әл-Фараби атындағы Қазақ ұлттық университеті

ӘОЖ 343.98:004(043) Қолжазба құқығында

ӘПСІМЕТ НҰРДӘУЛЕТ МҰХАМЕДИЯРҰЛЫ

Онлайн алаяқтық қылмыстарын сотқа дейінгі тергеу: қазіргі заманғы мәселелер

«8D04203 – Құқықтану»

Философия докторы (PhD) дәрежесін алу үшін
дайындалған диссертация

Отандық ғылыми кеңесші:
заң ғылымдарының кандидаты,
қауымдастырылған профессор
Е.Т. Алимкулов

Шетелдік ғылыми кеңесші:
Философия докторы (PhD),
экономикалық қылмыс саласы
бойынша аға оқытушы
П. Гилмор
(Портсмут қ., Ұлыбритания)

Қазақстан Республикасы
Алматы, 2026

МАЗМҰНЫ

НОРМАТИВТІК СІЛТЕМЕЛЕР..... 3
АНЫҚТАМАЛАР..... 4
БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР..... 5
КІРІСПЕ..... 6

1 ОНЛАЙН АЛАЯҚТЫҚ ҚЫЛМЫСТАРЫН СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІҢ ТЕОРИЯЛЫҚ-ҚҰҚЫҚТЫҚ НЕГІЗДЕРІ.. 16
1.1 Қоғамды цифрландыру жағдайындағы онлайн алаяқтықтың генезисі, ұғымы және құқықтық табиғаты..... 16
1.2 Онлайн алаяқтық қылмыстарын жіктеу және оның сотқа дейінгі тергеп-тексеру контекстіндегі процессуалдық мәні бар сипаттамалары..... 31
1.3 Онлайн алаяқтық пен дәстүрлі алаяқтық түрлерінің салыстырмалы-құқықтық және процессуалдық талдауы..... 43

2 ОНЛАЙН АЛАЯҚТЫҚ ҚЫЛМЫСТАРЫН СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІҢ ҚАЗІРГІ КЕЗЕҢДЕГІ НЕГІЗГІ МӘСЕЛЕЛЕРІ МЕН ЕРЕКШЕЛІКТЕРІ..... 53
2.1 Онлайн алаяқтық қылмыстары бойынша сотқа дейінгі тергеп-тексеруді бастау, тіркеу, бастапқы ақпаратты растау және латенттілік феномені..... 53
2.2 Қылмыстық процестегі цифрлық дәлелдемелерді жинау, бекіту және бағалау ерекшеліктері..... 66
2.3 Онлайн алаяқтық қылмыстарының трансшекаралық сипаты және оның сотқа дейінгі тергеп-тексеру тетігіне әсері..... 79
2.4 Цифрландыру жағдайындағы қылмыстық-процестік реттеудегі олқылықтар мен коллизиялар және құқық қолдану практикасының проблемалары..... 90

3 ОНЛАЙН АЛАЯҚТЫҚ ҚЫЛМЫСТАРЫН СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІ ЖЕТІЛДІРУДІҢ ТҰЖЫРЫМДАМАЛЫҚ БАҒЫТТАРЫ..... 103
3.1 Онлайн алаяқтық қылмыстарын сотқа дейінгі тергеп-тексерудің қылмыстық-процестік тетігін дамыту және тиімді тергеп-тексеру моделін қалыптастыру..... 103
3.2 Онлайн алаяқтық қылмыстарын сотқа дейінгі тергеп-тексеруде халықаралық тәжірибе мен цифрлық технологияларды интеграциялау... 121
3.3 Онлайн алаяқтық қылмыстарына қарсы іс-қимыл саласындағы Қазақстан Республикасының заңнамасын жетілдіру..... 132

ҚОРЫТЫНДЫ..... 149
ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ..... 158
ҚОСЫМША А..... 171

НОРМАТИВТІК СІЛТЕМЕЛЕР

Осы диссертацияда келесі стандарттарға нормативтік сілтемелер пайдаланылды:

1. ГОСТ 7.32-2017 «СИБИД. Ғылыми-зерттеу жұмыстары туралы есеп. Құрылымы және рәсімдеу ережесі» (түзетулермен);

2. ГОСТ 7.88-2003 «Ақпараттар, кітапханалық және баспа ісі бойынша стандарттар жүйесі. Жарияланымдардағы тарау атауларын және тарау атауларындағы сөздерді қысқарту ережелері».

АНЫҚТАМАЛАР

Осы диссертацияда келесі терминдер тиісті анықтамаларымен бірге қолданылды:

Онлайн алаяқтық – цифрлық ортада алдау жолымен жасалатын, қашықтан өзара іс-қимыл жасаумен және ақпараттық-коммуникациялық технологияларды міндетті түрде пайдаланумен сипатталатын, бөтен мүлікті құқыққа сыйымсыз өтеусіз иеленіп алу;

Электрондық (цифрлық) дәлелдемелер – ақпараттық жүйелерде, желілік ресурстарда, электрондық құрылғыларда цифрлық формада қалыптастырылған, сақталатын, өңделетін немесе берілетін, қылмыстық іс үшін мәні бар мән-жайларды белгілеу және тексеру үшін қолданылатын деректер (нәрселер);

Цифрлық артефакт – міндетті машиналық декодтауға жататын жасырын дәлелдемелік ақпараттың микродеңгейлі құрылымдық жеткізгіші (желілік логтар, IP-мекенжайлар, криптографиялық хеш-сомалар);

Цифрлық децепция – тек виртуалды кеңістік құралдарымен, қашықтықтан және жеке байланыссыз іске асырылатын, жәбірленушінің ерік білдіруін немесе ақпараттық жүйе алгоритмдерін когнитивтік бұрмалаудың күрделі тетігі. Сонымен қатар, бұл құбылыс объективті шынайылықты контактілі бұрмалаудан алдаудың қашықтан-виртуалды тетігіне көшуді білдіреді.

Face ID – Бет-әлпетті көлемді сканерлеу технологиясы (биометриялық аутентификация);

VPN (Virtual Private Network) – виртуалды жеке желі, желілік трафикті шифрлауды және анонимизациялауды қамтамасыз ететін технология;

Proxy (Прокси-сервер) – пайдаланушы мен мақсатты сервер арасында делдал қызметін атқаратын аралық сервер (бағдарламалар кешені);

TOR (The Onion Router) – анонимді желілік қосылымды орнатуға мүмкіндік беретін прокси-серверлер жүйесі (пияздық маршрутизация);

MAC-адрес (Media Access Control) – әрбір желілік жабдыққа берілетін бірегей идентификатор;

OSINT (Open-Source Intelligence) – ашық көздер бойынша барлау (жалпыға қолжетімді базалардан ақпарат іздеу және талдау).

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

Осы диссертациялық зерттеуде келесі қысқартулар мен аббревиатуралар қолданылды:

АКТ	–	Ақпараттық-коммуникациялық технологиялар
АҚШ	–	Америка құрама штаты
БҰҰ	–	Біріккен Ұлттар Ұйымы
ЕАЭО	–	Еуразиялық экономикалық одақ
СДТБТ	–	Сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімі
ЖСН	–	Жеке сәйкестендіру нөмірі
ІІМ	–	Ішкі істер министрлігі
МҚҰ	–	Микроқаржы ұйымы
ҚР БП ҚСжАЕК	–	Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитеті
ҚР	–	Қазақстан Республикасы
ҚР ҚК	–	Қазақстан Республикасының Қылмыстық кодексі
ҚР ҚМА	–	Қазақстан Республикасының Қаржылық мониторинг агенттігі
ҚР ҚПК	–	Қазақстан Республикасының Қылмыстық-процестік кодексі
ҚР ЦК	–	Қазақстан Республикасының Цифрлық кодексі
СДТБТ	–	Сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімі
ТМД	–	Тәуелсіз Мемлекеттер Достастығы
ЭЦҚ	–	Электрондық цифрлық қолтаңба

КІРІСПЕ

Жұмыстың жалпы сипаттамасы. Диссертациялық зерттеу жаһандық цифрландыру жағдайындағы онлайн алаяқтықты сотқа дейінгі тергеп-тексеру тетігін кешенді теориялық-құқықтық, криминалистикалық және праксиологиялық талдауға бағытталған. Зерттеу онлайн алаяқтықтың тарихи-құқықтық генезисін, «цифрлық децепция» мен құқық қолданудағы «цифрлық нигилизм» феномендерін, сондай-ақ дәстүрлі және виртуалды жымқыру модельдерінің қылмыстық-процестік ерекшеліктерін қамтиды. Ерекше назар электрондық (цифрлық) дәлелдемелердің гиперқұбылмалылығы мен жеделдетіліп деградациялануына, дәлелдеу процесіндегі когнитивтік кедергілерге, тергеп-тексерудің трансшекаралық (экстерриториялық) сипатына, сондай-ақ үлкен деректерді (Big Data) өңдеу мен предиктивті болжау үшін жасанды интеллект алгоритмдерін қылмыстық сот ісін жүргізуге кіріктіру мәселелеріне бөлінді. Жүргізілген зерттеу нәтижелері бойынша қылмыстық сот ісін жүргізудің инновациялық «артефактіге бағдарланған» моделі негізделді, тергеп-тексерудің 5 деңгейлі интегративті архитектурасы құрастырылды және цифрлық дәлелдемелерді заңдастыру мақсатында Қазақстан Республикасының қылмыстық-процестік заңнамасын жетілдіру бойынша ғылыми негізделген ұсыныстар кешені тұжырымдалды.

Зерттеу тақырыбының өзектілігі. Қоғамды жаһандық цифрландыру және финтех-индустрияның қарқынды дамуы мүліктік қылмыстарды жоғары жылдамдықты виртуалды ортаға көшіріп, олардың терең трансформациялануына әкеп соқты. Проблема ауқымы ұлттық қатер сипатына ие болды: егер 2018 жылы алаяқтықтың жалпы құрылымындағы (ҚР ҚК-нің 190-бабы) [1] интернет-алаяқтықтың үлесі маргиналды 1,8%-ды құраса, 2025 жылдың қорытындысы бойынша ол басым 60,5%-ға жетіп, тіркелген жағдайлардың бес есе сандық өсуімен қатар жүрді. Іс-әрекеттің қоғамдық қауіптілігі оның бұрын-соңды болмаған латенттілігімен (70%-ға дейін) және 6,3%-дан аспайтын материалдық залалды өтеудің өте төмен деңгейімен сындарлы түрде ушыға түседі. Мемлекет пен азаматтардың қаржылық қауіпсіздігіне төніп келе жатқан қатерді Қазақстан Республикасының Президенті Қ.К. Тоқаев ерекше атап өтіп, 2026 жылғы қаңтарда елімізде әрбір бесінші онлайн алаяқтық қана ашылатынын көрсетті [2]. Бұл киберқылмыспен күрес әдістерін түбегейлі қайта қарау, артта қалған тәсілдерден бас тарту және қарсы іс-қимылдың проактивті зияткерлік жүйелеріне көшудің шұғыл қажеттілігін туындатады.

Осы орайда, диссертациялық зерттеудің бағыты мен ұсынылып отырған инновациялық шешімдер Қазақстан Республикасының қазіргі заманғы стратегиялық мемлекеттік тұжырымдамаларымен тікелей үндеседі. Атап айтқанда, Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024–2028 жылдарға арналған тұжырымдамасында [3] интернет-алаяқтыққа қарсы күрес жасалып қойған әрекетке реактивті түрде ден қоюға ғана сайып келетіні ресми түрде мойындалып, ведомствоаралық өзара іс-қимыл алгоритмдерін және стратегиялық шараларды әзірлеудің өткір қажеттілігі

бекітілген. Сонымен қатар, зерттеу аясында ұсынылатын «артефактіге бағдарланған модель» және цифрлық дәлелдемелерді заңдастыру тетіктері 2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасының мақсаттарына, сондай-ақ электрондық ақпараттық ресурстар мен инфрақұрылымды қауіп-қатерлерден қорғауды көздейтін «Қазақстанның киберқалқаны» тұжырымдамасының [4] негізгі қағидаттарына толық сәйкес келеді. Бұл жағдай диссертациялық зерттеу тақырыбының тек ғылыми-теориялық қана емес, сондай-ақ мемлекеттің ұлттық және киберқауіпсіздік мүдделерін қорғау тұрғысынан жоғары практикалық әрі стратегиялық маңыздылығын бұлтартпай дәлелдейді.

Құқықтық проблематика консервативті қылмыстық-процестік заңнаманың гипердинамикалық технологиялық шынайылықтан іргелі артта қалуымен шартталған. Қолданыстағы ҚР ҚПК-де [5] «цифрлық дәлелдеменің» заңдық дефинициясы толығымен жоқ, ал виртуалды іздер физикалық «заттай дәлелдемелердің» (118-бап) немесе дәстүрлі жазбаша «өзге де құжаттардың» (120-бап) архаикалық шеңберіне жасанды түрде сыйғызылады. Негізгі коллизия тергеп-тексеруді бастау сатысында қаланған: ҚР ҚПК-нің 179-бабы азаматтық-құқықтық даудың белгілері болған кезде арыздарды тіркеуге императивті түрде тыйым салады. Цифрлық децепция мақсатты түрде заңды шарттар мен транзакциялар ретінде бүркемеленетіндіктен, бұл құқықтық сүзгі парадоксалды түрде сот төрелігіне қол жеткізуден бас тартуды легитимдейтін институционалдық тосқауылға айналады. Бұдан басқа, халықаралық құқықтық көмектің дәстүрлі бюрократияланған институттары (ҚР ҚПК-нің 559-бабы) ұрланған активтерді шығарудың экстерриториялылығымен және трансшекаралық сипатымен еңсерілмес қақтығысқа түсіп, шетелдік серверлердегі құбылмалы цифрлық іздердің жойылуына әкеп соғады.

Қазіргі заманғы қылмыстық құқық пен процесс доктринасында цифрлық жымқырулардың технологиялық және құқықтық мәнін біріктіруге қабілетті кешенді зерттеулердің тапшылығы байқалады. Ғылымда іс-әрекетті саралауға технологиялық, объектілік және формальды-құқықтық тәсілдерді жақтаушылар арасында өткір пікірталастар жалғасуда. Цифрлық іздердің материалдылығы, виртуалдылығы немесе гибридтілігі тұжырымдамалары арасында теңгерім жасайтын олардың табиғаты туралы бірыңғай түсінік жоқ. Ғылыми өзектілікті парадигмалық ауысудың объективті қажеттілігі күшейтеді: инновациялық артефактіге бағдарланған модельдің (мұнда қылмыскерді деанонимизациялауға әкелетін цифрлық кодтың өзі танымның бастапқы объектісі болып табылады) пайдасына ескірген субъектіге бағдарланған тергеп-тексеру логикасынан (бастапқыда субъект іздестірілген кезде) бас тарту. Сондай-ақ ұсынылған «қос объектілілік» (қаржы ұйымына да, дербес деректер субъектісіне де залал келтіру) тұжырымдамалары және құқық қолданудағы «цифрлық нигилизмді» еңсеру терең теориялық пайымдауды талап етеді.

Тергеу органдары мен соттар құқық қолданудың жүйелі институционалдық салдануымен бетпе-бет келіп отыр. Статистика апатты теңгерімсіздікті көрсетеді: тіркелген ондаған мың кибержымқырулардың тек 10-14%-ы ғана сотқа

жетеді, ал істердің басым көпшілігі (2025 жылы 22 мыңнан астамы) күдіктінің анықталмауы себебінен жаппай тоқтатыла тұрады (ҚР ҚПК-нің 45-бабы 7-бөлігінің 1-тармағы) [6]. Тергеу аппараты деректерді алуға арналған гибридті құзыреттер мен мамандандырылған бағдарламалық-аппараттық кешендердің өткір тапшылығын сезінуде. Дәлелдемелерді сотта бағалау сатысында (ҚР ҚПК-нің 125-бабы) бұлттық және криптографиялық қорғалған деректерге физикалық түрде қолдануға келмейтін оларды алудың және қағазға хаттамалаудың (ҚР ҚПК-нің 199-бабы) архаикалық рәсімдерін қатаң сақтаудың мүмкін еместігіне байланысты соттар цифрлық артефактілерді жаппай жол берілмейтін (ҚР ҚПК-нің 112-бабы) деп тануға мәжбүр. Бұл тергеу әрекеттерін алгоритмдеудің, іздерді шұғыл сақтау регламентін енгізудің және банктердің антифрод-жүйелерін қылмыстық процеске тікелей интеграциялаудың шұғыл практикалық қажеттілігін туындатады.

Диссертациялық зерттеудің мақсаты мен міндеттері. Диссертациялық зерттеудің мақсаты инновациялық артефактіге бағдарланған қылмыстық сот ісін жүргізу моделін құрастыру және Қазақстан Республикасының заңнамасын жетілдіру бойынша ғылыми негізделген ұсыныстар әзірлеу үшін жаһандық цифрландыру жағдайындағы онлайн алаяқтықты сотқа дейінгі тергеп-тексеру тетігін кешенді теориялық-құқықтық, криминалистикалық және праксиологиялық талдау болып табылады.

Қойылған мақсатты іске асыру үшін келесідей логикалық өзара байланысты міндеттер алға қойылды:

– онлайн алаяқтықтың теориялық негіздері мен тарихи-құқықтық генезисін ашу;

– онлайн алаяқтықтың көпфакторлы жіктеу моделін әзірлеу;

– алаяқтықтың дәстүрлі және цифрлық модельдеріне салыстырмалы-құқықтық талдау жүргізу;

– онлайн алаяқтықтың латенттілігі себептерін және институционалдық салдану детерминанттарын анықтау үшін сотқа дейінгі тергеп-тексеруді бастау сатысының нормативтік және құқық қолдану негіздерін талдау;

– гиперқұбылмалы цифрлық дәлелдемелерді тиімді жинауға, процестік бекітуге және бағалауға кедергі келтіретін тұжырымдамалық, рәсімдік және когнитивтік кедергілерді бағалау;

– желілік жымқырулардың трансшекаралық (экстерриториялық) табиғатының ұлттық юрисдикцияға әсерін зерделеу және онлайн алаяқтыққа қарсы іс-қимылдың озық халықаралық тәжірибесін зерттеу;

– қазіргі цифрландыру жағдайында Қазақстан заңнамасын жетілдіру мәселелерін айқындау.

Зерттеу объектісі мен пәні. Диссертациялық зерттеудің объектісі қаржылық және телекоммуникациялық ортаны жаһандық цифрландыру жағдайында онлайн алаяқтықпен байланысты қылмыстық құқық бұзушылықтарды сотқа дейінгі тергеп-тексеру процесінде қылмыстық сот ісін жүргізу саласында қалыптасатын, құқық нормаларымен реттелген қоғамдық қатынастар кешені болып табылады.

Диссертациялық зерттеудің пәні цифрлық дәлелдемелерді және сотқа дейінгі іс жүргізуді реттейтін ҚР қылмыстық, қылмыстық-процестік және сабақтас заңнамасының, сондай-ақ киберқылмысқа қарсы іс-қимыл саласындағы халықаралық-құқықтық актілердің нормалары болып табылады болып табылады.

Диссертациялық жұмыстың әдістемесі. Диссертациялық жұмыстың әдіснамалық негізін онлайн алаяқтық феноменін оның үздіксіз эволюциялық динамикасында және жаһандық цифрландыру процестерімен ажырамас өзара байланыста объективті қарастыруға мүмкіндік беретін ғылыми танымның жалпыға бірдей диалектикалық әдісі құрайды. Теориялық тұжырымдар мен практикалық ұсынымдардың дәйектілігі мен негізділігі жалпы ғылыми және арнайы заңдық әдістер жүйесін кешенді қолданумен қамтамасыз етіледі.

Талдау мен синтездің жалпы ғылыми әдістері, сондай-ақ жүйелі-құрылымдық тәсіл кибержымқырулардың көпфакторлы жіктеу моделін құрастыру және сотқа дейінгі тергеп-тексерудің инновациялық «артефактіге бағдарланған» парадигмасын әзірлеу кезінде қолданылды. Тарихи-құқықтық әдіс виртуалды децепция тетігінің генезисі мен трансформациялану кезеңдерін зерделеу үшін пайдаланылды.

Жұмыста салыстырмалы-құқықтық (компаративистік) әдіс қолданылды, оның көмегімен халықаралық практикаға пәнаралық талдау жүргізілді. Бұл әдіс алаяқтықтың дәстүрлі және цифрлық нысандары арасындағы сапалық айырмашылықтарды анықтады. Сонымен қатар ол романо-германдық және ағылшын-саксондық құқықтық отбасылардың киберқылмыстарды саралауға тұжырымдамалық тәсілдерін салыстыруға мүмкіндік берді. Аталған әдіс арқылы шетелдік технологиялық тергеп-тексеру модельдерінің және мемлекеттік-жекеменшік әріптестік тетіктерінің тиімділігі бағаланып, халықаралық стандарттардың ұлттық юрисдикцияға рецепциясы негізделді.

Формальды-құқықтық (догматикалық) әдіс Қазақстан Республикасының қолданыстағы қылмыстық және қылмыстық-процестік заңнамасының нормаларын түсіндіру, институционалдық коллизияларды (атап айтқанда, тергеп-тексеруді бастау кедергілерін) диагностикалау және нормативтік базаны жаңғырту бойынша нақты ұсыныстар әзірлеу кезінде пайдаланылды. Статистикалық және криминологиялық әдістер арқылы қылмыстылықтың динамикасына объективті баға берілді, эмпирикалық деректер жиынтығы негізінде оның процестік латенттілігінің деңгейі мен өңірлік өзгешелігі айқындалды.

Диссертациялық жұмыстың нормативтік негізі. Жұмыстың нормативтік-құқықтық арқауы Қазақстан Республикасының Конституциясынан, қолданыстағы қылмыстық (ҚР ҚК) және қылмыстық-процестік (ҚР ҚПК) заңнама нормаларынан тұрады. Зерттеу пәнаралық сипатта болғандықтан, сабақтас реттеуші заңнамаға да кең талдау жасалды: атап айтқанда, ҚР Азаматтық кодексі [7], «Жедел-іздестіру қызметі туралы» [8], «Микроқаржылық қызмет туралы» [9], «Төлемдер және төлем жүйелері туралы» [10] және «Қазақстан Республикасындағы цифрлық активтер туралы» [11] заңдары. Ресми түсіндіру актілерінің де орны бөлек, ең алдымен – ҚР Жоғары Сотының 2017

жылғы 29 маусымдағы №6 «Алаяқтық туралы істер бойынша сот практикасы туралы» нормативтік қаулысы [12], сондай-ақ іргелі халықаралық-құқықтық актілер, соның ішінде 2001 жылғы Киберқылмыс туралы Еуропа Кеңесінің конвенциясы [13] және БҰҰ-ның киберқылмысқа қарсы әзірленіп жатқан конвенциясының ережелері [14].

Диссертациялық жұмыстың эмпирикалық негізі. Зерттеудің эмпирикалық базасын отандық құқық қолдану практикасының репрезентативті материалдары мен ресми статистикалық деректер қалыптастырды. Праксиологиялық талдаудың іргетасы ретінде 2020 жылдан 2026 жылға дейінгі кезеңде онлайн алаяқтық туралы қылмыстық істер бойынша (атап айтқанда, ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағы бойынша) Қазақстан Республикасының соттары шығарған 127 сот үкімі массивін жүйелі түрде зерделеу қызмет етті. Жұмыстың статистикалық негізін Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің осы санаттағы қылмыстық істерді тіркеу, тоқтата тұру және сотқа жіберу динамикасы туралы 2018-2026 жылдарға арналған жиынтық есептері (№1-М нысаны) [6], сондай-ақ Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасының ресми талдамалық көрсеткіштері құрады [3].

Тақырыптың ғылыми зерттелу дәрежесі және зерттеудің теориялық негіздері. Киберқылмысқа қарсы іс-қимыл және ақпараттық-коммуникациялық технологиялар саласындағы қылмыстық құқық бұзушылықтарды тергеп-тексеру проблематикасы қазіргі заманғы заң ғылымының жіті назарында тұр және жинақталған доктриналық материалдың едәуір көлемімен сипатталады. Виртуалды жымқыруларды саралау мәселелерін және цифрлық децепция феноменін қоса алғанда, пайдакүнемдік қол сұғушылықтардың цифрлық трансформациялануының қылмыстық-құқықтық және криминологиялық аспектілерін түсінуге О.С. Капинус, Н.А. Лопашенко, Е.А. Русскевич, М.Д. Фролов, К.Н. Евдокимов, А.А. Энгельгардт, А.Г. Безверхов, В.В. Хилюта сияқты көрнекті шетелдік ғалымдар іргелі үлес қосты. Криминалистикалық қамтамасыз ету, процестік дәлелдеу, электрондық жеткізгіштерді алу және цифрлық іздердің түзілуі эволюциясы мәселелері В.А. Мещеряков, Е.Р. Россинская, П.С. Пастухов, С.В. Зуев, Ю.В. Гаврилин, Е.С. Шевченко, В.В. Коломинов, А.Н. Колычева және А.И. Зазулиннің еңбектерінде жан-жақты талданды, ал экстерриториялылық мәселесін А.Г. Волеводз пен А.Л. Осипенко қарастырды.

Дегенмен бұл зерттеулердің ғылыми маңызы қаншалықты жоғары болса да, олардың дені цифрлық ақпаратты дәстүрлі материалдық құрамдардың факультативті элементі деп қана бағалап, тергеп-тексерудің консервативті, классикалық парадигмасына бейілділігін сақтайды. Доктринада гиперқұбылмалы виртуалды артефактілерді олардың физикалық жеткізгіштерінен оқшау түрде процестік бағалау проблемалары тек фрагменттік түрде зерттелген және тұжырымдамалық тұрғыдан шешілмеген күйінде қалып отыр, ал көптеген процестік алгоритмдер трансұлттық бұлттық есептеулер және желілік іздердің автоматтандырылған деградациясы жағдайында үмітсіз ескірген. Дәстүрлі құқықтық сүзгілер қашықтан жасалатын алаяқтықты (оның

ішінде микрокредиттікті) азаматтық-құқықтық дау ретінде қате түсіндіретін қылмыстық процесті бастау сатысындағы институционалдық салдану феномені жүйелі түрде зерделенбеген.

«Цифрлық дәлелдемелерді» заңдастыру бөлігіндегі қолданыстағы доктриналық вакуум және ескірген субъектіге бағдарланған алгоритмдердің абсолютті тиімсіздігі қылмыстық сот ісін жүргізудің жаңа моделіне ғылыми негізделген көшу үшін осы диссертациялық зерттеуді жүргізудің объективті қажеттілігін туындатады.

Диссертацияның теориялық негізін қылмыстық, қылмыстық-процестік құқық, криминалистика, криминология, цифрлық (ақпараттық) құқық ғылымдарының және сот сараптамасы теориясының іргелі ережелері, доктриналық тұжырымдамалары мен тәсілдері кешені құрады. Зерттеудің зияткерлік іргетасы қылмыстылықтың цифрлық трансформациялануының қазіргі заманғы тұжырымдамаларына, виртуалды жымқырулардың көп объектілілік теориясына, ақпараттық қоғамда дәлелдеуді жаңғырту доктриналарына, сондай-ақ цифрлық криминалистиканың виртуалды және гибридті іздер туралы озық ілімдеріне негізделеді.

Мәлімделген проблематиканы ұлттық контексте теориялық пайымдаудың іргелі негізін қазақстандық заң мектебі өкілдерінің еңбектері қалыптастырады. Меншікке қол сұғушылықтарды қылмыстық-құқықтық бағалауға тұжырымдамалық тәсілдер, сондай-ақ қылмыстылықтың базалық криминологиялық параметрлері отандық ғалымдар: Е.И. Қайыржановтың, И.Ш. Борчашвилидің, С.М. Рахметовтың, А.Н. Ағыбаевтың, У.С. Жекебаевтың, Е.О. Алаухановтың, Р.Е. Джансараеваның және Б.Х. Төлеубековаңың классикалық және қазіргі заманғы зерттеулерінде қаланған.

Сонымен қатар, ұлттық қылмыстық саясат шеңберінде компьютерлік қылмысқа қарсы іс-қимыл ерекшелігі, құқықтық қатынастарды цифрландыру және онлайн алаяқтықты саралау мәселелері отандық ғылымның көрнекті қайраткерлері И.И. Роговтың, К.Н. Шакировтың, Т.К. Ерджановтың, Д.В. Татариновтың, сондай-ақ қазіргі заманғы қазақстандық зерттеушілер: Қ. Аратұлының, А.К. Нұрпейісованың, К.О. Қарабековтің, А.Т. Исмағұлованың, М.С. Бисалиевтің, А.А. Агарконың, А.Б. Құрымбаеваның, Б.Б. Қощеғұловтың, С.К. Жетписовтің және Р.Б. Джилкишиевтің жұмыстарында егжей-тегжейлі ашылады.

Өз кезегінде, Қазақстан Республикасындағы дәлелдеу, электрондық қылмыстық сот ісін жүргізу және цифрлық іздерді тіркеп-белгілеу проблемаларын қамтитын зерттеудің процестік-криминалистикалық блогы А.А. Аубакированың еңбектеріне, сондай-ақ Б.М. Нұрғалиевтің, Е.Н. Бегалиевтің, А.Н. Ахпановтың, М.Ч. Когамовтың, Р.Б. Джилкишиевтің, М.С. Бисалиевтің және басқа да бейінді мамандардың озық ізденістеріне сүйенеді. Диссертацияда проблеманы жан-жақты, кешенді талдау үшін Н.А. Лопашенконың, О.С. Капинустың, П.С. Пастуховтың, Е.Р. Россинскаяның, В.А. Мещеряковтың, В.Б. Веховтың және С.В. Зуевтің еңбектерінде ұсынылған шетелдік ғылыми мектептердің тұжырымдамалық идеялары да пайдаланылады.

Диссертациялық зерттеудің ғылыми жаңалығы. Диссертациялық

зерттеудің ғылыми жаңалығы гиперқұбылмалы цифрлық орта мен қылмыстық сот ісін жүргізудің консервативті нысаны арасындағы тұжырымдамалық алшақтықты еңсеруге мүмкіндік берген кибержымқыруларға қарсы іс-қимылдың тұтас теориялық-әдіснамалық және праксиологиялық негізін әзірлеу болып табылады.

Отандық қылмыстық процесс ғылымында алғаш рет ғылыми айналымға «цифрлық децепция» ұғымы енгізілді және онлайн алаяқтық генезисінің үш кезеңдік эволюциялық моделі негізделді. Виртуалды деректерді физикалық жеткізгішке архаикалық байлаудан түпкілікті бас тартуды қамтамасыз ететін «цифрлық дәлелдеменің» дербес дефинициясы алғаш рет ұсынылды. Сотқа дейінгі іс жүргізудің жүйелі салдануын түсіндіретін құқық қолданудағы «цифрлық нигилизм» және «технологиялық ұсталмаушылық» деструктивті феномендері алғаш рет тұжырымдамаланды. Бұдан басқа, материалдық-құқықтық деңгейде МҚҰ бастапқы жәбірленуші ретінде тану қажеттілігін дәлелдейтін микрокредиттік жымқырулардың «аномальді триада» (қос объектілілік) тұжырымдамасы алғаш рет негізделді.

Ескірген субъектіге бағдарланған парадигманың орнына келген және кінәліні дереу дербестендіруден гөрі цифрлық іздерді жедел тіркеп-белгілеудің абсолютті басымдығын белгілейтін сотқа дейінгі тергеп-тексерудің авторлық инновациялық «артефактіге бағдарланған» киберпроцестік моделі ұсынылды. Превентивті, инициациялық, артефактілік, атрибуттық және жолын кесушілік деңгейлерін ажырамас түрде біріктіретін сот ісін жүргізудің авторлық бес деңгейлі интегративті моделі ұсынылды. Процестік күрделілікті бағалау өлшемшартын біріктіре отырып, кибержымқырулардың авторлық көпфакторлы жіктемесі ұсынылды. Жаңа алгоритмдерді іске асыру үшін гиперқұбылмалы іздерді дереу криптографиялық бекітуді және күдіктілерді ұстап алу үшін жаңа негіз енгізуді (ҚР ҚПК-нің 131-бабының 4-бөлігіне толықтыру) талап ететін авторлық шұғыл тактикалық-криминалистикалық «72 сағат» алгоритмі ұсынылды.

Виртуалды іздердің түзілуі бөлігінде криминалистикалық трасологияның ережелері дамытылды: «гибридті іздердің» ерекшелігі бөліп көрсетілді және цифрлық деректердің өмір сүру жылдамдығы мен процестік инерттілік арасындағы асимметрияны түсіндіретін «жеделдетілген деградация» (мүмкіндіктердің тар терезесі) тұжырымдамасы ғылыми негізделді. Проактивті желілік деректер алмасуды және тергеу аппаратын банктік антифрод-жүйелермен өтпелі интеграциялауды қамтамасыз ететін құқықтық конвергенцияның гибридті платформалық моделін негіздеу есебінен ведомствоаралық және халықаралық ынтымақтастық туралы ережелер дамытылды.

Ұсынылған тәсілдермен қашықтан жасалатын жымқыруларды тиімді тергеп-тексеруді бұғаттаған елеулі нормативтік және доктриналық олқылықтың орны толтырылды. Цифрлық ақпарат мәртебесінің терминологиялық белгісіздігі жойылды, арыздарды тіркеу сатысындағы жасанды латенттілік проблемасы шешілді, сондай-ақ трансұлттық киберқылмыс алдында ұлттық тергеудің институционалдық оқшауланuы тұжырымдамалық түрде еңсерілді. Әзірленген инновациялық алгоритмдер жаппай цифрландыру жағдайында киберқылмыспен

күрес әдістерін түбегейлі қайта қарау жөніндегі мемлекеттің стратегиялық міндетіне тікелей жауап береді.

Зерттеудің ғылыми жаңалығы қорғауға ұсынылған келесі тұжырымдармен анықталады:

1. Цифрлық технологияларды енгізу сандық өсуге емес, пайдакүнемдік қол сұғушылықтар тетігіндегі іргелі сапалық ауысуға әкелгені дәлелденді, бұл авторлық үш кезеңдік эволюциялық модельмен (пайда болу, қалыптасу, институционалдану кезеңдері) расталады. Аталған феноменді дәл доктриналық бейнелеу үшін объективті шынайылықты контактілі бұрмалаудан алдаудың қашықтан-виртуалды тетігіне көшуді білдіретін «цифрлық децепция» ұғымы енгізілді;

2. Гибридті криминалдық феномен ретіндегі онлайн алаяқтықтың біріздендірілген ұғымы тұжырымдалды. Тиісті қылмыстық-процестік саралауды қамтамасыз ету мақсатында технологиялық, объектілік, құрылымдық және трасологиялық өлшемшарттарды біріктіретін көпфакторлы жіктеме әзірленді. Жіктеу құрылымына алғаш рет сотқа дейінгі іс жүргізудің тактикалық-ұйымдастырушылық алгоритмдерін таңдауды айқындайтын «тергеп-тексерудің процестік күрделілігі» (төмен, орташа, жоғары) өлшемшарты кіріктірілді;

3. Микрокредиттеу саласындағы онлайн алаяқтық қос объектілілікпен сипатталатыны негізделді: тікелей мүліктік залал қаржы ұйымына, ал қосымша ақпараттық зиян – деректері компрометацияланған жеке тұлғаға келтіріледі. Қаржы институты бастапқы жәбірленуші болып табылатыны дәлелденді, бұл ҚР ҚК-нің 190-бабы 2-бөлігін: «*қаржы ұйымының ақпараттық жүйесіне көрінеу жалған компьютерлік деректерді енгізу арқылы жымқыру*» деген арнайы саралаушы белгімен толықтыруды талап етеді.

Сонымен қатар, ресми соттық түсіндіру деңгейінде кибержымқырулардың сатылылығын регламенттеу қажеттілігі негізделді: құпия аутентификациялық ақпаратты (CVV-кодтарды, SMS-парольдерді) алдау жолымен иеленіп алуды алаяқтыққа оқталу ретінде саралау орынды, бұл туралы ҚР Жоғары Сотының 2017 жылғы 29 маусымдағы №6 нормативтік қаулысын толықтыру ұсынылады;

4. Қаржы институтын бастапқы жәбірленуші ретінде тану тұжырымдамасын процестік тұрғыдан іске асыру мақсатында, дербес деректері заңсыз пайдаланылған жеке тұлғалардың құқықтарын сотқа дейінгі қалпына келтіру тетігі әзірленді. Атап айтқанда, ҚР ҚПК-тің 193-бабы 19-1-бөлігін қосу арқылы келесідей нұсқа ұсынамыз: *«Сотқа дейінгі тергеп-тексеру сатысында қылмыстық іс бойынша несие беруші органды жәбірленуші ретінде тану және несие рәсімделген тұлғалардан несиелік шығындарды алып тастау жөнінде тергеу соттарына өтінішхат келтіреді»*.

ҚР ҚПК-тің 55-бабының 2-бөлігінің 5-1-тармағын қосу арқылы келесідей нұсқа ұсынамыз: *«Прокурордың ұсынуымен қылмыстық іс бойынша несие беруші органды жәбірленуші ретінде тану және несие рәсімделген тұлғалардан несиелік шығындарды алып тастау туралы мәселені қарайды»*;

5. Қылмыстық процестің дәстүрлі субъектіге бағдарланған логикасынан инновациялық артефактіге бағдарланған модельге парадигмалық көшудің объективті қажеттілігі негізделді. Бұл тұжырымдама цифрлық артефактіні

кейінгі деанонимизациялау үшін баламасыз бастапқы дереккөз ретінде қарастыра отырып, кінәлі адамды жедел дербестендіру әрекеттерінен гөрі гиперқұбылмалы цифрлық іздерді дереу криптографиялық тіркеп-белгілеудің абсолютті процестік басымдығын белгілейді;

6. Виртуалды деректерді физикалық жеткізгішке архаикалық процестік байлаудан түпкілікті бас тартуды қамтамасыз ететін «цифрлық дәлелдеменің» авторлық анықтамасы тұжырымдалды. Деректердің өмір сүру жылдамдығы мен тергеудің инерттілігі арасындағы асимметрияны түсіндіретін «цифрлық іздердің жеделдетілген деградациясы» криминалистикалық тұжырымдамасы негізделді, сондай-ақ тергеу органдарының виртуалды артефактілердің технологиялық ерекшелігін жүйелі түрде елемеуі – құқық қолданудағы «цифрлық нигилизм» деструктивті феномені тұжырымдамаланды. Ұсынылған тұжырымдаманы институционалдау мақсатында ҚР ҚПК-не өзгерістер кешені әзірленді:

– ҚР ҚПК-тің 7-бабына 59-тармағын енгізуді:

«*Цифрлық дәлелдемелер – ақпараттық жүйелерде, желілік ресурстарда, электрондық құрылғыларда цифрлық формада қалыптастырылған, сақталатын, өңделетін немесе берілетін, қылмыстық іс үшін мәні бар мән жайларды белгілеу және тексеру үшін қолданылатын деректер (нәрселер)»*.

– ҚР ҚПК-тің 112-бабының 2-бөлігіне келесідей толықтыру енгізуді:

«*Қылмыстық істі дұрыс шешу үшін маңызы бар нақты деректер: күдіктінің, айыпталушының, жәбірленушінің, куәнің, қорғалуға құқығы бар куәнің, сарапшының, маманның айғақтарымен; сарапшының, маманның қорытындысымен; заттай және цифрлық дәлелдемелермен, процестік әрекеттердің хаттамаларымен және өзге де құжаттармен белгіленеді*.

– ҚР ҚПК-тің 118-бабының 1-бөлігіне 6-тармақты енгізуді:

«Ақпараттық жүйелерде, желілік ресурстарда, электрондық құрылғыларда цифрлық формада қалыптастырылған, сақталатын, өңделетін немесе берілетін, қылмыстық іс үшін мәні бар мән жайларды белгілеу және тексеру үшін қолданылатын деректер (нәрселер)»;

7. Превентивті, инициациялық, артефактілік, атрибуттық және жолын кесушілік деңгейлерін ажырамас түрде біріктіретін тергеп-тексерудің авторлық бес деңгейлі интегративті архитектурасы ұсынылды. Оны іске асыру үшін ҚР ҚПК-нің 131-бабының 4-бөлігін ұстап алу үшін: *«қашықтағы серверлерде іздерді шұғыл криптографиялық бекіту қажеттілігіне байланысты үлестірілген ақпараттық жүйелерді пайдалана отырып сериялық онлайн алаяқтық жасады деген күдік болған кезде»* деген жаңа негізбен толықтыруды ұсына отырып, дәлелдемелерді сақтаудың императивті хронологиялық сүзгісі ретінде шұғыл «72 сағат» алгоритмін енгізу негізделді.

Диссертациялық зерттеудің теориялық және практикалық маңыздылығы.

Зерттеудің теориялық маңыздылығы онда цифрландыру жағдайындағы онлайн алаяқтыққа кешенді қылмыстық-құқықтық және процестік-криминалистикалық сипаттаманың берілуінде, тергеп-тексерудің инновациялық «артефактіге бағдарланған» моделінің ұсынылуында және қазіргі Қазақстанның қылмыстық сот ісін жүргізу жүйесіндегі цифрлық дәлелдемелердің дербес

орнының айқындалуында. Ғылыми тұжырымдарды заң мамандықтарының ғылыми мамандары, магистранттары мен докторанттары ғылыми, педагогикалық қызмет және цифрлық криминалистика саласындағы одан әрі әзірлемелер үшін пайдалана алады.

Зерттеудің практикалық маңыздылығы кибержымқыруларға қарсы іс-қимылдың мемлекеттік қылмыстық-процестік тетігі жүйесін, оның интегративті бес деңгейлі құрылымын және функционалдық мазмұнын (банктік антифрод-жүйелермен өзара іс-қимыл жасау алгоритмдерін қоса алғанда) жетілдіру жөніндегі ұсыныстардың мазмұнында. Ұсынымдарды заң шығарушы және құқық қолданушы органдар цифрлық қылмыстылықтың тиімді жолын кесу мақсатында Қазақстан Республикасының қылмыстық, қылмыстық-процестік және цифрлық құқығын одан әрі дамыту үшін пайдалана алады.

Зерттеу нәтижелерінің апробациясы. Диссертациялық зерттеу барысында алынған ғылыми нәтижелер Scopus базасына кіретін ғылыми журналда – 2, Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету Комитетінің тізімінде белгіленген ғылыми журналдарда – 8, алыс шетелдегі және Қазақстан аумағында өткізілген ғылыми халықаралық деңгейдегі конференциялар бойынша қалыптастырылған материалдар жинақтарында – 5 ғылыми мақалалар түрінде жарияланды.

Диссертациялық жұмыстың құрылымы мен көлемі. Диссертацияның құрылымы зерттеудің мақсаты мен міндеттеріне, сондай-ақ зерттелетін мәселенің ерекшелігіне негізделген. Жұмыс кіріспеден, он бөлімшеден тұратын негізгі мазмұнды қамтитын үш бөлімнен, қорытындыдан және пайдаланылған әдебиеттер тізімінен тұрады. Жұмыстың көлемі ғылыми диссертацияларға қойылатын белгіленген талаптарға сәйкес келеді.

1 ОНЛАЙН АЛАЯҚТЫҚ ҚЫЛМЫСТАРЫН СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІҢ ТЕОРИЯЛЫҚ-ҚҰҚЫҚТЫҚ НЕГІЗДЕРІ

1.1 Қоғамды цифрландыру жағдайындағы онлайн алаяқтықтың генезисі, ұғымы және құқықтық табиғаты

Қоғам дамуының қазіргі кезеңі адам тіршілігінің барлық салаларын іргелі түрде өзгертетін жүйелі әлеуметтік-экономикалық процесс ретінде әрекет ететін жаһандық цифрландырумен сипатталады. О.С. Капинус атап өткендей, ақпараттық қоғам дәуіріне қадам басу экономиканың, коммуникация тәсілдерінің және әлеуметтік байланыстар сипатының айтарлықтай трансформациялануына әкеп соқты [15, 5 б.]. Бұл ұстаным Қазақстан Республикасының мысалында «электрондық үкімет» веб-порталын (eGov.kz), үлкен деректерді өңдеу технологияларын енгізуде және ашық цифрлық платформаларды дамытуда көрініс тапқан цифрлық трансформациялаудың мемлекеттік стратегиясы сапалы жаңа институционалдық ортаны қалыптастыратынын атап көрсететін М.С. Бисалиевтің зерттеулерінде өзінің органикалық дамуын табады [16, 27 б.]. Өз кезегінде, К.О. Қарабеков аталған тәсілді нақтылай отырып, қаржы сервистерінің (финтех-индустрияның) жеделдетілген диджитализациясы және онлайн-банкинг жүйелерін жаппай енгізу жай ғана технологиялық жетістік емес, сонымен қатар мүліктік қатынастар архитектурасындағы терең өзгерістердің катализаторы болып табылатынын орынды көрсетеді [17, 78 б.]. Осы көзқарастарды салыстыру инфрақұрылымды цифрландыру экономикалық өзара іс-қимылдарды дәстүрлі физикалық байланыс жазықтығынан жоғары жылдамдықты виртуалды ортаға көшіре отырып, олардың моделін түбегейлі өзгертетін негізгі детерминант болып табылады деген қорытынды жасауға мүмкіндік береді.

Сонымен қатар, ақпараттық-коммуникациялық технологияларды қарқынды енгізу тек позитивті экономикалық әсерлерді ғана туындатпай, құқық бұзушылықтар жасау жағдайларын толығымен өзгерте отырып, сапалы жаңа криминогендік қатерлерді қалыптастырады. М.Д. Фроловтың пікірінше, цифрлық экономиканы құру автоматтандырылған деректерді өңдеу құралдарының арзандауымен бірге криминалдық әлем өкілдері үшін бұрын қолы жетпейтін жаңа мүмкіндіктер ашып, дәстүрлі пайдакүнемдік қол сұғушылықтардың сипатын едәуір өзгертті [18, 3 б.]. Бұл ойды С.А. Тамбиев толықтыра түседі: криминалдық құрылымдар заманауи инновациялық технологияларды өз әрекетіне сіңіріп, оларды қашықтан қаржылық әрі психологиялық ықпал жасаудың мықты құралына айналдырады, ал ондай ықпалдың алдында қауіпсіздіктің классикалық тосқауылдары дәрменсіз қалады [19, 64 б.]. Алайда К.Н. Евдокимов телекоммуникациялық желілер мен когнитивтік технологияларды жаппай қолдану қылмыстылыққа киберкеңістіктегі масштабтылық, анонимділік және өзін-өзі детерминациялау белгілерін бере отырып, оның жүйелі түрде модификациялануына әкеп соғатынын атап өтіп, бұл процестің тереңірек салдарларына негізді түрде көрсетеді [20, 16 б.]. Ұсынылған ғылыми көзқарастарды талдау цифрландырудың қағидатты түрде жаңа криминологиялық шынайылықты қалыптастыратынын,

оның шеңберінде онлайн алаяқтық мүліктік жымқырудың қарапайым түрі болудан қалатынын көрсетеді.

Белгіленген үрдістер мәнмәтінінде ақпараттық ортаның жай ғана қазіргі заманғы техникалық құрал немесе қоғамдық қауіпті іс-әрекет жасалатын орын емес, криминалдық өзара іс-қимылдың мәнін жүйелі түрде бұрмалайтын іргелі фактор ретінде әрекет ететінін атап өткен жөн. Біздің көзқарасымызша, цифрландыру жәбірленушінің ерік білдіруін қалыптастыру тетіктерін түрлендіре, алдау нысандарын және виртуалды мүліктік игіліктерді алып қою сипатын ерекшелей отырып, құқыққа қайшы іс-әрекеттерді жасау тәсілдері мен алгоритмдерін ғана емес, сонымен қатар алаяқтықтың құқықтық табиғатының өзін трансформациялайды. Мәмілелердің қашықтан жасалу сипаты, активтерді аудару процестерін автоматтандыру және әлеуметтік инженерия әдістерін пайдалану аталған құбылысты түсінуге арналған классикалық доктриналық тәсілдер өздерінің эвристикалық әлеуетін объективті түрде сарқитын жағдайлар жасайды.

Демек, оқшауланған феномен ретінде онлайн алаяқтықтың мәнін терең түсіну үшін, сондай-ақ сотқа дейінгі іс жүргізу шеңберінде оның процестік күрделілігін барабар бағалау үшін тек оның қазіргі заманғы технологиялық нысанын атап өту ғана жеткіліксіз. Цифрлық қылмыстылық дамуының анықталған іргелі заңдылықтары ерекше белгілерін анықтау және криминалдық децепция тетігінің оның дәстүрлі нысандарынан цифрлық нысандарына дейінгі эволюциясын белгілеу үшін осы құбылыстың тарихи-құқықтық генезисіне жүгінуді ғылыми тұрғыдан қажет етеді.

Цифрландыруды криминалдық трансформация факторы ретінде қарастырғанда, алаяқтықтың тарихи-құқықтық түп-тамырына үңілмеу мүмкін емес. Мұнда бір нәрсе айқын көрінеді: технология өзгереді, соған қарай алдау тәсілі бейімделеді, ал қылмыстық заң оларға кейін ілесіп жауап береді – үшеуі бір-бірінен ажырамайды. А.Б. Курумбаева мен Б.Б. Кощегулов алаяқтық жауапкершілігін реттеу кеңестік қылмыстық заңдардан егемен ұлттық заңнамаға дейін ұзақ жол жүргенін, әрі осы жол бойы заң диспозициясын құрудағы құқықтық техника ережелері технологиялық өзгерістерге ыңғайланып отырғанын атап өтеді [21, 46 б.]. К.Н. Евдокимов осыны нақтылай түседі: криминалдық практика мен қылмыстық құқық арасындағы алғашқы жарықшақ дәл сол тұста ашылған [20, 6 б.]. Қаскүнемдер қашықтан жаңылыстыру үшін электрондық поштаны игеріп үлгерген кезде, қылмыстық заң – 1959 жылғы Қазақ КСР ҚК-і, кейін оны алмастырған 1997 жылғы ҚР ҚК-і – алаяқтықты (177-бап) әлі күнге дейін тек мүлікті нақты иеленіп алу тұрғысынан бағалап отырды. Г.Р. Григорян осы алшақтықтың салдарын көрсетеді: классикалық материалдық нормалар виртуалды ортаға келмегендіктен, құқық қолданушы ескі конструкцияларды цифрлық алдаудың алғашқы көріністеріне зорлап таңуға мәжбүр болды, ал бұл кейінгі заңнамалық реформаларға негіз қалады [22, 5 б.]. Осы ұстанымдарды салыстыру бастапқы кезеңде технологиялық өзгерістер алдаудың мәнін өзгертпестен, тек аспаптық базаны ғана құрғанын, алайда сол кездің өзінде қылмыстық құқық реакциясының дамып келе жатқан криминалдық практикалардан артта қалуын белгілегенін атап өтуге мүмкіндік береді.

