**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БАС ПРОКУРАТУРАСЫ ЖАНЫНДАҒЫ
ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫ АКАДЕМИЯСЫ**

Коигелдина Айжан Даулетханкызы

Қызмет көрсету мен тауар сату саласындағы интернет желісі арқылы жасалатын алаяқтықты тергеу әдістемесі

Магистрлік дәрежесін алуға диссертация
7М04203 «Құқықтану»

Ғылыми жетекші:
Жоғары оқу орнынан кейінгі білім беру
институтының жалпы құқықтық пәндер
кафедрасының аға оқытушысы
кіші әділет кеңесшісі
заң ғылымдарының магистрі
_____ Н.Б. Рахимов

Қосымша ғылыми жетекші:
Жоғары оқу орнынан кейінгі білім беру
институтының жалпы құқықтық пәндер
кафедрасының аға оқытушысы
әділет кеңесшісі
заң ғылымдарының магистрі
_____ Р.Р. Жылқайдаров

Қосшы, 2021 ж.

ТҮЙІНДЕМЕ

Диссертациялық зерттеуде Қазақстан Республикасының ішкі істер органдарындағы қызмет көрсету және тауар сату саласындағы интернет желісі арқылы ақпарттық жүйені қолданушыға қатысты жасалатын алаяқтықты тергеудің қазіргі жағдайдағы мәселелері зерделенді.

Жұмыста аталған қылмыс түрінің криминалистикалық сипаттамасының ерекшеліктері атап өтіледі. Сонымен қатар халықаралық деңгейде шет мемлекеттердің компьютерлік қылмыстарды тергеу тәжірибесінде туындайтын мәселелер және жетістіктер туралы есебі зерделенді.

Қылмыстың бұл түрін тергеуде айтарлықтай массивті абоненттік деректер анықталуына байланысты "үлкен деректерді" немесе Big Data зерттеу, талдау үшін арнайы бағдарламаларды қолдану ұсынылады. Сондай-ақ алынған электронды дәлелдемелерді сақтау үшін қолданысқа «электронды сақтау камерасын» енгізу ұсынылады.

РЕЗЮМЕ

В диссертационном исследовании изучены вопросы расследования мошенничества, совершаемого в отношении пользователя информационной системы через сеть интернет в сфере оказания услуг и реализации товаров в органах внутренних дел Республики Казахстан в современных условиях.

В работе подчеркиваются особенности криминалистической характеристики данного вида преступления. Также был изучен отчет на международном уровне иностранных государств о проблемах и достижениях, возникающих в практике расследования компьютерных преступлений.

В связи с тем, что при расследовании данного вида преступления выявляются достаточно массивные абонентские данные, рекомендуется использовать специальные программы для исследования, анализа "больших данных" или Big Data. Также предлагается ввести в действие «электронную камеру хранения» для хранения полученных электронных доказательств.

SUMMARY of

In the dissertation research, the issues of investigation of fraud committed against the user of an information system via the Internet in the field of providing services and selling goods in the internal affairs bodies of the Republic of Kazakhstan in modern conditions are studied.

The paper emphasizes the features of the criminalistic characteristics of this type of crime. The report on the international level of foreign countries on the problems and achievements that arise in the practice of investigating computer crimes was also studied.

Due to the fact that the investigation of this type of crime reveals quite massive subscriber data, it is recommended to use special programs for research, analysis of "big data" or Big Data. It is also proposed to introduce an "electronic storage chamber" for storing the received electronic evidence.

МАЗМҰНЫ

НОРМАТИВТІК СІЛТЕМЕЛЕР

Осы диссертацияда мынадай стандарттарға сілтемелер пайдаланылған:

- Қазақстан Республикасының Конституциясы, 1995 жылғы 30 тамызда қабылданған;
- Қазақстан Республикасының Қылмыстық Кодексі, 2014 жылғы 3 шілдеде қабылданған;
- Қазақстан Республикасының Қылмыстық-процестік кодексі, 2014 жылғы 4 шілдеде қабылданған;
- "Жедел-іздестіру қызметі туралы" Заңы, 1994 жылғы 15 қыркүйекте қабылданған;
- Қазақстан Республикасы Бас Прокурорының 2014 жылғы 19 қыркүйектегі №89 Бұйрығымен бекітілген «Қылмыстық құқық бұзушылықтар туралы арызды, хабарды немесе баянатты қабылдау және тіркеу, сондай-ақ Сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімін жүргізу қағидалары»;
- Қазақстан Республикасы Жоғарғы Сотының 2010 жылғы 25 маусымдағы № 4 "Қылмыстық сот ісін жүргізуде адамның және азаматтың құқықтарын, бостандықтарын сот арқылы қорғау туралы" нормативтік қаулысы;
- «Интернет желісінің қазақстандық сегментінің кеңістігінде домендік аттарды тіркеу, пайдалану және бөлу қағидаларын бекіту туралы" Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 13 наурыздағы № 38/НҚ бұйрығы;
- Компьютерлік қылмыстар туралы конвенция (Еуропа кеңесінің киберқылмыс туралы конвенциясы, Будапешт, 2001 жылғы 23 қараша).

АНЫҚТАМАЛАР

Домен немесе DNS (Domain Name system) - домендік аттар жүйесі, домендік аттар туралы ақпарат алу үшін бөлінген деректер қоры. Домендік аттарға және Internet Protocol (IP) мекенжайларына сәйкестігі туралы ақпаратты қамтиды және 1032, 1034, 1035, 1122, 1133, 1591 Request for Comments (RFC) стандарттарына сәйкес жұмыс істейді.

Internet Service Provider – ISP – провайдер, интернет-қызмет көрсетуші. Пошта қызметін көрсетуші, интернет-дүкен, интернет-банкинг, Электронды үкімет және денсаулық сақтау веб-сайттары, Wikipedia және т.б.

Over-the-top технологиясы – Интернет арқылы видеоқызметтер көрсету әдісі. OTT термині видеосигналдың провайдерден қолданушының құрылғысына (приставка, компьютер, мобильді телефон) деректерді жолдау желілері арқылы жеткізу дегенді білдіреді. Дәстүрлі IPTV қызметіне қарағанда, көбінесе байланыс операторымен тікелей байланысы жоқ болып келеді.

IP-мекенжай (Internet Protocol Adress – адрес интернет протокола) – компьютерлік желідегі түйіннің бірегей желілік мекенжайы, ол TCP/IP хаттамалар стекі негізінде құрылады. TCP/IP (Transmission Control Protocol/Internet Protocol) деректерді беру хаттамалары.

MAC (Media Access Control) – мекенжайы, әр белсенді құрылғы бірлігіне немесе оның кейбір компьютерлік желідегі интерфейстеріне берілетін бірегей идентификатор.

URL-мекенжайы (Uniform Resource Locator – бірыңғайланған ресурсқа бағыттаушы) – электронды ресурстардың бірыңғайландырылған мекенжайлар жүйесі, немесе ресурстың (файлдың) орнын біртектес анықтаушысы.

IMEI (International Mobile Equipment Identity) – мобильді құрылғыны халықаралық сәйкестендіруші, GSM, WCDMA, IDEN және кейбір спутниктік телефондарды сәйкестендіру нөмірі.

Tor (The Onion Router) - онлайн анонимдікті қамтамасыз ететін бағдарлама.

IBM (International Business Machines) **Security i2 Analyst's Notebook** — визуалды талдау құралы, ол үлкен деректер көлемін мағынасы бар ақпаратқа айналдыруға мүмкіндік береді. Бұл шешім өзара байланысты желілілерді визуализация жасау, әлеуметтік желілерді талдау, кеңістіктегі және уақыттағы көрінісін жасау сияқты инновациялық функциялары бар, олар өз кезегінде дереккөздердегі жасырын заңдылықтар мен байланыстарды анықтауға мүмкіндік береді.

NetFlow - желілік трафикті есепке алуға арналған желілік хаттама, Cisco Systems компаниясы әзірлеген.

БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

БҰҰ ЕҚБ – Біріккен Ұлттар Ұйымы Есірткі және қылмыстылық бойынша басқармасы;
АСЕАН – Ассоциация государств Юго-Восточной Азии (Association of South East Asian Nations);
CVV коды - Card Verification Value/Code;
PIN-код (Personal Identification Number) – жеке сәйкестендіруші нөмір
CERT (Computer emergency response team) – компьютерлік оқиғаларға әрекет ету тобы
ГЛОНАСС глобальная навигационная спутниковая система
VPN (Virtual Private Network) – виртуалды жеке желі
NAT (Network Address Translation) – желі мекенжайларының аудармашысы
UMTS (Universal Mobile Telecommunications System) – әмбебап мобильді телекоммуникациялық жүйе
GPRS (General Packet Radio Service) – жалпы қолдану пакеттік радиобайланысы
UFED (Universal forensic extraction device)

КІРІСПЕ

Өзектілігі. XXI ғасыр – ол жаңа білім және технологиялар дәуірі. Бүгінгі күні жер бетінде 4-индустриялық революция жалғасуда, ол дегеніміз 21-ғасырдың басынан жасанды интеллекттің және Интернеттегі үлкен деректердің дамуының орын алуы. Мемлекетіміз өзінің егемендігінің төртінші онжылдығына аяқ басты. Болып жатқан пандемияға байланысты шектеу шараларының нәтижесінде азаматтар ақпарттық-технологиялар жетістіктерін қолданып, Интернет желісі арқылы көптеген тұрмыстық мәселелерін шешті, мысалы, банк операциялары, құжаттарды рәсімдеу, заттар, өнімдерді және қызметтерді сатып алу сияқты.

Алайда бұл ақпараттық-технологияларды қолданудың теріс қырлары да бар. Олардың бірі – қызмет көрсету мен тауар сату саласындағы интернет желісі арқылы ақпарттық жүйені қолданушыға қатысты жасалатын алаяқтық. Бұл қылмыс түрінің саны 2020 жылда 2019 жылмен салыстырғанда екі есе өсті. Ал биылғы жылмен салыстыратын болсақ 2020 жылдың бірінші үш айында алаяқтықтың бұл түрі 3311 болған, ал 2021 жылғы осыған ұқсас кезеңінде оның саны 8732 болды. Ішкі істер министрлігі интернет-алаяқтық санының күрт өсуін аталып өткен пандемияға орай енгізілген шектеу шараларының байланыстырады.

ҚР БП Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің есебіне жүгінетін болсақ интернет желісінде ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтық туралы қылмыстық істердің 70% бойынша сотқа дейінгі тергеу мерзімі «қылмыстық құқық бұзушылықты жасаған тұлға анықталмаған» деген негізде тоқтатылады.

Интернет желісінде ақпарттық жүйені қолданушыға қатысты орын алатын тауар сату мен қызмет көрсету саласындағы алаяқтықты тергеу барысында туындайтын проблемалардың себептері:

- мұндай қылмыстар шетелден жасалады, шет мемлекеттердің ресурстары пайдаланылады немесе жымқырылған ақша басқа елдердің аумағында қолма-қол ақшаға айналады;
- интернет ресурстардағы электронды дәлелдемелердің сақталу мерзімі өте қысқа, ал Қазақстан Республикасы және шетелдер арасында электронды дәлелдемелерді уақытша сақтау және кейіннен сұрау салу мәселесі бойынша халықаралық ынтымақтастық реттелмеген. Демек бұрыннан қалыптасқан құқықтық көмек көрсету процесі электронды дәлелдемелерге қатысты қолдануға келмейді.
- қылмыс түрін тергеу бойынша мемлекет аумағында құқық қорғау органдары, байланыс операторлары, қаржы ұйымдарының арасындағы ынтымақтастық реттелмеген;
- тауар сату және қызмет көрсету саласындағы интернет арқылы жасалатын алаяқтықты тергеу методикасы мен тактикасы туралы ғылыми базаның тапшылығы;

- аталған қылмыстарды тергеумен айналысатын тұлғалардың жеткілікті біліктілігінің жоқтығы;
- тауар сату және қызмет көрсету саласындағы алаяқтықты тергеу практикасының аздығы;
- ақпараттық технологиялар арқылы жасалатын қылмыстар латентті болып табылатындығы;
- аталған қылмысты алдын алу мен тергеу методикасы және тактикасы бойынша шет мемекеттермен тәжірибе алмасу жеткіліксіз;
- киберқылмыстар туралы Будапешт конвенциясы Қазақстан Республикасымен ратификацияланбаған.

Ақпарттық-технологиялар саласында алаяқтық жасаудың әртүрлі схемалары мен тәсілдері кеңінен таралған, қылмыскерлер ғылыми-техникалық прогрестің жетістіктерін және пандемияға байланысты орнаған жағдайды белсенді қолдануда.

Тауар сату және қызмет көрсету саласындағы ақпарттық жүйені қолданушыға қатысты алалықтың құрбандары тек жеке тұлғалар емес, сонымен бірге барлық меншік нысанындағы заңды тұлғалар, мемлекеттік және муниципалды органдар, мекемелер мен ұйымдар болып табылады.

Құқық қорғау органдарың қызметі ғылыми жұмыстар және олардың негізінде әзірленген тергеу жөніндегі практикалық ұсыныстарды қолданған кезде ғана интернет желісіндегі алаяқтыққа қарсы іс-қимыл тиімді болатыны анық. Бүгенде тергеушілер мен жедел уәкілдер әлі де ұқсастықтары бар компьютерлік қылмыстарды тергеу және жалпы қылмыстарды тергеу бойынша ұсыныстарды қолдануды жалғастыруда. Бұл әрине құқық қорғау органдарының аталған фактілерді уақтылы анықтау және ашуды тежеуге әкеліп соғады.

Ақпараттық технологияларды мемлекетімізде қолдануды жетілдіру үлкен жұмыс. Мемлекет басшысының 2017 жылғы 31 қаңтардағы "Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік" атты Қазақстан халқына Жолдауын іске асыру жөніндегі шаралар туралы" Қазақстан Республикасы Президентінің 2017 жылғы 15 ақпандағы № 422 Жарлығын іске асыру мақсатында Қазақстан Республикасының Үкіметі 2017 жылғы 30 маусымдағы № 407 қаулысымен Киберқауіпсіздік тұжырымдамасын ("Қазақстанның киберқалқаны") бекітті.

Тақырыптың ғылыми зерттелу дәрежесі. Ақпарттық технологияларды қолдану арқылы жасалатын алаяқтықты тергеу бойынша Ресей Федерациясының заң ғылымы кандидаттары И.Е.Мазуров, В.В.Коломинов, А.А.Комаров, Р.С.Атаманов, К.В. Камчатов және тағы басқалардың ғылыми жұмыстары бар. Скобелин С.Ю. Колычева А.Н. А.Л.Осипенко, А.И.Гайдин, М.В. Старичков, В.А.Антонов, В.Б.Вехов, Р.И.Оконенко, Р.Г.Бикмиев, Р.С. Бурганов, К.Е.Демин және А.А.Васильев және басқалар электронды дәлелдемелер және оларды алу, қарап-тексеру туралы ғылыми жұмыстар жазған.

Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясында тақырыппен байланысты келесі жұмыстар бар:

1) «Актуальные проблемы совершенствования практики расследования преступлении в сфере компьютерной информации», заң ғылымдарының кандидаты Назмышев Р.А., 2003 жыл;
2) «Противодействие мошенничеству, совершенному с использованием информационных технологий: современное состояние и перспективы развития Муратов К. С., 2019 жыл
3) «Особенности и тактика расследования, раскрытия уголовных правонарушений против собственности совершенных с использованием информационных технологий» Тажигулов Н.Т., 2017 жыл.

Ғылыми баслымдардың көп болғанына қарамастан, дәл осы тауар сату және қызмет көрсету саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықты тергеу методикасы қарастырылмаған. Өйткені көпшілік ғылыми жұмыстардың мазмұнында жоғары технологиялар саласындағы қылмыстар тақырыбында алаяқтық туралы жеңіл шолынып қана айтылады да, негізгі назар компьютерлік ақпараттандыру саласындағы алаяқтыққа аударылған. Сонымен қатар бұрын жазылған ғылыми басылымдарда дәстүрлі, оқиға орнын қарап-тексеру, жауап алу, беттестіру, сараптама жүргізу сияқты тергеу әрекеттерін жүргізуге көңіл бөлінген. Алаяқтықтың бұл түрінің жоғары латенттігі, олардың ашылу көрсеткіштернінің төмендігі, алаяқтықты тергеуде елеулі олқылықтардың болуы, терегудің тиісті әдістемелік қамтамасыз етудің жеткіліксіздігін көрсетеді. Осы жұмыста бүгінгі криминогендік жағдайды ескере отырып, жеке ақпарттық жүйені қолданушыға қатысты алаяқтықты тергеу методикасы ұсынылатын болады.

Зерттеу мақсаты қызмет көрсету мен тауар сату саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықты тергеу әдістерін ашып көрсету, ғылыми тұжырымдау.

Зерттеу объектісі қызмет көрсету мен тауар сату саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықты тергеумен байланысты қоғамдық қатынастар.

Зерттеу заты қызмет көрсету мен тауар сату саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықты тергеу әдістері мен тәсілдері.

Зерттеудің құқықтық базасы Казақстан Республикасының Конституциясы, Қазақстан Республикасының Қылмыстық кодексі, Қазақстан Республикасының Қылмыстық процестік кодексі, Қазақстан Республикасының Азаматтық кодексі, Ақпараттандыру туралы Заң, Дербес деректер және оларды қорғау туралы Заң, Электрондық құжат және электрондық цифрлық қолтаңба туралы Заң, Байланыс туралы Заң, Киберқауіпсіздік тұжырымдамасын бекіту туралы қаулы, Ақпараттық-

коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы қаулысы.

Диссертациялық зерттеу барысында қазіргі заманға сай ғылыми тану әдістері қолданылады, олардың қатарына мыналар жатады: жалпы ғылыми, арнайы, (құрылымды жүйелік, аксиматикалық), сонымен қатар эмипирикалық (айғақтарды зерттеу және жинау, сапалы талдау және синтез).

Зерттеудің әдістемелік және методологиялық негізі: методологиялық базаға құқықтық, тарихи құқықтық, заңдық-логикалық талдау, құжаттарды талдау, қылмыс статистикасы жатады.

Ғылыми жаңалықтың негіздемесі. Ақпарттық жүйені қолданушыға қатысты тауар сату және қызмет көрсету саласындағы интернет желісінде орын алатын алаяқтықты ақпараттық-технологиялардың заманауи жетістіктерін қылмыстарды ашу және тергеу қызметіне интеграциялау мәселелеріне арналған монографиялық сипаттағы кешенді ғылыми-практикалық зерттеу жүргізілгендігімен негізделеді. Жүргізілген зерттеу жұмысы аталған қылмыс түрін тергеу методикасын құрауға және негіздеуге мүмкіндік береді. Жекелеген процестік және тергеу әрекеттерін жүргізуді жоспарлау және ақпараттық-технологиялық қамтамасыз ету бойынша жаңа криминалистикалық ұсыныстар келтірілді.

Қорғауға шығарылатын тұжырымдар:

1) Қазақстан Республикасының әр облыс орталығында (қазір тек Нұр-Сұлтан және Алматы қалаларынан ғана алу жүргізу мүмкін) ұялы-байланыс операторларының кеңсесінен (филиалынан) абоненттер арасындағы кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтерді алуды жүргізудің мүмкіндігін ұйымдастыру.

2) Алынған электронды дәлелдемелерді қарап-тексеру кезінде «үлкен деректерді» талдау жасайтын бағдарламаларды қолдану. Көлемді ақпарат өңделетіндіктен, криминалистік маңызы бар деректерді алу, ақпараттық технологияларды пайдаланбай өте қиын немесе көп уақытты қажет ететінін, кейбір жағдайда мүмкін емес болып табылады.

Тәжірибе көрсеткендей бір ұялы телефонды, компьютерді, гаджетті, банк картасын және т.б. қолдану арқылы бірнеше алаяқтық жасалады. Ол телефон нөмірі бойынша телефонның IMEI кодын анықтау, ал әрі қарай осы код бойынша телефонға бұған дейін немесе кейін кандай абоненттік нөмірлер орнатылғанын анықтау. Демек қылмыстың субъектісіне қатысты «жаңа» эпизодтарды анықтау мүмкіндігі пайда болады. Осылайша банк карталарымен, электронды әмияндармен (жиі Каспий голд және киви әмиян) және IP мекенжайлармен жасауға болады. Алаяқты анықтағаннан кейін, қылмыстың санаты өзгереді, осы фактілерді ҚР ҚК 190-бабының 3-тармағы 3), 4) тармақшаларымен ауыр қылмыс ретінде (екі немесе одан да көп адамға қатысты, бірнеше рет жасалған алаяқтық) саралау мүмкіндігі пайда болады.

Қызмет көрсету мен тауар сату саласындағы интернет желісі арқылы ақпарттық жүйені қолданушыға қатысты жасалатын алаяқтықты тергеу әдістемесі жасалды.

3) Электрондық дәлелдемелерді қолданудағы басты мәселе – жол беру немесе сенімділік критерийлерін белгілеу және бұл заңды тұрғыдан тұжырымдалған жалпы қағидаттар емес, техникалық критерийлер болуы керек. Мұндай дәлелдерге әлі де сенімсіздік байқалса да, олар басқа дәлелдермен салыстырғанда анағұрлым сенімді, оларды алу және сақтау кезінде субъективті факторларды неғұрлым төмендетеді. Дәлелдемелерді сақтау камерасына ұқсас виртуалды электронды ақпаратты сақтауға арналған сертификатталған құру туралы ой, сондай-ақ осы деректерді сотқа олардың тұтастығы мен өзгермейтіндігін тексеру арқылы жолдайтын ведомствоаралық желілер құру туарлы ойлар қызықты деп ойлаймын. Қазір бұл туралы айту, әрине, ертерек, бірақ мұндай мүмкіндік қылмыстық процессте электрондық ақпаратты қолдануды дамытудың бағыты бола алады.
4) Ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықты тергеуді жеңілдеті үшін шетел уәкілетті органдарымен және провайдерлермен ынтымақтастық орнату үшін электронды құжаталмасуды пайдаланып, жаңа жеңіл жолын құрастыру және тиісті халықаралық нормативті құқықтық актілерді ратификациялауға шаралар қабылдау қажет.

Апробация және нәтижелерін енгізу. Қызмет көрсету мен тауар сату саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықты фактілерін тергеуді жетілдіру, оңтайландыру жолдарын тауып, практикаға енгізу. Диссертацияда айтылған негізгі тұжырымдар 2020 жылғы 10 сәуірде Қазақстан Республикасы Бас прокуратурасының жанындағы құқық қорғау органдары академиясы өткізген «Қазіргі заң ғылымының дамуы: теория және практика» халықаралық ғылыми-тәжірибелік конференциясына «Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтық - латенттігі жоғары қылмыс» және 2020 жылғы 26-27 қарашада өткен «Инновациялық зерттеулердің тиімділігін арттырудың модельдері мен әдістері» атты халықаралық ғылыми-тәжірибелік конференциясында «Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтықты тергеудегі шетел тәжірибесі» атты ғылыми мақалалар арқылы өз көрінісін тапты. Сондай-ақ диссератциялық зерттеу жұмысының нәтижелері Нұр-Сұлтан қаласы ПД Байқоңыр аудандық ПБ Тергеу бөлімінің қызметіне енгізілді.

1. БӨЛІМ. Қызмет көрсету мен тауар сату саласындағы интернет желісі арқылы жасалатын алаяқтық криминалистикалық талдау объектісі ретінде

1.1 Қызмет көрсету және тауар сату саласындағы алаяқтықтың пайда болуы, даму тенденциясы және жалпы криминалистикалық сипаттамасы

Құқық қорғау органдары коронавирустық пандемия кезінде киберқылмыстың өршуін бақылауда, интернет-алаяқтықтың жаңа жолдарын анықтап, азаматтардың алдану фактілерінің одан әрі өршитінін болжауда.

Әр жыл сайын олардың схемалары күрделі әрі егжей-тегжейлі ойластырылған болып барады, қылмыскерлер жаңа технологияларды аса табандылықпен игеруде, интернет-қызметтер нарығы алаяқтардың мүмкін емес тиімді ұсыныстарына толы, ал олардың құрбандары өздерінің активтарымен ерікті түрде бөлісуге дайын.

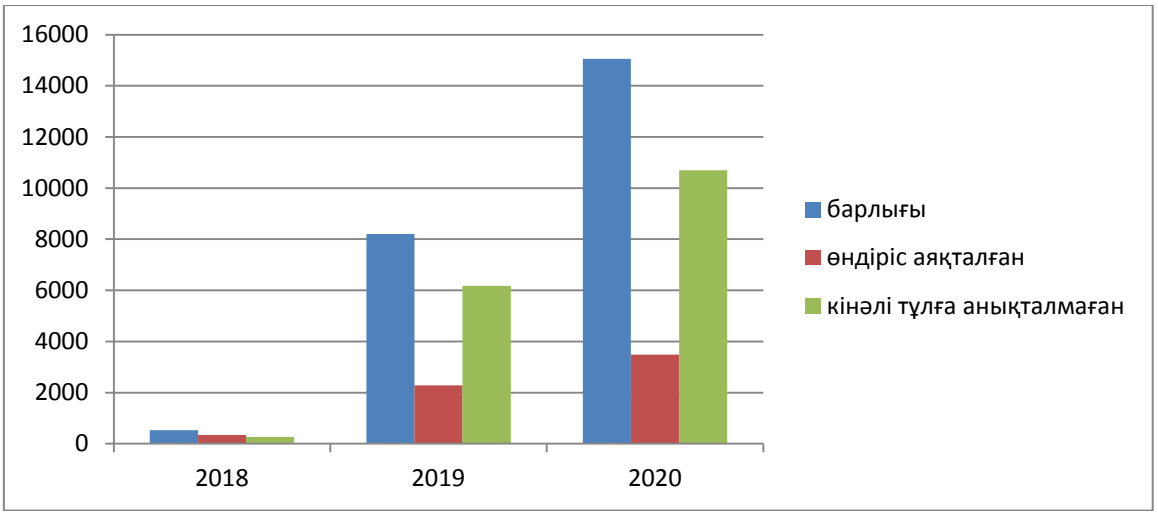
Кейбір жағдайда, алаяқтардың құрбаны болу үшін ақшаның да қажеті жоқ-өйткені олар әртүрлі айла-әрекеттер жасау арқылы адамдарды несие алуға мәжбүр етіп, оларды бар дүниесінен айырып тынады.

Интерполдың «interpol.int.» ресми сайтында жарияланған статистикасы бойынша әлемде жүріп жатқан коронавирустық пандемия кезінде көшедегі қылмыс деңгейі төмендеп, оның орнына IT-технология саласындағы қылмыстар пайда болған.

ҚР БП Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің есептерінен алынған мәліметтер бойынша 2018 жылы барлығы 535 интернет-алаяқтық тіркелген, 349 бойынша ақтамайтын негізде шешім қабылданған, ал 269 бойынша «қылмыстық құқық бұзушылықты жасаған тұлға анықталмаған» деген негізбен сотқа дейінгі тергеу мерзімі үзілген.

2019 жылы барлығы 8210 интернет-алаяқтық тіркелген, 2281 бойынша ақтамайтын негізде шешім қабылданған, ал 6172 бойынша «қылмыстық құқық бұзушылықты жасаған тұлға анықталмаған» деген негізбен сотқа дейінгі тергеу мерзімі үзілген.

2020 жылы барлығы 15058 интернет-алаяқтық орын алса, 3481 бойынша ақтамайтын негізде шешім қабылданған, ал 10699 бойынша «қылмыстық құқық бұзушылықты жасаған тұлға анықталмаған» деген негізбен сотқа дейінгі тергеу мерзімі үзілген[1].



Интернет желісіндегі алаяқтықтың даму тарихын С.Я.Казанцев келесі кезеңдерге бөледі:

I кезең 1970-1990 жылдар аралығында Интернет желісіндегі қылмыстылық түзілген. Бұл кезеңде интернеттегі қылмыстарды аздаған мамандар жасаған. Кейіннен компьютерлік қылмыстарды жасаушы мамандар пайда бола бастаған.

II кезең 1990-2000 жылдар аралығында Интернет дәстүрлі қылмыстарды жасау үшін қолданыла бастаған. Осы дәуірде ауқымды ұлттық «хаккерлер топтары» пайда болған. 2000 жылдардың басында Интернет-желісін қолданушылардың саны жүздеген миллионға жеткендітен және күніне мыңдаған жаңа қолданушылар қосыла бастағандықтан, қылмыстың бұл түрінің күрт өсуі таң қалдырмайды.

III кезең 2000 жылдан бастап осы күнге дейін жаһандық желідегі қылмыстылық ұлтаралық сипатқа ие болды. Кибертерроризмнің, халықаралық хакерлік топтар барлық Интернет қылмыстылықтың салаларынан көрініс тапқан. Интернет саяси мақсаттарда қолданыла бастады[2].

СССР аумағында алғаш компьютерді қолдану арқылы жасалған қылмыс ресми түрде 1979 жылы Вильнюс қаласында тіркелген. Осы факт компьютерлік қылмыстардың халықаралық тізілімдемесіне енгізілген және постсоветтік алаңда қылмыстың бұл түрінің дамуының бастапқы нүктесіне айналған. Дәл осы сәтте бұндай қылмыстарды жасаған үшін қылмыстық-құқықтық жауапкершілікке тарту мәселесі талқылана бастады [3].

Интернет желісіндегі қылмыстылықтың дамуы, оған қарсы іс-қимыл әдістемелерін жетілдіру мақсатында интернет-алаяқтықты жеке классификациялау қажеттілігі туындаған.

ҚР ІІМ мәліметтеріне сәйкес алаяқтықтың ең көп тараған түрі – ол интернет-аландардағы тауарларды сату немесе қызметтерді көрсету туралы хабарландыруларды орналастырумен байланысты.

Интернеттегі қылмыстардың көпшілігі трансшекаралық сипатта болғандықтан, тергеу процесінің жұмысын қиындатады. Өйткені жәбірленуші бір аймақта, ал алаяқ басқа аймақта немесе басқа елде болуы әбден ықтимал.

Қылмыстың тізбегі әдетте күрделі және бірнеше сатыдан тұрады. Олар әр түрлі банк шоттарын, карталарын, электронды әмияндарын, сонымен қатар үшінші тұлғаларға ресімделген абоненттік нөмерлерді пайдаланады. Көбінесе қолма-қол ақшаны алу үшін жалған адамдардың көмегіне жүгінеді. Аталған құқық бұзушылықты ашу мақсатында заңнама аясында алынған барлық деректерді мұқият талдауға белгілі бір уақыт қажет.

Біздің зерттеуіміздің деректеріне сәйкес, криминалистикалық сипаттама қылмыстарды тергеуде маңызды рөл атқаратындығы және оны дұрыс түсіну қылмыстарды жылдамырақ тергеуге ықпал ететіндігі белгілі болды. Қызмет көрсету және тауарларды сату саласындағы алаяқтықтың криминалистикалық сипаттамасы талдау деректеріне сүйенсек, аталған қылмыс санатының ерекшелігін, яғни бізге мәлім және бұрын зерттелген қылмыстардан айтарлықтай айырмашылықтары барын көрсетуге болады.

Бұл кезде криминалистикалық сипаттама, дәлелдеуді қажет ететін мән-жайлар, қылмыстық іс қозғау ерекшеліктері, бастапқы, кейінгі және соңғы сатыларындағы тергеу ерекшеліктері сияқты элементтерден тұратын қылмыстың жекелеген түрлерін тергеу әдістемесін пайдалану маңызды [4].

«Қылмысты тергеу әдістемесі» туралы ғылыми еңбектерін талдай келе, аталған ұғымға төмендегі анықтамалар берілетінін байқаймыз. Ең тиімді анықтаманы Ресей Федерациясының еңбек сіңірген ғылым қайраткері, заң ғылымдарының докторы В. Е. Корноухов берген: қылмысты тергеу әдістемесі – бұл қарама-қайшылыққа толы бастапқы тергеу жағдайының дәлелдеу тақырыбымен байланысты тактикалық міндеттер мен операциялар жүйесі(тергеу әрекеттерінің кешені мен жедел-іздестіру іс-шаралары және басқа шаралар), ол аралық және құқықтық тергеулерді белгілеу мақсатында дәлелдеулер жүйесін қалыптастыруға бағытталған [5].

Ал қылмыстардың криминалистикалық сипаттамасы дегеніміз нақтылы криминалистикалық әрекетті (қылмыс түрін немесе тобын) ғылыми талдаудан өткізу нәтижесі, оның белгілері мен ерекшеліктерінің жинағы. Мұндай абстрактілі ғылыми түсінікке түпнұсқалы ақпарат сипаттамасы, қылмысты жасау және жасыру туралы мәліметтер жүйесі, анықтауға жататын жағдайлардың ерекшелігі, қылмыскер болуы ықтимал адамның сипаттамасы, нақты қылмысқа тән жағдайларды суреттеу жинақталған [6].

Қызмет көрсету және тауар сату саласындағы алаяқтықты тергеу үшін қылмыстың криминалистік сипаттамасының танымдық мәні тергеудің бастапқы кезеңінде тергеушіде тергеу жүргізіліп жатқан қылмыс туралы нақты ақпараттың аз көлемде болуы.

Компьютерлік ақпарат саласындағы алаяқтықтың криминалистік сипаттамасының элементтеріне толығырақ тоқтайық. Қызмет көрсету және

тауарларды сату саласындағы алаяқтықтың криминалистік сипаттамасының негізгі компоненттері:

- Қызмет көрсету және тауарларды сату саласындағы алаяқтықтың жасалу жолдары;
- Қызмет көрсету және тауарларды сату саласындағы алаяқтық ізінің түзілу механизмдері;
- Қызмет көрсету және тауарларды сату саласындағы алаяқтықтың орны, уақыты;
- Қылмыстың жәбірленушісі;
- Қылмыскердің түр-тұлғасы;
- Ақпарттық жүйелерді қолданушыға қарсы жасалатын алаяқтықтың себептері және салдары.

Қызмет көрсету және тауарларды сату саласындағы алаяқтықтың келесі криминалистік ерекшеліктерін атап көрсетуге болады:

- Деректер бір түрден келесі түрге тез ауысып, интернет желісі бар кез-келген елге, кез-келген арақашықтыққа барлық машиналық тасымалдау құралдары арқылы тез тарайды және көбейеді;
- Цифрлық ақпараттарды алумен байланысты іс-әрекеттерде қиындықтар туындайды, өйткені бастапқы дереккөздерді, мәліметтердің таралу жолдарын, байланыс және тарату арналарын анықтау қиынға соғады;
- Арнайы техникалық құрал-жабдықтардың көмегімен деректерді оңай және тез жою;
- Компьютерлік деректерді алынбалы ақпарат тасымалдығыштарға көшіру.

