 616dc7.pdf (жүгінген күн: 04.04.2023ж.)

22. Сенатта қаржы пирамидаларына қарсы күрес тетіктері талқыланды. [Электрондық деректер] // - Қол жеткізу режимі: https://elorda.info/aleumet/17602-senatta-karzhy-piramidalaryna-karsy-kures-tetikteri-talkylandy (жүгінген күн: 04.04.2023ж.)

23. Петр Городов: в мире мало инструментов для борьбы с киберпреступностью. [Электрондық деректер] // - Қол жеткізу режимі: https://ria.ru/20210728/gorodov-1743169971.html (жүгінген күн: 04.04.2023ж.)

24. "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 Жарлығы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet. zan.kz/kaz/docs/U020000897_ (жүгінген күн: 14.04.2023ж.)

25. "Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімді ратификациялау туралы" Қазақстан Республикасының 2019 жылғы 9 желтоқсандағы № 277-VI ҚРЗ Заңы. [Электрондық деректер] // - Қол жеткізу режимі: https:// adilet.zan.kz/kaz/docs/Z1900000277/compare (жүгінген күн: 14.04.2023ж.)

26. "Қаржылық мониторингті дамытудың 2022-2026 жылдарға арналған тұжырымдамасын бекіту туралы" Қазақстан Республикасы Президентінің 2022 жылғы 6 қазандағы №1038 Жарлығы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/rus/docs/U2200001038/compare/kaz (жүгінген күн: 14.04.2023ж.)

27. Темиржанова Л.А., Абулгазина А.Ж. Проблемы обеспечения информационной безопасности правоохранительных структур и противодействие киберпреступлениям, киберхищениям (Национальный и зарубежный опыт). [Электрондық деректер] // - Қол жеткізу режимі: https://academy-rep.kz/uploads/7429706d3e0aa6c821bacfc49514837c.pdf (жүгінген күн: 14.04.2023ж.)

28. Грибунов О.П. К вопросу о противодействии экстремизму на объектах транспорта / О.П. Грибунов. — EDN SIQRWN // Вестник Восточно-Сибирского института МВД России. — 2013. — № 3 (66). — 9–16 б.

29. Қазақстан Республикасы Ішкі істер министрінің орынбасары Қ.Сөнтаевтың 02.02.2021ж. шығ.№1-3-6-41/309-И тапсырмасы.

30. Қазақстан Республикасы Бас прокуратурасының 1-Қызметінің тексеру нәтижесі туралы 22.09.2022ж. анықтамасы.

31. «Қазақстан Республикасының құқық қорғау жүйесін одан әрі жаңғыртудың 2014-2020 жылдарға арналған мемлекеттік бағдарламасын іске асыру жөніндегі іс-шаралар жоспарын бекіту туралы" Қазақстан Республикасы Үкіметінің 01.04.2014ж. №292 қаулысы. [Электрондық деректер] // - Қол жеткізу режимі: https://adilet.zan.kz/kaz/docs/ P1400000292 (жүгінген күн: 18.04.2023ж.)

32. Жыл басынан бері 7 мыңнан астам интернет-алаяқтық фактілері тіркелген. [Электрондық деректер] // - Қол жеткізу режимі: https://egemen.kz/article/343429-zhyl-basynan-beri-7-mynhnan-astam-internet-alayaqtyq-faktileri-tirkelgen (жүгінген күн: 02.06.2023ж.)

ҚОСЫМША 1. Енгізу актісі

«БЕКІТЕМІН»
Түркістан облысының
полиция департаменті
бастығының орынбасары
полиция полковнигі
_____А.О.Калдарбеков
«__» мамыр 2023 жыл

Магистрлік зерттеу нәтижелерін практикалық қызметке енгізу туралы
АКТ

Мына құрамда комиссия:

Төрағасы: Түркістан облысының Полиция департаментінің Тергеу басқармасының бастығы полиция подполковнигі Ж.Құлмахан.

Мүшелері: Түркістан облысының Полиция департаментінің Тергеу басқармасы бастығының орынбасарлары полиция подполковнигі М.Сейдилдаев және полиция подполковнигі К.Думшебаев.

Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау академиясының магистранты Ж.А.Ахметбектің "Қазақстан Республикасы ішкі істер органдарының интернет-алаяқтыққа қарсы іс-қимыл жөніндегі қызметінің ұйымдық-құқықтық аспектілері" тақырыбындағы магистрлік зерттеу өзекті екендігі және оның нәтижелері ішкі істер органдарының практикалық қызметіне енгізу үшін қызығушылық тудыратыны туралы осы акт жасалды.

Енгізу шешімі: Түркістан облысының Полиция департаментінің практикалық қызметінде қолдану, қолданыстағы заңнама мен жедел-тергеу практикасын жетілдіру бойынша ұсыныстар енгізу.

Комиссия төрағасы: **Ж.Құлмахан**

Комиссия мүшелері: **М.Сейдилдаев**

К.Думшебаев