Қалыптасу сатысына (2014-2018 жж.) өту қашықтан банктік қызмет көрсетудің және цифрлық инфрақұрылымның қарқынды дамуымен сүйемелденді. Қазақстан Республикасы Ұлттық Банкінің деректері бойынша, 2017 жылы интернет және мобильді банкинг арқылы жасалған операциялар көлемі алдыңғы жылмен салыстырғанда үш есе өсіп, 3 трлн теңгеге жетті [23]. Бір мезгілде пайдаланушылар базасы кеңейді: 2018 жылға қарай онлайн-банкинг жүйелерінде шамамен 12 млн пайдаланушы тіркелді [24]. Аталған процестер мобильді интернеттің енуінің өсуі және цифрлық құрылғыларды пайдаланушылар санының артуы аясында жүрді, бұл онлайн-сервистерді масштабтау үшін технологиялық негізді қамтамасыз етті. Ғылыми пікірталасты дамыта отырып, М.Д. Фролов технологиялық ортаның өзгеруі алдау тәсілдерінің тез әрі айтарлықтай трансформациялануына әкеліп, оған барған сайын виртуалды өлшем беретінін тұжырымдайды [18, 3 б.]. Сонымен қатар П.А. Гоибназарзода көршілес мемлекеттердің қылмыстық заңнамасының осы сын-қатерге реакцияларындағы айырмашылыққа негізді түрде назар аударады: мәселен, 2012 жылы ресейлік заң шығарушы РФ ҚК-нің 159.6-бабын (компьютерлік ақпарат саласындағы алаяқтық) қоса алғанда, бірқатар арнайы құрамдарды енгізе отырып, нормаларды казуистикалық бөлшектеу жолымен жүрді, бұл күтілгендей қылмыстық-құқықтық нормалардың бәсекелестігін туындатты [25, 152 б.]. Бұл тәсілге қарағанда, отандық заң шығарушының реакциясын бағалай отырып, А.Б. Курумбаева мен Б.Б. Кощегулов қазақстандық қылмыстық-құқықтық модельдің үлкен икемділігі туралы қорытындыға келеді: 2014 жылғы ҚР ҚК қабылдануымен заң шығарушы оны іс-әрекетті «ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен» жасау деген арнайы саралаушы белгімен толықтыра отырып, базалық норманың (190-бап) бірлігін сақтап қалды [21, 49 б.]. Бұдан шығатыны, осы кезеңде цифрлық технологияларды енгізу заң шығарушыны технологиялық факторларды қылмыстық заңның құрылымына тікелей кіріктіруге мәжбүр ете отырып, алдау практикасын байланыссыз ортаға түпкілікті көшірді.

Институционалдану сатысы (2019 жылдан бастап) өту цифрлық қаржы технологияларының күнделікті практикада сапалы бекітілуімен байланысты. Қазақстан Республикасы Ұлттық Банкінің деректері бойынша, 2019 жылы қолма-қол ақшасыз операциялар көлемі 14,1 трлн теңгені құрап, алдыңғы жылмен салыстырғанда екі еседен астам ұлғайды, бұл ретте транзакциялардың 50%-дан астамы интернет және мобильді банкинг арқылы жүзеге асырылды. Айта кетерлігі, дәл осы кезеңде қолма-қол ақшасыз операциялар алғаш рет қолма-қол қаражатты алу операцияларынан асып түсті, ал қашықтан банктік сервистерді пайдаланушылар саны 19,7 млн адамға жетті. Аталған көрсеткіштер цифрлық қаржы сервистерінің институционалдық норма мәртебесіне өткенін көрсетеді [26].

О.С. Капинустың пікірінше, қазіргі заманның технологиялық базасы жымқыру тәсілдерін түбегейлі өзгертті: бейматериалдық қаржылық активтерге қол сұғу үшін қаскүнемдер бір мезгілде екі тәсілді ұштастырады – әлеуметтік инженерия әдістерімен (психологиялық ықпал) қатар компьютерлік ақпаратқа заңсыз енеді әрі зиянды бағдарламаларды іске қосады (техникалық ену), әрі бұл

екеуін бір-бірінен бөліп қарауға келмейді [15, 6 б.]. Алайда А.А. Энгельгардт бұл жағдай құқық қолдануда айтарлықтай қиындықтар тудыратынын атап өтіп, құқықтық реттеуге қатысты мынадай көзқарас ұсынады: компьютерлік ақпарат саласындағы алаяқтық жәбірленушіні классикалық алдау немесе сенімін теріс пайдалану шеңберінен шығып, ақпаратты сақтау, өңдеу және беру құралдарының жұмысына тікелей араласуға айналды, бұл тәжірибеде күрт бұрылыстарды болдырмау үшін тиісті тәжірибе қалыптастырушы құжаттарда (жоғары сот инстанциялары деңгейінде) тұрақты түсіндірулерді талап етеді [27, 92-93 б.]. Осы тәсілдерді талдау қазіргі кезеңде технологиялық мүмкіндіктердің децепция практикасын толығымен өзіне бағындырып, оны тұрақты криминалдық институтқа айналдырғанын, бұған жауап ретінде қылмыстық құқық іздерді жасырудың және қылмыстық рөлдерді бөлудің күрделене түсетін нысандарына ден қоя отырып, саралау тетіктерін үздіксіз бейімдеуге мәжбүр екенін көрсетеді.

Жүргізілген ретроспективті талдау негізінде алғаш рет онлайн алаяқтық генезисінің авторлық үш кезеңдік эволюциялық моделі (пайда болу, қалыптасу, институционалдану кезеңдері) ұсынылды және негізделді, ол ізашарлардың фрагменттік тәсілдерінен айырмашылығы, технологиялық құрылыстардың ауысуы ықпалымен криминалдық практиканың трансформациялануының үздіксіз процесін дәлелдейді. Осы мәнмәтінде ғаламдық желінің алаяқтық схемалар эволюциясына тигізетін ықпалын егжей-тегжейлі тарихи талдау интернет криминалдық практикалардың трансформациялануының негізгі катализаторы болғанын растайды [28, 249 б.]. Іргелі ауысу орын алды: алаяқтық тікелей физикалық өзара іс-қимылға және объективті шынайылықты контактілі бұрмалауға негізделген классикалық нысаннан күрделі виртуалды-децептивті тетікке трансформацияланды. Аталған феноменді дәл доктриналық бейнелеу үшін ғылыми айналымға алғаш рет «цифрлық децепция» авторлық ұғымы енгізілді. Өз кезегінде, технологиялық факторды толық елемеуден мамандандырылған саралаушы белгілерді енгізуге дейін эволюцияланған қылмыстық заңнаманың реакциясы осы криминалдық құбылыстың жүйелі өзгеруін растайды. Анықталған тарихи-құқықтық заңдылықтар және зерттеліп отырған іс-әрекеттің құқықтық табиғатының дәлелденген күрделенуі оны түсінуге арналған ғылыми-теориялық тәсілдерді жүйелеудің және онлайн алаяқтықтың біріздендірілген авторлық дефинициясын әзірлеудің объективті қажеттілігін туындатады.

Қазіргі заманғы ғылым мен құқық қолдану практикасында онлайн алаяқтықтың біріздендірілген анықтамасының болмауы елеулі терминологиялық белгісіздік пен саралау қайшылықтарын туындатады. К.О. Қарабеков атап өткендей, ғалымдар арасында ортақ пікірдің жоқтығы түрлі теориялық тәсілдердің болуымен шартталған, олардың ішінде тарихи алғашқы модельдердің бірі ретінде қылмысты тікелей ЭЕМ-мен (электронды-есептеуіш машиналармен) байланыстыратын технологиялық тәсіл әрекет етеді [17, 20 б.]. Осы бағыт шеңберінде Т.Л. Тропина іс-әрекеттің техникалық инструментарийіне назар аудара отырып, киберқылмысты басым түрде компьютерлердің, компьютерлік бағдарламалар мен желілердің жұмысына заңсыз араласу призмасы арқылы айқындауды ұсынады [29, 9 б.]. Аталған ұстанымды дамыта

отырып, И.Г. Чекунов мұндай қол сұғушылықтардың мәнін телекоммуникациялық құрылғылар мен ғаламдық желілерді криминалдық мақсаттарда қасақана пайдалануға сайып әкеледі [30, 22 б.]. Сонымен қатар М.Д. Фролов технологиялық тәсілді талдай отырып, цифрлық экономика мен деректерді өңдеу құралдарының дамуы алаяқтықтың түрлері мен тәсілдерін айтарлықтай трансформациялап, оған толыққанды виртуалды өлшем бергенін атап көрсетеді; осыған байланысты ғалым компьютерлік алаяқтықты дәстүрлі алдау призмасы арқылы емес, ақпараттық-телекоммуникациялық инфрақұрылым нысандарының жұмыс істеу процесіне заңсыз араласу арқылы жасалатын жымқыру ретінде қарастыруды ұсынады [18, 3 б.]. Бұдан шығатыны, технологиялық тәсіл құбылыстың мәнін толық көлемде қамтуға мүмкіндік бермейді, өйткені ол қылмыстың қылмыстық-құқықтық табиғатын оның аспаптық базасымен алмастырады.

Белгіленген шектеулерден шығудың жолын іздеген зерттеушілер объектілік және формальды-заңдық тәсілдерге ден қояды. Объектілік тәсілді жақтайтын М.А. Ефремова онлайн алаяқтықтың айқындаушы белгісі деп меншік қатынастарынан ажырағысыз қосымша объект – ақпараттық қауіпсіздікке жасалатын кешенді қол сұғушылықты санайды [31, 13 б.]. Бұған қарама-қарсы формальды-заңдық тәсілдің жақтаушысы Е.В. Зотина цифрлық децепцияны бөлек құбылыс ретінде емес, дәстүрлі мүліктік жымқырудың аясында ғана қарауды ұсынады; мұнда ақпараттық-коммуникациялық технологиялар пиғылды жүзеге асырудың жаңа түрі ретінде ғана көрініс табады [32, 77 б.]. Бұл ұстанымды А.А. Энгельгардт орынды сынға алады: оның айтуынша, компьютерлік ақпарат саласындағы жымқыруды дәстүрлі белгілерімен қоса «алаяқтық» атаудың өзінде елеулі шарттылық бар. Себебі мұндай жағдайда жалған ақпараттан адам емес, компьютерлік бағдарлама адасады; демек классикалық нормаларды виртуалды ортаға өзгеріссіз көшіру термин жағынан да, саралау жағынан да шатасу туғызады – ғалым осыны дәйекті түрде негіздейді [33, 87 б.]. Осы пікірлерді салғастырғанда, қолданыстағы ғылыми тұжырымдардың бір жақты екені, онлайн алаяқтықтың гибридті қылмыстық феномен ретіндегі мәнін толық ашуға дәрменсіз екені байқалады.

Қылмыстық құқық теориясында да, құқық қолдану тәжірибесінде де «кибералаяқтық», «цифрлық алаяқтық», «компьютерлік алаяқтық» және «интернет-алаяқтық» (онлайн-алаяқтық) деген атаулар көбіне бір мағынада қатар жүреді. И.А. Орешков дәлелдегендей, атаулардың осындай шашырауы әрі бір ұғымға түрлі мазмұн телінуі құқықтық тілдің біркелкілігін бұзады, нормаларды іс жүзінде қолдануды қиындатады [34, 19 б.]. Сондықтан осы зерттеуде терминологиялық шатасуды болдырмау және заң тілінің дәлдігі мен айқындығын сақтау үшін аталған нұсқалардан бас тартылып, бірыңғай атау ретінде «онлайн-алаяқтық» термині қабылданды.

Бұған қоса, «онлайн-алаяқтық» ұғымын жалпы «киберқылмыс» санатынан айқын ажыратып алу қажет. К.О. Карабеков киберқылмысты кең, тектік ұғым деп бағалайды: бұл – ақпараттық-коммуникациялық технологиялар арқылы ақпараттық кеңістікте қашықтан жасалатын алуан қылмыстардың (жүйелерді бұзу, вирус тарату, ботнеттер құру, т.б.) жиынтығы [17, 19 б.]. Осы орайда А.Ә.

Қалиевтің жіктеуі ерекше құнды – ол киберқылмыстардың бәрін екі үлкен санатқа бөледі:

– киберге тәуелді қылмыстар (cyber-dependent crimes) – технологиялық инфрақұрылымның өзіне бағытталған әрекеттер (жүйелерді бұзу, саботаж);

– кибертехнологиялар арқылы жасалатын қылмыстар (cyber-enabled crimes) – цифрлық құралдарды қылмыстың тек тәсілі не құралы ретінде пайдаланатын дәстүрлі қылмыстар [35, 295 б.].

Ғалымның негіздеуінше, онлайн-алаяқтық нақ осы екінші санаттағы ең жиі кездесетін қылмыс. Басқаша айтқанда, киберқылмыс – виртуалды кеңістіктегі кез келген құқық бұзушылықты қамтитын ауқымды макроұғым, ал онлайн-алаяқтық оның бір ғана тармағы (түрлік ұғымы): мұнда мақсат компьютерлік жүйенің өзін бұзу емес, технологияны құрал етіп, бөтен мүлікті алдау арқылы иемдену.

Табылған олқылықтар мен терминологиялық анықсыздық зерттеліп отырған құбылыстың табиғатын тұтас бейнелейтін авторлық анықтаманы тұжырымдауды талап етеді. Қолданыстағы тәсілдердің шектеулерін ескере отырып, онлайн-алаяқтық деп мынаны түсінген жөн: жәбірленушінің еркін бұрмалау үшін ақпараттық-коммуникациялық технологияларды міндетті түрде қолданатын әрі тараптардың қашықтан әрекеттесуімен ерекшеленетін, цифрлық ортада алдау арқылы, пайда табу ниетімен бөтен мүлікті немесе оған деген құқықты құқыққа қайшы, өтеусіз иемдену. Бұл анықтаманың ғылыми жаңалығы – классикалық қылмыстық-құқықтық белгілерді (құқыққа қарсы иемдену мақсаты, алып қою тәсілі ретіндегі алдау) технологиялық детерминанттармен (цифрлық орта, қашықтық, телекоммуникациялық желілер) біртұтас ұштастыруында; нақ осы ұштасу аталған құбылысты сабақтас киберқылмыстардан айқын ажыратуға мүмкіндік береді. Ал бірыңғай терминологиялық аппаратты қалыптастыру мен онлайн-алаяқтықтың гибридті табиғатын бекіту оның құқықтық табиғатын қылмыс құрамының объективті және субъективті элементтері арқылы тереңдеп талдауға қажетті теориялық-әдіснамалық негіз қалайды.

Тұжырымдалған бірыңғай анықтама онлайн-алаяқтықтың құқықтық табиғатын тереңдеп зерттеуді талап етеді, ал ол табиғат қолданыстағы ҚР ҚК бекіткен қылмыс құрамы элементтерінің классикалық құрылымы арқылы неғұрлым толық ашылады. А.Б. Курумбаева мен Б.Б. Кощегулов байқағандай, ақпараттық технологиялар арқылы жасалатын қол сұғушылықтар көбейгенімен, олар бұрынғысынша меншікке қарсы бағытталады; цифрландыру өзгертетіні – осы әрекеттердің жасалу тәсілдері мен тетіктері ғана [21, 49 б.]. Осы ойды өрбіте отырып, М.Д. Фролов қолма-қол ақшасыз қаражат пен виртуалды активтердің қылмыс затына айналуы жиілегенін көрсетеді, бұл мүліктік қатынастар аясының материалдық заттар шегінен асып кеңейгенін аңғартады [18, 63 б.]. Г.Р. Григорян өз тарапынан мұндай әрекеттердің көп объектілі сипатын алға тартады: меншік қатынастарымен қатар қосымша объектіге – ақпараттық қауіпсіздік пен цифрлық инфрақұрылымның белгіленген жұмыс тәртібіне де зиян келеді [22, 17 б.]. Бұл пікірлерден шығатын қорытынды: онлайн-алаяқтықтың объектісі классикалық мүліктік өзегін сақтайды, бірақ ақпараттық қауіпсіздік пен цифрлық экономикалық қатынастарды қамтып едәуір кеңейеді, ал бұл өз кезегінде оны құқықтық қорғаудың күрделене түсетінін алдын ала айқындайды.

Объектінің өзгеруі заңды түрде қылмыстың объективті жағын да сапалық жағынан түрлендіреді; ол ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағы шеңберінде ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен іс-әрекетті жасаумен сипатталады. А.А. Энгельгардт өз еңбегінде К. Горобецтің тұжырымына сүйене отырып, объективті жақ ең алдымен тәсілде трансформацияланатынын атап көрсетеді: адаммен тікелей физикалық байланыс жасау және оны алдау виртуалды бағдарламалар мен цифрлық арналар арқылы жанама әсер етумен ығыстырылады [33, 86 б.]. Аталған тәсілді нақтылай отырып, М.Д. Фролов қашықтықтан жасалатын мұндай қылмыстарда мүлікті алып қою жәбірленушінің жаңылысу ықпалында болып, когнитивтік бұрмалану нәтижесінде активтерді өз бетінше беруіне тікелей тәуелді екенін негіздейді [18, 76 б.]. Сонымен қатар В.Г. Шумихин аппараттық-бағдарламалық кешендерді пайдалану мүлікті алып қою тетігін соншалықты өзгертетінін, оның дәстүрлі шеңберге сыймайтын жымқырудың қағидатты түрде дербес жаңа (жетінші) нысанын қалыптастыратынын көрсете отырып, неғұрлым радикалды көзқарас ұсынады [35, 93 б.]. Осы көзқарастарды салыстыра отырып, «байланыс → алдау → мүлікті беру» классикалық формуласы құрылымдық жағынан сақталатынын, бірақ іске асырудың өзге нысанына ие болатынын атап өткен жөн: ақпараттық-коммуникациялық технологияларды пайдалана отырып қашықтан әсер ету жәбірленушінің активтерді өз бетінше беруіне түрткі болады, бұл субъектілер арасындағы кеңістіктік-уақыттық байланысты үзеді.

Қылмыс жасалатын орта өзгергенде, оның субъектісіне берілетін сипаттама да өзгеріссіз қалмайды. Формальды-заңдық өлшеммен алғанда субъект – қылмыстық жауаптылық жасына толған, есі дұрыс жеке тұлға, бірақ А.С. Камко байқағандай, цифрлық ортадағы нақты орындаушы көбіне тұтас криминалдық тізбектің жалғыз буыны ретінде ғана қалып отыр [36, 84 б.]. Осы пікір О.В. Полстовалов пен Р.Р. Галяутдиновтың жұмыстарында өзінің дамуын табады, олар қылмыскерлердің тұлғасызануы және мамандануы үрдісін негізді түрде көрсетеді, мұнда жымқыру жасайтын адамдар шынайы өмірде бір-бірімен таныс емес және қатаң бөлінген міндеттерді орындай отырып, тек псевдонимдермен ғана әрекет етеді [37, 123 б.]. Аталған тәсілдерге сүйене отырып, авторлық ұстанымды негіздеуді қажет деп санаймыз: онлайн алаяқтық субъектісі іс жүзінде жеке орындаушының белгілерін жоғалтады және рөлдерді терең функционалдық бөлуі бар үлестірілген құрылымның айқын белгілерін иеленеді (зиянды бағдарламалық қамтылымды әзірлеушілер, әлеуметтік инженерлер, дропперлер және ұйымдастырушылар).

Жоғарыда аталған үлестірілген құрылым мен рөлдердің бөлінуі сот практикасының материалдарымен толық расталады. Зерттелген қылмыстық істердің эмпирикалық базасына сүйене отырып, қазіргі заманғы онлайн-алаяқтың неғұрлым толық және бөлшектелген криминологиялық портретін келесідей сипаттауға болады:

– әлеуметтік-демографиялық белгілері мен мәртебесі: Сотқа тартылғандардың басым көпшілігі – 20 мен 35 жас аралығындағы жастар. Білім деңгейі бойынша олар көбінесе орта немесе арнаулы орта білімге ие. Бұл санаттағы қылмыскерлердің басты әлеуметтік маркері – тұрақты жұмыс

орнының болмауы. Олар негізінен ресми түрде жұмысқа орналаспаған, тек бейресми табыс көздерімен (мысалы, жалдамалы жұмысшы) күн көреді немесе қаржылық қиындықтарды бастан кешіріп жүрген тұлғалар. Отбасылық жағдайына келсек, көптеген сотталушылардың асырауында кәмелетке толмаған балалары бар, бұл жайт сот отырыстарында жазаны жеңілдететін мән-жай ретінде (ҚР ҚК-нің 53-бабына сәйкес) тұрақты түрде қолданылады;

– қылмыстық-құқықтық сипаттамасы және рецидивке бейімділігі: Кибералаяқтардың басты ерекшелігі – олардың жоғары деңгейдегі криминализациялануы және рецидивке бейімділігі. Сот актілерін талдау көрсеткендей, көптеген алаяқтар бұрын дәстүрлі ұрлық (ҚР ҚК 188-бабы) немесе осыған ұқсас мүліктік қылмыстар үшін сотталған және жаңа эпизодтарды бұрынғы соттылығы өтелмеген кезде немесе пробациялық бақылауда жүріп жасайды. Кейбір тұлғалар бірнеше жыл қатарынан бірнеше рет сотталып, қылмыстық әрекеттерін тоқтатпай, оны табыс табудың тұрақты кәсібіне айналдырған. Бұл олардың түзелу жолына түспегенін және қоғамнан оқшаулауды талап ететін тұрақты қылмыстық бағыттылығын көрсетеді;

– психологиялық ерекшеліктері және әрекет ету тәсілі (Modus Operandi): Бұл қылмыскерлер жоғары бейімделгіштікке және базалық цифрлық сауаттылыққа ие. Олар смартфондарды, екінші деңгейлі банктердің қосымшаларын («Kaspi», «Home Credit Bank» және т.б.), электрондық коммерция сайттарын («OLX.kz», «Krisha.kz»), тіпті криптовалюталық платформаларды (мысалы, Bybit) қылмыстық мақсатта еркін әрі шебер пайдаланады. Олардың іс-әрекеттері әлеуметтік инженерияға негізделген: құрбандардың сеніміне кіру үшін олар өздерін медицина қызметкерлері, «ҚазПочта» курьерлері, автобөлшек сатушылары немесе пәтер иелері ретінде таныстырып, құрбандарға психологиялық қысым мен айла-шарғы жасайды. Сонымен қатар, олар жауапкершіліктен жалтару мақсатында қаражатты тікелей өз шоттарына емес, делдалдардың («дропперлердің») банк карталары мен электрондық әмияндары арқылы шығарудың көпсатылы схемаларын белсенді қолданады.

Бұл теориялық тұжырым бір қылмыстық тізбектің буындары арасындағы толық анонимділікті бейнелейтін сот практикасында өзінің даусыз растауын табады. Мәселен, №5532-25-00-1/20 қылмыстық ісі бойынша (Павлодар облысы Ақтоғай аудандық сотының 2025 жылғы 23 желтоқсандағы үкімі) [38] сот кінәлі адам көмектесуші рөлінде әрекет ете отырып, анықталмаған сыбайлас қатысушының («Kaz_man» желілік псевдонимімен әрекет еткен) нұсқауларын қатаң орындағанын анықтады. Бөлінген техникалық рөл шеңберінде көмектесуші жаппай жаңа SIM-карталарды сатып алып, оларды іске қосқан және кураторға «WhatsApp» мессенджерінде тіркелу үшін кодтарды қашықтан беріп отырған, содан кейін аккаунттар жәбірленушілерге тікелей алаяқтық қоңыраулар шалуды жүзеге асыру үшін басқа адамдарға берілген. Іс материалдары іс-әрекеттерді үйлестіру және үлестерді бөлу (криптовалютамен) сыбайлас қатысушылардың визуалды байланысынсыз тек қана цифрлық ортада орын алғанын растайды. Осы қылмыстық іс материалдарында жеке қылмыс субъектісінің бірыңғай «үлестірілген субъектілік құрамға» трансформациялануы көрнекі түрде бейнеленеді. Мұндай гибридті субъектінің іс-әрекеттері қатаң

аумақтық және функционалдық бытыраңқылыққа қарамастан, жалпы пайдакүнемдік мақсатпен және рөлдерді нақты бөлумен біріктірілген.

Аталған аумақтық бытыраңқылық және бүркемелеудің техникалық құралдарын пайдалану қарастырылып отырған іс-әрекеттің субъективті жағына өз ізін қалдырады. Дәстүрлі түрде субъективті жақ тікелей пиғыл түріндегі кінәмен және пайдакүнемдік мақсатпен сипатталады. Р.Н. Подольный атап өткендей, цифрлық ортаның ерекшеліктерін пайдалану қылмыскерде өзінің қолжетімсіздігі мен жазасыз қалуы туралы тұрақты иллюзия (сенім) қалыптастырады [39, 57 б.]. Өз кезегінде, А.А. Комаров қашықтан өзара іс-қимыл жасау кезінде пиғылды іске асыру ерекшелігі желідегі анонимділікпен детерминацияланғанын нақтылайды: бұл технологиялар қаскүнемге ең аз шығынмен әлеуетті құрбандарды жаппай қамтуға (бұқаралық әсер етуге) мүмкіндік береді [40, 17 б.]. Бұдан шығатыны, ғылыми зерттеулерде орынды көрсетілгендей, компьютерлік ақпарат саласындағы алаяқтықта пиғылдың интеллектуалдық және еріктік элементтері күрделене түседі: олар бөтеннің мүлкін құқыққа сыйымсыз алып қою фактісін ұғынуды ғана емес, сонымен қатар ақпаратты өңдеу процесін бұзу үшін күрделі технологиялық алгоритмдерді мақсатты түрде қолдануды (яғни алдын ала болжау мен қалауды) да қамтиды.

Қылмыс құрамының элементтерін талдауды түйіндегенде, онлайн-алаяқтықтың құқықтық табиғаты жүйелі сипатта екенін айтуға болады. Іс-әрекеттің классикалық түзуші элементтері – объект, объективті жақ, субъект және субъективті жақ – қолданыстағы заңнама аясында өзінің іргелі қылмыстық-құқықтық негізін жоғалтпайды, бірақ олардың нақты көрінісі цифрлық ортаның ықпалымен түбегейлі жаңа пішінге түседі. Осылайша жымқырудың материалдық-байланыстық парадигмасы виртуалды-қашықтық парадигмасына ауысады: қорғау объектісі кеңейеді, алдау жанама сипат алады, субъектілік құрам үлестіріледі, ал пиғылды жүзеге асыру тетігі күрделенеді. Мұндай күрделі құқықтық табиғат құқық қорғау жүйесінің алдына елеулі сын-қатер қояды әрі зерттеуді келесі кезеңге – цифрландыру жағдайындағы онлайн-алаяқтықтың криминологиялық сипаттамасын, жәбірленушілер осалдығының ерекшеліктерін және қалыптасып келе жатқан киберкриминалдық инфрақұрылымның қоғамдық қауіптілігін бағалауға – жетелейді.

Онлайн алаяқтықтың құқықтық табиғатын зерделеу оның криминологиялық қырларын талдауды заңды түрде талап етеді, ал бұл қырлар жаппай цифрландыру аясында бұрынғыдан бөлек, сапалық жаңа ауқымға шығады. М.Д. Фролов көрсеткендей, ақпараттық технологиялардың енуі пайдакүнемдік қол сұғушылықтардың латенттілігін туғызады, әрі оның деңгейі 85–99%-ға жетеді [18, 93 б.]. Бұл пікірге Р.Н. Подольный де қосылады: ол цифрлық қылмыстардың жоғары латенттілігі, әрекеттердің анонимденуіне байланысты, құқық бұзушыларды құқық қорғау жүйесінің қолы жетпейтіндей етіп қоятын сыни проблема деп есептейді [39, 57 б.]. К.О. Карабеков болса, бұл жасырындылықты көбіне онлайн-алаяқтықтың трансшекаралық сипатымен байланыстырады: қылмыскерлер шет мемлекет аумағынан әрекет ете отырып, құқық қорғау органдарының тікелей юрисдикциясынан тыс қалады [17, 46 б.]. Осы үш пікірді біріктіргенде мынадай тұжырым туады: жаппайлық, ауқымдылық және

экстерриториялылық – зерттеліп отырған құбылыстың іргелі криминологиялық белгілері, өйткені нақ солар қаскүнемдерге қылмыстық қудалаудан бұрын-соңды болмаған деңгейде қалқалануға мүмкіндік береді.

Экстерриториялылықпен қатар қылмыс субъектілерінің мінез-құлқы да елеулі өзгеріске ұшырайды: олар барған сайын ұйымшыл қылмыстық құрылымдардың құрамына енуде. О.В. Полстовалов пен Р.Р. Галяутдинов онлайн-алаяқтықтың заманауи түрлерінде рөлдер айқын бөлінетінін, мұнда технологиялық міндеттер жәбірленушімен тікелей байланыстан ажыратылғанын, ал қатысушылардың өздері жиі бірін-бірі танымайтынын атап өтеді [37, 122 б.]. Осы ойды өрбіте отырып, А.Д. Фокин «алаяқтық колл-орталықтардың» (call-орталықтардың) қызметіне бөлек тоқталады – ғылыми теорияда жеке санатқа айналған бұл орталықтардың қатысушылары жәбірленушінің санасын нысаналы түрде манипуляциялауға (психологиялық ықпал жасауға) құрылған әлеуметтік инженерия әдістерін кәсіби деңгейде қолданады [41, 96 б.].

Мұндай жымқырулардың топтық нысандары дамуының ерекше векторы қылмыстық әрекеттің тікелей жабық үлгідегі мамандандырылған мекемелер ішінде оқшауланууы болды. Мәселен, №3572-21-00-1/9 қылмыстық ісі бойынша (Қарағанды қаласы Октябрь ауданының №2 аудандық сотының 2021 жылғы 16 сәуірдегі үкімі) [42] алдын ала сөз байласу бойынша әрекет ететін адамдар тобының физикалық тұрғыдан наркологиялық диспансерде мәжбүрлеп стационарлық емделуде бола отырып, ақпараттық жүйелерді пайдаланушыларға қатысты жүйелі түрде алаяқтық әрекеттер жасағаны анықталды. Іс-әрекеттерді үйлестіру, интернет-сайттарда ойдан шығарылған хабарландыруларды орналастыру, жәбірленушілерді іздеу және манипуляциялар заңсыз пайдаланылатын мобильді телефондар мен SIM-карталар арқылы жүзеге асырылды. Бұл онлайн алаяқтықтың ұйымдасқан субъектісінің қоғамнан физикалық оқшауланудан жоғары тәуелсіздік дәрежесін көрсетеді.

Сот практикасында билік өкілеттіктерін имитациялау арқылы осындай психологиялық қысымның криминалдық күшеюінің тұрақты үрдісі тіркелген. Мәселен, №3511-23-00-1/5 қылмыстық ісі бойынша (Қарағанды қаласы Қазыбек би аудандық сотының 2023 жылғы 05 маусымдағы үкімі) [43] кінәлі адамдар пайдакүнемдік мақсаттарды көздей отырып, өздерін полиция қызметкерлері ретінде таныстырып, жеке кездесулер ұйымдастырғандығы анықталды. Лауазымды адамның атағын өз бетімен иемденіп алып, олар жәбірленушілердің қылмыстық іске қатысуы және күдіктілер мәртебесіне ауыстыру қатері желеуімен оларға басым психологиялық әсер еткен. Қорқып қалған құрбандар жалған «қылмыстық жауаптылықтан құтылу» үшін қаскүнемдерге өздерінің смартфондарын берген, олар арқылы соңғылары банктік қосымшаларда ірі тауарлық кредиттерді кедергісіз ресімдеген (іс-әрекеттерді сот ҚР ҚК-нің 190-бабы 3-бөлігінің 4-тармағында және 390-бабының 2-бөлігінде көзделген қылмыстардың жиынтығы бойынша саралаған). Бұл сот прецеденті ақпараттық жүйенің технологиялық осалдығы тікелей психологиялық әкімшілендіру әдістерімен ажырамас байланыста болатын қазіргі заманғы алаяқтық схемалардың гибридті сипатын сенімді түрде дәлелдейді.

Өз кезегінде, А.С. Камко пен Ю.Ю. Комлев ақпараттық әсер ету адамның әлсіздіктерін, қорқыныштары мен эмоцияларын манипуляциялау арқылы жеке тұлғаға терең психологиялық қысым жасаумен ажырамас байланысты екенін орынды атап өтіп, мұндай қол сұғушылықтардың тек технологиялық табиғатын сыни тұрғыдан бағалайды (мұндай жағдайларда шабуыл жасалатын объект ретінде компьютер емес, адамның өзі әрекет етеді) [36, 26 б.; 44, 379 б.]. Аталған көзқарастарды салыстыру қазіргі заманғы кибералаяқтықтың бағдарламалық қамтылымның осалдықтарына ғана емес, көбінесе өнеркәсіптік ауқымда ұйымдасқан топтар іске асыратын айлалы психологиялық әсер етуге сүйенетінін көрсетеді.

Әлеуметтік инженерия әдістерін пайдалану виртуалды ортадағы жәбірленушілердің осалдығы проблемасын сөзсіз өзектендіреді. Бүгінгі таңда әлеуметтік желілердің алгоритмдері мен цифрлық платформаларды қаскүнемдер алдауды масштабтау және пайдаланушыларды психологиялық манипуляциялауды күшейту үшін белсенді түрде қолданады [45, 21 б.]. А.В. Майоров атап өткендей, цифрландыру процестері ерекше цифрлық виктимділікті туындатады, онда электрондық сервистердің белсенді пайдаланушыларының өзі қашықтан алдауды тануға қабілетсіз болып шығады [46, 10 б.]. Бұл тәсіл А.С. Камконың зерттеуінде нақтыланады, ол виктимді мінез-құлық көбінесе азаматтардың шектен тыс сенгіштігімен, олардың келіп түсетін ақпаратқа сыни қарамауымен және ақпараттық қауіпсіздік мәдениетінің жалпы төмен деңгейімен шартталғанын тұжырымдайды [36, 104-105 б.]. Алайда Д.В. Жмуров осалдық цифрлық платформалардың архитектурасының өзінде және электрондық коммерция жүйелерін нормативтік реттеудегі кемшіліктерде қаланған кездегі кибервиктимизацияның техногендік алғышарттарын көрсете отырып, проблеманы неғұрлым кеңінен түсіндіруді ұсынады [47, 143 б.]. Баяндалғандар онлайн алаяқтықтың виктимологиялық көрінісі субъективті факторлардың (құқықтық бейхабарлық, шектен тыс сенгіштік) да, пайдакүнемдік пиғылды іске асыру үшін қолайлы орта жасайтын объективті технологиялық тәуекелдердің де ықпалымен қалыптасатыны туралы қорытынды жасауға мүмкіндік береді.

Осы диссертациялық зерттеудің эмпирикалық базасын 2021 мен 2026 жылдар аралығында Қазақстан Республикасының соттары шығарған 127 сот үкімінен тұратын массив құрады. Таңдаманың географиялық ауқымы репрезентативті жалпыұлттық сипатқа ие және республикалық маңызы бар қалалардың (Астана, Алматы, Шымкент), сондай-ақ Ақтөбе, Ақмола, Алматы, Атырау, Қарағанды, Маңғыстау, Павлодар және Түркістан облыстары соттарының сот актілерін қамтиды. Зерттелген актілерді бірінші сатыдағы соттар: негізінен аудандық және оларға теңестірілген қалалық соттар, сондай-ақ қылмыстық істер жөніндегі мамандандырылған ауданаралық соттар қабылдаған.

Талдау пәні ретінде алаяқтық туралы қылмыстық істер санаты алынды. Үкімдердің абсолюттік көпшілігі ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану жолымен жасалған жымқыруларға (ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағы және 3-бөлігінің 4-тармағы) байланысты. Тағылған баптың бөлігіне қарай бұл құқық бұзушылықтар ауырлығы орташа және ауыр қылмыстар ретінде сараланады. Зерттелген істердің бірқатарында

басқа да мүліктік құқық бұзушылықтармен, атап айтқанда ұрлықпен (ҚР ҚК-нің 188-бабы) және ұсақ-түйек жымқырумен (ҚР ҚК-нің 187-бабы) процестік жиынтық тіркелген.

Эмпирикалық таңдаманың маңызды процестік және ғылыми мәні бар өзге де сипаттамаларына бір үкім шеңберінде бірнеше дербес эпизодтардан тұратын қылмыстық әрекеттің айқын сериялылығы жатады. Бұдан басқа, істердің осы санаты бойынша қазіргі құқық қолдану практикасының ерекшелігі – сот ісін жүргізуді цифрландыру және процестік үнемдеу: істердің едәуір бөлігі бейнеконференцбайланыс жүйелерін (соның ішінде «Zoom» платформасы арқылы) қолдана отырып электрондық форматта қаралған, ал сот талқылаулары жаппай қысқартылған тәртіппен немесе кінәні мойындау туралы мәміле түріндегі процестік келісімдерді бекіту шеңберінде өткізілген.

Осы орайда, зерттеліп отырған 127 сот үкімінің эмпирикалық материалдарын талдау қылмыстық әрекеттердің және құқық қолдану практикасының нақты типологиясын жасауға, сондай-ақ оларды бірнеше айқын санатқа бөліп қарастыруға мүмкіндік береді:

1-тип: Цифрлық және құқықтық сауатсыздыққа негізделген виктимділік (аса сенгіштік және дербес деректерді қорғау дағдыларының болмауы). Бұл санатты бөліп көрсетудің негізгі критерийі – жәбірленушілердің цифрлық гигиена қағидаларын жүйелі түрде сақтамауы және биометриялық сәйкестендірудің, дербес деректердің құқықтық маңызын түсінбеуі болып табылады. Зерттелген сот актілерінің эмпирикалық базасы көрсеткендей, елімізде қаржылық қызметтердің цифрландырылу деңгейі халықтың құқықтық және технологиялық сауаттылығынан әлдеқайда озып кеткен. Бұл топтағы жәбірленушілер өздерінің бұғаттан шығарылған ұялы телефондарын, банк қосымшаларының құпия сөздерін және транзакцияларды растайтын СМС-кодтарды бөгде адамдарға, сондай-ақ әріптестеріне немесе туыстарына ешбір күмәнсіз, өз еркімен береді. Олардың санасында смартфонға физикалық қол жеткізу мен заңды түрде қаржылық міндеттемелердің (несиелік шарттардың) туындауы арасындағы тікелей себеп-салдарлық байланыс мүлдем қалыптаспаған. Жәбірленушілер цифрлық аутентификация құралдарын жеке басты куәландыратын құжат немесе электрондық цифрлық қолтаңба ретінде қабылдамайды.

Бұл санаттың басты белгісі – жәбірленуші мен қылмыскердің арасында жасанды не шынайы сенім қатынасының орнауы. Тәжірибеде жәбірленушілер қаскүнемдердің «интернеттен бірдеңені шұғыл қарап беру», «туысыма хабарлама жолдау» немесе «қоңырау шалу» тәрізді қарапайым өтінішіне сеніп, өзінің басты байланыс әрі қаржы құралы – смартфонын қолына ұстатып жіберетін жағдайлар жүйелі түрде кездеседі. Сот практикасы бұл осалдықты алаяқтардың мемлекеттік қызмет не әлеуметтік көмек сылтауымен ептілікпен пайдаланатынын аңғартады. Мәселен, №3528-23-00-1/20 қылмыстық іс бойынша (Қарағанды облысы Шахтинск қалалық сотының 2023 жылғы 11 маусымдағы үкімі) [48] қылмыстық топ мүшелері өздерін «Қазпошта» не медицина қызметкерлеріміз деп таныстырып, жәбірленушінің бетін «Ashyq» қосымшасына сканерлейміз деген жалған сылтаумен суретке түсірген. Ал іс жүзінде дәл сол сәтте банк қосымшаларындағы «Face ID» биометриясынан өтіп, жәбірленушінің

атына ірі көлемде тауар және ақша несиесін ресімдеп үлгерген. Сенімге кіре отырып, жақындарының (әріптестерінің, туыстарының) телефонын сұрап алып, соларға жасырын несие рәсімдеу фактілері де жиі ұшырасады. Осы мысалдардың бәрі бір нәрсені айқын көрсетеді: жәбірленуші физикалық құрылғысына рұқсат берген сәтте өзінің барлық мүліктік құқығын қылмыскердің қолына табыстап қояды. Аталған санат зерттелген жалпы массивтің шамамен 30–35%-ын құрайды. Виктимділіктің мұндай түрі азаматтардың заманауи технологияға көзсіз сенуінен, құқықтық жауапкершілікті сезінбеуінен және қылмыстық ниетті аңғара алмауынан туындайды. Алаяқтар осы осалдықты аса шеберлікпен пайдаланып, қылмысын әдеттегі тұрмыстық жағдайдың астына жасырады.

2-тип: Пайдакүнемдік виктимділік (нарықтық бағадан төмен тауарлар мен қызметтерге, негізсіз үнемдеуге ұмтылу) – бұл ең көп таралған топ. Екінші санатты бөліп көрсетудің негізгі критерийі – жәбірленушінің мінез-құлқындағы экономикалық мотивтер, яғни тез байып кетуге, тауарларды немесе қызметтерді нарықтық құнынан айтарлықтай төмен бағаға сатып алуға, сол арқылы негізсіз қаржылық үнемдеуге деген қатты ұмтылысы. Зерттелген сот үкімдерінің эмпирикалық материалдарына сүйенсек, бұл топ қашықтан жасалатын алаяқтық қылмыстар құрылымындағы ең көп таралған виктимдік модель болып табылады және оның үлесі барлық істердің шамамен 45-50% құрайды. Бұл жағдайда жәбірленушілердің объективті талдау және сыни ойлау қабілеті өте арзан бағамен ұсынылған тиімді тауарды немесе қызметті жіберіп алмау қорқынышымен толықтай бұғатталады. Олар транзакциялық тәуекелдерді саралау мүмкіндігінен мүлдем айырылады.

Бұл санаттың басты сипаттамасы – жәбірленушілердің ғаламтор желісіндегі қашықтан жасалатын мәмілелердің базалық қауіпсіздік ережелерін толықтай елемеуі. Қылмыскерлер «OLX.kz», «Kolesa.kz», «Instagram» сияқты танымал электрондық коммерция алаңдары мен әлеуметтік желілерде тұрмыстық техника, ұялы телефондар, автобөлшектер сату немесе пәтерді нарықтан төмен бағамен жалға беру туралы визуалды тартымды, бірақ мазмұны жалған хабарландырулар орналастырады. Олар жасанды сұраныс пен ажиотаж тудыру арқылы жәбірленушіні тез арада шешім қабылдауға итермелейді. Жәбірленушілер тауардың шынайылығын, сатушының жеке басын растайтын ешқандай заңды құжат талап етпестен, мүлдем танымайтын белгісіз тұлғалардың банк шоттарына алдын ала төлем (аванс) немесе тіпті тауардың толық сомасын өз еркімен аударады. Мәселен, №7141-25-00-1/1908 қылмыстық ісі бойынша (Астана қаласының Қылмыстық істер жөніндегі ауданаралық сотының 2025 жылғы 05 қыркүйектегі үкімі) [49] сотталушы «Instagram» желісінде «Lu-na» аккаунты арқылы демалыс үйлерін жалға беру туралы жалған жарнама салып, жәбірленушілерден 60 000 теңгеден алдын ала төлем алып отырған. Осыған ұқсас, №5511-22-00-1/31 қылмыстық ісі бойынша (Өскемен қаласы №2 сотының 2022 жылғы 24 мамырдағы үкімі) [50] бойынша «OLX.kz» сайты арқылы пәтерді арзан бағаға жалға беру сылтауымен бір ғана алаяқ 80-нен астам адамды алдаған. Осыған ұқсас жүздеген істерде жәбірленушінің қарапайым экономикалық сақтық шараларын сақтамауы қылмыстың мінсіз аяқталуына тікелей жағдай жасаған. Пайдакүнемдік виктимділік алаяқтарға құрбандарды ұзақ уақыт іздеудің қажеті

жоқтығын, керісінше, жәбірленушілердің арзан тауар мен оңай олжа іздеп, қылмыскерлердің тұзағына өздігінен келіп түсетіндігін дәлелдейді. Бұл санаттағы қылмыстардың өсу динамикасы азаматтардың экономикалық мінез-құлқындағы ажиотаждық факторлармен тығыз байланысты.

3-тип: Әлеуметтік-психологиялық осалдыққа және манипуляцияға негізделген виктимділік (мемлекеттік көмек алуға немесе делдалдардың уәдесіне сену). Үшінші санатты қалыптастырудың іргелі негізіне жәбірленушілердің нақты әлеуметтік мәртебесінен, тұрмыстық жағдайынан туындайтын қажеттіліктер және соның салдарынан кәсіби психологиялық манипуляцияға жоғары бейімділігі жатады. Бұл спецификалық топқа кіретін азаматтар көбінесе мемлекеттік бағдарламалар арқылы жеңілдіктер, тұрғын үй субсидияларын, қайтарымсыз гранттар алуға тырысатын немесе жеке қаржылық қиындықтарын шешу үшін делдалдардың «көмегіне» жүгінуге мәжбүр болатын тұлғалар болып табылады. Олардың үлесі зерттелген эмпирикалық массивте шамамен 15-20% деңгейінде бағаланады, алайда келтірілетін моральдық және институционалдық зиян орасан зор.

Бұл санаттың басты ерекшелігі – қылмыскерлердің жәбірленушінің көкейкесті әлеуметтік мәселесі мен құқықтық сауатсыздығын манипуляция тетігіне айналдыра білуінде. Жәбірленуші қиын өмірлік жағдайдың (көпбалалы отбасы, жұмыссыздық) кесірінен не мемлекеттік мекемедегі күрделі бюрократиялық кедергіден құтылғысы келіп, интернеттегі бейтаныс адамға шексіз сеніп қалады. Мысалы, №3511-23-00-1/5 қылмыстық іс бойынша (Қарағанды қаласы Қазыбек би аудандық сотының 2023 жылғы 05 маусымдағы үкімі) [43] қылмыскерлер өздерін полиция қызметкеріміз деп таныстырған. Осы санатқа ақшалай тарыққан азаматтарға қолма-қол қаражат тауып беремін деп уәде етіп, солардың атына банктерден тауар несиесін ресімдеп жіберу тәжірибесі де жатады. Мұндай виктимдік үлгінің ерекше қаупі – жәбірленуші тек тікелей материалдық зиян шегіп қоймайды, оның мемлекеттік және әлеуметтік институттарға деген сенімі де қатты шайқалады. Қылмыскерлер азаматтың әлеуметтік мұқтажы мен үмітін негізгі манипуляция құралына айналдырып, оны ауыр қаржылық қамытқа (тәуелділікке) салады.

Кәмелетке толмағандар қатысатын тергеу әрекеттерінің ерекшеліктері. Бөлек назар аударуды қажет ететін мәселе – онлайн-алаяқтық істерінде кәмелетке толмаған баланың жәбірленуші не куәгер (құрал ретінде пайдаланылған тұлға) ретінде қатысуы. Кәмелетке толмағандар цифрлық жағынан сауатты болғанымен, өмірлік тәжірибесінің тапшылығы оларды киберқылмыскерлер үшін оңай олжаға айналдырады – мысалы, онлайн-ойын аккаунттарын сатып алу-сату немесе арзан гаджет алмастыру кезінде. Мұндай жағдайларда тергеу әрекеттерінің тактикасы айтарлықтай өзгереді. Қылмыстық-процестік заңнама баланың психикасын қорғауға қатаң талаптар қояды. Сот практикасы дәлелдегендей, мысалы, №3570-20-00-1/149 қылмыстық ісі бойынша (Қарағанды қаласы Октябрь аудандық сотының 2020 жылғы 11 желтоқсандағы үкімі) [51], кәмелетке толмаған куәгерден жауап алу және оның құрамында электрондық хат-хабарлар (цифрлық іздер) бар «Ксиоми» маркалы ұялы телефонын алу міндетті түрде оның заңды өкілінің (анасының) қатысуымен ғана жүргізілген. Осы

талапты бұлжытпай орындау – кәмелетке толмағандардан алынған электрондық (цифрлық) дәлелдемелердің сотта жарамдылығын қамтамасыз етудің кепілі.

Бұл ретте ерекше деструктивті психоәлеуметтік әсерге халықтың неғұрлым осал топтары, атап айтқанда кәмелетке толмағандар ұшырайды, бұл қорғаудың предиктивті және превентивті қорғау стратегияларын енгізуді қажет етеді [52, 8 б.].

Субъективті фактор криминологиялық тұрғыдан ерекше бір қырынан ашылады: мұнда жәбірленушінің өз бойындағы бастапқы құқыққа қарсы ниетпен астасқан виктимді мінез-құлқы көрінеді. Сот практикасында адамдардың біліктілік сертификатын, жүргізуші куәлігін не өзге де заңсыз артықшылықты алмақ болып, кибералаяқтарға қаражатын өз қолымен беретін жағдайлары кездеседі. Ниетінің заңға қайшы екенін біле тұра әрекет ететін мұндай жәбірленуші, шындап келгенде, көлеңкелі қызмет нарығының кеңеюіне және киберқылмыстың өршуіне себепші болады. Осыған байланысты құқық бұзушылықтардың кешенді профилактикасы шеңберінде мұндай адамдарды дербес әкімшілік жауаптылыққа тарту туралы мәселені қарастырған орынды. Мұндай шара криминалдық сұраныстың тұйық шеңберін үзуге және азаматтардың өзіндік «сыбайластық» виктимділігі деңгейін төмендетуге мүмкіндік береді.

Анықталған криминологиялық детерминанттарды қорытындылай келе, мынадай авторлық ұстанымды белгілеуді қажет деп санаймыз: жаһандық цифрландыру жымқырудың жекелеген тәсілдерін жай ғана түрлендіріп қоймай, онлайн алаяқтықтың тұрақты криминалдық инфрақұрылымының қалыптасуына ықпал етеді. Бұл инфрақұрылым кешенді сипатқа ие және өзіне технологиялық (желілерді анонимдеу, зиянды бағдарламалық қамтылымды пайдалану), ұйымдастырушылық (үлестірілген қылмыстық топтар, трансшекаралық колл-орталықтар) және мінез-құлықтық (жаппай әлеуметтік инженерия, цифрлық виктимділікті пайдалану) элементтерін органикалық түрде біріктіреді. Мұндай өзін-өзі жаңғыртатын криминалдық экожүйенің қалыптасуы жеке тұлғаларға да, жалпы мемлекет экономикасына да орасан зор залал келтіретін қарастырылып отырған қол сұғушылықтардың қоғамдық қауіптілігінің сапалық және сандық өсуін көрсетеді. Алаяқтықтың ұлттық қауіпсіздікке төнетін жүйелі қатерге трансформациялануын растайтын анықталған криминологиялық сипаттамалар зерттеліп отырған проблематиканы теориялық-құқықтық талдаудың жалпы қорытындыларын шығаруды талап етеді.

Жүргізілген теориялық-құқықтық талдау жаһандық цифрлық ортаның қалыптасуы алдау тетігін тікелей тұлғааралық байланыс жазықтығынан қашықтан виртуалды децепция саласына көшіре отырып, оның терең трансформациялануының іргелі катализаторы болды деп қорытынды жасауға мүмкіндік береді. Осындай технологиялық ауысу қылмыстық заңнаманың сапалы жаңа криминалдық сын-қатерлерге кейінгі бейімделуін объективті түрде детерминациялады, бұл әзірленген онлайн алаяқтықтың авторлық дефиниціясында өзінің шоғырландырылған көрінісін тапты. Ұсынылған ұғымның ғылыми жаңалығы дәл жымқырудың базалық қылмыстық-құқықтық белгілері мен ерекше цифрлық сипаттамалардың органикалық синтезінде жатыр.

Бұдан шығатыны, зерттеліп отырған феноменнің құқықтық табиғаты айқын жүйелі сипатқа ие: қылмыс құрамының классикалық элементтері өзінің доктриналық негізін сақтайды, алайда оларды практикалық іске асыру нысаны қол сұғушылықтың көп объектілігін, ақиқатты бұрмалаудың жанамалығын және субъектілік құрамның үлестірілгендігін туындата отырып, ақпараттық-коммуникациялық технологиялардың ықпалымен толығымен қайта формattалады.