Қарастырылып отырған қылмыстық іс-әрекеттің күрделілігін ескере отырып, бұл алаяқтықтың орындау тәсілінің толық құрылымы бар екенін атап өткен жөн. Ол алаяқтықты жасаудағы даярлықтан және оны жүзеге асыру тәсілінен, сонымен қатар қылмыстың іздерін жасыруға бағытталған әрекеттерден тұрады. Қызмет көрсету және тауарларды сату саласындағы алаяқтықтың ерекшелігі қылмыскерлер даярлық кезеңінің өзінде-ақ, қылмыстың іздерін жасыруға бағытталған іс-әрекеттерді жүзеге асыратындықтарын ескерген жөн. Мысалы, абоненттік нөмерлерді үшінші тұлғаларға сату немесе иесінің деректері көрсетілмейтін виртуалды әмиян тіркеу.

Таңдалған әдіске байланысты қылмыскерлер арнайы сайттарды әзірлейді, ол жерде жәбірленуші өзінің банктік картасы туралы ақпаратты көрсетеді. Сол сияқты, алаяқтық жасау әдісіне байланысты құралдар мен жабдықтар (компьютер, компьютерлік бағдарламалар, интернет, ұялы телефон, әлеуметтік желі, мессенджерлер және т.б.), сонымен қатар алаяқтық жасау кезінде берілген рөлдері бойынша өздеріне жүктелген міндеттерді атқаратын адамдар таңдалып алынады.

Аталған адамдарды таңдаудағы ерекшелік, кейбір жағдайларда олар өздерінің іс-әрекеттерінің шынайы мақсатын біле бермейді (банктік

шоттарды ашу, құрал ретінде қолдану үшін сатып алынған абоненттік нөмір, курьерлік қызмет және т.б).

Осы іс-әрекетті жасау тәсілдерінің толық тізбесі болмағандықтан, мен біздің республика аумағында қызмет көрсету және тауарларды сату саласында алаяқтық жасаудың кең таралған тәсілдерімен таныстырғым келеді:

1. Интернет-сауда саласындағы алаяқтық. Дүкендегі тауарға тапсырыс беріп, төлегеннен кейін пайдаланушы оны мүлдем алмайды немесе пошта арқылы бос қорапты алып, оған төлемақы жасайды.

Мысалға кең таралған схемалардың бірі: алаяқтар өз құрбандарын сатылатын мүліктің немесе ұсынылатын қызметтің төмен бағасымен, жеделдігімен, жаппайсатылым және т.б. қызықтыру арқылы өздеріне көңіл аудартады. Сатып алушылардан электронды әмиян немесе банктік картаға алдын-ала төлемақы жасалуы сұралады. Бірнеше күн ішінде "сатушы" тауарларды тез жеткізуге уәде береді, содан кейін із-түссіз жоғалады. Әдетте, алаяқтықтың осындай түрін жасауда виртуалды электрондық төлем жүйелері, сондай-ақ үшінші тұлғаларға ресімделген банктік төлем карталары пайдаланылады.

Сондай-ақ, алаяқтар жалған интернет-дүкен немесе атақты сайттардың аналогын жасап, ол жердегі тауарларға төлем жасау әдістерін көрсетеді. Сайттың сенімді екенін анықтау өте қиын. Аударылған барлық ақша дүкен иесінің шотына түседі, ол алдын-ала төлем алғаннан кейін тауарды жібермеуі немесе сапасыз, тіпті басқа түрін жіберуі мүмкін.

2. Жалған сатып алушылар тауарларды, автокөліктерді және т.б. сатып алу сылтауымен орналастырылған хабарландырулар бойынша қоңыраулар шалады. Әңгіме барысында «сатып алушы» тауарды алатындығы туралы келісімге келіп, басқа адамға сатылып кету қаупінен сақтану мақсатында кепіл ретінде кепілпұл алуын сұрайды. Ақшаны аудару үшін пластикалық картасының нөмерін сұрайды. Біраз уақыттан кейін олар жәбірленушіге тағы да қоңырау шалып, телефонға SMS-хабарлама түрінде келген кодты хабарлауды сұрайды, бұл ақша аудару үшін қажет. Немесе азаматқа ең жақын банкоматқа баруын және олардың айтқанын картамен байланысты іс-әрекеттерді жасауды сұрайды. Шын мәнінде, код алаяқтарға интернет-банкингті қосып, шотты басқару үшін қажет.

3. Ақпараттық жүйе саласындағы алаяқтықтың алдыңғы схемасына ұқсас, келесі бір түрі ол пәтер, қымбат көлік сатып алумен байланысты. Алаяқтар төмен бағамен көрсетілген пәтерлер, автокөліктерді сату туралы хабарландыру орналастырады. Алайда сатып алушы көрсетілген абоненттік нөмірге хабарласа алмайды (немесе хабарламада мессенджердің байланыс нөмірі көрсетіледі). Хат алмасу барысында алаяқ басқа қалада немесе шетелде екенін түсіндіреді. Ақшаның болуына кепілдік ретінде өзіне немесе туысына халықаралық төлем жүйесінде (Unistream, Western Union және т.б.)

шот ашуды және онда келісілген соманы аударуды сұрайды. Шот иесінің рұқсатынсыз ешкім ақша ала алмайтындығына сенімді болғандықтан, аңқау сатып алушылар ақшаны аударады және чектің суретін алаяққа жібереді.

4. Алаяқтар көптеген хабарландыруларды зерттейді. Жәбірленушіні таңдап алғаннан кейін, олармен мессенджер арқылы сатып алушы ретінде хат алмасады да, сатып алу туралы жалған келісімге келеді. Ақша аудару үшін алаяқтар сілтеме жібереді де, оны басуды сұрайды. Бір қарағанда сілтеме ешқандай күдік тудырмайды, бірақ сілтеме басылған сәтте, пайдаланушыны фишингтік сайтқа өткізіп жібереді. Бұл сайтта банктік картаны, CVV-кодты, ЖСН көрсетіп,сауалнама толтыру қажет. Барлық деректемелер толтырылғаннан кейін банктік картадан ақшаны рұқсатсыз алу жүзеге асырылады. Жоғарыда көрсетілген деректемелерді алғаннан кейін алаяқтар тез арада төлем картадағы барлық қаржыны ұрлап алады. Осы уақытта сайт бірнеше секунд ішінде бұғалауланады да ешқандай із қалдырмайды. Пандемия кезінде ақпараттық жүйеде дәл осындай схема бойынша алаяқтықтың жаңа тәсілі пайда болды, бұл жерде алаяқтар өздерін жеткізу қызметіненбіз дейді.

5. Жұмысқа орналастыру, қандай да бір бұйымды әзірлеу бойынша қызметтер көрсету, несиеге ақшалай қаражат алуға жәрдемдесу, әлеуметтік төлемдерді алуға көмек көрсету, риэлторлық қызметтер саласындағы алаяқтық.

6. Танымал тұлғалармен жалған бейнероликтерді қолдану схемалары. Қолданушыға қарап шыққаннан кейін тіркеу сілтемесіне өтіп, тегін немесе тиімді бағамен тауарды алу ұсынылады. Бұндай схемаларды дипфейктермен жасалған схемалар деп те атайды. Сілтеме арқылы өткеннен кейін жәбірленуші фишингтік сайтқа түседі де, алаяқтық құрбанының енгізген жеке деректері қылмыскер қолына түседі.

Ақпарттық жүйе арқылы жасалатын алаяқтық өзіне тән арнайы із қалдырады. "Цифрлық іздер" ақпараттық кеңістіктегі компьютерлік және өзге де цифрлық құрылғылардың, олардың жүйелері мен желілерінде кез келген іс-әрекеттің (қосу, құру, ашу, іске қосу, өзгерістер енгізу, жою) жасалу іздерін білдіреді.

Электрондық ақпараттың құрылу, өңделу және сақталу ерекшелігі, осы мақсаттар үшін материалдық құралдар (ұялы телефондар, компьютерлер және т.б.) қолданылады. Аталған құрылғылардың жадында электрондық ақпараттың материалдық-фиксация жасалу мүмкіндігін көрсетеді. Компьютерлік ақпаратты анықтау, алу және зерттеу үшін, тіпті оның бұғатталуын немесе жойылуын және т.б. ескерсек те, цифрлық іздер сақталған компьютерлік құралдар алынады.

Келесі криминалистік сипаттама – ол қызмет көрсету және тауарларды сату саласындағы алаяқтықтың жасалу уақыты. Ол нақтыланбаған.

Қылмыстық істерді зерттеу барысында, қылмыстың бұл түрі тәуліктің әртүрлі уақытында және әртүрлі уақыт кезеңдерінде жасалғанын көруге болады.

Криминалистикадағы қылмыс орны дәстүрлі түрде қылмыстың объективті жағы жүзеге асырылатын орын ретінде анықталады. [7]

ҚР ҚПК-нің 188 бабына сәйкес, қылмыстық құқықбұзушылық қай ауданда (облыста, республикалық маңыздылығы бар қалада) жасалды, сол жерде сотқа дейінгі тергеу жүргізіледі.

Сотқа дейінгі тергеп-тексерудің жедел және толық болуы мақсатында ол қылмыстық құқық бұзушылық анықталған орын бойынша, сондай-ақ күдікті немесе куәлардың көпшілігі тұратын жерде жүргізілуі мүмкін.

Қазақстан Республикасы Жоғары Сотының 2017 жылғы 29 маусымдағы №6 «Алаяқтық туралы істер бойынша сот практикасы туралы» нормативтік қаулысының 8 тармағы негізінде, алаяқтық жымқырылған мүлік алып қойылған және кінәлінің немесе басқа адамдардың заңсыз иеленуіне өткен және олар оны меншік мүлкі ретінде өздерінің қалауы бойынша пайдалануға немесе билік етуге нақты мүмкіндік алған сәттен бастап аяқталды деп танылады.

И.Н.Воробецтің айтуы бойынша, желідегі ақпараттың қозғалысын бақылау мүмкіндігінің басты ерекшелігі – ол IP-хаттамамен сипатталған интернет желісіндегі мекенжай жүйесі желіге қосылған әрбір компьютерге бірегей сәйкестендіру нөмірін (IP-мекенжай) беру негізінде құрылған. IP мекенжайы-нүктелермен бөлінген төрт Ондық сандар жиынтығы (мысалы, 192.168.100.47.). Ыңғайлы болу үшін цифрлы мекенжайлар домендік атауды түрлендіру жүйесін қолдана отырып, таңбалармен ауыстырылады. Домен жүйесі белгілік атауларды IP мекенжайларға айналдырады және домен атауын цифрлы мекенжайға кері айналдыра алады. IP мекенжайлар статистикалық және динамикалық болуы мүмкін. Желіде ақпаратты орналастыру, оған қол жеткізу, сондай-ақ желіішілік ақпарат алмасу арнайы мамандандырылған ұйымдардың - қызметтерді жеткізушілердің (провайдерлердің) қатысуымен жүзеге асады [8].

Сондай-ақ интернет, жергілікті желілер және т.б. бойынша хабарламаларды, электрондық хаттарды, оларды алуға келісім бермеген адамдарға жіберетін субъектілер бар, әдетте, KZ домендік аймағынан тыс жердегі электрондық мекенжайларды пайдаланады, бұл олардың IP-мекенжайлары туралы мәліметтерді дәл уақытында алуға мүмкіндік бермейді.

Қазіргі заманғы ақпараттық және банктік технологиялардың дамуына байланысты ұялы байланыс арқылы эфирге шығу, сондай-ақ шотқа түскен ақшаны басқару, оның ішінде оларды қолма-қол ақшаға айналдыру, осындай басқа да қызметтерді көрсету әлемнің кез-келген жерінде мүмкін.

Мысалы, жәбірленуші тұрғылықты жері бойынша интернет-дүкеннен автокөліктің қосалқы бөлігін сатып алып, ақша аударады. Бұл жағдайда, жәбірленуші ақша аударған кезден бастап, қаскүнем өз қалауымен ақшаны басқару құқығына ие болды, сол себепті басқа адамдардың мүлкін алдау арқылы иемдену жәбірленушінің тұрған жерінде орын алғандықтан, қаскүнемнің ақша алған жерін анықтау артық деп есептеймін.

Осыдан қорыта келе алаяқтықтың объективті жағы, кез-келген жымқыру, біреудің мүлкін заңсыз алу, сондай-ақ біреудің мүлкіне иелік етудегі қылмыс орны-біреудің мүлкін алып қойған орын (мысалы, банк, банкомат, жәбірленушінің тұрғылықты жері) болып саналады.

Көрсетілген жағдайларда алаяқтық жәбірленушінің шотынан ақшалай қаражатты алдау немесе сенімге қиянат келтіру жолымен өз шотына алған тұлғаның, немесе жымқырылған қаражат кінәлінің қылмыстық әрекеттерінен, басқа адамдардың шоттарына түскен сәттен бастап аяқталды деуге болады.

Сондықтан, алаяқтықтың аяқталу орны болып жәбірленушілердің ақша аударған орны болып табылады, өйткені дәл осы жерде ол зардап шеккен болып тұр.

Осыған байланысты, алаяқтықтың аяқталу орны деп жәбірленуші қылмыскерге ақша аударған жерді айтуға болады. Бұл орында сотқа дейінгі тергеу басталып, қылмыстық іс тергелуі қажет. Сонымен қатар қылмыс жасалған жердің, қылмыс аяқталған жердің және сотқа дейінгі тергеу жүргізілетін жердің түсініктерін анықтап алу қажет.

Алдын ала тергеу жүргізілетін орын ҚР ҚПК-нің 188-бабына сәйкес анықталады, бірақ заңнамада қылмыс жасалған жердің анықтамасы берілмеген. Бұл барлық жағдайларды жеке-жеке заңда көрсетудің мүмкін еместігімен байланысты. Қылмыстың жасалу орнын әрбір нақты жағдайда құқық қорғаушы қылмыс құрамының ерекшеліктеріне, жасалған әрекеттің сипатына, қорғалатын қоғамдық қарым-қатынастарға зиян келтіруде қолданған құралдар мен тәсілдеріне қарап, өзі анықтайды.

Осылайша, әртүрлі өңірлердің ішкі істер органдарына алаяқтық туралы хабарламаларды негізсіз жолдап әуре-сарсаңға салмау мақсатында, бірден сотқа дейінгі тергеу жұмыстарын жәбірленушілер ақша қаражатын аударған орнынан бастап, соған байланысты қылмыстық істі тергеуді бастаған жөн болар еді.

Қызмет көрсету және тауарларды сату саласындағы алаяқтықтың криминалистік сипаттамасы санатының құрамдас бөлігіне, қылмыстық іс-әрекетті жүзеге асыру үшін оның материалдық, әлеуметтік-психологиялық, қоршаған ортаның өндірістік факторларын қамтитын қылмыс жасау жағдайы кіреді. Қоршаған орта қызмет көрсету және тауарларды сату саласындағы алаяқтықтың криминалистік сипаттамасының барлық басқа бөліктерін

құруға, қылмыскерлер мен зардап шеккен тараптардың мінез-құлық ерекшеліктерін табуға әсер етеді.

Ақпараттық жүйені қолданушыларға қарсы жасалған қылмысқа тән белгілердің бірі – қылмыскерлердің ер адам болуы. Интернетті пайдаланушылар арасында әйелдер мен ерлердің арақатынасы бірдей болғанына қарамастан, ер адамдардың қылмыстық белсенділігінің жоғары екенін көруге болады. Интернет-қылмыскерлер арасында ер адамдардың басым болуы, көптеген дәстүрлі қылмыстардағы сияқты, ертеден қалыптасқан ерлердің әлеуметтік белсенділігінде жатыр. Әртүрлі интернет-қылмыскерлердің жасын талдай келе, қылмыстық іс-әрекеттердің басым көпшілігін 35 жасқа дейінгі адамдар жасағанын байқауға болады, ал 18-25 жас аралығындағы қылмыскерлер жиі кездеседі. Зерттеу аясында зерделенген қылмыстық істердің ішінен интернет-қылмыскерлердің көп жағдайда тұрақты жұмыс орны және жоғары білімі жоқ екеніндігін атап өткім келеді. Тұрақты табыс көзінің болмауы, бұл Интернет желісінде жасалатын қылмыстардың себебі болып табылады.

Тауар сату мен қызмет көрсету саласындағы алаяқтықтың құрбаны тек қылмыс туралы ақпарттың көзі болып табылмайды, сонымен қоса қылмыстық істі ашудағы маңызы бар жан-жақты зерттеуге жататын объект болып табылады. Ерекше қызығушылық тудыратын жайт ол қылмыскер мен алаяқтың арасында туындайтын қарым-қатынасты зерделеу, оның негізгі құрамы құрбанның сенгіштігі мен беріліп кетушілігі, оның виктимдік мінез-құлыққа бейімділігі.

Виктимдік — ол биологиялық, психологиялық ерекшеліктер және әлеуметтік дәрежемен қамтылатын тұлғаның өзіне қатысты қылмыстың орын алуына ықпал ету қасиеті [9].

Ақпарттық жүйені қолданушыларға қатысты қылмыстар туралы виктимологиялық зерттеулер жәбірленушінің жынысына байланысты виктимдіктің дифференциациясы анықталмағанын көрсетеді. Интернет кеңістігіндегі ер адамдар саны 54,8% және әйел адамдар 45,2%. Киберқылмыстардың жәбірленушілерідің көрсеткіштері де мөлшермен осындай пайызда бөлінген [10].

Тауар сату және қызмет көрсету саласындағы интернет арқылы жасалатын алаяқтық құрбандарының жас мөлшеріне келетін болсақ зерделенген қылмыстық істер бойынша жәбірленушілердің орта есеппен 35 жасы басымырақ. Менің ойымша оған себеп болатыны жас адамдар ақпараттық жүйені белсенді қолданатындығы, әлдеқайда интернет-дүкендер, электронды әмияндар мүмкіндіктерін жиі қолданады.

Алайда қылмыскерлер әр түрлі тәуекел тобына арналған құрбанмен қарым-қатынас ерекшеліктерін ойластырған (айла, қулық, алдау құралдары) және оларды қолдануда. Олар: сәнді киімдерді немесе геджеттерді сатып алудағы, жылжымалы немесе жылжымайтын мүлікті, жиһаздарды және тағы басқа бағалы тауарларды сатып алудағы жалған делдалдық, несие алудағы

көрсетілетін көмек, сондай-ақ жалған мемлекеттік, жергілікті өкілетті органдардың көмегі, әлеуметтік үстемақы, дәрі-дәрмек, кей кезде тіпті жай көңіл бөлу (қарт адамдарға қатысты). Алдаудың күшті әсер ету тәсілдерін алаяқ әр нақты жағдайда құрбанмен қарым-қатынас барысында ашылатын құрбанның жеке басының ерекшеліктеріне байланысты қолданады.

Сонымен, виктимологиялық көз-қараспен қарағанда тауар сату және қызмет көрсету саласындағы интернет арқылы жасалатын алаяқтықтың құрбандарына әлеуметтік-демографиялық, психологиялық мінез-құлық ерекшеліктері тән.

Тауар сату және қызмет көрсету саласындағы интернет арқылы жасалатын алаяқтық құрбандарының келбетін жалпылама суреттейтін болсам:

1) әйел адам да еркек адам да құрбан болуы мүмкін;
2) жасы кез-келген болуы мүмкін, алаяққа оның мүлкі болып, оны иелене алса болғаны;
3) білімі және әлеуметтік жағдайы әртүрлі болуы мүмкін. Ол қылмыскердің криминалдық-кәсіпқойлығына байланысты;
4) жанұя жағдайы маңызды емес;
5) еңбек ету саласы, экономикалық қызмет саласы және қаражаттың көлемі (мүліктің түрі және бағасы) алаяқтықтың түріне зор әсері бар.
6) ықтимал құрбанның құқықтық сауаттылығы немесе сауатсыздығы оның виктимдік деңгейіне әсер етуі әбден мүмкін;
7) ықтимал құрбанның психологиялық және физиологиялық жағдайы да оның виктимдік деңгейіне әсер етеді.

Қорытындылай келе, тауар сату және қызмет көресту саласындағы интернет арқылы жасалатын ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықтың криминалистикалық сиппатамасын қысқаша түйіндеуге болады. Қылмыстың бұл түрін жасау жолдары заманға байланысты өзгеріп отырады. Демек, нақты жасалу жолдарын анықтап алу мүмкін емес, әлеуметтік-экономикалық жағдайға байланысты жаңарып отырады.

Ал аталған қылмыс түрін тергеудің ерекшелігі – «цифрлық іздер» қалдырылуы. Олардың құрылу, өңделу және сақталу жолдарының күнделікті жаңаруына байланысты құқық қорғау органдарының «цифрлы іздермен» жұмысының бірге аяқ алып жүруі маңызды.

Тауар сату және қызмет көресту саласындағы интернет арқылы жасалатын алаяқтық тәуліктің кез-келген уақытында орын алуы мүмкін, ал қылмыс орнын анықтау туралы мәселелер бар.

Зерттеу аясында зерделенген қылмыстық істердің ішінен интернет-қылмыскерлердің көп жағдайда тұрақты жұмыс орны және жоғары білімі жоқ екеніндігін атап өткім келеді. Олардың орта жасы 35 жас дейін және басым көпшілгі 18-25 жас аралығында. Тұрақты табыс көзінің болмауы, бұл Интернет желісінде жасалатын қылмыстардың себебі болып табылады.

Қылмыс құрбанының да жас мөлшері 35, бірақ әлеуметтік дәрежесі рөл атқармайды. Оның себебі тауар сату және қызмет көресту саласындағы интернет арқылы жасалатын алаяқтықтың жолы «балық аулау» іспеттес болып келгендіктен, «қармаққа» әртүрлі тұлғалар түседі.

Криминалистикалық сипаттаманың құрамдас бөлігі - ақпарттық жүйелерді қолданушыға қарсы жасалатын алаяқтықтың себептері және салдарына зерттеу жұмысының 3- бөлімінде кеңірек тоқталып өтемін.

1.2 Қызмет көрсету мен тауар сату туралы жалған хабарлама беру арқылы жасалатын алаяқтықты тергеу бойынша шет мемлекеттердің тәжірибесі

COVID-19 пандемиясы адамдар мен қоғамды барлық жағынан өте осал етті. Осы дағдарыс кезінде біз жұмыс, байланыс, сатып алу, бөлісу және ақпарат алу үшін, сондай-ақ әлеуметтік алыстауды азайту үшін компьютерлік жүйелерге, мобильді құрылғыларға және Интернетке көбірек сенім артамыз. Қылмыскерлер бұл осалдықтарды өз мүдделері үшін қолдануда.

Компьютерлік және телекоммуникациялық технологиялар дамуы Қазақстан Республикасының аумағындағы ақпараттық жүйені қолданушыларға қатысты қылмыстардың шет мемлекеттер аумағынан жасалуына мүмкіндік берді. Демек бұл қылмыс түрі аймақаралық және трансшекаралық болып табылады. Мысалы, қылмыскер ТМД елдерінің немесе БАӘ, Тайланд сияқты елдердің байланыс операторларын, домендерін қолдануы мүмкін.

Мұндай заңсыз әрекеттерді ашудың және тергеудің күрделілігі олардың жоғары латенттігімен, жәбірленушімен жеке байланыста болмай заңсыз әрекеттерді жасауымен, компьютерлік ақпараттың ерекшеліктерімен, атап айтқанда: электронды сақтау формасымен, оның жойылу жылдамдығымен, жеңілдігімен және нақты иесінің белгісіздігімен анықталады. Сондықтан осы санаттағы қылмыстардың едәуір бөлігінің ашылуы мүмкін емес, ал қылмыстық істер қылмыс жасаған адамдарды анықтау мүмкін болмағандықтан тоқтатылады.

Байланыс операторларынан және басқа ұйымдардан қажетті ақпаратты жедел алу ақпараттық технологияларды қолдану арқылы жасалған алаяқтық әрекеттерді ашуда жетістікке жеткізеді және кінәлілерді жауапқа тартуға ықпал етеді. Жедел ақпарат алу банк секторындағы алаяқтық әрекеттерді тергеу үшін де өте маңызды. Қылмыскерлер ақша аударымы кезінде бірнеше жеке шоттар арқылы жиі қолданатын болғандықтан, қылмыстық тергеу органы олардың қозғалысын анықтау үшін бірнеше рет сотқа несиелік ұйымнан әр шот бойынша үзінді-көшірме алуға рұқсат сұрап жүгінуге мәжбүр.

Бұл жағдайлар қызмет көрсету мен тауар сату саласындағы интернет желісі арқылы жасалатын алаяқтықтың ашылуын, кінәлілерді анықтауды едәуір қиындатады және нәтижесінде тергеудің кешеуілдеуіне әкеледі.

Мысалы, Ресейдің ішкі істер органдарының бұл қылмыс түрін тергеу тәжірибесін келтірсек, Астрахан облысында өзі құрған интернет-дүкен арқылы мобильді құрылғылар мен электронды тұрмыстық техниканы арзандатылған бағамен сатқан азамат П-ға қатысты қылмыстық іс қаралды. Жарнамаланған тауарлар болмаған, ал П. төлемді алғаннан кейін оларды клиенттерге жеткізбеген. Қылмыстық іс жүргізу барысында «Yandex Money» серіктестігінен бірнеше рет алаяқтық жасау мақсатында пайдаланылған виртуалды шот туралы ақпарат сұралды.

Сонымен қатар, сатып алушылардың көптігіне байланысты Beeline ұялы байланыс операторына, VimpelCom ААҚ-на абоненттік құрылғылардың қосылуларына егжей-тегжейлі сұраулар жолданды. Тергеу аяқталғаннан кейін қылмыстық іс сотқа жіберілді, бірақ оған дейін тергеу мерзімін бірнеше рет ұзартуға мәжбүр болды [11].

Бірқатар жағдайларда ақша аударылатын сим-карталардың нақты иелерін анықтау мүмкін емес, өйткені абоненттік нөмірлер жоқ адамдарға жалған, жоғалған құжаттар арқылы тіркеледі немесе корпоративті клиенттер қолданады.

Қарастырылып жатқан заңсыз әрекеттерді құжаттандырудың ерекшеліктері, оларды ашу үшін іздерді белгілеудің маңыздылығы құқық қорғау органдары қызметкерлерінің заңдық, криминалистикалық дағдыларды меңгеріп қана қоймай, сонымен қатар компьютерлік ақпарат саласында арнайы білімдерге ие болуы керектігін көрсетеді.

Ақпараттық-коммуникациялық технологияларды қолдана отырып жасалған қылмыстардың алдын-алу, анықтау, құжаттандыру, ашу және тергеу жұмыстарының тиімділігін арттыру мақсатында Ресейдің Ішкі істер министрлігінің көптеген аумақтық органдарында, әдетте, анықтау, тергеу және қылмыстық жедел іздестіру департаменттерінің қызметкерлерінен тұратын мамандандырылған тергеу топтары құрылады, осындай қылмыстарды тергеу үшін арнайы мамандандырылған қызметкерлер енгізілуде.

Ресейдің ішкі істер министрлігі жүйесінің оқу орындарында құқық қорғау органдары ақпараттық қауіпсіздік, ақпараттық-талдауды қамтамасыз ету саласында және компьютерлік сот сараптамасы бойынша мамандар даярланады.

Қарастырылып отырған қылмыстардың аймақаралық сипатына байланысты ішкі істер органдарының қызметкерлері қылмыстың аяқталатын орнын анықтауда объективті қиындықтарға тап болған, бұл өз кезегінде тергеуге дейінгі тексерулер мен қылмыстық істер материалдарының аумақтылығының негізсіз бағытына, олар бойынша процессуалдық шешімдер қабылдаудың кешеуілдеуіне әкелді.

Осы жағдайды шешу үшін Ресей ішкі істер министрлігінің басшылығы аумақтық органдарға нұсқаулық жіберді, онда өтініш берушіден қабылдау орны бойынша белгіленген санаттағы өтініштерді қарау кезінде лауазымды тұлғалардың шұғыл жауап беру міндеттері нақты белгіленді, бұл жұмыстың тиімділігін арттырды.

Министрлік қылмыстарды анықтайтын, ашатын және тергейтін полиция қызметкерлерінің кәсіби деңгейін арттыру мақсатында тұрақты негізде әдістемелік және ақпараттық қамтамасыз етуді жүзеге асырады, қызметтік оқыту жүйесінде біліктілікті арттыру курстары ұйымдастырылады.

Бұл шараларды жүзеге асыру алаяқтыққа қарсы іс-қимылдың оң тәжірибесін дамытуға мүмкіндік береді.

Құқық бұзушылар қылмыс жасау кезінде пайдаланатын абоненттік нөмірлерді, банктік шоттарды, IP-мекен-жайларды және т.б. ақпаратты жедел жинақтау үшін Ресейдің Ішкі істер министрлігінің бірқатар аумақтық органдары тиісті мәліметтер базасын жасап шығарды.

Мысалы, Ресейде Мурманск облысы бойынша ІІМБ-да «Дистанционное мошенничество» автоматтандырылған іздеу жүйесі жасалып, қолданысқа енгізілді. Оның көмегімен аталған қылмыс түрлері ашылып, кінәлі тұлғалар анықталды, сондай-ақ әр-түрлі тергеу бөлімшелерінің өндірісінде болған бір тұлғаға қатысты қылмыстық істерді бір өндіріске біріктіруге негіз болған мәліметтер алынды.

Сонымен қатар, Ресей Федерациясының Ішкі істер министрлігі мен «Ресей Жинақ банкі» арасында электрондық құжат айналымы туралы келісімді жүзеге асыру аталған қылмыстарды тергеу кезінде органның сұрауларын қарау уақытын едәуір қысқартты.

Мемлекетіміздің қылмыстық қудалау органдары ақпараттық жүйені қолданушыларға қатысты жасалған алаяқтықты анықтау, тергеу, саралау және сот ісін жүргізуде толықтай ынтымақтасып, COVID-19 пандемиясын өз қылмыстық мақсаттары үшін қолданғандарды жауапқа тартуы қажет.

2001 жылдың қарашасында Венгрияда, Будапештте қол қойылған киберқылмыс туралы конвенция, киберқылмыс пен электронды дәлелдемелер туралы өзекті халықаралық келісім болып саналады.

Будапешт конвенциясы:

- заңсыз кіруден, мәліметтер мен жүйелерге қол сұғудан бастап, компьютерлік алаяқтық пен балалар порнографиясына дейінгі әрекеттерді қылмыстық жауапкершілікке тартуды;

- тергеуге арналған процессуалдық құқық құралдары кез-келген қылмысқа байланысты киберқылмыс пен электронды дәлелдемелердің қауіпсіздігін;

- тиімді халықаралық ынтымақтастықты қамтиды.

Әрдайым Киберқылмыс туралы Будапешт конвенциясының көмегімен орнатылған ынтымақтастық бойынша баяндамалар дайындалады. Бұл баяндамалардың мақсаты Конвенцияның артықшылықтары мен әсерін, және оның киберқылмыстар бойынша ынтымақтастыққа мүдделі мемлекеттермен және мүдделі тараптармен диалогты жеңілдету тұрғысынан жетістіктерін көрсету. Бұл осы келісімшартқа қатысушылар ұсынған ақпаратқа негізделген.

Баяндамада Будапешт конвенциясының пайдалы әсеріне дәлелдер келтірілген:

- бүкіл әлем бойынша ұлттық киберқылмыс пен электронды дәлелдемелер туралы заңнама;
- осындай заңнамаға негізделген ішкі тергеулер;
- халықаралық ынтымақтастық, оның ішінде ауыр және ұйымдасқан киберқылмысты қоса алғанда;

- мемлекеттік-жекеменшік ынтымақтастық;
- қылмыстық сот төрелігі жүйесінің әлеуетін күшейту.

Кез-келген ел Конвенцияны ішкі заңнамаға басшылық ретінде қолдануына болады,бірақ оған қосылу қосымша артықшылықтар береді:

- ол халықаралық ынтымақтастықтың құқықтық негізі ретінде қызмет етеді;
- тараптар Конвенцияны одан әрі дамытуға басшылық немесе қосымша хаттамалар арқылы үлес қосады;
- конвенцияға мүше болу, атап айтқанда осы келісім бойынша құрылған «байланыс пункттерінің 24\7 тәулік бойы жұмыс істейтін желіде» мүше болуды білдіреді;
- тараптар жеке сектормен ынтымақтастықты жақсартады;
- осы Шартқа қосылуға өтініш білдірген қатысушылар мен мемлекеттер, басымдық елдер қатарына және әлеуетті арттыру орталықтарына айналуы мүмкін.

Бұл шарт Еуропа Кеңесінің мүшелері, сондай-ақ Канада, Жапония, Оңтүстік Африка және Америка Құрама Штаттары арасында жасалғанмен, оған кез-келген мемлекет қосыла алады және көптеген Африка, Америка және Азия, Тынық мұхиты аймағындағы елдер бұл мүмкіндікті киберқылмыспен күресте тиімді қылмыстық әділет мүддесі үшін пайдалануда.

Сонымен, Будапешт конвенциясы – бұл тек заңды құжат емес, бұл тараптардың жүздеген маман-практиктері осы конвенцияның нақты ережелерінен басқа, төтенше жағдайларды қоса алғанда, нақты жағдайларда ынтымақтастықты жеңілдететін тәжірибе алмасуға және қарым-қатынас құруға мүмкіндік беретін негіз.

Будапешт конвенциясының негізінде 65 мемлекет заңның үстемдігін қамтамасыз ету үшін тиімді ынтымақтастық жасауда. Потенциалды арттыру бағдарламаларын жүзеге асыру нәтижесінде қазір көптеген мемлекеттер жедел әрекет ете алады [12].

Тәжірибедегі өзара көмек мысалдары:

Швейцариядан шығатын киберқылмыс туралы сұраныстардың көпшілігі АҚШ-тағы Facebook, Google және басқа американдық интернет-провайдерлерден ақпарат алу үшін жіберіледі. Соңғы екі жылда Түркия, Гана және тараптарға енбеген Гонконг пен Нигерияға бағытталған сұраныстар көбейген.

Швейцария Будапештік ережедегі «Деректерді сақтау туралы өтініштер» деген 29-бапты жиі қолданатындықтарын атап өтті.

Шри-Ланка 37 халықаралық сұраныс жіберіп, оның отызына жауап алғанын хабарлады. Ол Facebook-тің жалған аккаунттарын құру үшін

пайдаланылған бірнеше телефон нөмірлерін анықтай алды, нәтижесінде қылмыстық тергеу сәтті өтті.

Словакия Республикасы өзара көмекке жиі жүгінеді, ол үшін Конвенция оған заңды негіз береді. Көбінесе Конвенцияның 23, 25 және 31 баптары қолданылады (29-бапқа қосымша ретінде). Шетелдік сұраныстар дәлелдемелердің әртүрлі формаларын сұрайды, соның ішінде тіркелушілер туралы деректер, трафик және мазмұн. Словакиялық сұраныстардың көпшілігі Microsoft, Google, Facebook, Instagram), сондай-ақ басқа да ірі немесе тіпті кішігірім қызметтерге жіберіледі.

Конвенцияға мүше болуға байланысты жеке сектормен ынтымақтастықты жақсарта отырып, көптеген тараптар маңызды артықшылықтар беретін екі мүмкіндікті атап көрсетеді: американдық провайдерлерден сақтауға тікелей сұраныс салу мүмкіндігі және американдық провайдерлерден тіркелушілер туралы ақпаратты тікелей сұрау мүмкіндігі.

Чили конвенцияға қосылғаннан кейін, оның жеке сектормен ынтымақтастығы, әсіресе чилилік емес интернет-провайдерлермен жақсарғанын түсіндірді. Facebook, Instagram, Uber, Google, Microsoft және басқа компаниялар конвенциясының 18-бабына сәйкес чилилік тіркелушілер туралы ақпаратты, соның ішінде IP туралы ақпаратты, осы компаниялармен тікелей ынтымақтастық жасау арқылы алады. Ковенцияға қосылу алдында Чили ынтымақтастығы аз болған, интернет-провайдерлер оның өтініштеріне жауап бермегенін мәлімдеді.

Израиль мемлекетінің «24-7 contact points» желісін қолдану бойынша өз тәжірибесі бар. 2019 жылғы сәуір мен мамыр айларында іскерлік электронды поштадағы қорғалған ақпаратты алумен байланысты алаяқтық бойынша дәлелдемелерді сақтау туралы сұрау жолданған және оларға үш еуропалық елден жауап алынған. Анықталған IP-мекенжайлар бойынша израильдік күдікті анықталған. Нақты уақыт режимінде тергеу барысында қылмыс жасау үшін пайдаланылған бірнеше израильдік ұялы телефондар анықталды. Осы әркеттер жүзеге асырылу барысында аталған елдер арасында тергеуді өрбіту үшін қажетті қосымша ақпараттар алу бойынша тікелей байланыс орнады.

Келесі бір мысал, Израиль бір еуропалық елден оның үкімет жүйесін бұзуға оқталған күдіктінің IP – мекенжайы бойынша дәлелдемелерді сақтау туралы сұрау алды. IP-мекен жайы осы провайдер бойынша күдікті ретінде латиноамерикандық ел азаматына әкелді. Әрі қарай сервердің көшірмесі алынып және ақпарат ұлттық CERT-ке жолданды.

Израиль ұлттық полициясының экономикалық қылмыстар бойынша бөліміне адамды өлтіру және куәларды фальсификациялау туралы қоқан-лоққы көрсеткен күдікті бойынша хабарлама Telegram арқылы түскен.

Кейіннен күдікті IP-мекенжайлары Азияның оңтүстігіндегі коммуникациялық компаниянікі екені анықталды. Барлық дәлелдемелерді ескерсек күдікті шифрлаудың бірнеше күрделі түрін қолданатыны байқалған (Telegram и VPN). Алайда Оңтүстік Азия елі Telegram есепке алу жазбасына байланысты қоқан-лоққы көрсеткен күдікті туралы егжей тегжейлі ақпарат ұсына алды.

2019 жылғы қыркүйекте Израиль Президенті мен премьер-министрінің жаңалықтар сайтында әртүрлі профильдерден қоқан-лоққы көрсетілген комментарийлар жазылған. Жаңалықтар сайтынан алынған ақпарат екі профиль бір IP-мекенжайына байланғанын, ол американдық байланыс компаниясына қатысты екенін көрсеткен. Жедел сұрау АҚШ–тың тәулік бойы қызмет атқаратын байланыс пунктіне күдіктіні тез арада анықтау үшін жолданған. Тергеу барысында күдікті АҚШ-та заңсыз тұрып жатқан Израиль азаматы екені анықталды. Артынан АҚШ депортация бойынша жұмыстар бастады және Изральге күдікті келгенде ол қамауға алынады.

2019 жылғы ақпанда Испания Ұлыбританияның байланыстағы тұлғасынан NetFlow трафигінің IP-мекенжайы бойынша дәлелдемелерді сақтау туралы сұрау алды (ол хаттама IP және бастапқы көздің порты туралы ақпаратты статистикалық мақсатта және торды басқару үшін сақтайды). Ол испандық интернет-провайдердің ақпараты тергеуді өрбіту үшін қажет болған. Бұндай ақпарат екі тәулік қана сақталатын еді, алайда Испаниядағы байланыстағы тұлға оны жедел арада сұрау салу арқылы алды.

2019 жылғы мамырда Испаниядағы жеке торға баса көктеп кіру фактісін тергеу барысында байланыстағы тұлға Израильдегі қызмет көрсетушінің контентін сақтау туралы сұрау жолдады. Сервис виртуалды жеке сервер болып шыққан, ал «24-7 contact points» тек деректерді сақтап қана қоймай, оның жазылушылары (подписчики) туралы жаңа ақпарат ұсынды, ол өз кезегінде тергеуді әрі қарай өрбітуге көмектесті.

Италия «24-7 contact points» желісін негізінен электрондық дәлелдемелерді (журналдар, есептер және т.б.) сақтауды сұрау туралы хаттарды жолдау және оларға жауап алу үшін қолданылатынын атап өтті.

Көптеген істерде итальяндық байланыс пункті абонент туралы негізгі ақпарат бойынша сұраулар жолдап, қабылдады, қолдануға жарайтын болса полициядан полицияға дереу мәлімделді.

Сонымен қатар, Италия желіні ақпаратты беруде пайдалы деп тапты және басқа елдердегі маңызды инфрақұрылымдарға қатысты кибершабуылдар мен киберқауіптер туралы ескертулер жолдады.

2018 жылы Италия 39 кіріс сұрауын алды және 69 сұрау жолдады. Оған 28 ел қатысты.

Франция Будапешт Конвенциясының тәулік бойы жұмыс істейтін желісін тек күрес үшін ғана емес, компьютерлік қылмыстармен, сонымен

бірге электронды дәлелдерді қажет ететін барлық мәселелерді шешу үшін кеңінен қолданады.

«24-7 contact points» деректерді сақтай алатын маңызды рөлімен қатар байланысушы тұлғаға бастапқы техникалық немесе заңгерлік кеңес бере алады. 2019 жылы француз байланыс орталығы Будапешт Конвенциясына қатысты 268 сұранысты өңдеді және олардың барлығы деректерді сақтау туралы. Олар 130 кіріс (24 елден) және 138 шығыс сұраныстарын қамтыды.

Қорытындылай келсек, интернет желісіндегі алаяқтықтың субъектісі қылмысты жасау үшін алуан түрлі әрекеттер ойлап табуда, ал қылмыстық қудалау органдары оны анықтау мен ашу, дәлеледеу мақсатында шаралар қолдануда.

БҰҰ Бас Ассамблеясы өзінің 73/187 «Қылмыстық мақсатта ақпараттық-коммуникациялық технологияларды пайдалануға қарсы іс-қимыл» деп аталатын резолюциясында, Бас хатшыдан мүше мемлекеттерден қылмыстық мақсатта ақпараттық-коммуникациялық технологияларды пайдалануда қарсы іс-қимылда кездесетін қиындықтар туралы ақпаратқа сұраныс және осы ақпаратқа негізделген баяндаманы жетпіс төртінші сессияда қарастыру үшін Бас ассамблеяға жіберуді сұрады.

Осы шақыруға жауап ретінде келесі мүше мемлекеттер өз пікірлерін білдірді: Австралия, Австрия, Аргентина, Армения, Беларуссия, Боливия (Плуринаттық мемлекет), Ботсвана, Бразилия, Венгрия, Венесуэла (Боливария Республикасы), Гана, Германия, Грузия, Израиль, Үндістан, Иордания, Ирак, Иран (Ислам Республикасы), Ирландия, Испания, Италия, Канада, Катар, Қытай, Колумбия, Корея Халықтық Демократиялық Республикасы, Коста-Рика, Ливан, Лихтенштейн, Малайзия, Марокко, Моңғолия, Мьянма, Нидерланды, Никарагуа, Жаңа Зеландия, Норвегия, Перу, Португалия, Ресей Федерациясы, Румыния, Сальвадор, Сауд Арабиясы, Сербия, Сингапур, Сирия Араб Республикасы, Словакия, Словения, Ұлыбритания және Солтүстік Ирландия Біріккен Корольдігі, Америка Құрама Штаттары, Тәжікстан, Тайланд, Түркия, Филиппиндер, Франция, Чехия, Швейцария, Шри-Ланка, Эстония, Оңтүстік Африка және Жапония.

Ұсыныстарда көрсетілген ақпарат ұлттық және халықаралық деңгейдегі мәселелерді шешу үшін қабылднаған шараларды, сондай-ақ оларды шешу үшін қабылданған қолданыстағы уақытша механизмдерді қамтиды. Мүше мемлекеттер техникалық және технологиялық мәселелер туралы ақпарат беріп, осы мәселелерді шешудегі тәжірибелерімен бөлісті. Сондай-ақ, олар қылмыстық мақсатта ақпараттық-коммуникациялық технологияларды қолданудағы қарсы іс-қимылда халықаралық ынтымақтастықтың маңыздылығын атап өтті.

Австралия мемлекеттердің қылмыстық мақсатта ақпараттық-коммуникациялық технологияларды қолданумен күресу кезіндегі ең үлкен қиындықтарға мыналар жатады:

- ұлттық құқық қорғау органдары киберқылмыстарды тиімді тергеу және соттың қудалау мақсатында алынатын деректері мен тікелей деректердің өзіне қол жеткізуде қиындықтарға тап болады. Бұрын, көп жағдайда, деректер елдің ішінде сақталған еді, сондықтанда оларға ішкі тергеу өкілеттілігі арқылы қол жеткізуге болатын. Бүгінгі таңда, ғаламдық желілік байланыстың кең таралуы мен «бұлтты есептеулер» қолданысқа енгендіктен деректер әртүрлі қызметтер, жеткізушілер, аудандар және юрисдикциялар арасында таралып кетуде. Деректердің орналасуын анықтау қиындық тудыруы мүмкін және оларды күрделі әрі баяу халықаралық құқықтық ынтымақтастық процесі нәтижесінде алуға болады. Over-the-top технологиясы негізінде байланыс қызметтерді пайдалану деңгейінің ауқымдылығының кеңеюі, деректерді сақтайтын байланыс операторлары мен қызмет ұсынушыларға дәстүрлі рұқсат алу құқықтық қабілеттілігі киберқылмыстарды тергеу үшін барлық қажетті мәліметтер жиынтығын қамтымайтындығын білдіреді.
- Австралия киберқылмыс туралы Еуропалық Кеңес Конвенциясы сияқты келісімшарттық шешімдер құқық қорғау органдарына басқа мемлекетте сақталған деректерге қол жеткізуге рұқсат алу үшін негіз болатынын атап өтті. Мысалы, жария етуге заңды мүмкіндігі бар адамның келісімін алу немесе деректер жалпыға қол жетімді болған кезде. Осы байланыс шеңберінен тыс шығып кететін, соның ішінде мемлекеттік органдардың келісімін талап ететін шектеулер, киберқылмыстарды тергеуді жүргізуде және қылмыстық қудалауда үлкен қиындықтар тудырады.

Дәстүрлі құқықтық ынтымақтастықтың халықаралық тетіктері, мысалға өзара құқықтық көмек көрсету кезінде, сұранысты қанағаттандыру қиынға соғуы мүмкін, бұл дегеніміз киберқылмыстарды тергеудің кешеуілдеуіне әкеледі. Мақсатқа жеткізе алатын жедел шешімдер, олар мемлекеттердің құзыретті органдары, құқық қорғау органдары, және қажет болған жағдайда ішкі заңнамаға сәйкес, байланыс қызметтерін жеткізушілер арасындағы халықаралық ынтымақтастықтың балама нұсқалары қамтамасыз ете алады.

Канада киберқылмыстарды тергеуде келесі кедергілерді атап өтті: киберқылмыстықта жаңа қиындықтар туындаған кезде Конвенцияны тараптардың қолданыстағы ережелерін пайдалануға көмектесетін нұсқаулық беру арқылы бейімдеу мүмкіндігі бар, ол 24\7 тәулік бойы қызмет жасайтын желімен және әлеуетті арттырудың тиімді бағдарламалар жұмысымен толықтырылған. Конвенция тараптары халықаралық ынтымақтастық тетіктерін жетілдіруге де күш салуда, өйткені аталған қылмыс түрін тергеу басқа юрисдикциялардағы ақпаратқа қолжетміділікті күннен күнге көбірек талап етуде. Канада Конвенцияны қолдайды және оған қатысуға ниет білдірген және қатыса алатын елдер үшін заңдық тұрғыдан міндетті негіз

ретінде де, оған қосылмаған елдерде де ішкі заңнаманы дамыту үлгісі ретінде қол жетімді ең жақсы нұсқа деп санайды.

Аргентина киберқылмыспен күрестегі дағдыларды үйрету мен цифрлық дәлелдемелерді жинау, қылмыстық қудалауды тиімді қамтамасыз етудегі ең күрделі мәселе екенін мәлімдеді. Барлық жұмсалатын күштер жүйелік операторлар туралы білімді жоғарылатуға бағытталуы тиіс, осылайша қолданыстағы заңдар мен халықаралық құжаттарды тиімді пайдалануды қамтамасыз етуге болады. Бұл аталған қылмыстарға қарсы тиімді шаралар қабылдауды ғана емес, сонымен бірге соттағы істі қараудағы тараптардың негізгі құқықтарының сақталуын қамтамасыз етуге мүмкіндік береді.

Армения Конвенцияны негізінде атқарылған келесі жұмыстар туралы мәлімдеді: ақпараттық жүйелер арқылы орын алатын қылмыстар туралы деректер негізінен шетелде жасалуымен немесе қылмыс іздері бірқатар елдердің серверлік жүйелерінде жасырылуымен байланысты. Сондықтан, мұндай жағдайларда тергеуді әртүрлі елдердің заңнамасындағы айырмашылықтар қиындатады. Нәтижесінде сұралған ақпарат, әдетте, сұраныс жіберілген құқық қорғау органына жете бермейді.

Аремения киберқылмыс туралы Еуропалық Кеңестің конвенциясының тиісті ережелеріне сәйкес полицияның ұлттық байланыс орталығы ресейлік емес әлеуметтік желілерді қолданушыларды анықтау және жария ету үшін шаралар қабылдады. Қылмыстық істер немесе істерге қатысты сұраныстар, тәулік бойы қызмет атқаратын байланыс орталықтарының желісі арқылы жүзеге асырылады. Арменияның хабарламасы бойынша, мамандандырылған бөлімшелер аймақтық полиция бөлімшелеріне олардың өтініштері бойынша (ауызша немесе жазбаша) салалық мәселелер бойынша кәсіби көмек пен кеңес береді. Сонымен қатар, аймақтық полиция бөлімдері басшыларының қатысуымен оқу курсы ұйымдастырылды, оның барысында компьютерлік қылмыстардың сипаттамалары және дәлелдемелерді жинау процесі жан-жақты түсіндірілді.

Беларусь БҰҰ-ға хатында: қазіргі заманғы есірткімен байланысты қылмыстың жаңғыртылуы және заңсыз есірткі айналымында даркнет пен криптовалютаны қолдануды ескере отырып, Беларусь мүше мемлекеттер қызметінің басым бағыттарының бірі – ұлттық деңгейде даркнеттегі қылмыстық әрекеттің әдіс-тәсілдерін анықтау мен қылмысты жасаудағы құралдарға қатысты ақпарат алмасуды ұйымдастыру деп санайды. Қылмыстық мақсатта ақпараттық-коммуникациялық технологияларды пайдалануға қарсы тұрудың бір жолы – ол құқық қорғау органдарының қызметкерлеріне даркнет жұмысы мен криптовалюта индустриясының принциптерін түсіндіру.

Халықаралық заңнама туралы сұрақ бойынша Қытай ұйымдасқан қылмысқа қарсы Конвенция, киберқылмыспен күресу үшін халықаралық ынтымақтастықтың жаңа талаптарына тиімді жауап бере алмайтындығын айтты. Қазірдің өзінде киберқылмысқа қарсы күрестегі сала бойынша аймақтық конвенциялар бар, олар Еуропалық Кеңес, Шанхай ынтымақтастық ұйымы, Араб мемлекеттерінің лигасы және Африка одағы әзірлеген. Мүше мемлекеттердің қолдану аясы мен осы конвенциялардың мазмұнындағы айырмашылықтарға байланысты халықаралық киберқылмысқа қарсы іс-қимыл туралы заңнама бөлшектенген сипатта көрсетілген. Осыған байланысты Қытай халықаралық қауымдастыққа шұғыл түрде киберқылмыспен күресу үшін жаһандық заңнамалық базаны құру және күн өткен сайын өршіп бара жатқан қылмыстық жағдаймен, әсіресе «бұлтты есептеулер», жасанды интеллект, заттар интернеті, криптовалюта сияқты жаңа технологиялардың пайда болуынан туындайтын жаңа қатерлермен бірлесіп күресу қажет деп мәлімдеді. Қытай барлық мемлекеттер келіссөздер жүргізіп, БҰҰ-ның қамқорлығымен және қолданыстағы аймақтық конвенциялардың тәжірибесіне сүйене отырып, барлық елдер үшін ашық киберқылмыс туралы бүкіләлемдік конвенцияны әзірлеуі керектігі туралы көзқарасты қолдады.

Грузия киберқылмысқа қарсы күрестің басты мәселеелрдің бірі - деректерге трансшекаралық қол жеткізудің мүмкін еместігі екенін айтты. Күнделікті дамып келе жатқан «бұлтты есептеу» ортасындағы дәстүрлі өзара құқықтық көмек көрсету тетіктері айтарлықтай ескірген. Грузия деректерге трансшекаралық қол жетімділікті реттеуді тоқтату немесе жеңілдету - бұл киберқылмыстарды тергеу мен қудалаудың тиімділігін арттыру мақсатында сөзсіз жүзеге асатын реформа деп санайды. Алайда, бұл реформаларды мемлекеттер көпжақты құжаттар шеңберінде жүргізуі керек, ал юрисдикциялар арасындағы процессуалдық өкілеттіктер сенімді кепілдіктермен қамтамасыз етілуі қажет.

Материалдық құқықтың сұрақтары бойынша, Грузия 1999 жылғы Қылмыстық кодекстің 284-286 баптарын Еуропалық Кеңестің киберқылмыс туралы конвенциясының 2-6-баптарының ережелеріне сәйкес құрылғыларды (ақпарттық жүйені) құқыққа қайшы пайдалануды қылмыстық жауапкершілікке тарту туралы мәлімдеді. Барлық киберқылмыстарды сотқа дейін қудалау қарапайым қылмыстар сияқты жүзеге асады. Мысалы, соңғы кездері кибер алаяқтық сияқты қылмыстар саны көбейіп кетті, бірақ Грузия соттары мұндай істерге қарапайым алаяқтыққа қолданатын заңнама нормаларын қолданады.

Шетелдік интернет қызметтерді жеткізушілермен ынтымақтастықтың арқасында, Грузияның құқық қорғау органдары Грузияда көрсетілетін қызметтерге байланысты әр түрлі ғаламдық интернет компанияларынан

(Facebook, Apple, Microsoft және т.б.) абоненттер туралы ақпарат алғандықтарын айтты. Мысалы, Грузия әлемдегі ең көп ақпаратты жария ететін он елдің қатарына кірді, 2017-2018 жылдар аралығында процедуралық қажеттіліктер үшін Facebook желісінде жарияланған ақпараттардың деңгейі 94 пайызды құрады. 2018 жылы Грузияда халықаралық ұсыну өкімінің формасын енгізді, ол ел соттары жеке немесе заңды тұлғаларға Грузияның аумақтық юрисдикциясынан тыс жерде өкім беруге рұқсат береді. Ол үшін келесі шарттар орындалуы қажет: тапсырыс алған адамның келісімі, электрондық деректерін ерікті түрде ашу және тұлғаны қабылдаушы шетелдің заңнамаға немесе атқарушы биліктің саясатына сәйкес осындай ақпаратты жариялауға рұқсаты болса. Прокурор мұндай өкімді соттан алып,содан кейін оны лауазымды тұлға арқылы бас прокурорға жіберуге міндетті. Мұндай өкімді орындамау заңды жауапкершілік туғызбайды. Еуропалық Кеңестің киберқылмыс туралы конвенциясының 18-бабына сәйкес Грузия, Грузияда көрсетілетін қызметтерге байланысты Facebook және басқа да халықаралық қызмет көрсетуші желілердің мекенжайына халықаралық ұсыну өкімін жолдаған.

Сингапур да өздерінде басқа юрисдикцияларда орын алатын проблемалардың жиі кездесетінін атап өтті. Олардың қатарына қылмыскерлер өздерінің қылмыстық мақсаттарына жаһандану нәтижесінде қол жетімділіктің кеңеюін және технологиялардың барлық жерде таралуын тиімді пайдалануы жатады.

Тәжікстан үкіметтер ведомствоаралық және аймақаралық ақпарат алмасуды қамтамасыз етуді қолға алу, көптеген елдердегі киберқылмыстарды тергеудегі кедергілерді жою, ақпаратты тез алу мақсатында заңнамаға, тәжірибеге және рәсімдерге қажетті өзгерістер енгізу, әртүрлі ақпараттық ресурстардан түскен сұраныстарды өңдеу және электронды дәлелдемелерді беруді қамтамасыз ету қажет екенін айтқан. Жүйелі түрде мамандандырылған курстарды ұйымдастыру және ішкі істер органдарының қызметкерлеріне киберқылмыспен күрестегі кәсіби даярлықты жүргізуді және интернет пен басқа да ақпараттық-коммуникациялық технологияларды пайдалануды қамтамасыз ету, барлық мүше-мемлекеттердің мүдделеріне сай келетін ақпараттық-коммуникациялық технологияларды қолданумен байланысты қылмыстармен күресте ынтымақтастық сұрақтары бойынша, БҰҰ-ның әмбебап конвенциясын әзірлеу және қабылдау қажет дейді.

Таиландта көптеген киберқылмыстарды тергеу кезінде электрондық дәлелдемелерді жинау қиындықтары туғызатындығын атап өтті. Себебі киберқылмысты тергеу кезіндегі маңызды дәлелдемелерді алуға мүмкіндіктің жоқтығы, өйткені интернет қызмет көрсетуді жеткізушілер мен Facebook, Line, Instagram, WeChat және WhatsApp сияқты әлеуметтік желілерінде сақталатын компьютерлік трафик туралы мәліметтер, ал олар өз кезегінде

шет елдерде тіркелгендіктен және Таиландтың компьютерлік қылмыс туралы заңы негізінде құқықтық көмек көрсетуге міндетті емес. Осылайша, құқық қорғау органдары осы дәлелдемелерді өзара құқықтық көмек туралы келісімдердің ресми арналары арқылы сұрауға мәжбүр. Бұл уақытты қажет ететін процесс болғандықтан қиындықтар тудыруы әбден мүмкін. Ынтымақтастықтың бейресми арналары арқылы алынған ақпарат оның құндылығына қарамастан сотта дәлел ретінде қабылданбайды.

Таиланд бірде-бір ел киберқылмыстың алдын алумен және оны тоқтатумен жалғыз күресе алмайды деген шешімге келген. Сондықтанда мүше мемлекеттер арасындағы халықаралық ынтымақтастық пен диалог өте маңызды. Таиланд осы салада белсенді жұмыс істейтін жалғыз платформа - киберқылмысты жан-жақты зерттеу жөніндегі сарапшылар тобына қатысады. Таиланд сарапшылар тобының мандаты мен қызметі 2021 жылдан кейін де ұзартылады деп үміттенеді.

Америка Құрама Штаттары келесіні мәлімдеді: трансұлттық қылмыстық ұйымдар ақпараттық-коммуникациялық технологияларды, оның ішінде даркнет желісін шабуылдарды жеңілдету үшін ғана емес, сонымен бірге ұрланған деректерге онлайн сауда-саттық құру үшін қолдану арқылы киберқылмыстық қауіп-қатердің аясын кеңейтті.

Мемлекеттердің мүмкіндіктері шектеулі болса, ішкі нормативтік-құқықтық базаларын жаңартпаса және өздерінің тергеу органдарын киберқылмыспен күресуге дайындамаса киберқылмыстарды қылмыстық жауапкершілікке тарту үшін серіктестерімен бірлесе жұмыс жасауда қиындықтарға тап болады деп мәлімдеді Америка Құрама Штаттары. Кейбір елдер жалпы қылмыстық заңдарға сүйенеді, ал киберқылмыс туралы арнайы заңдар қабылдау тиімді.

Қылмыстық сот орындаушылары үшін электрондық дәлелдемелерді қолдану сұрақтары бойынша мамандандырылған даярлықты жүргізу аса қажет. Міне, сондықтанда АҚШ БҰҰ ЕҚБ-ның Дүниежүзілік киберқылмыстық бағдарламасына, сондай-ақ АҚШ Ұйымы, Еуропа Кеңесі, АСЕАН және Африка экономикалық қоғамдастығы қаржыландыратын оқыту бағдарламаларына донор болып табылады. АҚШ мүше мемлекеттерді, әсіресе дамушы елдерді осындай бағдарламаларға көбірек көңіл бөлуге шақырады.

Мәселе электронды дәлелдемелерді алуда туындайды. АҚШ басқа мүше мемлекеттер сияқты шет елдерден киберқылмыстарды тергеу кезінде құқық қорғау органдары жиі қолданатын электронды дәлелдерге қол жеткізуде қиындықтарға тап болады. Атап айтқанда, АҚШ электронды дәлелдемелер туралы сұраныстарға тиімді жауап беру үшін заңды өкілеттілігі немесе мүмкіндігі жоқ мүше мемлекеттерден көмек алу қиынға соғады.

АҚШ өз аумағында басқа елдерден электронды дәлелдемелер алу туралы мыңдаған сұраныстарды орындау кезінде де қиындықтарға тап болады. Көбінесе бұл мәселелер басқа елдердің АҚШ талаптарын түсінбегендіктен немесе АҚШ заң стандарттарын сақтау үшін жеткілікті ақпарат бермегендіктен туындайды. Өзара құқықтық көмек сұрауында қамтылған ақпараттың болмауына байланысты, АҚШ билігі шетелдік серіктестерден түсініктемелер мен қосымша ақпарат іздеуге мәжбүр, бұл осы сұраныстардың орындалуының кешігуіне әкеледі. БҰҰ ЕҚБ орталық және құзыретті органдар үшін жаңа құралдарды әзірлеуде. АҚШ бұдан әрі мүше мемлекеттерді өзара құқықтық көмек көрсету талаптары мен процедураларын орындау әлеуетін арттыруға, соның ішінде электронды дәлелдемелердің тиісті сұраныстарын әзірлеуді үйрету арқылы шақырады.

Мүше мемлекеттер өзара іс-қимылдың заңды негізі ретінде электронды дәлелдемелер алу үшін екі жақты өзара құқықтық көмек шарттарын, сондай-ақ Еуропалық Кеңестің киберқылмыс туралы конвенциясы мен Ұйымдасқан қылмыс туралы конвенциясы сияқты көпжақты конвенцияларды қолданады.

Сондай-ақ, 80-нен астам ел жоғары технологиялар саласындағы қылмыстармен күрестегі тәулік бойы желілік байланыс нүктелеріне белсенді қатысып, деректердің қауіпсіздігі мен басқа да сұраныстарды қанағаттандыруға үлес қосуда. АҚШ мүше мемлекеттерге киберқылмыспен күресу үшін осындай шарттар және желілерге қосылуға және оларды қолдануға кеңес береді.

Баяндалғанның негізінде қорытындылайтын болсам елімізде ең алдымен мемлекет аумағында орын алған алаяқтықты жылдам ашу, қажетті ақпаратты жедел алу мақсатында қылмыстық қудалау органдары және байланыс операторлары, банктер, тағы басқа ұйымдар арасындағы ынтымақтастықты реттеу қажет. Өйткені цифрлы дәлелдеменің жойылуы мүмкіндігі өте жылдам, ал интернет арқылы жасалатын қылмыс саны күннен күнге артылуда.

Мемлекетіміздің қылмыстық қудалау органдарында шешілуі қажет тағы бір мәселе - арнайы жоғары оқу орындарында интернет арқылы жасалатын қылмыстарды ашу мен дәлелдеу үшін мамандар дайындау және оларды ортақ іске жұмылдыру. Өйткені тергеуші, жедел уәкіл, криминалистке жоғары оқу орнында ешкім ақпаратық технологиялар арқылы орындалатын қылмыстарды тергеуді үйретпейді. Қызметке келгенде олар әр қайсысы өзінің көрсеткішін жасау үшін әрекет қылады. Ол дегеніміз қызметкердің оқу орнында оқып тоқып келген білімін пайдалана алатын, оған ашылуы жеңілірек, жалпы қылмыстық істерге бейім болатыны анық. Егерде аталған қызметкерлер бір бөлімге біріктіріліп, ортақ мақсат қойылса, бұл бағыттағы жұмыс жемісті болатыны анық. Өйткені тергеуші, жедел уәкіл, криминалист бір-бірінің мүмкіндіктерін біледі және оларды тиімді

қолдана алады. Мамандардың білімі ақпараттық технологиялардың даму үрдісімен бірге аяқ алып жүруі үшін олардың білімі үнемі сертификатталып отыруы қажет.

Компьютерлік қылмыстар туралы конвенцияны (Будапешт, 2001 жылғы 23 қараша) Қазақстан Республикасы келіспейтін бабын ескерту арқылы ратификациялау мүмкіндігін қарастыру қажет. Ол Ковенцияның «24-7 contact points» желісін қолдану бұл қылмыс түрін ашуға біраз көмектесетіні анық. Бір сөзбен айтқанда мемлекетіміздің шекарасынан «шығып» кететін қылмыс болғандықтан, қылмыстық қудалау органдарының қызметкерлері де ағылшын тілін, ақпараттық технологияларды, қылмыстық процесті меңгеруі шарт.

Белорусь ұсынғандай ұлттық деңгейде даркнеттегі қылмыстық әрекеттің әдіс-тәсілдерін анықтау мен қылмысты жасаудағы құралдарға қатысты ақпарат алмасуды ұйымдастыру қажет.

Қытай Халық Республикасының айтқанындай қазірдің өзінде киберқылмысқа қарсы күрестегі сала бойынша аймақтық конвенциялар бар, олар Еуропалық Кеңес, Шанхай ынтымақтастық ұйымы, Араб мемлекеттерінің лигасы және Африка одағы. Мүше мемлекеттердің қолдану аясы мен осы конвенциялардың мазмұнындағы айырмашылықтарға байланысты халықаралық киберқылмысқа қарсы іс-қимыл туралы заңнама бөлшектенген сипатта көрсетілген. Осыған байланысты шұғыл түрде киберқылмыспен күресу үшін жаһандық заңнамалық базаны құру және күн өткен сайын өршіп бара жатқан қылмыстық жағдаймен, әсіресе «бұлтты есептеулер», жасанды интеллект, заттар интернеті, криптовалюта сияқты жаңа технологиялардың пайда болуынан туындайтын жаңа қатерлермен бірлесіп күресу қажет дегенді қолдаймын. Қытай барлық мемлекеттер келіссөздер жүргізіп, БҰҰ-ның қамқорлығымен және қолданыстағы аймақтық конвенциялардың тәжірибесіне сүйене отырып, барлық елдер үшін ашық киберқылмыс туралы бүкіләлемдік конвенцияны әзірлеуі керектігі туралы көзқарасы өте көңілге қонымды және қажет.

2.1. Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтық бойынша сотқа дейінгі тергеуді бастау ерекшеліктері және бастапқы тергеу әрекеттері

Кез-келген мемлекетте әрдайым қылмысты ашу барысында нақты бір қиыншылықтарды туғызатын латентті қылмыстардың белгілі бір саны бар. Мұқият жасырылатын қылмыстардың қатарына тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтық қол сұғушылықтар да жатады.

А.А. Жмыхов жаһандық интернет желісінің оны қолдану арқылы қылмыс жасауға ықпал ететін үш ерекшелігін бөліп көрсетеді: желіде қылмыскердің анонимді іс-қимыл жасауы (нақты әлемде отырып, виртуалды әлемде қылмыс жасайды); жәбірленуші мен қылмыскердің аумақтық алшақтығы; дәстүрлі құралдарға қарағанда компьютерлік орта тауардың жақсысын және ол туралы толығырақ ақпарат ұсынады [13].

Интернет желісіндегі алаяқтық — бұл адамды немесе компьютерлік жүйені алдауға бағытталған, қылмыс мотивациясы пайдақорлық болып табыладын, жаһандық интернет желісіне қосылған компьютерлік жүйелердің технологиялық және коммуникациялық мүмкіндіктерін қолдану арқылы жасалатын қылмыстар жиынтығы болып сипатталады [14].

Құқық бұзушылардың ақпараттық-технологиялар жетістіктерін, мысалы IP-телефония, шетелдік интернет-ресурстар, динамикалық IP-мекенжайлар, электронды төлем жүйелерін, шифрланған байланыс жүйелерін, мобильді байланыс құралдарын қолдануы қылмыскерді қылмыс жасау үстінде ұстау мүмкіндігінен айырады. Жәбірленушімен визуалды байланыс жоқ болуына орай көбіне алаяқтар бетпе-бет байланыссыз қылмыс жасау амалына көшуде. Осындай қылмыс жасау амалдары қылмыстық іс-әрекеттің жоғары латентті болуына ықпал етеді және қылмыстың географиясының ұлғайтуға, ұйымдасқан топ құра отырып орындауға деген құштарлықты арттырады.

Р.М. Акутаев барлық латентті қылмыстылықты, қылмыс және оны жасаған тұлғаның анықталуын және есепке алынуын ескере отырып, екі басты қылмыстар жиынтығына бөлу қажет деп санайды:

1) табиғи-латентті;

2) жасанды-латентті.