Өз кезегінде, аталған құқықтық және технологиялық гибридизация өзін-өзі жаңғыртатын киберкриминалдық инфрақұрылымды қалыптастыра отырып, іс-әрекеттің криминологиялық құрылымының түбегейлі күрделенуіне заңды түрде әкеп соғады. Оған тән гиперлатенттілік, экстерриториялылық, қол сұғушылықтардың жаппайлығы және әлеуметтік инженерия әдістерін пайдалану тиімді құқық қорғаушылық қарсы іс-қимылды сыни тұрғыдан қиындататын негізгі факторлар ретінде әрекет етеді. Тұжырымдалған қорытынды анықталған тарихи-құқықтық, догматикалық және криминологиялық заңдылықтар одан әрі зерттеу үшін сенімді теориялық-әдіснамалық негіз құрайтынын атап өтуге мүмкіндік береді. Онлайн алаяқтықтың мәнін жүйелі түрде түсіну оның көп факторлы жіктемесін әзірлеуге және сотқа дейінгі тергеп-тексеру мәнмәтінінде ерекше процестік мәні бар сипаттамаларды анықтауға көшудің объективті ғылыми қажеттілігін туындатады.

1.2 Онлайн алаяқтық қылмыстарын жіктеу және оның сотқа дейінгі тергеп-тексеру контекстіндегі процессуалдық мәні бар сипаттамалары

Онлайн алаяқтықтың бұрын тұжырымдалған, оны кешенді жүйелі феномен ретінде танитын анықтамасы тиісті қылмыстық-процестік дифференциацияны қамтамасыз ету үшін көп факторлы типология жасауды қажет етеді. А.Ю. Головин байқағандай, қылмыстардың базалық криминалистикалық жіктемесі қылмыстық құқық ғылымына қарағанда әлдеқайда кең өлшемшарттарға сүйенеді әрі сотқа дейінгі іс жүргізудің тиімді, толық құрылымды әдістемесін құруға іргетас болады [53, 31-32 б.]. Осыны нақтылай отырып, М.В. Стояновский тергеп-тексеру бойынша ұйымдастырушылық және тактикалық ұсынымдар әзірлеуге арқау болатын тармақталған терминологиялық жүйе дәл жіктемелік зерттеулер арқасында қалыптасатынын көрсетеді [54, 469 б.]. В.А. Мещеряков болса жіктеменің тек ғылыми талдау үшін емес, тікелей құқық қолдану практикасы үшін де айқындаушы мәні бар екенін атап өтеді: ол жоғары ақпараттық белгісіздік жағдайында тергеу органдары әрекетінің алгоритмдерін ретке келтіруге жол ашады [55, 70 б.]. Осы пікірлерді салыстыра келгенде, онлайн-алаяқтықты жіктеу таза теориялық құрал ғана емес, процестік тетіктерді нақты цифрлық қол сұғушылықтардың өзгешелігіне бейімдеуге мүмкіндік беретін, сотқа дейінгі тергеп-тексеруді ұйымдастыруға қажет қолданбалы тірек ретінде де қызмет ететіні аңғарылады.

Пәрменді жіктемелік модельді әзірлеу қатаң әдіснамалық қағидаттарға сүйенуді талап етеді. Д.А. Илюшиннің зерттеулері көрсеткендей, ақпараттық технологиялар саласындағы қылмыстарды кез келген бөлу виртуалды ортадағы

криминалдық көріністің үздіксіз эволюцияланатын барлық нысандарын қамтуды қамтамасыз ете отырып, логикалық толықтық талабына сай болуға тиіс [56,]. Бұл тезисті Р.Н. Подольный дамытады, ол бөліп көрсетілетін іс-әрекеттердің типтері саралауға тікелей ықпал етуге және қылмыстық іс жүргізудің ерте сатыларының өзінде нақты оңтайлы тергеу әрекеттерін таңдауды айқындауға тиіс болатын процестік маңыздылық пен операционалдылық қағидаттарын сақтау қажеттілігін дәлелді түрде негіздейді [39, 35-36 б.]. Сонымен қатар Р.Б. Джилкишиев жекелеген өлшемшарттарды олардың ішкі өзара байланыстарын ескермей оқшаулап қолдану тергеп-тексерудің фрагменттілігіне және дәлелдемелік базаның жойылуына сөзсіз әкеп соғатынын тұжырымдай отырып, аталған талаптарды сотқа дейінгі іс жүргізуді ұйымдастырудағы қатаң жүйелілік қағидатымен (системный подход) толықтыруды ұсынады [57, 95-96 б.]. Баяндалған ғылыми көзқарастардың интеграциясы типологиялаудың әдіснамалық негізі шектен тыс абстрактілікті жоя отырып, құбылысты жан-жақты қамту мен оның құқық қолданушының қажеттіліктеріне қатаң қолданылуының үйлесімді ұштасуына құрылуға тиіс екенін көрсетеді.

Белгіленген қағидаттарды сақтау мәнмәтінінде онлайн алаяқтықты жіктеудің нақты өлшемшарттарын негіздеу ерекше маңызға ие болады. Базалық негіздерді бөліп көрсету кезінде И.Г. Чекунов пайдаланылатын аппараттық-бағдарламалық байланыс арналарының ерекшелігіне және қол сұғушылық бағытталған қорғалатын игіліктердің сипатына байланысты іс-әрекеттерді саралай отырып, басым түрде технологиялық және объектілік өлшемшарттарға сүйенеді [30, 9-11 б.]. Ғылыми пікірталасты дамыта отырып, О.В. Полстовалов пен Р.Р. Галяутдинов қазіргі заманғы қашықтан жасалатын жымқыруларда топтық нысандардың үлесі айтарлықтай артып келе жатқанына назар аударады. Ғалымдар мұндай қылмыстар көбінесе әрбір сыбайлас қатысушының рөлі нақты функционалдық бөлінген және жақсы жолға қойылған бизнес-процесс ретінде әрекет ететін үлестірілген ұйымдасқан құрылымдар арқылы іске асырылатынын дәлелдейді [37, 125 б.]. Алайда В.В. Поляков дәл цифрлық іздердің пайда болу, тіркеп-белгілеу және алып қою ерекшелігі бүкіл қылмыстық істің процестік перспективасын детерминациялайтындықтан, трасологиялық өлшемшартты бірінші кезектегі ретінде бөліп көрсете отырып, назарды дәлелдеу жазықтығына ауыстыруды ұсынады [58, 123 б.]. Ұсынылған тәсілдерді талдау бірөлшемді жіктеменің өзінің эвристикалық әлеуетін объективті түрде сарқығанын сенімді түрде дәлелдейді, осыған байланысты қылмыстық іс жүргізудің қазіргі заманғы ғылымы зерттеліп отырған феноменнің технологиялық, объектілік, құрылымдық және трасологиялық параметрлерін біріктіретін кешенді модельді қажет етеді.

Баяндалған ережелер ұсынылған әдіснаманың онлайн алаяқтықты айрықша күрделі, көп деңгейлі криминалдық құбылыс ретінде жіктеуге тұтас және жан-жақты тәсілді қамтамасыз ететінін атап өтуге мүмкіндік береді. Қалыптастырылған көп факторлы негіз қылмысты оңайлатылған техникалық қабылдау тәуекелін жояды және мамандандырылған тергеу алгоритмдерін әзірлеу үшін сенімді теориялық іргетас жасайды. Кешенді типологиялауға деген анықталған объективті қажеттілік бөліп көрсетілген негіздердің мазмұнын егжей-тегжейлі ашудың логикалық қажеттілігін туындатады, бұл қарастырылып

отырған қоғамға қауіпті іс-әрекеттерді жіктеудің технологиялық, объектілік және құрылымдық өлшемшарттарын дәйекті түрде талдауға көшуді алдын ала шешеді.

Онлайн алаяқтықтың көп факторлы жіктемесін іске асыру қылмыс жасау тәсілдерінің қаскүнемдер қолданатын аппараттық-бағдарламалық құралдарға тікелей тәуелділігін көрсететін технологиялық өлшемшартқа бірінші кезекте жүгінуді көздейді. Е.С. Шевченко атап өткендей, киберқылмыстардың жіктемесі іргелі түрде субъектінің біліктілік деңгейіне және ол таңдайтын ақпараттық технологиялардың күрделілігіне негізделеді, бұл байланыстың цифрлық арналары арқылы жәбірленушіге әлеуметтік-технологиялық әсер етудің ерекшелігін детерминациялайды [59, 53-54 б.]. Бұл ой ақпараттық технологиялардың операциялық және коммуникативтік-үйлестірушілік функцияларды орындайтынын атап көрсететін А.А. Рудыхтың зерттеулерінде өзінің дамуын табады [60, 44 б.]. Сонымен қатар К.А. Мира қолданылатын технологиялар коммуникацияны қамтамасыз етіп қана қоймай, сонымен қатар қалыптасатын цифрлық іздердің сипатын да айқындайтынын алға тартып, осы тәсілді нақтылай түседі [61, 17 б.]. Дегенмен эмпирикалық деректер бұл доктриналық тәсілді толымсыз деп тануға негіз береді: АКТ енді жай коммуникация мен бүркемелеу құралы болудан әлдеқашан асып түсті. Бүгінде ол қол сұғушылық бағытын адам психикасынан қаржы институттарының бағдарламалық кодына қарай ауыстырып, алгоритмдік тосқауылдарды айналып өтудің әрі скорингтік жүйелерді тікелей манипуляциялаудың дербес құралына айналды. Осы пікірлерді салғастырғанда, технологиялық өлшемшарттың дәлелдеу процесінде іргелі маңызы бар екені көрінеді: қолданылатын алдау алгоритмдерінің өзгешелігі мен цифрлық арналар арқылы әсер ету ерекшелігі дәлелдеме көздерінің сипатын айқындап қана қоймайды, сотқа дейінгі тергеп-тексерудің ең бастапқы кезеңінің өзінде арнайы білімге жүгінудің (атап айтқанда, компьютерлік-техникалық сараптама тағайындаудың) объективті процестік қажеттілігін де туғызады.

Мұндай қажеттілік дербес деректерді қорғауға сыни қатер төндіретін фишинг, вишинг және фарминг сияқты қазіргі заманғы жымқыру алгоритмдерінің үздіксіз жетілдірілуімен тікелей байланысты [62, 89 б.].

Криминалистикалық аспектіде қашықтан алаяқтық жасаудың неғұрлым көп таралған тәсілдеріне (технологияларына) мыналар жатады:

– «претекстинг» – түрлі құпия ақпаратты ұсыну туралы өтінішпен ойдан шығарылған (легитимді) желеумен жәбірленушіге хабарламалар жіберу;

– «телефондық фрикинг» (вишинг) – жәбірленушіні қажетті деректерді өз еркімен беруге итермелеу үшін әлеуметтік инженерия әдістерін қолдана отырып, оған тікелей телефон қоңырауларын шалу;

– «фишинг» – жәбірленушінің аутентификациялық деректерін заңсыз иеленіп алу мақсатында ресми сайттарды визуалды түрде имитациялайтын құқыққа қарсы (жалған) интернет-ресурстарды пайдалану;

– зиянды бағдарламалық қамтылымды енгізу – құрбанның дербес компьютерлік құрылғысына (немесе смартфонына) оларды кейіннен жасырын жүктеп алу үшін платформалар мен интернет-дүкендерде зиянды бағдарламаларды орналастыру.

Технологиялық фактормен қатар, цифрландыру жағдайында күрделі құқықтық нысандарға ие болатын тікелей қол сұғушылық затына байланысты онлайн алаяқтықты саралауды қамтамасыз ететін объектілік белгі жіктеменің аса маңызды өлшемшарты ретінде әрекет етеді. А.П. Перетолчиннің пікірінше, азаматтық-құқықтық айналымның кеңеюі қылмыстық-құқықтық қорғау орбитасына тек классикалық банктік көрсетілетін қызметтер мен қолма-қол ақшасыз ақша қаражаты ғана емес, сонымен қатар қылмыстық және азаматтық заңнаманы синхрондауды талап ететін цифрлық құқықтардың да тартылуына әкелді [63, 96 б.]. Аталған тәсілді нақтылай отырып, А.В. Маилян қашықтан банктік қызмет көрсету жүйелеріне, электрондық әмияндарға және өзге де қаржы құралдарына қол сұғушылықтарды дербес жіктемелік топ ретінде бөліп көрсету қажеттілігін атап көрсетеді [64, 41 б.]. Алайда М.Д. Фролов криптовалюта және өзге де цифрлық активтер сияқты жаңа виртуалды объектілердің пайда болуына негізді түрде назар аударады, олардың екіұдай мүліктік табиғаты іс-әрекеттерді саралау кезінде өткір пікірталастар тудыратынын көрсетеді [18, 72 б.]. Ұсынылған пікірталасты талдау объектілік өлшемшарт дәлелдеу процесінде міндетті түрде анықталуға жататын азаматтық-құқықтық элементтердің ерекшелігін (активтің мәртебесін, қаржылық қызметтер көрсету тәртібін, мүліктік құқықтардың тиесілілігін) айқындай отырып және нақты материалдық нормаларды қолдану шекараларын белгілей отырып, жасалған іс-әрекеттің қылмыстық-құқықтық сараланuын тікелей детерминациялайтынын көрсетеді.

Пайдаланылатын технологиялар мен қол сұғушылық объектілерінің ажырамас өзара байланысы қылмыстық әрекетті ұйымдастыру нысандарын көрсететін құрылымдық өлшемшарттың эволюциясын заңды түрде алдын ала айқындайды. А.К. Щербаченко тұжырымдағандай, қазіргі заманғы қашықтан алаяқтық тұрақтылық пен ұйымдасқандық дәрежесі бойынша сараланатын жеке қол сұғушылықтардан күрделі топтық нысандарға эволюцияланды [65, 42 б.]. Бұл тезисті дамыта отырып, А.Г. Корпеев қылмыстардың желілік табиғаты әртүрлі юрисдикцияларда бола отырып, қылмыстық процестерді қашықтан басқара алатын топ қатысушыларының шашыраңқы орналасуын детерминациялайтынын көрсетеді [66, 144 б.]. Өз кезегінде, осы тәсілдерге негізделе отырып, қазіргі жағдайда рөлдерді терең функционалдық бөлуі бар криминалдық әрекетті ұйымдастырудың үлестірілген түрлері бүгінгі жағдайда сөзсіз басым деген авторлық ұстанымды негіздеуді жөн көреміз. Мұндай желілік құрылымда техникалық мамандар (алгоритм мен интерфейс әзірлеушілері), әлеуметтік инженерлер (қашықтан алдау операторлары) және активтерді айналымнан шығарушылар (дропперлер) бір-бірімен жеке байланысқа түспестен, әркайсы дербес жұмыс істейді. Осындай құрылымдық ерекшеліктің дәлелдеуде сыни маңызы бар, себебі ол сотқа дейінгі тергеп-тексеру органдарынан криминалдық желінің әрбір функционалдық оқшауланған қатысушысының тартылу дәрежесін дәлелдеуге және жауаптылығын дараландыруға бағытталған пиғылды анықтаудың қағидатты түрде өзге алгоритмдерін қолдануды талап етеді.

Тергеу органдарының тікелей пиғылды және «алдын ала сөз байласу бойынша адамдар тобында» саралаушы белгісін дәстүрлі әдістермен дәлелдеу

әрекеттері, әсіресе орындаушының бейхабарлығы туралы сөз болғанда, жиі процестік күйреуге ұшырайды. Сот практикасының базалық тәсілі мынадай: егер орындаушы бастамашының шынайы криминалдық ниеттерін ұғынбаса, адамдар тобында алаяқтық жасауға деген пиғыл туралы тұжырымдар болжамдарға негізделген деп танылады (бұл, мысалы, Алматы қаласы Бостандық ауданының №2 аудандық сотының №7550-21-00-1/516 іс бойынша 2022 жылғы 03 қазандағы үкімімен ішінара ақтау үкімінің логикасымен расталады) [67]. Киберқылмыстар саласында үйлестірушілердің толық анонимділігіне байланысты бұл проблема азаматтық-құқықтық жауаптылықтың теңгерімсіздігіне әкеп соғады. Мәселен, №5532-25-00-1/20 қылмыстық ісі бойынша (Павлодар облысы Ақтоғай аудандық сотының 23.12.2025 ж. үкімі) [38] сот көп миллиондық залалды (10 000 000 теңге) тек қана техникалық көмектесушіден өндіріп алды. Бұл ретте сот соңғыларының анықталмағандығын, оларға қатысты істің жеке іс жүргізуге бөліп шығарылғандығын және айыптау үкімінің шығарылмағандығын негізге ала отырып, жәбірленуші тарапқа бұл өндіріп алуды киберқылмыстың негізгі ұйымдастырушыларымен «ортақ» деп танудан бас тартты. Бұл сот актілері субъективті жақты анықтаудың және жауаптылығын бөлудің консервативті әдіснамасы ауыр қаржылық ауыртпалықты тек анықталған төменгі деңгейдегі орындаушыларға ғана қалдыра отырып, қылмыстық топтардың криптографиялық фрагментациясын адекватты түрде еңсере алмайтынын дәлелдейді.

Қарастырылған негіздерді салыстыру олардың тек бірыңғай жүйенің өзара байланысты элементтері ретінде ғана жұмыс істейтінін көрсетеді: технологиялық инструментарий қол сұғушылық объектісін таңдауды айқындайды, ал цифрлық активтердің ерекшелігі криминалдық топтардың тиісті құрылымдық күрделенуін талап етеді. Бұдан технологиялық, объектілік және құрылымдық өлшемшарттардың жиынтығы дәл қылмыстық-құқықтық саралауды жүзеге асыруға ғана емес, сонымен қатар адекватты дәлелдеу стратегиясын құруға мүмкіндік беретін онлайн алаяқтықтың базалық типологиялық негізін құрайды деген аралық қорытынды шығады. Сонымен қатар ұсынылған жіктеменің эвристикалық әлеуетін практикалық іске асыру виртуалды ортадағы қылмыстық әрекеттің бейнелену тетіктерін терең түсінбейінше мүмкін емес, бұл цифрлық іздерге трасологиялық талдау жасауға және қылмыстық сот ісін жүргізу шеңберінде олардың дәлелдемелік мәнін бағалауға көшудің логикалық қажеттілігін туындатады.

Көп факторлы жіктеменің логикалық жалғасы ретінде іздердің қалыптасу эволюциясы призмасы арқылы онлайн алаяқтықтың криминалистикалық негізін зерттеуге мүмкіндік беретін трасологиялық өлшемшарт әрекет етеді. Ақпараттық-коммуникациялық технологияларды криминалдық практикаға енгізу іздердің классикалық теориясының виртуалды кеңістік жағдайларына қолданылуы туралы мәселені өзектендірді. Н.П. Майлис атап өткендей, трасологияның базалық әдіснамасы қазіргі заманғы болмыста өзінің эвристикалық қуатын жоймайды, тек жаңа объектілерге бейімделуді ғана талап етеді, себебі цифрлық орта іздің тек сыртқы пішінін өзгертеді, ал ақпараттың бейнелену заңдылықтарын өзгеріссіз қалдырады [68, 492 б.]. В.А. Мещеряков

болса мүлдем өзгеше жол ұсынады: өзіндік математикалық табиғатына қарай материалдық іздерге де, идеалды іздерге де толық сыймайтын виртуалды іздерді ол жеке, дербес санатқа шығарады [55, 112 б.]. Өз кезегінде, бұл ұстаным В.Б. Вехов тарапынан негізді сынға ұшырайды, ол электрондық-цифрлық іздердің қатаң материалдық табиғатқа ие екенін, өйткені олар электромагниттік өзара іс-қимылдар нәтижесінде пайда болатынын және аппараттық-бағдарламалық кешендердің нақты физикалық жеткізгіштерінде тіркеп-белгіленетінін сенімді түрде дәлелдейді [69, 83 б.].

Тергеу практикасы тұрғысынан алғанда, цифрлық іздің орналасу орнына негізделген жіктеме де маңызды болып табылады. В.Б. Вехов электрондық-цифрлық іздерді мынадай түрлерге бөлуге болатынын көрсетеді:

1. Із-бейнелер:
– электромагниттік сигналдар;
– файлдар;
– компьютерлік бағдарламалар;
– деректер базасы;
– электрондық хабарламалар;
– электрондық құжаттар;
– ЭЕМ желісіндегі (компьютерлік желідегі) электрондық парақшалар;
– Интернет желісіндегі сайттар.
2. Із-заттар:
– ақпараттың машиналық тасымалдағыштары;
– интегралдық микросхемалар мен микроконтроллерлер;
– ЭЕМ (компьютерлер);
– ЭЕМ жүйелері (компьютерлік жүйелер);
– ЭЕМ желілері (компьютерлік желілер) [70, 81-95 б.].

Ұсынылған ғылыми көзқарастарды салыстыру цифрлық орта із ұғымын және оны визуалдандыру тетіктерін шынымен де түбегейлі трансформациялайтынын, бірақ із қалыптасуының жалпы мәні криминалистикалық танымның материалистік парадигмасы шеңберінде қалатынын көрсетеді.

Қазіргі криминалистика ғылымында цифрлық іздердің табиғатына қатысты пікірталастар әлі де жалғасуда. Кейбір ғалымдар оларды материалдық та, идеалдық та емес, дербес «виртуалды іздер» деп санағанымен, жетекші криминалистердің ғылыми ұстанымы неғұрлым негізді болып табылады. Олардың тұжырымдамасына сәйкес, цифрлық іздер – бұл көрінбейтін материалдық іздердің ерекше түрі. Бұл ұстаным кез келген цифрлық ақпараттың физикалық тасымалдағышта (қатқыл диск, жады микросхемасы) электромагниттік өзара іс-қимылдар арқылы бекітілетіндігімен және материалдық негізсіз (тасымалдағышсыз) дербес өмір сүре алмайтындығымен түсіндіріледі. Сонымен қатар, тергеу тәжірибесінде цифрлық іздерді алу және оқу күрделілігіне қарай жіктеудің маңызы зор. В.Е. Пономаревтің зерттеулері негізінде цифрлық іздер мен олардың тасымалдағыштарын оларға қол жеткізу, алып қою және арнайы маман тарту қаншалықты қажет екеніне қарай үш

деңгейге (санатқа) бөлген жөн [72, 13 б.].

Бірінші санат (базалық, жеңіл деңгей) – ашық қолжетімді, әрі алу барысында ақпаратты жоғалту қаупі жоқ беткі іздерді қамтиды (флэш-жинақтағыштардағы, оптикалық дискілердегі файлдар); тергеуші оларды IT-маманды тартпай-ақ өз бетінше процестік тұрғыдан ресімдей алады.

Екінші санат (орташа күрделілік деңгейі) – құпия сөзбен қорғалған, жойылған не автономды қуат көзі бар құрылғылардағы (смартфон, ноутбук) іздерге қатысты; мұнда ақпараттың бұзылуына жол бермеу үшін маман тарту міндетті.

Үшінші санат (жоғары немесе аса күрделі деңгей) – бұлтты серверлерде, таратылған блокчейн-желілерінде, анонимизаторларда орналасқан немесе криптографиялық шифрланған іздерден тұрады. Мұндай артефактілерді алу мен деанонимизациялау аса күрделі алгоритмдерді және жоғары білікті IT-сарапшылардың кешенді зерттеулерін қажет етеді.

Цифрлық із қалыптасуының дәлелденген материалдық негізін ескере отырып, классикалық трасология мен қазіргі заманғы киберкриминалистиканың жетістіктерін кіріктіретін жіктемелік модельді қалыптастырудың объективті қажеттілігі туындайды, бұл ұсынылып отырған тәсілдің ғылыми жаңалығын құрайды. Онлайн алаяқтықтың іздік көрінісі құрылымында серверлердің лог-файлдары, IP және MAC-адрестер, жүйелік тізілімдердің метадеректері және мобильді құрылғылардың конфигурациясы туралы мәліметтер жататын материалдық цифрлық іздер бірінші кезектегі маңызға ие. Олармен қатар, В.А. Козинкин Р.С. Белкиннің іргелі іліміне сүйене отырып атап өткендей, қылмыстық оқиға қоршаған ортада бейнелену барысында материалдық іздермен қатар міндетті түрде идеалды іздер де қалдырады, ал олардың бейнеленуі мен қабылдану сапасы тікелей тұлғаның субъективті-психологиялық қасиеттеріне (жәбірленушілер мен куәгерлердің криминалдық оқиға процесін субъективті психоэмоционалдық қабылдауына және жадында сақтауына) тәуелді болады [72, 37 б.]. Өз кезегінде, А.Д. Цветкова виртуалды коммуникация жағдайында енгізудің техникалық параметрлері мен орындаушының психофизиологиялық ерекшеліктері ажырамас түрде тоғысатын компьютерлік (пернетақталық) қолтаңбаның ерекше дәлелдемелік мәнге ие болатынына назар аударады [73, 59 б.]. Қашықтан алдаудың ерекшелігін ескере отырып, аталған тәсілдерді синтездей келе, техникалық аппараттық-бағдарламалық элементтер мен пайдаланушының мінез-құлықтық (когнитивтік) сипаттамаларының ажырамас үйлесімін білдіретін үшінші, ерекше санатты – гибридті іздерді бөліп көрсету туралы авторлық ұстанымды негіздеуді қажет деп санаймыз. Гибридті іздерге веб-ресурстар бойынша навигацияның бірегей паттерндерін, пернетақталық қолтаңбаның жеке ерекшелігін, сондай-ақ электрондық құрылғылардың кэшінде тіркеп-белгіленген, әлеуметтік инженерия әдістерін қолдана отырып жазысқан хат-хабарлардың лингвистикалық маркерлерін жатқызған жөн. Осы триаданы бөліп көрсету киберқылмыс жасау процесінде пайда болатын криминалистикалық маңызы бар ақпараттың барлық спектрін неғұрлым толық және жүйелі түрде қамтуға мүмкіндік береді.

Осындай активті, пассивті және гибридті цифрлық артефактілерді тиімді

анықтау, алып қою және криминалистикалық зерттеу табысты тергеп-тексеру үшін іргелі әдіснамалық негіз ретінде әрекет етеді [74, 175 б.].

Қашықтан жасалатын алаяқтыққа тән болып табылатын жоғарыда келтірілген із түрлері мен олардың жіктемелерін жеткілікті толық деп тануға болады. Сонымен қатар көрсетілген із түрлерінің ішінде қашықтан жасалатын алаяқтықты жасаған тұлғаны тікелей анықтауға «жұмыс істейтін» іздер топтарын бөліп көрсету орынды. Осыған байланысты цифрлық іздерді мынадай топтарға бөлуді ұсынамыз:

1) қылмыскердің тұлғасын анықтауға жәрдемдесетін іздер;

2) қылмыскердің орналасқан жерін анықтауға жәрдемдесетін іздер;

3) қылмыскердің тұлғасының белгілері мен қасиеттері туралы диагностикалық ақпарат алуға жәрдемдесетін іздер.

Бірінші топқа қылмыс жасаған тұлға туралы немесе ол туралы ақпарат алуға мүмкіндік беретін іздер жатады. Олардың қатарында:

– пайдаланушының анкеталық деректерін көрсететін іздер,

– пайдаланушының сайттарға кіру белсенділігі туралы мәліметтер (жеке деректері бар файлдар мен cookies-файлдар),

– түпкілікті жабдықтың, ақпараттық жүйелер мен компьютерлік желілердің цифрлық идентификаторлары (IP-мекенжай, сайттың домендік атауы).

Екінші топқа қашықтан қол жеткізуге арналған серверлерді (VPN) пайдаланбаған жағдайда компьютерлік құрылғының нақты орналасқан жерін көрсететін іздер жатады. Мұндай іздер байланыс операторларының базалық станцияларында, сондай-ақ қылмыскерге интернетке кіруді қамтамасыз ететін провайдерлердің серверлерінде болады.

Үшінші топқа қылмыс жасаған тұлғаның биологиялық, әлеуметтік және психологиялық қасиеттерін диагностикалауға мүмкіндік беретін іздер кіреді.

Бұларға, мысалы, мыналар жатады:

– слиптерде, чектерде, SIM-картада, мобильді телефонда қалған қол саусақтарының іздері (дактилоскопиялық сараптама);

– ұялы байланыс операторында сақталатын алаяқтың дауысының жазбасы (фоноскопиялық сараптама);

– сөйлеу іздері бар файлдар (лингвистикалық сараптама).

Біз бөліп көрсеткен із топтарын анықтау – қылмыскерді анықтауға бағытталған тергеуші қызметінің негізгі мақсаты болып табылады. Ал осы мақсатқа сәтті қол жеткізуді біз қашықтан жасалатын алаяқтықты тергеудің жалпы жүйесінде мұндай іздерді іздеу, табу және зерттеу бойынша тергеушінің іс-әрекеттерінің криминалистикалық алгоритмін әзірлеумен байланыстырамыз.

Қарастырылған жіктеме тікелей процестік мәнге ие, өйткені іздің түрі оны тіркеп-белгілеудің, зерттеудің және кейіннен дәлелдеу процесінде пайдаланудың ерекшелігін қатаң детерминациялайды.

Қарастырылып отырған типтік іздестіру жағдаяттарын шешу үшін тергеушіге ең алдымен қылмыскер туралы криминалистикалық мәні бар ақпарат көздерін айқындау қажет. Негізгі тұжырымдарды келесідей түрде қалыптастыруға болады:

1) қылмыскердің тұлғасын анықтауға бағытталған тергеушінің әрекеттері, ең алдымен, оның тұлғасы туралы, сол тұлға қалдырған іздерде көрініс тапқан ақпаратты іздеу мен алуға бағытталады. Осыған байланысты мұндай әрекеттер алгоритмдерін әзірлеу техникасының маңызды құрамдас бөлігі – қайда және қандай іздер пайда болатыны туралы, соның ішінде ақпараттық ортадағы іздер туралы білім алу.

2) қашықтан жасалатын алаяқтықты жасаған тұлғаны анықтауға жәрдемдесетін іздердің қалыптасу механизмі – қылмыскердің әрекеттері, оның белгілері мен қасиеттерінің ақпараттық ортада заңды түрде бейнелену процесі болып табылады.

3) қашықтан жасалатын алаяқтықты жасаған тұлға туралы ақпарат жинауға мүмкіндік беретін іздерді үш топқа бөлуге болады:

– қылмыскердің тұлғасын анықтауға жәрдемдесетін іздер;

– қылмыскердің орналасқан жерін анықтауға жәрдемдесетін іздер;

– қылмыскердің тұлғасының белгілері мен қасиеттері туралы диагностикалық ақпарат алуға жәрдемдесетін іздер.

Ю.В. Гаврилин негізді түрде көрсеткендей, материалдық цифрлық іздерді анықтау, алып қою және процестік бекіту арнайы білімді қолданусыз және компьютерлік-техникалық сараптамаларды міндетті түрде жүргізусіз объективті түрде мүмкін емес, бұл олардың гиперқұбылмалылығымен және рұқсатсыз модификациялануға аса осалдығымен шартталған [75, 97 б.]. Оларға қарағанда, жәбірленушінің санасында алдау көрінісін қалыптастыратын идеалды іздер тергеушінің жауап алу және тактикалық қызметінің іргелі негізін құрайды. Бұл ойды дамыта отырып, А.Д. Фокин идеалды іздермен жұмыс істеу құқық қолданушыдан құрбанның когнитивтік бұрмалануларын еңсеру және қашықтан вербалды немесе мәтіндік байланысты егжей-тегжейлі реконструкциялау үшін заң психологиясы мен психиатриясының әдістерін (арнайы білімді) пайдалануды талап ететінін атап өтеді [41, 163 б.]. Ал гибридті іздердің болуы алып қойылған цифрлық артефактінің техникалық объективтілігін және желіде нақты құқыққа қарсы манипуляцияларды жүзеге асырған адамның субъективті еркін синхронды бағалауды талап ететін дәлелдеудің кешенді сипатын алдын ала айқындайды.

Баяндалғандар трасологиялық өлшемшарт саралаудың жай ғана теориялық негізі ретінде әрекет етпей, онлайн алаяқтықтың жіктемесі мен қылмыстық-процестік дәлелдеудің практикалық тетігі арасындағы ажырамас байланысты қамтамасыз ететінін атап өтуге мүмкіндік береді. Ақпараттық-коммуникациялық технологиялардың ықпалымен із ұғымының трансформациялануы құқық қолданушыдан дәлелдемелік базаны қалыптастыру кезінде цифрлық ортаның ерекшелігін терең түсінуді талап етеді. Өз кезегінде, із қалыптасудың анықталған заңдылықтары істердің осы санатына тән латенттілікпен, экстерриториялылықпен және іс-әрекет жасау ортасының жоғары техногенділігімен ажырамас ұштасқан, бұл зерттеліп отырған феноменді сотқа дейінгі тергеп-тексерудің жалпы процестік мәні бар сипаттамаларын жүйелеуге көшудің логикалық қажеттілігін туындатады.

Онлайн алаяқтықтың трасологиялық негізін зерттеу логикалық түрде сотқа дейінгі тергеп-тексерудің өзгешелігін айқындайтын, процестік мәні бар

белгілерін жүйелеуді талап етеді. Мұнда бірінші орынға қылмыстық әрекеттің айқын техногендік сипаты шығады, ал ол дәлелдемелік базаны жедел тіркеп-белгілеу қажеттілігінен бөліп қарауға келмейді. Е.С. Шевченко байқағандай, компьютерлік ақпараттың құбылмалылығы дереу процестік әрекет етуді талап етеді, себебі кез келген кідіріс криминалистикалық маңызы бар деректердің қайтарымсыз жойылуына апарады [59, 107 б.]. Осы ойды өрбіте отырып, А.Г. Волеводз әрекеттің техногендік табиғаты тергеп-тексерудің бастапқы сатысын түбегейлі өзгертетінін атап көрсетеді: қылмыс туралы хабарламаны дәстүрлі тексеру қылмыстық істі ресми қозғау сәтіне дейін цифрлық артефактілерді сақтау жөніндегі шұғыл шараларға орнын береді [76, 176 б.]. Өз кезегінде, В.Д. Курушин мен В.А. Минаев техногендік деректерді процестік бекіту мамандарды міндетті және кідіріссіз тартуды талап ететінін, ал бұл жұмыстың алғашқы сағаттарының өзінде жедел-тергеу тобының іс-әрекеттерін үйлестіруді күрделендіретінін негізді түрде көрсетеді [77, 156 б.]. Келтірілген ұстанымдарды салыстыру техногенділік пен жедел тіркеп-белгілеу императиві құқық қолданушыдан қылмыстық процесті инициациялау кезеңінде ақпараттық тапшылықты еңсерудің стандартты емес алгоритмдерін қолдануды талап ете отырып, дәлелдеу акцентін вербалды көздерден (жауап алулардан) цифрлық ортаны процестік бекітуге ауыстыратыны туралы қорытынды жасауға мүмкіндік береді.

Технологиялық ерекшеліктің салдары ретінде бұл жағдайда криминологиялық емес, таза процестік құбылыс ретінде қарастырылатын латенттіліктің бұрын-соңды болмаған деңгейін қалыптастыратын субъектілердің процестік анонимділігі әрекет етеді. А.Л. Осипенконың пікірінше, қылмыскерлердің IP-адрестерді жасыру құралдарын, шифрлауды және анонимді төлем жүйелерін пайдалануы күдіктінің жеке басын анықтауды аса күрделі техникалық-заңдық міндетке айналдыра отырып, дәлелдеудің классикалық тетігін тұралатады [78, 21-22 б.]. Бұл тезис процестік латенттілік қылмыстық іс қозғау сатысынан айып тағуға көшудің мүмкін еместігінен көрініс табатынын, соның нәтижесінде істердің абсолютті көпшілігі айыпталушы ретінде жауапқа тартылуға жататын адамның анықталмауына байланысты тоқтатыла тұратынын тұжырымдайтын В.А. Машлякевичтің ұстанымымен толықтырылады [79, 21 б.]. Латенттілік жәбірленушінің қылмыс туралы мәлімдеуге құлықсыздығымен байланысты болатын дәстүрлі жымқыруларға қарағанда, онлайн алаяқтықтың процестік латенттілігі сотқа дейінгі тергеп-тексеру органы анонимделген инфрақұрылыммен бетпе-бет келіп, өзінің процестік инструментарийін сарқатын тығырыққа тірелген тергеу жағдайларымен детерминацияланған. Бұдан анонимділік нәтижелерін көбінесе қылмыстық-процестік заңнаманың қатаң нормалары шеңберінде заңдастыру қиынға соғатын ұзаққа созылатын және ресурсты көп қажет ететін жасырын тергеу әрекеттері мен жедел-іздестіру іс-шараларын жүргізуді талап ете отырып, дәлелдеу процесін түбегейлі трансформациялайтыны шығады.

Аталған процестік кедергілер аумақтық тергеулілік пен үйлестірудің дәстүрлі қағидаттарын бұзатын онлайн алаяқтықтың трансшекаралық сипатымен еселеп күшейеді. К.О. Карабеков атап өткендей, цифрлық қол сұғушылықтардың

экстерриториялылығы салдарлардың туындау орны, қылмыскердің орналасқан жері және дәлелдемелік ақпараты бар серверлердің орналасу юрисдикциясы арасындағы кеңістіктік алшақтыққа әкеп соғады [17, 143 б.]. Аталған проблеманы нақтылай отырып, М.В. Жижина мен Д.В. Завьялова рәсімдік асимметрияға негізді түрде назар аударады: ұлттық заңда бекітілген сотқа дейінгі тергеп-тексерудің процестік мерзімдері құқықтық көмек туралы халықаралық сұрау салуларды орындаудың ұзақтығымен еңсерілмейтін қайшылыққа түседі, бұл тергеушілерді іс бойынша іс жүргізуді тоқтата тұруға объективті түрде мәжбүрлейді [80, 108 б.]. Осы тәсілдерді талдау трансшекаралық сипаттың тергеп-тексеруді жай ғана күрделендіріп қоймай, ведомствоаралық және мемлекетаралық өзара іс-қимылдың қағидатты түрде жаңа тетіктерін қалыптастыруды, үйлестіруді бюрократиялық жазықтықтан Интерпол арналары мен мамандандырылған халықаралық платформалар арқылы цифрлық деректермен жедел алмасу форматына көшіруді талап ететінін көрсетеді, ал бұл қазіргі сәтте процестік тұрғыдан әлсіз реттелген.

Аталған сипаттамаларды жүйелеу негізінде техногенділік, жедел тіркеп-белгілеу қажеттілігі, анонимділік, латенттілік және трансшекаралық сипат жиынтығы онлайн алаяқтықты тергеп-тексерудің тұрақты жоғары процестік күрделілік деңгейін қалыптастыратыны туралы авторлық тәсілді негіздеуді қажет деп санаймыз. Қылмыстық процесті ұйымдастыруды оңтайландыру мақсатында осындай іс-әрекеттерді тергеп-тексеру күрделілігін рангілік бағалауды енгізу ұсынылады:

– процестік күрделіліктің төмен деңгейі дәлелдемелерді жинау байланыс операторларына стандартты сұрау салулармен қамтамасыз етілетін базалық телекоммуникациялық құралдарды (мысалы, телефон арқылы алдаудың қарапайым нысандары) пайдалана отырып, бір ұлттық юрисдикция шегінде жалғыз қылмыскердің іс-әрекет жасауымен сипатталады;

– күрделіліктің орташа деңгейі кешенді сараптамаларды тағайындауды және ұзаққа созылатын жасырын тергеу әрекеттерін жүргізуді талап ететін, анонимдеу құралдарын ішінара қолдана отырып, ел ішінде адамдардың үлестірілген тобы жасаған іс-әрекеттерге беріледі;

– процестік күрделіліктің жоғары деңгейі халықаралық құқықтық көмек рәсімдерін бастауды талап ететін, терең шифрлауды, криптовалюталық транзакцияларды және шетелдік серверлік инфрақұрылымды пайдалана отырып, трансұлттық ұйымдасқан құрылымдар іске асыратын алаяқтықтарға имманентті түрде тән. Тиісінше, күрделіліктің жоғары деңгейіне жатқызылған қылмыстық істер процестік параличке байланысты іс жүргізуді тоқтата тұрудың және жәбірленушілерге материалдық залалды өтеу мүмкін еместігінің барынша жоғары ықтималдығымен сипатталатын ерекше тәуекел тобын қалыптастырады.

Онлайн алаяқтықтың анықталған қасиеттері классикалық процестік нысанның тиімділігіне күмән келтіретін жүйелі сипаттағы сын-қатерлерді туындататынын атап өту керек. Зерттеліп отырған іс-әрекеттің процестік мәні бар сипаттамалары сотқа дейінгі іс жүргізудің жекелеген кезеңдерін жай ғана қиындатып қоймай, дәлелдемелерді жинау алгоритмдерін тұжырымдамалық түрде қайта қарауды, арнайы білімді пайдалану шектерін кеңейтуді және өзара

іс-қимыл институттарын жаңғыртуды талап етеді. Іс-әрекеттің технологиялық, құрылымдық, кеңістіктік және криминалистикалық ерекшеліктерінің тығыз астасуымен шартталған тергеп-тексерудің дәлелденген көп факторлы күрделілігі бұған дейін қарастырылған барлық өлшемшарттарды бірыңғай жүйеге біріктіруге деген объективті қажеттілікті туындатады. Бұл логикалық түрде онлайн алаяқтықты жіктеудің интегративті моделін қалыптастыру және осы тармақшаның қорытынды тұжырымы шеңберінде зерттеудің жалпы қорытындыларын шығару қажеттілігін алдын ала айқындайды.

Технологиялық, объектілік, құрылымдық және трасологиялық өлшемшарттарды жеке-жеке талдаудың табиғи қорытындысы – зерттеліп отырған құбылыс жайлы тұтас ғылыми түсінік құру үшін оларды бір жүйеге біріктіру қажеттігі. А.Ю. Головин байқағандай, базалық криминалистикалық жіктемелер бірыңғай әдіснамалық мақсатқа бағынып, қылмыстық әрекеттің ішкі заңдылықтарын ашқанда ғана толыққанды білім жүйесіне айналады [53, 33 б.]. Осы ойды өрбіте отырып, В.А. Мещеряков цифрлық қол сұғушылықта ақпараттық орта қол сұғушылық затын, құрал-жабдықты және қалатын іздерді бір-бірінен ажыратпай тұтастырып, бірыңғай теориялық конструкт құруды талап ететінін атап өтеді [55, 66 б.]. Д.Ю. Гостевский өз тарапынан мұндай криминалистикалық модельдеу дәлелдеудің процестік шектеулерін ескеруге міндетті екенін, олай болмаса модельдің құқық қолданушы үшін қолданбалы құны түгел жойылатынын негіздейді [81, 46 б.]. Келтірілген ұстанымдарды салыстыру онлайн алаяқтықты жіктеу объективті түрде көп факторлы сипатқа ие екендігі және технологиялық, объектілік, құрылымдық және трасологиялық элементтерді қамтитын тығыз өзара байланысты жүйені білдіретіні туралы қорытынды жасауға мүмкіндік береді. Осы интегративті модель шеңберінде қатаң детерминация байқалады: технологиялық инструментарий виртуалды объектіні таңдауды айқындайды, бұл криминалдық топтың тиісті үлестірілген құрылымын қалыптастыруды талап етеді, ал ол өз кезегінде ерекше электрондық-цифрлық іздік көріністі генерациялайды.

Құбылыстың дәлелденген жүйелілігін ескере отырып, ұсынылып отырған тәсілдің ғылыми жаңалығы криминалистикалық алгоритмдер мен процестік тетіктердің органикалық интеграциясын қамтамасыз ететін көп факторлы жіктемелік модельді әзірлеуде жатыр. Оның үстіне, ұлттық мәнмәтіндегі қазіргі заманғы киберқатерлердің латенттілігі мен трансшекаралық сипатының жоғары деңгейі туралы К.О. Карабековтың зерттеулеріне сүйене отырып [17, 144 б.], ұсынылған модельге тергеп-тексерудің процестік күрделілігін бағалауды енгізу ғылыми жаңалықтың қағидатты маңызды элементі ретінде әрекет етеді. Осы күрделіліктің деңгейі жіктемелік факторлардың комбинациясына (мысалы, үлестірілген құрылымды трансшекаралық серверлік инфрақұрылыммен ұштастыра пайдалану) тікелей тәуелді болады және сотқа дейінгі іс жүргізудің тактикалық-ұйымдастырушылық алгоритмдерін таңдауды алдын ала айқындайды. Бұл авторлық жіктеме жоғары практикалық маңызға ие: ол цифрлық қол сұғушылықтарды саралау кезінде пайдаланылуы мүмкін, сондай-ақ сотқа дейінгі тергеп-тексеру органдарына бастапқы ақпаратты тексеру сатысының өзінде ықтимал тәуекелдер мен ресурстық шығындарды дәл

болжауға мүмкіндік бере отырып, тергеу практикасы үшін ұсынылады.

Процестік күрделілік өлшемшартымен толықтырылған осы интегративті жіктемелік модель сотқа дейінгі тергеп-тексеру проблемаларын зерттеуге әрі құқық қолдану практикасын жетілдіруге сенімді әдіснамалық тірек болады. Ал цифрлық децепцияның жіктемелік белгілерін жүйелі түрде түсіну онлайн алаяқтық пен дәстүрлі алаяқтықты тереңдеп, салыстырмалы-құқықтық және процестік тұрғыдан талдауды қажет етеді – бұл криминалдық тетіктің қаншалықты өзгергенін нақты өлшеп көрсету үшін керек.

1.3 Онлайн алаяқтық пен дәстүрлі алаяқтық түрлерінің салыстырмалы-құқықтық және процессуалдық талдауы

Онлайн алаяқтықтың мәнін гибридті табиғаттағы оқшау феномен ретінде айқындау және оның белгілерін көп факторлы жіктемелік модель аясында жүйелеу – зерттеудің алғашқы кезеңінде атқарылған істер – ғылыми танымды келесі сатыға, салыстырмалы талдауға көшуді теориялық-әдіснамалық тұрғыдан қажет етеді. Н.А. Лопашенко орынды ескерткендей, мүліктік қол сұғушылықтың өзгеріп келе жатқан түрлерін бағалағанда мәселені инциденттердің сандық өсуіне ғана теліп, оны әрекет жасалатын сыртқы ортаның ауысуын тіркеумен шектеуге болмайды [82, 600 б.]. Бұл ұстаным Е.А. Русскевичтің көзқарасымен белгілі бір ғылыми айтысқа түседі: соңғысы, керісінше, ақпараттық-коммуникациялық технологиялар енгізілген жағдайда криминалдық мінез-құлық парадигмасының өзі түбегейлі сапалық өзгеріске ұшырайтынын, ал бұған құқықтық баға беру үшін мүлдем жаңа әдіснамалық құрал керек екенін алға тартады [83, 12-14 б.]. Осы екі көзқарасты салыстырғанда мынадай қорытынды туады: зерттеліп отырған киберкриминалдық құбылыстың шынайы табиғатын ашу үшін салыстырмалы тәсіл сөзсіз қажет, бірақ ол сипаттамалық белгілерді формальды түрде қатар қоюға емес, дәстүрлі және онлайн алаяқтық арасындағы терең сапалық айырмашылықтарды анықтауға бағытталуға тиіс.

Бұл әдіснамалық міндетті орындау қылмыс құрамының категориялық аппаратына және негізгі қылмыстық-процестік институттарға сүйене отырып, салыстыру объектілері мен өлшемшарттарын нақты айқындауды талап етеді. П.А. Гоибназарзоданың пайымынша, пәнаралық компаративистік әдіснама құқықтық жүйелердің цифрландыру сын-қатерлеріне сәйкестігін бағалауға және құқық қолданудағы догматикалық қалыптарды еңсеруге қолайлы құрал [25, 216 б.]. Сондықтан салыстырмалы талдауды өзара байланысты үш вектор бойынша құрған орынды әрі қисынды.

Біріншіден, материалдық-құқықтық аспект объектінің, объективті және субъективті жақтардың мазмұндық өзгеруін бағалау мақсатында алаяқтықтың дәстүрлі құрамы мен оның цифрлық туындыларын салыстыруды көздейді.

Екіншіден, процестік-құқықтық аспект материалдық жеткізгіштерге негізделген сотқа дейінгі тергеп-тексерудің классикалық үлгісі мен қазіргі цифрлық дәлелдеу үлгісін сыни тұрғыдан қатар қоюды қажет етеді.

Үшіншіден, халықаралық-құқықтық аспект ұлттық құқық қолдану аясы мен киберқылмыстың жаһандық сипатын ескеретін озық шетелдік тәсілдердің

арақатынасын талдауды талап етеді.

Осы өлшемшарттарды біріктіру зерттеудің аталған кезеңіндегі негізгі гипотезаны ұсынып, кейіннен тексеруге сенімді әдіснамалық негіз болады. Гипотеза мынаған саяды: онлайн алаяқтық алаяқтықтың материалдық-құқықтық құрылымын да, оны тергеп-тексерудің процестік үлгісін де жүйелі түрде өзгертеді. Басқаша айтқанда, криминалдық децепцияны виртуалды ортаға көшіру бір типті эпизодтардың санын көбейтіп қана қоймайды, ол із қалыптасу тетігі мен пиғылды іске асыру тәсілінде іргелі сапалық өзгеріс туғызады, ал бұл дәстүрлі тергеу алгоритмдерін цифрлық деликтілерге қолданудың объективті тиімсіздігін алдын ала айқындайды.

Практикада бұл эпизодтардың сандық жинақталуы айыптау деконструкциясының тұрақты прецедентін қалыптастыра отырып, заңды процестік тетіктермен оңай бұзылады. Сериялық кибержымқыруларды тергеп-тексеру кезінде бірінші эпизод бойынша кінәлі адамның жәбірленушімен татуласуы (ҚР ҚК-нің 68-бабының 1-бөлігі негізінде) оны тоқтатуға автоматты түрде әкеп соғады, бұл барлық кейінгі эпизодтар үшін «бірнеше рет жасалу» саралаушы белгісін алгоритмдік түрде жояды. Мәселен, қылмыстық іс бойынша (№1-577/2022 қылмыстық ісі бойынша ШҚО Өскемен қаласы №2 сотының 2022 жылғы 08 желтоқсандағы үкімі) [84] жәбірленуші микроқаржы ұйымдарының бірімен татуласуына байланысты соттың бірнеше рет жасалу белгісін алып тастауға және неғұрлым жеңіл жаза тағайындай отырып, сотталушының әрекеттерін ҚР ҚК-нің 190-бабы 3-бөлігінің 4-тармағынан 2-бөлігінің 4-тармағына қайта саралауға міндетті болғаны анықталды. Тергеудің бастапқы саралауын бұзатын бірдей процестік редукция №7560-21-00-1/25 (Алматы қаласы Жетісу ауданының №2 аудандық сотының 2021 жылғы 24 ақпандағы үкімі) [85] және №7141-25-00-1/1908 қылмыстық ісі бойынша (Астана қаласының Қылмыстық істер жөніндегі ауданаралық сотының 2025 жылғы 05 қыркүйектегі үкімі) [49] істері бойынша тіркеп-белгіленген.

Ұсынылған теориялық-әдіснамалық негіздер және құқықтық болмыстың трансформациялануының көп деңгейлі сипатын негіздеу мәлімделген компаративтік тәсілді тікелей іске асыруға көшуге мүмкіндік береді. Аталған жайт виртуалды өзара іс-қимыл жағдайында олардың материалдық-құқықтық табиғатының өзгеруінің нақты ерекшелігін анықтау үшін дәстүрлі және цифрлық алаяқтық модельдеріндегі қылмыс құрамының элементтеріне бірінші кезекте салыстырмалы-құқықтық талдау жасаудың объективті логикалық қажеттілігін туындатады.