Табиғи-латентті – қылмыс туралы ақпарат тұлғаларға, мекемелерге, ұйымдарға, кәсіпорындарға мәлім болса, бірақ оларға қатысты заңда көзделген іс-шаралар жүзеге асырылмаса, құқық қорғау органдарымен есепке алынбаған, олар бойынша сотқа дейінгі тергеу басталмаған болса;

Жасанды латенттікті тудыратын факторлар мәселесі арнайы талдау мен зерттеуді қажет етеді, өйткені олар қылмыстық әділсот органдарының қызметі саласында көп кездеседі және заңдылықтың жай-күйіне, құқық қорғау құндылықтарының қауіпсіздік деңгейіне және мемлекеттің қылмыстық саясатының тиімділігіне тікелей байланысты.

Субъективті-латентті қылмыстар, демек ашылмаған қылмыстар, факт мәлім және есепке алынған, бірақ қылмыс жасаған тұлға анықталмаған және қылмыстық жауапқа тартылмаған жағдайда. Бұл жағдайда қылмыстың латенттігі емес, қылмыс жасаған субъектінің латенттігі туралы сөз қозғалып жатыр. Осындай жағдайларда қылмыс жасаған кінәлі тұлға оның анықталмауы себебінен қылмыстық заңмен көзделген өзіне қатысты жазаны өтемесе [15].

Қылмыстардың латенттігінің кейбір критерийлерін 1993 жылы Ресейде өткізілген «Жасырын қылмыс: таным, саясат, стратегия» атты халықаралық ғылыми-практикалық семинар жинағының авторлары (С.Ф.Милюков, В.Е.Квашис, И.В.Вавилова, Д.Б.Булгаков) жасаған қылмыстың латенттігі анықтамасынан да көруге болады «... құқық қорғау органдарымен жарияланбаған немесе тіркелмеген актілер немесе қылмыстық сот төрелігі жүйесі бұдан әрі ешқандай шаралар қабылдамаған әрекеттер» [16].

Осылайша, қолданыстағы жіктеулердің көпшілігінің негізі қылмыстың латенттігін қалыптастыру механизмі болып табылады. Алайда қылмыстардың латенттігінің объективті және субъективті себептері бар, соған байланысты бөлу осы критерий негізінде жасалуы мүмкін. Зерттеушілердің жоғарыда келтірілген дәлелдерін талдай отырып, қылмыстардың латентігінің ең қолайлы классификациясын Р.М. Акутаев жасаған деп табамын.

Қылмысты анықтаудағы бастапқы кезең бастапқы ақпаратты іздеу болып табылады. Мәліметтерді Интернет желісіндегі ақпараттық ресуртстардан жедел-іздестіру шаралары арқылы іздеу қажеттігін көрсететін бірқатар себептер бар, ол себептердің бірі қылмыстың дәлелдемелері немесе қылмыстың мән-жайын анықтауға жәрдемдесетін электронды деректерді процестік әрекет арқылы анықтау, алу қиынға соғатынын (кейде мүмкін емес екенін) білу қажет. Электронды ақпараттың ерекшелігі – ол процестік бекітілгенге дейін жойылып кетуі мүмкін. Сонымен қатар, ақпаратты жою қылмыскердің тікелей байланысымен ғана емес, қашықтықта, оңай, интернет желісін қолдану арқылы орын алуы мүмкін.

Қылмыстың осы түрін ашу көп уақыт және еңбекті қажет етеді. Тәжірибеде олар «ізі суымай» ашылмайды. Ол жедел уәкілдердің жедел-іздестіру шараларының классикалық әдіс-тәсілдерін қолдануды айтарлықтай қиындатады. Бірінші орынға техникалық байланыс каналдарынан ақпаратты алу, компьютерлік ақпаратты алу сияқты техникалық құралдарды қолданумен байланысты жедел іздестіру шаралары шығады.

Тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықты ашу көп жағдайларда өте қиын, ал қаскүнемді анықтау көбінесе күрделі, кейде мүмкін емес, ол дәлелдемелерді жинауда проблемалар туғызады. Бұның барлығы құқық қорғау органдары жағынан алаяқтардың қылмыстық іс-әрекеттерін әшкерелеу және оларды қылмыстық жауапкершілікке тарту бойынша жұмысты ұйымдастыруда сапалы жаңа көзқарасты талап етеді.

Құқықтық әдебиеттерді, қылмыстық істер материалдарын және басқа да отандық және шетелдік дереккөздерді зерттей келе, тауар сату және қызмет көрсету саласындағы ақпараттық жүйені пайдаланушыларға қатысты жасалған алаяқтықты тергеу және тергеудің сәттілігі тергеудің дер кезінде басталуына байланысты екенін анық көруге болады. Тергеу органдарының қызмет көрсету және тауарларды сату саласындағы алаяқтықты ашу мен тергеу кезіндегі жұмыстың сапасы, құқық бұзушылық туралы өтінішке немесе хабарламаға қаншалықты жедел жауап бергеніне байланысты.

Тергеудің бастапқы кезеңіндегі тергеуші мен анықтаушы қызметінің үш негізгі әрекеттері мыналар:

1. Тергеушіге, анықтаушыға түскен қылмыс туралы ақпаратты бағалау.
2. Аталған құқық бұзушылық белгілері бар алғашқы ақпаратта қажетті деректер жеткілікті болмаған кезде келіп түскен өтініштер мен хабарламаларды тексеру.
3. Сотқа дейінгі тергеудің қажеттігі туралы маңызды шешімдерді процессуалдық талаптарға сәйкес қабылдау және ресімдеу.

Бұл қызмет қылмыстық процестік заңнамасымен және өзге де нормативтік актілермен реттелуге тиіс. Ол туралы «Қылмыстық құқық бұзушылықтар туралы арызды, хабарды немесе баянатты қабылдау және тіркеу, сондай-ақ Сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімін жүргізу қағидаларын бекіту туралы» Қазақстан Республикасы Бас Прокурорының 2014 жылғы 19 қыркүйектегі №89 Бұйрығы бар.

Қызмет көрсету және тауарларды сату саласындағы интернеттегі ақпараттық жүйені қолданушыға қатысты жаслатын алаяқтық фактісі бойынша сотқа дейінгі тергеуді бастау үшін себептер мен негіздер төмендегідей:

1. Арыз беруші тікелей жүгінген (өзі келген) кезде жасалған, дайындалып жатқан қылмыстық құқық бұзушылық туралы арыз.
2. Кінәсін мойындап келу.
3. Қылмыстық құқық бұзушылық туралы мәліметтерді, оның ішінде бұқаралық ақпарат құралдарынан алған кезде қылмыстық қудалау органдарының қызметкерлері баянат жасайды.
4. Лауазымды тұлғаның баянаты.

Тергеу жұмысының бірқатар кемшіліктері бар:

- осы санаттағы қылмыстардың аз ашылуы;
- тергеулер көбінесе ұзаққа созылып, жасалған қылмыстық әрекеттердің толық ашылмауының және қылмыстық жазалардың әлсіреуінің бірден-бір себебі болып табылады.

Тергеу жүргізілетін жетекші бағыттар нақты тергеу жағдайына байланысты. Тергеу жағдайына байланысты туындаған болжамдар қатаң бекітілген жедел-іздестіру шаралары немесе тергеу әрекеттері арқылы тексеріледі. Бұл өз кезегінде тергеуге байланысты әртүрлі ақпаратты таңдау, зерттеу және қолдануға байланысты операцияларды түрлендіруге әкеп соғады. Қылмыс субъектісі туралы ақпараттың толық болмауы тергеу

әрекеттерін жоспарлауды белгілі бір ұйымдастырушылық және жедел іздестіру шараларын жүргізуді талап етеді.

Тергеушіге көмектесу үшін тергеу әрекеттерінің белгілі бір алгоритмін құру және әзірлеу мүмкіндігі бар, оның негізі типтік тергеу жағдайларының кешені болып табылады. Бұл алгоритмде қызмет көрсету және тауарларды сату саласындағы алаяқтықты тергеуді ұйымдастыру және жүргізу үшін әдістемелік және қажетті нұсқаулар мен ұсыныстар беру маңызды. Типтік тергеу жағдайларына байланысты белгілі бір әрекеттерді орындау алгоритмі, қажетті ұсыныстар жиынтығы керек. Мұндай типтік жағдайлар әртүрлі тергеу кезеңдеріне тән. Типтік жағдайларды қарастырғанда, қылмыстық әрекеттерді жасауда, белгілі бір іздердің, қылмыскерлердің қоладанатын әдістерінің, бүркемелер жасау үшін жаңадан пайда болып отыратын әдістерді ескеру қажет. Ғылым мен техниканың соңғы әзірленімдері иен жетістіктері ерекше назар аударуды талап етеді, өйткені олар қылмыстық әлеммен күрес жөніндегі іс-шараларды өткізу кезінде пайдалы.

Тергеу және сот практикасын талдау кезінде, сотқа дейінгі тергеуді жоспарлау кезеңінде екі типтік (тексеру) жағдай қалыптасқанын аңғарамыз. Демек қылмыскердің жеке басы анықталмаған, ұсталмаған.

1. Қылмыскерлер заңсыз әрекеттерді жасауды жалғастырады және компьютерлік алаяқтық жасалып отырған адаммен тығыз байланыста болады.
2. Қылмыс аяқталды және қылмысқа қатысы бар адам мен алаяқтар арасындағы байланыс жоқ.

Тергеуші немесе анықтауды жүргізуші адам үшін бірінші жағдай неғұрлым қолайлы екендігін және оны шешу кезінде қылмыскерлерді жеке-жеке ұстауға немесе дәлелдемелік және бағдарлаушы ақпараттың неғұрлым көп көлемін жинауға (егер олар Қазақстан Республикасының Құқық қорғау органдарының құзыреттілігінде болса) мүмкіндік бар екенін атап өту қажет. Екінші жағдай өте қолайсыз және мұндай ақпаратты алу процесін едәуір қиындатады.

Қылмыстық іс бойынша тергеушінің қызметі тиімді болуы үшін оның жұмысы дұрыс ұйымдастырылуы және қылмыстық қудалау органдарының жұмысының бір жүйеге келтірілуі қажет. Ең алдымен сотқа дейінгі тергеудің басында жүргізілетін тексеру жоспарын жасау қажет. Жоспар белгілі бір ұстанымдарды қамтиды:

- құжаттар жиынтығы және қылмыс құрамын, жасалған әрекеттің заңсыздығын растайтын бақа да материалдарды алу; жедел-іздестіру материалдарын алу.
- қызметкерге, тергеу жүргізетін органдарға ұсынылған және қолда бар құжаттардың түпнұсқалығы мұқият тексерілуін (мысалы, банк платикалық картасына қызмет көрсету туралы келісім-шарт).
- өтініш беруші сілтеме жасаған адамдарға қойылуы қажетті сұрақтарды; жасалған әрекеттің ықтимал куәгерлері ретінде осы адамдар туралы ақпараттарды жинауды;

- жәбірленуші және куәлерден жауап алуды;
- сотқа дейінгі тергеп-тексеруді жүзеге асыратын адамға нәрселер мен құжаттарды оларға иелік ететін адамдардың бастамасы бойынша беру;
- компьютерлік-техникалық құралдарды, интернет желісіндегі сайт парақшасын, электронды поштадағы хабарламаларды қылмыс жасаудың ықтимал құралы ретінде қарап-тексеру жүргізуді;
- қызмет көрсету және тауарларды сату саласындағы алаяқтық үшін ақпараттық жүйелерді пайдалану технологиясын оқуды;
- мамандармен кеңесті; тергеу әрекеттеріне қатысатын білікті мамандарды шақыруды ресімдеуді;
- ықтимал кінәліні ұстау үшін қажетті шараларды таңдауды;
- тінту жүргізуді;
- бағдарламалық-техникалық сараптаманы қамтитын әртүрлі сараптамаларды анықтау және қажет болған жағдайда тағайындауды;
- байланыс операторларына, банктерге, провайдерлерге сұрау жолдау, қажет болған жағдайда халықаралық тапсырма жолдауды.

Бұл объективтілік деңгейді жоғарылатады, қылмыстың мән-жайын тез, толық және жан-жақты анықтауға, қылмыскерді іздеуге және анықтауға мүмкіндік береді. Қылмыстық іс бойынша жұмыс жоспарын құрғанда, тергеуші болашақтағы барлық іс-әрекеттерді ойластыруы қажет, қазіргі жағдайда дәлелдемелерді нәтижелі жинау мен бағалауды қамтамасыз ететін әдістер мен құралдарды таңдауы қажет.

Криминалистика туралы әдебиетте тергеуді жоспарлаудың әртүрлі анықтамалары бар. Тергеуді жоспарлау тәсіліне,ақыл-ой процесі ретінде қарауымыз қажет. Жоспарлау - бұл қызмет көрсету және тауарларды сату саласындағы алаяқтықты тергеудің міндетті шарттарының бірі. Бұл тергеу міндеттерін бөлу, олардың шешу жолдары мен әдістерін заң талаптарына сәйкес анықтаудан тұратын ойлау процесі. Жоспарлаудың бастамасы нақты негіз болып табылады. Бұл негіз қылмыс туралы ақпараттан құралған. Бұл мәліметтердің алу жолдары іс жүргізу мен жедел-іздестіру болып табылады.

Тергеу міндеттерін анықтау, нұсқаларды құру, жолды таңдау және тексерудің әдістері нақты деректердің қаншалықты толық алынғанына байланысты. Тергеудің бастапқы кезеңінде қылмыс немесе оның белгілері бар оқиға туралы алынған ақпарат шектеулі болады. Бұл тергеу жоспарын жасау қиындық тудырады. Бұл тергеушіні жаңа фактілерді анықтау көлеміне байланысты, жұмыс жоспарын қайта қарауға және толықтырып отыруға міндеттейді. Жоспарлау-бұл үздіксіз жүретін процесс. Оның тоқтатылуы қылмыстық іс бойынша соңғы шешімнің қабылдануымен байланысты болады.

Жоспарлаудың объективті шарты - тергеушіде жасалған қылмыс туралы нақты мәліметтер болуында. Оның теориялық білімі мен кәсіби тәжірибесі істі бойынша дұрыс шешім қабылдауына негіз болады.

Компьютерлік ақпаратқа өзгерістер енгізудің оңай және қарапайым болуы оның басты қасиеті, сондықтан тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықты анықтау және ашу құқық қорғау органдарының оның жасалу фактісі бойынша жедел әрекет етуіне байланысты.

Жәбірленушінің пошта жәшігінде қылмыстың іздері бар (алаяқтың логині, пошта жәшігінің атауы). Құқық бұзушыны анықтау үшін келесі шараларды қолданған жөн:

1. Жәбірленушінің пошта жәшігін алаяқ туралы дәлелдемелерді (пошта жәшігін анықтау, бүркенген атын анықтау, хат алмасуды алу) алу мақсатында карап-тексеру.

Жәбірленушінің пошта жәшігінің каталогтарында барлық хат алмасу жүргізілген мекен-жайлардың есепке алу жазбалары сақталады.

2. Әлеуметтік желінің иесіне немесе басқа мемлекеттердің құқық қорғау органдарына сұрау жіберу.

Бұл шара IP мекен-жайларды, пошта жәшігінің жасалған және Интернетке кіру уақытын, сондай-ақ тіркеу кезінде көрсетілген жеке деректерді, пошта жәшігін іске қосу үшін, абоненттік нөмірді анықтау үшін қажет [17].

Сонымен, тауар сату және қызмет көрсету саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықтың бастапқы тергеу кезеңінде:

1) қылмыстық істі тергеу жоспарын құру;
2) жәбірленушіден жауап алу;
3) қылмыс орын алған техникалық құрылғыны қарап-тексеру жүргізіледі;

Тергеу әрекеті кезеңдерінің жүйесі:

1) тергеу әрекетін жүргізуге дайындықтан;
2) тергеу әрекетін жүргізуден;
3) оның жүргізілуін және нәтижесін бекітуден;
4) алынған дәлелдемелерді бағалаудан тұрады [18].

Тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты орын алған алаяқтықты тергеу әдетте жәбірленушіден жауап алу тергеу әрекетінен басталады. Жауап алуды жүргізудің көп кездесетін басты қателігі алынған жауаптың толық еместігі болып табылады. Оның себебі тергеушінің өндірісінде бірнеше қылмыстық іс болғандықтан, ол барлық істер бойынша ақпараттарды есінде сақтай бермейді. Сондықтан жауап алуды дұрыс ұйымдастыру және жәбірленушіден толық ақпарат алу үшін алдымен оған қойылатын сұрақтарды дайындап алу қажет. Бұл тергеу әрекетіне дайындық кезеңі.

Жауап алу тергеу әрекетінің екінші кезеңі ол кіріспе кезең. Бұл кезеңде жәбірленушінің жеке басын куаландыратын құжаттар тексеріліп, оған ҚР ҚПК 26-тарауына сәйкес құқытары түсіндіріліп өтеді. Жауап алудың келесі үшінші кезеңі ол жәбірленушінің өзіне қатысты орын алған қылмыс туралы

еркін түрде әңгімелеп беруі. Осы сәтте жауап алудың негізгі маңызды сәті жәбірленушімен психологиялық байланысты ұстану қажет. Оның жауап беру сәтінде есіне түсіре алмай отырған деректер бар екені байқалса оған алаяқтық орын алған ақпараттық жүйені қосып беру қажет. Жәбірленуші жүйеге ену сәтінен бастап тергеушіге қажетті барлық ақпаратты жеткізе алады. Әсіресе тергеушіге алаяқтың ақпараттық жүйедегі есепке алу жазбалары маңызды, сондай-ақ әрине провайдер, байланыс операторы, банк есепшоттары, виртуалды әмиян туралы және т.б. қылмыстық іс үшін маңызды деректер.

Тауар сату және қызмет көрсету саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықты тергеудегі келесі маңызды тергеу әрекеті оқиға орны болып табылатын ақпараттық жүйе орнатылған техникалық құрылғыны қарап-тексеру.

ҚР ҚПК 219-бабына сәйкес қылмыстық құқық бұзушылықтың іздерін және өзге де материалдық объектілерді табу және анықтау, оқиғаның жағдайларын анықтау және іс үшін маңызы бар мән-жайларды айқындау мақсатында сотқа дейінгі тергеп-тексеруді жүзеге асыратын адам жергілікті жерді, үй-жайларды, нәрселерді, құжаттарды, тірі адамдарды, мәйіттерді, жануарларды қарап-тексеруді жүргізеді. Қарап-тексеруді жүзеге асыратын адамның нұсқаулары осы тергеу әрекетінің барлық қатысушылары үшін міндетті.

Зерттеу тақырыбы бойынша қарап-тексеруге компьютер, телефон, гаджет, интернет-ресурс, сайт, ақпараттық жүйені қолданушының әлеуметтік желідегі жеке парақшасы және т.б. жатады. Бұл тергеу әрекетін жүргізу барысында ғылыми-техникалық құралдар қолданылады және тергеушінің әр іс-қимылы суретке немесе бейнежазбаға түсірілуі қажет. Сондай-ақ тергеу әрекетін бастамас бұрын, терегу әрекетін жүргізуге дайындық барысында ақпараттық жүйелерді қолданудан хабары бар тұлғаларды куәгер ретінде таңдап алған абзал. Өйткені куәгерлерден болашақта қылмыстық қудалау процесінде куәгер ретінде жауап алуы әбен мүмкін.

ҚР ҚПК 119-бабының нормаларына сәйкес тергеу әрекетінің хаттамасына тергеушінің барлық іс-қимылы суреттеліп, рет-ретімен жазылады. Тергеу әрекетін сипаттау техникалық құралдың сыртқы деректері (марка, модель, имей код және т.б.) детальды суреттеледі, әрі қарай интернет-браузерге (Google, Yandex және т.б.) кірген уақыттан егжей-тегжейлі суреттеу жалғастырылады. Хаттамада сондай-ақ алдымен интернет-ресурстың сілтемесі және тұлғаның деректемелері көрсетіледі.

Жоғарыда көрсетілген әрекеттерді тіркеген кезде, жасалған барлық нәрсені хаттамада нақты көрсету керек, бірақ тек ауызша сипаттама белгілі бір фактілерді субъективті бағалауға әкелуі мүмкін. Бұл басқа тергеу әрекеттерін жүргізу кезінде де мүмкін, бірақ мұнда электронды ақпарат тасымалдаушыларымен жүргізілетін операцияларды сипаттау кезінде хаттамада материалдың шамадан тыс көптігіне және жасалатын әрекеттердің күрделілігіне байланысты ауызша сипаттауда проблемалар туындауы мүмкін.

Бұл жағдайда электронды құрылғыларды қарап-тексеру, алу, тінту кезінде бейнетүсірілімді қолдану арқылы шешуге болады, оның көмегімен құрылғы экраны әрдайым кадрда болуы қажет, тергеуші немесе маман жасаған барлық іс-әрекеттер көрсетіледі.

Интернет желісінде орналасқан ақпаратты қарап-тексеру ерекшеліктері бар. Ақпараттың бастапқы тасымалдаушысын алу жүргізбей-ақ, мысалы тексеріліп отырған веб-ресурстың сервері басқа мемлекетте орналасқан жағдайда компьютерлік ақпаратты алғанда оның түпнұсқасын басқа жаққа апару емес, тек дубликатын, көшірмесін алу жүргізіледі. Демек ақпарат бастапқы қалпында қала береді, ал тергеу өзіне жаңадан қажетті дәлел ақпаратты алады. Интернеттегі ақпаратты алу кезінде оны цифрлы тасымалдаушыға көшіру жүзеге асады. Цифрлы тасымалдаушы ұзақ уақытқа ақпарат сақтау мүмкіндігі бар мысалы, қатты диск, флэш-карта, оптикалық диск. Қарап-тексеру хаттамасында цифрлы тасымалдаушыға интернет ақпарат алынғаны туралы жазба қалдырылады.

Интернет-ақпаратты бекіту құралдары ретінде жол берілуі мүмкін құралдарға келесілерді жатқызуға болады: басып шығарылған скриншоттар немесе веб–сайт беттері, ресми деректемелер (сайттың URL-мекенжайы, жүгінген күні, ақпаратты тіркеген кездегі компьютердің жүйелік уақыты және т. б.), сайттың контенті (мазмұны) туралы веб–ресурсты хостинг (орналастыру) қызметін ұсынатын ұйымның хабарламасы немесе тіркеушінің домендік атаудың нақты иесі кім екендігі туралы хабарламасы.

Скриншоттарды сақтауды тергеудің бастапқы кезінде жасау қажет, өйткені барлық интернет-алаңдағы бұғатталған интернет-дүкеннің өзінің ай сайынғы төлемақы төленетін жалға алынған «бұтағы» болады. Ал алаяқтар ұсталған жағдайда ай сайынғы жалға алу жарнасы төленбеген соң барлық ақпараттар, қайта қалпына келтіру мүмкіндігінсіз сайттан өшіріледі.

Әрі қарай, тексеруден кейін электронды тасымалдаушыны дұрыс орау керек, мұнда әдеттегі процеспен салыстырғанда белгілі бір ерекшеліктерді бөліп көрсетуге болады. Барлық құрылғылар, атап айтқанда, барлық порттар, слоттар, кірістер мен шығулар, криминалистік маңызды ақпараттың сақталуын қамтамасыз ету үшін және өзгерістер енгізілмес үшін мөрленуі керек. Бірақ электронды іздердің ерекшеліктеріне байланысты осы құрылғыларға мүмкін байланыссыз қол жетімділіктің алдын алу үшін ақпарат тасымалдаушысына кіруді бұғаттайтын арнайы қап – Фарадея қабы ойластырылды.

Мұндай құрылғы болмаған жағдайда заттарды пластикалық пакетке (қапқа) немесе қорапқа орау ең сенімді тәсіл болып табылады, пакеттің аузы жіппен тігіледі, жіп түйіні түсіндірме жазбасы бар биркамен желімделеді. Кейбір мамандар тергеу барысында, тінту мен алудың дайындық кезеңінде тергеушіге (анықтаушыға) электрондық тасымалдаушыны орау мақсатында тергеу әрекетінің объектісі қандай болатынын ескеру қажет екенін көрсетеді. Сараптамалық зерттеудің нәтижесі болып табылған ақпарат тасымалдағыштың қаншалықты дұрыс және сауатты оралатындығына

байланысты. Сот сарапшылары электронды құрылғыларды орау ережелерінің бұзылғанын ескереді, өйткені барлық қосқыштар мен қосу/өшіру/қайта қосу түймелеріне еркін қол жеткізуге болатын болса, бұл электрондық тасымалдағыштағы ақпараттың одан әрі бұрмалануына әкелуі мүмкін.

Электрондық ақпарат құралдарын іздеу және алу кезінде маманның қатысу қажеттілігін анықтауға қатысты бірнеше қарама-қарсы пікірлер бар. Келесі көзқарастарды бөліп көрсетуге болады:

1) Егер ақпаратқа қол жеткізу мүмкін болмаса, белгілі бір тергеу әрекеттерін жүргізу қажеттіліктеріне қарай тергеушінің қалауы бойынша маман тартуға болады.

мұндай тексеру хаттамасы одан әрі компьютердің немесе өзге де цифрлық құрылғының жазбаларына тиісті сараптама жүргізілмеген жағдайда да рұқсат етілетін дәлел болып табылады.

2) Ғалымдардың келесі тобы алынған электрондық құрылғы түріне байланысты маманның қатысу қажеттілігін негіздейді.

Мысалы, А.Л.Осипенко, А.И.Гайдин, М.В. Старичков, В.А.Антонов ұялы телефонды, флэш-карталарды, камераны алу кезінде маман осы тергеу әрекетіне қатыспауы мүмкін екенін айтады. Бұл тәсіл бұрынғыға біршама ұқсас, өйткені маманның қатысуы жеке жағдайлар болған кезде ғана қажет деп айтылады. Алайда, бұл жерде мәселе мұндай қатысуды қажет етпейтін электрондық құрылғылар тобын анықтауда болып тұр, бұл, сөзсіз, қолдану кезінде даулы жағдайларды тудырады. Сонымен қатар, мұндай жағдайда құрылғыларды осы топқа жатқызу үшін олардың жалпы белгілерін анықтау немесе электронды ақпарат тасымалдаушылардың толық тізімін бекіту қажет болады, ол технологиялардың дамуына байланысты қиын болып табылады[19].

3) РФ ҚПК-нің императивтік ережелеріне сәйкес электрондық ақпарат тасымалдағыштармен тергеу әрекеттерін жүргізу кезінде маманның қатысуын міндетті. В.Б.Вехов электронды құрылғыларға қатысты тінту жүргізу кезінде маманды шақыру тергеушінің құқығы емес міндеті екенін айтқан. Алайда, Ресей Федерациясының соттары бұл норманы орындауды қолдамайтын көрінеді. Өйткені соттар электронды дәлелдемелерді алу тергеу әрекетін маман қатыспағаны үшін заңсыз алынған дәлелдеме деп танымаған. Сондай-ақ, белгілі бір тергеу әрекетіне дайындық кезеңінде маман тарту қажеттілігі туралы мәселені шешу кезінде қиындықтар туындайды, өйткені тергеуші қылмыс жасалған жерге барған кезде алдын-ала осы санатпен нақты байланысты қылмыстарды қоспағанда, электронды ақпарат тасымалдаушылардың болуын алдын-ала болжай алмайды.

Электрондық ақпарат тасымалдағыштарды алу кезінде маманның қатысуы арнайы білімді қолдану қажеттілігі туындаған және тасымалдаушыда сақталатын ақпаратты жоғалту қаупі туындаған жағдайда ғана қажет деп есептеймін.

Мысалы, алуды жүргізу кезінде ақпаратты басқа электрондық ақпарат тасығыштарға көшіру жүргізілсе, маманның қатысуы міндетті, өйткені бұл жағдайда ақпаратты жоғалту немесе өзгерту қаупі бар.

Электрондық құрылғыларды алу барлық жағдайларына маманның қатысуы қылмыстарды ашу және тергеу кезінде тергеу әрекеттерін жүргізудің жеделдігіне байланысты әрдайым мүмкін бола бермейді, алайда ақпарат жоғалуы мүмкін жағдайларда маманды тарту қажет. Бұл электрондық іздерді тиімді пайдалануға ықпал етеді. Егер тергеушінің осы тергеу әрекетін жүргізуге маман тарту мүмкіндігі болса, мұны осы құрылғылардағы ақпаратқа төнген қауіптіліктің бар жоқтығына қарамастан жасауға болады.

Келесі даулы мәселе-маманның құзыретіне қойылатын талаптарды анықтау, маманның қажетті білім деңгейіне қатысты күмән туындайды: бұл тек жоғары білім болуы керек пе немесе орта мамандандырылған арнайы білімі бар маман тартылуы мүмкін бе, сондай-ақ мұндай адам қандай лауазымға ие болуы керек? жұмыс тәжірибесі қандай? Бұл мәселелер заңнамалық деңгейде де, ведомстволық деңгейде де шешілмеген күйінде қалып отыр.

А.Л. Осипенко, А.И. Гайдин, мұндай маман күрделі нақты мәселелерді (желілік жабдықты пайдалану ерекшеліктері, ақпаратты шифрлау процедуралары және т. б.) түсінуі керек, олардың практикалық шешімінде жеткілікті дағдыларға ие болуы керек (мысалы, дәлелдемелерді анықтау мен бекітудің криминалистикалық құралдарын қолдану әдістемесін меңгеруі қажет деп есептейді[20].

Қазіргі уақытта мұндай мамандарды аккредиттеу, сертификаттау, білім беру стандарттары жоқ. Іс жүзінде қолдану үшін тергеушіге әртүрлі жағдайларда тергеу әрекеттерін жүргізуге тартылған мамандардың қажетті біліктілігі мен мамандануын анықтауға мүмкіндік беретін ұсынылған талаптардың үнемі жаңартылып отыратын тізімі пайдалы болар еді.

Сонымен қатар, маманның білім деңгейіне тек ресми талаптарды белгілемеуіміз қажет, осы мәселеге және осындай адамның біліктілігіне жан-жақты қарау керек.

Ғалымдар да, тергеу және жедел бөлімшелер қызметкерлері де тартылған мамандардың қажетті дайындығының жоқтығын атайды. Тергеуші тергеу әрекеттерін жүргізер алдында тиісті құзыреттің бар-жоғына, маманның электрондық ақпарат тасығыштарды алу, тіркеу, зерттеу кезінде жұмыс істеу дағдыларына ие екендігіне көз жеткізу мүмкіндігін ойластыруды ұсынады, өйткені тергеуші тергеу әрекетінің сапалы болуына жеке жауапты. Алайда, қазіргі уақытта барлық тергеушілер маманның деңгейін анықтай алмайды.

Біз осы мәселенің шешімі ретінде болашақ тергеушілер мен анықтаушыларды жоғары білімнің негізгі бағдарламасы аясында немесе қайта даярлау немесе біліктілікті арттыру арқылы оқытуда ақпараттық–компьютерлік білімді кеңейтуді ұсынатын көзқараспен келісемін.

Осылайша, маманның электрондық ақпараттарды және электронды құралдарын алуға байланысты тергеу әрекеттерін жүргізуге қатысу мәселелері одан әрі зерттеуді қажет етеді деп қорытынды жасауға болады.

ҚР Конституциясының 18-бабында жеке салымдар мен жинақтардың, жазысқан хаттардың, телефон арқылы сөйлескен сөздердің, пошта, телеграф арқылы және өзге де хабарлардың құпиясына қол сұғылмаушылық құқығы бекітілген. Бұл құқықты шектеуге заңда тікелей белгіленген жағдайларда және тәртіппен ғана жол беріледі. Дәл осындай ереже қылмыстық сот ісін жүргізудің негіз қалаушы қағидаттарының бірі ретінде де белгіленген.

Алайда лауазымды тұлғалардың іс-әрекеттері жеке адамның мемлекет алдындағы қорғалу деңгейін айтарлықтай төмендетуі мүмкін. Сонымен, кез-келген тергеу әрекеті адам құқықтарын шектеуге әкеледі, оның ішінде жеке және отбасылық құпия да бар. Әсіресе, мұндай әрекет қазіргі уақытта біздің қоғам қол жеткізген жоғары технологиялардың таралу деңгейіне байланысты адам өмірі туралы негізгі ақпарат көзі болып табылатын электронды тасымалдаушылармен байланысты болып тұр. Құқық қорғау органдарының мұндай шектеуге жол беретіндігіне сот тәжірибесі дәлел, өйткені тергеушінің заңсыз әрекеттерін, яғни компьютерді, телефонды және т.б. тексеру кезіндегі азаматтардың шағымдарын көруге болады.

ҚР Конституциясы мен қылмыстық заңнама нормаларының негізінде, хат жазысу, жеке, отбасылық құпиясын бұзуға әкеп соғатын деректерді тікелей алуға байланысты тергеу әрекеті тек соттың санкциясымен ғана мүмкін. Алайда, заңнамада, ұялы телефоннан мәліметтерді алу үшін соттың санкциясын алу қажеттілігі бекітілмеген. Мұндай қарама-қайшылық тәжірибеде ақпарат құралдарынан мәлімет алу соттың бақылауынсыз жүретіндігін көрсетеді.

Р.И.Оконенконың пікірінше, электронды құрылғыдан ақпарат алу оның мәні бойынша қарап-тексеру емес, тінту болып табылады, өйткені электронды іздер еркін қол жетімді емес, оларды алу үшін арнайы техникалық және криминалистік құралдарды қолдану және тиісті хаттамамен рәсімдеу қажет. Маман мұндай әрекетті жүзеге асыру үшін міндетті түрде алдын-ала сот санкциясының қажеттілігі керек деген қорытындыға келеді. Бірақ сонымен бірге, егер электронды тасымалдаушы қылмыс жасау әдісі, құралы ретінде болса немесе онсыз оны жасау мүмкін болмаса, мысалы, компьютерлік ақпарат саласындағы қылмыстар, сот шешімін алудың қажеті жоқ[21].

Р.Г.Бикмиев, Р.С. Бурганов сондай-ақ электрондық тасымалдағышты сот шешімінсіз алып қоюға және иесінің келісіміне қарамастан қолда бар ақпаратты қарауға мүмкін деген қорытындыға келеді. Осы тұрғыдан алғанда, Адам құқықтары туралы еуропалық соттың қызықты ұстанымы бар, осыған сәйкес электронды тасымалдаушыларды қарап-тексеру соттың санкциясымен мүмкін, ал санкциясыз тексеру кейінге қалдыруға болмайтын жағдайларда мүмкін болады, бұл жағдайда айыптаушы тексеру жүргізілгеннен кейін, сотқа осы фактіні дәлелдеуі керек[22].