Дәстүрлі және цифрлық алаяқтық модельдеріне салыстырмалы-құқықтық талдау жасау олардың құқықтық табиғатының сапалық айырмашылықтарын анықтау үшін қажетті әдіснамалық кезең ретінде әрекет етеді. Аталған нысандарды салыстыруды ақпараттық қоғам жағдайында тұжырымдамалық күрделенуге ұшырайтын қылмыстық қол сұғушылық объектісінен бастау қисынды. А.В. Шульга атап өткендей, дәстүрлі парадигма шеңберінде классикалық материалдық тауар алмасу жазықтығында іске асырылатын тек мүліктік қатынастар ғана алаяқтық объектісі ретінде әрекет етеді [86, 11 б.]. Сонымен қатар М.А. Ефремова мүліктік мүдделер ақпараттық қауіпсіздік пен

телекоммуникациялық жүйелердің орнықтылығын қамтамасыз ету жөніндегі қатынастармен ажырамас түрде бірігетіндіктен, цифрлық ортада кешенді, көп деңгейлі объект қалыптасатынын негізді түрде көрсете отырып, киберқолсұғушылықтарды бағалауға өзге тәсілді ұсынады [31, 13 б.]. Осы ұстанымдарды салыстыру объект бөлігіндегі модельдер арасындағы айырмашылық сандық емес, қатаң сапалық сипатқа ие деген қорытынды жасауға мүмкіндік береді: іс-әрекеттің базалық мүліктік табиғаты бұзылмай, құқықтық қорғаудың гибридті нысанына ие болатын цифрлық экономикалық қатынастар элементтерін қосу есебінен объектінің органикалық кеңеюі орын алады.

Объектінің сапалық жағынан өзгеруі қылмыстың объективті жағындағы түбегейлі айырмашылықтарды заңды түрде айқындайды. А.Г. Безверховтың пікірінше, алаяқтықтың дәстүрлі моделі классикалық алдауға сүйенеді: мұнда мүлік тікелей беріледі, ал кінәлі мен құрбанның арасындағы тікелей тұлғааралық физикалық байланыс міндетті шарт саналады [87, 117 б.]. В.В. Хилюта бұған қарама-қарсы жағдайды көрсетеді: цифрландыру тұсында физикалық байланыстан мүлде бас тартылады, ал алдаудың өзі ақпараттық-коммуникациялық технологиялар арқылы жанама әсер ету түріне көшеді [88, 62 б.]. Осыдан объективті жақтың құқықтық табиғаты түбегейлі өзгереді деген қорытынды шығады. «Байланыс → мүлікті беру» классикалық парадигмасын енді екі жаңа цифрлық модель алмастырады. Алғашқысы – «қашықтан әсер ету → өз бетінше беру»: мұнда құрбан әлеуметтік инженерияның ықпалына түсіп, транзакцияны өз қолымен жасайды. Екіншісі – «деректерді жасырын жинау → құпия түрде инициациялау»: бұл жолы қаскүнемнің әрекеті жәбірленушінің активін беруге саналы келісімін мүлде қажет етпейді, керісінше, тікелей ақпараттық жүйелердің биометриялық және скорингтік алгоритмдеріне бағытталады.

Қылмыс субъектісін салыстырмалы талдау кезінде осыған ұқсас сапалық трансформация байқалады. А.С. Камко атап өткендей, егер дәстүрлі алаяқтық жәбірленушімен тікелей жеке байланысқа түсетін жеке субъектілермен немесе оқшауланған топтармен сипатталса, телекоммуникациялық және компьютерлік технологияларды қолдану бұл жеке (физикалық) байланыс қажеттілігін жояды; бұл өз кезегінде қашықтан әрекет ететін сыбайластарды іріктеу мүмкіндігін арттырып, олардың жаңа үлгідегі қылмыстық топтарға бірігуіне әкеп соғады [36, 78 б.]. Цифрлық ортаның ерекшелігін нақтылай отырып, бірқатар авторлар жымқырулардың онлайн-нысандары орындаушылары аумақтық жағынан алшақтатылған және жеке таныс емес үлестірілген құрылым арқылы іске асырылатынын атап көрсетеді. Алайда, эмпирикалық базаны талдауға негізделе отырып, авторлық ұстанымды негіздеген жөн: қазіргі заманғы онлайн алаяқтықта жай ғана «үлестірілген» емес, гибридті (офлайн-онлайн) субъектілік құрам қалыптасады. Банктік биометриялық қорғау жүйелерінің күшейтілуі анонимді киберұйымдастырушыларды цифрлық құралдарды дәстүрлі контактілі сыбайлас қатысу әдістерімен біріктіре отырып, құрбандармен тікелей физикалық байланысқа түсу үшін жергілікті сыбайлас қатысушыларды тартуға мәжбүрлейді.

Рөлдердің осылай өзгеруінің айқын мысалы – №3528-23-00-1/20 көп

эпизодты қылмыстық іс (Қарағанды облысы Шахтинск қалалық сотының 2023 жылғы 11 маусымдағы үкімі) [48]. Сот сыбайлас қатысудың күрделі тізбегін анықтаған: бір кінәлі (күзет ұйымының бастығы) өзіне бағынышты адамдардың ЖСН мен байланыс деректерін заңсыз жинау үшін қызмет бабын пайдаланған. Кейін қылмыстық топтың басқа мүшелері (бірлесіп орындаушылар) жәбірленушілерге барып, өздерін «Қазпошта» жеткізу қызметінің қызметкеріміз (тапсырыс хат табыстау сылтауымен) не медицина қызметкеріміз («Ashyq» қосымшасында мәртебе жаңарту үшін) деп таныстырған да, міндетті бейнетіркеу деген желеумен олардың бет-әлпетін сканерлеген. Ал шын мәнінде дәл сол сәтте қаскүнемдер бөгденің интернет-банкингін өз құрылғыларына байлап, өз смартфондарындағы банк қосымшаларында биометриялық аутентификациядан өткен. Құрбандардың шоттарына түгел қол жеткізген соң, олардың атына көп миллиондық тауар және ақша қарыздарын еш кедергісіз ресімдеп алған. Мұндай тәжірибе кибертоптардың құрамында «дерек жеткізушілер» мен «контактілі инженерлер» тәрізді бөлек рөлдердің пайда болғанын айғақтайды. Бұл күрделену қылмыстық құқықтағы сыбайлас қатысудың классикалық догматикалық құрылымын бұзбайды, қайта әрекеттердің бірлескендігі мен келісілгендігі белгілерін қашықтан, анонимді өзара әрекеттесу жағдайына бейімдеу арқылы оны сапалық жағынан түрлендіреді.

Қашықтық сипат пен технологиялық жанамалық, өз кезегінде, іс-әрекеттің субъективті жағында да айқын із қалдырады. Н.А. Лопашенко байқағандай, классикалық алаяқтықта тікелей пиғыл нақты бір адамды алдауға бағытталады әрі тікелей психологиялық үстемдік арқылы жүзеге асады [89, 217 б.]. Осы қырды киберқылмыс тұрғысынан өрбіте отырып, Д.В. Завьялова цифрлық ортада пиғыл жанама әрі технологиялық негізде қалыптасатынын түйіндейді: кінәлі өз әрекетінің алгоритмдік сипатын алдын ала түсінеді және әлеуетті құрбандарды жаппай, тұлғасыз түрде іздеу үшін автоматтандырылған жүйелерді әдейі іске қосады [90, 64 б.]. Демек, онлайн алаяқтықта пиғылдың зияткерлік және еріктік элементтері сапалық жағынан өзгереді: оларға пайдакүнемдік мақсат қана емес, өз тұлғасын жасыратын цифрлық ортаны технологиялық тосқауыл ретінде пайдалану ниеті де қосылады.

Қылмыс құрамы элементтерінен байқалған осы сапалық айырмашылықтар қолданыстағы ҚР ҚК аясында саралаудың елеулі өзгешелігін туғызбай қоймайды. А.Б. Курумбаева мен Б.Б. Кощегулов жымқыру жөніндегі классикалық нормаларды технологиялық мәнмәтінсіз қолдану мүмкін емес екенін негіздейді: сондықтан іс-әрекетке заманауи құқықтық баға беру (атап айтқанда, ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағы бойынша – ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану арқылы) құқыққа сыймсыз алып қою фактісін де, цифрлық инфрақұрылымға әсер ету ерекшелігін де қамтитын кешенді саралауды қажет етеді [21, 49 б.]. Мұның өзі цифрлық орта қылмыстық заң нормаларын қолдануға тікелей ықпал ететінін, іс-әрекетке заңдық баға бергенде виртуалды элементтерді міндетті түрде ескеру керектігін көрсетеді.

Салыстырмалы-құқықтық талдауды түйіндегенде, цифрландыру жағдайында алаяқтықтың құқықтық табиғаты сапалық тұрғыдан түбегейлі

өзгеретінін атаған жөн. Физикалық байланыс пен тікелей алып қоюға сүйенетін дәстүрлі жеке-материалдық үлгіден жүйелі-виртуалды парадигмаға заңды көшу жүріп жатыр, ал бұл парадигма қол сұғушылықтың кешенді объектісімен, виртуалды децепциямен, субъектінің үлестірілген құрылымымен және технологиялық жанамаланған пиғылмен ерекшеленеді. Іс-әрекеттің материалдық-құқықтық құрылымының осылай жүйелі өзгергені дәлелденген соң, процестік дәлелдеуде тек классикалық әдістерге сүйенудің тиімсіз екені айқындалады; нақ осы жайт процестік-құқықтық талдауға және онлайн алаяқтықты сотқа дейінгі тергеп-тексеру үлгісінің іргелі өзгеруін зерттеуге көшуді алдын ала қажет етеді.

Алаяқтықтың бұрын айқындалған материалдық-құқықтық табиғаты сапалық жағынан өзгерген соң, оны сотқа дейінгі тергеп-тексерудің дәстүрлі және цифрлық үлгілерін салыстыру сөзсіз қажет болады – тек осылай процестік құрылымның мәндік өзгерістерін көруге болады. Салыстыруды іс жүргізуді бастау себептері мен негіздерінен өрбіткен қисынды, өйткені нақ осы тұс түбегейлі өзгеріске ұшырайды. Дәстүрлі тергеп-тексеру үлгісі тарихи тұрғыдан іс жүргізуді бастаудың классикалық түрлеріне – жәбірленушінің жеке арызына не кінәні мойындап келуге – сүйенеді, мұнда бастапқы ақпарат физикалық өзара әрекетке тікелей қатысқан адамдардан келеді. Осыны бүгінгі жағдаймен салғастыра келіп, Р.Б. Джилкишиев жаңа цифрлық ортада қылмысты анықтау тетігі электрондық өтініштерге, ақпараттық жүйелер деректерін автоматтандырылған талдауға және желілік транзакцияларды мониторингтеуге қарай ойысатынын негіздейді [57, 102 б.]. Бұл көзқарас В.В. Коломиновтың зерттеулерінде жалғасын табады: ол киберқылмысты тергеудің бастапқы сатысында алдын ала түсетін цифрлық ақпараттың рөлі көбіне жәбірленушілердің посткриминалдық арыздарынан асып түсетінін көрсетеді, себебі құрбандар қаражаттың қашықтан есептен шығарылған сәтін тіпті аңғармай қалады [91, 178 б.]. Демек, онлайн алаяқтықты анықтау тетігі сапалық жағынан өзгереді әрі сотқа дейінгі іс жүргізу ресми басталғанға дейін цифрлық ақпаратты проактивті жинаудың процестік маңызын еселеп арттырады.

Іс жүргізуді бастау сатысындағы екпіннің ауысуы дәлелдемелік база табиғатының өзгеруімен тікелей байланысты: мұнда дәстүрлі материалдық жеткізгіштердің орнын цифрлық деректер басады. В.Е. Пономарев көрсеткендей, классикалық заттай дәлелдемелер физикалық тұрақтылығымен әрі қолмен ұстауға келетіндігімен ерекшеленеді, ал цифрлық ақпарат, керісінше, аса тұрақсыз, оңай құбылмалы әрі қашықтан бір сәтте өзгертілуі не жойылуы мүмкін [71, 98 б.]. Осы ойды нақтылай отырып, С.В. Зуев пен А.И. Зазулин цифрлық деректердің өзгешелігі оларды процестік тіркеп-белгілеудің дербес – «цифрлық фиксация» деп аталатын – әдістерін жасауды талап ететінін түйіндейді, өйткені мұндай әдіс бастапқы кодтың болмашы да болса бұрмалануына жол бермеуге тиіс. Авторлардың пайымынша, ол дәстүрлі бейнежазба мен фотосуреттен өзгеше, себебі ақпаратты бинарлық код деңгейінде хэш-сома арқылы бекітуге негізделеді [92, 85 б.]. Ал осы доктриналық талаптарды қолданыстағы ҚР ҚПК нормаларымен салыстырғанда өткір мәселе ашылады: отандық заңнама цифрлық дәлелдемелерді әлі күнге «өзге де құжаттар» не материалдық объектілердің

ескірген санаттарына жасанды түрде сыйғызып келеді, ал бұл олардың жеткіліксіз реттелгенін көрсетеді әрі шынайы виртуалды онтологиясын бейнелемейді.

Аталған нормативтік вакуум зерттеу объектісі физикалық кеңістіктен ақпараттық жүйеге ауысатын тергеу әрекеттерін жүргізу кезінде барынша айқын көрініс табады. Е.С. Шевченконың пікірінше, материалдық жағдайды визуалды тексеруге бағдарланған дәстүрлі тактика (мысалы, оқиға орнын классикалық қарап-тексеру) криминалистикалық маңызы бар ақпарат қашықтағы серверлер мен бұлтты қоймаларда үлестірілген киберкеңістікте мүлдем тиімсіз болып шығады [59, 133 б.]. Ғылыми пікірталасты дамыта отырып, Ю.В. Гаврилин мен А.В. Победкин құқық қолданушылардың ескі процестік нысандарды цифрлық ортаны зерттеуге бейімдеу әрекеттері желілік өзара іс-қимыл динамикасы мен деректерді криптографиялық қорғауды ескермейтін процестік нормалардың толық бейімделмегенін ашып көрсететініне назар аударады [93, 110 б.]. Демек, жай ғана техникалық жаңғыртуды емес, цифрлық ортаны зерттеуге бағытталған тергеу әрекеттерінің регламентациясын тұжырымдамалық түрде қайта қарауды талап ететін тергеу қарап-тексеруі объектісінің өзінің іргелі трансформациясы орын алады.

Тергеу әрекеттерімен қатар, тергеп-тексеруді жедел-іздестіру және сараптамалық сүйемелдеу тетіктері де сапалық трансформацияға ұшырайды. Физикалық байқау мен контактілі жұмысқа негізделген дәстүрлі жедел-іздестіру іс-шаралары, А.Л. Осипенко негізді түрде атап өткендей, тиімділігі қолданылатын техникалық құралдарға (трафикті талдау жүйелеріне) және телекоммуникациялық провайдерлермен ведомствоаралық өзара іс-қимылдың жеделдігіне тікелей, сыни тәуелділікте болатын цифрлық коммуникацияларды жоғары технологиялық бақылаумен алмастырылады [94, 275 б.]. Сонымен қатар Е.Р. Россинская сараптамалық қамтамасыз етудің терең эволюциясын атап көрсетеді: классикалық дәстүрлі сараптамалардың орнына аппараттық-бағдарламалық кешендердің, деректер базаларының және алгоритмдердің қазіргі заманғы кешенді IT-зерттеулері келеді [95, 22 б.]. Осы факторларды салыстыру арнайы білім рөлінің бұрын-соңды болмаған өсуін көрсетеді, онсыз қазіргі заманғы тергеуші электрондық ақпаратты қабылдау, алып қою және декодтау мүмкіндігінен объективті түрде айырылады.

Дәстүрлі және цифрлық процестік институттарды салыстырмалы түрде салғастыру нәтижелерін қорытындылай келе, классикалық субъектіге орталықтандырылған парадигма өзінің эвристикалық әлеуетін объективті түрде сарқығанын тұжырымдау қажет. Анықталған жүйелі ақаулар тұжырымдамалық негіздемесі осы зерттеудің үшінші тарауында ұсынылатын сотқа дейінгі іс жүргізудің қағидатты түрде жаңа, артефактіге орталықтандырылған моделін әзірлеудің императивті қажеттілігін дәлелдейді.

Сотқа дейінгі тергеп-тексерудің процестік конструкциясының анықталған сапалық трансформациясы және онымен ұштасқан нормативтік олқылықтар ұлттық сот төрелігі жүйесінің тек ішкі юрисдикциялық мүмкіндіктер шеңберінен шығатын сын-қатерлермен бетпе-бет келіп отырғанын көрсетеді. Артефактіге орталықтандырылған модель мемлекеттің процестік оқшауланuы жағдайында

тиімді жұмыс істей алмайтыны туралы фактіні түсіну логикалық түрде трансшекаралық өзара іс-қимылдың оңтайлы тетіктерін іздеу және озық шетелдік тәжірибені рецепциялау үшін халықаралық-құқықтық мәнмәтінге жүгіну қажеттілігін туындатады.

Зерттеудің алдыңғы кезеңдерінде анықталған сотқа дейінгі іс жүргізудің процестік трансформациясы ұлттық тетіктердің киберқылмыстылықтың жаһандық сын-қатерлеріне адекваттылығын бағалау үшін халықаралық-құқықтық мәнмәтінге жүгінудің объективті қажеттілігін туындатады. Д.В. Завьялова негізді түрде атап өткендей, ақпараттық технологиялар саласындағы қылмыстарды және оларды тергеп-тексеру жөніндегі әдістемелік ұсынымдарды оларды жалпыәлемдік феномен ретінде жүйелі талдау мәнмәтінінен тыс қарастыру мүмкін емес [90, 8 б.]. Қылмыстық құқық доктринасында (оның ішінде Е.А. Русскевичтің [83] және басқа да ғалымдардың еңбектерінде) Ресей Федерациясының заңнамасына енгізілген өзгерістер сыни тұрғыдан бағаланады. Атап айтқанда, С.В. Маликов цифрлық ақпарат аясындағы қылмыстарды реттеудегі олқылықтар сот практикасында бірыңғай тәсілдің болмауына әкелетінін негіздейді [96, 506 б.]. Бұған қарама-қарсы, англосаксондық құқықтық жүйе мемлекеттерінде (атап айтқанда, Ұлыбритания мен АҚШ-та) базалық заңнамалық актілер алдаудың кез келген нысандарын технологиялық қабығына қарамастан қамтитын «цифрлық тергеу» модельдері мен eDiscovery стандарттарына негізделген. Осы аспектіні бағалай отырып, А.Б. Курумбаева мен Б.Б. Кощегулов Қазақстан Республикасының моделі арнайы саралаушы белгілерді (ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағы) интеграциялай отырып, бірыңғай норманы сақтауымен оңтайлы аралық жағдайды иеленеді деген қорытындыға келеді [21, 47 б.]. Сонымен қатар, материалдық құқықтың жеткілікті икемділігіне қарамастан, отандық практикада Будапешт конвенциясының ережелерін толық ауқымда имплементациялау деңгейі (әсіресе цифрлық дәлелдемелерді жинау рәсімдері мен халықаралық ынтымақтастық бойынша) әлі де төмен болып қалуда. Қазақстан бұл Конвенцияға қосылу алдында тұр, бұл ұлттық заңнаманы халықаралық стандарттарға сай цифрлық іздерді бекіту алгоритмдерімен толықтыруды талап етеді.

Аталған нормативтік айырмашылық цифрлық децепцияға қарсы іс-қимылдың институционалдық модельдерінің ерекшелігін тікелей детерминациялайды. А.Л. Осипенконың пікірінше, Еуропалық Одақ елдері мен АҚШ-та киберқылмыстарды тергеп-тексерудің жоғары нәтижелілігіне кең экстратерриториялық өкілеттіктері бар автономды бөлімшелерді құруды көздейтін терең институционалдық мамандану есебінен қол жеткізіледі [94, 135-136 б.]. Осы ұстанымды дамыта отырып, С. Шайсултанов пен тең авторлар озық шетелдік тәжірибе интернет-провайдерлер, қаржы институттары және технологиялық корпорациялар нақты регламенттелген процестік мәртебеге және мамандандырылған тергеу топтарының сұрау салулары бойынша цифрлық ақпаратты жедел ұсыну міндетіне ие болатын ажырамас мемлекеттік-жекешелік әріптестікке негізделетінін негізді түрде атап көрсетеді [97, 265 б.]. Салыстырмалы салғастыру деректермен алмасудың тәулік бойы жұмыс істейтін желілеріне негізделген кіріктірілген батыстық модельдерден айырмашылығы,

посткеңестік елдердегі сотқа дейінгі іс жүргізудің институционалдық тетігі бұрынғысынша жеке сектормен өзара іс-қимыл киберинциденттерге ден қою қарқынын сыни тұрғыдан баяулататын, негізінен формальды-сұрау салу сипатында болатын классикалық бюрократиялық иерархияға сүйенетінін көрсетеді.

АҚШ, ЕО және Ұлыбританияның озық тәжірибесін Қазақстанға бейімдеу қажеттілігі олардың цифрлық криминалистика мен предиктивті аналитикадағы технологиялық көшбасшылығынан туындайды (мысалы, АҚШ-тағы eDiscovery және Ұлыбританиядағы Digital Case File стандарттары) [98, 131-б.]. Дегенмен бұл тәжірибені ұлттық топыраққа сол қалпында көшіру елеулі тәуекел тудырады. Мұндай тәуекелдің бір көзі – АҚШ-тың прецеденттік құқығы мен Қазақстанның континенталдық құқықтық жүйесі арасындағы концептуалдық алшақтық, екіншісі – ұлттық IT-инфрақұрылым мен деректерді қорғау деңгейіндегі «нормативтік турбуленттілік» (normative turbulence) [16, 155-б.].

Сол себепті Қазақстан Республикасының Қылмыстық-процестік кодексіне шетелдік тәжірибені көзсіз қайталамайтын, нақты мақсатқа бағытталған өзгерістер енгізу қажет:

ҚР ҚПК-нің 7-бабына «жасанды интеллект» ұғымының ресми анықтамасын енгізген жөн: «аналитикалық, предиктивті және оқыту міндеттерін алдын ала белгіленген алгоритммен шектелмей орындай алатын бағдарламалық немесе аппараттық-бағдарламалық кешен»;

11 және 24-баптарда ЖИ қолданылғанда азаматтардың конституциялық құқықтарын қорғау мен кінәсіздік презумпциясын сақтау кепілдіктерін бекіту қажет – яғни алгоритм процестік тұлғаның шешімін ешқашан алмастырмайды, ол тек көмекші (auxiliary) құрал ретінде ғана танылуға тиіс;

ҚР ҚПК-нің 125-бабында ЖИ арқылы талданған цифрлық дәлелдемелердің жарамдылық шарттарын (түпнұсқалығы, сенімділігі және қайталанымдылығы) айқындау, ал 16-бабында жеке өмірге қол сұғылмаушылықты алгоритмдік араласудан және ауқымды деректерді (Big Data) негізсіз сүзуден қорғайтын шектеулерді қатаң бекіту қажет [99, 22-23 б.].

Жалпы алғанда, жасанды интеллектіні сотқа дейінгі тергеп-тексеруге енгізуді талдау оның шынайы техникалық және құқықтық шектеулерін объективті бағалауды талап етеді. Техникалық сәулет тұрғысынан бұл жүйелер оқшауланған емес, бірыңғай интеграциялық платформа (СДТБТ немесе «Қамқор» базалары) арқылы жұмыс істеуі шарт. Осындай экожүйеде (мысалы, DeepJudge AI немесе Legora AI сияқты озық шешімдердің сәулеттік принциптері бойынша) алгоритмдік ашықтық, құжаттарды қауіпсіз құрылымдау, процестік сүзгілер және тергеушінің әрбір әрекетін өзгертілмейтін аудит журналдарында (лог-файлдарда) міндетті түрде тіркеу қамтамасыз етілуі тиіс [99, 28-30 б.]. Тек осындай қатаң процестік кепілдіктер мен техникалық бақылау механизмдері орнатылған жағдайда ғана жасанды интеллект жүйелері адам құқықтарын бұзбай, қылмыстық сот ісін жүргізудің тиімділігін арттыра алады.

Институционалдық бытыраңқылық қазіргі заманғы цифрлық технологиялардың қылмыстық құдалау процесіне интеграциялануының жеткіліксіз деңгейімен ажырамас байланысты. Шетелдік практиканы талдай

отырып, А. А. Толыбаева мен авторлар озық юрисдикцияларда сотқа дейінгі тергеп-тексеру электрондық құжаттарды жай ғана сақтауды емес, сонымен қатар цифрлық іздер массивтерін автоматтандырылған жіктеуді, индекстеуді және корреляциялық талдауды қамтамасыз ететін өтпелі ақпараттық платформаларға (АҚШ-тағы eDiscovery, Эстониядағы e-File немесе Ұлыбританиядағы Digital Case File) сүйенетінін негіздейді [98, 131 б.].

Өз кезегінде П.С. Пастухов мұндай технологиялық шешімдерді («платформалық ойлау») енгізу анонимді субъектілер арасындағы жасырын желілік байланыстарды тиімді анықтауға мүмкіндік беретінін айтады. Автордың пайымдауынша, цифрлық платформалар дәлелдеу парадигмасын түбегейлі өзгертіп, оны үлкен деректерді (Big Data) «автоматтандырылған режимде» өңдеу форматына көшіреді, бұл адам факторынан туындайтын қателіктерді айтарлықтай азайтады [100, 529 б.].

Жүргізілген халықаралық салыстырмалы-құқықтық талдау нәтижелерін қорыту анықталған өзгерістердің жүйелі сипатын тіркеп-белгілейтін тұтас авторлық ұстанымды тұжырымдауға мүмкіндік береді. Онлайн алаяқтыққа қарсы іс-қимылдың қазіргі заманғы ұлттық моделі сотқа дейінгі тергеп-тексерудің әлеуетін дәстүрлі процестік конструкциялардың шеңберімен шектейтін айқын фрагменттілікпен объективті түрде сипатталады. Бұл жай-күй құқық қолданудың оқшауланған проблемасы болып табылмайды, қайта алаяқтық феноменінің өзінің неғұрлым терең трансформациясын көрсетеді.

Жүргізілген талдау сөз жекелеген модификациялар туралы емес, екіжақты табиғаты бар іргелі өзгеріс туралы болып отырғанын растайды. Бір жағынан, материалдық-құқықтық конструкцияның сапалық эволюциясы орын алды: алаяқтық классикалық жеке-материалдық модельден қолсұғушылықтың кешенді объектісіне, қашықтықтан цифрлық децепцияға және үлестірілген ұжымдық субъектіге негізделген күрделі жүйелі-виртуалды парадигмаға трансформацияланды. Екінші жағынан, бұл материалдық-құқықтық өзгеріс тергеп-тексерудің процестік моделінің трансформациясын – субъект-центристік тәсілден цифрлық іздерді тіркеп-белгілеу және талдау басымдыққа ие болатын дәлелдеу әдістеріне өтуді заңды түрде негіздеді.

Дәл осы қылмыстың жаңа табиғаты мен қарсы іс-қимылдың ұлттық тетігінің сақталып отырған фрагменттік ұйымдастырылуы арасындағы сәйкессіздік компаративистік зерттеу барысында анықталған негізгі қарама-қайшылықты қалыптастырады. Кешенді шетелдік модельдерден айырмашылығы, ұлттық жүйе дискреттік сипатты сақтайды, бұл объективті түрде нүктелі жаңғыртуды емес, құрылымдық бейімделуді талап етеді.

Осыған байланысты Қазақстан Республикасы үшін өзара байланысты үш векторды қамтитын киберқатерлерге қарсы іс-қимылдың интеграцияланған моделін имплементациялау негізделген деп танылады.

Біріншіден, цифрлық дәлелдемелердің құбылмалы және трансшекаралық табиғатын ескере отырып, олармен жұмыс істеудің арнайы процестік регламентін қалыптастыру арқылы нормативтік айқындық қажет.

Екіншіден, автономды кибербөлімшелерді дамытуды және құқық қорғау органдарының жекеше IT-сектормен өзара іс-қимылының тікелей тетіктерін

нормативтік бекітуді болжайтын институционалдық мамандану сыни тұрғыдан маңызды.

Үшіншіден, тергеу ақпаратын автоматтандырылған түрде жинау және аналитикалық өңдеу үшін зияткерлік цифрлық платформаларды енгізуге бағдарланған толыққанды технологиялық қамтамасыз ету талап етіледі.

Аталған ережелердің синтезі қорытынды тұжырымды тіркеп-белгілеуге мүмкіндік береді: материалдық-құқықтық және процестік феномен ретіндегі алаяқтықтың трансформациясы жүйелі сипатқа ие және қарсы іс-қимылдың кешенді, институционалдық және технологиялық интеграцияланған моделі түріндегі симметриялы жауапты талап етеді.

Классикалық және онлайн алаяқтық арасындағы анықталған айырмашылықтардың дәлелденген жүйелілігі дәстүрлі құқық қолдану инструментарийі цифрлық орта жағдайларына тұжырымдамалық түрде бейімделмегенін растайды. Материалдық-құқықтық және процестік болмыстың қосарлы трансформациясының негізделген тұжырымдамасы қылмыстық сот ісін жүргізудің ағымдағы жай-күйін сыни тұрғыдан ұғыну қажеттілігін объективті түрде туындатады. Анықталған теориялық-әдіснамалық заңдылықтар онлайн алаяқтықты сотқа дейінгі тергеп-тексеру сатысындағы қолданыстағы нормативтік коллизияларды, латенттілікті, цифрлық дәлелдемелерді жинау проблемаларын және трансшекаралық өзара іс-қимыл кедергілерін тереңдетіп талдау үшін сенімді ғылыми іргетас қалыптастырады.

2 ОНЛАЙН АЛАЯҚТЫҚ ҚЫЛМЫСТАРЫН СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІҢ ҚАЗІРГІ КЕЗЕҢДЕГІ НЕГІЗГІ МӘСЕЛЕЛЕРІ МЕН ЕРЕКШЕЛІКТЕРІ

2.1 Онлайн алаяқтық қылмыстары бойынша сотқа дейінгі тергеп-тексеруді бастау, тіркеу, бастапқы ақпаратты растау және латенттілік феномені

Қазақстан Республикасының қылмыстық-процестік заңнамасы негізсіз өтініштерді іріктеп тастау үшін құқықтық сүзгі ретінде тарихи түрде құрастырылған сотқа дейінгі іс жүргізуді бастаудың қатаң нормативтік моделін бекітеді. ҚР ҚПК-тің 180-бабына сәйкес қылмыстық құқық бұзушылық белгілерін объективті түрде көрсететін жеткілікті деректердің болуын талап ететін тергеп-тексеруді бастауға себептер мен негіздерді қатаң регламенттеу осы конструкцияның базалық элементі ретінде әрекет етеді. Бір жағынан, Л.Л. Абрамова процестік заңның логикасы құқық қолданушының бастапқы ден қою сатысының өзінде іс-әрекеттің криминалдық белгілерін анықтау қабілетінің презумпциясына негізделеді, бұл оның айқын физикалық іздері бар материалдық бағдарланған қылмыстылыққа тән екендігі туралы классикалық теориялық ұстанымды негіздейді [101, 119 б.]. Екінші жағынан, ҚР ҚК-нің 190-бабы бойынша сараланатын онлайн алаяқтықтың ерекшелігі осы консервативті презумпциямен тікелей жүйелі қайшылыққа түседі, өйткені цифрлық децепция дәстүрлі айқындықтан тұжырымдамалық түрде айырылған және заңды азаматтық-құқықтық қатынастар түрінде бүркемеленеді.

Виртуалды жымқыру тетігінің ерекшелігіне байланысты бастапқы ақпаратты құқықтық бағалаудың іргелі проблемасы туындайды. Осы феноменді талдай отырып, М.Ю. Подваркова қашықтан когнитивті әсер етуге назар аударады, бұл ретте жәбірленуші іс-әрекеттің сыртқы жағына шартты жай ғана орындамау көрінісін бере отырып, транзакцияға мүлдем өз еркімен бастамашылық жасайды [102, 79 б.]. Бұл тәсіл дәлелі өзге аналитикалық векторға ие А.Б. Сабырбаеваның ұстанымымен ғылыми диалогқа түседі: егер М.Ю. Подваркова азаматтық-құқықтық қатынастар елесінің субъективті-мінез-құлық факторын бөліп көрсетсе, онда А.Б. Сабырбаева қылмыс жасаудың шынайы тетігін сенімді жасыратын және тергеуді дәстүрлі идеалды және материалдық іздерден айыратын виртуалды ортаның объективті-технологиялық анонимділігін атап көрсетеді [103, 162 б.]. Осы ғылыми көзқарастарды жоғары сот сатысының императивті ұстанымымен салыстыру сыни құқықтық коллизияны айқындайды. ҚР Жоғарғы Сотының №6 Нормативтік қаулысының 10-тармағы шартты жасасқанға дейін немесе жасасу сәтінде жымқыру пиғылын нақты белгілеуді тікелей талап етеді. Алайда ҚР ҚПК-тің 179-бабының 1-бөлігі азаматтық-құқықтық мәмілелерден немесе даулардан туындайтын арыздарды СДТБТ-де тіркеуге үзілді-кесілді тыйым салады. Тұйық процестік тығырық қалыптасады: желідегі қасақана алдауды дәлелдеу үшін банктік мәліметтерді және IP-қосылыстардың детализациясын талап етіп алдыруды қоса алғанда, жасырын және процестік іс-шаралар кешенін жүргізу объективті түрде талап етіледі,

оларды СДТБТ-де арыз ресми тіркелгенге дейін іске асыру іс жүзінде және заңды түрде мүмкін емес.

Аталған нормативтік-эмпирикалық алшақтықтарды қорыту бастапқыда азаматтарды қылмыстық қудалау орбитасына негізсіз тартудан қорғау үшін құрастырылған процестік тосқауыл (ҚР ҚПК-тің 180-бабы) киберқылмыстарға қатысты құқық бұзушылықтарды жасырудың заңды тетігіне айналды деген авторлық ұстанымды тұжырымдауға мүмкіндік береді. Негізгі проблемалық гипотеза ретінде бастапқы ден қоюды салдандыратын факторлардың жүйелі триадасын бөліп көрсеткен жөн: қылмысты азаматтық деликт түрінде бастапқы бүркемелеу, транзакциялардың абсолютті технологиялық анонимділігі және инициациялау сатысының қатаң процестік шектеулері. Бұл гипотезаның негізділігі құқық қолдану практикасының сыни көрсеткіштерімен дәлелденеді, мұнда да зерттеушілердің акценттерінде тұжырымдамалық айырмашылық байқалады. Біріншіден, К.О. Карабеков интернет-алаяқтық латенттілігінің сыни, 70 % деңгейіне жеткенін көрсете отырып, проблеманың сандық аспектісін тұжырымдайды [17, 97 б.]. Екіншіден, А.Д. Мухамеджанова проблеманы ахуалдық құқық қолдану іркілістері разрядынан жүйелі ақаулар санатына ауыстыратын осы теріс көрсеткіштің динамикадағы институционалдық тұрақтылығын тіркеп-белгілей отырып, құбылыстың сапалық жағын зерттейді [104, 54 б.].

Демек, ашылмаған немесе номенклатуралық іске шығарылған арыздардың орасан зор көлемі әмбебап процестік модельді инновациялық цифрлық қатерлерге қолданудың заңды нәтижесі болып табылады. Қолданыстағы нормативтік конструкцияның тиімді сүзгі ретінде қызмет етуге айқын қабілетсіздігі сотқа дейінгі тергеп-тексеруді инициациялау сатысының жүйелі дағдарысын айғақтайды. Анықталған коллизия бастапқы ден қою тетігіндегі цифрлық дәлелдемелік базаның жоғалуының нақты фазаларын дәл оқшаулауға мүмкіндік беретін, ішкі кезеңдер мен процестік шешімдерді қабылдау алгоритмдеріне егжей-тегжейлі проблемалық-процестік талдау жасауға көшудің қатаң логикалық қажеттілігін туындатады.

Адамды қылмыстық сот ісіне заңды түрде тартудың басты шарты – нормативтік себептер мен негіздер жүйесіне сүйенетін, сотқа дейінгі тергеп-тексеруді бастаудың қатаң реттелген тәртібі. ҚР ҚПК-нің 180-бабына сәйкес процестік тетік себептердің түпкілікті тізбесі арқылы қосылады, олардың қатарында жеке тұлғалардың арызы, лауазымды адамдардың хабары және онлайн-платформалардағы ақпарат бар. Бұл нормалардың мәні мынада: тіркеуге алудың фактілік негізі болу үшін оқиғаның және нақты қылмыстық құқық бұзушылық құрамының объективті белгілерінің бар екенін тікелей аңғартатын жеткілікті дерек қажет. Осы нормативтік нұсқауларды түсіндіре келіп, Л.Л. Абрамова заң бастапқы ден қою сатысының өзінде-ақ фактілік негіздерді айқын тіркеп-белгілеуді талап ететінін орынды атап өтеді [101, 114-115 б.]. Осы классикалық, материалдық жаққа бағдарланған тәсілді өрбіте отырып, П.А. Капустюк бастаған зерттеушілер тергеп-тексеруді заңды түрде бастау үшін криминалдық белгілерді кідіріссіз байқау шарт екенін табандылықпен алға тартады [105, 16 б.].

Бір жағынан, қылмыстық қол сұғушылықтың айқындығы презумпциясына сүйенетін бұл модель дәстүрлі қылмыстылық тұрғысынан тұжырымдамалық жағынан аяқталған көрінеді. Екінші жағынан, желілік жымқыру тетігін бағалағанда консервативті құқықтық форма мен іс-әрекеттің виртуалды мазмұны арасында терең жүйелі қайшылық байқалады. ҚР ҚК-нің 190-бабы алаяқтықты бұрыннан балама белгілер арқылы айқындайды: алдау немесе сенімді теріс пайдалану жолымен жымқыру. Алайда цифрлық ортаның өзгешелігі бұл белгілердің аражігін догматикалық тұрғыдан қатаң ажыратуды талап етеді. Субъектілер толық анонимді болғандықтан әрі тұлғааралық не қызметтік байланыс мүлде болмағандықтан, онлайн алаяқтық тек технологиялық алдау арқылы жасалады, ал байланыссыз қол сұғушылықта сенімді теріс пайдалану тұжырымдамалық жағынан орын алуы мүмкін емес.

Бұл теориялық пайым құқық қолдану практикасында толық расталады: сот органдары айыптау актілерінен «сенімді теріс пайдалану» белгісін жүйелі түрде алып тастап келеді. Соттар қашықтан алдау жағдайында (соның ішінде микроқаржы ұйымдарына жасалған шабуылда) кінәлі мен жәбірленушінің арасында алдын ала сенім қатынасы болмайтынын негізге алады. Мұндай процестік шешімдер бірқатар іс бойынша қабылданған, атап айтқанда №7560-21-00-1/25 қылмыстық іс (Алматы қаласы Жетісу ауданының №2 аудандық сотының 24.02.2021 ж. үкімі) [85], №5522-20-00-1/199 қылмыстық іс (Павлодар облысы Екібастұз қалалық сотының 2021 жылғы 02 сәуірдегі үкімі) [106], сондай-ақ №7511-22-00-1/725 қылмыстық іс (Алматы қаласы Алмалы аудандық сотының 2022 жылғы 02 қарашадағы үкімі) [107] бойынша. Осы фактілердің бәрінде соттар іс-әрекетті тек ақпараттық жүйені пайдаланушыны алдау деп саралап, сенімді теріс пайдалану белгісін императивті түрде алып тастады; бұл цифрлық өрісте классикалық конструкциялардың өміршең еместігін айғақтайды.

Сот практикасы АКТ-ның осынша ауқымды жалған азаматтық-құқықтық қатынастар құрастыруға қалай жұмсалатынын айқын аңғартады. Айталық, №5522-21-00-1/146 қылмыстық іс бойынша (Павлодар облысы Екібастұз қалалық сотының 2021 жылғы 06 желтоқсандағы үкімі) [108] кінәлінің виртуалды алдаудың мультиплатформалық желісін құрғаны анықталды: ол ақшаны «айналдыру» жайлы жалған пікірлерді көрсету үшін «Instagram» желісіндегі аккаунтты, ал жоқ автомобиль сату мен пәтер жалдау туралы хабарландыруларды жаппай тарату үшін «Kolesa.kz» және «OLX.kz» платформаларын пайдаланған. Ағындарды үйлестіруді ол бөтеннің банк карталары мен жеке басты куәландыратын құжаттардың жалған фотосуреттерін қолданып, «WhatsApp» мессенджері арқылы жүргізген. АКТ-ны нақ осылай, тек алдау архитектурасы ретінде тізбектеп пайдалану басқа бір іс бойынша да – №5511-22-00-1/31 қылмыстық іс (Өскемен қаласы №2 сотының 2022 жылғы 24 мамырдағы үкімі) [50] – тіркелген; мұнда кінәлі жалғыз смартфонмен «OLX.kz» платформасында жылжымайтын мүлікті жалға беру желеуімен жымқырудың сексеннен астам эпизодын жасаған. Бұл істер АКТ заңды мәміле елесін тудыруға іргелі негіз болатынын дәлелдейді.

В.В. Коломинов пен М.Ю. Подваркованың ұстанымдарын талдау ғылыми тәсілдердің іргелі алшақтығын көрсетеді: егер біріншісі бастапқы ден қою

сәтінде қылмыс белгілерін анықтауды талап ететін нормативтік конструкцияның әмбебаптығын тұжырымдамалық түрде жақтаса [109, 147 б.], онда екіншісі бұл талапты бастапқы сатыда іске асырудың эмпирикалық мүмкін еместігін дәлелдейді, өйткені іс-әрекеттің цифрлық табиғаты қасақана алдау фактісін күнделікті қаржылық операциялар фасадымен сенімді түрде жасырады [102, 79 б.].

Біздің ойымызша, тергеп-тексеруді бастау сәтін бастапқы қылмыстық пиғылдың айқындығына қатаң нормативтік тұрғыдан байлау виртуалды децепцияның технологиялық бүркемелеуімен шешілмейтін қақтығысқа түседі. Бұрынырақ негізделгендей, мұндай бүркемелену ҚР ҚПК-тің 179-бабының императивтік шектеуінің құрбандардың сот төрелігіне қол жеткізуін бұғаттайтын институционалдық тосқауылға сөзсіз трансформациялануына әкеледі.

Осы криминалдық бүркемелеуді көрнекі түрде көрсететін барынша жаппай схема танымал сауда платформаларында жалған хабарландырулар жасау болып табылады. Осыған ұқсас мән-жайлар бірқатар істер бойынша анықталған. Мәселен, сол №5511-22-00-1/31 қылмыстық ісі бойынша (Өскемен қаласы №2 сотының 2022 жылғы 24 мамырдағы үкімі) [50] сотталушының сексеннен астам жәбірленушіден алдын ала төлем ала отырып, «OLX.kz» сайтында пәтерлерді жалға беру туралы жалған хабарландырулар орналастырғаны анықталды. Кепілақы талап ету арқылы жылжымайтын мүлікті жалған жалға берудің бірдей практикасы «Krisha.kz» платформасын белсенді пайдалана отырып, №7135-23-00-1/179 қылмыстық ісі бойынша (Астана қ. Қылмыстық істер жөніндегі ауданаралық сотының 2023 жылғы 26 мамырдағы үкімі) [110], сондай-ақ №7141-25-00-1/1908 қылмыстық ісі бойынша (Астана қаласының Қылмыстық істер жөніндегі ауданаралық сотының 2025 жылғы 05 қыркүйектегі үкімі) [49] тіркеп-белгіленген. Бұл сот актілері қаражатты аударудың сыртқы еріктілігі осындай схемалар шеңберінде құрбандар мінез-құлқының тұрақты паттерні болып табылатынын растайды.

Онлайн алаяқтықтың бұрын-соңды болмаған латенттілігі тергеу органдарының субъективті кемшіліктерінен емес, жүйелі факторлардың объективті жиынтығынан келіп шығатынын түсіну маңызды: мұнда қол сұғушылықтың шарттық процесс болып бүркемелеуі, желідегі субъектілердің толық анонимдігі және бастапқы ақпаратты тексерудегі процестік шектеулер бірге әрекет етеді. Осы қырды тереңдете талдай отырып, А.Б. Сабырбаева виртуалды оқиға орнында идеалды да, материалдық та іздердің болмауы анықтау органдарын тіркеудің процестік шегінен өту үшін керекті деректерді жедел жинайтын құқықтық құралдардан айыратынын нанымды түрде көрсетеді [103, 162 б.]. Доктринада бұған дейін айтылған аса жоғары латенттілікті эмпирикалық тұрғыдан растайтын дәйек – осы қатердің жүйелі сипатын бекітетін Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасының көрсеткіштері. Бұл орайда А.Д. Мухамеджанова аталған теріс үрдістің алаңдатарлық тұрақтылығына назар аударады, ал ол бұл мәселені уақытша ұйымдастырушылық қиындық деп түсіндіруге еш мүмкіндік қалдырмайды [104, 54 б.].

Осы проблемалық-нормативтік талдау сотқа дейінгі тергеп-тексеруді бастаудың қолданыстағы моделі қазіргі киберқылмыстың өзгешелігіне

икемделмегенін көрсетеді. Қылмыс құрамының айқын белгілері болуы туралы заңнамалық талап бастапқы сигнал түскен сәтте қылмыстық қудалау тетігін тежейді әрі процестік әрекеттер басталғанға дейін цифрлық алдауды әдеттегі міндеттемені орындамаудан ажыратуға мүмкіндік бермейді. Бастау сатысындағы осы жүйелі дағдарыс арыздарды тексерудің ішкі кезеңдерін егжей-тегжейлі талдауды қажет етеді, өйткені нақ сол кезеңдерде цифрлық дәлелдемелік базаның қайтарымсыз жоғалуына апаратын функционалдық ақаулар анықталады.

Бастапқы деректерді жинаудың жалғасы ретінде цифрлық ортада мазмұны елеулі өзгеретін жедел тексеру кезеңі әрекет етеді. Оның нормативтік негізі – уәкілетті органдарды анықтамалар алу, байланыс желілерін бақылау және абоненттердің қосылыстары туралы ақпаратты талап етіп алдыру инструментариймен қамтамасыз ететін «Жедел-іздестіру қызметі туралы» ҚРЗ-ның 1 және 11-баптары. Алайда бұл өкілеттіктерді іске асыру екінші деңгейдегі банктермен және интернет-провайдерлермен корпоративтік өзара іс-қимылға толық тәуелді. С.М. Голятина бұл кезеңнің тиімділігі деректермен алмасу жылдамдығына сыни тәуелділікте болатынын, бұл биллингтік және қаржылық ақпаратты алуда уақыттық кідірістерді туындататынын атап өтеді [111, 79 б.]. Жағдай заңмен қорғалатын құпияға қол жеткізуді қатаң санкциялау туралы ҚР ҚПК-тің 122-бабының талаптарымен ушыға түседі. В.В. Коломинов жедел деректерді дәлелдеу процесіне интеграциялау кезіндегі заң шығарушының ақталған сақтығын атап көрсетеді, бұл бастапқы тексеру сатысында-ақ мәліметтердің едәуір массивінің процестік перспективасының жоғалуына әкеледі [91, 103 б.]. Жедел-іздестіру қызметі туралы заңның 14-бабын технологиялық болмыспен салыстыру іс-әрекет белгілерін нақты анықтау мен оларды процестік тіркеп-белгілеу мүмкіндігі арасындағы институционалдық алшақтықты көрсетеді.

Анықталған кедергілер жедел тексерудің орталық проблемасын – іс-әрекеттің субъективті жағын дәлелдеуді алдын ала айқындайды. ҚР Жоғарғы Сотының №6 Нормативтік қаулысының 10-тармағында баяндалған ҚР ҚК-нің 190-бабының конструкциясы классикалық модельге негізделеді: кінәлінің пиғылы мүлікті бергенге дейін немесе беру сәтінде қалыптасады, ал алдау заңсыз баюмен тікелей себептік байланыста болады. Осы парадигмаға қарсы М.Д. Фролов онлайн алаяқтықтағы темпоралды инверсия феноменін көрсетеді: жәбірленуші алдау фактісін желіде мүліктік әрекеттерді өз еркімен жасағаннан кейін айтарлықтай кешігіп ұғынады [18, 76 б.]. К.А. Мира құқық қолданушыны классикалық идеалды іздерден айыратын желілік өзара іс-қимылдың жанамаланған сипатына байланысты пиғылды жедел анықтау қиындайтынын тұжырымдайды [61, 56 б.]. Бұл көзқарастарды жоғары сот сатысының ұстанымымен салыстыру өткір қайшылықты анықтайды: алдау мен пайдакүнемдік мақсатты синхронды анықтау туралы догматикалық талап электрондық транзакция фактісінің өзі сырттай заңды қаржылық операциямен бірдей болатын қашықтан децепцияның ерекшелігімен шешілмейтін қақтығысқа түседі.

Материалдық құқық пен цифрлық із түзілу ерекшелігі арасындағы алшақтықты шеше отырып, авторлық ұстанымды тұжырымдаған жөн. Онлайн

жымқыруларды тергеп-тексеруде құқық қолданушы жедел тексеру кезеңінде ақпараттық асимметрия жағдайында қалады: іс-әрекеттің объективті жағы автоматтандырылған банктік жүйелер арқылы кідіріссіз тіркеледі, ал субъективті жағы анонимді интерфейстермен және процестік шектеулермен жасырылады. Қолданыстағы құқықтық инструментарий қудалау органына бастапқы сатыда қашықтағы контрагенттің міндеттемені орындамауы азаматтық-құқықтық факторлармен емес, бастапқыда қылмыстық пиғылмен детерминацияланғанын дәлелдеуге мүмкіндік бермейді.

Баяндалғаннан шыға отырып, жедел тексеру кезеңі өзінің ағымдағы нормативтік жай-күйінде еңсерілмейтін темпоралдық және дәлелдемелік шектеулермен сипатталатынын тұжырымдау қажет. Сигналды верификациялаудың қатаң мерзімдері мен рәсімдерін ұйғаратын қолданыстағы құқықтық модель жымқырылған цифрлық активтерді маршруттаудың лездік жылдамдығына тұжырымдамалық түрде бейімделмеген. Осының салдарынан бастапқыда заң шығарушымен азаматтарды қылмыстық қол сұғушылықтардан қорғауға арналған сүзгі ретінде жобаланған саты деформацияланады және жәбірленушілердің сот төрелігіне қол жеткізуін бұғаттайтын институционалдық тосқауылға трансформацияланады. Қолданыстағы жүйенің виртуалды анонимділік жағдайында субъективті жағын анықтау проблемасын жедел еңсеруге дәлелденген қабілетсіздігі инициациялаудың аяқтаушы кезеңі – жиналған материалдарды процессуализациялауды талдауға көшудің ғылыми қажеттілігін объективті түрде туындатады.

Онлайн алаяқтықты сотқа дейінгі тергеп-тексеруді инициациялау сатысының аяқтаушы элементі ретінде заңдық мәні қылмыстық құқық бұзушылықты тіркеу туралы биліктік шешім қабылдаудан және жиналған жедел деректер массивін қатаң регламенттелген процестік нысанға трансформациялаудан тұратын процессуализациялау кезеңі әрекет етеді. Бұл өтудің нормативтік негізі ретінде тергеп-тексерудің басталуын СДТБТ-де тіркеумен байланыстыратын ҚР ҚПК-тің 179-бабының ережелері, сондай-ақ бастапқы мәліметтерді лауазымды адамның баянаты арқылы міндетті түрде заңдастыруды талап ететін ҚР ҚПК-тің 184-бабының нұсқамалары қызмет етеді. Қосымша процестік тосқауыл ретінде жасырын іс-шаралар материалдарының дәлелдеу процесіне тек оларды процестік тексеруден кейін ғана жіберілетінін белгілейтін «Жедел-іздестіру қызметі туралы» ҚРЗ-ның 14-бабының императиві әрекет етеді. Деректерді интеграциялау тетігін бағалай отырып, И.А. Грудинин ақпараттың қылмыстық сот ісін жүргізуге кіру процесі объективті қиындықтармен ұштасатынын әділетті түрде атап өтеді, өйткені жедел және процестік мәліметтер қағидатты түрде әртүрлі гносеологиялық және құқықтық табиғатқа ие [112, 82 б.]. Бұл тезисті дамыта отырып, В. А. Гущин жасырын қызмет нәтижелерін заңдастырудың күрделенген рәсімі толыққанды дәлелдемелік базаны уақтылы қалыптастыруға кедергі келтіретін жасанды тосқауылдарды құрастыратынын көрсетеді. Автор жедел ақпаратты процестік нысанға көшіру кезіндегі «деректің жоғалуы» немесе «бұрмалануы» тәуекелі онлайн алаяқтық сияқты жоғары технологиялық қылмыстарда дәлелдеу парадигмасын әлсіретететінін атап өтеді [113, 132 б.].