Бұл ұстанымға ұқсас норма ҚР ҚПК бар, ол 254-баптың 3-тармағында айрықша жағдайларда, іздестіріліп жатқан және (немесе) алып қойылуға жататын объект оны табуды ұзаққа созудан жоғалуы, бүлінуі немесе қылмыстық мақсатта пайдаланылуы мүмкін болғанда не іздестіріліп жатқан адам жасырынуы мүмкін болғанда тінту және алу тергеу судьясының санкциясынсыз, ҚПК 220-бабының он төртінші бөлігінде көзделген тәртіппен жүргізілуі мүмкін делінген.

Тұлғаның жазбаша келісімімен ғана электронды деректерді алуды жүргізу ұсынылады, егер мұндай адам келісім беруден бас тартса, онда мәліметтерді алу соттың санкциясымен жүргізілгені дұрыс. Егер жоғарыда айтып өткендей, электронды дәлелдемелердің жойылып кету қаупі төніп тұрса, соттың санкциясынсыз алу жүргізуге болады, алайда кейіннен қылмыстық қудалау органы бұл әрекетін сот алдында негіздеуі қажет. Менің ойымша, бұл дұрыс шешім және адамның жеке өміріне қол сұғылмаушылық қағидасын бұзбайды.

Электрондық тасымалдағыштағы барлық ақпаратқа қатысты сот бақылауын қамтамасыз ету қажет, өйткені ол адамның барлық жеке және әлеуметтік өмірін қамтиды. Бұл аса маңызды конституциялық құқықтардың бірі болып табылатын жеке өмірге қол сұғылмаушылық, жеке және отбасылық құпия, хат жазысу, телефон арқылы сөйлесу, пошта, телеграф және өзге де хабарлар құпиясын сақтауға ықпал етеді.

Сонымен, электронды іздерді тапқаннан кейін оларды қарап-тексеру қажет. Қазіргі таңда біздің қоғамымызға ақпараттандырудың тез енуіне байланысты, ақпараттық – технологиялық көздердің және электронды іздердің орналасқан жерлерінің тізімі тек артып келеді. Мұндай көздерге файл, URL, IP мекенжайы, MAC мекенжайы, телефонның IMEI, бейнежазба, аудиожазба, DNS, навигациялық қызмет, геолокация және басқалар кіреді.

А.Н.Колычева электрондық тасымалдағыштарды қарап-тексеруді интернет–сайттарды, парақшаларды, электрондық поштаны, хабарламалар тарихын, абоненттің Интернет және (немесе) абоненттік құрылғылардың қосылулар ақпараттарын қарап-тексерулерге жіктеуді ұсынады.

Электрондық іздер цифрлық белгілердің электромагниттік әрекеттесуінен тұратын із жасау механизмімен ерекшеленеді және техникалық құралдардың көмегімен анықталады. Желідегі ақпарат алмасудың ең көп таралған стандарттарына TCP/IP деректерді беру хаттамалары кіреді.

IP мекенжайлары, MAC мекенжайлары, кэштелген қосымшалар деректері, компьютерлік жүйедегі, сервердегі пайдаланушылардың жұмысының тарихы және журналдары, файлдар және олрадың физикалық мекенжайлары, атаулары, қосылымдардың детализациясы дәлелдеудегі маңызды ақпараттық нысандардың көзі деп айтуға болады [23].

MAC мекенжайы сияқты жиі кездесетін технологиялық көзді қарастыруға болады. Бұл жабдықтың желілік картасына берілген бірегей

цифрлық нөмірі, IP немесе виртуалды мекен–жайға қарағанда физикалық мекенжай болып табылады [24].

MAC мекенжайы қолданушыны және ақпарат алушыны анықтау үшін қажет, бірақ мекенжайдың белгілі бір адамға тиесілі болуы ақпарат көзі дәл осы адам екенін көрсетпейтін жағдайлар туындауы мүмкін. Бұл қылмыстық істер бойынша тергеуде қателіктерге әкелуі мүмкін [25].

Пайдаланушының MAC мекенжайын анықтау электрондық ақпарат тасымалдаушысы бар қылмыстарды неғұрлым тиімді ашуға ықпал етуі мүмкін, оны анықтау әдетте мұндай қылмыстарды тергеудің бірінші кезеңдеріне жатады.

Тағы бір электрондық іздерді табудағы жиі қолданатын ақпараттық және технологиялық көз – ол телефонның IMEI. IMEI (International Mobile Equipment Identity) – желідегі құрылғыны анықтайтын сан (әдетте 15 разрядтық). Ол GSM, WCDMA және IDEN желілерінің ұялы телефондарында, сондай-ақ кейбір серіктік телефондарда қолданылады. Әдетте, IMEI төрт жерде көрсетіледі: құрылғының өзінде, батареяның астында, қаптамада және кепілдік талонында. Сондай-ақ, IMEI телефонды бақылау және ұрлық кезінде ұялы телефонды байланыс операторы бұғаттау үшін қолданылады [26].

Телефонның IMEI-ін абоненттер және (немесе) абоненттік құрылғылар арасындағы байланыс туралы ақпарат алу сияқты тергеу әрекеті аясында алуға болады.

Телефон IMEI-і, атап айтқанда, абоненттік құрылғының IMEI коды немесе телефон аппараттарының базалық станцияға қатысты орналасқан жері туралы ақпаратты анықтауға мүмкіндік береді. Алайда, телефонның IMEI деректері, сондай-ақ адамның жеке өміріне, жеке және отбасылық құпиясына қатысты шектеулерге әкелуі мүмкін, тергеу әрекеттерін жүргізу кезіндегі барлық электрондық дәлелдерді алу мүмкіндігі туралы мәселе әлі күнге дейін ғылыми қоғамдастықта және құқық қорғаушылар арасында дұрыс шешілмеген.

Қазақстан Республикасы Жоғарғы Сотының 2010 жылғы 25 маусымдағы № 4 "Қылмыстық сот ісін жүргізуде адамның және азаматтың құқықтарын, бостандықтарын сот арқылы қорғау туралы" нормативтік қаулысының 12-тармағында, "Жедел-іздестіру қызметі туралы" Заңның 11-бабының 3-тармағындағы арнайы жедел-іздестіру іс-шаралары облыс (қала) прокурорының және жоғары тұрған прокурорлардың санкциясымен ғана жүргізілуі мүмкін деп көрсетілген.

Навигациялық сигналдар арқылы ақпарат алу екі негізгі технология арқылы жүзеге асырылады – олар GSM желісінің базалық станциялар желісі, яғни абонентінің белгілері бойынша ұялы байланыс станциялары және ғаламдық навигациялық ғарыштық жүйелер (ГЛОНАСС, GPS) және олардың ішкі жүйелері арқылы[27].

Географиялық координаттар әртүрлі электронды тасымалдаушылардан (мобильді құрылғылар, бұлтты серверлер, планшеттер және т. б.), соның

ішінде картада іздеудің, маршрутты құрудың және т.б. нақты нәтижелерін көрсету үшін адамның орналасқан жері туралы деректерді сұрайтын орнатылған қосымшалардан алынуы мүмкін. Әрі қарай, бұл ақпарат қызмет көрсету серверіне жіберіледі немесе құрылғының есінде сақталады [28].

Қылмыстық процесте навигация жүйелерінің деректері дәлелді немесе бағдарлы ақпарат ретінде пайдалануы мүмкін. Мұндай мәліметтер, егер қатыстылық, жол берілушілік және анықтық критерилеріне сәйкес келген жағдайда ғана дәлелдемелер болып табылады және нысан бойынша не өзге құжатты, не навигация құралдарын пайдалануды көрсете отырып, тиісті тергеу әрекетінің хаттамасын ұсынады.

Сенімділікке келетін болсақ, мамандардың пікірінше, геолокация жүйелерінің жалпы қателігі 3,5% - дан аз [29].

Тиісті ақпараттың рұқсат етілуі туралы мәселені шешу кезінде мынадай проблемаларды атап өткен жөн: жалпы мақсаттағы навигациялық аспаптарды оқиға орнының координаттарын анықтау кезінде қолдану мүмкіндігі, сондай–ақ осы жүйелерді қолдану бойынша қандай да бір тәжірибелік ұсыныстардың болмауы.

Навигация жүйелерін пайдаланудың тиімділігін сот тәжірибесі де дәлелдейді. Сонымен, көптеген сот актілерінде оқиға орнының координаттарын анықтауда ғаламдық навигациялық серіктік жүйелерді қолдану туралы айтылады, жақын жерде тұрақты бағдарлар (орман, дала, тайга) болмаған кезде бұл ерекше маңызды. Сондай-ақ, кейбір шешімдерде қылмыс жасаған адамды, оның қозғалу бағытын анықтау кезінде ұялы телефондағы немесе көлік құралындағы навигациялық құралдардың көмегімен анықталатын, қылмыс құралын, қылмыстың жеке іздерін табу кезінде геолокация жүйелерін пайдалану тікелей көрсетіледі.

Осылайша, қызмет көрсету және тауарларды сату саласындағы алаяқтықты ашу және тергеу үдерісінде навигациялық серіктік жүйелер маңызды қызмет атқарады деген қорытындыға келуге болады, алайда оларды қолдану мәселесін нақтылау, анықтау және тәжірибелік нұсқаулықтарды құрастырып шығару дәлелдерді табуды айтарлықтай жеңілдетеді.

Ғылымда жиі талқыланатын мәселелердің бірі – ол қандай да бір терминді элктронды ақпаратқа қатысты қолдану және оның мазмұны туралы пікірлердің әр алуандығында. Мұндағы негізгі мәселе электрондық іздердің мәні мен мазмұнын дәл анықтау болып табылады, ал "электрондық", "виртуалды", "ақпараттық", "цифрлық", "компьютерлік" және т.б. терминдердің қолданылуы дәлелдемелерді жинауда шешуші роль атқармайды.

Жекелеген елдердің заңдары электронды түрде алынған дәлелдемелерді мүлдем қабылдамайды, бұл ақпараттық технологиялардың қазіргі даму жағдайына және қылмыстық әлемнің өзгеріп жатқан тенденцияларына сәйкес келмейтін сияқты.

Электрондық дәлелдемелерді жинау мен сақтауға қатысты мемлекеттер арасындағы тиімді ынтымақтастыққа кепілдік беретін еуропалық және

халықаралық деңгейде бірқатар жалпы директивалар мен ұсыныстар әзірлеу керек.

Бұл осы ережелерді отандық заңнамаға енгізуге де ықпал етеді, бұл, бір жағынан, қылмыстарды тергеу саны мен сапасының артуына, екінші жағынан, оны жүзеге асыру кезінде азаматтардың құқықтарының сақталуына әкеледі. Осы мақсатта кейбір халықаралық актілерге тоқталайық.

Электрондық дәлелдемелер қылмыстық процестің құрамдас бөлігі ретінде, дәлелдердің дербес түрі ретінде ешбір елде қарастырылмаған. Көптеген мемлекеттер дәстүрлі дәлелдердің электронды түрде болу мүмкіндігі туралы айтады. Еуропалық соттарда электронды дәлелдемелерді реттеу барлық дәлелдерге қатысты жалпы ережелер арқылы жүзеге асырылатыны айтылған.

Кейбір елдерде, мысалы, АҚШ-та электронды дәлелдемелерді пайдалану мәселесі ең алдымен Федералды дәлелдеу ережелерімен реттеледі. Ережелердің 101-тармағында кез келген түрдегі жазбаша материалдар туралы айтылған жағдайда, электрондық нысанда сақталатын ақпарат та ескеріледі делінген , яғни оларды реттеу үшін жалпы ережелер қолданылады [30].

Электрондық дәлелдемелерді зерттеудің неғұрлым тәжірибелік мәселелерін қарау кезінде АҚШ Әділет министрлігі Ұлттық Әділет институтымен бірлесіп әзірлеген электрондық дәлелдемелердің Сот сараптамасы жөніндегі нұсқаулыққа жүгінуге болады. Бұл нұсқаулық компьютерлік–техникалық және өзге де сараптамаларды жүргізу кезінде тиісті мекемелердің сарапшылары үшін көзделген және ұсынымдық сипатта жасалған. Нұсқаулықта электрондық дәлелдемелер ретінде сақталған немесе көшірме нысанда сотта қолданылуы мүмкін ақпарат танылады. Мұндай ақпарат ордер негізінде немесе тікелей провайдерден алынуы мүмкін. Бізге ерекше болып көрінетін жағдай, ол осыған сәйкес процеске қатысушы тұлғалардың электрондық құрылғыларын пайдалану дағдыларын тексеру ұсынылады, бұл электрондық ақпараттың өзгеру немесе жоғалу қаупінің алдын алуға көмектеседі. Мұндай дәлелдемелер тексеру кезінде немесе дұрыс қолданбаған кезде бүлінуі, өзгертілуі немесе жойылуы мүмкін, бұл дәлелдемелерді қорғауды және сақтауды қамтамасыз ететін арнайы сақтық шараларын қолдануды қажет етеді делінген [31].

Нұсқаулықта электрондық дәлелдемелерді алу және бағалау мәселелерімен қатар, сараптама жүргізу кезінде фиксация және хаттамалау мәселесі қарастырылған, бірақ менің ойымызша, оларды электронды ақпарат тасымалдағыштармен тергеу әрекеттеріне қатысатын маманға жүктеуге болады. Мысалы, әрекеттердің қайталанбауын қамтамасыз ету, анықталған бұзушылықтарды және кез-келген әрекеттерді құжаттау, авторизация жасалған пайдаланушылар, топология, парольдер туралы қосымша ақпаратты анықтау, операциялық жүйе, бағдарламалық жасақтама нұсқасы, жаңартулар, жүйеге енгізілген өзгерістерді құжаттау мүмкіндігі көрсетілген. Осылайша, нұсқаулықтың неғұрлым практикалық мәселелерге бағытталғанын ескерсек,

кейбір ережелерін мемлекетімізде электрондық дәлелдемелердің жалпы мәселелерін қарау кезінде пайдалануы мүмкіндігі бар.

Ұлыбритания аумағында электрондық дәлелдемелерді пайдалану мәселесін реттеу кезінде "The Good Practice Guide for Computer Based Electronic Evidence" басшылығы қызықты болып көрінеді, ол электрондық тасымалдаушылардан ақпарат алудың нормалары мен ережелерін қамтитын және тергеушілерге және тергеуді жүзеге асыратын басқа тұлғаларға, адвокаттарға, процестің басқа қатысушыларына бағытталған кешенді акт болып табылады. Нұсқаулықта қазақстандық тәжірибеде қолданылуы мүмкін қағидалар бекітілген, атап айтқанда: сотта қолдануға болатын мәліметтерге өзгерістер енгізуге тыйым салу; маман тиісті біліктілікке ие болуы керек, басқа қатысушыларға өзінің іс-әрекетінің реттілігі мен мәнін түсіндіре білуі керек; алынған дәлелдемелерді тәуелсіз бағалау мүмкіндігі; тергеуші заңның сақталуына және осы қағидалардың орындалуына жауап береді. Электрондық ақпаратты жазу кезінде орындаушы барлық компоненттердің фотосуреттерін және бейнелерін көрсетеді, егер мүмкін болмаса, кейін осы жүйені қайта құру үшін, барлық кірістер және шығулар көрсетілген схема жасайды. Маңызды болуы мүмкін электрондық органайзерлер және жеке виртуалды көмекшілерге ерекше назар аударылады, олардың барлығын қолдану тез дамуда.

Нұсқаулықта жеке электронды тасымалдағыштарды(видео, телефондар, электрондық пошта және т.б.) іздеу және тіркеу бойынша ұсыныстар, тінту алдында жасалатын іс-әрекеттер туралы нұсқаулар, тергеу тобымен кімді және нені өзімен тергеу әрекетіне алу қажеттілігі туралы брифинг (жиналыс) өткізу көрсетілген. Қазақстандық тергеушілер, мамандар және басқа да процеске қатысушылар бұндай ережелерге назар аударғаны жөн. Мұндай құжатты кем дегенде ведомстволық деңгейде жасау электрондық ақпаратты дәлел ретінде пайдалану мәселелеріндегі сенімділікке ықпал етеді және қылмыстарды тергеудің тиімділігін арттырады. Дәл осы бағыт қазіргі заманғы ғылым және тәжірибеде басымдыққа ие болуы тиіс.

Электрондық іздердің ұғымы тек қызмет көрсету және тауарларды сату саласында алаяқтық жасаумен ғана емес, сонымен қатар із қалдыратын кез-келген электрондық ақпарат тасымалдаушысы қолданылатын басқа қылмыстармен де байланысты.

Электронды іздердің ақпараттық және технологиялық көздері көп және осы саладағы тұрақты прогреске байланысты тек көбейетіні анық. Бұл мәселені қарау кезінде тасымалдаушылар немесе оның сипаттамалары маңызды емес, мұндай көздерден алынатын электронды ақпарат маңызды.

Ең маңызды аспект-дәстүрлі дәлелдемелерден өзгеше болатын электрондық дәлелдердің жол берілу критерийлерін анықтау. П.С. Пастуховтың пікірінше, қылмыстық процесте электрондық ақпаратты енгізу мәселесі дәлелдердің жол берілетін дәлелдемелер стандарты олардың

жазбаша түрде болуына негізделген, бұл процесстік құжат айналымын электронды түрге ауыстыруға кедергі келтіреді [32].

Осы уақытқа дейін ғалымдар мен практиктер арасында мұндай дәлелдердің сенімділігі туралы қарама-қайшы пікір бар, олардың нақтылығы мен дәлдігіне қарамастан, сарапшылар оларды сотта қабылдау дәстүрлі дәлелдерге қарағанда үлкен кепілдіктерді қажет ететінін айтады[33].

Ұсынылған электрондық дәлелдердің сенімділігін, олардың дұрыстығын, түпнұсқалығын тексерудің бірыңғай құралдарын құру дұрыс шешім болуы мүмкін. Көбісі электрондық ақпараттың тексерілетіндігін, өзгермейтіндігін, оларды тәжірибеде қолданған кезде негізгі сапа ретінде анықтайды [34].

Мамандар электронды дәлелдемелерді тексеру құралдарын әртүрлі жолдармен белгілейді, мысалы, компьютерлік-техникалық сараптама жүргізу, криптографиялық хэш қызметі – кез-келген элктрондық ақпаратты растау, халықаралық ұйымдар әзірлеген бірыңғай қағидаттарды пайдалану, оларды ҚР ҚПК мәтініне енгізу немесе бланкеттік норма жіберу.

Хэш-қызметі немесе жинақтау қызметі – белгілі бір алгоритммен орындалатын, еркін ұзындықтағы кіріс деректер массивін белгіленген ұзындықтағы биттік (шығыс) жолына түрлендіретін қызмет. Көптеген қолданыстағы хэш-қызметтер арасында криптографиялық тұрақты қызметті бөліп қарау қалыптасқан, өйткені оларға қосымша талаптар қойылады.

Бұндай дәлелдемелерге жол берушіліктің техникалық критерийлерін емес, электронды тасымалдаушылардың ерекшеліктерін бекітуге болады, мысалы, ақпарат тасымалдаушыда болу фактісі, тергеу кезінде жасау, арнайы құрылғыларды қолдану қажеттілігі, тікелей әсер етпестен мазмұнына өзгерістер енгізу мүмкіндігі.

Электрондық дәлелдемелерді қолданудағы басты мәселе – жол беру немесе сенімділік критерийлерін белгілеу және бұл заңды тұрғыдан тұжырымдалған жалпы қағидаттар емес, техникалық критерийлер болуы керек. Мұндай дәлелдерге әлі де сенімсіздік байқалса да, олар басқа дәлелдермен салыстырғанда анағұрлым сенімді, оларды алу және сақтау кезінде субъективті факторларды неғұрлым төмендетеді.

Дәлелдемелерді сақтау камерасына ұқсас электронды дәлелдемелерді сақтауға арналған сертификатталған компьютерлерді жабдықтау туралы ой, сондай-ақ осы деректерді сотқа олардың тұтастығы мен өзгермейтіндігін тексеру арқылы жолдайтын ведомствоаралық желілер құру туарлы ойлар қызықты деп ойлаймын. Қазір бұл туралы айту, әрине, ертерек, бірақ мұндай мүмкіндік қылмыстық процессте электрондық ақпаратты қолдануды дамытудың бағыты бола алады.

Қазіргі таңда қоғам өмірінің барлық салаларында, соның ішінде адамдардың қылмыс жасау және оларды жасыру, қылмыстарды тергеу мен ашуға кедергі жасауда технологиялар, ақпараттандыру жаппай қолданылады, сондықтан электронды дәлелдер қылмыстық іс бойынша өте маңызды болып табылады.

Тергеу барысында айтарлықтай мүмкіндіктерге ие киберқылмыспен күрес жөніндегі бөлімшелерінің техникалық әлеуетін пайдалану арқылы қол жеткізуге болады, олар арнайы құралдардың көмегімен күдіктілердің байланыс арналары арқылы беретін ашық ақпараттарын ұстап алады; арнайы техниканың көмегімен алаяқтық фактісін растайтын деректерді алу және кейіннен алынуы және заттай дәлелдемелер ретінде іске қоса тіркелуі мүмкін объектілерді анықтау; қылмыскер интернетке кірген желілік мекенжайды анықтау; оның жеке басын, алдау мақсатында пайдаланатын электрондық шоттарын және қылмыстық істі ашуға қажетті басқа да ақпаратты анықтау.

Қызмет көрсету және тауарларды сату саласындағы алаяқтық туралы істер бойынша сотқа дейінгі тергеуді жүргізу кезінде тергеушіге (анықтау жүргізетін адамға) жедел қызметкерлерге куәларды, сондай-ақ белгіленген алаяқтықты жасауға қатысы бар адамдарды анықтауға бағытталған жедел-іздестіру іс-шараларын жүргізу туралы тапсырма берген орынды.

Жедел-іздестіру қызметінің мүмкіндіктерін белсенді пайдалану, қылмыс жасаған адамдарды анықтауға және оларды ұстауға мүмкіндік береді. Оларды әсіресе құқық қорғау органдарына жүгінген адамға қатысты алаяқтық жасауды жалғастырған жағдайда пайдалану тиімді. Бұл жағдайда қылмыстық іс-әрекеттің барлық қатысушыларын ұстауға және дәлелдемелер мен нұсқаулық ақпаратты жинауға бағытталған бірлескен іс-қимыл жоспарын әзірлеу және іске асыру ең тиімді тәсіл болып табылады.

Тергеуші сотқа дейінгі тергеу барысында жәбірленушілерден, сондай-ақ заңды тұлғалардан алынған ақшаны қылмыскерлердің қолма-қол ақшаға айналдыру орындарына ерекше назар аудару керек. Өйткені қаржы мекемелерінде алаяқтар өздері немесе үшінші тұлғалардың көмегімен ақшалай қаражатты алуы мүмкін. Тергеуші осындай мекемелерді, олармен тікелей байланыса алатын адамдарды анықтауға, сондай-ақ қылмыскерлер бейнебақылауға түсіп қалған техникалық құралдардан ақпарат алуға жұмысын бағыттауы тиіс. Сондықтанда, тергеуші осындай адамдардың барлығынан жауап алып, олардың іздері (қол қою, қолжазба үлгілері, қол іздері және т. б. түрінде), қаржылық операцияларды көрсететін құжаттар, қылмыскерлердің бейнелері және т. б. талап етуі керек.

Тауарларды сату және қызмет көрсету саласында алаяқтық жасауда қылмыскерлер қылмыс жасау барысында қосалқы әрекеттерді жүзеге асыратын адамдардың көмегін жиі пайдаланады(интернет-байланыс қызметтерін ұсыну келісімін өз аттарына ресімдеу, банк карталарын, қолма-қол ақшаға айналдыру және т.б.). Көп жағдайда бұл адамдар өздерінің қылмыстық іс-әрекетке барып жатқандарын білмейді, өйткені қылмыскерлер оларға шынайы ақпарат бермейді. Аталған адамдардың иелігінде нақты адамдардың жасалған қылмысқа қатыстылығын куәландыратын жүргізілген операциялардың есептік құжаттары болуы мүмкін. Сонымен қатар, мұндай адамдармен байланыс орнату кезінде қылмыскерлер бүркемелеу құралдарына жүгінбейді, бұл қылмыскерлердің жеке басының шынайы белгілерін, сондай-ақ олардың қылмыс барысында қолданған құралдарын

анықтау мүмкіндігіне жағдай жасайды. (қылмыскерлер қозғалған көліктер, телефон нөмірлері, тұрғылықты мекен-жайлар және т.б.).

Тергеуші бұл процессуарлық әрекеттерді өзі орындай алады немесе оларды жедел бөлімшелердің қызметкерлеріне сеніп тапсыра алады.

Тергеуші қызмет көрсету және тауарларды сату саласында алаяқтық жасаған қылмыскерлерді жедел бөлімшелердің көмегінсіз мүлде ұстай алмайтын жағдайлар болатындығын атап өткен жөн.

Электрондық іздерді табу және оларды жинау арнайы жабдықты қолданумен байланысты. Қолданылатын техникалық-криминалистикалық құралдардың ерекшеліктері жойылған және қолжетімсіз деректерді тез және қауіпсіз қалпына келтіру және талдау, зақымдалған ақпаратты қалпына келтіру мүмкіндігінен тұрады. Құқық қорғау органдары UFED аппараттық-бағдарламалық кешенін сәтті қолдануда. Бұл құрылғы телефон кітапшасы, мәтіндік хабарламалар, фотосуреттер, бейне суреттер, қоңыраулар журналдары (шығыс, кіріс, қабылданбаған), дыбыстық файлдар сияқты ұялы телефонның деректерін толық алуға мүмкіндік береді; SIM идентификаторын клондау, телефон мазмұнын желілік операцияларсыз талдау және PIN–кодпен бұғатталған SIM–картаны "бұзу" қажеттілігі; далалық жағдайдағы мобильді сот зертханасы, оқиға болған жерде қолдану портативті, жылдам және ыңғайлы [35].

Тағы бір ерекше техникалық-криминалистикалық құрал-Мобильді Криминалист, бұл маманның құрылғы туралы жалпы ақпаратқа, соның ішінде контактілерге, қоңырауларға, хабарламаларға, фотосуреттерге, бейнелерге, аудиоға, 400-ден астам қосымшадан алынған мәліметтерге тіпті электрондық құрылғыдан жойылған барлық деректерге қол жеткізуін қамтамасыз етеді: Facebook, Google+, Safari, WhatsApp және т.б. [36].

Мобильді Криминалист сонымен бірге алынған деректерді талдауға арналған, қажет болған жағдайда жедел тергеу жүргізу үшін ерекше маңызды. Ол әр түрлі көздерден контактілерді біріктіруге, барлық оқиғаларды хронологиялық тәртіпте құруға; тұрақты өрнектер, хэш жиынтықтар, телефон нөмірлері, төлқұжаттар және басқа критерийлер бойынша деректерді іздеуге, бір немесе бірнеше адамның қозғалыс маршруттарын құруға, ең көп баратын жерлерді және бірнеше адамның жалпы болу орындарын анықтауға мүмкіндік береді. Бұл бағдарламалардың шетелдік аналогтары XRY Logical болып табылады – бұл файлдық жүйенің онлайн режимінде деректерді қылмыс орнында құрылғыдан алуға және қалпына келтіруге мүмкіндік беретін жылдам алу әдісі, оларды осы жүйеге қарамастан құрылғының операциялық жүйесімен тікелей байланыстырады [37].

Сондай–ақ En Case Forensic, компьютерлік-техникалық сараптама жүргізуге арналған жергілікті бағдарламалық жасақтама бар, бұл электрондық дәлелдерді іздеудің және деректерді сотқа ұсынудың халықаралық стандарты болып табылады. En Case Forensic сарапшыларға қатты дискідегі ақпаратты криминалистикалық талдау арқылы ықтимал

дәлелдемелерді анықтауға және алынған дәлелдердің сенімділігі мен тұтастығын сақтай отырып, алынған нәтижелер туралы толық есептер дайындауға мүмкіндік береді [38].

Қылмыс жасау кезінде "үлкен деректерді" немесе Big Data зерттеу, талдау үшін арнайы бағдарламалар қарастырылған – IBM i2 Analyst's Notebook, "Сегмент–С", "Следопыт" және т.б. жиі қолданылатын болған. Олардың міндеттері массивті үлкен электрондық ақпараттарды аналитикалық зерттеу болып табылады. Мысалы, бұл қылмыстық әрекеттер сериясында қолданылатын көлік құралдарын орнату; бір немесе бірнеше оқиғалармен байланысты мобильді құрылғыларды анықтау; тергеуге қызығушылық танытқан күдіктілердің, жәбірленушілердің және т.б. әлеуметтік шеңберден адамдарды анықтау, олардың қарым-қатынас жүйесі және т. б.

Бұл бағдарламалардың көпшілігі адамның кінәсін дәлелдеуде шешуші болуы мүмкін немесе керісінше, күдіктінің қылмыс жасауға қатысы жоқтығын анық көрсетуі мүмкін. Бұл мәселені шешу үшін, ең алдымен, IT-технологиялар саласында арнайы білімі бар және арнайы құрал-жабдықтары бар мамандар электронды дәлелдемелерді алуға және зерттеуге тарту қажет. Бүгінгі күннің ақиқаты электрондық іздер мен олардың тасымалдаушыларын зерттеудің жаңа әдістерінің көбеюін көрсетіп отыр, сол себепті тергеушілердің, криминалистердің, мамандар мен сарапшылардың үнемі кәсіби деңгейінің дамуын, олардың біліктілігін арттыруды, олар қолданатын құрал-жабдықтар мен бағдарламалық қамтамасыз етуді үнемі жаңартып отыруымыз қажет.

Үлкен деректер технологияларын енгізу жөніндегі жобалар елеулі қаржылық инвестицияларды талап етеді. Алайда, алаяқтықтан салдарынан келген залал құны туралы статистикалық көрсеткіштері бұқаралық ақпарат құралдарында жарияланған: «2021 жылғы қаңтарда елде "алаяқтық" бабы бойынша 4 мың қылмыстық құқық бұзушылық тіркелді — бұл өткен жылғы қаңтарға қарағанда бірден 30,9% - ға артық. Мұндай мәліметтер finprom.kz. берілген. Олардың ішінде басым бөлігі (43,3%) интернет-алаяқтыққа түсті: 1,8 мың құқық бұзушылық. "Алаяқтық" бабы бойынша аяқталған қылмыстық істер бойынша құқық бұзушылықтармен келтірілген залалдың белгіленген сомасы 2021 жылғы қаңтарда 1,8 млрд теңгені құрады, бір жыл бұрын 3,1 млрд теңге болған еді. Жеке тұлғаларға ең көп шығын келтірілген — 1,1 млрд теңге. Мемлекетке келтірілген залал 529,9 млн теңгені, заңды тұлғаларға - 82,7 млн теңгені құрады» [39].

Осыны ескере отырып, мемлекеттік-жекешелік әріптестік негізде бизнес-қоғамдастықпен өзара іс-әрекет жасау арқылы қосымша қорларды тарту тетіктерін пайдаланған жөн. Шетелдік тәжірибеде ірі IT-компаниялар (атап айтқанда, IBM, Google, Amazon) полицейлерді цифрлық ортада ақпарат алудың негіздеріне оқыту жүйесіне қомақты сома (3,5 млрд долларға дейін) салатындығы және мемлекеттік-жекеменшік әріптестік негізде құрылған, полицияға арналған бағдарламалық-аппараттық шешімдерді әзірлеуді, енгізуді жүзеге асыратын, полицияны жаңғыртуды қолдау консорциумына

қатысатындығы туралы мысалдар өте көп[40]. Ақпараттық-талдамалық технологияларды қолданудың тиімділігін арттырудың басты мақсаты тиісті кадрлардың жеткіліктідеңгейде болуын қамтамасыз ету керектігін мойындау керек. Ішкі істер органдарының әрбір қызметкері қазіргі жағдайда жедел маңызды ақпараттың цифрлы көздерін табу бойынша құзыреттерге ие болуға міндетті. Қылмысқа қарсы күресті жедел-іздестіруді қолдаудың белсенді моделіне толығымен көшуді байыпты ғылыми қолдау, біздің ойымызша, өзекті мәселелерді жан-жақты зерттеу үшін мамандандырылған пәнаралық зерттеу топтарын құруды болжайды.

Киберкеңістікте әртүрлі сайттарында, әлеуметтік желілерде, мессенджерлерде, электрондық пошталарда, IP-телефония хабарламаларында, банк операцияларында, электрондық сауда қосымшаларында, көлік қатынастарында, электрондық құжат айналымында және тағы басқадай ақпараттық жүйелерде анықталуы мүмкін жедел ақпараттар шоғыры бар.

Көбіне тергеу барысында және сот сараптамаларын жасау кезінде зерттеуге жататын мәліметтер цифрлы ақпараттың ауқымды жиынтығы болып табылады, оны қазіргі уақытта жоғарыда атап өткен, Big Data (үлкен деректер) деп атауды ұсынады. Осы жөнінде толығырақ айтсақ, қарастырылып отырған мәселе тұрғысынан үлкен деректер дегеніміз - бұл қылмыстық-құқықтық маңызы бар, сондай-ақ математикалық және статистикалық әдістермен өзгертуді қажет ететін, сот-сараптамалық маңызы бар ақпараттарды табу және криминалистика мен қылмысты тергеуде жұмыс жасайтын криминалистикалық модельдерді, тұжырымдар мен шешімдерді қолдану[41]. Қылмыстарды тергеу үшін маңызды ақпаратарды (соның ішінде электрондық дәлелдемелерді) алу үшін анықталған электрондық ақпарат пен үлкен деректерді тасымалдаушыларды тереңірек зерттеуге әртүрлі бағдарламалық-талдамалық кешендер қолданылады. Олардың бірі жоғарыда мысалға келтірілген IBM i2 Analyst’s Notebook.

IBM I2 Analyst ' s Notebook провайдерлерден, байланыс операторларынан алынған немесе алып қойылған мобильдік құрылғыларды техникалық зерттеуге, талдауға мүмкіндік береді. Зерттеу нәтижелері кестелер, диаграммалар түрінде жасалынып, зерттеу туралы анықтама немесе сарапшының қорытындысы түрінде ұсынылады, сондай-ақ топтық қылмыс жасаушылардың рөлдері мен қарым-қатынастарын тексеруге болады.

Қылмыстың мән-жайларын анықтау мақсатында қылмыс жасаған адамға және жәбірленушіге (кейбір жағдайларда — куәгерлерге) тиесілі компьютерлердегі, ноутбуктердегі, нетбуктардағы, планшеттердегі және өзге электронды құрылғылар, басқа да алынған ақпарттар зерделеніп, одан мәліметтер алу үшін тікелей пайдалануға болады. Ақпараттық-аналитикалық кешендердің келесі мүмкіндіктерді бар:

- бір абоненттік нөмірді, компьютерді, мобильді құралды, банк картасын, электронды кошелекті бірнеше қылмыстық іс-әрекеттерді

дайындау және жасау кезінде пайдалану туралы деректерді алу немесе керісінше бір немесе бірнеше қылмыспен байланысты құралды анықтау;

- тергеуге мүдделі күдіктілердің, жәбірленушілердің және т.б. қарым-қатынас шеңберіндегі адамдардың, олардың өзара байланыс жүйесін анықтау;

- әр түрлі абоненттік құрылғылардың байланыс тізбегін орнату;

- белгілі бір уақыт кезеңдерінде абоненттік құрылғының орналасқан жерін және белгілі бір қозғалыс бағыттарын анықтау;

- тергеліп жатқан қылмыстың мән-жайын және жасырынған қылмыскердің тұрған жерін анықтау;

Сонымен қатар, бүгінгі таңда тергеуде пайдалану үшін пайдалы талдамалы деректерді интернет желісінің ашық көздерінен алуға мүмкіндік беретін веб-аналитиканың бірқатар мамандандырылған құралдары бар екенін атап өткен жөн. Мұндай бағдарламалар (олардың кейбіреулері тегін) үлкен көлемде белгілі бір ақпаратты алуға бағытталған, оның ішінде тергеу үшін пайдалы:

- әр түрлі әлеуметтік желілердегі бір адамның бірнеше парақтары туралы, оның ішінде жалған мәліметтер бойынша тіркелген бір қолданушыны анықтау үшін;

- алаяқтың Интернет желісіне (жалған онлайн-дүкен, сату немесе қызмет көрсету туралы хабарлама орналастыру) шығу үшін қолданған құрылғынының IP-идентификаторын;

- белгілі бір тұлғаның Интернет желісіндегі белсенділігі туралы ақпарттарды алуға (мысалы, оның пайдаланған телефон нөмірі бойынша);

- әлеуметтік желілерде және электрондық төлем жүйелерінде тіркеу үшін, хабарландыруларды орналастыру кезінде және т.б.

Қазақстан Республикасы Үкіметінің 2017 жылғы 12 желтоқсандағы №827 қаулысымен бекітілген "Цифрлық Қазақстан" мемлекеттік бағдарламасында былай делінген «Сенімді құқықтық ортаны және азаматтардың құқықтары мен бостандықтарын, заңды тұлғалар мен мемлекеттің мүдделерін қатаң қорғауды қамтамасыз ету үшін осы бағытты біртұтас, жаһандық цифрландыруды талап етеді. ... Сонымен қатар құқық қорғау органдарын одан әрі цифрландыру шеңберінде олардың қызметінің тиімділігін арттыру үшін ақпараттық-аналитикалық жүйелер енгізілетін болады» [42].

Жоғарыда айтылғандарды қорытындылай келе, электрондық іздерді және ауқымды деректерді (Big data) пайдалану арқылы қылмыстарды тергеу жөнінде жұмыс істеу технологияларын зерделеу бүгінгі күннің шындығы екенін ескере отырып, криминалистиканы одан әрі дамыту және оны іс жүзінде қолдану үшін жаңа мүмкіндіктерді ашуға назар аударғанымыз жөн. Сондықтан қазіргі уақытта аталған мәселеге арналған тұрақты мақсатты зерттеулер, конференциялар, дөңгелек үстелдер және басқа да ғылыми іс-шаралар өткізу өзекті болып отыр.

Ауқымды электронды деректерді ақпараттық технологияларды пайдаланбай талдау өте қиын немесе көп уақытты қажет ететінін, кейбір жағдайда мүмкін емес екенін түсіну керек.Тәжірибе көрсеткендей бір ұялы телефонды, компьютерді, гаджетті, банк картасын және т.б. қолдану арқылы бірнеше алаяқтық жасалады. Ол телефон нөмірі бойынша телефонның IMEI кодын анықтау, ал әрі қарай осы код бойынша телефонға бұған дейін немесе кейін кандай абоненттік нөмірлер орнатылғанын анықтау. Демек қылмыстың субъектісіне қатысты «жаңа» эпизодтарды анықтау мүмкіндігі пайда болады. Осылайша банк карталарымен, электронды әмияндармен (жиі Каспий голд және киви әмиян) және IP мекенжайлармен жасауға болады.

Атап айтқанда, алаяқты анықтағаннан кейін, қылмыстың санаты өзгереді, осы фактілерді ҚР ҚК 190-бабының 3-тармағы 3), 4) тармақшаларымен ауыр қылмыс ретінде (екі немесе одан да көп адамға қатысты, бірнеше рет жасалған алаяқтық) саралау мүмкіндігі пайда болады.

Қылмыстық қудалау органдары алдымен ауыр және аса ауыр қылмыстарды ашуды мақсат етеді. Ақпарттық-технологиялар жетістігін қолдану бірнеше орташа ауырлық санатындағы алаяқтықты біріктіріп, ауыр санатқа қайта дәрежелеуге мүмкіндік беретіндіктен, оның жедел жағдайды оңалтуға ықпал ететіні анық. Сондай-ақ ҚК-тің бабының санкциясы қатаңырақ болып келетіндігі алаяқтардың менмендігін бәсеңдетеді, бұнымен қоса қылмыстың бұл түрін ашу пайызын ұлғайса құқық қорғау органдарының қызметіне азаматтардың сенімі артатыны да белгілі.

2.2 Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтықты тергеудің өзге кезеңдері

Тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты орын алған алаяқтықты тергеудің өзге кезеңдері өте маңызды. Ол типтік тергеу жағдайына негізделген алаяқтың аталған қылмысқа қатыстылығы мен оның кінәсін дәлелдеуге бағытталған тергеушінің іс-әрекетінің бағдарламасы.

Зерттеу жұмысында тауар сату және қызмет көрсету саласындағы интернетте ақпараттық жүйені қолданушыға қатысты орын алған алаяқтық бойынша күдікті анықталмаған деген типтік тергеу жағдайы қарастырылған. Осы негізде типтік тергеу жағдайына байланысты тергеуді жоспарлау туралы жеке әдістеме құрау қажет. Осы тергеу жағдайында тереуші келесі тапсырмаларды орындау қажет: бастапқы тергеу әрекеттерінен алынған алғашқы деректерді саралау, куәлерді анықтап олардан жауап алу, қылмыстың жасалу әдісін саралау, қылмыскерді анықтауға бағытталған шаралар кешенін ұйымдастыру, техникалық байланыс желілерінен ақпарттарға сұрау салу, оның ішінде халықаралық тапсырмалар, халықаралық құқықтық көмек көрсету туралы сұрау салулар жолдау, банктерге және басқа қаржы ұйымдарына сұрау салулар жолдау, сотқа дейінгі тергеп-тексеруді жүзеге асыратын адамға нәрселер мен құжаттарды оларға иелік ететін адамдардың бастамасы бойынша беру жүргізу, сотқа дейінгі тергеп-тексеруді жүзеге асыратын адамның талап етуі бойынша нәрселер мен құжаттарды беру, тінту және алу жүргізу, алынған нарселер мен құжаттарды қарап-тексеру, олардың қылмыстық іс үшін маңызы болса қылмыстық іс материалдарына қосу, қажет болған жағдайда жасырын тергеу әрекеттерін және сараптамалар түрлерін жүргізу.

Тергеу әрекеттерін жүргізу кезінде тергеушінің қолындағы бастапқы тергеу кезеңінде жиналған криминалистикалық маңызы бар материал жан-жақты зерттеліп, көңіл бөлінуі қажет. Өйткені тергеуші бастапқы кезеңде бағыттаушы ақпараттардың барлығын жинап алады.

Қылмыстық іс материалдарына растайтын құжаттарды тіркеу қажет (SMS-басылымдары, мобильді телефонның счеты арқылы ақшалай қаражаттың қозғалуы туралы мәліметтерді, тауар немесе қызмет үшін төленген төлемдерді растайтын чектер, ақшалай қаражатты қолма-қол ақшаға айналдырғанын растайтын чектер, егер басқа счетке ақшалай қаражат аударылған болса, онда сол счет бойынша ақшалай қаражаттың қозғалу туралы мәліметтері қылмыстық іс материалдарына тіркеледі).

Зерттеу барысында зерделенген қылмыстық істердің материалдарын саралау осындай қылмыстарды тергеудің басты проблемаларын көрсетті. Олар ақпараттарды алудың қиындығы, банктермен, ұялы байланыс операторларымен және провайдерлермен тиісті ынтымақтастықтың жоқтығы, қылмыс орын алған интернет-ресурстар және құрылғыларды жылдам анықтаудың заңды мүмкіндіктері жоқтығы, «ізі суымай» қылмыс

жасауға қатысы бар тұлғаларды анықтау мүмкіндігінің жоқтығы (бұл қылмыс түрі қашықтан жасалады, сонымен қатар бас бостандығынан айыру орындарында отырған тұлғалармен және шет мемлекеттерден). Бұл дегеніміз тергеушінің тергеу әрекеттерін және басқа да процесстік әрекеттерін жүзеге асыруда, дәлелдер жинау және нақты жағдайды анықтауда ынтымақтастық (жеке тапсырма, тергеу әрекетін жүргізу үшін тергеу судьясының санкциясын алу және т.б.) орнату үшін белсенді әрекет етуін талап етеді.

Қылмысты орындауда алаяқ көбіне ұялы телефон байланысын қолданады. Осы дәлел көзінен алынған ақпаратты вербалды тергеу әрекеттерін жүргізуде белсенді қолдану қажет. Қазіргі заманғы техникалық мүмкіндіктерге байланысты компьютерлік-техникалық сипаттағы қылмысқа қатысы бар барлық объектілерді алу қажеттілігі туралы айтылған ұстанымды растайды, тергеу әрекеттерімен ұштастыра отырып, олар белгілі бір адамдар туралы, оның ішінде тергеуге алынған алаяқтыққа қатысты адамдар туралы ғана емес, сонымен қатар олардың белгілі бір уақыт аралығында орналасқан жерлері туралы да айтарлықтай көлемде ақпарат алуға мүмкіндік береді. Техникалық құрылғыда телефон номерлері, хабарламалар, кіріс-шығыс журналдарында тұлғаның байланысқан абоненттерін қашан және қанша уақыт сөйлескені, ғаламдық желі интернетке шығу, соның ішінде ұялы байланыс операторы Wi-Fi арқылы шығу туралы ақпараттар бар.

Жеке электронды құрылғының (ұялы телефон, смартфон, планшет және жеке компьютер) ЧИП-картасы арқылы ақпараттарды, оларды қолданушыны анықтауға және оның микропроцессорын зерделеу мәліметтерді алуға мүмкіндік бар. К.Е.Демин және А.А.Васильев GPRS/UMTS жүйелері үшін мобильді төлем жүйелерін қолданғанда транзакциялар арқылы MSISDN (жылжымалы абоненттің халықаралық ISDN номері), оның PIN-кодын, барлық жүргізілген транзакцияларын анықтауға болады дейді [43].

Жауап алудың және басқа да тергеу әрекеттерінің қорытындысы бойынша қылмыстық іс үшін маңызы бар нарселер мен құжаттардың орны немесе орналасуы мүмкін жерлер туралы ақпарат алынады. Егер ондай ақпарат бастапқы тергеу әрекеттері жүргізілгенде алынса, көбірек дәлел ақпарат алу үшін осындай нарселер мен құжаттарды анықтау және алу мақсатында тінту немесе алу тергеу әрекеті жүргізілуі қажет.

Тінту кейінге қалдыруға жатпайтын тергеу әрекеті болып сипатталады, ал алу нәрселер мен құжаттардың нақты орны анықталғанда немесе тұлға оларды тергеушіге өз еркімен беруді қаласа жүргізіледі.

Егер тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты интернетте орын алатын алаяқтық бойынша қылмыскер анықталған жағдайда тінтуді шұғыл арада жүргізу қажет, өйткені оның дер кезінде жүргізілуі дәледемелерді, қылмыс құралын анықтау және алуға ықпал етеді.

Тінту және алу жүргізу барысында мүмкіндігінше барлық алаяқтық жасауға дайындық кезінде пайдаланылуы мүмкін компьютерлік желілерге

(әсіресе Интернет желісіне қатысты) қосылған және іздерді жасыру үшін қолданылуы мүмкін (қалыптасқан тергеу жағдайына сәйкес) техникалық құрылғылар мен құралдарды алу ұсынылады.

Тінту мен алуды жүргізу кезінде, мүмкін дәлел көздері ретінде, барлық ақпаратты сақтаудың электрондық құралдарын алу қажет. Бұл ұялы телефон, смартфон, планшет және жеке компьютер, USB флэш-дискілері, қатты магниттік дискілердегі тасымалдаушылар, ықшам дискілер (CD-R, CD-RW) басқа ақпарат көздері және т. б. [44].

Үй-жайларды, автомашиналарды тінту кезінде ұялы телефондар және тағы басқа электронды тасымалдағыштарды анықтауға мүмкіндік беретін тиісті техникалық құралдарды қолданған абзал. Тінту немесе алу хаттамасында ұялы телефондар және басқа құрылғылар қай жерде және қандай жағдайда табылды олар өз еркімен берілген немесе мәжбүрлеп алып қойылғаны көрсетілуге тиіс. Барлық алынатын құрылғыларды олардың саны, жеке белгілері мен құнын нақты көрсете отырып, хаттамаға енгізу қажет. Егер тінту кезінде мобильді құрылғыларды жоюға немесе жасыруға әрекет жасалған болса, олардың жадында сақталған ақпаратты өшіруге бағытталған әрекеттер болса, онда бұл туралы хаттамада тиісті жазба жасалады және қабылданған шаралар көрсетіледі.

Көрсетілген салдардың туындауына жол бермеу мақсатында тергеуші тінту немесе алу жүргізу басталғанға дейін көрсетілген теріс салдардың туындауына жол бермеуге бағытталған шараларды қабылдауы қажет. Қауіпсіздікке ерекше назар аудару керек, алынатын компьютерлік-техникалық құралдардың өздері, сондай-ақ олардың қылмыс жасауға қатыстылығын айғақтайтын іздер бар құралдар мен құрылғыларға бұл жағдайға ерекше назар аудару қажет.

Қолданыстағы заңнамаға сәйкес тергеліп жатқан алаяқтыққа қатысты ақпарат қана алуға жатады, тергеуші оның мазмұнын анықтауы керек және оқиғаға қатысы бар болса ғана көшіруі тиіс. Алайда ақпараттың аса көлемділігіне байланысты тергеуші бірден қандай ақпараттың қылмысқа қатыстылы бар екенін анықтай алмауы мүмкін немесе кей жағдайларда қажетті парольдердің болмауы себебінен техникалық құрылғылар алып қоюға жатады.

Ұялы байланыс абоненттерінің кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтірін алу ҚР ҚПК 55-бап 1-бөлігі 15-тармағын басшылыққа ала отырып сотқа дейінгі тергеуді жүргізуші тұлғаның, тергеу судьясымен санкцияланған, негізделген қаулысымен жүргізіледі.

Мысалға келтіретін болсам, «Картел» ЖШС бас кеңсесі Нұр-Сұлтан қаласы Жалайыр, 2 мекенжайы бойынша орналасқан және осы компанияның талабы бойынша ұялы байланыс абоненттерінің кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтірі Нұр-Сұлтан қаласында ғана беріледі. Ол дегеніміз Қазақстанның басқа аумақтарындағы тергеушілер Beeline ұялы байланыс операторының телефон номері бар тұлғалардың (ол тұлға күдікті және күзетпен ұсталған болуы мүмкін) қосылулары туралы

мәліметті алуы үшін Нұр-Сұлтан қаласына телекоммуникациялық компанияның бас кеңсесіне келуі қажет. Бұл жағдай тергеудің жедел және толық, жан-жақты, объективті жүруіне кедергі келтіреді.

2018 жылы АҚШ-та Бұлтты заң қабылданды. Бұл заңда АҚШ сәйкес келісім-шарттарға отырған, өзге мемлекеттер аумағында орналасқан ақпарттық-коммуникациялық технологиялар қызметін ұсынушылардан, оның филиалдарынан және еншілес компанияларынан (оның ішінде американдық провайдерлер бар) коммуникациялық деректердің барлық түрлерін алу туралы ордері бар өтінішпен өзара тікелей алмасу режимі қарастырылған [45, 172].

Жәбірленушіден жауап алу кезінде абоненттік номердің басқа тұлғаға тіркелгені анықталса, сол тұлғадан куә ретінде жауап алынады. Жауап алу хаттамасында қашан және қандай себеппен абоненттік нөмір жәбірленушіге берілгені анықталуы қажет.

Деректерді тергеуші байланыс операторына дәлелді сұраныс жіберу арқылы немесе электрондық құрылғы мен ондағы ақпаратты алып қоюға бағытталған тергеу әрекеттерін жүргізу барысында (затты қарау, сот сараптамасын тағайындау, жедел–іздестіру іс-шараларын жүзеге асыру кезінде) алуы мүмкін. Алайда, осы әдістерді іс жүзінде жүзеге асыру кезінде кейбір мәселелер туындауы мүмкін.

Байланыс операторлары құқық қорғау органдарынан көп мөлшердегі сұраныстарды қабылдап алады, сол себепті кейбір жағдайларда шұғыл болып табылатын қажетті ақпаратты алу үдерісін баяулатады. Маман бұл мәселенің шешімін мобильдік операторға әзірленген және енгізілген жедел сұрау салу жүйесін құру деп көреді, оның көмегімен жүйеде тіркелген құқық қорғау органдарының қызметкері жеке кабинет арқылы қажетті ақпаратты ала алады.

Егжей-тегжейлі қосылулар туралы мәліметтерді алған соң, оны қарап-тексеру жүргізу қажет. Олар әдетте ақпараттың көлемі үлкен болғандықтан электронды тасымалдаушылармен жолданады. Қарап-тексеру хаттамасында электронды тасымалдаушылардағы қосылулар туралы егжей-тегжейлі мәліметтерді дәлме-дәл көрсету маңызды. Өйткені хаттамадағы мәліметтердің қате болуы хаттаманы жол берілмейтін дәлелдеме деп тануға себеп болуы мүмкін.

Тауар сату және қызмет көрсету саласындағы интернетте ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтық фактілері туралы қылмыстық істер бойынша нәрселер мен құжаттарды қарап-тексеру қылмыс механизмі, оның орындалу тәсілі, қылмыстық іс субъектілерінің әрекеттердің реті, алынған ақпараттың ұсынылған нұсқаларға сәйкестігі туралы криминалистік маңыздылығы бар ақпараттарды анықтауға бағытталған. Сонымен қатар, қарап-тексеру арқылы нақты тұлғаның қылмыс жасауға қатыстылығын дәлелдейтін іздер анықталады және бекітіледі, компьютерлік-техникалық құралдар және электронды дәлелдемелер алынады.

Алаяқтықтың осы түрін жасауда жиі қолданылатын қылмыс құралы электронды төлем жүйелері (терминал арқылы көпшілігі QIWI кошелекті қолданған) және байланыс пен әп-сәтте хабарламалармен алмасуға мүмкіндік беретін қосымшалар (Telegram, Whatsapp және т.б.) қолданылады. Электронды төлем жүйелерін қылмыс жасау мақсатында белсенді қолдану себебі, оларды тіркеу үшін тек мобильді телефон нөмірі жеткілікті және әрі қарай Интернет арқылы қашықтан немесе мобильді қосымша арқылы қолдану мүмкіндігі бар.

Желілер туралы, клиенттер және олардың белсенділігі туралы ақпарат алу үшін тергеуші (анықтаушы) әлеуметтік желі мамандарымен, оның ішінде провайдерлермен өзара тығыз байланыста болғаны жөн.

Алаяқтық құрбаны мен қылмыстық іс субъектісі арасындағы "электрондық" байланыс фактісін анықтау барысында, абонент (байланыс қызметтерін пайдаланушы) және оператор (тиісті лицензиялар негізінде осындай қызметтерді көрсететін заңды тұлға) арасындағы байланыс қызметтерін көрсету туралы шартты алу қажеттілігі туындайды, бұл ғаламдық желі интернетке қосылғанын, басқа ақпараттық ресурстарға қосылғанын, қашықтан қосылуды куәландыратын және т. б. көрсетеді. Сонымен қатар, жәбірленушінінің жеке қосылу параметрлері, сондай-ақ оператордың (провайдердің) иелігінде болатын болжамды қылмыскердің IP-мекенжайын анықтау үшін қажетті құжаттар талап етілуі қажет.

Зерттеу жұмысының 1-бөлімінде айтылып өткендей тауар сату және қызмет көрсету саласындағы интернетте ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтық жаһандық және транснационалды сипатқа ие, ол дегеніміз халықаралық ынтымақтастық оны тергеуде басты фактор болып табылады.

Халықаралық ынтымақтастықтың негізгі мақсаттары:

- тиісті салада халықаралық ынтымақтастықты жетілдіру;
- халықаралық нормалар және ұсынымдар негізінде ұлттық заңнаманы сәйкес келтіру;
- мемлекеттердің қылмыстарды тергеуде құқық қорғау органдарының іс-әрекеттерінің бірлігіне қол жеткізу [45, 141];

Өзге салалардағы сияқты, мемлекеттердің бірлесіп әрекет етуі киберқылмыстарға қарсы іс-қимыл саласында да конвенциялық (құқықтық келісім-шарт) және институционалды (халықаралық ұйымдар шеңберінде) механизмдерге негізделеді.

Ғылыми әдебиеттерде киберқылмыстарға қарсы іс-қимыл туралы заманауи халықаралық ынтымақтастық келесі ерекшеліктермен сипатталады:

- ынтымақтастықтың аумақтық ұйым және интеграциялық бірлестіктердің шеңберінде өздерінің ынтымақтасу механизмдерін құру арқылы бөлшектеліп даму тенденциясы;
- құбылыстарды түсінудің және негізгі жалпылама қолданылатын, соның ішінде ғылыми түсініктердің жоқтығы;

- заңнаманың дамуы ақпараттық-технологиялыр дамуынан, соның ішінде киберқылмыстың жаңа түрлерінен қалып қоюы құқықтық вакуумы;
- ынтымақтастық процедураларының егемендік қағидасына қатысты мемлекеттер арасындағы қарам-қайшылықтары [46].

Зерттеу жұмысының 1-бөлімінде аталып өткендей Қытай Халық Республикасы өзінің есебінде ақпараттық қылмыстарға қарсы іс-қимыл туралы әмбебап конвенция құрастырудың бастамашыларының бірі болып отыр. Бұл бағыттағы жұмысты ағымдағы жылда бастау БҰҰ-да жоспарланған.

Сондай-ақ зерттеу жұмысының 1-бөлімінде атап өтілген маңызды құжаттардың бірі-компьютерлік ақпарат саласындағы қылмыс туралы Конвенция (Будапешт, 23 қараша 2001жылғы).

Осы қылмыстарды тергеу жөніндегі қызметті іске асырудың негізгі қағидаты ретінде адам құқықтары мен бостандықтарын тиісінше қорғау, оның ішінде 1950 жылғы Адам құқықтары мен негізгі бостандықтарын қорғау туралы еуропалық конвенцияда, 1966 жылғы Азаматтық және саяси құқықтар туралы халықаралық пактіде, сондай-ақ басқа да халықаралық шарттарда көзделген міндеттемелерден туындайтын құқықтарды қоса алғанда, соттық немесе өзге де тәуелсіз қадағалауды қамтамасыз ету қажеттігі атап өтілген. Конвенция компьютерлік деректерді тінту мен алудың, нақты уақыт тәртібінде жинаудың жалпы ережелерін, бұл ретте нақты деректердің сақталуы, олардың өзгермейтіндігі мен түпнұсқалылығын қамтамасыз етілуі қарастырылған.

Бұл құжат мемлекеттің компьютерлік ақпарат саласындағы қылмыстарға қарсы күрес жөніндегі қызметінің жалпы бағыты ретінде әрекет етеді, бірақ дәлел ретінде электрондық ақпаратты алу, бекіту, зерттеу бойынша нақты ұсыныстарды көздемейді.

Қазақстан Республикасы бұл Конвенцияны ратификацияламаған. Өйткені Конвенцияның 32-бабы, «b» тармағында: тарап басқа тараптың келісімінсіз өз аумағындағы компьютерлік жүйе арқылы басқа тараптың аумағында сақталған компьютерлік деректерге қол жеткізе немесе ала алады, егер бұл тарап осы деректерді осындай компьютерлік жүйе арқылы ашуға құқығы бар тұлғаның заңды және ерікті келісімі бар болса делінген. Бұл Конвенцияға қатысушы мемлекеттердің азаматтарының құқықтарына, мемлекеттердің егемендігіне және қауіпсіздігіне зақым келтіруі мүмкін.

Еуропалық парламент әзірлеген қылмыстық істерде электрондық дәлелдемелерді алу және сақтау туралы ережені келтіруге болады. Ол электронды дәлелдемелерді алу және сақтау мәселелері бойынша мемлекетаралық ынтымақтастыққа көп көңіл бөледі, бірақ оны ұқсастықпен және жалпы ережелер бойынша ғана қолдануға болады.

Ережеде электронды дәлелдер дегеніміз – жазылушылар туралы ақпарат, метадеректер немесе провайдер ұсынған мазмұн деректері сияқты электронды түрде сақталатын мәліметтер деген анықтама берілген [47].

Регламентте провайдердің қатысуынсыз электрондық ақпаратты сақтау жүйелеріне тікелей қол жеткізу қамтамасыз етілетін ұстаным негізделеді, бұл жаңа технологияларды енгізу қажеттігіне алып келеді. Бұл жеке деректерді қорғау, жеке, отбасылық өмір, қол сұғылмаушылық, қауіпсіздік және провайдердің өз істерін ұйым ретінде жүргізу құқығын шектеуі мүмкін, бірақ оларды қамтамасыз ету тетігін әзірлеу әр мемлекеттің құзыретіне жатады, дегенмен бұл мәселені шешу ең қиын мәселе болып көрінеді.

Сот әлі күнге дейін осындай сұрауларды санкциялайтын орган ретінде қалыптасқан, бұл осы жүйенің жұмыс жасауы сот бақылауынсыз мүмкін еместігін көрсетеді. Регламентте мәселелердің бірі ретінде электрондық дәлелдемелерді алу және сақтау кезінде мемлекеттік органдар мен провайдерлер ынтымақтастығының жеткіліксіз екендігі көрсетілген, бұл біздің елімізде ғана емес, халықаралық кеңістікте де орын алады. Уәкілетті тұлғалардың мұндай деректерді сақтау жүйесіне кіру мүмкіндігі құқықтық шектелуі тиіс.

Сонымен Қазақстан Республикасының киберқылмысқа қарсы іс-қимыл туралы шетелдермен ақпараттық-коммуникациялық технологиялар саласында арнайы жетекші келісімі жоқ. Қазақстанда қылмыстық істер бойынша құқықтық көмек көрсету туралы сұрау салу және көрсету жалпылама әмбебап, жалпықылмыстық аумақтық және секторлы халықаралық құралдар қолданылады. Олар 2000 жылғы Палермо конвенциясы (БҰҰ), 1993 жылғы Минск конвенциясы (ТМД). Қазақстан Украина, Бразилия, Вьетнам, Венгрия, Монако, Румыния, Италия, Болгария, АҚШ, Чехия, Монголия, Сербия, Испания, Канада, Иордания және т.б. елдермен құқықтық көмек көрсету туралы екіжақты келісім шарттарға қол қойған.

ТМД шеңберінде жоғары технологиялар саласындағы қылмыстарға қарсы іс-қимыл бойынша құқықтық-келісім ынтымақтастығы 2018 жылғы 28 қыркүйектегі Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімге негізделеді, Қазақстан оны 2019 жылғы 9 желтоқсанда ратификациялаған.

2014 жылғы 23 желтоқсандағы Ұжымдық қауіпсіздік туралы ұйым шеңберінде ақпарат саласындағы қылмыстық әрекетке қарсы іс-қимыл бойынша Ұжымдық қауіпсіздік туралы шарт ұйымына мүше мемлекеттердің өзара іс-қимылы туралы хаттамасы бар.

Шанхай ынтымақтастық ұйымының шеңберінде халықаралық ынтымақтасты дамыту тиімді болады. 2009 жылғы 16 маусымдағы Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді айтуға болады. Құжаттың 3-бабында ынтымақтастықтың негізгі бағыттарының бірі ақпараттық қылмыстарға қарсы іс-қимыл делінген.

Қылмыстық қудалау органдарының қызметкерлері ақпараттық-коммуникациялық технологиялар (әртүрлі көздерде әртүрлі аталады:

электронды, цифрлы, виртуалды дәлелдемелер) саласындағы шетелдік провайдерлерден деректер алу қажет болған жағдайда келесі іс-әрекет алгоритмін ескерген жөн.

1. Егер қосылулар туралы мәліметтер алу қажет болса дереу оны сақтау туралы сұрау жолдау қажет. Өйткені оларды сақтау мерзімі қысқа немесе ол елдің заңымен, провайдермен белгіленбеген болуы мүмкін. Әйтпесе құқықтық көмек көрсету туралы сұрау салушылар көп уақыт өткен соң сұрау салынған мәліметтердің жоқтығы жөнінде жауап алады. Ол шетелдік партнердің және тергеудің күшін көрінеу орындалмайтын іс-әрекетке жұмсалуына әкеп соғады. Мәліметтерді сақтау туралы сұрау бір сәтте бір немесе бірнеше каналдар арқылы жолданады:

- Қазақстан Республикасының аумағында қызмет көрсететін шетелдік провайдерге, егер ол өзінің ресми жарияланған саясатында шетелдік құқық қорғау және сот органдарымен тікелей қарым-қатынас жасай алатынын көрсетсе, сондай-ақ осындай электронды сұрауларға арнайы портал ұстаса;
- құқық қорғау (полиция) ынтымақтастығы каналдары арқылы: Интерпол байланыс желілері және ұқсас желілер арқылы; шетел құқық қорғау органдарының мекенжайына Қазақстан Республикасының халықаралық келісім-шарттар негізінде, өзара түсіністік қағидаты негізінде немесе ведомствоаралық келісімдер негізінде; Қазақстан Республикасында елшілік немесе елшілік ұжымдарымен сенім білдірілген полиция байланыс офицерлеріне және басқа құқық қорғау органдарына.

Әрі қарай болған хабарламалар бойынша электронды дәлелдемелерді ұсыну туралы сұрау салуды жолдау кезінде сақталған материалдың провайдер хабарлаған сілтеме номер, код немесе басқа деректемелерін көрсетіп, сақтау жасалғаны туралы сілтеме жасау қажет.

2. Абонент (подписчик) туралы мәліметтерді ұсыну туралы сұрау салу шетел провайдеріне немесе құқық қорғау (полиция) ынтымақтастығы каналдары арқылы көрсетілген тәртіпте жолданады. Алайда көп елдер және провайдерлер осы мәліметтерді сұрау туралы өтінішпен тек құқықтық көмек көрсету тәртібінде сұрау салуды талап етеді, әсіресе олар динамикалық IP-мекенжайларды қолданушылардың жеке басын анықтауларға қатысты болса. Осыған байланысты сұрау салу шетел уәкілетті органдарына ҚР ҚПК 560-бабына сәкес жолданады.

3. Абоненттер және (немесе) абоненттік құрылғылар арасындағы қосылулар туралы ақпаратты, оның ішінде трафик, орналасқан жері бойынша триангуляциялық биллинг (ұялы байланыс операторларының базалық станцияларының орналасуы туралы) туралы ақпаратты алу қажет болған жағдайда ҚР ҚПК 253, 254-бабтары негізге 560-бап бойынша шетел уәкілетті органдарына құқықтық көмек көрсету туралы сұрау салу жолданады. Тергеу соттымен санкцияланған қаулы бірге жолданады.

Хабарламалардың мазмұны (контент) жайлы ақпарат, басқа да электронды хабарламалардың мазмұнын алу, дәл қазіргі уақытта болып

жатқан байланыс (сөйлесу, хабарламалармен алмасу) туралы ақпарат алу, тыңдау, басқа да электронды ақпарат алу туралы сұрау салу құқықтық көмек көрсету тәртібінде ҚР ҚПК 560-бабының тәртібінде жолданады. АҚШ қылмыстық іс бойынша дәл қазіргі уақытта болып жатқан байланыс (сөйлесу, хабарламалармен алмасу) туралы ақпарат алу, тыңдау туралы халықаралық құқықтық көмек көрсетпейді.

Алайда көп елдер осындай шараларды жүргізу туралы өтінішпен құқықтық ынтымақтастық емес, тек құқықтық көмек көрсету тәртібінде сұрау салуды талап етеді. Осыған байланысты сұрау салу шетел уәкілетті органдарына ҚР ҚПК сәйкес нормаларының негізінде жолданады.

Электронды дәледемелерді сақтау немесе ұсыну туралы сұрау салуды жазу кезінде нақтылықты қамтамасыз ету қажет, ол дегеніміз Интернет желісіндегі ақпарттық ресурсқа ену уақыты туралы мәліметтерді секундын, сағаттық белдеу туралы мәлімет, кірілген ресурстың (сайттың) IP-мекенжайы, хаттаманың атауы немесе байланыс орнатылған порттың номері, оларсыз шетелдік серіктестің сұрау салуды орнидауы мүмкін емес болуы мүмкін.

Қазақстан Республикасының жедел-іздестіру қызметі туралы заңының 18-бабы 2-тармағына сәйкес жедел-іздестіру қызметін жүзеге асырушы органдары басқа мемлекеттердің аумақтарында өзара іс-қимылды және жедел-іздестіру шараларын осы Заңда, сондай-ақ тиісті шарттар мен келісімдер негізінде сол мемлекеттердің заңдарымен белгіленген тәртіп пен шекте жүргізеді.

Заманауи халықаралық қылмыстық құқықтың дамуы сатысында қылмыстық істер бойынша құқықтық көмек көрсету тек ратификациялауға жататын мемлекетаралық деңгейдегі келісім-шарттармен, басқа мемлекеттердің міндеттемелері көрсетілген, заңмен өзара түсіністік қағидаты бекітілген халықаралық-құқықтық құжаттармен ғана реттеледі. Одан басқа нақты қылмыстық істер бойынша мемлекетаралық ad hoc келісім-шарттарға отыру арқылы және оларды орындау туралы ұлттық заң қабылдау арқылы құқықтық көмек көрсетудің арнайы түрі бекітіледі.