Талданып отырған кезеңнің басты проблемасы – жедел-іздестіру қызметінің нәтижелері цифрлық іздерді тіркеп-белгілеу тұрғысынан консервативті процестік талаптармен әрең үйлеседі. ҚР ҚПК-нің 120-бабы компьютерлік ақпаратты қамтитын материалдарды формально түрде құжат деп таныса да, құқық қолдану тетігі бір кедергіге тіреледі: заңда цифрлық дәлелдемелердің нақты анықтамасы да, оларды кідіріссіз бекітудің арнайы тәртібі де жоқ. Осы теориялық-құқықтық олқылықты зерттеген А.И. Зазулин терминологиялық шашыраңқылық пен цифрлық ақпараттың материалдық табиғатына бірыңғай көзқарастың жоқтығы цифрлық артефактілерді нәтижелі пайдалануды іс жүзінде тежейтін «белгісіз» процестік мәртебе туғызатынын түйіндейді [114, 5-6 б.]. Мұның практикалық салдарын нақтылай келіп, А.Б. Сабырбаева реттеудегі олқылықтар себебінен ресми тергеп-тексеру басталғанға дейін жиналған аса құнды мәліметтер қатаң процестік сүзгіден өткенде заңдық күшін біржола жоғалтатынын көрсетеді [103, 164 б.].

Бұл құқықтық коллизияны құқық бұзушылықты тіркеу кезінде уәкілетті лауазымды адамдардың бастапқы ақпаратты бағалаудағы таза формальды көзқарасы одан әрі ушықтырады. Оның себебін қарастыра отырып, Л.Л. Абрамова шешім қабылдайтын субъектілер қылмыстық қудалауды негізсіз бастау қаупінен сақтанып, бастапқы деректердің көлемі мен сапасына қойылатын талаптарды жасанды түрде көтеретінін, ал бұл іс жүргізуді бастау мерзімін созып жіберетінін атап өтеді [101, 185 б.]. Мүлде қарама-қарсы ұстанымды Е.С. Шевченко ұсынады: ол киберқылмысты тергеу жағдайында процестік формализмге тіптен жол беруге болмайтынын ескертеді, өйткені цифрлық орта қаскүнемдерге криминалистикалық маңызы бар ақпаратты санаулы секундта қашықтан жоюға мүмкіндік береді [59, 57 б.].

Аталған авторлардың ұстанымдарын салыстыру айқын тұжырымдамалық қайшылықты анықтауға мүмкіндік береді: егер Л.Л. Абрамова талаптарды асыра бағалауды процестік қателіктерден қорғаушы әкімшілік тетік ретінде қарастырса, онда Е.С. Шевченко мұндай формализм заңдылықтың кепілі емес, бүкіл қылмыстық істің дәлелдемелік перспективасының бұзылуының тікелей катализаторы ретінде әрекет ететінін үзілді-кесілді дәлелдейді.

Анықталған қайшылықтарды шеше отырып, негізделген авторлық ұстанымды тұжырымдаған жөн. Онлайн жымқыруларды тергеп-тексеру жағдайында құқық қолданушының толыққанды тергеп-тексеру басталғанға дейін фрагментті виртуалды деректерді дәстүрлі материалдық құрамдар призмасы арқылы бағалау талабы процестік анахронизм болып табылады. Цифрлық ақпараттың мобильділігі мен қылмыстық істі инициациялау рәсімдерінің статикалығы арасындағы жүйелі қақтығыс материалдарды келісуге және тіркеуге кететін уақытша кідірістердің қылмыскерлер үшін логтарды, транзакцияларды жою және IP-мекенжайларды өзгерту бойынша еркін мүмкіндіктер терезесін құруына әкеледі.

Алдыңғы кезеңдердің объективті қиындықтарын тіркеу сатысының белгіленген құқықтық тосқауылдарымен синтездей отырып, бастапқы ақпаратты жинаудың, оны жедел тексерудің және одан әрі процессуализациялаудың бірізді кезеңдерінің жиынтығы сотқа дейінгі іс жүргізудің институционалдық «тар

өткелін» қалыптастырады деген қорытынды жасау қажет. Дәл осы виртуалды децепцияның динамикалық технологиялық табиғаты мен қылмыстық процестің архаикалық нысаны арасындағы шешілмейтін қақтығыспен детерминацияланған нормативтік-практикалық алшақтық шеңберінде цифрлық дәлелдемелік базаның жүйелі және барынша ауқымды жоғалуы орын алады.

Инициациялау сатысының функционалдық деформацияларына жасалған процестік талдаудың логикалық жалғасы ретінде цифрландыру жағдайында таза криминологиялық санат шеңберінен шығатын және айқындаушы қылмыстық-процестік мәнге ие болатын латенттілік феноменін зерттеу әрекет етеді. Алаяқтықты алдау немесе сенімді теріс пайдалану жолымен жымқыру ретінде нормативтік құрастыру (ҚР ҚК-нің 190-бабы) цифрлық қол сұғушылықтардың басым көпшілігі тергеп-тексеруді бастауға себептерді регламенттейтін ҚР ҚПК-тің 180-бабының нормативтік тосқауылын еңсере алмайтындығымен бетпе-бет келеді. Осы параличтің табиғатын зерттей отырып, Б.Э. Шавалеев пен Р.С. Атаманов сияқты зерттеушілер виктимологиялық және психологиялық факторларды бөліп көрсетеді [115, 141 б.; 116, 205 б.]: жәбірленушілердің арыз беруге жаппай құлықсыздығы жаппай шабуылдар кезіндегі жеке залалдың болмашылығымен және тергеп-тексерудің табысты болатынына терең сенбеушілікпен (құқық қорғау органдарына күдікпен қараумен) детерминацияланады. Баламалы ракурсты назарды таза техникалық детерминанттарға аудара отырып, Р.Н. Подольный келесіні ұсынады [39, 57 б.]: мұнда желілік анонимизациялау, цифрлық бүркемелеу және шифрлау құралдарын қолдану субъектінің құқық қорғау органдары үшін абсолютті ұсталмайтындығы (қолжетпестігі) туралы тұрақты сезімді туындатады. Осы ұстанымдарды салыстыру ғылыми акценттердің жай ғана айырмашылығын емес, өзара шартталған дуальдылықты айқындайды: криминалдық ортаның техникалық басымдығы құрбандардың психологиялық апатиясын объективті түрде генерациялайды. Анықталған байланыс авторлық ұстанымды тұжырымдауға мүмкіндік береді: онлайн алаяқтықтың латенттілігі базалық деңгейде құқық қолданушыны процестік ден қоюға арналған заңды себептен айыра отырып, бастапқы сигналдың түсуін тікелей бұғаттайтын монолитті мінез-құлықтық-технологиялық тосқауыл ретінде қалыптасады.

Осылайша, бұл қылмыстардың латенттілігін (жасырындылығын) оның туындау табиғатына қарай екі айқын санатқа бөліп қарастыру қажет:

– Табиғи (субъективті немесе виктимологиялық) латенттілік: бұл тікелей жәбірленушілердің өз бастамасымен (немесе әрекетсіздігімен) туындайтын жасырындылық. Практика көрсеткендей, мұндай латенттілікке бірнеше фактор әсер етеді: көбінесе келтірілген шығынның болмашылығы (мысалы, алдын ала төлем ретінде аударылған 10 000 – 15 000 теңге), ұзаққа созылатын бюрократиялық тергеу рәсімдеріне уақыт жұмсағысы келмеуі, полицияның виртуалды кеңістіктегі (көбінесе басқа елде немесе қалада отырған) қылмыскерді таба алатынына терең сенбеушілік, сондай-ақ жәбірленушінің алаяқтардың айласына оңай түсіп қалған өзінің аңғалдығы үшін ұялу сезімі. Осы себептерге байланысты құрбандар құқық қорғау органдарына арызданудан мүлдем бас тартады;

– Жасанды (жүйелі немесе құқық қолдану) латенттілік: бұл тікелей қылмыстық іс жүргізу заңнамасындағы кедергілермен (ҚР ҚПК нормаларымен) байланысты болатын жасанды тосқауыл. Яғни, жәбірленуші полицияға ресми түрде жүгінген күннің өзінде, тергеу органдары көп жағдайда интернет-алаяқтықты «азаматтық-құқықтық дау» немесе «шарттық міндеттемелерді орындамау» ретінде қате бағалайды. Осыған сүйеніп, ҚР ҚПК-нің 179-бабына (СДТБТ-ға тіркеуге жатпайтын арыздар) сілтеме жасай отырып, қылмыстық іс қозғаудан және арызды тіркеуден негізсіз бас тартады. Бұл жағдай қылмыстың нақты статистикасын жасанды түрде төмендетіп қана қоймай, іс жүзінде онлайн-алаяқтардың жазасыз қалуын заңдастырады. Бұл теориялық тұжырымдар диссертациялық зерттеу аясында құқық қорғау органдарының қызметкері арасында жүргізілген сауалнама нәтижелерімен бұлтартпай дәлелденеді (А қосымшасы). Сауалнамаға қатысушылардың 80%-ы (30%-ы үнемі, 50%-ы ішінара) СДТБТ-ға тіркеу сатысында интернет-алаяқтықты азаматтық-құқықтық міндеттемелерді орындамаудан ажырату кезінде елеулі қиындықтарға тап болатынын растады. Мұның тікелей салдары ретінде сауалнамаға қатысушылардың 50%-ы (20%-ы өте жиі, 30%-ы мерзімді түрде) іс материалдарының азаматтық-құқықтық дау сылтауымен номенклатуралық іске негізсіз шығарылатынын немесе ҚР ҚПК-нің 35-бабымен қысқартылатынын көрсетті. Бұл статистика біз бұрын негіздеген ҚР ҚПК-нің 179-бабының императивтік шектеулеріне байланысты туындайтын «жасанды латенттілік» феноменінің құқық қолдану практикасында жүйелі сипатқа ие екенін объективті түрде айғақтайды.

Латенттіліктің осы субъективті (виктимологиялық) қыры тікелей жәбірленушінің мінез-құлқымен байланысты болғандықтан, құрбандарды ғылыми зерттеулерге сүйеніп нақты типтерге бөлген орынды. Алғашқы топты цифрлық сауаты төмен адамдар құрайды: олар фишингтік сілтеменің қаупін аңғармай, өзінің дербес деректері мен банк реквизиттерін алаяқтың қолына өз еркімен ұсынады. Екінші топты «тез байығысы келетін», ашкөздіктен туатын виктимділік құрайды – мұнда адамдар онлайн-казиноға, жалған инвестициялық жобаға және қаржы пирамидасына біле тұра араласып, ақыры алаяқтардың құрбанына айналады. Үшінші топты бөлек атаған жөн: бұлар – күрделі технологияның, соның ішінде жасанды интеллект пен дипфейктің (deepfake) құрбандары, өйткені мұндай жоғары технологиялық алдау тіпті цифрлық сауаты мол азаматтың өзін психологиялық тұрғыдан адастыра алады.

Киберқылмыстың құрбаны кәмелетке толмаған адам болса, тергеу әрекеттеріне ерекше процестік әрі тактикалық талап қойылады. С.В. Глазатова мен А.И. Бастрыкиннің еңбектерінде негізделгендей [117, 8 б.; 118, 7 б.], баланың жас ерекшелігі мен психологиялық жетілмегендігі ескеріліп, одан жауап алу міндетті түрде психолог, педагог және кәсіби қорғаушы (заңды өкіл) қатысқанда жүргізілуге тиіс; нақ осы кәмелетке толмаған жәбірленушінің қайталама виктимизациясына жол бермей, алынған жауаптың объективтілігін қамтамасыз етеді.

Осы ретте виктимологиялық алдын алу шараларын күшейту кейінге қалдыруға болмайтын міндетке айналады. М.С. Бисалиев пен А.С. Камко тәрізді

ғалымдардың зерттеулері көрсеткендей, халықтың цифрлық сауаттылығын арттыру үшін ақпараттық науқандармен шектелмей, орта мектеп пен жоғары оқу орнының білім беру бағдарламасына «кибергигиена» мен ақпараттық қауіпсіздік негіздері бойынша міндетті курстар енгізу қажет [16, 64 б.; 36, 115 б.]. Сондай-ақ А.А. Пудовкиннің тұжырымдарына сүйеніп, жәбірленушінің бұзылған мүліктік құқығын қалпына келтірудің нақты жолы ретінде транзакцияның күшін жоюдың халықаралық рәсімін (chargeback) ұлттық банк заңнамасы деңгейінде жеңілдетіп бекіту ұсынылады [119, 17 б.]. Бұған қоса, қылмыс ашылмай қалған не қаражат трансшекаралық юрисдикцияларға шығарылып кеткен жағдайда жәбірленушіге жедел материалдық көмек көрсету үшін қаржы ұйымдары мен электрондық төлем жүйелерінің қатысуымен арнайы өтемақы (компенсациялық немесе сақтандыру) қорларын институционалдық түрде бекіту – мемлекеттік қорғаудың ең оңтайлы шешімі. Б.Э. Шавалеевтің пікірінше, осындай компенсациялық тетіктер мен «банктердің ден қою шараларын» жетілдіру ақпараттық технологиялар арқылы жасалатын жымқырудың өсіп келе жатқан көлемін тиімді тежеуге мүмкіндік береді [115, 167 б.].

Аталған сыртқы тосқауыл құқық қорғау жүйесінің өзінің ішкі қайшылықтарымен заңды түрде ушыға түседі. Арыздарды тексеру кезеңінде құқық қолданушы азаматтық-құқықтық дау белгілері бар материалдарды тіркеуге ҚР ҚПК-тің 179-бабында белгіленген тыйыммен императивті түрде бұғауланған, ал жасырын криминалдық белгілерді анықтау «Жедел-іздестіру қызметі туралы» ҚРЗ-ның 11-бабына сәйкес жасырын іс-шаралар кешенін талап етеді. Осы кезеңдегі процестік іркілістің себептерін бағалай отырып, М.Ю. Подваркова іс-әрекетті қате саралауды сөзсіз тудыратын виртуалды децепцияны заңды шарттар түрінде жасанды бүркемелеуге нұсқай отырып, проблеманың түбірін ұйымдастырушылық жазықтықтан көреді [102, 80 б.]. Бұл тәсілге қарама-қарсы К.Н. Евдокимов бейінді мамандардың тапшылығына және ведомствоаралық үндестірудің болмауына байланысты құқық қорғау органдарының ден қоюындағы жүйелі кідірістерден көрініс табатын терең институционалдық дағдарысты диагностикалайды [120, 64 б.]. Аталған көзқарастарды талдау тұжырымдамалық алшақтықты көрсетеді: егер бірінші автор бастапқы себепті бүркемеленген іс-әрекетті құқықтық интерпретациялаудағы қиындықтардан көрсе, онда екіншісі қарсы іс-қимыл аппаратының өзінің құрылымдық-функционалдық дәрменсіздігін дәлелдейді. Біздің ойымызша, қарастырылып отырған ақаулар ҚР ҚПК-тің 179-бабының нормативтік талаптарымен сот төрелігін бұғаттаудың бірыңғай тетігіне интеграцияланады. Тергеудің институционалдық әлсіздігі оны іс қозғалғанға дейін іс-әрекетті әшкерелеу құралдарынан айырады, бұл өз кезегінде органдарды тіркеуден формальды түрде бас тарту үшін азаматтық-құқықтық даудың болуы туралы ұйымдастырушылық желеуді пайдалануға мәжбүрлейді. Демек, жасырын киберқылмыстылық қылмыскерлердің технологиялық мүмкіндіктерін құқық қолданудың ұйымдастырушылық ақауларымен ажырамас байланыстыратын кіріктірілген криминологиялық-процестік феномен болып табылады.

Зерттеліп отырған жүйелі іркілістің ауқымы объективті бағалауды талап етеді, өйткені ресми статистика цифрлық криминализацияның шынайы көрінісін

бұрмалайды. Криминологиялық бағалау модельдерін қолдана отырып, интернет-жымқырулардың жазасыздығы мен жасырындығы деңгейі сыни шекке жететіні туралы біз бұрын мәлімдеген тезис расталады. Осы қауіпті динамиканың процестік салдарын талдай отырып, В.В. Коломинов ақпараттың түсуіндегі толық кешігу кезек күттірмейтін тергеу әрекеттерін уақтылы жүргізуді фатальды түрде салдандыратынын атап көрсетеді [91, 130 б.]. Осы аспектіні тереңдете, Е.С. Шевченко провайдерлердің серверлерінде сақтау мерзімі қатаң шектелген гиперқұбылмалы цифрлық іздердің (логтардың, кэштелген деректердің) қайтарымсыз физикалық жоғалуын тұжырымдай отырып, зерттеу фокусын ұйымдастырушылық кідірістен материалдық-техникалық жазықтыққа ауыстырады [59, 107 б.]. Тәсілдердің айырмашылығы айқын: В.В. Коломинов кідірісті процестік қарқынның жоғалуы ретінде қарастырады, ал Е.С. Шевченко оны іздік көріністің толық жойылу себебі ретінде түсіндіреді.

Осылайша, арызды уақтылы тіркеудің мүмкін еместігі ҚР ҚПК-тің 161-бабында регламенттелген қамтамасыз ету шараларын іске асыруды тікелей бұғаттайды. Нәтижесінде уақыттағы процестік алшақтық қаскөйлерде абсолютті жазасыздық сезімін қалыптастыра отырып және көлеңкелі сериялық инфрақұрылымның дамуын ынталандыра отырып, шығыс операцияларын жедел тоқтата тұруды және шығарылатын электрондық активтерге тыйым салуды жоққа шығарады. Латенттілік, тергеп-тексеруді инициациялаудың институционалдық кідірісі және цифрлық дәлелдемелік базаның жойылуы арасындағы дәлелденген ажырамас себеп-салдарлық байланыс классикалық тергеу алгоритмдерінің эвристикалық әлеуетінің сарқылуын объективті түрде көрсетеді және цифрлық дәлелдемелерді жинаудың, тіркеп-белгілеудің және бағалаудың тұжырымдамалық, процестік және технологиялық ерекшеліктерін егжей-тегжейлі зерттеу қажеттілігін алдын ала айқындайды.

Бұрын анықталған сотқа дейінгі тергеп-тексеруді инициациялау сатысының сал болуын детерминациялайтын нормативтік негіздерді егжей-тегжейлі талдау азаматтық-құқықтық даудың осылайша аталатын «құқықтық елесінің» қалыптасуының ішкі тетігін ашып көрсетуге мүмкіндік береді. ҚР ҚПК-тің 179-бабының телеологиялық мақсаты әдеттегі мүліктік жанжалдарды шешу үшін қылмыстық құдалау құралдарын пайдаланудың негізсіз әрекеттерін іріктеп тастаудан тұрады. Алайда осы норманы цифрлық ортаға экстраполяциялау жүйелі құқық қолдану бұрмалануларына әкеледі. М.Ю. Подваркова негізді түрде атап өткендей, жәбірленушілердің цифрлық интерфейстерге және веб-ресурстардың легитимді дизайнына шамадан тыс сенімі олардың ақшалай қаражатты аудару бойынша сырттай өз еркімен жасайтын әрекеттерін туындатады, бұл тергеу органымен стандартты азаматтық мәміленің белгісі ретінде формальды түрде түсіндіріледі [102, 79 б.]. Нәтижесінде бастапқыда заң шығарушы құқықтық тәртіпті қорғау үшін құрастырған нормативтік сүзгі желілік децепцияны легитимациялаудың институционалдық құралына парадоксальды түрде трансформацияланады.

Аталған құқықтық елес материалдық құқықтың консервативті талаптары арқылы қатаң бекітіледі. ҚР Жоғары Сотының №6 Нормативтік қаулысының 10-тармағы алаяқтықты саралауды шартты жасасқанға дейін немесе жасасу сәтінде

пиғылды міндетті түрде анықтаумен императивті түрде байланыстырады. Желілік жымқыруларда алдау тікелей қашықтан өзара іс-қимыл алгоритміне интеграцияланғандықтан, ал қол сұғушылықтың субъективті жағы желінің анонимділігімен сенімді түрде жасырылғандықтан, криминалдық белгілерді бастапқы анықтау орындалмайтын процестік міндетке айналады. Осы нормативтік диссонанстың салдары ретінде, Н.Ю. Макарова негізді түрде дәлелдегендей, тергеу субъектілерінің киберқылмысты міндеттемелерді орындамаудан (азаматтық-құқықтық даудан) аражігін ажырату қиындығына тап болу фактісі әрекет етеді [121, 20 б.]. Бұл мән-жай арыздарды номенклатуралық іске шығарудың немесе қылмыстық құқық бұзушылық құрамының жалған жоқтығы үшін ҚР ҚПК-тің 35-бабы негізінде іс жүргізулерді негізсіз тоқтатудың жаппай практикасына сөзсіз әкеледі.

Іс-әрекетті СДТБТ-де заңды тіркеуге кедергі келтіретін (ҚР ҚПК-тің 180-бабы) деректердің жасанды жеткіліксіздігінің туындау табиғатын бағалау кезінде ғылымда қатаң бәсекелес екі ұстаным қалыптасты. Бір жағынан, В.В. Коломинов бұл коллапсты объективті процестік тығырықтың болуымен дәлелдейді: бастапқы тексеру сатысында егжей-тегжейлі биллингтік ақпаратқа және цифрлық активтердің транзит маршруттарына легитимді қол жеткізудің болмауы құқық қолданушыға бастапқы қылмыстық пиғылды растауға физикалық түрде мүмкіндік бермейді [91, 103 б.]. Екінші жағынан, В.А. Машлякевич құқық қорғау жүйесі жағдайға техникалық талдау жасау әрекеттерінсіз, тек өтініш берушінің өзінен формальды түрде түсініктемелер алумен шектелетін аса үстірт тексеру іс-шараларын жүргізу арқылы процесті жасанды түрде бұғаттайтынын дәлелдей отырып, субъективті детерминантаның басымдығын үзілді-кесілді алға тартады [79, 98 б.].

Ұсынылған ұстанымдарды талдау алшақтықты көрсетеді: егер бірінші автор жүйелі түрде бас тартуларды процестік инструментарийдің объективті тапшылығымен негіздесе, онда екіншісі дәл сол бас тартуларды құқық қолданушының кәсіби тоқырауының және тіпті қолда бар өкілеттіктер шеңберінде де деректерді жинауды жүзеге асыруға тікелей құлықсыздығының салдары ретінде саралайды. Біздің ойымызша, аталған факторларды оқшауланған түрде қарама-қарсы қою әдіснамалық тұрғыдан қате, өйткені цифрлық орта жағдайында олар бірыңғай тұйық институционалдық циклді құрайды. Қылмыстық іс қозғалғанға дейін криминалистикалық трекингтің мәжбүрлеу шараларын заңды қолданудың объективті заңнамалық мүмкін еместігі тергеушіде материалдың нөлдік перспективасына деген сенімділікті туындатады. Бұл сенімділік субъективті пассивтілікті заңды түрде катализдейді: қолда бар цифрлық артефактілер мен цифрлық деректемелерді мұқият тіркеп-белгілеудің орнына, лауазымды адам аударымның сыртқы еріктілігін ҚР ҚПК-тің 179-бабының бұғаттаушы нормасын қолдану үшін заңдық желеу ретінде қасақана пайдалана отырып, ең аз процестік қарсылық жолын таңдайды.

Фактикалық мән-жайларды осылайша жүйелі түрде қате құқықтық бағалаудың заңды қорытындысы ретінде статистикада көрініс тапқан процестік парадокс әрекет етеді: істерді тіркеудің орасан зор өсуі (2025 жылы 28 851-ге дейін) сотқа жолданған істер үлесінің 10-14% белгісіндегі үрей тудыратын

тоқырауымен қатар жүреді, бұл тергеуді фатальды тығырыққа тіреп, ҚР ҚПК-тің 45-бабы 7-бөлігінің 1-тармағын жаппай қолдануға және дәстүрлі емес «анықталмаған субъектінің латенттілігін» қалыптастыруға әкеледі [6]. Аталған эмпирикалық көрсеткіштер сотқа дейінгі іс жүргізудің дәстүрлі құқықтық сүзгілері киберқылмыстардың алгоритмдік табиғатымен тұжырымдамалық түрде үйлеспейтіндігінің бұлтартпас дәлелі ретінде қызмет етеді. Тергеп-тексеруді инициациялаудың классикалық моделінің реттеушілік әлеуетінің сарқылуы цифрлық дәлелдемелерді жинаудың, тіркеп-белгілеудің және тексерудің процестік, гносеологиялық және технологиялық негіздерін іргелі зерттеу қажеттілігін туындатады.

Жүргізілген зерттеу нәтижелерін жүйелеу онлайн алаяқтықты сотқа дейінгі тергеп-тексеруді инициациялауды бірреттік процестік акт ретінде емес, күрделі үш кезеңдік процестік-криминалистикалық конструкция ретінде қарастыруға мүмкіндік береді. Бұл парадигма өзіне бірізді сатыларды қамтиды: бастапқы ақпаратты жинау (ҚР ҚПК-тің 180-бабы), сигналды жедел тексеру («Жедел-іздестіру қызметі туралы» ҚРЗ-ның 11-бабы) және СДТБТ-де тіркеу арқылы мәліметтерді міндетті процессуализациялау (ҚР ҚПК-тің 179-бабы). Аталған нормативтік модельдің заңдық мәні дәстүрлі түрде азаматтарды қылмыстық процесс орбитасына негізсіз тартудан қорғау үшін өтініштерді бірізді сүзгіден өткізуден тұрады. Алайда цифрлық ортамен соқтығысқан кезде сыни функционалдық деформация айқындалады: конструкция элементтері бір-бірін толықтырмайды, керісінше өзара бұғаттайды. Осы іркілістің табиғатын талдай отырып, В.В. Коломинов нормативтік базада қаланған консервативті процестік шектеулер дәлелдемелік базаның бастапқы тапшылығын еселеп ушықтыра отырып, ерте кезеңдерде виртуалды іздерді уақтылы бекіту мүмкіндігін объективті түрде салдандыратынын дәлелдейді [91, 39 б.].

Анықталған құрылымдық деформация желілік жымқырулар контексінде жай ғана криминологиялық фон емес, процестік тетікті бұзудың деструктивті жүйелі факторы ретінде әрекет ететін бұрын-соңды болмаған латенттілік феноменімен ажырамас байланысты. ҚР ҚК-нің 190-бабының талаптары жымқыру және қасақана алдау фактісін анықтауды императивті түрде ұйғарады. А.Д. Фокиннің ұстанымын талдау кезінде біз бұрын атап өткендей, виртуалды децепцияны заңды азаматтық-құқықтық мәмілелер түрінде бүркемелеу ерекшелігі дұрыс құқықтық бағалауды бұғаттайтын ақпараттық вакуумді қалыптастырады [41, 138-139 б.]. В.В. Коломинов пен А.Д. Фокиннің ұстанымдарын салыстыру жүйелі дағдарыстың бастапқы себептерін түсінудегі іргелі алшақтықты көрсетеді: егер біріншісі проблеманың түбірін құқық қолданушының гиперқұбылмалы цифрлық артефактілерге қол жеткізуін физикалық түрде бұғаттайтын қатаң процестік шеңберден көрсе, онда екіншісі іс-әрекеттің сыртқы заңдылығымен жаңылысқан тергеудің интерпретациялық дәрменсіздігіне назар аударады.

Осы ғылыми пікірталасты шеше отырып, негізделген авторлық ұстанымды тұжырымдаған жөн. Нормативтік тосқауылдар мен құқық қолдану қателерін оқшауланған түрде қарама-қарсы қою әдіснамалық тұрғыдан қате, өйткені киберқылмыстылық жағдайында олар бірыңғай тұйық институционалдық циклді

құрайды. Іс ресми тіркелгенге дейін жасырын цифрлық іздерді кідіріссіз алуға арналған заңды құралдары жоқ қылмыстық қудалау органы қол сұғушылықты шарттық процесс түрінде сырттай бүркемелеуді ҚР ҚПК-тің 179-бабының императивтік тыйымын қолдану үшін ыңғайлы желеу ретінде пайдаланады. Нәтижесінде нормативтік тосқауылдар негізсіз бас тартуларды туындатады, бұл бас тартулар жасырын қылмыстылықтың өсуін қайталама түрде ынталандыра отырып және тергеп-тексеруге арналған толыққанды бастапқы базаның қалыптасуын түпкілікті бұғаттай отырып, теріс құқық қолдану практикасын легитимациялайды.

Анықталған институционалдық паралич жүргізілген зерттеудің ғылыми жаңалығын үш негізгі бағыт бойынша негіздеуге мүмкіндік береді.

Біріншіден, инициациялаудың үш кезеңдік моделі дербес процестік-криминалистикалық конструкция ретінде тұжырымдамаланған, бұл криминалистикалық маңызы бар деректердің қайтарымсыз жоғалу нүктелерін диагностикалауға және дәстүрлі процестің статикалық нысаны мен киберқылмыстылықтың аса жоғары мобильділігі арасындағы іргелі қақтығысты ашып көрсетуге мүмкіндік берді.

Екіншіден, іс-әрекетті технологиялық бүркемелеу бастапқы ден қоюдың процестік-ұйымдастырушылық тығырықтарымен алгоритмдік түрде жымдасқан онлайн алаяқтық латенттілігінің күрделі көпфакторлы табиғаты дәлелденді.

Үшіншіден, К.О. Карабековтың зерттеулерімен эмпирикалық түрде нығайтылған латенттілікті сандық бағалаудың авторлық тәсілі ұсынылды [17, 93 б.]. Осы тұжырымдама шеңберінде латенттілік құрғақ статистикалық қателік ретінде емес, қолданыстағы нормативтік модельдің цифрлық деликтілерге қарсы іс-қимыл жасау үшін жарамсыздық дәрежесін объективті түрде өлшейтін дәл аналитикалық құрал ретінде қарастырылады.

Осылайша, онлайн алаяқтықты сотқа дейінгі тергеп-тексеруді инициациялау сатысы терең жүйелі дағдарыс жағдайында тұр. Толығымен материалдық іздерге және қылмыстық пиғылдың физикалық айқындығына бағдарланған дәстүрлі процестік тетіктер қазіргі заманғы пайдакүнемдік қылмыстылықтың цифрлық табиғатына тұжырымдамалық түрде сәйкес келмейді және қылмыстық қудалауды ең ерте кезеңде салдандырады. Инициациялау сатысының анықталған нормативтік және ұйымдастырушылық шектеулері іс бойынша толыққанды іс жүргізу басталғанға дейін де цифрлық іздік көріністің фатальды бұзылуын қатаң түрде алдын ала айқындайды. Осы дәлелденген процестік вакуум цифрлық дәлелдемелерді жинау, тіркеп-белгілеу және бағалау тетіктерін тұжырымдамалық-құқықтық әрі технологиялық тұрғыдан тереңдете талдауды қажет етеді.

2.2 Қылмыстық процестегі цифрлық дәлелдемелерді жинау, бекіту және бағалау ерекшеліктері

Цифрлық технологиялардың дамуы дәлелдемелік ақпараттың табиғатын түбегейлі өзгертті, бірақ оны қылмыстық-процестік реттеу тұжырымдамалық жағынан әлі аяқталмаған, үзік-үзік күйінде қалып отыр. Қазақстан

Республикасының қолданыстағы қылмыстық-процестік заңнамасы дәлелдемелердің физикалық жеткізгіштеріне қатаң иек артуын жалғастыруда. Атап айтқанда, ҚР ҚПК-нің 111-бабы дәлелдеме деп хаттамаларда және өзге де құжаттарда қамтылған нақты деректерді таниды, ал 120-бабы соңғыларының қатарына компьютерлік ақпаратты қамтитын материалдарды жатқызады. Оның үстіне ҚР ҚК-нің 3-бабы «электрондық жеткізгішті» ақпаратты сақтауға арналған материалдық объект деп қана, императивті түрде айқындайды.

Бұл нормативтік модель ғылымда В.Я. Дорохов ұсынған дәлелдеудің классикалық теориясына сүйенеді: ол ақпаратты тіркеп-белгілеу тарихи тұрғыдан қолмен ұстауға келетін материалдық іздерге негізделетінін, мұнда физикалық нысан мазмұнмен ажырағысыз байланыста болатынын тұжырымдайды [123, 112 б.]. Алайда қылмыстылықтың цифрлануы осы парадигманы қайта қарауды талап етеді. Бірқатар заманауи зерттеуші, мәселен В.А. Мещеряков, нақты аппараттық құрылғыға тәуелсіз виртуалды іздердің дербес ақпараттық табиғатын тану керектігін орынды көрсетеді [123, 74-76 б.]. Осы тұжырымдарға сүйеніп әрі Қазақстан Республикасы қылмыстық-процестік заңнамасының өзгешелігін ескеріп, ҚР ҚПК-те «цифрлық дәлелдеме» ұғымын бекіткен жөн деп есептейміз. Ол – виртуалды ортада тергеп-тексерілетін оқиғаның мән-жайын объективті түрде көрсететін, тұтастық, қайта жаңғыртылымдық және атрибутталымдық қасиеттеріне ие тіркеп-белгіленген ақпараттық құрылым.

Бұл теориялық қайшылық құқық қолдану практикасына тікелей түседі, онда құқықтық жүйе виртуалды деректерді дәстүрлі институттарға жасанды түрде бейімдеуге тырысады. Ұлттық сот ісін жүргізу моделін талдай отырып, А.А. Толыбаева және тең авторлар ҚР ҚПК нормалары цифрлық деректерді классикалық заттай дәлелдемелердің немесе құжаттардың архаикалық шеңберіне күштеп сыйғызатынын тұжырымдайды [98, 133 б.]. Мұның практикалық салдары ретінде алып қоюды регламенттейтін ҚР ҚПК-тің 118-бабын қолдану тәртібі әрекет етеді: құқық қолданушы іздестіріліп отырған ақпараттың өзін емес, физикалық жабдықты алып қоюға мәжбүр. Бұл аспектіні тереңдете отырып, М.С. Бисалиев цифрлық дәлелдемелердің базалық нормативтік дефициясының болмауы оларды тіркеп-белгілеу және алып қою рәсімдерінің сыни белгісіздігіне әкеп соғатынына, бұл бұлтты есептеулер мен бөлінген желілер жағдайында техникалық тұрғыдан мағынасыз болып табылатынына назар аударады [16, 12-13 б.]. Проблемаға өзге қырынан А.И. Зазулин келеді, ол фатальды құқық қолдану тығырығын көрсетеді: заңның деректердің денесіз табиғатын толық елемеуіне байланысты тергеушілер жиі физикалық түрде қолмен ұстауға болатын заттың болмауын дәлелдеменің мүлдем болмауымен теңестіреді [114, 112-113 б.]. М.С. Бисалиев пен А.И. Зазулиннің ұстанымдарын салыстыру зерттеу фокустарының айырмашылығын айқындайды: егер бірінші автор проблеманың түбірін трансұлттық желілермен жұмыс істеу кезінде нормативтік талаптардың техникалық орындалмауынан көрсе, онда екіншісі физикалық объектілер санаттарымен ойлауды жалғастыратын процестік ойлаудың өзінің іргелі ақауын диагностикалайды.

Анықталған доктриналық және заңнамалық коллизияларды шеше отырып,

негізделген авторлық ұстанымды тұжырымдау қажет. Дәлелдеудің ескірген материалистік парадигмасын сақтау терең нормативтік вакуумді қалыптастырады. Іздері қашықтағы серверлер бойынша бөлінген кибержымқыруларды тергеп-тексеру кезінде материалдық жеткізгіштерді алып қою туралы заң талабы қылмыстық сот ісін жүргізуді объективті түрде бұғаттайды. Қалыптасқан терминологиялық диссонансты еңсеру мақсатында айналымға мынадай авторлық дефиницияны енгізу ұсынылады: цифрлық дәлелдеме – цифрлық ортадағы криминалдық оқиғаларды объективті түрде көрсететін және тұтастық, қайта жаңғыртылушылық және атрибутталушылық қасиеттеріне ие тұрақты тіркеп-белгіленген ақпараттық құрылым. Цифрлық іздерді дәл осылай тұжырымдамалық түсіну қылмыстық сот ісін жүргізудегі қазіргі заманғы дәлелдемелік базаның сенімді іргетасын қалыптастырады [124, 77 б.]. Бұл тәсілдің ғылыми маңыздылығы деректерді материалдық объектіге архаикалық түрде байлаудан түпкілікті бас тартудан және виртуалды іздердің криминалистикалық сипаттамаларын дәлелдемелердің жол берілуінің іргелі процестік кепілдіктерімен органикалық интеграциялаудан тұрады.

Цифрлық ақпараттың сақталып отырған заңды мәртебесінің белгісіздігі онлайн алаяқтық туралы істер бойынша дәлелдеудің барлық кейінгі сатыларында жүйелі құқық қолдану проблемаларын детерминациялайды. Консервативті тергеу рәсімдерінің гиперқұбылмалы желілік ортамен анықталған үйлесімсіздігі таным объектісін тұжырымдамалық түрде қайта ұғынудың ғылыми қажеттілігін туындатады. Бұл институционалдық тосқауылды жою тікелей ақпараттық-телекоммуникациялық кеңістікте цифрлық іздерді генерациялау, тіркеп-белгілеу және олардың заңды түрде деградацияға ұшырау тетіктеріне егжей-тегжейлі трасологиялық талдау жүргізуді талап етеді.

Цифрлық дәлелдемелердің тұжырымдамалық табиғатын ашу үшін оларды қалыптастырудың базалық тетігін криминалистикалық трасология тұрғысынан, әрі қолданыстағы нормативтік реттеудің қатаң аясында зерттеуге тура келеді. Қылмыстық-процестік заңнаманың негізгі ережелері, атап айтқанда ҚР ҚПК-нің 118 және 120-баптары, тарихи тұрғыдан классикалық механистік модельге сүйенеді, онда із тек бір физикалық объекті белгілерінің екіншісінде материалдық бейнеленуі ретінде ғана түсініледі. Бұл архаикалық конструкцияға қарама-қарсы, ҚР Цифрлық Кодексінің 16 және 76-баптарының жаңа ережелері виртуалды артефактілердің мүлдем өзге – ақпараттық, материалдық емес мәнін бекітеді [125]. Осы нормативтік-гносеологиялық қақтығысты талдай отырып, В.Б. Вехов киберкеңістікте дәстүрлі физикалық (контактілі) өзара іс-қимыл электромагниттік импульстер арқылы ақпараттық бейнеленуге толығымен жол беретінін әділетті түрде атап өтеді [70, 84-85 б.]. Бұл іргелі ойды дамыта және нақтылай отырып, А.Н. Колычева желілік іздердің кеңістіктік физикалық нысанының толық болмауын тұжырымдайды, олардың деректермен алмасудың қатаң хаттамаларына абсолютті алгоритмдік бағыныштылығын атап көрсетеді [126, 39 б.]. Аталған доктриналық және нормативтік тәсілдердің синтезі авторлық ұстанымды тұжырымдауға мүмкіндік береді: виртуалды із түзілудің қазіргі заманғы құрылымы механикалық әсер етуді емес, «із түзуші – іздік орта – із қабылдаушы объект» триадасын білдіреді, мұнда заң (ҚР ҚПК) парадоксальды

түрде объективті түрде тек машинамен оқылатын жазбаларды жүйелі түрде беру және маршруттау орын алатын жерде қолмен ұстауға болатын физикалық өзгерістерді іздеуді талап етеді.

Сипатталған тетіктің күрделі алгоритмдік құрылымы генерацияланатын артефактілерді әр алуан етеді, ал бұл оларды нақты құқықтық жүйелеуді қажет етеді. Заң шығарушы түрлі көздермен жұмыс істеуге белгілі бір процестік құралдарды арнаған: абоненттердің қосылыстары туралы ақпаратты алу (ҚР ҚПК-нің 244-бабы) және серверлерден деректерді жасырын түсіріп алу (ҚР ҚПК-нің 245-бабы). Осы нормативтік шеңберге сүйене отырып, В.Б. Вехов электронды-цифрлық іздерді екі іргелі топқа бөлуді ұсынады: іздер-бейнеленулер (файлдар, бағдарламалар, деректер базасы) және іздер-заттар (материалдық тасымалдаушылар, компьютерлік желілер) [70, 81 б.]. Бұған қоса, Р.Б. Джилкишиевтің виртуалды іздерді олардың өзгеруіне қарай жіктеу тәсілін де (пайда болу, жойылу және модификациялану іздері) ескерген маңызды [57, 60-61 б.]. Цифрлық іздердің негізгі криминалистикалық сипаттамаларына файл өлшемі, оның құрылу және өзгеру уақыт белгілері, сондай-ақ лог-файлдардағы жазбалар жатады. Осы сипаттамаларды «72 сағат» шұғыл алгоритмі аясында дұрыс бекіту гиперқұбылмалы дәлелдемелердің деградацияға ұшырап, жойылу қаупін азайтады. Дегенмен құқық қолдану тетігі бір қиындыққа тіреледі: объективті дәлелдемелік ақпарат бірнеше тәуелсіз із қабылдаушы объект пен телекоммуникациялық провайдер юрисдикциясының арасында бөлініп кетеді. Цифрлық артефактілермен қатар виртуалды децепция тетігі жауап алу арқылы бекітілетін (ҚР ҚПК-нің 115-бабы) идеалды іздерді де сөзсіз қалыптастырады, бірақ байланыссыз алаяқтық жағдайында олар легитимді интерфейстерді қабылдаудан туатын когнитивтік елестердің әсерінен қатты бұрмаланады. Түрлі типтегі іздердің тұрақтылық қасиеті түбегейлі бөлек болғандықтан, әрқайсысын анықтауға өзге тетік керек – нақ осы жайт процестік дәлелдеудің басты тосқауылына айналады.

Цифрлық артефактілердің өмір сүру мерзімі әрқилы болуы олардың уақыттық динамикасын криминалистиканың орталық проблемасына айналдырады. Дәлелдемелердің жоғалу себебін бағалай отырып, В.Б. Вехов желілік және транзакциялық іздердің пассивті деградациясына тоқталады әрі олардың жоғалуын объективті аппараттық стандарттармен және провайдерлердің тәуелсіз серверлерінде деректерді сақтаудың қатаң шектеулі мерзімімен түсіндіреді [70, 269 б.]. Осы аппараттық бағдарланған тәсілден айырмашылығы, Е.С. Шевченко криминалистикалық маңызы бар ақпараттың жойылуының басты себебі ретінде оның гиперқұбылмалылығы және қаскөйлердің өздерінің қашықтан берілетін командалар мен автоматты тазарту скрипттері арқылы секунд үлестерінде белсенді, мақсатты түрде жоюы әрекет ететінін дәлелдейді [59, 107 б.]. Ұсынылған көзқарастарды талдау іздердің жоғалу табиғатын түсінудегі алшақтықты көрсетеді: егер біріншісі оны инфрақұрылымның қалыпты институционалдық шектеулерімен (пассивті фактор) байланыстырса, онда екіншісі деградацияны криминалдық ортаның қасақана техникалық қарсы іс-қимылының нәтижесі (белсенді фактор) ретінде саралайды.

Біздің ойымызша, «цифрлық іздердің жеделдетілген деградациясы» тұжырымдамасын бөліп көрсету орынды. Бұл процесс инфрақұрылымдық (пассивті) және криминалдық (белсенді) факторлардың жиынтық әсерімен шартталған, бұл сотқа дейінгі тергеп-тексеру органдары дәлелдемелерді заңды процестік тіркеп-белгілеуді жүзеге асыруға қабілетті болатын кезеңді объективті түрде қысқартады. Жымқырылған активтерді криптовалютаға лездік конвертациялауды немесе оларды дропперлердің көпдеңгейлі тізбектері арқылы аударуды қамтитын желілік қол сұғушылықты монетизациялау ҚР ҚПК-тің 244 және 245-баптары бойынша санкцияланған іс-шараларды тергеу процестік түрде инициациялап үлгергенге қарағанда алгоритмдік тұрғыдан айтарлықтай тезірек жүзеге асырылады. Цифрлық із түзілудің гиперқұбылмалы табиғаты мен қылмыстық процестің консервативті қарқыны арасындағы жылдамдықтардың дәлелденген асимметриясы артефактілердің өмір сүру ұзақтығындағы айырмашылық сәл ғана кідіріс кезінде дәлелдеудің бірыңғай тізбегінің үзілуін сөзсіз тудыруына әкеледі.

Цифрлық іздердің жеделдетіліп деградациялануы тұжырымдамасы тәжірибелік қызметкерлердің нақты көрсеткіштерімен расталады. Жүргізілген сауалнамаға сәйкес (Қосымша А), сауалнамаға қатысушылардың 60%-ы интернет-провайдерлер мен банктерден жауап алу мерзімдерінің сыни түрде созылып кететінін (45%-ы 10-нан 30 тәулікке дейін, 15%-ы 30 тәуліктен астам) атап өтті, бұл криминалистикалық ақпараттың фатальды жоғалуына әкеледі. Бұған қоса, сауалнамаға қатысқандардың 40%-ы өз тәжірибесінде қылмыскерлердің тәркіленген құрылғылардағы ақпаратты қашықтан (дистанциялық түрде) жойып жіберу (remote wipe) жағдайларымен тікелей бетпе-бет келген. Осы технологиялық қатерді сезіне отырып, тергеушілердің 65%-ы тінту және алу барысында компьютерлік техниканы тәркілеу кезінде IT-маманның қатысуын үзілді-кесілді міндетті деп санайды. Бұл эмпирикалық деректер дәстүрлі қағаз сұрау салулар мен аппараттық құрылғыларды арнайы радиоэлектрондық оқшаулаусыз жай ғана алып қоюдың виртуалды ортада мүлдем тиімсіздігін көрсетеді.

Трасологиялық және нормативтік талдау нәтижелерін қорытындылай келе, ұсынылған модель дәлелдемелік ақпараттың үздіксіз жоғалуының объективті процесін ғылыми түрде түсіндіруге мүмкіндік беретінін тұжырымдау қажет. Виртуалды іздердің анықталған ақпараттық тұрақсыздығы цифрлық дәлелдемелерді тікелей жинау кезеңінде құқық қолданушы бетпе-бет келетін қолданыстағы процестік нысандар мен нақты технологиялық тосқауылдарға сыни талдау жасау қажеттілігін туындатады.

Цифрлық іздердің табиғатын тұжырымдамалық талдаудың табиғи жалғасы – оларды жинаудың сыни сатысын зерттеу, ал бұл сатының тиімділігі қолданылатын процестік құралдардың орындылығына тікелей тәуелді. Осы кезеңнің нормативтік негізі – ҚР ҚПК-нің 118, 122, 252 және 253-баптары, олар тарихи тұрғыдан тек құқық бұзушылық қаруы не құралының физикалық белгісі бар материалдық объектілерді табуды, бекітуді және алып қоюды реттейді. Осы нұсқаулардың цифрлық ортадағы әсерін бағалай отырып, М.С. Бисалиев классикалық нормаларды механикалық түрде қолдану дәлелдеу процесін

бұрмаламай қоймайтынын дәлелдейді: виртуалды ақпарат өзінің экстерриториялық болмысынан айырылып, аппараттық құрылғыға жасанды түрде байланып қалады [16, 85 б.].

Эмпирикалық база цифрлық ізді жалғыз құрылғыға телу процестік фикция екенін растайды, өйткені қаскүнемдер іс жүзінде аппаратураны әдейі көптеп, қосарлап пайдаланады. Мәселен, №3570-20-00-1/149 қылмыстық ісі бойынша (Қарағанды қаласы Октябрь аудандық сотының 2020 жылғы 11 желтоқсандағы үкімі) [51] қылмыстық топтың қызметінің жолын кесу кезінде заттай дәлелдемелер ретінде үнемі ауыстырылып тұратын ондаған SIM-карталарымен бірге әртүрлі маркалы («iPhone», «Samsung Galaxy», «Huawei», «Redmi») оннан астам смартфон алып қойылды. Бұл құрылғылар әртүрлі жалған аккаунттарды әкімшілендіру және дроптардың атына ресімделген банктік карталарға байлау үшін синхронды түрде пайдаланылғаны анықталды. Әрбір транзакция немесе профиль үшін жеке физикалық торап бөлінетін мұндай техногендік артықтық жекелеген жеткізгіш бойынша дәстүрлі криминалистикалық сәйкестендіруді көрінеу тиімсіз етеді.

Нормативтік ақауларды талдауды дамыта отырып, А.А. Толыбаева және тең авторлар алып қоюдың консервативті талаптарының құбылмалы деректердің ерекшелігіне тікелей сәйкес келмеуінен және бөлінген ақпаратты қашықтан жинауды егжей-тегжейлі регламенттеудің толық болмауынан көрініс табатын терең рәсімдік коллизияны диагностикалайды [98, 130 б.]. Осы ұстанымдарды талдау зерттеу фокустарының айырмашылығын көрсетеді: егер М.С. Бисалиев объектінің онтологиялық бұрмалануына (іздестіріліп отырған деректерді физикалық жеткізгішпен алмастыруға) назар аударса, онда А.А. Толыбаева бастаған авторлар ұжымы деформацияның бастапқы себебін қашықтан алып қою тетіктері бөлігінде абсолютті процестік вакуумнің болуынан көреді. Біздің ойымызша, заң шығарушының материалистік тұжырымдаманы қатаң ұстануы қашықтағы серверлерде орналасқан криминалистикалық маңызы бар ақпараттық құрылымды қылмыстық юрисдикциядан тыс қалдыра отырып, құқық қолданушыны пластик пен металды алып қоюды процестік түрде рәсімдеуге мәжбүрлейді. Мұның заңды салдары ретінде тергеудің байланыс операторлары мен банктерге сұрау салуларды жіберудің бюрократияландырылған тетігіне мәжбүрлі түрде өтуі әрекет етеді.