Қылмыстық құқықтық, процессуалдық ынтымақтастық халықаралық құқық қорғау (полициялық) бойынша көмек көрсетуден айырмашылығы бар. Құқық қорғау бойынша көмек көрсету халықаралық, үкіметаралық, және ведомствоаралық келісімдермен реттелетін бағыттаушы ақпаратпен алмасу және жедел-іздестіру жұмысын қамтиды. Құқықтық көмек көресту және полициялық көмек көрсетуді бөлу мемлекетішілік құқықта қамтылмаған және әр мемлекетте әр түрлі.

Процесстік және жедел-іздестіру қызметі шетелдік құқық қорғау саласында және халықаралық құқықтық құжаттарда бірігіп кетуіне байланысты құқық қорғау бойынша көмектесу құқықтық көмектің ішіне кіреді.

«Көмек көрсету туралы сұрау салу» термині Қазақстан Республикасының қылмысқа қарсы іс-қимыл саласындағы көптеген мемлекетаралық және үкіметаралық келісім-шарттарында қолданылады.

Интернетке шыққан құрылғыны кей кезде провайдерде ондай техникалық мүмкіндік болмағандықтан анықтау мүмкін емес болады. Өйткені IP-мекенжайды жасыратын бағдарламалар қолданулыуы мүмкін. Олар Tor және тағы басқа прокси серверлер, анонимайзерлер, VPN болуы мүмкін. Бірақ Ресейлік ғалымдардың пікірінше қиынға соқса да анықтауға болады егер «IP-мекенжайлардың пулдарын қолданғанда деректерді жолдау құрылғысында NAT (Network Address Translation) технологиясы Интернетке кіру үшін қолданылса, бір сыртқы IP-мекенжайы көптеген абоненттерге қызмет көрсету үшін бөлінуі мүмкін». [45, 158] Шетелден келіп түскен динамикалық IP-мекенжайды сұрау салуда егер интернет ресурске ену туралы уақыт секундына дейін нақты көрсетілмесе, сағаттық белдеу көрсетілмесе, ресурс IP-мекенжайы (сыртқы сайт), қосылаулар жүргізілген порт нөмірі немесе хаттама атауы көрсетілмесе, жауап беруші әдетте айтарлықтай массивті абоненттік деректер жолдайды. Ол дегеніміз оның ішінде қылмыстық іске қатысы жоқ тұлғалар туралы мәліметер де бар деген сөз. Шетелдік орындаушы оны сұрау салушы өз бетімен електен өткізу (data mining), саралау, салыстыру үшін жолдайды.

Кейде абонент жалған деректертер арқылы тіркелген болып шығады, ал ол көрсеткен мекенжай жоқ немесе ол мекенжай бойынша іске қатысы жоқ басқа тұлға анықталады. Одан жиі кезедесетіні қылмыскер бөтеннің деректерін бүркену үшін, ұрланған қаражатты қолма-қол ақшаға айналдыру немесе аудару үшін қолданады. Дәлелдемелердің бұндай кемістіктерін бұндай жағдайда куәлерден және күдіктілерден жауап алу, беттестіру жүргізу, нәрселерді және құжаттарды алу және қарап-тексеру арқылы толтырады.

2019 жылы EuroPolice бағдарламасы бойынша өзара іс-қимыл жасауда БҰҰ Есірткі және қылмыстылық бойынша басқармасы, БҰҰ Қауіпсіздік кеңесі Контртеррористік комитет орындаушы диреткоры, Халықаралық прокурорлар ассоциациясымен бірлесіп «Басқа елдерден электронды дәлелдемелерге сұрау салу тәртібі бойынша практикалық нұсқаулық» шығарылып ол орыс тіліне аударылған. Бүгінгі күні бұл жан-жақты басылым тәртіпсақшыларына халықаралық ынтымақтастықта заттай дәлелдемелерді жинаудың ретін, осы саладағы халықаралық нормалар жайлы егжей-тегжейлі ақпараттарды, ақпараттық-коммуникациялық технологиялар саласындағы негізгі қызмет көрсетушілердің шет мемлекеттердің уәкілетті органдарының электронды дәлелдемелерді сақтау және ұсыну туралы сұрау салуларын қарау ережелері туралы, соның ішінде оларды құқықтық көмек көрсету туралы сұрау салусыз төтенше және ерікті түрде ашу, телекоммуникациялық хабарламаларды нақты уақыт режимінде бақылау және ұстау туралы шет мемлекеттердің сұрауларын орындау құқықтық мүмкіндіктері туралы ақпараттарды қамтиды.

Электронды дәлелдемелерді алу, бағалау, қолдану процесін дамыту және жетілдіру ғана емес сондай-ақ шетелдік серіктестермен қарым-қатынас жасайтын электронды каналдарды да дамыту, заңды мәні бар халықаралық электронды құжаталмасуды қамтамасыз ету қажет. Мысалы короновирустық инфекция пандемиясы кезінде, 2020 жылы көптеген мемелекеттердің қылмыстық істер бойынша құқықтық көмек көрсету және құқықтық қатынас бойынша орталық органдары кіріс-шығыс құжаталмасу тәртібінің тек қағаз жүзіне көшкендігі және уақытша сұрау салуларды орындауды тоқтату туралы хабарлады[45, 162].

Интерпол шеңберінде I – 24/7 желісі, оған қосылған I-SECOM қорғалған байланыс желісі, электронды дәлелдемелерді дереу сақтау жөнінде жедел шараларды қабылдау үшін жұмыс жасайды.

Осылайша, тауар сату және қызмет көрсету саласындағы интернетте ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтық фактілері туралы қылмыстық істер бойынша тергеу және басқа да процесстік әрекеттерін жүргізу белгілі бір ерекшеліктері бар, олар қылмыстық әрекеттің механизмімен, сондай-ақ оны жасаған субъектілерге байланысты толық белгіленген. Тергеу әрекетінің оң нәтижесі мен мақсатына жету үшін тергеуші әр түрлі тактикалық әдістерді және мамандардың көмегін қолдана отырып, оны жүргізуге мұқият дайындалуы қажет.

Алайда аталған қылмысы түрін тергеудегі ең жиі жүргізілетін тергеу әрекеті – абоненттер арасындағы ұялы байланыс абоненттерінің кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтірі алуды жүргізудің өзі Қазақстан Республикасының аумағында болса да, Нұр-Сұлтан қаласының аумағында ғана жүргізіледі. Бұл жағдай тергеудің кешеуіне әкеп соғады. Сондықтан мемлекетіміздің әр облыс орталығында ұялы-байланыс операторларының кеңсесінен абоненттер арасындағы ұялы байланыс абоненттерінің кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтірі алуды жүргізудің мүмкіндігін ұйымдастыру қажет.

Ал шетелден алынатын деректерге келетін болсақ, бұл процесстің жүргізілу тәртібі тергеуді әуре-сарсаңға салатындығын айтуға болады. Қазақстан Республикасының киберқылмысқа қарсы іс-қимыл туралы шетелдермен ақпараттық-коммуникациялық технологиялар саласында арнайы жетекші келісімі жоқ. Қазақстанда қылмыстық істер бойынша құқықтық көмек көрсету туралы сұрау салу және көрсету жалпылама әмбебап, жалпықылмыстық аумақтық және секторлы халықаралық құралдар қолданылады. Ол дегеніміз, мысалы, Қазақстан Республикасының облыстарының бір қаласындағы тергеуші ол қалада орын алған алаяқтық бойынша шетел провайдерінен деректер алу үшін алдымен тергеу судьясынан санкция алады, сосын оны құқықтық көмек көрсету туралы сұрау салуға қоса беріп, қалалық прокуратураға жолдайды, әрі қарай қалалық прокуратура облыстық прокуратураға жолдайды, ал облыстық прокуратура Бас прокуратураға жолдайды. Бас прокуратурада ол сұрау салу келісілсе,

шетелдің уәкілетті органына халықаралық келісім шарттың негізінде немесе өзара түсіністік қағидатына негізделе отырып жолданады.

Бұл ретте ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықты тергеуді жеңілдету үшін шетел уәкілетті органдарымен және провайдерлермен ынтымақтастық орнату үшін электронды құжаталмасуды пайдаланып, жаңа жеңіл жолын құрастыру және тиісті халықаралық нормативті құқықтық актілерді ратификациялауға шаралар қабылдау қажет.

3. Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтықтың алдын алу.

3.2 Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтыққа ықпал ететін себептер мен факторлар

Бүгінгі күні жер бетінде 4-индустриялық революция жалғасуда, ол дегеніміз 21-ғасырдың басынан жасанды интеллекттің және Интернеттегі үлкен деректердің дамуының орын алуы. Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтық - өмірімізіде орын алып жатқан 2-ақпарттық революцияның жағымсыз құбылысы.

Ақпараттық технологиялардың дамуы оларды қолданып жасалатын қылмыс санының өсуіне ықпал етеді. Осыған байланысты құқық қорғау органдарының қызметкерлерінің білімі де бұл құбылыспен бірге аяқ алып жүруі және оған қарсы-іс қимыл әдістері де жетіліп отыруы қажет.

Зерттеу жұмысының барысында ақпараттық жүйені қолданушыға қатысты орын алған алаяқтық фактілері бойынша қылмыстық істерді зерделеген соң бірқатар себептер және жағдайлар туралы қорытынды жасауға болады. Кримногендік себептер:

- компьютерлік технологияны қолданып жасалатын құқыққа қайшы іс-әрекеттердің шын мәнінде әжеп тәуір пайдаға әкелетіндігі және салыстырмалы түрде жылдам және «қауіпсіз» болуы;
- құқық қорғау органдары қызметінің тиімсіздігі, қылмыскерлердің өздерінің жазасыз қалатындығына сенімділігі;

Әлеуметтік себептер:

- жаппай ақпараттық технологиялардың, ақпараттық-телекоммуникациялық желілердің, ақпараттық қызмет көрсетудің, электронды құжат алмасудың дамуы және жетілуі алаяқтардың іс-әрекетіне оңтайлы жағдайды туғызады;
- қоғамның ақпарттық, компьютердік қылмыстылыққа деген немқұрайлы көзқарасы;
- Интернет русурсты қолдану облысы және уақыттың өсуі;
- Интернеттегі және компьютерлік тасымалдағыштардағы ақпарттың ұлғаюы;
- ақпарттық жүйені қолданушылардың тауар және қызмет түрін онлайн-сатып алуда асқан сенгіштігі (тауар және қызметті алғанға дейін, олардың ақысын төлеу, әсіресе банктік шот арқылы емес, интернет-әмиян арқылы);

Әлемдік тәжірибе көрсеткендей, қылмыстық виктимизацияны зерттеу қылмыстың нақты ауқымын, оның латенттілігін және адамдардың виктимдікке жақындығын, қылмыстық ахуалдың қазіргі жағдайын талдауға, қылмысқа қарсы күрестің күшейтілген шараларын қабылдауға және халықтың қылмыстық құрбан болуына қарсы тұру жолдарын анықтауға ықпал етеді [48].

Құқықтық себептер:

- ақпараттық жүйеде орын алатын қылмыстарға қарсы іс-қимыл туралы заңнаманың кемшіліктері;
- компьютерлік қылмысты тергеудегі қалыптасқан тергеу және сот тәжірибесінің жоқтығы;
- ақпарттық жүйені қолданып жасаған қылмыстар үшін жазаның жеткілікті қатаң емесітігі;

Кадрлық себептер, интернет желісінде орын алатын қылмыстарды тергеудегі қылмыстық қудалау органдарының қызметінің кемшіліктері:

- қылмыстың салдарын елеусіз деп санау;
- алаяқтың кінәсін тиісті дәлелдей алмау;
- қылмыстың күрделі түрін тергеуге ынтасының жоқтығы.

Зерттеу жұмысының 1-бөлімінде атап өткендей интертте орын алған алаяқтықтың саны жылдан жылға өсуде, ал оларды ашу пайызы төмен. Демек жедел-іздестіру және тергеу жұмысының деңгейі төнген қауіпке сәйкес келмейді.

Тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолдануға қатысты орын алған алаяқтықтың латенттілігі құқық қорғау органдары қызметкерлерінің объективті және субъективті мүмкіндіктерімен байланысты болып келеді. Көбінесе олар қысқа мерзім ішінде қарауға тиісті қылмыстар туралы жедел мәліметтер көлемінің үнемі өсуіне байланысты тез жауап бере алмайды. Өйткені қызмет ұсынушылар және құқық қорғау органдараның арасында және құқық қорғау органдарының, сот органдарының өзара қарым-қатынастары тергеуді әуре-сарсаңға салады.

Құқық қорғау органдарының ресурстарының шектеулі болуы, қылмыстар туралы келіп түсетін белгілердің барлығына бірдей жауап бере алмауына әкеп соғады, сондықтан олар байқалмай қалады.

Статистикалық есептің кемшіліктерін осы латенттіліктің бір түріне жатқызуға болады. Мысалы, тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты орын алған алаяқтық, банк мекемелеріндегі көбінесе несиелік-қаржылық саладағы құқық бұзушылық ретінде ескеріліп, жоғары технологияларды қолдану саласындағы істердің шынайы жағдайын көруге мүмкіндік бермейді.

Сондай-ақ, құқық қорғау органдарының қызметкерлері хабардар болып, бірақ белгілі бір себептермен оларды есепке алмау фактілеріне тоқталу қажет. Мұндай жағдайлар белгілі бір ауданда, қалада немесе аймақта статистикалық әртүрлі айла-амалдар жасау арқылы қылмыстық құқық бұзушылықтардың жоқтығына көз жеткізу мақсатында жасалынуы мүмкін.

Кейбір жағдайларда қылмыстарды жасыру қызметкердің жеке мүддесінің негізінде туындауы мүмкін. Бұл құқық қорғау органының қылмысты ашуға міндетті қызметкерлердің, сондай-ақ көптеген заңгерлердің,

соның ішінде құқық қорғау органдарында қызмет атқаратындардың білімінің жеткіліксіздігіне байланысты сенімділіктің болмауына байланысты.

Ұйымдастырушылық-техникалық себептер:

1) компьютерлік қылмыстардың жоғары латенттігі. Осыдан көптеген алаяқтардың өзінде артықшылығым бар деп және осал тұстарым жоқ деп санауы туындайды. Латенттіктің негізгі себептері анықтаудың қиындығы, жаңадан IT-технологиялардың ойлап табылауы, Интернет желісін және мобильді компьютерлік құрылғыларды қолданушылардың ұлғаюы, электронды құжаталмасуға көшу, көпшілікке жасырын виртуалды кеңістікте қылмыс жасау, мемлекет тарапынан киберкеңстікті және бұқаралық ақпарат құралдарын тиімді бақылаудың жоқтығы, қылмыс құрбандарының құқық қорғау органдарына өтініш білдіргісі келмейтіндігі.

Жәбірленушілердің кінәлілердің жазаға тартылатындығы және ақшалай қаражаттың қайтарылатындығына сенімсіздігі, сондай-ақ азаматтардың құқықтық білім деңгейінің төмендігі мен заңды негізде өз құқықтары мен мүдделерін қорғай алмауы жатады.

Интернет желісінде ақпараттық жүйені қолданушыға қатысты орын алатын қылмыстардың тағы бір себебі: қоғамның әлеуметтік даму деңгейі мен технологиялық даму деңгейдің арасындағы айырмашылық. Адам ақпараттық технология саласында дамыса, оны моральдық тұрғыдан дамыды деп санауға жатпайды, сондықтан бұндай жағдайда жауапкершілік сезімі тиісті деңгейде қалыптаспауы мүмкін. Мемлекет қоғамдық өмірдің әртүрлі ортасында байқалатын қоғамның белсенді компоненттерін ескере отырып, жаңару және жаңарудан туындайтын мәселелерді шешуде. Жаңару компьютерлік жүйелерді жиірек қолданудан көрінеді.

Тауар сату және қызмет көрсету саласында ақпараттық жүйенің қолданушыға қатысты орын алатын алаяқтықтың себептерінің бірі моральдық нормалардың төмендігі және әлсіздігі. Қажетті адамгершілік қасиеттерінің жоқтығы, ал жалпы қабылданған мінез-құлық стандарттары көбінесе ақпараттық әлеуметтік талаптарға сәйкес келмейді. Компьютерлік қылмыстарды жасаудың әлеуметтік себептері қазақстандық азаматтарының моральдық және ғылыми даму сатыларының сәйкес келмеуінде.

Жәбірленушінің мінез-құлқы мен іс-әрекеті қылмыс жасау үшін қолайлы жағдай тудыруы мүмкін. А. Л. Ситковский виктимологиялық алдын-алу – виктимдік мінез-құлықты қалыптастыратын және қылмыс жасауға себепші болатын факторларды, жағдайларды анықтауға, жоюға немесе бейтараптандыруға бағытталған әлеуметтік институттардың ерекше қызметі; қорғау қасиеттерін қалпына келтіру немесе жандандыру мақсатында тәуекел топтарын және виктимділігі жоғары дәрежелі нақты адамдарды анықтау;

жеке және заңды тұлғаларды қылмыстардан қорғаудың қолда бар арнайы құралдарын әзірлеу не жетілдіру деген [49].

Тергеу жағдайының құрамын кешенді талдаусыз және қараусыз қылмыс механизміндегі жәбірленушілердің виктимологиялық рөлін анықтау мүмкін емес.

Аталған қылмысты жасау кезінде жәбірленушінің субъективті қасиеттері шешуші рөл атқарады. Мәселен, менмендік, ұқыпсыздық, өз мүмкіндіктерін жоғары бағалауы, дағдылары мен тәжірибелерін артық бағалауы, бейқамдық қылмыс жасауға көбінесе себеп болады. Бұдан басқа, жәбірленушінің субъективті қасиеттерінен және қалыптасқан жағдайдан басқа, виктимогендік факторларды да ескеру қажет.

2) Көпшілік веб-сайттардың осалдығы ақпарттық жүйені қолданушының жеке деректерінің жария болуына әкеп соғыуы мүмкін. Мысалы, егіз сайттар арқылы алаяқтардың жасаған сайтына ақпараттық жүйені қолданушыны өтікіп жібереді, ал жеке деректер алаяқтардың қолына түседі.

Сондай-ақ Интернет желісінде әртүрлі мазмүндағы, соның ішінде криминалды ақпараттар, жарнамалар, кеңінен таралған. Бұл ақпарттарға адамдар жеңіл қол жеткізе алады, ал Интернетте құқықтық мәдениеті және адамгершілігі әртүрлі деңгейде дамыған адамдар отырады. Әрине компьютерлік қылмыстың санының және сапасының өсуі қоғамдық өмірдің әртүрлі саласындағы қарама-қайшылықтардың өсуіне, құқық қорғау органдарының жиі реформаға ұшырауына, заңнаманың кемшіліктеріне, құқықты қолданудағы осалдықтарға байланысты.

Құқық қорғау органдары өз тәжірибесінде ақпарттық-технологиялар арқылы жасалатын алаяқтыққа ықпал ететін себептер мен жағдайлар туралы әртүрлі ақпарат көздерін пайдаланады:

- белгілі бір аймақтағы жедел жағдайды сипаттайтын және бағалайтын материалдар;
- тергеу жүргізілген қылмыстық істер бойынша ақпарат;
- статистикалық мәліметтер;
- бұқаралық ақпарат құралдарындағы хабарламалар;
- құпия көмек көрсеткен адамдардың хабарламалары;
- әкімшілік тәжірибе құжаттары;
- жедел-іздестіру сипатындағы құжаттар;
- құзыретті тұлғалардың хабарламалары, азаматтардың хаттары мен өтініштері;
- бастапқы ақпаратты тексеру құжаттары;
- жедел есепке алу туралы мәліметтер (оның ішінде мұрағаттық);

- жедел-іздестіру және жедел-техникалық сипаттағы белгілі бір шаралар нәтижелерімен ақпарат.

Бұндай ақпарат көзерінен алынған деректерді өңдегеннен кейін жалпы алдын алу шараларын әзірлеуге және өткізуге мүмкіндік болады.

Мұндай қызметтің, алаяқтық және оларды жасауға қолайлы жағдайлар туғызатын себептерді анықтауға бағытталған қазіргі заманғы технологияларды қолдана отырып жымқырудың нақты жағдайларын болдырмау үшін жаһандық маңызы зор.

Қорытындылай келетін болсақ, тауар сату және қызмет көрсету саласындағы ақпараттардың жүйені қолданушыға катысты орын алған алаяқтық жасауға ықпал еткен себептерін және жағдайларын тану жалпы алдын алу шараларының бастапқы сатысында жүзеге асырылады. Бұл себептер мен жағдайларды криминогендік, әлеуметтік, құқықтық, кадрлық, ұйымдастырушылық-техникалық деп жіктеуге болады.

Қылмыстың детерминанттарын анықтаған соң оларды жою үшін тиімді шаралар қолданылуы керек. Мұндай шараларды ішкі істер басқармасы қызметкерлері, сондай-ақ құқық бұзушылықтардың себептері мен оларды жасауға ықпал етуі мүмкін жағдайларды жоюға көмектесуге міндетті тиісті мемлекеттік және қоғамдық құрылымдар жүзеге асыра алады.

Құқық бұзушылықтарды тудыратын себептердің үлкен бөлігі және олардың жасалуына қолайлы жағдайлар әртүрлі салада, меншіктің әр түрлі нысандарымен байланысты кездеседі, сондықтан оларды тек жедел қызметкерлердің жоюы қиынға соғады.

3.2 Қызмет көрсету мен тауар сату саласындағы интернет арқылы жасалатын алаяқтықтың алдын алудың жалпы және арнайы шаралары

Заманауи ақпараттық-технологиялар қоғамдық өмірімізге тереңінен еніп, тек жаңа мүмкіндіктер ғана емес, сонымен қатар ақпараттық жүйені қолданушыға қарсы қылмыстарды туындатты. Ақпараттық-телекоммуникациялық технологияның дамуы алаяқтардың көбіне жазадан құтылып кету мүмкіндігіне жол береді, өйткені қылмыстық заңнама ақпараттық-технологиялар саласындағы қылмыстарға осал бейімделген. Алайда онлайн-сауда, банк операциялары, деректерді жылдам жолдау, заманауи байланыс форматы, электронды білім алу, ойын-сауық порталдары қоғамдық өмірге және мемлекетке толығымен енген.

Криминологияда алдын алудың дәстүрлі үш түрі бар: жалпы, арнайы және, зерттеу тақырыбы бойынша, тауар сату және қызмет көрсету саласындағы ақпараттық жүйені қолданушыға қатысты интернетте орын алатын алаяқтықтың алдын алуға жеке бағытталған шаралар.

Жалпы алдын алу шаралары туралы 2012 жылғы 6 қаңтардағы № 527-IV «ҚР ұлттық қауіпсіздігі туралы» Заңында айтылған.

Ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықтың алдын алудың арнайы шараларына:

- құқықтық шаралар, олар қылмыстық заңнаманы бірқатар түсініктерге анықтама беру арқылы жетілдіру, тергеу және сот тәжірибесін жетілдіру, тергеу және сот тәжірибесінің біртектес болуы үшін Қазақстан Республикасының Жоғарғы сотының ақпараттық-технологиялар саласындағы қылмыстарды тергеу тәжірибесі туралы қаулысын шығару. Қолданыстағы заңнаманы қоғамда болып жатқан құбылыстарға уақытылы әрекет ету үшін қолдану мүмкіндігін талдау. Заң жобаларын криминологиялық сараптамадан өткізуді ұйымдастыру, құқықтық шығармашылық және құқық қолдану деңгейінің халықаралық қылмыспен күрес стандарттарына сәйкес келуі. Сондай-ақ екі жақты, көпжақты мемлекетаралық келісім-шарттарға отыру.

Интернет-технологияларын қолдану арқылы жасалған алаяқтық саласындағы заңнаманы жетілдіру жөніндегі жұмыс, өз кезегінде қылмыстың осындай түрінің латенттілік дәрежесін төмендетеді.

- рухани және мәдени шаралар. Бұқаралық ақпарат құралдарының ақпараттық-технологияларды қолдану арқылы орын алатын алаяқтықтар туралы халықты хабардандыру жұмысын жандандыру, тұрғындарды құқықтық насихаттау және құқықтық білімін көтеру;

Бұқаралық ақпарат құралдары арқылы интернетте жасалатын алаяқтықтың мәселелерін түсіндіру арқылы азаматтардың құқықтық нигилизміне қарсы күрес. Қоғамның назарын жоғары технологиялар саласындағы қылмыстың көбеюінің жағымсыз тұстарына көңіл аудартуымыз қажет. Жоғары технологиялар саласында латенттік қылмыстарды анықтау және талдау үшін әлеуметтік әдістер мен тәсілдерді қолдану: жергілікті тұрғындарға жаппай сауалнама жүргізу, сараптамалық бағалау, БАҚ материалдарды талдау. Интернет-технологиялар арқылы жасалатын алаяқтық саласындағы қылмыстық әрекеттерді жасаудың әлеуметтік аспектісіне ерекше назар аударған жөн.

Интернет желісіндегі қылмысқа қарсы іс-қимыл жүйесінде бұқаралық ақпарат құралдарын пайдалануда бірнеше бағытты біріктіру керек. Мысалы, халық алдында осы қылмыстарға қарсы күрестің нәтижелері туралы есеп беру, құқықтық сана-сезімді және қылмыстық көріністерге төзбеушілікті қалыптастыруға бағытталған құқықтық насихатты жүргізу, алаяқтық қол сұғушылықтан қорғанудың құралдары және әдістері туралы халықты ақпараттандыру, интернет желісіндегі алаяқтықты жүзеге асырудың жаңа жолдары туралы хабардандыру. Ақпараттық-технологияларды қолдана отырып жасалған қылмыстардың ерекшелігіне байланысты, бұл ақпаратты уақтылы жеткізудің қылмысты ескерту әсері өте жоғары, әсіресе бұқаралық ақпарат құралдарында ұсынылған ақпарат жүйелілі, көрнекі және уақтылы болса. БАҚ-пен жұмыс істеуге қоғамдық ұйымдарды да тарту қажет.

- ұйымдастырушылық-басқарушылық және техникалық (халықаралық-құқықтық ынтымақтастықты жетілдіру, ақпараттық-жүйені қолданушыға қарсы қылмыстарға қарсы іс-қимылдар бойынша құқық қорғау органдарының өзара және басқа да іске қатысы бар ұйымдардың бірлесіп іс-қимыл жасау деңгейін көтеру);

Ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықтарға қарсы іс-қимыл жөніндегі қызметті ақпараттық-аналитикалық қамтамасыз етуді жетілдіру қажет. Бұл жұмыс криминологиялық маңызды ақпараттарды жинау және бір жүйеге келтірумен байланысты бірқатар міндеттерді шешеді, әрі қарай оны талдау және жіктеу, осы негізде істердің нақты көрінісін анықтау, жағдайдың даму үрдісін болжауға мүмкіндік береді. Ақпараттық-аналитикалық жұмыстың нәтижелерін құқықтық шығармашылықта және құқық қорғау тәжірибесінде қолдану қажет, әйтпесе оның мағанасы болмайды.

Елде құқық қорғау құрылымдарының жұмыс істеу тиімділігін арттыру және халықтың оларға деген сенімін арттыру, ақпараттық-технологиялар арқылы жасалатын қылмыстарды зерттеудің статистикалық әдістерін

жетілдіру - сөзсіз қылмыстардың осындай түрінің латенттілігін төмендетуге мүмкіндік береді.

- криминалистикалық шаралар. Олар ақпараттық жүйені қолданушыға қатысты алаяқтықты тергеу әдістемесін жетілдіру және жаңа әдістеме ойлап табу, құқық қорғау органдарының ақпарттық жүйені қолданушыға қатысты алаяқтықтарды тергеу тәжірибесін біріктіріп саралау, соның негізінде аталған қылмыс түрлерін ашу және тергеу туралы әдістеме құру.

Құқық қорғау қызметкерлерінің кәсіби деңгейіне қатаң талаптар қою арқылы құқық қорғау органдары қызметінің сапасын арттыру. Осы мақсатта заңдық бағыттағы жоғары оқу орындарында ақпарттық жүйені қолданушыға қатысты жасалатын қылмысты зерделеу жөніндегі арнайы курстар енгізілуі тиіс.

Алдын алу шараларының оң нәтижесіне тек мемлеткет және азаматтық қоғам институттары жергілікті басқару органдары, білім және ғылым ұйымдары, бұқаралық ақпарат құралдары, қызмет ұсынушылар, байланыс операторлары, қаржы ұйымдары және т.б. келісіп іс-әрекет етуі нәтижесінде жетуі мүмкін.

Ақпараттық-технологияны қоланып жасалатын алаяқтыққа қарсы іс-қимыл бойынша жұмысты ғылыми қамтамасыз ету қажет. Ғылыми-зерттеу жұмысының нәтижесі бейімделіп тәжірибеде қоданылса, негізгі нәтиже осы болып табылады. Құқық қорғау органдарының күшін үйлестіру бастапқы криминологиялық ақпаратты (қылмыс туралы арыздар мен хабарламаларды тіркеуден) жинаудан басталады.

Тауар сату және қызмет көрсету саласындағы акпараттық жүйені қолданушыға қатысты орын алған алаяқтықтың нақты себептерін және олардың орындалуына ықпал еткен жағдайларды анықтау, оларды жою жөніндегі шараларды жүзеге асыру құқық қорғау органдары қызметкерлерінің қызметінің негізін құрайды. Құқық бұзушылықтың алдын-алу, қоғамның қылмыстық дәрежесін төмендетудің қуатты тетігі болуымен байланысты, сондықтан мемлекеттік құрылымдар барлық сатыларда тиімді алдын алу іс-шараларын жүргізуі тиіс.

Қазақстан Республикасының Заңдылықты, құқықтық тәртіпті және қылмысқа қарсы күресті қамтамасыз ету жөніндегі үйлестіру кеңесі отырысының 2021 жылғы 4 наурыз № 1кс/21-01 алаяқтықпен және қаржылық пирамидалармен күрес саласындағы уәкілетті органдардың күш-жігерін үйлестіру туралы хаттамасында алаяқтықпен күрес саласында Ішкі істер министрлігіне келесілер ұсынылған:

- алаяқтық фактілерінің, әсіресе ақпараттық технологияларды пайдалана отырып жасалатын фактілердің алдын алу және жолын кесу бойынша қосымша шаралар қабылдауды қамтамасыз ету;

- Қаржылық мониторинг агенттігімен бірлесіп, кредит беру және банк қызметі саласындағы алаяқтыққа қарсы іс-қимыл бойынша жұмысты жандандыру;

- IT-технологиялар саласында арнайы білімі бар интернеталаяқтыққа қарсы іс-қимыл жөніндегі тиісті жедел-тергеу бөлімшелері қызметкерлерінің штат санын ұлғайту мәселесін қарастыру;

- Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігімен бірлесіп: - іздестіріліп жатқан адамдардың мемлекеттік қызметтерге жүгіну фактілері туралы іздестіру бастамашысын дереу хабардар ету (өзара іс-қимыл алгоритмі);

- ұрланған телефонға SIM-картаны орнату әрекеті кезінде байланыс операторлары сұрау салу бастамашысын онлайн хабарлау үшін Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің сәйкестендіру кодтарының дерекқорын Ішкі істер министрлігінің БДБ-мен интеграциялау («қылмыстық заттар» есебі);

- республикалық маңызы бар қалалар мен облыс орталықтары филиалдарындағы абоненттер және олардың қосылыстары туралы мәліметтерді алуды жүргізу;

- алаяқтық фактілерін барынша азайту үшін пайдаланушыларды онлайн алаңдарда (OLX, Krisha, Kolesa және т. б.) олардың жеке басын сәйкестендіре отырып, тіркеу тәртібін өзгерту мәселелерін пысықтау;

Ақпарат және қоғамдық даму министрлігіне Ішкі істер министрлігімен, Қаржылық мониторинг агенттігімен және жергілікті атқарушы органдармен бірлесіп халық арасында алаяқтықтың әртүрлі тәсілдері туралы, оның ішінде әлеуметтік желілерде интернет-алаяқтықтың схемалары туралы алдын алу ақпаратын орналастыру арқылы ақпараттық түсіндіру жұмысын жалғастыру ұсынылған.

Бас прокуратураға мүдделі мемлекеттік органдармен бірлесіп, алаяқтықтың жаңа нысандарын ашу және тергеу тәсілдерін тұжырымдамалық түрде қайта қарасын, соның ішінде шет елдердің (РФ, Германия) тәжірибесін ескере отырып, Қылмыстық кодекстің 190-бабынан кредит беру, банк қызметі, 3 интернет-алаяқтық саласында жауаптылықты көздейтін дербес құрамдарды уәкілетті органдардың құзыретін негізге ала отырып, олардың нақты тергеулігін айқындай отырып шығарудың орындылығын қарастыру тапсырылған.

Үйлестіру кеңесінің шешімінің ҚР Бас прокуратурасына берілген тапсырмасы бойынша шет мемлекеттердің ақпарттық жүйеде орын алатын жымқыруды реттейтін құқықтық нормаларын талдап көрейік.

Францияның Қылмыстық кодексінде компьютерлік қылмыстар үшін жауапкершілік көздейтін нормалар "Мүліктік қылмыстар және құқықбұзушылытар " атты үшінші кітабының ішінде «Автоматтандырылған деректерді өңдеу жүйелеріне қол сұғу туралы" тарау орналастырылған, бұның нормалары оны заңсыз қолданған үшін жауапкершілікті көздейді. Ол қылмыстық-құқықтық қорғауға жеке деректер, сондай-ақ телекоммуникациялық жүйелер жататынын көрсетеді. Ақпарттық жүйеде орын алатын жымқыру туралы арнайы нормалар жоқ.

Англо-саксондық құқықтық жүйе заңнаманы кодификациялауды көздемейді, осыған байланысты Ұлыбританияда заң компьютерлік қылмыстар туралы әртүрлі статуттарда айтылған: Компьютерді заңсыз пайдалану туралы заң, Телекоммуникациялар туралы заң (алдау), Электрондық хабарлама туралы заң, сондай-ақ Жеке деректерді қорғау туралы заң, Телевизиялық лицензиялар туралы, Әлеуметтік қамтамасыздандыру саласындағы алдауға қарсы күрес туралы. Алайда, аталған ережелердің ешқайсысы тікелей ақпараттық жүйедегі жымқыру үшін жауапкершілікті қарастырмайды. Басқаша айтқанда, компьютерлік ақпарат кейбір жағдайларда ол қылмыстың объектісі ретінде, кейбіреуінде – қылмыстың заты, ал кейде қылмыс жасаудың құралы, тәсілі болып келеді.