Ұйымдардан мәліметтерді талап етіп алдыру арқылы деректерді жинау тетігін іске асыру өткір темпоральды-технологиялық қақтығысты айқындайды. ҚР ҚПК-тің 122-бабының талаптарына орай банктік немесе заңмен қорғалатын өзге де құпияны құрайтын ақпаратты талап етіп алдыруға тек прокурордың санкциясымен ғана жол беріледі, бұл сөзсіз уақытша кідірістерді туындатады. Кибержымқыруларды тергеп-тексеру жағдайында бұл процестік баяулық технологиялық ортаның агрессивті қарсы іс-қимылымен бетпе-бет келеді. Осы факторды зерттей отырып, А.А. Калиев криминалдық инфрақұрылым мәліметтерді дешифрленген түрде дәстүрлі ұстап қалуды жоққа шығаратын криптографиялық қорғауды, өтпелі шифрлауды және желілік анонимизациялау технологияларын (VPN, пияздық маршрутизаторлар) жаппай қолданатынын атап көрсетеді [127, 298-299 б.]. Цифрлық қарсы іс-қимыл көрінісін толықтыра

отырып, Н.С. Зиновьева бұлтты архитектуралардың бөлінген сипатына нұсқайды, мұнда фрагменттелген дәлелдемелер ұлттық юрисдикция шегінен шығарылып қана қоймай, лог-файлдарды автоматты түрде циклдік қайта жазу алгоритмдері арқылы жүйелі түрде жойылуға ұшырайды [128, 152 б.]. А.А. Калиев пен Н.С. Зиновьеваның ұстанымдарын салыстыру кезінде технологиялық тосқауылдың табиғатын бағалауда тұжырымдамалық алшақтық айқындалады: біріншісі тергеп-тексеруді бұғаттауды қылмыс субъектілерінің бүркемелеу құралдарын белсенді қолдануымен байланыстырады, ал екіншісі еңсерілмейтін кедергі ретінде бұлтты сервистердің өздерінің пассивті, автоматтандырылған архитектурасы әрекет ететінін дәлелдейді. Анықталған алшақтық кешенді авторлық ұстанымды негіздеуге мүмкіндік береді: сұрау салуларды санкциялау рәсімінің формализациялануы қаскөйлердің белсенді криптографиясымен де, инфрақұрылымның пассивті алгоритмдерімен де шешілмейтін қақтығысқа түседі. Құқық қорғау органы құпияға қол жеткізуді заңдастырудың рәсімдік сатыларын еңсергенше, технологиялық орта тергеудің нормативтік рұқсат етілген мерзімдерін дәлелдемелердің жойылуының сыни факторына айналдыра отырып, іздік көріністі кепілді түрде нөлге түсіріп үлгереді.

Аталған нормативтік-технологиялық алшақтық терең институционалдық дағдарыстың салдарынан құқықтық нұсқамаларды практикалық іске асыру деңгейінде еселеп күшейе түседі. Заң шығарушы виртуалды іздерді жинау ерекшелігін ұғына отырып, ҚР ҚПК-тің 80 және 126-баптарында ғылыми-техникалық құралдарды пайдалана отырып жәрдем көрсету үшін маманды тарту кепілдігін бекітті. Алайда құқық қолдану тетігі осы нормалардың іс жүзіндегі дәрменсіздігін көрсетеді. Институционалдық тығырықтың себептерін бағалай отырып, К.Н. Евдокимов бөлінген желілік артефактілерді заңды түрде сауатты және зақымдамай шығарып алуға қабілетті цифрлық криминалистика саласындағы бейінді мамандардың өткір кадрлық тапшылығының болуын тұжырымдайды [20, 237 б.]. Таза кадрлық тәсілге қарама-қарсы, В.А. Мещеряков проблеманың түбірі тергеу бөлімшелерінің мамандандырылған аппараттық-бағдарламалық кешендермен жеткіліксіз техникалық жарақтандырылуында жатқанын, оларсыз тіпті құзыретті қызметкер болғанның өзінде виртуалды іздерді декодтау объективті түрде мүмкін емес екенін үзілді-кесілді дәлелдейді [55, 38-39 б.]. Келтірілген ұстанымдарды талдау детерминанттардың басымдығы туралы айқын пікірталасты көрсетеді: К.Н. Евдокимов адами капиталды басты орынға қояды, ал В.А. Мещеряков – материалдық-техникалық базаны. Кадрлық осалдық пен аппараттық сарқылу бөлінбейтін деструктивті симбиозды құрайтыны туралы авторлық қорытындыны тұжырымдау негізделген деп саналады. Блокчейн-желілерге мониторинг жүргізуге арналған озық аналитикалық құралдардың болмауы ҚР ҚПК-тің 80 және 126-баптарының нормаларын жұмыс істемейтін декларацияларға айналдыра отырып және мемлекеттің шифрланған мәліметтерді жинауды жүзеге асыру қабілетін түпкілікті салдандыра отырып, кез келген маманның құзыреттерін жоққа шығарады.

Дәлелдемелерді жинау сатысына проблемалық-нормативтік талдау жасау нәтижелерін қорытындылай келе, онлайн алаяқтық туралы істер бойынша бүкіл

дәлелдеу процесінің жүйелі деформациясының болуын тұжырымдау қажет. Цифрлық деректерді толыққанды және уақтылы бекітудің мүмкін еместігі негативті факторлардың кешенді триадасының: процестік архаикалықтың, агрессивті технологиялық қарсы іс-қимылдың және тергеу аппаратының институционалдық әлсіздігінің бір мезгілде және ажырамас әсер етуімен детерминацияланған. Қылмыстық сот ісін жүргізудің дәстүрлі әдістері базалық айғақтарды іздеу кезеңінде-ақ тергеп-тексерудің жалпы тиімділігін сыни түрде төмендететін виртуалды қол сұғушылықтар алдында мүлдем дәрменсіз болып шығады. Алып қоюдың консервативті рәсімдерін ақпараттың құбылмалы массивтеріне бейімдеудің дәлелденген практикалық мүмкін еместігі кейінгі сатыларда фатальды процестік қайшылықтардың туындауын логикалық түрде алдын ала айқындайды және виртуалды іздерді процестік тіркеп-белгілеудің конструктивті ақауларына егжей-тегжейлі талдау жасау қажеттілігін туындатады.

Цифрлық деректерді жинау процесінің логикалық жалғасы ретінде онлайн алаяқтықты тергеп-тексеру жағдайында қолданыстағы қылмыстық-процестік нысанның іргелі конструктивті ақауларын көрсететін оларды міндетті түрде процестік бекіту әрекет етеді. Заңға сәйкес, нақты деректер хаттамаларда тіркелгеннен кейін ғана дәлелдемелер ретінде пайдаланылуы мүмкін, бұл ретте ҚР ҚПК-тің 120-бабы компьютерлік ақпаратты қамтитын материалдарды дәстүрлі құжаттарға формальды түрде теңестіреді. Осы нормаларды қолдану тетігін интерпретациялай отырып, А.А. Аубакирова процестік нысан тарихи түрде егжей-тегжейлі сипаттамалық хаттамалар жасау арқылы физикалық іздерді материалдандыруға бағдарланғанын дәлелдейді [129, 29 б.]. Классикалық тәсілмен тікелей полемикаға А.А. Толыбаева бастаған авторлар ұжымы түседі, олар ҚР ҚПК-те бекітілген хаттамалауға қойылатын талаптар аса маңызды цифрлық метадеректер мен жүйелі автоматтандырылған журналдарды құқықтық өріс шеңберінен тыс қалдыра отырып, цифрлық құжаттаманың ерекшелігін мүлдем ескермейтінін тұжырымдайды [98, 132-133 б.]. Ұсынылған ғылыми ұстанымдарды салыстыру айқын тұжырымдамалық қайшылықты диагностикалауға мүмкіндік береді: дәстүрлі парадигма материалдық объектіні егжей-тегжейлі визуалды сипаттауды талап етеді, ал қазіргі заманғы тәсіл гиперқұбылмалы және жасырын электрондық ақпарат үшін мұндай тіркеп-белгілеудің толық дәрменсіздігін дәлелдейді.

Анықталған алшақтықты шеше отырып, авторлық ұстанымды тұжырымдау қажет: консервативті қағаз конструкцияларды виртуалды іздердің денесіз табиғатына механикалық түрде қолдану объективті түрде қате болып табылады. Қолданыстағы процестік нысан бекіту сатысын институционалдық тоскауылға айналдыра отырып, дәлелдемелерді тиісінше, криминалистикалық тұрғыдан дәйекті тіркеп-белгілеуді қамтамасыз етуге қабілетсіз.

Дәстүрлі бекіту нысанының цифрлық деректерге шектеулі қолданылуы құқық қолдану практикасының тұрақты типтік ақауларын туындатады. ҚР ҚПК-тің 199-бабы тергеу әрекетінің хаттамасында қолданылатын ғылыми-техникалық құралдарды, оларды пайдалану шарттарын және әсер ету объектілерін көрсетуді императивті түрде талап етеді. Іс жүзінде бұл норма өрескел бұрмаланады: тіркеп-белгілеу рәсімі жазбаны бұғаттайтын мамандандырылған аппараттық-

бағдарламалық қамтылымды қолданбай, скриншоттарды басып шығару арқылы экранды визуалды қарап-тексеруге сайып келеді, бұл бастапқы цифрлық кодты түзетелмейтіндей етіп бұзады. Осы кезде туындайтын қателердің табиғатын талдай отырып, А.Н. Колычева басты ақауды желілік өзара іс-қимылдың сыртқы атрибуттарының фатальды бұрмалануынан, атап айтқанда уақыттық параметрлерді (серверлік және локальды уақыттың рассинхронизациясы) және абоненттік құрылғылардың дараландырушы белгілерін тіркеп-белгілеу кезіндегі өрескел дәлсіздіктерден көреді [126, 114 б.]. Проблеманы өзге көзқараспен С.З. Шихалиева зерттейді, ол технологиялық стандарттарды жаппай сақтамаудың, атап айтқанда – алып қойылатын файлдың криптографиялық хеш-сомасын есептеу және процестік бекіту қажеттілігін толық елемеудің салдарынан дәлелдеменің ішкі құрылымының бұзылуына назар аударады [130, 261 б.]. Ғылыми тәсілдердің анықталған айырмашылығы процестік ақаудың екіжақты табиғатын көрсетеді: егер біріншісі іздің оқиғамен кеңістіктік-уақыттық байланыстарының жоғалуына фокусталса, онда екіншісі оның тұтастығы мен өзгермейтіндігінің математикалық кепілдігінің сыни жоғалуын дәлелдейді.

Осы аспектілерді синтездей отырып, тергеу әрекетінің мәтіндік хаттамасы жасырын метадеректерді де, транзакциялар логтарын да, математикалық алгоритмдерді де барабар көрсетуге объективті түрде қабілетсіз екенін тұжырымдау қажет. Нәтижесінде примитивті сипаттамалық тәсіл цифрлық артефакт пен тергеп-тексерілетін онлайн алаяқтық оқиғасы арасындағы гносеологиялық байланысты толығымен үзеді.

Осы жол таңдалған сәтте дәлелдеменің сақталу тізбегі (chain of custody) үзіледі, ал үзілістің ақыры белгілі: цифрлық артефакт жол берілмейтін деп танылу қатеріне тап болады – озық шетелдік тергеу тәжірибесін салғастыра зерделеу дәл осы заңдылықты бекітеді [131, 7 б.]. Тіркеудің мұндай құрылымдық ақаулары істің алдағы соттық тағдырын бірден нашарлатады. ҚР ҚПК-нің 112-бабы бұл тұста біржақты: процестік әрекеттің жүргізілу тәртібі елеулі бұзыла отырып алынған мәлімет дәлелдеу қауқарынан айырылады. Норманың нақты қолданысын саралаған М.С. Бисалиев отандық соттардың цифрлық деректерге әдеттен тыс қатаң өлшемдер таңатынын көрсетеді: құрылғыны қарау кезінде куәгерлердің шақырылмауы да, ҚР ҚПК-нің 126-бабы талап ететін сертификатталған құрал-жабдық көрсетілмей жасалған көшірме де – бәрі бірдей дерлік дәлелдемені алып тастауға желеу болады [16, 96-97 б.]. Бұл ұстанымға дәлелдеудің жалпы теориясы тарапынан қарсы дауыс та естіледі. В.С. Балакшин таза рәсімдік сылтаумен дәлелдемені шеттету мәліметтің шынайылығын мазмұны жағынан сынап-байқау міндетін негізсіз ысырып тастайтынын алға тартып, мұндай тәжірибені өткір айыптайды [132, 363 б.]. Екі көзқарастың аражігі – терең теориялық-құқықтық жарылым: біріншісі үшін заң әрпін мүлтіксіз ұстану жол берілушіліктің тіреуі болса, екіншісі нақ сол формализмнен объективті ақиқатты құртатын құралды аңғарады.

Біздің ойымызша, цифрлық орта жағдайында қорғау тарапы процестік нысанның архаикалығын басты қару ретінде тиімді пайдаланатынын мойындау қажет. Қағаз хаттамалардың толық болмауына байланысты файлдардың аутентиктілігін сәтті даулау формальды бұзушылықтардың деректердің

объективті дәлелдемелік құндылығын толығымен жоққа шығаруына әкеліп, кибержымқыру туралы техникалық дәйекті ақпаратты заңдық тұрғыдан түкке тұрғысыз материалға айналдырады.

Ескірген нормативтік база, ақаулы құқық қолдану практикасы және теріс соттық салдарлар арасындағы анықталған қайшылықтарды қорытындылай келе, тұрақты «цифрлық нигилизм» феноменінің қалыптасуының авторлық тұжырымдамасын негіздеуді қажет деп санаймыз. Бұл құбылыстың мәні тергеп-тексеру субъектілерінің виртуалды дәлелдемелерді тіркеп-белгілеуге қойылатын ерекше технологиялық талаптарды (хештеуден бас тарту, метадеректерді елемеу) жүйелі және саналы түрде елемеуінен және оларды қағаз актілерін примитивті түрде жасаумен алмастыруға тырысуынан тұрады. Цифрлық нигилизм тергеудің оқшауланған тактикалық қателігі емес, терең когнитивтік диссонанстың заңды нәтижесі болып табылады: құқық қолданушы ұшпа және оңай түрлендірілетін цифрлық ақпаратпен бетпе-бет келе отырып, қолмен ұстауға болатын физикалық заттар санаттарымен ойлауды жалғастырады.

Баяндалғанды қорытындылай келе, қылмыстық-процестік заңнамада біріздендірілген техникалық-құқықтық стандарттардың болмауы және дәстүрлі бекіту нысанының цифрлық іздер табиғатына абсолютті сәйкес келмеуі олардың заңдық маңызының қайтарымсыз төмендеуіне әкеледі деп қорытындылау қажет. Ақаулы тіркеп-белгіленген цифрлық ақпарат объективті түрде жан-жақты және заңды процестік бағалаудың пәні ретінде әрекет ете алмайды. Бұл тұжырымдамалық кедергі сот төрелігі виртуалды артефактілермен жұмыс істеудің қорытынды сатысында – оларды тікелей бағалау процесінде бетпе-бет келетін когнитивтік-әдіснамалық тосқауылдар мен шектеулерді іргелі зерттеу қажеттілігін туындатады.

Жинау және процестік бекіту процестерінің заңды қорытындысы ретінде дәлелдеудің қорытынды сатысы – цифрлық дәлелдемелерді бағалау әрекет етеді. Қылмыстық-процестік заңнама ҚР ҚПК-тің 125-бабының императивті қағидасын бекітеді, оған сәйкес әрбір дәлелдеме қатыстылығы, жол берілетіндігі, анықтығы тұрғысынан бағалануға жатады, ал олардың жиынтығы тергеп-тексеру субъектісінің ішкі сенімі бойынша бағаланады. Алайда осы классикалық стандартты онлайн алаяқтықты тергеп-тексеру ерекшелігіне экстраполяциялау құқық қолданушының іргелі когнитивтік-әдіснамалық тосқауылдарын айқындайды. Криминалистикалық ойлаудың тұжырымдамалық негіздерін зерттей отырып, Д.В. Бахтеев қауіпті когнитивтік бұрмалауды диагностикалайды: тергеушінің санасы электрондық құжаттың сыртқы нысанын абсолютті ақиқат ретінде қабылдап және оның шығу тегінің күрделі алгоритмдік табиғатын толығымен елемей, визуалды қабылданатын ақпаратты (скриншоттарды, графикалық интерфейстерді) асыра бағалауға бейім [133, 231 б.]. Осы тезисті дәлелдеу теориясы тұрғысынан тереңдете отырып, А.И. Зазулин цифрлық ақпарат бағдарламалық-аппараттық декодтаусыз адаммен тікелей қабылдана алмайтынын, соның салдарынан тергеушілер жасырын техникалық сипаттамаларды (метадеректерді, хеш-сомаларды, жүйелік логтарды) терең талдауды жай ғана визуалды көзбен шолумен жүйелі түрде алмастыратынын үзілді-кесілді көрсетеді [114, 112-113 б.]. Ұсынылған ұстанымдарды салыстыру

проблеманың өзара толықтырушы аспектілерін айқындауға мүмкіндік береді: егер Д.В. Бахтеев тергеушінің интерфейстердің легитимді дизайны алдындағы психологиялық осалдығына назар аударса, онда А.И. Зазулин машиналық кодты тікелей сезімдік танудың гносеологиялық мүмкін еместігіне нұсқайды. Осы мәселені шеше отырып, авторлық ұстанымды тұжырымдаған жөн: виртуалды орта жағдайында құқық қолданушының ішкі сенімі бұрмаланған визуалды көшірмені үстірт-интуитивті қабылдау негізінде қалыптасады, ол заңдық маңызы бар цифрлық түпнұсқамен қате теңестіріледі, бұл құқықтық бағалаудың объективтілігін фатальды түрде бұзады.

Ерекше интуитивті қабылдау қылмыстық-процестік доктринаның объективті олқылықтарының арқасында сөзсіз тамыр жаяды. ҚР ҚПК-тің 120-бабы компьютерлік ақпаратты қамтитын материалдарды формальды түрде құжаттар деп танығанына қарамастан, құқық қорғау жүйесі қатаң әдіснамалық тапшылық жағдайында жұмыс істейді. Осы тосқауылды бағалай отырып, Е.Р. Россинская цифрлық деректерді кешенді талдаудың ғылыми сынақтан өткен, біріздендірілген әдістемелерінің өткір жоқтығын тұжырымдайды, мұның нәтижесінде оларды бағалау жүйесіз, тек қызметкерлердің шашыраңқы жеке тәжірибесі негізінде ғана жүргізіледі [134, 195-196 б.]. Сонымен бірге Е.С. Шевченко желілік анонимизациялау технологияларын жаппай қолдануға байланысты қылмыскерді дәйекті дараландырудың мүмкін еместігін дәлелдей отырып, проблема фокусын әдістемелердің жоқтығынан криминалистикалық реконструкцияның еңсерілмейтін шектеріне ауыстырады [59, 135-136 б.]. Осы ғылыми көзқарастарды талдау бағалау дағдарысының табиғатын түсінудегі алшақтықты көрсетеді: Е.Р. Россинская проблеманы стандарттарды әзірлеу арқылы жойылуға жататын, еңсерілетін ұйымдастырушылық-ғылыми олқылық ретінде қарастырса, ал Е.С. Шевченко физикалық атрибуция мүмкіндігінің өзін толығымен жоққа шығаратын іргелі технологиялық тығырықты диагностикалайды. Біздің ойымызша, бұл проблеманы цифрлық сәйкестікті цифрлық жазбалардың жиынтығы ретінде айқындайтын ҚР ЦК-нің 40-бабының призмасы арқылы қарастырған жөн.

Институционалдық проблема жай ғана әдістемелердің жоқтығында емес, тұжырымдамалық қақтығыста жатыр: қылмыстық процесс жеке тұлғаны дербестендіруді және оның субъективті кінәсін анықтауды талап етеді, ал цифрлық орта тергеушіге криптографиялық алгоритмдердің артында сенімді жасырылған виртуалды профильді (цифрлық сәйкестікті) ғана реконструкциялауға мүмкіндік береді. Демек, дәлелдемелерді бағалау жойылмайтын құқықтық белгісіздік жағдайында жүзеге асырылады.

Толық когнитивтік және әдіснамалық вакуум жағдайында дәлелдеу процесін объективтендіру заңды түрде сот сараптамасы институтымен қамтамасыз етілуге тиіс. ҚР ҚПК-тің 270-бабының нормативтік конструкциясы арнаулы ғылыми білімді міндетті түрде тартуды ұйғарады, ал ҚР ҚПК-тің 116-бабы сарапшының қорытындысына дербес дәлелдеме мәртебесін береді. Алайда кибержымқыруларды тергеп-тексеру кезінде бұл құралдың процестік рөлі сыни түрде құнсызданған болып шығады. Сарапшы мүмкіндіктерінің шектерін зерттей отырып, А.И. Семикаленова компьютерлік-техникалық сараптама транзакция

тетігін немесе кодты зиянды түрлендіру фактісін анықтауға қабілетті, бірақ құрылғының артында отырған нақты адамды үзілді-кесілді сәйкестендірудің гносеологиялық мүмкіндігінен айырылғанына негізді түрде назар аударады [136, 71-72 б.]. Талдауға өзге ұстанымдардан А.А. Толыбаева және тең авторлар келеді, олар бастапқы себеп ретінде тергеудің субъективті формализмі әрекет ететінін дәлелдейді: сарапшылардың күрделі технологиялық түйіндері оқшауланған техникалық қосымша болып қала отырып, құқық қолданушымен істің өзге материалдарымен синтезделмейді [98, 133-134 б.]. Ұсынылған тәсілдердің қайшылығы айқын: егер А.И. Семикаленова проблеманың түбірін сарапшының өзінің құзыретінің объективті шектерінен көрсе, онда авторлар ұжымы қылмыстық құдалау органының аналитикалық дәрменсіздігін диагностикалайды. Авторлық ұстанымды қалыптастыра отырып, екі фактор да дәлелдеу процесінің деградациялануының бірыңғай тетігін құрайтынын мойындау қажет. Жоғары технологиялық білім физикалық сәйкестендіру тосқауылын еңсеруге қабілетсіз, ал тергеуші жеткіліксіз цифрлық құзыреттілігіне байланысты сарапшының тар техникалық түйіндерін пиғылдың заңдық конструкциясына экстраполяциялай алмайды. Нәтижесінде сараптама іс бойынша ақиқатты кепілді түрде анықтауға қабілетті процестік құрал функциясынан айырылады.

Цифрлық дәлелдемелермен жұмыс істеудің қорытынды сатысы терең жүйелі паралич жағдайында тұрғанын тұжырымдау қажет. ҚР ҚПК-тің 125-бабының дәлелдемелерді ішкі сенім бойынша бағалау туралы классикалық талабы виртуалды артефактілердің алгоритмдік табиғатымен функционалдық үйлесімсіздікті көрсетеді. Визуалды қабылданатын электрондық құжаттардың түсініктілік елесі стандартталған аналитикалық әдістемелердің өткір тапшылығымен және сарапшылық білімді формальды түрде интеграциялаумен еселене отырып, құқықтық бағалаудың жүйелі түрде бұзылуына әкеледі. Желілік қол сұғушылықтардың материалдық емес табиғаты мен оларды бағалаудың дәстүрлі материалистік әдіснамасы арасындағы дәлелденген алшақтық дәлелдеу процесін ғылыми қатаңдық пен негізділіктен айырады. Когнитивтік, рәсімдік және технологиялық тосқауылдардың анықталған жиынтығы қоғамды цифрландыру жағдайында қылмыстық-процестік дәлелдеудің тұжырымдамалық жаңа, бейімделген моделін әзірлеу қажеттілігін объективті түрде туындатады.

Жүргізілген құқықтық талдау нәтижелерінің синтезі бұрын анықталған шашыраңқы проблемаларды онлайн алаяқтық туралы істер бойынша дәлелдеу процесінің терең жүйелі деформациясын көрсететін бірыңғай теориялық модельге тұжырымдамалауға мүмкіндік береді. Анықталған институционалдық дағдарыстың іргетасы ретінде қылмыстық-процестік заңдағы цифрлық дәлелдемелер мәртебесінің бастапқы тұжырымдамалық белгісіздігі әрекет етеді. Заң шығарушы виртуалды ақпаратты фрагментті түрде, тек дәстүрлі жазбаша құжаттар (ҚР ҚПК-тің 120-бабы) немесе классикалық физикалық заттай дәлелдемелер (ҚР ҚПК-тің 118-бабы) призмасы арқылы ғана қарастыруды жалғастыруда. Бұл ретте бейінді заңнамада – ҚР ЦК-нің 16-бабында тікелей бекітілген деректердің дербес денесіз, алгоритмдік табиғаты толығымен елеусіз қалады.

Анықталған доктриналық коллизия құқық қолдану іркілістерінің қайтымсыз

тізбекті реакциясын іске қосады, онда терминологиялық белгісіздік цифрлық іздерді жинау және тіркеп-белгілеу кезеңдеріндегі фатальды процестік қателерді тікелей детерминациялайды және еселеп күшейтеді. Хаттамалауға (ҚР ҚПК-тің 199-бабы) және алып қоюға (ҚР ҚПК-тің 122-бабы) қойылатын консервативті талаптармен императивті түрде бұғауланған сотқа дейінгі тергеп-тексеру органы бөлінген ақпараттық массивтерге архаикалық материалдық алгоритмдерді механикалық түрде қолдануға мәжбүр. Жағдай объективті технологиялық ортаның дәлелдемелік ақпараттың қайтарымсыз жоғалуын жеделдетуімен сыни түрде ушыға түседі: электрондық деректердің ұшпалығы, өтпелі шифрлауды қолдану және логтарды автоматты түрде жою тергеу әрекеттерін санкциялаудың ұзаққа созылатын бюрократиялық рәсімдерімен шешілмейтін физикалық қақтығысқа түседі. Осы тізбектің қорытынды деструктивті элементі ретінде терең институционалдық тосқауылдар әрекет етеді. Цифрлық артефактілерді ішкі сенім бойынша (ҚР ҚПК-тің 125-бабы) объективті бағалау үшін қажетті арнайы білімнің өткір тапшылығы және ғылыми негізделген әдістемелердің болмауы тиімсіз практиканы түпкілікті бекітеді. Нәтижесінде тергеудің виртуалды іздерді дәстүрлі әдістермен тіркеп-белгілеуге жасаған кез келген әрекеттері формальды бұзушылықтардың көзіне айналады, бұл ҚР ҚПК-тің 112-бабының тікелей нұсқауына орай нақты деректерді дәлелдемелер ретінде жол берілмейтін деп тануға сөзсіз әкеп соғады.

Ұсынылған тәсілдің ғылыми жаңалығы сотқа дейінгі іс жүргізудің процестік, криминалистикалық және технологиялық аспектілерін органикалық интеграциялаудың нәтижесі болып табылатын цифрлық дәлелдемелер проблемаларының кешенді моделін құрудан тұрады. Маңызды теориялық нәтиже ретінде тар «мүмкіндіктер терезесі» авторлық тұжырымдамасын тұжырымдай отырып, цифрлық іздердің бейімделген трасологиялық моделін енгізу әрекет етеді. Бұл тұжырымдаманың мәні телекоммуникациялық желіде виртуалды артефакттың физикалық өмір сүру кезеңі құқық қолданушыға оны легитимді процессуализациялау үшін қажетті уақыттан объективті түрде қысқа екенін дәлелдейді. Ғылыми жаңалықтың екінші негізгі элементі ретінде «цифрлық нигилизм» феноменін қазіргі заманғы құқық қолдану практикасының мәндік сипаттамасы ретінде тұжырымдамалау әрекет етеді. Бұл санат тергеу органдарының виртуалды дәлелдемелердің ақпараттық ерекшелігін жүйелі түрде елемеуін және олардың цифрлық кодты примитивті қағаз хаттамалар түрінде жасанды түрде материалдандыруға деген иррационалды ұмтылысын ғылыми тұрғыдан түсіндіреді.

Ұсынылған жүйелі интеграция ағымдағы бөлімнің қорытынды бағдарламалық түйінін тұжырымдауға мүмкіндік береді: цифрлық дәлелдемелермен жұмыс істеудің отандық жүйесі терең институционалдық және гносеологиялық дағдарыс жағдайында тұр. Бұл паралич толығымен консервативті нормативтік-құқықтық база, статикалық құқық қолдану практикасы және қазіргі заманғы киберқылмыстылықтың жоғары динамикалық технологиялық шынайылығы арасындағы сыни сәйкессіздікпен шартталған. Қылмыстық процестің виртуалды іздерді жедел тіркеп-белгілеуге дәлелденген қабілетсіздігі апатты түрде масштабталады және онлайн алаяқтықтың

трансшекаралық табиғатымен күшейе түседі. Жымқырылған активтер мен электрондық деректер шетелдік юрисдикцияларда орналасқан серверлер бойынша лездік бөлінетін жағдайларда ұлттық процестік инструментарий өзінің тиімділігін түпкілікті жоғалтады. Аталған нормативтік-технологиялық тығырық қылмыстық сот ісін жүргізу саласындағы халықаралық құқықтық ынтымақтастықтың процестік тетіктерін дербес талдауға логикалық түрде өтудің өткір ғылыми қажеттілігін объективті түрде қалыптастырады.

2.3 Онлайн алаяқтық қылмыстарының трансшекаралық сипаты және оның сотқа дейінгі тергеп-тексеру тетігіне әсері

Зерттеудің алдыңғы кезеңінде анықталған цифрлық дәлелдемелерді жинаудың тұжырымдамалық және технологиялық дағдарысы онлайн алаяқтықтың объективті трансшекаралық табиғатымен бетпе-бет келген кезде іргелі түрде ушыға түседі және еңсерілмейтін сипатқа ие болады. Қылмыстық заң аумақтылықтың базалық қағидасын бекітеді: ҚР ҚК-нің 7-бабына сәйкес, мемлекет аумағында жасалған құқық бұзушылық деп оның шегінде басталған, жалғастырылған немесе аяқталған іс-әрекет танылады. Алайда желілік жымқырулардың эмпирикалық құрылымы қылмыс элементтерінің географиялық шашыраңқылығын имманентті түрде алдын ала айқындайды. Бұл феноменді бағалай отырып, Д.В. Завьялова киберкеңістіктің экстерриториялық табиғаты қылмыстық қудалау шектерін айқындау кезінде бұрын-соңды болмаған қиындықтар туындата отырып, классикалық мемлекеттік шекараларды жоятынын атап өтеді [90, 173-174 б.]. Осы тезисті дамыта отырып, К.О. Карабеков қашықтан жымқырулардың геокеңістіктік моделі трансұлттық ұйымдасқан топтардың «Call-орталықтарын» елден тыс жерде перманентті орналастыруға негізделетінін, бұл орындаушыларға физикалық қолжетімсіздікті қамтамасыз ететінін тұжырымдайды [17, 49 б.]. Жасыру тетігін талдауды тереңдете отырып, И.М. Нурбеков Интернеттің жаһандық құрылымына байланысты қылмыстың цифрлық іздері шетелдік операторлар мен провайдерлердің телекоммуникациялық жабдықтарында объективті түрде қалып қоятынын, бұл тергеу процесін ұлттық юрисдикция шеңберінен еріксіз шығаратынын атап көрсетеді [136, 225-226 б.]. Бұл архитектураның қорытынды элементі ретінде айналымы оқшауланған режимдермен, атап айтқанда «Қазақстан Республикасындағы цифрлық активтер туралы» ҚРЗ-ның 11-бабымен реттелетін шетелдік криптовалюталық платформалар арқылы активтерді шығару әрекет етеді. Аталған ұстанымдар мен нормативтік нұсқамалардың синтезі қылмыстық-құқықтық тұрғыдан бірыңғай қылмыс іс жүзінде трансшекаралық компоненттердің оқшауланған жиынтығына ыдырайтынын көрсетеді.

«Криминалдық қызметтің аталған архитектуралық орталықсыздандырылуы процестік өкілеттіктердің ұлттық шектерімен өткір қақтығысқа түседі. Заң шығарушының юрисдикцияның шектеулілігін ҚР ҚК-нің 8-бабында (шетелдіктердің Қазақстан Республикасының мүдделеріне қарсы қылмыстары үшін жауаптылығы) бекітілген экстерриториялық қағидатты қолданумен өтеуге

тырысуы іс жүзінде орындалмаушылықтың институционалдық тосқауылымен бетпе-бет келеді. Осы тосқауылдың табиғатын зерттей отырып, Л.В. Терентьева бастапқыдан шексіз киберкеңістікте егеменді юрисдикцияны орнатуға бейімделмеген дәстүрлі аумақтылық қағидатының өзінің тұжырымдамалық шектеулілігі мен ескіруіне әділетті түрде нұсқайды [137, 144 б.]. Онымен Я.М. Матвеева мен С.М. Оленниковтардың зерттеулері пікірталасқа түседі, олар басты кедергі аумақтылық қағидатының тұжырымдамалық әлсіздігінде емес, трансшекаралық элементтердің көптігі процестік әрекеттерді уақтылы жүргізуді бұғаттай отырып, егемендіктердің қақтығысын тудыратын қылмыстық-құқықтық юрисдикциялардың агрессивті бәсекелестігінің қалыптасуында жатқанын негіздейді [138, 33 б.].

Келтірілген ғылыми тәсілдерді салыстыру юрисдикциялық дағдарысты интерпретациялаудағы айқын алшақтықты диагностикалауға мүмкіндік береді: егер Л.В. Терентьева проблеманы құқықтық вакуумнің (құқықтың цифрлық ортаға қолданылмауының) құрылуынан көрсе, онда Я.М. Матвеева мен С.М. Оленников құқықтық аса қанығушылық (әртүрлі ұлттық заңдардың артық қақтығысуы) жағдайын диагностикалайды. Анықталған теориялық қайшылықты шеше отырып, негізделген авторлық ұстанымды тұжырымдау қажет. Іс жүзінде екі фактор да ұлттық тергеудің абсолютті процестік оқшаулану жағдайын қалыптастыра отырып, кумулятивті түрде әрекет етеді. Қазақстан Республикасының қылмыстық қудалау органы де-факто тек транзакцияны инициациялау нүктесін және жәбірленушінің тұрған жерін ғана бақылайды. Сонымен бірге негізгі дәлелдемелік массивтер, цифрлық басқару орталықтары және шығарылған капитал шетелде қалады. Бұл институционалдық алшақтық мемлекеттік деңгейде киберқылмыстардың ашылуының төмен болуының іргелі себебі ретінде тікелей танылады, бұл 2024-2028 жылдарға арналған Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз ету тұжырымдамасында ресми түрде бекітілген.

Анықталған нормативтік және технологиялық коллизиялар авторлық доктриналық тұжырымдаманы ұсыну және негіздеу үшін база қалыптастырады: қазіргі жағдайларда онлайн алаяқтықты жай ғана трансұлттық іс-әрекет ретінде емес, объективті жағының айқын трансшекаралық (экстерриториялық) сипаты және із түзілудің мультиюрисдикциялық тетігі бар қылмыс ретінде саралау қажет. Ұсынылған конструкция шеңберінде объективті жағы (когнитивтік әсер ету, деректерді енгізу), жасау құралдары (шетелдік маршрутизаторлар) және қоғамға қауіпті зардаптары (электрондық активтерге құқықтардың ауысуы) әртүрлі мемлекеттердің аумақтары арасында перманентті және ажырамас түрде бөлінген. Бұл ретте соттылықты тергеп-тексеру аяқталған жер бойынша айқындайтын ҚР ҚПК-тің 314-бабының процестік қағидасы сот ісін жүргізуді тек формальды түрде оқшаулауға қабілетті, бірақ тергеу кезеңінде дәлелдемелік базаның іс жүзіндегі бөлшектенуін объективті түрде жоймайды.

Цифрлық жымқырулардың геокеңістіктік құрылымын зерттеу нәтижелерін қорытындылай келе, юрисдикциялық фрагментация тергеп-тексерудің ерекше күрделілігін туындататын орталық детерминациялаушы фактор ретінде әрекет ететінін тұжырымдау қажет. Бірыңғай қылмыстық тетіктің мемлекеттік

шекаралармен бөлінуі сотқа дейінгі тергеп-тексеру органының біржақты жария және жасырын процестік әрекеттерді жүргізу мүмкіндігін физикалық және заңдық тұрғыдан бұғаттайды. Егеменді юрисдикцияның дәлелденген шектеулілігі сипатталған кеңістіктік және құқықтық тосқауылдарды еңсерудің жалғыз легитимді институты ретінде әрекет ететін халықаралық құқықтық көмек тетіктерінің рәсімдік асимметриясына сыни талдау жасау қажеттілігін туындатады.

Ұлттық сотқа дейінгі іс жүргізуді салдандыратын юрисдикциялық фрагментацияның логикалық салдары ретінде тергеу органдарының халықаралық құқықтық көмек тетіктеріне жүгінуінің объективті қажеттілігі әрекет етеді. Бұл институттың базалық контурлары трансшекаралық сұрау салулардың негізгі векторларын: шетелдік провайдерлерден деректер алуды, жаһандық платформалардың серверлерінен ақпаратты талап етіп алдыруды, криптовалюталық активтердің қозғалысы туралы мәліметтерді ашуды және кінәлі адамдарды экстрадициялауды регламенттейтін ҚР ҚПК-тің 557-бабында бекітілген. Осы нормаларды іске асырудың құқықтық режимдерін жүйелей отырып, К.А. Толпекин өңірлік өзара іс-қимылдың (ТМД және ЕАЭО шеңберінде) салыстырмалы түрде оңайлатылған тетіктерін және алыс шетелдермен классикалық көпсатылы рәсімдерді қамтитын сараланған тәсілді бөліп көрсетеді [139, 91 б.]. Дүниежүзілік қоғамдастықтың процестерді жеделдетуге деген айқын ұмтылысы Компьютерлік қылмыстар туралы конвенцияның (2001 ж.) 35-бабында және БҰҰ-ның Киберқылмыстылыққа қарсы перспективалық конвенциясының (2025 ж.) 41-бабында көзделгендей, электрондық деректерді дереу сақтау үшін тәулік бойы жұмыс істейтін байланыс желілерін енгізу әрекеттерінен көрініс табады. Алайда Д.В. Завьялова халықаралық-саяси конфронтация (саяси келіспеушіліктер) дәлелдемелік ақпаратпен легитимді алмасуды толығымен жоққа шығаратын жағдайларда абсолютті институционалдық тығырықтың болуын әділетті түрде диагностикалайды [90, 163 б.]. Бұл тұжырымның эмпирикалық растамасы ретінде трансұлттық коммуникациялық платформалардың өкілдерімен өзара іс-қимыл жасаудың жүйелі мүмкін еместігін ресми түрде тіркейтін 2024-2028 жылдарға арналған Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз ету тұжырымдамасының ережелері қызмет етеді.

Онлайн-алаяқтықтың трансшекаралық (экстерриториялық) сипаты құқық қолдану практикасының күнделікті шынайылығына айналғанын жүргізілген сауалнама нәтижелері де дәлелдейді (Қосымша А). Практик-қызметкерлердің 50%-ы (15%-ы әрбір қылмыстық іс бойынша, 35%-ы істердің жартысында) киберқылмыстарды тергеп-тексеру кезінде шетелдік юрисдикцияларға халықаралық тергеу тапсырмаларын (құқықтық көмек көрсету туралы сұрау салуларды) жолдау қажеттілігіне үнемі тап болатынын көрсетті. Бұл деректер қылмыстық әрекеттің инфрақұрылымы (серверлер, крипто-әмияндар, IP-мекенжайлар) ұлттық юрисдикциядан тыс орналасатындықтан, ішкі тергеу әдістерінің ресурстық әлеуетінің толық сарқылғанын және халықаралық өзара іс-қимылды жаңғыртудың императивті қажеттілігін көрсетеді.

Мемлекетаралық қатынастардың тиімділігін жоққа шығаратын орталық

кедергі ретінде сұрау салуларды орындаудың нормативтік детерминацияланған уақыттық сипаттамалары әрекет етеді. Осы рәсімдердің ұзақтығын зерттей отырып, А.Г. Волеводз эмпирикалық көрсеткіштерді келтіреді: ресми өтінішхаттарды орындаудың орташа мерзімі ТМД елдері үшін екі жарым айға дейінгі, Еуропа мемлекеттері үшін алты айдан он екі айға дейінгі, және АҚШ құқық қорғау органдары үшін жиырма айдан астам уақытты құрайды [76, 206 б.]. Осы мерзімдердің кибержымқыру фактілерін дәлелдеуге әсерін бағалай отырып, Д.В. Завьялова аталған уақыттық шеңберлер виртуалды іздердің физикалық өмір сүру кезеңінен теңдессіз асатыны, мұның нәтижесінде іздестіріліп отырған логтар мен IP-мекенжайлар жауапты алғанға дейін көп уақыт бұрын шетелдік провайдерлермен автоматтандырылған түрде қайта жазылатыны туралы негізделген қорытындыға келеді [90, 156 б.]. Өз кезегінде, А.Г. Волеводз құқықтық көмек тетігі бастапқыдан тек статикалық материалдық іздері бар классикалық қол сұғушылықтарды тергеп-тексеру үшін ғана құрылымдалғанын, соның салдарынан ол өте жылдам ақпараттық алмасудың ерекшелігіне тұжырымдамалық түрде бейімделмегенін атап көрсете отырып, проблематиканы таза хронологиялық жазықтықтан доктриналық жазықтыққа ауыстырады [76, 206-207 б.]. Д.В. Завьялова мен А.Г. Волеводздың ұстанымдарын салыстыру ғылыми фокустардың айырмашылығын айқындауға мүмкіндік береді: егер біріншісі дәлелдемелердің деградациялануының бастапқы себебін тапсырмаларды орындау мерзімдерінің эмпирикалық созылып кетуінен көрсе, онда екіншісі виртуалды ортамен жұмыс істеу үшін классикалық құқықтық көмектің процестік дизайнының өзінің іргелі жарамсыздығын дәлелдейді.

Анықталған ғылыми пікірталасты шеше отырып, халықаралық құқықтық көмектің «процестік асимметриясының» итеративті авторлық тұжырымдамасын тұжырымдау қажет. Бұл құбылыстың мәні дәстүрлі құқықтық мемлекетаралық өзара іс-қимыл жылдамдығының цифрлық қылмыстарды жасау, алгоритмдік бүркемелеу және технологиялық жасыру жылдамдығынан сыни түрде артта қалуында жатыр. Аталған асимметрия шешілмейтін нормативтік қайшылықтар кешенін тудырады.

Біріншіден, ҚР ҚПК-тің 192-бабымен (бір айдан екі айға дейін) шектелген сотқа дейінгі тергеп-тексерудің қысқа базалық мерзімдері мен халықаралық рәсімдердің шектен тыс ұзақтығы арасында өткір юрисдикциялық қақтығыс туындайды. Бұл құдалау органын белсенді дәлелдеу процесін іс жүзінде тоқтата тұра отырып, ҚР ҚПК-тің 45-бабының негіздері бойынша мерзімдерді формальды түрде үзуге мәжбүрлейді.

Екіншіден, цифрлық деректердің гиперқұбылмалылығы мен сертификатталған аудармалармен және елтаңбалық мөрлермен жабдықталған сұрау салулардың қатаң жазбаша нысаны туралы ҚР ҚПК-тің 560-бабының императивті талаптары арасында диссонанс байқалады.

Үшіншіден, сұрау салуларды тек қана орталықтандырылған түрде Бас прокуратура арқылы жіберуді қатаң ұйғаратын ҚР ҚПК-тің 559-бабының нормалары мен тергеушілердің провайдерлермен тікелей байланыста болуға деген тактикалық қажеттілігі арасындағы қақтығыс айқын.

Сипатталған қайшылықтардың табиғатын талдай отырып, Д.В. Завьялова

проблеманың түбірін сұрау салуларды жасау және қанағаттандыру процесін шектен тыс құжаттық бюрократияландырудан көреді [90, 112 б.]. Онымен өзіндік полемикаға И.М. Нурбеков түседі, ол басты институционалдық ақау ретінде таза бюрократияны емес, төменгі тергеу бөлімшелерін (тікелей орындаушыларды) деректермен жедел тікелей алмасу мүмкіндігінен айыратын өзара іс-қимылдың баса көрсетілген орталықтандырылған сипаты («Орталық органдар» монополиясы) әрекет ететінін сенімді түрде дәлелдейді [136, 148-149 б.]. Осы ұстанымдарды салыстыра отырып, айқын алшақтықты айқындау қажет: бірінші автор рәсімдік формализмге (қағаз нысанына) фокусталады, ал екіншісі ведомстволық иерархияны (маршрутизация арналарын) сынайды. Екі фактордың да кумулятивті түрде әрекет ететінін атап өткен жөн. Құжаттарды қатаң формализациялау олардың орталық аппараттар мен дипломатиялық ведомстволардың инстанциялары арқылы өтуінің көпсатылылығымен еселене отырып, халықаралық құқықтық көмекті қылмыстарды ашудың тиімді құралынан ішінде онлайн алаяқтықтың дәлелдемелік базасы абсолютті заңды жолмен жойылатын заңды хронологиялық тосқауылға айналдырады.

Жүргізілген нормативтік және доктриналық талдауды қорытындылай келе, халықаралық құқықтық көмек институты өзінің қолданыстағы консервативті түрінде өте шектеулі, көбінесе номиналды тиімділікке ие екенін тұжырымдау қажет. Классикалық конвенциялық тетік трансұлттық бұлтты инфрақұрылымда бөлінген цифрлық дәлелдемелерді тиісінше тіркеп-белгілеуді және олардың сақталуын қамтамасыз етуге объективті түрде қабілетсіз. Мемлекетаралық рәсімдердің дәлелденген жүйелі дәрменсіздігі криминалдық орта мақсатты түрде тұрғызатын қосымша тосқауылдарды талдау қажеттілігін туындатады. Құқықтық өзара іс-қимыл әлеуетінің сарқылуы процестік инерттілікке қабаттаса отырып, абсолютті цифрлық ұстатпаушылық эффектісін тудыратын қылмыс субъектілері белсенді түрде қолданатын желілік анонимизациялау технологияларын тереңдетіп зерттеу қажеттілігін алдын ала айқындайды.

Трансшекаралық өзара іс-қимыл тетіктерінің процестік асимметриясы сотқа дейінгі іс жүргізуге жойқын әсер ететін мамандандырылған жасыру технологияларын қылмыс субъектілерінің белсенді қолдануымен сыни түрде ушыға түседі. Қылмыстық-процестік заңнама ақпараттық вакуумді еңсеруге ұмтыла отырып, арнайы инструментарийді көздейді: ҚР ҚПК-тің 243 және 244-баптары байланыс желілерін жасырын бақылауды және абоненттер қосылулары туралы ақпаратты алуды регламенттейді. Бұл нормалардың заңдық мақсаты провайдерлермен тікелей өзара іс-қимыл жасау арқылы деректерді беру маршруттарын қадағалаудан тұрады. Алайда осы өкілеттіктерді іске асыру қуатты аппараттық қарсы іс-қимылмен бетпе-бет келеді. С.М. Голятина киберқылмыстылықтың базалық арсеналы ретінде виртуалды жеке желілер (VPN), прокси-серверлер және шетелдік маршрутизаторлар әрекет ететінін тұжырымдайды [111, 82 б.]. Осы аспектіні дамыта отырып, М.Х. Марас (М.-Н. Maras) өзінің зерттеуінде шифрлау мен трафикті анонимдеу технологиялары цифрлық пакеттердің бүкіл жүру маршрутын сенімді түрде бүркемелейтінін, бұл тергеушілердің шабуыл көзін анықтау мүмкіндігін іс жүзінде жоққа шығаратынын негіздейді [140, 44 б.]. Өз кезегінде, П.В. Рудых бұл

технологиялық кешен геолокацияны (қылмыс орнын) түбегейлі бұрмалайтынын және құрылғының нақты физикалық тұлғаға тиесілілігін анықтауды техникалық тұрғыдан мүмкін емес ететінін нақтылайды [60, 131 б.]. Нормативтік нұсқамалар мен технологиялық шынайылықты салыстыру заңның жұмыс істеуге қабілетсіздігін көрсетеді: тергеу ҚР ҚПК нормаларын қолдана отырып, қаскөйдің нақты IP-мекенжайының орнына тек аралық транзиттік тораптардың деректемелерін ғана легитимді түрде тіркеп-белгілейді.

Виртуалды іздердің анықталған техникалық көрінбеуі ұлттық құқықтық режимдердің қақтығысымен детерминацияланған олардың заңдық қолжетімсіздігіне заңды түрде трансформацияланады. Цифрлық деректерді қорғау және криптографиялық қорғау құралдарын қолдану жөніндегі базалық талаптар ҚР ЦК-нің 98-бабында тікелей бекітілген. Дербес деректерді қорғаудың осыған ұқсас, ал көбінесе неғұрлым қатаң императивтері (zero-log архитектуралық саясатына дейін) шетелдік юрисдикцияларда әрекет етеді. Осы фактордың әсерін бағалай отырып, К.О. Карабеков трафикті көпдеңгейлі анонимизациялау лог-файлдарды заңды түрде талап етіп алдыруды толығымен бұғаттай отырып, белсенділікті тікелей құқықтық ынтымақтастықты қолдамайтын юрисдикцияларға қасақана ауыстыратынын дәлелдейді [17, 102 б.]. Ақпаратқа қол жеткізу режимдеріндегі айырмашылықтармен еңсерілмейтін институционалдық тосқауыл қалыптасатынына назар аударатын М.С. Бисалиев түбегейлі өзге ұстанымдардан көрінеді: байланыс торабын деанонимизациялаудың теориялық мүмкіндігі болғанның өзінде мәліметтерді заңдық тұрғыдан алу жеке өмірге қолсұғылмаушылық туралы ұлттық нормалармен бұғатталады [16, 26 б.]. Осы ұстанымдарды талдау тәсілдердің терең алшақтығын көрсетеді: егер К.О. Карабеков проблеманың түбірін мемлекеттердің ынтымақтасуға деген геосаяси құлықсыздығынан көрсе, онда М.С. Бисалиев приваттылықты қорғаудың заңды тетіктері сот төрелігі үшін бөгетке айналатын іргелі құқықтық парадоксты диагностикалайды. Біздің ойымызша, онлайн жымқыруларды тергеп-тексеру жағдайында екі фактор да бірыңғай деструктивті симбиозды құрайды. Ақпаратты қорғаудың императивті ұлттық және халықаралық стандарттары қылмыстық қудалау органының күш-жігерін толығымен жоққа шығара отырып және із түзілудің процестік тізбегін бірінші шифрланған серверде-ақ үзе отырып, криминалдық трафик үшін абсолютті легитимді қалқан ретінде әрекет етеді.

Сипатталған тығырықты еңсеруге тырыса отырып, құқық қолданушы тактикалық қарсы шараларға жүгінеді, алайда доктринада оларды бағалау өткір ғылыми пікірталастарды тудырады. Тергеу инструментарийі амалсыздан ҚР ҚПК-тің 122-бабының тәртібімен қаржы ұйымдарына ресми сұрау салуларға және ашық ақпарат көздерін (OSINT) талдауға сүйенеді. Осы тәсілді талдай отырып, Е.С. Шевченко транзакцияларға ретроспективті талдау және абоненттік құрылғыларды жанама техникалық сәйкестендіру тергеушіге қашықтан жымқыру көрінісін сәтті қалпына келтіруге мүмкіндік беретінін тұжырымдай отырып, мұндай шаралардың жоғары тиімділігін негіздейді [59, 89-90 б.]. Ал А.Л. Осипенко ашық көздерден деректерді фрагментті түрде жинау және жанама сәйкестендіру әрекеттері терең шифрлаудың жүйелі процестік әсерін объективті

түрде өтей алмайтынын және тұрақты дәлелдемелік нәтижені қамтамасыз етпейтінін дәлелдей отырып, бұл ұстанымды үзілді-кесілді сынайды [141, 86 б.]. Аталған көзқарастарды салыстыру Е.С. Шевченконың тактикалық оптимизмі мен А.Л. Осипенконың процестік скептицизмі арасындағы тікелей қайшылықты көрсетеді. Соңғысының объективті дұрыстығын мойындау қажет. Айналма маневрлерді қолдану тетігі айқын шектеулілікке ие: профильдерді зерттеу және қаржылық талдау тергеуді сөзсіз тек номиналды жалған тұлғаларға (дропперлерге) немесе анонимді шоттарға ғана әкеледі [142, 13 б.], ал жабдықты сәйкестендіру әрекеттері құрылғының бірегей параметрлерін бағдарламалық алмастырумен толығымен жоққа шығарылады.

Үкімдерді талдау көрсеткендей, қылмыскерлер жәбірленушіні саналы ерік білдіру процесінен әдейі шеттетіп, аппараттық-бағдарламалық құралдарды тек өз іздерін жасыру үшін ғана емес, сонымен қатар банктердің қауіпсіздік алгоритмдерін тікелей айналып өту үшін де пайдаланады. Мәселен, №5516-22-00-1/28 қылмыстық ісінде (Павлодар облысы Ақсу қалалық сотының 2022 жылғы 17 шілдедегі үкімі) [143] сотталушы өзінің туыстары мен көршілері болып табылатын жәбірленушілермен жеке кездесіп, тұрмыстық сылтаулармен (ХҚКО-дан анықтама алу, мобильді қосымшаларға тіркелу) оларды смартфонға суретке түсірген. Осы сәтте банк жүйесі олардың бет-бейнесін биометриялық сәйкестендіруден өткізген, соның негізінде микрокарыздар рәсімделіп, алынған қаражат кейін букмекерлік кеңселердің шоттарына аударылған. Адамдар тобы азаматтарды суретке түсіру үшін заңды «Ашық» мемлекеттік қосымшасын тек сылтау ретінде пайдаланып, банктік «Face ID» биометриясынан заңсыз өту мақсатында АКТ-ны фондық режимде қолданған. Мұндай тәсіл №3528-23-00-1/20 қылмыстық ісінде көрініс тапқан (Қарағанды облысы Шахтинск қалалық сотының 2023 жылғы 11 маусымдағы үкімі) [48]. Бұл прецеденттер АКТ-ның байланыс құралы ретіндегі рөлінен шығып, қаржы ұйымдарының аппараттық-бағдарламалық қорғанысын еңсеретін дербес құралға айналғанын көрсетеді. Бұл проблема қаскөйлер цифрлық сәйкестікті алмастыру үшін терең синтез (deepfake) технологияларын қолданған кезде күрделене түседі. Мұндай жағдайда дәлелдеу процесі жаңа процессуалдық қиындықтарға тап болады, өйткені дәстүрлі дәлелдемелер цифрлық бейненің түпнұсқалығын әрдайым растай алмайды [144, 360 б.]. Сондықтан дәлелдемелерді жинау мен тексерудің қалыптасқан тактикалық тәсілдері мұндай қылмыстарды тиімді әшкерелеуге жеткіліксіз болып отыр.

Анықталған технологиялық және нормативтік тосқауылдардың синтезі «технологиялық ұстатпаушылық» тұжырымдамасын тұжырымдауға мүмкіндік береді. Технологиялық ұстатпаушылық желілік анонимизациялаудың көпдеңгейлі құралдарын деректерге қол жеткізу режимдеріндегі юрисдикциялық айырмашылықтармен ажырамас үйлесімде пайдалану қылмыскердің шын жеке басын легитимді түрде анықтауды мүмкін емес ететін ерекше криминалистикалық-процестік жағдайды білдіреді. Трафикті шифрлау алгоритмдері іс-әрекеттің нақты мән-жайларын жай ғана бүркемелеп қоймайды, олар дәлелдеудің классикалық инструментарийінің жүйелі параличін тудырады. Бұл жағдай шеңберінде консервативті процестік құралдар өзінің танымдық

құндылығын қайтарымсыз жоғалтады, ал цифрлық деректер атрибуцияланушылықтың негізгі қасиетінен айырылады.

Жүргізілген талдау нәтижелерін қорытындылай келе, жасырудың технологиялық тетіктері процестік тосқауылдардың сапалы жаңа түрін құрастыратынын тұжырымдау қажет. Криптографияның әсерінен электрондық ақпараттың объективті техникалық қолжетімсіздігі оның абсолютті процестік қолжетпестігіне түпкілікті трансформацияланады. Тергеу нақты адамның қашықтан жымқыруды жасаудағы кінәсін растайтын дәлелдемелердің тұйықталған, жол берілетін және анық жүйесін қалыптастырудың кез келген мүмкіндігінен айырылады. Дәстүрлі тергеу әдістерінің технологиялық ұстатпаушылық эффектісі алдында объективті түрде дәрменсіз екендігі туралы дәлелденген факт қылмыстық-процестік нысанның өзін жаңғырту жолдарын іргелі зерттеуге және цифрлық ортаның сын-қатерлеріне барабар инновациялық тергеп-тексеру тетіктерін әзірлеуге логикалық түрде өтудің ғылыми қажеттілігін детерминациялайды.

Трансшекаралық онлайн алаяқтықты тергеп-тексерудің тиімділігі тек сыртқы юрисдикциялық және технологиялық факторлармен ғана емес, сонымен қатар институционалдық-ұйымдастырушылық шектеулер кешенімен бетпе-бет келетін ұлттық құқық қорғау жүйесінің ішкі жай-күйімен де объективті түрде детерминацияланған. Функцияларды бөлудің базалық нормативтік негізі ретінде кәсіби маманданууды қамтамасыз ету мақсатында әртүрлі ведомстволар арасындағы заттық тергеулікті қатаң регламенттейтін ҚР ҚПК-тің 187-бабы әрекет етеді. Алайда цифрлық жымқырулардың ерекшелігі олардың кешенді сипатында жатыр, мұнда алаяқтық компьютерлік ақпаратқа заңсыз қол жеткізумен және қылмыстық кірістерді заңдастырумен ажырамас түрде ұштасады, бұл құзыреттер коллизиясын тудырады. Осы фактордың әсерін бағалай отырып, А.С. Камко құқық қолдану практикасында құқық қорғау органдарының киберқылмыстылықтың барлық аспектілеріне өз бетінше ықпал етуге қабілетсіздігінен туындайтын мемлекеттік органдар арасындағы сыни құрылымдық алшақтықты («бөлінген жауапкершілік» мәселесін) тұжырымдайды [36, 131 б.]. Проблемаға өзге көзқарас тұрғысынан С.М. Голятина келеді, ол басты кедергі ретінде жедел және процестік әрекеттерді міндетті ведомствоаралық келісу кезіндегі таза бюрократиялық кешіктірулер әрекет ететінін дәлелдейді [111, 80 б.]. Ұсынылған ұстанымдарды талдау дағдарыстың табиғатын түсінудегі алшақтықты көрсетеді: егер А.С. Камко бастапқы себепті тергеуліктің құрылымдық белгісіздігінен көрсе, онда С.М. Голятина рәсімдік формализмге назар аударады. Біздің ойымызша, екі фактор да бірыңғай деструктивті тетікті құрайды, онда маманданудың нормативтік талабы (ҚР ҚПК-тің 187-бабы) парадоксальды түрде тергеуді фрагменттейді. 2024-2028 жылдарға арналған Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз ету тұжырымдамасында ресми түрде танылған өзара іс-қимылдың интеграцияланған алгоритмдерінің болмауы қажетті келісу рәсімдерін ең ерте кезеңдерде құбылмалы дәлелдемелердің қайтарымсыз жоғалуына әкелетін хронологиялық тосқауылға трансформациялайды.

Анықталған ұйымдастырушылық коллизиялар процестік императивтермен

тікелей қайшылыққа түсетін терең кадрлық тапшылықтың болуымен заңды түрде ушыға түседі. ҚР ҚПК-тің 24-бабы тергеушіге істің мән-жайларын жан-жақты зерттеу үшін заңда көзделген барлық шараларды қолдану міндетін жүктейді. Осы міндетті жоғары технологиялық ортада іске асыру үшін заң бейінді мамандарды тартуға рұқсат береді (ҚР ҚПК-тің 80-бабы, «Жедел-іздестіру қызметі туралы» ҚРЗ-ның 8-бабы). Осы тетікті зерттей отырып, К.Н. Евдокимов тергеуге жәрдем көрсете алатын желілік әкімшілендіру және бағдарламалау саласындағы тәуелсіз сарапшылардың өткір тапшылығының болуын тұжырымдайды [20, 130-131 б.]. Сыртқы құзыреттерді тартуға бағдарланған тәсілмен Е.С. Шевченко қатаң полемикаға түседі, ол техникалық білімді терең интеграциялаусыз құқық қолданушының өзінің базалық заңгерлік білімі оған виртуалды децепцияның іздік көрінісін барабар бағалауға мүмкіндік бермейтінін бұлтартпай дәлелдейді [59, 131 б.]. Аталған авторлардың көзқарастарын салыстыру кадрлық аштықты еңсеру стратегиясындағы тұжырымдамалық қақтығысты айқындайды: К.Н. Евдокимов тартылатын IT-мамандар пулын экстенсивті түрде кеңейтуге ставка жасайды, ал Е.С. Шевченко тергеушінің өзінің білім беру бейінін қарқынды трансформациялауды талап етеді. Екінші тәсілдің объективті басымдығын мойындау қажет. Тек ҚР ҚПК-тің 80-бабына ғана сүйену қауіпті процестік тәуелділікті қалыптастырады: машиналық кодтың табиғатын түсінбейтін тергеуші дәлелдемелерді бағалау функциясын техникалық маманға механикалық түрде қайта сеніп тапсырады. Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасында анықталған ведомстволық оқу орындарының төмен ғылыми әлеуеті қолданыстағы даярлау жүйесі қазіргі заманғы киберқатерлердің зияткерлік күрделілігіне мүлдем сәйкес келмейтінін растайды.

Іргелі кадрлық осалдық процестік өкілеттіктерді іске асыруды тікелей бұғаттайтын апаттық техникалық шектеулермен ажырамас байланысты. ҚР ҚПК-тің 126-бабы дәлелдеу кезінде ғылыми-техникалық құралдарды пайдалануды императивті түрде ұйғарады. Осы норманың іс жүзінде іске асырылуын бағалай отырып, А.А. Рудых арнайы бөлімшелердің трафикті дешифрлауға және үлкен деректер аналитикасына арналған озық аппараттық-бағдарламалық кешендерге деген өткір қажеттілігін әділетті түрде атап көрсетеді [60, 13 б.]. Сонымен бірге А.В. Комов цифрлық артефактілерді қауіпсіз алып қоюды жүзеге асыруға физикалық тұрғыдан тіпті мүмкіндік бермейтін кәдімгі аумақтық органдардың ескірген материалдық-техникалық жарақталуы базалық бөгет ретінде әрекет ететінін эмпирикалық материалда дәлелдей отырып, проблеманы айтарлықтай қарапайым деңгейде диагностикалайды [145, 154 б.]. Осы ғылыми пікірлерді талдау технологиялық ақаудың локализациялануындағы алшақтықты көрсетеді: А.А. Рудых жоғары технологиялық аналитикалық софттың жоқтығына, ал А.В. Комов қарапайым аппараттық қамтамасыз етудің тапшылығына нұсқайды. Осы тәсілдерді нормативтік шынайылықтармен синтездей отырып, тапшылық жүйелі көпдеңгейлі сипатқа ие екенін тұжырымдау қажет. Құқық қорғау органдарының компьютерлік техникамен тек 44 %-ға ғана жарақталу фактісін ресми мойындау [3] ҚР ҚПК-тің 126-бабының ұйғарымдарын жұмыс істемейтін декларацияға айналдырады. Ұлттық жүйе

аппараттық деңгейде де, бағдарламалық деңгейде де ұшпа іздермен легитимді жұмыс істеуді қамтамасыз етуге объективті түрде қабілетсіз. Нәтижесінде технологиялық вакуум түзіледі: виртуалды іздерді алып қою және дешифрлау физикалық тұрғыдан орындалмайтын болады, бұл кепілді түрде олардың қайтарымсыз жоғалуына әкеледі және қылмыстық қудалау органын жоғары технологиялық криминалдық инфрақұрылым алдында көрінеу ұтылысты жағдайға қояды.

Нормативтік базаны, ведомстволық статистикалық бағалауларды және доктриналық ұстанымдарды кешенді талдау нәтижелерін қорытындылай келе, мынаны тұжырымдау қажет: құқық қорғау жүйесінің институционалдық дайын еместігі сотқа дейінгі іс жүргізудің нәтижелілігін сыни түрде төмендететін дербес, қуатты негативті детерминант ретінде әрекет етеді. Ішкі ведомствоаралық алшақтық гибридті заңдық-техникалық құзыреттердің тапшылығымен және ескірген инфрақұрылыммен еселене отырып, мемлекеттің онлайн алаяқтықтың жоғары технологиялық қатерлеріне симметриялы жауаптар қалыптастыру қабілетін физикалық түрде бұғаттайды. Қалыптасқан терең дағдарысты еңсеру объективті түрде ҚР ҚПК нормаларын нүктелік түзетуді емес, ауқымды институционалдық реформалауды: ақпараттық алмасудың өтпелі ведомствоаралық алгоритмдерін енгізуді, цифрлық тергеушілердің қағидаты жаңа генерациясын қалыптастыруды және тергеу аппаратын толық технологиялық жаңғыртуды талап етеді. Анықталған ішкі тосқауылдар кешені кибержымқыруларды тергеп-тексеру шектеулерінің жүйесін логикалық түрде аяқтайды және талданған қатерлерге қарсы іс-қимылдың қолданбалы криминалистикалық және қылмыстық-процестік модельдерін әзірлеуге ғылыми негізделген қажеттілікті туындатады.

Жүргізілген проблемалық-процестік талдау нәтижелерін жүйелеу онлайн алаяқтықты тергеп-тексеру тосқауылдарын кешенді деструктивті жүйе ретінде зерттеудің объективті қажеттілігін туындатады. Базалық бөгет ретінде ҚР ҚПК-тің 314-бабымен регламенттелген сотқа дейінгі тергеп-тексеруді жүргізу орнын айқындаудың классикалық қағидаларын виртуалды қол сұғушылықтарға қолданудың абсолютті мүмкін еместігі әрекет етеді. Осы дағдарыстың табиғатын бағалай отырып, Л.В. Терентьева бастапқы юрисдикциялық фрагментация құқық қорғау органдарының әртүрлі егеменді мемлекеттердегі серверлер бойынша бөлінген цифрлық дәлелдемелерге легитимді қол жеткізуін сыни түрде шектейтінін тұжырымдайды [137, 122-124 б.]. Өз кезегінде, А.Г. Волеводз аумақтық алшақтық рәсімдік асимметрия тетігін іске қосатынына: халықаралық құқықтық көмек көрсету туралы сұрау салуларды жіберудің қатаң формализацияланған тәртібі (ҚР ҚПК-тің 557 және 559-баптары) гиперқұбылмалы электрондық ақпараттың қайтарымсыз жоғалуына әкелетін орасан зор инерттілікпен ерекшеленетініне негізді түрде нұсқай отырып, проблеманы уақыттық шеңберлер призмасы арқылы диагностикалайды [76, 238 б.]. Бұл ұстанымдарды салыстыру тергеу параличінің бастапқы себебін түсінудегі тұжырымдамалық алшақтықты көрсетеді: егер Л.В. Терентьева оны шетелдік серверлердің абсолютті кеңістіктік-құқықтық қолжетпестігінен көрсе, онда А.Г. Волеводз басты проблема деректердің өмір сүру жылдамдығы мен

халықаралық көмек институтының процестік ебедейсіздігі арасындағы хронологиялық алшақтық екенін дәлелдейді. Құқықтық және хронологиялық тосқауылдар бәсекелеспейді, қайта сотқа дейінгі іс жүргізу тиімсіздігінің еңсерілмейтін бастапқы контурын қалыптастыра отырып, синхронды түрде әрекет етеді деп пайымдау негізді болып табылады. Юрисдикциялық шекараларды легитимді түрде еңсеру әрекеттері халықаралық ынтымақтастықтың мәнін толығымен жоққа шығара отырып, кепілді түрде рәсімдік баяулыққа соқтығысады.

Анықталған нормативтік-аумақтық диссонанс жасырын тергеу әрекеттерін іске асыру процесінде еселеп күшейе түседі. Абоненттер қосылулары туралы ақпаратқа санкцияланған қол жеткізу және байланыс желілерін бақылау (ҚР ҚПК-тің 243 және 244-баптары) іс жүзінде агрессивті технологиялық қарсы іс-қимылмен бетпе-бет келеді. Осы феноменді зерттей отырып, Н.С. Зиновьева көпдеңгейлі желілік анонимизациялау және криптографиялық қорғау шетелдік ақпараттық тораптарға процестік қол жеткізу болғанның өзінде субъектілерді криминалистикалық сәйкестендіруді түбегейлі қиындататынына нұсқайды [128, 152 б.]. Технологиялық детерминизммен өткір полемикаға А.А. Рудых түседі, ол мұндай сын-қатерлердің еңсерілместігі бейінді мамандардың кадрлық тапшылығы мен әлсіз аналитикалық базадан көрініс табатын ұлттық тергеу жүйелерінің терең институционалдық-ұйымдастырушылық шектеулерімен шартталғанын атап көрсетеді [60, 151 б.]. Аталған тәсілдерді салыстыру кезінде айқын қайшылық байқалады: Н.С. Зиновьева тергеу параличінің түбірін криминалдық инфрақұрылымның сыртқы технологиялық басымдығынан көреді, ал А.А. Рудых құқық қорғау аппаратының өзінің ішкі ұйымдастырушылық және техникалық дәрменсіздігіне назар аударады. Істің мән-жайларын жан-жақты және объективті зерттеу туралы ҚР ҚПК-тің 24-бабының талаптары мәнмәтінінде авторлық ұстанымды қалыптастыра отырып, аталған факторлар бірыңғай деструктивті симбиозды құрайды деп қорытындылау қажет. Трафикті сыртқы криптографиялық бүркемелеу құқық қолданушыны жоғары технологиялық трансшекаралық қол сұғушылықтарға симметриялы жауап қалыптастырудың кез келген мүмкіндігінен айыра отырып, ведомствоаралық алшақтықпен және тергеулікті бөлу проблемаларымен (ҚР ҚПК-тің 187-бабы) түпкілікті бекітіледі.

Ұсынылған теориялық коллизияларды қорытындылау тергеу тығырықтарын бағалауға сапалы жаңа интегративті тәсіл ретіндегі трансшекаралық тосқауылдардың төрт факторлы типологиясын әзірлеуге негізделген жүргізілген зерттеудің ғылыми жаңалығын негіздеуге мүмкіндік береді. Бұл жаңалықтың іргелі элементі ретінде «қылмыстың мультиюрисдикциялық құрамы» феноменін тұжырымдамалау әрекет етеді. Желілік қол сұғушылықтар тетігін интерпретациялай отырып, И.М. Нурбеков онлайн алаяқтықтың объективті жағының элементтері, жасау құралдары және қылмыстық зардаптары әртүрлі құқықтық жүйелер арасында органикалық түрде бөлінгеніне әділетті түрде назар аударады [136, 118 б.]. Осы тезисті ҚР ҚК-нің 190-бабындағы ережелермен қатар қойғанда мынадай көрініс ашылады: іс-әрекеттің объективті жағын құрайтын дәстүрлі материалдық қаңқа енді тұтас күйінде қалмай, әрқайсысы

экстерриториялық қылмыстық қудалаудың тәсілдерін түбегейлі қайта қарауды талап ететін жеке трансұлттық бөлшектерге тарамданады. Осы арада авторлық технологиялық ұстатпаушылық моделі қағидаттық салмақ иеленеді – ол желілік анонимизацияны бұрынғыдай жай ғана криминалистикалық қиындық деп емес, дәлелдеме жинаудың заңды жолдарын тұйыққа тірейтін түбегейлі процестік бөгет ретінде қайта таразылайды. Модельдің түсіндіру қуаты дәл осында: юрисдикциялық олқылық пен бүркемелеудің бағдарламалық құралы тоғысқанда пайда болатын синергетикалық әсерді ол бір-бірлеп, дәйекті ашып береді. Ұсынылып отырған типология тағы бір қарапайым, бірақ қағидаттық жайтты айқын аңғартады: технологиялық және институционалдық коллизияларды бір мезгілде бейтараптандырмай тұрып, шектеудің біреуін ғана шешу – айталық, халықаралық құқықтық көмек рәсімін қағаз жүзінде жеделдету – қылмыстың ашылуын қамтамасыз ете алмайды.

Осы синтетикалық жүйелеудің қорытындысын жинақтай келе, тараудың түйінді бағдарламалық тұжырымын атап өтуге болады: онлайн алаяқтықтың трансшекаралық табиғаты жай ғана кедергілер жиынтығын емес, тереңдігі мен қабаттылығы жағынан кешенді процестік дағдарысты туындатады. Осы дағдарыс шеңберінде юрисдикциялық, хронологиялық, технологиялық және ұйымдастырушылық факторлар жай ғана қатар өмір сүріп қоймайды, сотқа дейінгі іс жүргізудің институционалдық тығырығын құрай отырып, тізбекті реакция қағидаты бойынша бір-бірін өзара күшейтеді. Дәстүрлі қылмыстық сот ісін жүргізудің криминалдық орта тұрғызған эшелондалған қорғаныс желісін еңсере алмауы классикалық тергеу алгоритмдерінің эвристикалық әлеуетінің сарқылуын объективті түрде айғақтайды. Сонымен бірге анықталған көпдеңгейлі трансшекаралық шектеулер құқық қолдану тиімсіздігінің тек сыртқы катализаторы ретінде ғана әрекет етеді, олар отандық қылмыстық-процестік реттеудің жүйелі ішкі коллизияларымен органикалық түрде толықтырылады және масштабталады. Анықталған факт оларды кейіннен егжей-тегжейлі талдаудың қатаң логикалық және ғылыми қажеттілігін детерминациялайды.

2.4 Цифрландыру жағдайындағы қылмыстық-процестік реттеудегі олқылықтар мен коллизиялар және құқық қолдану практикасының проблемалары

Трансшекаралық және технологиялық тосқауылдарды зерттеу логикалық түрде Қазақстан Республикасының ішкі қылмыстық-процестік заңнамасын жүйелі талдау қажеттілігіне алып келеді. Бұған дейін дәлелденгендей, құқықтық реттеудің қолданыстағы моделі архаикалық материалистік парадигманы сақтап отыр. ҚР ҚПК нормаларында белгіленген ұғымдық вакуум және виртуалды деректерді классикалық құжаттар мен заттарға жасанды түрде теңестіру терең доктриналық жікті тудырады. Осы проблеманы талдай отырып, А.И. Зазулин заңды нормативтік нақтылаудың болмауы ерекше цифрлық артефактілердің (жүйелік логтар, IP-мекенжайлар, скриншоттар) тұрақты дербес мәртебеге ие болмауына әкелетінін, мұның нәтижесінде олардың жол берілушілігі тек ситуациялық және субъективті-бағалау сипатына ие болатынын тұжырымдайды

[114, 101-103 б.]. Сонымен бірге А.А. Толыбаева мен тең авторлар кибержымқырулар тетігіндегі бөлінген деректер массивтерінің орасан зор іс жүзіндегі маңыздылығы мен олардың көмескі, бұлыңғыр нормативтік бекітілуі арасындағы сыни алшақтыққа нұсқай отырып, коллизияны кеңірек диагностикалайды [98, 127-128 б.]. Осы ұстанымдарды салыстыру зерттеу акценттерінің айқын айырмашылығын көрсетеді: егер А.И. Зазулин басты қатерді нақты ұшпа іздердің процестік осалдығынан көрсе, онда авторлар ұжымы нормативтік базаның өзінің институционалдық дәрменсіздігін дәлелдейді. Осы пікірталасты шеше отырып, авторлық ұстанымды тұжырымдау қажет: электрондық ақпарат табиғатының заңды белгісіздігі қылмыстық қудалаудың бүкіл конструкциясына қауіп төндіре отырып, барлық кейінгі сатыларға автоматты түрде трансляцияланатын бастапқы процестік іркілісті қалыптастырады.

Дәлелдеу құқығының аталған коллизиялары бұған дейін талданған инициациялау сатысының институционалдық тосқауылын ушықтыра түседі, мұнда ҚР ҚПК-тің 179-бабын қолдану тетігі жасанды латенттіліктің және құбылмалы іздерді жоғалтудың тікелей катализаторы ретінде әрекет етеді.

Аталған процестік паралич логикалық түрде дәлелдемелерді тікелей тіркеп-белгілеу тетігіндегі терең ақауларды алдын ала айқындайды. ҚР ҚПК-тің 123 және 199-баптары нақты деректердің нысаны тарихи түрде материалдық жеткізгіштерді және заттық әлемнің физикалық қабылданатын объектілерін көзбен шолып сипаттауға бағдарланған хаттамаларда бекітілуін қатаң талап етеді. Осы нормалардың іс жүзіндегі дәрменсіздігін зерттей отырып, М.С. Бисалиев техникалық-құқықтық вакуумге: заңда алып қойылатын файлдардың криптографиялық хэш-сомаларын міндетті түрде есептеу және бекіту сияқты криминалистикалық тұтастық (integrity) алгоритмдерінің регламенттелуі толығымен жоқ екеніне назар аударады [16, 97-98 б.]. Проблеманы өзге көзқарас тұрғысынан Е.С. Шевченко қарайды, ол «ұшпа» (volatile) деректерге консервативті қағаз нысандарын механикалық түрде қолдану олардың дәлелдемелік күшін архаикалық рәсімдерді формальды түрде сақтауға тәуелді ететінін атап көрсетеді. Автор дәстүрлі «материалдық» іздерді (мысалы, ноутбукты дактилоскопиялық ұнтақпен өңдеу) бірінші кезекте бекіту әрекеттері техникалық құрылғының жұмысына кері әсер етіп (информацияға қол жеткізуді бұғаттап), цифрлық артефактілердің қайтарымсыз жоғалуына әкелуі мүмкін екенін бұлтартпай дәлелдейді [59, 107 б.]. Ұсынылған ұстанымдарды салыстыру тұжырымдамалық алшақтықты айқындайды: М.С. Бисалиев қажетті инновациялық стандарттардың жоқтығын тіркейді, ал Е.С. Шевченко ескірген материалдық ритуалдардың процеске жойқын әсерін сынайды. Авторлық тәсілді негіздей отырып, осы ақаулардың симбиозы ҚР ҚПК-тің 112-бабын қолданудың сыни тәуекелін тудырады деп қорытындылау қажет. Техникалық тұрғыдан анық цифрлық артефактілер сөзсіз тек формальды негіздер бойынша жол берілмейтін болып танылады, өйткені бөлінген машинамен оқылатын деректерді алып қоюдың материалдық бағдарланған тәртібін сақтау физикалық тұрғыдан мүмкін емес.

Процестік іркілістер жүйесіндегі аяқтаушы буын ретінде электрондық

деректерді объективтендірудің негізгі құралы болып табылатын сот сараптамасы арқылы ақпаратты бағалау сатысы әрекет етеді. Сараптамалық зерттеулерді тағайындаудың жалпы қағидалары (ҚР ҚПК-тің 273-бабы) виртуалды объектілердің ерекшелігіне мүлдем бейімделмеген. Осы институционалдық олқылықты бағалай отырып, Е.Р. Россинская заңда цифрлық криминалистиканың мамандандырылған стандарттарының сыни түрде жоқтығын және өзгермелі деректерді зерттеудің легитимді әдістерінің нормативтік белгісіздігін тұжырымдайды [134, 195 б.]. Проблематиканы тереңдете отырып, А.И. Семикаленова бұлтты қоймалармен байланысты жағдайлардың шешілместігіне нұсқайды: сараптаманың қашықтан жасалатын нысандарын регламенттеудің өте шектеулілігі дәлелдеудің бүкіл ауыртпалығын маманның жеке техникалық құзыреттілігінің субъективті деңгейіне ауыстырады [146, 118 б.]. Осы пікірлерді талдау сараптамалық дағдарыстың локализациялануындағы айырмашылықты көрсетеді: жалпы әдіснамалық тапшылықтан экстерриториялық зерттеулердің рәсімдік блокадасына дейін. Біздің ойымызша: нормативтік вакуум жағдайында компьютерлік-техникалық сараптаманы жүзеге асыру сарапшы қорытындысының мәртебесін (ҚР ҚПК-тің 116-бабы) фатальды түрде құнсыздандырады. Цифрлық кодпен жұмыс істеудің процестік алгоритмдерінің жоқтығы қорғау тарапына объект қасиеттерінің ықтимал санкцияланбаған өзгеруі желеуімен зерттеу нәтижелеріне кедергісіз дау айтуға мүмкіндік береді.

«Архаикалық норма → практикалық дәрменсіздік → дәлелдеу үшін негативті салдарлар» тізбегін талдау мынадай қорытынды жасауға мүмкіндік береді: рәсімдік-құқықтық коллизиялар жүйелі сипатқа ие. Олар әрбір сатыда сотқа дейінгі іс жүргізудің тиімділігін айтарлықтай төмендететін институционалдық тосқауылдар кешенін қалыптастырады. ҚР ҚПК-те берік орныққан консервативті материалдық бағдарланған модель виртуалды іздік көрініс барабар құқықтық реттеуді қамтамасыз етуге объективті түрде қабілетсіз. Терминологиялық, рәсімдік және сараптамалық олқылықтармен детерминацияланған цифрлық дәлелдемелердің процестік мәртебесінің тұрақсыздығы тергеп-тексеру тиімділігін төмендетудің тұрақты практикасын қалыптастырады. Цифрлық іздермен жұмыс істеу үшін дәстүрлі тетіктердің анықталған абсолютті жарамсыздығы процестік алгоритмдерді іргелі қайта қараудың және электрондық қылмыстық сот ісін жүргізудің инновациялық парадигмасын жобалауға логикалық көшудің ғылыми қажеттілігін объективті түрде алдын ала айқындайды.

Процестік реттеудің тұжырымдамалық осалдығы жайлы теориялық түйіндер бос қалмайды – оларды құқық қолдану практикасын эмпирикалық зерделеу объективті түрде тексеріп, растайды. Осы мақсатта зерттеу барысында 2020-2026 жылдар аралығында ҚР соттары онлайн алаяқтық істері бойынша (нақтырақ айтсақ, ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағы бойынша) шығарған 127 үкімнің жиынтығы жүйелі талдаудан өткізілді. Талдаудың басты нысанасы айқын: қылмыстық орта цифрланған жағдайдағы құқық қолданудың қайталанып отыратын типтік үлгілерін ашу. Осылайша қашықтан жымқыру мен оны дәлелдеудің тұрақты криминологиялық әрі процестік заңдылықтарын көруге жол ашылды. Жинақталған сот актілерінің бұл корпусы диссертацияның негізгі

эмпирикалық тірегі рөлін атқарады: кейінгі теориялық қорытындылар да, тұжырымдамалық ұсыныстар да тікелей осы материалды кешенді зерттеуден өрбиді.

Неге дәл 2018 жыл шек ретінде алынды деген сұрақтың жауабы статистиканың өз табиғатында жатыр. Бұған дейінгі кезеңнің (2018 жылға дейінгі) деректері алаяқтықты жасалу тәсілі бойынша ажыратпаған, сондықтан онлайн-сегментті жеке бөліп алып салғастыруға мүлде келмейді – есеп бір бапқа топтастырылған жалпы санмен ғана шектелген. Тап осы жылдан бастап ҚР ресми қылмыстық статистикасына алаяқтықтың егжей-тегжейлі құрылымы – соның ішінде интернет-алаяқтық пен ақпараттық-коммуникациялық технологиялар арқылы жасалатын өзге де түрлерін бөлектеп көрсету – енгізілді. Дәл осы әдіснамалық бетбұрыс динамиканы жылдар бөлігінде салыстыруға мүмкіндік берді, сол себепті эмпирикалық база нақ 2018 жылдан есептеледі.

Зерттеу ҚР ҚК-нің 190-бабындағы алаяқтықтың барлық көрінісін емес, тек ақпараттық жүйелер мен ғаламтор арқылы жасалатынын ғана қамтиды. Мұндай шектеу зерттеу пәнінен туындайды: онлайн алаяқтық мұнда өзіндік криминологиялық құбылым ретінде дербес қарастырылады.

Алаяқтықтың жалпы құрылымында, әрине, интернеттен бөлек басқа да тармақтар бар – несиелеу саласындағы, төлем карточкаларын қолдану арқылы, сақтандыру мен өзге мүліктік қатынастардағы алаяқтық. Дегенмен өсудің ең айқын қарқынын, әрі осы қылмыс түрінің тұтас бет-бейнесін өзгертетін басым ықпалды көрсетіп отырған нақ интернет-алаяқтық – зерттеудің фокусы да осымен түсіндіріледі.

Алаяқтық құрылымындағы ығысуды сандық тұрғыдан бағалау үшін ҚР ҚК-нің 190-бабы бойынша тіркелген қылмыстардың жалпы көлемі мен интернет-алаяқтықтың арасалмағын 1-кесте арқылы қарастырайық.

1-кесте – Қазақстан Республикасындағы алаяқтық қылмысы саны (ҚР ҚК-нің 190-бабы) және 2018-2025 жж. интернет-алаяқтықтың үлесі

Жыл	**Барлық алаяқтық (190-бап)**	**Интернет-алаяқтық**	**Интернет-алаяқтықтың үлесі, %**
2018	29 282	517	1,8 %
2019	32 286	7 769	24,1 %
2020	33 653	14 155	42,1 %
2021	41 083	21 405	52,1 %
2022	43 499	20 569	47,3 %
2023	44 786	21 777	48,6 %
2024	45 156	22 870	50,6 %
2025	47 483	28 851	60,5 %
Дереккөз: ҚР БП ҚСжАЕК-тің «Тіркелген қылмыстық құқық бұзушылықтар туралы» №1-М нысанындағы есептерінің деректері негізінде автормен құрастырылды [6]			

1-кестедегі сандар бір ғана нәрсені – көрсеткіштің өскенін – айтпайды; олардың астарында пайдакүнемдік қол сұғушылық тетігінің өзегінде жүрген терең құрылымдық жылжу жатыр. Интернет-алаяқтықтың салмағы 2018 жылы небәрі 1,8 % болса, 2025 жылға қарай 60,5 %-ды алып, басым тармаққа айналды. Бірақ мұны «цифрландыру жағдайындағы терең трансформация» деп атай салу құбылыстың неден өрбігенін түсіндірмейді.

Криминологиялық факторлық талдау осынау бұрын-соңды болмаған секірістің артында тұрған детерминанттар шоғырын ажыратып беруге мүмкіндік береді. Мұндай өсу бір ғана себептің салдары емес – оның төркінінде бірнеше үрдістің тоғысуы жатыр, әрі олар бір мезгілде әрекет еткенде ғана осындай қарқын береді. Әсіресе 2020-2021 жылдардағы кенеттен өрлеу (24,1 %-дан 52,1 %-ға дейін) жеке қарауды талап етеді, өйткені бір жыл ішіндегі мұндай қарқынды өзгеріс жүйелік ауысудың айқын белгісі болып табылады.

Бірінші қатарда – макроэкономикалық және әлеуметтік сипаттағы, нақтырақ айтқанда пандемиялық детерминант тұр. 2020 жылы COVID-19 салдарынан енгізілген қатаң карантин цифрландыруды үдеткен ең қуатты катализатор рөлін атқарды. Тұрғындардың басым бөлігі онлайн-тұтынуға әрі қашықтан көрсетілетін қаржы қызметіне жедел ауысуға мәжбүр болды. Мұндағы түйінді жайт – көшудің өзінде емес, оның жеделдігінде: цифрлық орталарды бұрын пайдаланбаған адамдар оларға бір мезгілде, әрі қауіпсіздіктің қарапайым дағдылары қалыптаспай тұрып тартылды. Фишингтік хабарламаны тану, күмәнді сілтемеден сақтану, деректемелерін бөтен адамға айтпау сияқты машықтар халықтың елеулі бөлігінде әлі орнықпаған еді. Осылайша қысқа мерзімде аса ауқымды виктимогенді орта қалыптасты, ал оның ерекшелігі – құрбандыққа айналуы ықтимал адамдардың санында ғана емес, олардың бір уақытта, біртектес осалдықпен пайда болуында.

Екінші фактор – технологиялық-инфрақұрылымдық. 2022-2025 жылдардағы өсу екінші деңгейлі банктердің лездік аударымдарды, онлайн-кредиттеуді (микроқаржы ұйымдарын қоса) және қашықтан биометриялық верификацияны жаппай қолданысқа енгізуімен тікелей корреляцияланады. Бұл құралдардың бастапқы мақсаты – азаматтық айналымды жеделдету мен қаржы қызметінің қолжетімділігін арттыру, алайда дәл сол қасиеттер қылмыскер үшін де қолайлы алаңға айналды. Аударымның лездігі қаражатты кейін қайтарып алуға уақыт қалдырмайды; онлайн-кредиттеу құрбанның атынан қысқа мерзімде қарыз рәсімдеуге жол ашады; қашықтан верификация болса жеке қатысу қажеттігін жойып, алаяқтық рәсімді автоматтандыруға мүмкіндік береді. Нәтижесінде қол сұғушылықты нақты уақыт режимінде монетизациялау техникалық тұрғыдан оңайлады. Жағдайды ушықтырған тағы бір жайт – мемлекеттік әрі жеке дереккөздерден ҚР азаматтарының дербес деректерінің бірнеше мәрте ауқымды тарап кетуі. Мұндай ағып кетулер киберқылмыскерге құрбан туралы алдын ала мәлімет – тегі, шоты, байланыс арналары – беріп, әлеуметтік инженерияны жалпы сипаттан нақты тұлғаға бағытталған, әрі сол себепті әлдеқайда сенімді әрекетке айналдырды.

Үшінші фактор институционалдық-құқықтық жазықтықта жатыр. Тіркелген қылмыс санының шапшаң өсуімен қатар тоқтатыла тұрған істердің саны да

соншалықты жылдам ұлғайды – 2-кестеде көрсетілгендей, 2025 жылы бұл көрсеткіш 22 426 іске жетті. Екі қисықтың қатар өсуі кездейсоқ емес: ол қылмыстың көбеюі мен оны ашу қабілетінің арасындағы алшақтықты айғақтайды. Құқық қорғау жүйесінің цифрлық іздердің экстерриториялық табиғатына дайын болмауы мұнда шешуші рөл атқарды – қаражат бірнеше юрисдикция арқылы өткенде, дәстүрлі тергеу тетіктері жеткіліксіз болып шықты. Оған транзиттік шоттарды (дропперлерді) бұғаттаудың заңды алгоритмдерінің жоқтығы қосылды: қаражат қозғалысын жедел тоқтататын тетік болмаған соң, ұрланған сома тізбектелген шоттар арқылы тез таратылып үлгерді. Осы екі олқылық қаскөйлердің бойында жазадан құтылу сезімін орнықтырды, ал жазасыздық сезімі – қылмыстың қайталануына түрткі болатын аса қауіпті детерминанттардың бірі. Соңғысы, өз кезегінде, кибержымқырулардың сериялық сипат алуына әрі институционалдануына тікелей себеп болды.

Осылайша, Қазақстандағы цифрлық ортаның қарқынды криминализациялануы жеделдетілген әлеуметтік цифрландырудың, финтех-өнімдердің агрессивті дамуының және қылмыстық-процестік институттар реакциясының кешігуінің синергетикалық қабаттасуының нәтижесі болды. Алаяқтық құрылымының аталған трансформациясы оны тергеп-тексерудің тиімділігіне тікелей әсер етеді және тиісті процестік көрсеткіштерді талдау қажеттілігін туындатады. Осыған байланысты ақпараттық жүйелер мен интернет желісін пайдалана отырып жасалған тіркелген қылмыстардың серпінін, сондай-ақ оларды тергеп-тексеру нәтижелерін талдау қажет деп пайымдалады.

2-кесте – Қазақстан Республикасындағы 2018-2025 жж. ақпараттық жүйелер мен интернет желісін пайдалана отырып жасалған алаяқтықтың серпіні және тергеп-тексеру нәтижелері

Жыл	**Тіркелгені (СДТБТ)**	**Сотқа жолданғаны**	**Сотқа жолданғандардың үлесі, %**	**Ашылмағаны (тоқтатыла тұрғаны)**
2018	517	127	24,6%	269
2019	7 769	599	7,7%	5 997
2020	14 155	10 408	26,8%	18 474
2021	21 405	2 308	10,8%	16 578
2022	20 569	2 627	12,8%	15 928
2023	21 777	2 209	10,1%	18 007
2024	22 870	2 868	12,5%	18 062
2025	28 851	4 145	14,4%	22 426
2026*	5 275	634	12%	1 505
Дереккөз: *ҚР БП ҚСжАЕК-тің «Тіркелген қылмыстық құқық бұзушылықтар туралы» №1-М нысанындағы есептерінің деректері негізінде автормен құрастырылды [6]*				
****ескертпе:*** *2026 ж. (қаңтар-наурыз) деректері алдын ала сипатқа ие*				

Сотқа дейінгі тергеп-тексерулерді тоқтата тұру құрылымын қосымша талдау жағдайлардың басым көпшілігі қылмыстық құқық бұзушылықты жасаған адамның анықталмауына (ҚР ҚПК-тің 45-бабы 7-бөлігінің 1-тармағы) байланысты екенін көрсетеді. Мәселен, 2020 жылы бұл көрсеткіш 18 060 жағдайды, 2025 жылы – 22 338-ді құрады, бұл цифрлық ортаның анонимділігімен шартталған интернет-алаяқтықты тергеп-тексерудің негізгі проблемасын айғақтайды. Күдіктінің Қазақстан Республикасының шегінен тыс жерде болуын, халықаралық құқықтық көмек көрсету немесе сараптамалар тағайындау қажеттілігін қоса алғанда, тоқтата тұрудың өзге негіздері бірен-саран сипатқа ие және жалпы құрылымға айтарлықтай әсер етпейді.

Мұнда статистикадан айқын оқылатын процестік парадоксты бөлекше атаған жөн. Істерді тіркеу орасан өскеннің үстіне (2025 жылы 28 851-ге жетті), сотқа жолданғандардың үлесі сын көтермес деңгейде – небәрі 10-14% төңірегінде – қалып отыр. Бұл алшақтық киберқылмыстылықтағы латенттіліктің мүлде жаңа, процестік кейіп киінгенін көрсетеді. Дәстүрлі криминологиялық латенттілік мәлімделмей қалған қылмысты меңзесе, мұндағы жағдай өзгеше: біз анықталмаған субъектінің латенттілігіне тап болып отырмыз. Қылмыстың өзі СДТБТ-да объективті түрде тіркелген, транзакция да верификацияланған; бірақ тергеуде трансұлттық желілік тораптарды деанонимизациялайтын құралдар мен мемлекетаралық деректер алмасу алгоритмдері болмағандықтан, іс түбегейлі тығырыққа тіреледі де, ҚР ҚПК-тің 45-бабы 7-бөлігінің 1-тармағы жаппай қолданысқа түседі. Қылмыстық істердің басым бөлігінің нақ адамның анықталмауы негізінде тоқтатылуы интернет-алаяқтықтың криминологиялық қырын аңғартады: латенттілік деңгейі шектен тыс жоғары, ал қылмыс субъектісін сәйкестендіру – өз алдына бөлек қиындық.

Бұл құбылыс тек жасырындығымен ерекшеленіп қана қоймайды. Оның криминологиялық бейнесінде аумақтық біркелкісіздік те айқын аңғарылады, демек феноменнің табиғаты сандық өлшемдермен ғана емес, кеңістікте орналасу үлгісімен де ашылады. Латенттіліктің тік өлшеміне осылайша көлденең, географиялық өлшем қосылады, ал бұл оны кешенді талдауды одан сайын міндеттейді: онлайн алаяқтық қай жерде, неге жиірек ұя салатынын түсінбей тұрып, оған қарсы шараны нақты нысанаға бағыттау қиын.

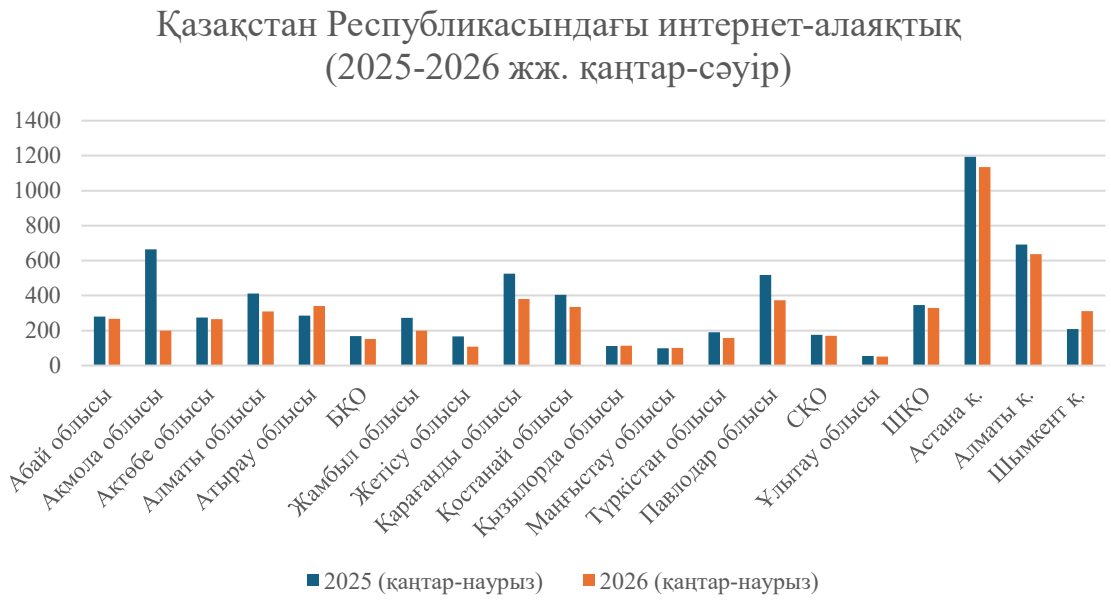
2025 жылдың қорытындысы интернет-алаяқтықтың ең әуелі ірі урбанизацияланған орталықтарға шоғырланатынын көрсетеді. Тіркелген қылмыстардың басым үлесі Астана қаласына (4558), Алматы қаласына (3046) және Қарағанды облысына (2594) келеді. Салыстырмалы жоғары көрсеткіштер Павлодар (2206), Алматы (1780) және Қостанай (1673) облыстарында да байқалады. Мұндай таралым кездейсоқ емес – ол интернет-алаяқтықтың қарқыны өңірдің цифрлық инфрақұрылымымен, халық санымен әрі тығыздығымен, экономикалық белсенділік деңгейімен тығыз байланысты екенін меңзейді. Логика қарапайым: цифрлануы озық, қаржы айналымы қарқынды аймақта әлеуетті құрбандардың саны да, транзакция көлемі де мол, демек қылмыскер үшін «жұмыс алаңы» да кең – сол себепті бұл қылмыс түрінің ұшырасу ықтималдығы да арта түседі.

Керісінше көрініс – ең төмен көрсеткіштер тобы – аталған байланысты тағы

бір қырынан растайды. Ең төмен сандар халқы аз, әлеуметтік-экономикалық қарқыны бәсең өңірлерде тіркелген – Ұлытау облысындағы (322) және Жетісу облысындағы (654) деректер кеңістіктік таралымдағы дифференциацияны айқын айғақтайды. Бұл айырманы бір ғана демографиямен түсіндіру жеткіліксіз; оған интернетке қолжетімділік деңгейі, тұрғындардың цифрлық сауаттылығы және қаржылық операциялардың жиілігі сынды факторлар да қосылады.

Өңірлік құрылымдағы өзгерістердің нақ қазіргі бетбұрысын дәлірек аңғару үшін статиканы ғана емес, қозғалысты да қараған жөн – сол себепті 2025 жыл мен 2026 жылдың қаңтар-сәуір айларын салғастыра талдаған орынды. Осындай салыстыру бір мезеттік суретте көрінбейтін динамиканы – жекелеген өңірлердегі өсім не кему үрдісін, қылмыстылықтың кеңістікте қайта таралу сипатын – ашып береді (1-суретті қараңыз).

1-сурет – Қазақстан Республикасындағы интернет-алаяқтықтың өңірлік серпіні (2025–2026 жж. қаңтар–сәуір)



Дереккөз: Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің ақпараттық-талдамалық порталының деректері негізінде автормен құрастырылды [147].

2025 жылды 2026 жылдың қаңтар-сәуірімен қатар қойған салыстыру ел өңірлерінің көпшілігінде тіркелген интернет-алаяқтықтың жалпы бәсеңдегенін аңғартады (–15,55 %). Бұл кему бірқалыпты емес: Ақмола, Қарағанды, Павлодар облыстарында қысқару айтарлықтай сезіледі, ал мұның өзі өңірлік үрдістердің әркелкілігін көрсетеді.

Дегенмен барлық жерде бірдей төмендеу жоқ – кейбір өңірде керісінше өсім тіркелген. Ең қомақты ұлғаю Атырау облысында (18,9 %) және Шымкент қаласында (50 %) байқалады, оған Қызылорда мен Маңғыстау облыстары қосылады. Мұндай ауытқу криминалдық белсенділіктің құқық қорғау инфрақұрылымы сирегірек өңірлерге ойысып, қылмыстық тәсілдердің цифрлық

ортаның жергілікті жағдайына бейімделіп жатқанын меңзейді.

Бағыты қарама-қарсы болғанмен, интернет-алаяқтықтың өңірлік қаңқасы орнықты күйінде қалып отыр: құқық бұзушылықтың ең тығыз ұйысқан нүктесі әлі де Астана мен Алматы қалалары – мұның астарында цифрланудың жоғары деңгейі, халық тығыздығы және экономикалық қарым-қатынастардың қарқыны жатыр.

Серпіндегі осы алшақтықтар бір қорытындыны бекітеді: интернет-алаяқтық біртектес құбылыс емес, сондықтан алдын алу мен тергеп-тексеруді аумақтық ерекшелікке қарай саралап құру керек. Сонымен бірге қол сұғушылықтың жергілікті бояуы мен өңірлік шоғырлануына қарамастан, құқық қорғау жүйесі бүкіл ел көлемінде ортақ бір институционалдық тосқауылға тіреледі.

Базалық проблема ретінде қылмыстық құдалау тетігінің тотальды тиімсіздігі әрекет етеді. Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасының деректері негізінде бұған дейін анықталғандай, арыздар санының өсуі мен залалды өтеудің ең төменгі деңгейі арасындағы сыни алшақтық істер тергеудің виртуалды ортада субъектіні деанонимизациялау қабілетсіздігіне байланысты жаппай тоқтатыла тұратын сотқа дейінгі іс жүргізудің бастапқы сатыларындағы фатальды процестік шығындарды айғақтайды. Осы тенденцияның қалыптасу тетігін нақтылай отырып, К.О. Карабеков құқық қорғау жүйесі тек қарапайым, нашар бүркемеленген эпизодтарға ғана нәтижелі түрде ден қоюға қабілетті екенін, ал күрделі көпдеңгейлі цифрлық децепция мүлдем жазасыз қалатынын дәлелдейді [17, 145 б.]. Ұсынылған ғылыми көзқарастарды салыстыру зерттеу акценттерінің айқын айырмашылығын көрсетеді: егер С.М. Голятина іркілісті процестің хронологиялық шкаласында (бастапқы кезең) локализацияласа [111, 106 б.], ал К.О. Карабеков жоғары технологиялық схемалар алдында тергеудің сапалық құрылымдық дәрменсіздігін диагностикалайды [17, 102 б.]. Аталған тәсілдерді тергеп-тексеру мерзімдерін үзуді регламенттейтін ҚР ҚПК-тің 45-бабының нормасымен синтездей отырып, негізделген авторлық ұстанымды тұжырымдау қажет. Бастапқы материалдардың басым көпшілігінің тоқтатыла тұрған істер санатына өтуі жай ғана статистикалық қателік емес, консервативті процестік сүзгі істің одан әрі қозғалуын алгоритмдік түрде бұғаттайтын технологиялық шамадан тыс жүктемеге жүйенің заңды реакциясы болып табылады. Анықталған эмпирикалық заңдылық құдалауды инициациялаудың нормативтік моделі кибержымқырулардың гипермобильділігімен тұжырымдамалық тұрғыдан үйлеспейтінін сенімді түрде дәлелдейді.