1986 жылы АҚШ-та "Алаяқтық және компьютерлермен байланысты теріс пайдалану туралы" Заң қабылданды. Осы Заңның 18-бөлім 47-тарау 1030-параграфында компьютерге кіру арқылы алаяқтық жасағаны үшін жауапкершілік қарастырылған. Осы нормада алаяқтық ниетте компьютерге кіру, компьютерді алаяқтық іс-әрекеттер жасау арқылы құнды мүлік алу үшін пайдалану, бір жыл ішінде құны 5 мың доллардан асатын компьютерлік уақытты, яғни компьютерлік желіні және сервисті заңсыз пайдалану үшін жауапкершілік белгіленген. Осылайша АҚШ-та Компьютерлік алаяқтық дәстүрлі алаяқтықтан бөлінген, аталған нормалардың мәні - компьютерге кіруде және компьютерді пайдалануда.

Германия Федеративтік Республикасының Қылмыстық кодексінде 263а параграфында компьютерлік алаяқтық жеке бөлінген. Қылмыс жасау мақсатында өзіне немесе үшінші тұлғаға басқаның мүлкіне зиян келтіру арқылы құқыққа қарсы мүліктік пайда алу компьютерлік деректерді өңдеу нәтижесіне дұрыс емес бағдарламаларды құрастыру, дұрыс емес немесе толық емес деректерді қолдану, рұқсатсыз қолдану немесе өзге де деректерді заңсыз өңдеу үшін жауапкершілік белгіленген. Бұл жағдайда компьютерлік ақпарат жымқыру тәсілі.

Түркия Қылмыстық кодексінде компьютерлік алаяқтық қарастырылмаған, алайда 504-баптың 3-тармағында қылмыс құралы ретінде пошта, телеграф, телефон байланыс мекемелерінің құралдарын пайдалану арқылы алаяқтық жасағаны үшін жауапкершілік белгіленген.

Шет мемлекеттердің заңнамаларын талдай келе, бірқатар елдер (Ұлыбритания, Франция) киберкеңістіктегі жымқыруларға қатысты қылмыстың құрамдас бөлігі ретінде көрсетіп, жалпы мүлікке қатысты нормаларды қолданады, ал кейбір елдер (АҚШ, ГФР) компьютерлік ақпартты қолдану арқылы жасалған жымқыруларды бөлек қылмыс құрамы ретінде бөлген, тағы басқаларында (Турция) ол тек саралау белгісі ретінде бекітілген. Шет мемлекеттердің заңнамаларындағы бұндай айырмашылықтары тек құқықтық техниканың ерекшелігімен ғана байланысты емес, осы саланы құқықтық реттеудің жоғары динамикасына, ақпарттық технологиялардың әрдайым жылдам өзгерістерге ұшырауына және оларды құқыққа қайшы пайдаланудың жаңа тәсілдерінің пайда болуына байланысты. Осыны ескере отырып, тауар сату және қызмет көрсету саласындағы ақпараттық желіні қолданушыға қатысты орын алатын алаяқтыққа қарсы іс-қимылда басым бағыттар ретінде заң нормаларын өзгерту емес, ақпараттық технологиялардың мүмкіндіктерін белсенді пайдалану қажет деп есептеймін.

Алаяқтықтың бұл түрін ескертуде қылмыстардың виктимологиялық алдын-алу шаралары ерекше рөл атқарады, өйткені осы қылмыс құрбандарының виктимизациялау процесінде қылмысты жасағанға дейінгі және жасау кезіндегі мінез-құлқы қылмыстың құрамдас бөлігі болып табылады. Сондықтан, осы саладағы алаяқтықтың алдын-алудың тиімділігін арттырудың қажетті шаралардың бірі, қылмыстың осы түрінің ықтимал құрбандарына бағытталған, виктимологиялық алдын-алу шаралары.

Виктимизация қылмыс құрбанының тікелей іс-әрекетін білдіреді, бұл іс-әрекеттер арқылы алаяқ құрбанның мүлкін өз иелігіне алу мақсатына жетеді, одан кейін өз меншігіне айналдырады. Мұндай жағдайларда өзін виктимді ұстағандықтан алаяқтықтың құрбанына ұшырағалы тұрған адамға төніп тұрған қауіп-қатерді, виктимизациядан құтылу мақсатында түсіндіру қажет. Виктимизацияның алдын алу өзіндік мақсат емес, қылмыстың алдын алу шараларының криминологиялық құралы болып табылады. Қылмыстың виктимологиялық факторларын және жәбірленушінің жеке басын ескере отырып, алаяқтыққа қарсы іс-қимылды осы қылмысты терең зерттеуден бастау қажет. Бұл алдын алу шарасының мақсаты ақпараттық жүйені қолданушыға қатысты жасалатын алаяқтықтың жасалуына әсер ететін виктимологяилық факторларға әсер ету болып табылады.

Виктимологиялық профилактика бірнеше аспектілерден тұрады. Ұйымдастырушылық тұрғыдан алғанда, виктимологиялық профилактика құқық қорғау органдары қызметкерлерін арнайы даярлықтан өткізумен ерекшеленеді. Кәсіби білім мен практикалық білімнің жеткіліксіздігі олардың алдын алу іс-шараларын уақтылы жүзеге асыруына мүмкіндік бермейді. Бұл қазіргі уақытта интернет желісінде ақпараттық жүйені қолданушыға қатысты орын алатын қылмыстардың виктимологиялық алдын алу шараларын ұйымдастыру және тактикасы туралы арнайы әдістемелік ұсынымдардың,

осындай қылмыстардың құрбандарымен жұмыс істеудің нақты әдістерінің жоқытығымен байланысты.

Ақпараттық жүйені қолданушыға қатысты жасалған қылмыстардың виктимологиялық алдын-алу шараларын ақпараттық қамтамасыз етуді жетілдіру қажет. Құқық қорғау органдарының бұқаралық ақпарат құралдарымен бірлескен жұмысы виктимологиялық профилактиканың сәттілігінің кепілі болып табылады. Интернеттегі алаяқтықтардың виктимологиялық профилактикасын жүзеге асыру субъектілеріне мемлекет құқық қорғау органдары, сондай-ақ қоғамдық құрылымдар және басқа да мемлекеттік емес құрылымдар жатады. Қылмыстың осы түрінің виктимологиялық алдын-алу шаралары, виктимдіктің әртүрлі нәтижелерінің заңдылығы болып табылатын, мінез-құлықтың әртүрлі түрлерін қамтиды: ұқыпсыздық, адамдардың асқан қызақойлығы, пайдаланушының немқұрайлылығы, қарапайым қорғану шараларын білмеуі, жас және зияткерлік ерекшеліктері және т. б. Виктимологиялық қорғау реттеу механизмі ретінде тек құқық нормалары ғана емес, сонымен қатар мораль, этикалық мінез-құлық ережелері болып табылады. Жалпы виктимологиялық алдын-алу шаралары кең ауқымды әлеуметтік алдын алуға бағытталуы, әлеуметтік қауіпті құбылыс ретінде интернет желсінідегі алаяқтықты азайту мақсатында жүргізілуі тиіс.

Ақпараттық-телекоммуникациялық желілерде алаяқтық схемаларын белсенді пайдаланудың факторларының бірі жаһандық интернет желісіндегі іскерлік қатынастарды құқықтық реттеудің жеткіліксіздігі, оның ішінде азаматтық заңнама бойынша мәміленің электрондық нысаны, электрондық төлем құралдарын пайдалану арқылы жүргізілетін қызметтер, интернет-аукциондар өткізу, қашықтықтан саудаға қатысу мәселелері.

Қатысушылардың құқықтық мәртебесінің белгісіздігі жағдайында электрондық саудаға қатысушы пайдаланушыларға арналған бірқатар алдын-алу шараларын ұсынудың мәні бар:

1. Сырттай бағалау. Бұл жағдайда интернет-сатып алушыларға келесі ұсынымдар беруге болады: интернет-дүкеннің безендірілуіне ерекше назар аудару қажет, демек ең алдымен сайттың дизайнына көңіл аударыңыз. Сенімді пікір ретінде сол сайттың өзінде орналастырылған пайдаланушылардың пікірлерін қабылдауға болмайды. Бұл жағдайда сенімді пікірлерді басқа сайттардан іздеу абзал. Баннер жарнамасы веб-парақшаның қанша бөлігін алатынына назар аудару керек. Оң пікірлерді бірде-бір жарнама алаңы жоқ сайттар немесе еншілес ұйымдарының жарнамасы бар, немесе, керісінше, Бас кеңсе жарнамалайтын кәсіпорындар сайттары алады. Жарнаманың болмауы – пайдаланушыға қосымша ыңғайлылық. Жарнаманың болуы дүкен тауарларды сатудан емес, жарнамадан пайда табатынын білдіреді.

2. Баға саясаты. Тауардың бағасы нарықтық жағдаймен анықталады және орташа деңгейден күрт төмен болуы мүмкін емес екенін пайдаланушылар түсінуі керек. Интернетте өнімді іздеуге мүмкіндік беретін

қызметтер жеткілікті. Олар көптеген ұсыныстардың ішінен тауардың орташа құнын анықтауға көмектеседі.

3. Шарттар мен құқықтар. Жаңа интернет-дүкенге кіргенде, сайттың келесі бөлімдеріне ерекше назар аудару керек: "Дүкен туралы", "төлем туралы" және " жеткізу туралы". Заңды түрде әрекет ететін интернет-дүкендер әрқашан өздері туралы толық ақпаратты орналастырады: заңды тұлғаның мекенжайын, телефонын, деректемелерін және есеп айырысу шотын көрсетеді. Мұндай дүкендер әдетте "тауарды жеткізген соң төлеу" жүйесі бойынша жұмыс істейді. Көптеген жағдайларда алаяқтар электрондық төлем жүйелерін қолдана отырып, жеткізілім үшін алдын-ала төлем жасауды сұрайды. Ақпараттың болмауы, тауарды алудың күрделі жүйесі, алдын-ала төлем жасау туралы ұсыныс – бұл белгілер алаяқтық схемасы.

Фишингке қарсы тұру үшін бүгінде ақпаратты қорғау бағдарламалық және техникалық құралдарды жетілдірудің әртүрлі әдістері қолданылады: бір жағынан, пошта қызметтерінің фишингке қарсы және спамға қарсы сүзгілерді үнемі жаңартып отыруы, екіншіден қолданушылардың құпия ақпаратпен алмасу жәнге оны сақтау үшін жеткілікті қорғалған пошта қызметтерін және жәшіктерін пайдалану.

Виктимологиялық профилактика мақсатында пайдаланушыларға ең қолайлы, қорғалған, ықтимал қауіп туралы дереу ескертетін және дұрыс бейімделген веб-браузерді пайдалануға кеңес беру қажет. Бұл тек браузерлерге ғана емес, сонымен қатар басқа бағдарламаларға да қатысты, мысалы WebMoney электрондық әмияндары сияқты. Сонымен қатар, осы бағдарламалық жасақтаманың көптеген өндірушілерінің антивирустық пакеттері пайдаланушыларды фишингтен қорғайтын модульдермен толықтырылды.

Тәжірибе көрсеткендей, негізгі проблема пайдаланушылардың өздері жеке ақпаратты қорғау мәселелесіне немқұрайлылықпен қарайтынына байланысты. Сондықтан Интернет желісіндегі алаяқтықтың алдын алу бойынша халық арасында ақпараттық-ағарту қызметі құқық қорғау органдарының маңызды міндеті болып табылады. Сонымен бірге, қылмыскерлер қолданатын алаяқтық схемалардын халыққа нақты сипаттап жеткізудің қажеті жоқ, өйткені бұл схемалар жылдам өзегерді, ақпарттық жүйені қолданушыларды алдаудың жаңа тәсілдері үнемі және тұрақты түрде пайда болуда. Сондықтан халықты алаяқтықтың жаңа тәсілдері туралы хабардар ету керісінше әсер етуі мүмкін: халықтың ең зардап шегуге бейім топтары (қарт адамдар, сенгіш және ұқыпсыз пайдаланушылар және т. б.) мұндай ақпарат қызықтырмауы мүмкін, ал қылмыскерлер өздерінің "әріптестерінің" жаңа идеяларын игеруі ықтимал.

Құқық қорғау органдары қызметкерлерінің негізгі мақсаты, ең алдымен, азаматтарға қандай іс-ірекеттерді жасамау абзал екені сияқты қарапайым қауіпсіздік ережелерін жеткізуден тұруы керек:

- тегін қызметтерді, түрлі жүлделерді немесе елеулі жеңілдіктерді уәде ететін Интернеттегі жарнамалық сілтемелер бойынша өту;

- белгісіз адресаттардан хат-хабарларды қарау;

- әлеуметтік желілерде алаяқтар болуы мүмкін бейтаныс пайдаланушылармен қарым-қатынас жасау;

- SIM-карталарды қолдан сатып алу немесе төлқұжат деректерін күмәнді кеңселерге қалдыру;

- қиындыққа тап болған туыстарымен, таныстарымен проблемаларды шешуде делдалдық қызметтер ұсынатын адамдарға ақша аударымдарын жөнелту;

- жеке ақпараттың әлеуметтік желісінің профиліндегі көрсету, оның ішінде сіздің өмір салтыңыз, жоспарланған кетулер және т. б.;

Осылайша, жоғары технологияларды пайдалана отырып жасалатын қылмыстардың виктимологиялық алдын алу шаралары қоғамның әртүрлі топтарының виктимизациясын ескере отырып ұйымдастырылуы тиіс; осы қызмет түрін қамтамасыз етудің әртүрлі аспектілерін ескеруі; ақпараттық – коммуникациялық кеңістікте сақтық шараларын ұстану қажеттілігін ұғынуға бағытталуы тиіс. Интернет желісіндегі алаяқтықтың алдын алу шаралары жүйелі түрде болу керек, соның ішінде ерекше бір орын виктимологиялық аспектіге арналуы қажет.

ҚОРЫТЫНДЫ

Тауар сату және қызмет көресту саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықтың криминалистикалық сиппатамасын қысқаша түйіндеуге болады. Қылмыстың бұл түрін жасау жолдары заманға байланысты өзгеріп отырады. Демек, нақты жасалу жолдарын анықтап алу мүмкін емес, әлеуметтік-экономикалық жағдайға байланысты жаңарып отырады.

Ал аталған қылмыс түрін тергеудің ерекшелігі – «электронды іздердің» қалдырылуында. Олардың құрылу, өңделу және сақталу жолдарының күнделікті жаңаруына байланысты құқық қорғау органдарының «электронды іздермен» жұмысының бірге аяқ алып жүруі маңызды.

Алаяқтықтың аяқталу орны болып жәбірленушілердің ақша аударған орны болып табылады, өйткені дәл осы жерде ол зардап шеккен болып тұр. Осыған байланысты, алаяқтықтың аяқталу орны деп жәбірленуші қылмыскерге ақша аударған жерді айтуға болады. Бұл орында сотқа дейінгі тергеу басталып, қылмыстық іс тергелуі қажет.

Тауар сату және қызмет көресту саласындағы интернет арқылы жасалатын алаяқтық тәуліктің кез-келген уақытында орын алуы мүмкін,сондықтан қылмыс орнын анықтау туралы мәселелер бар.

Зерттеу аясында зерделенген қылмыстық істердің ішінен интернет-қылмыскерлердің көп жағдайда тұрақты жұмыс орны және жоғары білімі жоқ екеніндігін атап өткім келеді. Олардың орта жасы 35 жас және басым көпшілгі 18-25 жас аралығында. Тұрақты табыс көзінің болмауы, бұл Интернет желісінде жасалатын қылмыстардың себебі болып табылады.

Қылмыс құрбанының да жас мөлшері 35, бірақ әлеуметтік дәрежесі рөл атқармайды. Оның себебі тауар сату және қызмет көресту саласындағы интернет арқылы жасалатын алаяқтықтың жолы «балық аулау» іспеттес болып келгендіктен, «қармаққа» әртүрлі тұлғалар түседі.

Тауар сату және қызмет көресту саласындағы интернет арқылы ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықты тергеудің шет мемлекеттер тәжірибесіне келетін болсақ, Компьютерлік қылмыстар туралы конвенцияны (Будапешт, 2001 жылғы 23 қараша) Қазақстан Республикасы келіспейтін бабын ескерту арқылы ратификациялау мүмкіндігін қарастыру қажет. Ол Ковенцияның «24-7 contact points» желісін қолдану бұл қылмыс түрін ашуға біраз көмектесетіні анық. Бір сөзбен айтқанда мемлекетіміздің шекарасынан «шығып» кететін қылмыс болғандықтан, қылмыстық қудалау органдарының қызметкерлері де ағылшын тілін, ақпараттық технологияларды, қылмыстық процесті меңгеруі шарт.

Белорусь ұсынғандай ұлттық деңгейде даркнеттегі қылмыстық әрекеттің әдіс-тәсілдерін анықтау мен қылмысты жасаудағы құралдарға қатысты ақпарат алмасуды ұйымдастыру қажет.

Қытай Халық Республикасының айтқанындай қазірдің өзінде киберқылмысқа қарсы күрестегі сала бойынша аймақтық конвенциялар бар, олар Еуропалық Кеңес, Шанхай ынтымақтастық ұйымы, Араб мемлекеттерінің лигасы және Африка одағы. Мүше мемлекеттердің қолдану аясы мен осы конвенциялардың мазмұнындағы айырмашылықтарға байланысты халықаралық киберқылмысқа қарсы іс-қимыл туралы заңнама бөлшектенген сипатта көрсетілген. Осыған байланысты шұғыл түрде киберқылмыспен күресу үшін жаһандық заңнамалық базаны құру және күн өткен сайын өршіп бара жатқан қылмыстық жағдаймен, әсіресе «бұлтты есептеулер», жасанды интеллект, заттар интернеті, криптовалюта сияқты жаңа технологиялардың пайда болуынан туындайтын жаңа қатерлермен бірлесіп күресу қажет дегенді қолдаймын. Қытай барлық мемлекеттер келіссөздер жүргізіп, БҰҰ-ның қамқорлығымен және қолданыстағы аймақтық конвенциялардың тәжірибесіне сүйене отырып, барлық елдер үшін ашық киберқылмыс туралы бүкіләлемдік конвенцияны әзірлеуі керектігі туралы көзқарасы өте көңілге қонымды және қажет.

Ал шетелден алынатын деректерге келетін болсақ, бұл процесстің жүргізілу тәртібі тергеуді әуре-сарсаңға салатындығын айтуға болады. Қазақстан Республикасының киберқылмысқа қарсы іс-қимыл туралы шетелдермен ақпараттық-коммуникациялық технологиялар саласында арнайы жетекші келісімі жоқ. Қазақстанда қылмыстық істер бойынша құқықтық көмек көрсету туралы сұрау салуда жалпылама әмбебап, жалпықылмыстық аумақтық және секторлы халықаралық құралдар қолданылады. Ол дегеніміз, мысалы, Қазақстан Республикасының облыстарының бір қаласындағы тергеуші ол қалада орын алған алаяқтық бойынша шетел провайдерінен деректер алу үшін алдымен тергеу судьясынан санкция алады, сосын оны құқықтық көмек көрсету туралы сұрау салуға қоса беріп, қалалық прокуратураға жолдайды, әрі қарай қалалық прокуратура облыстық прокуратураға жолдайды, ал облыстық прокуратура Бас прокуратураға жолдайды. Бас прокуратурада ол сұрау салу келісілсе, шетелдің уәкілетті органына халықаралық келісім шарттың негізінде немесе өзара түсіністік қағидатына негізделе отырып жолданады.

Бұл ретте ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтықты тергеуді жеңілдету үшін шетел уәкілетті органдарымен және провайдерлермен ынтымақтастық орнату үшін электронды құжаталмасуды пайдаланып, жаңа жеңіл жолын құрастыру және тиісті халықаралық нормативті құқықтық актілерді ратификациялауға шаралар қабылдау қажет.

Аталған қылмыс түрін тергеудегі ең жиі жүргізілетін тергеу әрекеті – абоненттер арасындағы ұялы байланыс абоненттерінің кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтірі алуды жүргізудің өзі Қазақстан Республикасының аумағында болса да, Нұр-Сұлтан қаласының аумағында ғана жүргізіледі. Бұл жағдай тергеудің кешеуіне әкеп соғады. Сондықтан мемлекетіміздің әр облыс орталығында ұялы-байланыс операторларының кеңсесінен абоненттер арасындағы ұялы байланыс

абоненттерінің кіріс және шығыс қосылулары туралы егжей-тегжейлі мәліметтірі алуды жүргізудің мүмкіндігін ұйымдастыру қажет.

Тауар сату және қызмет көрсету саласындағы ақпараттық желіні қолданушыға қатысты орын алатын алаяқтыққа қарсы іс-қимылда басым бағыттар ретінде заң нормаларын өзгерту емес, ақпараттық технологиялардың мүмкіндіктерін белсенді пайдалану қажет деп есептеймін.

Электрондық іздерді және ауқымды деректерді (Big data) пайдалану арқылы қылмыстарды тергеу жөнінде жұмыс істеу технологияларын зерделеу бүгінгі күннің шындығы екенін ескере отырып, криминалистиканы одан әрі дамыту және оны іс жүзінде қолдану үшін жаңа мүмкіндіктерді ашуға назар аударғанымыз жөн. Сондықтан қазіргі уақытта аталған мәселеге арналған тұрақты мақсатты зерттеулер, конференциялар, дөңгелек үстелдер және басқа да ғылыми іс-шаралар өткізу өзекті болып отыр.

Ауқымды электронды деректерді ақпараттық технологияларды пайдаланбай талдау өте қиын немесе көп уақытты қажет ететінін, кейбір жағдайда мүмкін емес екенін түсіну керек.Тәжірибе көрсеткендей бір ұялы телефонды, компьютерді, гаджетті, банк картасын және т.б. қолдану арқылы бірнеше алаяқтық жасалады. Ол телефон нөмірі бойынша телефонның IMEI кодын анықтау, ал әрі қарай осы код бойынша телефонға бұған дейін немесе кейін кандай абоненттік нөмірлер орнатылғанын анықтау. Демек қылмыстың субъектісіне қатысты «жаңа» эпизодтарды анықтау мүмкіндігі пайда болады. Осылайша банк карталарымен, электронды әмияндармен (жиі Каспий голд және киви әмиян) және IP мекенжайлармен жасауға болады.

Атап айтқанда, алаяқты анықтағаннан кейін, қылмыстың санаты өзгереді, осы фактілерді ҚР ҚК 190-бабының 3-тармағы 3), 4) тармақшаларымен ауыр қылмыс ретінде (екі немесе одан да көп адамға қатысты, бірнеше рет жасалған алаяқтық) саралау мүмкіндігі пайда болады.

Қылмыстық қудалау органдары алдымен ауыр және аса ауыр қылмыстарды ашуды мақсат етеді. Ақпарттық-технологиялар жетістігін қолдану бірнеше орташа ауырлық санатындағы алаяқтықты біріктіріп, ауыр санатқа қайта дәрежелеуге мүмкіндік беретіндіктен, оның жедел жағдайды оңалтуға ықпал ететіні анық. Сондай-ақ Қылмыстық кодекс бабының санкциясы қатаңырақ болып келетіндігі алаяқтардың менмендігін бәсеңдетеді, бұнымен қоса қылмыстың бұл түрін ашу пайызын ұлғайтса құқық қорғау органдарының қызметіне азаматтардың сенімі артатыны да белгілі.

Бүгінгі күні қоғам өмірінің барлық салаларында, соның ішінде адамдардың қылмыс жасау және оларды жасыру, қылмыстарды тергеу мен ашуға кедергі жасауда технологиялар, ақпараттандыру жаппай қолданылады, сондықтан электронды дәлелдер қылмыстық іс бойынша өте маңызды болып табылады.

Дәлелдемелерді сақтау камерасына ұқсас электронды дәлелдемелерді сақтауға арналған сертификатталған компьютерлерді жабдықтау, деректерді сотқа олардың тұтастығы мен өзгермей жолдануын қамтамасыз ететіні анық.

Тауар сату және қызмет көрсету саласындағы интернетте ақпараттық жүйені қолданушыға қатысты орын алатын алаяқтық фактілері туралы қылмыстық істер бойынша тергеу және басқа да процесстік әрекеттерін жүргізудің белгілі бір ерекшеліктері бар, олар қылмыстық әрекеттің механизмімен, сондай-ақ оны жасаған субъектілерге байланысты толық белгіленген. Тергеу әрекетінің оң нәтижесі мен мақсатына жету үшін тергеуші әр түрлі тактикалық әдістерді және мамандардың көмегін қолдана отырып, оны жүргізуге мұқият дайындалуы қажет.

Тауар сату және қызмет көрсету саласындағы ақпараттардың жүйені қолданушыға катысты орын алған алаяқтық жасауға ықпал еткен себептерін және жағдайларын тану жалпы алдын алу шараларының бастапқы сатысында жүзеге асырылады. Бұл себептер мен жағдайларды криминогендік, әлеуметтік, құқықтық, кадрлық, ұйымдастырушылық-техникалық деп жіктеуге болады.

Қылмыстың детерминанттарын анықтаған соң оларды жою үшін тиімді шаралар қолданылуы керек. Мұндай шараларды ішкі істер басқармасы қызметкерлері, сондай-ақ құқық бұзушылықтардың себептері мен оларды жасауға ықпал етуі мүмкін жағдайларды жоюға көмектесуге міндетті тиісті мемлекеттік және қоғамдық құрылымдар жүзеге асыра алады.

Құқық бұзушылықтарды тудыратын себептердің үлкен бөлігі және олардың жасалуына қолайлы жағдайлар әртүрлі салада, меншіктің әр түрлі нысандарымен байланысты кездеседі, сондықтан оларды жоюмен тек жедел қызметкерлер айналысу қиынға соғады.

Осылайша, жоғары технологияларды пайдалана отырып жасалатын қылмыстардың виктимологиялық алдын алу шаралары қоғамның әртүрлі топтарының виктимизациясын ескере отырып ұйымдастырылуы тиіс; осы қызмет түрін қамтамасыз етудің әртүрлі аспектілерін ескеруі; ақпараттық – коммуникациялық кеңістікте сақтық шараларын ұстану қажеттілігін ұғынуға бағытталуы тиіс. Интернет желісіндегі алаяқтықтың алдын алу шаралары жүйелі түрде болу керек, соның ішінде ерекше бір орын виктимологиялық аспектіге арналуы қажет.

ПАЙДАЛАНЫЛҒАН ДЕРЕККӨЗДЕРДІҢ ТІЗІМІ:

1. ҚР БП Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің 1-м есебі.
2. С.Я. Казанцев және басқалар. Информатика и математика для юристов. ЮНИТИ - ДАНА, 2010 жыл. 439 – 450 беттер.
3. У.С. Зинина. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Автореферат. 2011 жыл. 32 – 34 беттер.
4. Н.К. Коровин.Криминалистика. Оқу құралы. Новосибирск: НГТУ, 2014 жыл. 308 бет.
5. В.Е. Корноухов. Методика расследования преступлений: теоретические основы: книга, Москва, Норма 2010 жал. 138 бет.
6. Е.І.Қайыржанов, А.О. Шакенов. Жекелеген қылмыс түрлерін тергеу ерекшеліктері. Оқу құралы – Алматы, «Ес.ҚЫДЫР», 2007ж. - 8 б.
7. Р.С. Белкин. Криминалистическая энциклопедия. 2-баспа Москва, Мегатрон XXI, 2000 жыл. 115 бет.
8. И.Н. Воробец. Глобальная сеть Интернет, как пространство для совершения преступлений. Халықаралық ғылыми тәжірибелік конференцияға баяндама. Москва. МЭЙЛЕР, 2012 жыл. 71 бет.
9. К.В. Астафьев. Виктимологический аспект мошенничества уголовно-правовое и криминологическое исследование. Автореферат. Казань, 2007 жыл.
10. В. Федоренко. Виктимологический аспект преступлений в сети Интернет. «Zakon.ru». URL: https://zakon.ru/blog/2012/01/19/viktimologicheskij_aspekt_prestuplenij_v_seti_internet (өтінім берілген күн 22.04.2021 жыл).
11. А. Горовой. Расследование технологий обмана. http://pda.ormvd.ru/pubs/101/the-investigation-techniques-of-deception/ (өтінім берілген күн 22.04.2021 жыл)
12. The Budapest Convention on Cybercrime: benefits and impact in practice Strasbourg, 13 July 2020 T-CY(2020)16.
13. А.А. Жмыхов. Компьютерная преступность за рубежом и ее предупреждение. Диссертация, Москва, 2003 жыл. 178 бет.
14. М.К.Каминский, А.М.Каминский. Криминалистика, дәрістер курсы, Ижевск, Jusest, 2012 жыл. 358 бет.
15. Р.М. Акутаев. Криминологический анализ латентной преступности. Диссертация, Санкт- Петербург, 1999 жыл, 62-67 беттер.
16. Латентная преступность: познание, политика, стратегия. Сборник материалов международного семинара. Москва, 1993 жыл. 32 бет.
17. У.А. Ерекеш, Р.С. Дюсетаев, А.С. Оразалы, «Некоторые особенности проведения оперативно-розыскных мероприятий и следственных действий по

уголовным правонарушениям, совершаемым с использованием информационных технологий», Типовые методические рекомендации, Астана: МВД, 2016 жыл. 9 бет.
18. Н.К. Имангалиев, Л.А.Темиржанова, А.А. Ешназаров, М.Г. Ажибаев, Р.С. Дюсетаев. Алгоритм расследования киберпреступлений (особоенности составления процессуальных документов): Практическое пособие, Алматы, ТОО «Лантар Трейд», 2019 жыл. 16 бет.
19. В.Ф. Васюков, А.В.Булыжкин. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел, Российский следователь. 2014жыл, N2, 3-бет.
20. А.Л. Осипенко, А.И. Гайдин, Правовое регулирование и тактические особенности изъятия электронных носителей информации, Вестник ВИ МВД России. 2014 жыл. №1. 156-163 беттер.
21. Р.И. Оконенко, Электронные доказательства и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе. Диссертация, Москва, 2016 жыл, 84–117 беттер.
22. Р.Г. Бикмиев, Р.С. Бурганов, Выемка и осмотр электронных устройств, оқу құралы, 2018 жыл, № 1, СПС «КонсультантПлюс» (өтінім берілген күн 22.04.2021 жыл)
23. А.Н. Колычева, «Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет». Диссертация, Москва, 2018 жыл. 40-45 беттер.
24. М.Н. Курьянова, О.Н. Товба, «Проблемы раскрытия и расследования преступлений, связанных с распространением материалов порнографического характера в сети Интернет», Россия IIM Жаршы, 2016 жыл. №3, 123 беттер.
25. О.Ю.Стороженко, «Система технических средств для обеспечения функций оперативно–розыскных мероприятий», Россия IIM Жаршы, 2014 жыл. №3 (25). 70-бет.
26. А. Колосова, Д. Намиот, «Цифровые сертификаты для владельцев мобильных телефонов», International Journal of Open Information Technologies, 2013 жыл. №4. 7 бет.
27. А.В. Головчанский, «Об использовании средств спутниковой навигации в целях установления и фиксации координат места происшествия», Россия IIM Жаршы, 2015 жыл, №2, 64 бет.
28. В.Ю. Кузовлев, «Использование возможностей средств навигации в установлении обстоятельств совершения преступлений», Известия ТулГУ. 2017 жыл, №4–2., 160 бет.
29. А.А. Якимов, «Использование возможностей навигационных спутниковых систем в расследовании преступлений». URL: http://elib.bsu (өтінім берілген күн 22.04.2021 жыл).

30. Federal Rules of Evidence. Вашингтон, 2013 жыл.
31. Forensic Examination of Digital Evidence, A Guide for Law Enforcement. URL: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (өтінім берілген күн 22.04.2021 жыл).
32. П.С. Пастухов, Электронные доказательства в нормативной системе уголовно–процессуальных доказательств, Пермь, жыл сайынғы ғылыми журнал. 2019 жыл, № 1, СПС «КонсультантПлюс» (өтінім берілген күн 22.04.2021 жыл).
33. С.В. Зуева, Основы теории электронных доказательств, монография, Москва, Юрлитинформ, 2019 жыл, 79 бет.
34. В.Н. Григорьев, О.А. Максимов, Об электронных носителях информации в уголовном судопроизводстве, Вестник ННГУ, 2019 жыл, №3. 67 бет.
35. UFED System. Универсальное устройство извлечения судебной информации.
36. https://www.oxygensoftware.ru/ru/company/clients
37. http://kazinfoservice.kz/?product=xry-logical
38. http://barys-systems.kz/products/7/16/
39. https://kapital.kz/gosudarstvo/93994/v-kazakhstane-uchastilis-sluchai-internet-moshennichestva.html
40. А.Л. Осипенко, Перспективы использования информационно-аналитических технологий в оперативно-розыскной деятельности, Общество и право, 2018 жыл, № 4(66).
41. А.А. Бессонов, О некоторых возможностях современной криминалистики в работе с электронными следами, Вестник МГЮА, 2018/3.
42. Қазақстан Республикасы Үкіметінің 2017 жылғы 12 желтоқсандағы №827 қаулысымен бекітілген "Цифрлық Қазақстан" мемлекеттік бағдарламасы.
43. К.К. Демин, А.А.Васильев, Проблемы производства осмотра информационно-телекоммуникационных систем, 50-ші Криминалистикалық оқулардың жинақ материалдары, Москва, Россия ІІМ Басқару академиясы, 2009 жыл, 2-бөлім 444-бет.
44. С.Ю. Скобелин, Использование специальных знаний при работе с электронными следами, Российский следователь, 2014 жыл, №20, 31-33 беттер.
45. К.В. Камчатов және басқалар, Методика борьбы с компьютерными преступлениями, РФ Прокуратурасы, 2020 жыл, 172, 141 беттер.
46. Л.П. Шматкова, Международное сотрудничество в борьбе с киберпреступленями: состояние и перспективы, Молодой ученый, 2016 жыл, №28.
47. Предложение о регламенте европейского парламента и совета о Европейских постановлениях о производстве и сохранении электронных доказательств по уголовным делам, COM/2018/225, 2018/0108 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:225:FIN (өтінім берілген күн 22.04.2021 жыл).

48. А.В. Сизов, Причины и условия совершения преступлений в сфере компьютерной информации, Информационное право, 2015 жыл, №2, 27-29 беттер
49. А.Л. Ситковский, Виктимологическая характеристика и профилактика корыстных преступлений против собственности граждан, РФ ІІМ, Москва, 1998 жыл, 238-бет.