Анықталған статистикалық іркіліс, бұған дейін дәлелденгендей, кибержымқыруды легитимді азаматтық даудың көрінісіне трансформациялайтын және жасанды латенттілікті катализациялайтын ҚР ҚПК-тің 179-бабын құқық қолданудың жүйелі бұрмалануларымен тікелей шартталған.

Сонымен қатар, анықталған саралау тығырықтары жиналған цифрлық дәлелдемелерді бағалаудың деструктивті практикасымен логикалық түрде ушыға түседі. Нақты деректерді жол берілетіндігі мен анықтығы тұрғысынан бағалауды талап ететін ҚР ҚПК-тің 125-бабының ұйғарымдарын іске асыру виртуалды орта жағдайында қылмыстық істердің сот перспективасының сыни тұрақсыздығын көрсетеді. Сот сәтсіздіктерінің табиғатын зерттей отырып, А.И. Зазулин құқық

қолдану практикасының шамадан тыс формализмге ұрынуын диагностикалайды: дәлелдеу субъектілері алынатын цифрлық кодтың мазмұндық анықтығын толығымен елемей, хаттамалаудың архаикалық нысанын қатаң сақтауға сөзсіз басымдық береді [114, 101-102 б.]. Талдауға өзге көзқарас тұрғысынан қағаз рәсімдерінің объективті орындалмайтындығына назар аударатын М.С. Бисалиев келеді: ұшпа деректерді алып қоюдың классикалық тәртібінен технологиялық негізделген болмашы ауытқу оларды процестен автоматты түрде шығарып тастауға әкеледі [16, 97 б.]. Аталған тәсілдерді талдау ғылыми пікірталастың бар екенін айғақтайды: егер А.И. Зазулин судьялық және тергеулік ойлаудың субъективті консерватизмін сынаса, онда М.С. Бисалиев алып қою технологиясы мен ескірген бекіту рәсімі арасындағы еңсерілмейтін институционалдық тосқауылдың бар екенін дәлелдейді. Біздің ойымызша, ҚР ҚПК-тің 112-бабының императивті тыйым салуын (дәлелдемелердің жол берілмеуін) цифрлық артефактілерге қолдану заңдылық кепілдігін айыптауды бұзу құралына трансформациялайды. Формальды қағаз рәсімін сақтау объективті ақиқатты анықтаудан басым түседі, мұның нәтижесінде кибержымқырудың техникалық верификацияланатын іздері заңдық күшін қайтарымсыз жоғалтады.

Тергеу сәтсіздіктерінің эмпирикалық статистикасын бекітетін аяқтаушы контур ретінде терең институционалдық дағдарыс әрекет етеді. Істің мән-жайларын жан-жақты зерттеу туралы ҚР ҚПК-тің 24-бабының нормативтік талабы кадрлық және технологиялық тапшылық жағдайында физикалық тұрғыдан орындалуы мүмкін емес. Бұған дейін анықталғандай, мамандандырылған аппараттық-бағдарламалық кешендердің тапшылығы іздерді табу процесін физикалық тұрғыдан бұғаттайды. Өз кезегінде, Е.Р. Россинская фокусты коммуникацияларға ауыстыра отырып, басты институционалдық әлсіздік сыни уақыттық кідірістерді тудыратын провайдерлермен және цифрлық платформалармен ведомствоаралық өзара іс-қимылдың шеттен тыс фрагментациясында жатқанын атап көрсетіп, бұл көріністі толықтырады [134, 196 б.]. Көзқарастардың айырмашылығы айқын: А.А. Рудых ақауды ішкі материалдық базада локализациялайды, ал Е.Р. Россинская – сыртқы интеграциялық байланыстарда. Тергеудің жарақтандырылуын тек 44% деңгейінде тіркейтін Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасының ресми деректеріне сүйене отырып авторлық ұстанымды негіздей келе, технологиялық жұтаңдық пен ақпараттық оқшаулану бірыңғай еңсерілмейтін вакуумді құрайды деп қорытындылау қажет [3]. Тергеу аппараты активтерді шығару маршруттарының шифрын ашуға арналған нақты құралдарынан айырылған болып шығады.

Алынған статистикалық деректер дәлелдеудің материалдық бағдарланған нормативтік моделі мен онлайн алаяқтықтың виртуалды табиғаты арасындағы сыни жүйелі алшақтықтың бар екенін сөзсіз растайды. Құқық қолдану практикасы бастапқыда заң шығарушы азаматтардың құқықтарын қорғау үшін құрастырған процестік сүзгілер сот төрелігі үшін еңсерілмейтін тосқауылдарға трансформацияланған тұрақты деструктивті модельдің қалыптасуын көрсетеді. Саралау, дәлелдеу және институционалдық деңгейлердегі анықталған кешенді ақаулық цифрлық іздермен жұмыс істеудің қылмыстық-процестік тетігін іргелі

реформалаудың тұжырымдамалық бағыттарын әзірлеудің объективті қажеттілігін туындатады.

Құқық көздері жүйесінде ҚР Жоғары Сотының нормативтік қаулылары Қазақстан Республикасы Конституциясының 4 және 81-баптарына сәйкес құқық қолдану практикасының біркелкілігін қамтамасыз етуге бағытталған доктриналық-құқықтық бағдарлардың аса маңызды функциясын атқарады. Кибержымқыруларды тергеп-тексеруге қатысты бейінді акт ретінде ҚР Жоғары Сотының №6 нормативтік қаулысы әрекет етеді. Жоғары сот сатысы классикалық тәсілдерді цифрлық ортаға бейімдеуге әрекет жасады: қатаң түрде шарт жасасқанға дейін немесе жасасу сәтінде туындайтын пиғылды дәлелдеуге қатаң талаптар белгіленді, қылмыстың жасалу орны жәбірленушінің геолокациясы бойынша айқындалды, сондай-ақ «ақпараттық жүйені пайдаланушыны алдау» айрықша санаты енгізілді. Осы новеллаларды талдай отырып, А.Б. Курумбаева мен Б.Б. Кощегулов аталған түсіндірулер объективті түрде дәлелдеу стандарттарын күшейтуге және қылмыстық-құқықтық деликтілер мен аралас азаматтық құқықтық қатынастардың аражігін ажыратудың нақты өлшемшарттарын қалыптастыруға бағытталғанын әділетті түрде атап көрсетеді [21, 51 б.].

Іргелі түсіндірулердің болуына қарамастан, оларды іс жүзінде іске асыру терең құқық қолдану диссонансын көрсетеді. Сотқа дейінгі тергеп-тексеру сатысында тұжырымдалған құқықтық ұстанымдарды жүйелі түрде елемеу байқалады: қылмыстық қудалау органы тараптардың бастапқы ниеттеріне таза формальды бағалауды жүзеге асырады. Осы процесті зерттей отырып, Е.И. Майорова, В.В. Улейчик және Л.В. Яковлева тұлғасындағы авторлар ұжымы алаяқтықты азаматтық-құқықтық даулардан ажырату алгоритмі сыни тұрғыдан тұрақсыз күйінде қалып отырғанын атап көрсетеді [148, 46 б.]. Проблеманың эмпирикалық базасын дамыта отырып, А.Б. Сабырбаева тұжырымдайды: цифрлық платформалар арқылы қаражатты сырттай ерікті түрде аударымдармен бетпе-бет келгенде, тергеушілер қылмыстық-құқықтық бағалауды жекеқұқықтық конструкциялармен жаппай алмастырады [103, 152 б.]. Заңды қорытынды ретінде арыздарды тіркеуді бұғаттайтын және сот практикасының шеттен тыс біртекті еместігін консервациялайтын ҚР ҚПК-тің 179-бабын негізсіз қолдану әрекет етеді.

Ресми соттық түсіндіру тиімділігінің шектеулі болу себептері өткір доктриналық пікірталас тудырады. Жоғары сот сатыларының ықпалын бағалай отырып, М.С. Бисалиев түсіндірулер материалдық құқық олқылықтарының орнын ішінара толтыратыны, алайда онлайн алаяқтықтың технологиялық аспектілері мен цифрлық дәлелдемелерді жинау алгоритмдерін нормативтік нақтылаудың жеткіліксіздігіне байланысты олардың әлеуеті ашылмайтыны туралы ұстанымды негіздейді [16, 45 б.]. Бұл тәсілмен абстрактілі құқықтық тұжырымдамалар мен цифрлық шынайылық арасындағы еңсерілмейтін алшақтықтың бар екенін дәлелдейтін В.В. Коломинов қатаң тұжырымдамалық қайшылыққа түседі [91, 56 б.]. Осы ғылыми көзқарастар іргелі алшақтықты көрсетеді: егер М.С. Бисалиев проблеманы жойылатын құқықтық олқылық (технологияларға бейімделудің толық еместігі) ретінде сараласа, онда В.В.

Коломинов пиғылды дәлелдеудің дәстүрлі матрицасының әлеуметтік инженерия, фишинг және желілік анонимділік құралдарымен абсолютті гносеологиялық үйлесімсіздігін диагностикалайды.

Біздің ойымызша, іс жүзінде аталған екі фактор да соттық түсіндіру институтының өзінің мүмкіндіктерінің шегін аша отырып, кумулятивті түрде әрекет етеді. Жоғарғы Сот классикалық мысалдарды (нақты қаржылық мүмкіндіктің болмауы, қолдан жасалған құжаттарды пайдалану) қолдана отырып, тек физикалық шынайылықта ғана тиімді жұмыс істейтін материалдық-құқықтық құралдарды ұсынады. Субъект криптографиялық алгоритмдермен, алмастырылған IP-мекенжайлармен және транзиттік шоттармен жасырылған киберкеңістік жағдайында, алдын ала қалыптасқан пиғылды дәлелдеу ұшпа іздерді жинаудың жоғары технологиялық процестік рәсімдерін қолдануды талап етеді. Демек, архаикалық процестік нысан Жоғарғы Соттың материалдық-құқықтық талаптарын тергеу аппараты үшін физикалық түрде орындалмайтын ете отырып, құқық қолданушыны электрондық деректерді тіркеп-белгілеуге арналған легитимді құралдардан айырады.

Беделді нормативтік бағдарлардың болуына қарамастан, оларды іс жүзінде іске асыру сыни тұрғыдан шектеулі күйінде қалып отыр, бұл тұрақты құқық қолдану практикасының қалыптасуына еңсерілмейтіндей кедергі келтіреді. Ресми соттық түсіндіру актілері қылмыстық-процестік реттеудің терең жүйелі ақауларының орнын толтыруға объективті түрде қабілетсіз. Нормативтік қаулылардың реттеушілік әлеуеті құқықтық вакуумді шешілмеген күйінде қалдыра отырып, тергеп-тексеруді инициациялаудың іргелі процестік тосқауылдарын жоймайды. Бұл тұжырымдамалық тығырық киберқылмыстарды тергеп-тексерудің жаңа, жүйелі процестік-технологиялық моделін пәндік әзірлеу қажеттілігін туындатады.

Жүргізілген доктриналық, нормативтік және праксиологиялық талдау нәтижелерін қорыту онлайн алаяқтық туралы істер бойынша сотқа дейінгі іс жүргізудің бастапқы сатыларында анықталған кемшіліктер терең жүйелі сипатқа ие деп тұжырымдауға мүмкіндік береді. Институционалдық дағдарыстың негізінде консервативті қылмыстық-процестік реттеу мен қазіргі заманғы қылмыстылықтың объективті цифрлық табиғаты арасындағы іргелі қайшылық жатыр. Осы дағдарыстың бастапқы себептерін зерттей отырып, А.И. Зазулин барабар ұғымдық аппараттың және цифрлық санаттардың (атап айтқанда, ҚР ҚПК-тің 120-бабында) заңды мәртебесінің болмауы құқық қолданушыны нормативтік бағдарлардан айыратын бастапқы гносеологиялық вакуумді қалыптастыратынын дәлелдейді [114, 101 б.]. Проблеманы талдауға өзге көзқарас тұрғысынан басты ақау терминдерде емес, өткір рәсімдік коллизияларда жатыр деп тұжырымдайтын А.А. Толыбаева бастаған авторлар ұжымы келеді: физикалық хаттамалауды (ҚР ҚПК-тің 199-бабы) императивті түрде талап ететін дәлелдемелерді жинаудың дәстүрлі нысандары виртуалды іздердің гиперқұбылмалы ерекшелігімен еңсерілмейтін қақтығысқа түседі [98, 131 б.]. Өз кезегінде, Е.Р. Россинская нормативтік кемшіліктер кадрлық тапшылықта көрініс тапқан еңсерілмейтін технологиялық шектеулердің (желілік анонимизацияның) және институционалдық тосқауылдардың фоны ғана болып табылатынын атап

көрсете отырып, зерттеу фокусын сыртқы ортаға ауыстырады [134, 194 б.].

Келтірілген ғылыми тәсілдерді салыстыру тергеу параличінің бастапқы себебінің локализациялануындағы айқын айырмашылықты диагностикалауға мүмкіндік береді: гносеологиялық олқылық (А.И. Зазулин), рәсімдік ақаулық (А.А. Толыбаева) немесе технологиялық-институционалдық дәрменсіздік (Е.Р. Россинская). Осы ғылыми пікірталасты шеше отырып, негізделген авторлық ұстанымды тұжырымдау қажет. Аталған тосқауылдарды оқшауланған түрде қарастыру әдіснамалық тұрғыдан қате болып табылады, өйткені олар бірыңғай, қатаң детерминацияланған жүйені құрайды. Заңның тұжырымдамалық олқылықтары сөзсіз рәсімдік тығырықтарды тудырады, олар өз кезегінде агрессивті цифрлық ортамен еселеп ушыға түседі және тергеу аппаратының ұйымдастырушылық инерттілігімен бекітіледі. Әрбір фактор басқалардың деструктивті катализаторы ретінде әрекет ететін процестік деформациялардың көшкін тәрізді жиналуының қайтымсыз эффектісі туындайды.

Анықталған нормативтік қайшылықтардың синтезі қылмыстық-процестік реттеудің конструктивтік ақауларының квадрупольдік моделін әзірлеуде кристалданады. Осы модельдің біріктіруші буыны ретінде біз бұған дейін негіздеген құқық қолданудағы «цифрлық нигилизм» феномені әрекет етеді. П.С. Пастуховтың құқықтық сананың консерватизмі туралы түйіндеріне және С.М. Голятинаның праксиологиялық деректеріне сүйене отырып, дәл осы когнитивтік тосқауыл құқық қолданудың жүйелі бұрмалануларын детерминациялайды деген қорытындыға келеміз. Ол архаикалық нормаларды формальды түрде қолдану ҚПК-тің қорғау сүзгілерін неліктен кибержымқырулардың жасанды латенттілігін мультипликациялау тетіктеріне трансформациялайтынын түсіндіреді.

Жүргізілген көп аспектілі талдаудың қорытындысы ретінде жүйелі түйін әрекет етеді: онлайн алаяқтықты сотқа дейінгі тергеп-тексеруді қазіргі заманғы қылмыстық-процестік реттеу терең тұжырымдамалық алшақтық жағдайында тұр. Дәлелдеудің дәстүрлі материалистік парадигмасы, статикалық құқық қолдану практикасы және гипердинамикалық технологиялық шынайылық өзара мүлдем келісілмеген. Қолданыстағы материалистік догмаларды сақтау сөзсіз фатальды салдарларға: қылмыстық қудалаудың жалпы тиімділігінің апатты түрде төмендеуіне, бастапқы кезеңдерде электрондық дәлелдемелік ақпараттың қайтарымсыз жоғалуына және ақаулы құқық қолдану практикасының қалыптасуына алып келеді.

Қолданыстағы консервативті модель шеңберінде желілік деликтілерді тергеп-тексеру тиімділігін арттыру объективті түрде мүмкін емес. ҚР ҚПК-тің жекелеген баптарына механикалық түрде нүктелі өзгерістер енгізу дәлелдеу құралдарының жүйелі параличінің орнын толтыруға қабілетсіз. Классикалық нысандардың эвристикалық және реттеушілік әлеуетінің сарқылуы сотқа дейінгі тергеп-тексерудің қағидатты түрде жаңа процестік-технологиялық моделін әзірлеу қажеттілігін баламасыз түрде туындатады. Бұл модельді қалыптастыру цифрлық дәлелдемелердің дербес ақпараттық табиғатын тікелей заңнамалық тануға, озық IT-құралдарды тергеу қызметіне легитимді түрде интеграциялауға және процестік рәсімдерді трансшекаралық виртуалды кеңістіктің сын-қатерлеріне түбегейлі бейімдеуге қатаң бағдарлануға тиіс.

3 ОНЛАЙН АЛАЯҚТЫҚ ҚЫЛМЫСТАРЫН СОТҚА ДЕЙІНГІ ТЕРГЕП-ТЕКСЕРУДІ ЖЕТІЛДІРУДІҢ ТҰЖЫРЫМДАМАЛЫҚ БАҒЫТТАРЫ

3.1 Онлайн алаяқтық қылмыстарын сотқа дейінгі тергеп-тексерудің қылмыстық-процестік тетігін дамыту және тиімді тергеп-тексеру моделін қалыптастыру

Алдыңғы зерттеу кезеңінің нәтижелерін қорыту онлайн алаяқтықты сотқа дейінгі тергеп-тексерудің анықталған тосқауылдары қолданыстағы сот ісін жүргізу моделінің терең құрылымдық дағдарысын құрайтынын бұлжытпай дәлелдейді. Осы құбылыстың табиғатын талдай отырып, А.А. Толыбаева бастаған авторлар ұжымы тергеудің құбылмалы іздермен жұмыс істеуге қабілетсіздігінен көрініс тапқан құқық қолданудың эмпирикалық проблемалары киберқатерлерге барабар ден қоюды бұғаттайтын ауқымды процестік дағдарысты қалыптастыратынын тұжырымдайды [98, 127 б.]. Бұл праксиологиялық тәсілден айырмашылығы, А.И. Зазулин дағдарыс цифрлық ортамен соқтығысуы кезінде дәлелдеудің базалық моделінің өзін параличке ұшырата отырып, қолданбалы емес, таза құрылымдық сипатқа ие екенін дәлелдейді [114, 103 б.]. Ұсынылған ұстанымдарды талдау деградация тереңдігін бағалаудағы айырмашылықты көрсетеді: егер А.А. Толыбаева бастапқы себепті тергеу практикасының ақауларынан көрсе, онда А.И. Зазулин қылмыстық-процестік доктринаның өзінің іргелі дәрменсіздігін диагностикалайды. Біздің ойымызша, анықталған жүйелі іркіліс заңның жекелеген нормаларын фрагменттік өзгерту шеңберінде объективті түрде еңсерілуі мүмкін емес. Желілік жымқырулар латенттілігінің аномальді жоғары деңгейі, халықаралық өзара іс-қимыл институттарының параличі және аппараттың технологиялық жеткіліксіздігі сотқа дейінгі іс жүргізу негіздерін тұжырымдамалық қайта қарауға деген императивті қажеттілікті детерминациялайды.

Институционалдық параличтің іргелі себебі тарихи түрде субъектіге орталықтандырылған логикада құрылған қылмыстық процестің консервативті архитектурасында жатыр. ҚР ҚПК-тің 111 және 118-баптарының талаптары адамды бастапқы анықтауды және оның іс-әрекетінің физикалық тұрғыдан сезілетін іздерін іздестіруді талап ете отырып, «субъект → дәлелдемелер» векторын баламасыз бекітеді. Осы тығырықты зерттей отырып, П.С. Пастухов процесті жаңғырту архаикалық стереотиптерден толық бас тартуды объективті түрде талап ететінін сенімді түрде дәлелдейді, өйткені ақпараттық қоғамда материалдық іздерді іздестірудің дәстүрлі алгоритмі мүлдем жұмыс істемейді [100, 526 б.]. Трансформация идеясын дамыта отырып, Д.В. Бахтеев виртуалды артефактілерді барабар қабылдау үшін тергеушінің криминалистикалық ойлауын түбегейлі өзгерту қажеттілігін негіздей отырып, акцентті когнитивтік аспектіге ауыстырады [133, 305 б.]. П.С. Пастухов пен Д.В. Бахтеевтің көзқарастарын салыстыру талап етілетін жаңғыртудың әртүрлі деңгейлерін айқындайды: біріншісі объективті нормативтік-процестік қайта құруды талап етеді, ал екіншісі құқық қолданушының субъективті психологиялық трансформациясына назар

аударады. Осы тәсілдерді синтездей отырып, инновациялық «артефактіге орталықтандырылған кибер-процестік модельге» көшудің авторлық тұжырымдамасы негізделеді. Ұсынылған парадигма шеңберінде цифрлық із (желілік лог, IP-мекенжай, транзакция) дәлелдемелік ақпараттың бастапқы көзі ретінде танылады, ал тергеп-тексеру логикасы векторын императивті түрде «із → субъект» бағытына өзгертеді, мұнда заңдық маңызы бар деанонимизация экстерриториялық ортаны жоғары технологиялық талдаудың заңды қорытындысына айналады.

Мұнда бір техникалық жайтты естен шығармаған жөн: бүгінгі киберқылмыскерлер шынайы IP-мекенжайы мен тұрған жерін бүркеу үшін VPN (виртуалды жеке желі), прокси-серверлер, TOR (The Onion Router) секілді анонимизация құралдарын қарқынды пайдаланады, ал бұл тергеуді едәуір ауырлатады. Дегенмен осы бөгеттерді бұзып өтіп, қылмыскерді деанонимизациялаудың заманауи техникалық жолдары да жетілген.

Ең әуелі – шашыраңқы желілік артефактыларды бір арнаға жинау үшін ашық дереккөздерді барлау (OSINT – Open Source Intelligence) жүйелерін кеңінен іске қосу. Д.В. Завьялова көрсеткендей, Maltego не Recon-ng тәрізді бағдарламалық кешендер қылмыскердің желіде бұрын жіберген қателерін, тіркелу тарихын, жалған аккаунттары мен крипто-әмияндарының арасындағы көзге ілінбейтін байланыстарды автоматты түрде талдап шығады [92, 60 б.].

Екінші жол – прокси мен TOR желісінің шығу түйіндерін (exit nodes) қадағалау және трафикті таймингтік тұрғыдан талдау (timing analysis). Тереңдетілген пакеттік инспекция (DPI – Deep Packet Inspection) технологиялары мен байланыс операторларының лог-файлдарын қатар қойып, анонимді желіге кірген әрі одан шыққан пакеттердің көлемі мен уақытын сәйкестендіру арқылы нақты пайдаланушыны математикалық дәлдікке жуық анықтауға болады [57, 182 б.].

Үшінші тәсіл жедел-іздестіру шаралары аясында қолданылады: арнайы «тұзақ-сайттар» (honeypots) не бақылаудағы фишингтік сілтемелер құрылады. Мұндай қақпан қылмыскерді VPN әлі іске қосылмай тұрған сәтте немесе қорғалмаған сессия кезінде сілтемені ашуға итермелеп, оның шынайы цифрлық іздерін – MAC-мекенжайын, құрылғының метадеректерін, нақты IP-адресін – тіркеп қалуға жол ашады. Түйіні: анонимизация құралы қылмыскерге мүлтіксіз қалқан бола алмайды, ал аталған техникалық әдістерді біртұтас тергеу алгоритміне ұластыру деанонимизацияны әлдеқайда тиімді әрі нәтижелі етеді [57, 162 б.].

Мәлімделген артефактіге орталықтандырылған парадигманы іске асыру қылмыстық-процестік тетікті өзара байланысты төрт бағыт бойынша кешенді құрылымдық реформалау қажеттілігін детерминациялайды. Тұжырымдамалық (дефинициялық) деңгейде цифрлық дәлелдемелердің ақпараттық табиғатын заңды бекіту талап етіледі. Осы аспектіні бағалай отырып, М.С. Бисалиев технологиялық даму мен құқықтық реттеу арасындағы алшақтықтан туындайтын өткір «нормативтік турбуленттілікті» атап көрсетеді. Бұл жағдайды еңсеру үшін виртуалды іздердің табиғатын ескеретін арнайы құқықтық режимдерді енгізіп, олардың ҚР ҚПК-тің 120-бабында бекітілген «өзге де

құжаттар» (электрондық құжаттар) қатарындағы орнын нақтылау қажеттілігі туындайды [16, 60-61 б.]. Өз кезегінде, институционалдық бағыт бейінді кибербөлімшелерді құру қажеттілігін туындатады. Бұл тосқауылды қарастыра отырып, Е.Р. Россинская кадрлық-технологиялық тапшылық Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасында көзделген дәлелді аналитика қағидаттарын қолдануды объективті түрде бұғаттайтынын дәлелдейді [149, 95-96 б.]. Осымен қатар халықаралық бағыт ҚР ҚПК-тің 559-бабында бекітілген инерциялық дипломатиялық рәсімдерден түбегейлі бас тартуды талап етеді. Осы проблеманы талдай отырып, Д.В. Завьялова фатальды юрисдикциялық фрагментацияны диагностикалайды, оны тек нақты уақыт режимінде деректермен жеделдетілген трансшекаралық алмасу арқылы ғана еңсеру мүмкін болады [90, 169-170 б.]. М.С. Бисалиевтің, Е.Р. Россинскаяның және Д.В. Завьялованың ұстанымдарын талдау дағдарыстың көпвекторлылығын көрсетеді: ішкі ұғымдық вакуум тергеудің технологиялық әлсіздігімен ушыға түседі және сыртқы юрисдикциялық шекаралармен түпкілікті бекітіледі. Рәсімдік бағыт – деректерді қашықтан тіркеп-белгілеудің және сақтаудың ерекше техникалық-құқықтық стандарттарын әзірлеу – монолитті реформалық модельді құрай отырып, ұғымдық аппаратты институционалдық мүмкіндіктермен және халықаралық сұрау салулармен синхрондауға қабілетті орталық байланыстырушы буын ретінде әрекет етеді деп пайымдау негізді болып табылады.

Онлайн алаяқтықты ашу алгоритмдерін реформалау дәлелдемелердің автономды денесіз табиғатын тануға негізделген қағидатты түрде жаңа процестік парадигмаға көшуді үзілді-кесілді талап етеді. Тұжырымдалған артефактіге орталықтандырылған тұжырымдама таза доктриналық абстракция деңгейінде қала алмайды, өйткені криминалдық ортаның технологиялық трансформациясы қатаң құқықтық нақтылауды талап етеді. Жаңа процестік алгоритмдерді жүйелі түрде интеграциялаудағы анықталған объективті қажеттілік әрбір тергеу әрекетінің алгоритмдерін пысықтай отырып, сотқа дейінгі тергеп-тексеруді жүргізудің егжей-тегжейлі, кезең-кезеңмен интегративті моделін әзірлеу қажеттілігін туындатады.

Тұжырымдамалық артефактіге орталықтандырылған парадигма сотқа дейінгі тергеп-тексерудің жүйелі көпдеңгейлі құрылымын құру арқылы өзінің объективті процестік және ұйымдастырушылық нақтылануын талап етеді. Желілік жымқыруларға тиімді қарсы іс-қимыл превентивті, процестік және технологиялық тетіктерді бірыңғай ажырамас матрицаға терең интеграциялау шартымен ғана объективті түрде мүмкін болады. Осы процесті талдай отырып, А.Л. Осипенко киберқылмыстылыққа қарсы тиімді күрес фрагментарлық емес, желілік ақпараттық кеңістіктегі нақты криминогендік жағдайды ескеретін кешенді нормативтік құқықтық актілерді қабылдау арқылы ғана мүмкін болатынын негізді түрде дәлелдейді [150, 312 б.]. Нормативтік іргетасы ретінде «Қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл туралы» ҚРЗ-ның 4-бабы [151] мен «Төлемдер және төлем жүйелері туралы» ҚРЗ-ның 25-1-бабы негізінде банктердің қауіпсіздік жүйелері мен қаржылық мониторинг тетіктерін

интеграциялаумен қамтамасыз етілетін тергеп-тексерудің бастапқы, превентивті деңгейін қалыптастыру әрекет етеді. Осы деңгейді зерттей отырып, В.О. Давыдов пен И.В. Тишутина оның функционалдық мақсаты цифрлық ортаға үздіксіз криминалистикалық мониторинг жүргізуге және жәбірленушінің ресми жүгінуіне дейін криминалдық белсенділік маркерлерін ерте автоматтандырылған түрде анықтауға саятынын тұжырымдайды [152, 24 б.]. хнологиялық бағытпен өткір пікірталасқа Д.В. Завьялова түседі, ол таза профилактикалық шаралардың шектеулілігін әділетті түрде атап өтіп, уақыттың шеттен тыс тапшылығы жағдайында СДТБТ-де электрондық хабарларды жедел тіркеуді қамтамасыз етуге арналған инициациялық деңгейге олардың жіксіз трансформациялануының объективті қажеттілігін атап көрсетеді [90, 95-96 б.]. Келтірілген пікірлерді талдау кезеңдерге басымдық берудегі айырмашылықты көрсетеді: бірінші авторлар сотқа дейінгі аппараттық-бағдарламалық скринингтің рөлін абсолюттендіреді, ал Д.В. Завьялова оның дереу процессуалдаусыз құқықтық осалдығын диагностикалайды. Біздің ойымызша, превентивті және инициациялық деңгейлер бірыңғай ажырамас тетік ретінде жұмыс істеуге тиіс. Антифрод-орталықтар тіркеген технологиялық аномалия дабылдың цифрлық сигналын дәлелдеудің легитимді процесіне лездік трансформациялауды қамтамасыз ете отырып және жасанды латенттіліктің классикалық проблемасын жоя отырып, ҚР ҚПК-тің 179-бабын қолдану үшін тікелей және жеткілікті себеп ретінде әрекет етуге міндетті.

Процестік инициациялаудан кейін дереу артефактілік деңгей әрекетке кіріседі, оның функционалы нақты деректерді жинау және бекіту туралы ҚР ҚПК-тің 122 және 123-баптарының императивті нормаларымен қатаң регламенттелген. Осы кезеңнің мән-жайын саралаған А.Н. Колычева цифрлық кеңістіктегі дәлелдеудің түп қазығы деп мынаны атайды: құбылмалы цифрлық іздердің тұтастығы мен өзгермейтіндігін сақтай отырып, оларды қатаң процестік-технологиялық тәртіппен тіркеп-белгілеу (фиксациялау) [125, 37-38 б.]. А.В. Кулаевский осы ойды әрі қарай өрбітеді әрі бір маңызды ескертпе жасайды: артефактіні жекелеп, статикалық күйде тіркеу – егер оның артынша атрибутивтік деңгейге шапшаң ұласпаса – практикалық құнынан айырылады; ал бұл деңгейдің мәні бөлшектелген желілік профильдерді тереңдете талдау арқылы қылмыскердің шынайы жеке басын динамикада анықтауда жатыр [153, 103 б.]. Ғылыми көзқарастардағы анықталған алшақтық гносеологиялық акценттердің қақтығысын көрсетеді: А.Н. Колычева іздің объективті нысанын сақтауға (объектінің статикасына) назар аударады, ал А.В. Кулаевский қол сұғушылық субъектісін танып-білуді (сәйкестендіру динамикасын) басты орынға қояды. Авторлық тәсілді негіздей отырып, аталған деңгейлердің бөлінбейтіндігін тұжырымдау қажет. Ғылыми-техникалық құралдарды (ҚР ҚПК-тің 126-бабы) пайдалана отырып, артефактілік деңгейде материалдық емес машиналық кодты алу атрибутивтік деңгей үшін жалғыз ғана мүмкін болатын дәлелдемелік базаны құрайды. Тек легитимді түрде тіркеп-белгіленген цифрлық із ғана нақты адамның кінәлілігін дәлелдеу туралы ҚР ҚПК-тің 113-бабының талаптарының орындалуын қамтамасыз ете отырып, анонимді виртуалды белсенділікті нақты физикалық субъектімен заңдық тұрғыдан байланыстыруға мүмкіндік береді.

Интегративті архитектураның аяқтаушы элементі ретінде жолын кесу деңгейі әрекет етеді. Тергеп-тексерудің телеологиялық мәнін зерттей отырып, Н.В. Поляков кез келген процестік әдістеменің тиімділігін тек бұзылған құқықтардың реституциясы (көлеңкелі капиталдарды заңды экономикаға қайтару басымдығы) тұрғысынан бағалауды ұсынады, бұл ретте криминалдық қызметті технологиялық бұғаттауды және шығарылған активтерді жедел қайтаруды қамтамасыз ететін тетіксіз сот ісін жүргізудің сыни аяқталмағандығын негізді түрде атап көрсетеді [154, 136 б.]. Назарды тергеудің ақпараттық-танымдық міндеттеріне шоғырландыратын алдыңғы авторлардан айырмашылығы, Н.В. Поляков фокусты құқық қалпына келтіру функциясына ауыстырады. Авторлық ұстаным осы тәсілмен толық ынтымақтасады: бөлінген электрондық мүлікті процестік бұғаттау (ҚР ҚПК-тің 161-бабы) және күдікті транзакцияларды тоқтата тұру тетігін қолдану («Қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл туралы» ҚРЗ-ның 11-бабы) модельдің мағыналық шыңы ретінде әрекет етеді. Жымқырылған қаражатқа іс жүзінде тыйым салмай субъектіні сәйкестендіру жәбірленуші тарап үшін барлық алдыңғы процестік тізбекті қолданудың нәтижелерін құнсыздандырады.

Демек, сотқа дейінгі тергеп-тексерудің ұсынылып отырған интегративті моделінің архитектурасы бес өзара байланысты деңгейден тұратын қатаң процестік иерархия болып табылады:

– превентивті деңгей – банктердің қауіпсіздік жүйелерімен цифрлық ортаға автоматтандырылған криминалистикалық мониторинг жүргізу;

– инициациялық деңгей – СДТБТ-да электрондық хабарларды (аномалияларды) жедел тіркеу;

– артефактілік деңгей – құбылмалы цифрлық іздердің криптографиялық тұтастығын қамтамасыз ете отырып, оларды процестік-технологиялық тіркеп-белгілеу;

– атрибутивтік деңгей – желілік профильдерді талдау негізінде қылмыскердің шынайы жеке басын динамикалық түрде анықтау;

– жолын кесу деңгейі – криминалдық қызметті технологиялық бұғаттау және шығарылған активтерге жедел тыйым салу.

Ұсынылып отырған сотқа дейінгі тергеп-тексерудің интегративті моделі сатылардың механикалық жиынтығы емес, тұрақты себеп-салдарлық байланыстары бар қатаң логикалық бірізділік болып табылады деп қорытындылау қажет. Превентивті, инициациялық, артефактілік, атрибутивтік және жолын кесу деңгейлерінің қатаң өзара шарттылығы мынадай қағиданы детерминациялайды: тым болмағанда бір элементті толыққанды іске асырудың мүмкін еместігі дәлелдеу жүйесін сөзсіз бұзады. Ерте анықтаудың болмауы инициацияны құнсыздандырады; алғашқы сағаттардағы метадеректерді тіркеп-белгілеу ақаулары заңдық атрибуцияны бұғаттайды; деанонимизацияның болмауы активтерді қайтаруды жоққа шығарады. Ұсынылған бес деңгейлі архитектура жедел-іздестіру, технологиялық және процестік қызмет арасындағы жасанды ведомстволық шекараларды жояды. Ол цифрлық іздердің

экстерриториялық табиғатына тұжырымдамалық тұрғыдан бағдарланған және желілік аномалияны анықтаған кезден бастап залалды іс жүзінде өтеуге дейін ажырамас технологиялық үздіксіздікті қамтамасыз ететін онлайн алаяқтықты сотқа дейінгі тергеп-тексерудің ғылыми негізделген жүйелі негізін қалыптастырады. Анықталған құрылымдық тұтастық осы модельдің қылмыстық қудалау органдарының практикалық қызметінде жұмыс істеуінің өзіндік алгоритмдері мен тактикалық тәсілдерін егжей-тегжейлі талдау қажеттілігін туындатады.

Бұған дейін ұсынылған интегративті модель архитектурасының тиімділігі сотқа дейінгі іс жүргізуге консервативті тәсілдерді түбегейлі қайта қарауды талап ететін оның жұмыс істеу тетігімен объективті түрде детерминацияланады. ҚР ҚПК-тің 118 және 122-баптарының ұйғарымдарына сүйенетін дәстүрлі қылмыстық процесс тарихи түрде физикалық күдіктіні іздестіру және кейіннен оның кінәсінің материалдық дәлелдемелерін жинау төңірегінде құрылады. Виртуалды кеңістік жағдайында бұл субъектіге орталықтандырылған логика кибержымқырулардың экстерриториялығымен толығымен параличке ұшырайды.

Осы дағдарысты еңсеру жолдарын талдай отырып, А.В. Кулаевский дәлелдеудің классикалық канондарынан толық бас тартпай, керісінше, дәстүрлі криминалистикалық ұсынымдарды цифрлық іздермен жұмыс істеуге бейімделген қатаң формализацияланған бірізді іс-әрекеттер жүйесіне (алгоритмге) түрлендіру арқылы құқық қолданушының қызметін қайта құрылымдау қажеттілігін негіздейді [153, 86 б.]. Осы тәсілге және бұған дейін негізделген артефактіге орталықтандырылған логикаға сүйене отырып, тергеп-тексеру тетігі қатаң процестік формула арқылы іске асырылуға тиіс: «цифрлық із → тіркеп-белгілеу → талдау → субъектіні анықтау → жолын кесу».

Мәлімделген артефактіге орталықтандырылған парадигманы іске асыру үшін орталық кедергі ретінде темпоральды фактор әрекет етеді. СДТБТ-де (ҚР ҚПК-тің 179-бабы) хабарлама тіркелгеннен кейін тергеу электрондық ортаның физикалық-ақпараттық қасиеттерімен бетпе-бет келеді. Осы қырды бажайлаған А.Н. Колычева уақыт өтісімен цифрлық іздердің жойылатынын, бұғатталатынын не орнынан ауысатынын, ал бұдан барып дәлелдемелік ақпараттың біржола ұшып кету қатері туындайтынын ескертеді – нәтижесінде іздерді заңды жолмен тіркеп-белгілеуге қалатын уақыт терезесі шектен тыс тарылады [126, 122 б.]. Осы шектеуден шығудың жолы ретінде сотқа дейінгі іс жүргізудің бастапқы сатысын – провайдерлер мен қаржы институттарынан дерек алу мерзімін – императивті түрде қысқартатын «72 сағат» алгоритмін енгізу негізделеді. Мұндай тәсіл цифрлық іздердің жойылуының алдын алу үшін ақпарат алмасу мерзімін 1-3 күнтізбелік күнмен (72 сағатпен) шектеуді ұсынатын қазіргі криминалистикалық ұсынымдармен толық үндеседі [111, 153 б.].

Мұнда IT-сарапшылар мен телекоммуникация мамандарының бір ескертпесін елеусіз қалдыруға болмайды: байланыс операторлары лог-файлдарды ұзақ мерзімге – 6 айдан 3 жылға дейін – сақтайды. Бірақ ұсынылып отырған «72 сағат» алгоритмі провайдерлердің статикалық базаларын нысанаға алмайды; ол ұзақ сақтауға көнбейтін, гиперқұбылмалы (volatile), уақытша

іздердің тез деградациялану циклін меңзейді.

Халықаралық форензика тәжірибесі мұны нақты мысалдармен растайды. Уақытша контенттің табиғатына сай кейбір сервистер (мәселен, Snapchat және өзгелері) жарияланған деректі 24 сағат ішінде серверден қайтарымсыз жояды [90, 165 б.]; ал мессенджерлерде автоматты жою таймері (self-destruct timer) қосылып қойса, деректі тек алғашқы сағаттарда ғана криптографиялық бекітіп үлгеруге болады. Оған қоса, перифериялық байланыс жабдығының (маршрутизаторлардың) жедел жадында (ОЗУ) және транзиттік желілік құрылғыларда ақпарат трафик көлеміне қарай бар болғаны бірнеше секундтан бірнеше сағатқа дейін ғана тұрады, ал құрылғы сөнген не қайта жүктелген сәтте үстінен жаңа дерек жазылып, әлгі із біржола өшеді [71, 72 б.]. Сонымен қатар, қылмыскердің нақты орналасқан жерін растайтын жергілікті бейнебақылау камераларындағы (кіреберіс және аула) архивтік бейнеақпараттың циклдік қайта жазылу мерзімі көбінесе небәрі 5 күнді құрайды, ал процестік жауаптарды күту 30 күнге дейін созылады [155, 94-95 б.].

Осы технологиялық шектеулерді ескере отырып, ұсынылып отырған алгоритмнің неліктен 24 немесе 48 сағатты емес, дәл 72 сағаттық дедлайнді құрайтынын өзге де жетекші криминалист-ғалымдардың зерттеулерімен негіздеу қажет.

Біріншіден, 24 сағаттық мерзімнің трансулттық сұрау салулар үшін мүлдем жарамсыздығы А.Н. Колычева мен И.М. Нурбековтың еңбектерімен дәлелденеді. А.Н. Колычева заңсыз әрекеттерді бекіту үшін ең алдымен абоненттің географиялық орналасуын (IP-мекенжайы арқылы) және аппараттық құралдарын міндетті түрде жедел орнату қажеттілігін алға тартады [126, 89 б.]. Ал И.М. Нурбеков халықаралық құқық қорғау ынтымақтастығында материалдарды адресаттарға берудің ұзақ мерзімділігін басты кедергі ретінде атайды. Шетелдік IT-корпорацияларға халықаралық сұрау салуларды аудару, ресімдеу, IP-мекенжайларды бұғаттау және орындау үшін 24 сағат физикалық әрі бюрократиялық тұрғыдан абсолютті түрде жеткіліксіз [136, 82 б.].

Екіншіден, 48 сағаттық стандартты мерзім цифрлық форензиканың (Digital forensics) ауқымды әрі күрделі техникалық талаптарына төтеп бере алмайды. Д.В. Завьялова өз диссертациясында қазіргі заманғы қылмыстық істер бойынша сарапшыларға 1,4 миллиард қағаз бетіне тең келетін ауқымды деректер массивтерін (мессенджерлер, әлеуметтік желілер) талдау қажеттілігін және құрылғыларда парольдердің болуы (оны бұзу жылдарға созылатындықтан) ақпараттық зерттеуді бұғаттайтын басты фактор екенін көрсетеді [90, 143-144 б.]. Бұған қоса, В.Е. Пономарев пен А.И. Зазулиннің зерттеулеріне сәйкес, ұшпа (энергияға тәуелді) ақпаратты алу үшін арнайы аппараттық бұғаттағыштарды (write-blockers) қолдану, ауқымды деректердің мінсіз побиттік көшірмесін жасау және олардың криптографиялық хэш-сомаларын есептеу [71, 151 б.], орасан зор уақытты (бірнеше айға дейін) талап етеді [114, 144 б.]. Осыған орай, 48 сағат ішінде құрылғылардың парольдерін бұзып, деректерді тұтастығын жоғалтпай толық көшіріп үлгеру технологиялық тұрғыдан мүмкін емес.

Осы ғылыми пайымдар мен нақтыланған фактілерді бір арнаға тоғыстырғанда 72 сағаттың мәні ашылады: бұл – екі шектің ортасындағы ғылыми

негізделген, әрі объективті түрде қажет «алтын аралық». Төменгі шегінде – халықаралық сұрау салулардағы ведомствоаралық кідірістерді еңсеруге және парольмен жабылған ауқымды деректердің побиттік көшірмесін түсіруге жететін ең аз уақыт; жоғарғы шегінде – ұшпа (volatile) цифрлық іздер біржола жойылып бітетін ең соңғы техникалық межес.

Бұл алгоритмді ҚР ІІМ мен ҚМА-ның ведомстволық нұсқаулықтарына енгізу ұсынылады, әрі нақ бір ескертпемен: ол ҚР ҚПК-тің 112-бабы бойынша дәлелдемені жол берілмейтін деп тануға негіз емес, міндетті тактикалық-криминалистикалық стандарт ретінде кіргізілуге тиіс. Оның міндеті – құбылмалы іздерді жедел криптографиялық бекітуге бағытталған, кезек күттірмейтін тергеу әрекеттерінің сөзсіз басымдығын бекіту. Ал осындай жедел іс жүргізуге заңды негіз беру үшін ҚР ҚПК-тің 131-бабының 4-бөлігіне бұрын негізделген толықтыруды сол күйінде сақтаған жөн: «трансұлттық ұйымдасқан топ (қылмыстық ұйым) құрамында киберқылмыстар жасады деген негізді күдік болған кезде, адам криптографиялық қорғалған цифрлық іздерді қашықтан жоюы немесе цифрлық активтерді жедел шығаруды жүзеге асыруы мүмкін деп пайымдауға жеткілікті деректер болғанда және бұл әрекеттердің жолын кесу кезек күттірмейтін жоғары технологиялық тергеу іс-шараларының кешенін жүргізуді талап еткенде».

Ұсынылып отырған алгоритм жалпы ереже бойынша 48 сағатты құрайтын адамды процестік ұстап алудың конституциялық мерзімдеріне (ҚР ҚПК-тің 131-бабының 4-бөлігі) қол сұқпайтынын атап өту маңызды. Оның басты мақсаты – адамды уақытша ұстау изоляторында физикалық ұстау үшін емес, ұшпа іздерді криптографиялық бекіту үшін қатаң процестік дедлайн белгілеу.

«72 сағат» алгоритмі шеңберінде талап етілетін жеделдікке қол жеткізу қылмыстық процесте технологияларды пайдалану шектері туралы ғылыми көзқарастардағы іргелі айырмашылықтарды айқындайды. К.А. Мира қазіргі заманғы тергеп-тексеру әрекеттерін дәстүрлі жүргізумен қатар, талдамалық толықтыру ретінде нейрондық желілерді (жасанды интеллектті) қолдануды талап етеді деп тұжырымдайды [61, 122-123 б.]. Осы тәсілді одан әрі тереңдете отырып, А.А. Рудых ақпараттық технологияларды криминалистикада тек қосалқы (техникалық-криминалистикалық) құрал ретінде қарастырудан бас тарту қажеттілігін алға тартады және олардың процестік дәлелдеудің өзіне органикалық түрде интеграциялануға міндетті екенін үзілді-кесілді дәлелдейді [60, 5 б.]. Осы ұстанымдарды салыстыру IT-құралдардың мәртебесін түсінудегі концептуалды айырмашылықты айқындайды: К.А. Мира оларды тергеушіні когнитивтік қолдауға арналған сыртқы қондырма ретінде қарастырса, ал А.А. Рудых олардың толық процестік сіңірілуін талап етеді. Анықталған алшақтықты шеше отырып, авторлық ұстанымды тұжырымдау қажет: интегративті модельдің жұмыс істеуі қатаң гибридті сипатта болуға тиіс. Процестік іс-шаралар (ҚР ҚПК-тің 244 және 245-баптары) мамандандырылған алгоритмдер тергеуге жай ғана көмектесіп қоймай, жымқырылған активтерді олар криптографиялық жасырылғанға дейін лездік процестік бұғаттаудың іргелі драйвері ретінде әрекет ететін қаржылық мониторингтің антифрод-жүйелерімен («Төлемдер және төлем жүйелері туралы» ҚРЗ-ның 25-1-бабы) ажырамас симбиозда іске асырылуға

міндетті.

Дәлелдеудің синхрондалған ішкі тетігі киберқылмыстылықтың сыртқы экстерриториялық архитектурасымен сөзсіз қақтығысқа түседі. Орталық инстанциялар арқылы ұзаққа созылатын дипломатиялық қарым-қатынастар арқылы іске асырылатын халықаралық құқықтық көмек көрсетудің дәстүрлі тәртібі (ҚР ҚПК-тің 559-бабы) виртуалды ортаның серпініне объективті түрде төтеп бере алмайды. Осы институционалдық тығырықты зерттей отырып, Д.В. Завьялова шетелдік құзыретті органдарға жіберілген консервативті сұрау салуларды орындау мерзімі (орта есеппен жарты жыл) цифрлық іздердің өте тұрақсыз табиғатына байланысты олардың өмір сүру кезеңінен апатты түрде асып түсетінін, сәйкесінше бұл терең рәсімдік асимметрия дәстүрлі тәсілді іс жүзінде мағынасыз ететінін негізді түрде тұжырымдайды [90, 155 б.]. Осы түйінге сүйене отырып, авторлық ұстаным халықаралық компонент факультативтік сатыдан тергеп-тексерудің шұғыл жедел құралына трансформациялануға міндетті екендігінде жатыр. Интегративті модель Компьютерлік қылмыстар туралы конвенцияның (2001 ж.) 29 және 35-баптарымен, сондай-ақ БҰҰ-ның Киберқылмысқа қарсы конвенциясының (2024 ж.) 25-бабымен регламенттелген тәулік бойғы желілер (24/7) мен электрондық деректердің сақталуын жедел қамтамасыз ету туралы шұғыл сұрау салулар тетіктерін тікелей қолдануды талап етеді. Трансшекаралық деректерді жедел өңдеудің сөзсіз басымдығы шетелдік серверлерде ақпаратты қасақана жою мүмкіндігін бұғаттайды.

Сотқа дейінгі тергеп-тексерудің интегративті моделінің жұмыс істеуінің әзірленген тетігінің ғылыми жаңалығы мынада жатыр. Біріншіден, ҚР ҚПК-тің 131-бабының 4-бөлігін толықтыру арқылы қылмыстық процесс құрылымына ұшпа дәлелдемелерді сақтаудың императивті хронологиялық сүзгісін (жеделдетілген ден қою алгоритмін) интеграциялау қажеттілігі негізделді. Екіншіден, қылмыстық-процестік әрекеттерді қаржылық антифрод-жүйелермен өтпелі гибридті синхрондау тетігін бекіту арқылы IT-технологиялардың рөлі туралы доктриналық қайшылық шешілді. Үшіншіден, физикалық тұлғаны іздестіруден цифрлық іздің бастапқылығын қамтамасыз ететін артефактіге орталықтандырылған логиканың баламасыздығы дәлелденді. Ұсынылған модельді іс жүзінде іске асыру онлайн алаяқтықтың трансұлттық табиғаты мен гипердинамикасына толық барабар процестік жауапты қалыптастырады. Гибридті алгоритмдерді легитимациялаудағы анықталған объективті қажеттілік қолданыстағы құқықтық өріске енгізілуге тиіс нақты заңнамалық дефиниялар мен қылмыстық-процестік новеллалар кешенін әзірлеу қажеттілігін туындатады.

Екінші тарау шеңберінде дәлелденгендей, ҚР қолданыстағы ҚПК-нің физикалық объектілерге (118-бап) және қағаз құжаттарға (120-бап) қатаң бағдарлануы виртуалды іздермен жұмыс істеу үшін институционалдық тосқауыл қалыптастырады. Бұл алшақтықты еңсеру дефиниялық өзгерістердің перманентті кешенін іске асыруды баламасыз түрде талап етеді.

Заңның тұжырымдамалық вакуумін талдай отырып, А.И. Зазулин бірыңғай мамандандырылған ұғымдық аппараттың болмауы виртуалды деректердің құқықтық белгісіздігін тудыратынын, бұл іс жүзінде ҚР ҚПК-тің 125-бабы

шеңберінде оларды бағалаудың шеттен тыс тұрақсыз және субъективті практикасын қалыптастыратынын негізді түрде атап көрсетеді [114, 6 б.]. Бұған дейін анықталған тұжырымдамалық проблемаға сүйене отырып, физикалық субстанциясы жоқ цифрлық объектілердің ерекше онтологиялық мәртебесін ескеріп, осы санатты дәстүрлі материалдық объектілерден тікелей нормативтік оқшаулау қажеттілігі туралы М.С. Бисалиевтің ұстанымын қолдау қажет [16, 45 б.]. Сонымен бірге П.С. Пастухов міндетті түрде машиналық декодтауға жататын жасырын дәлелдемелік ақпараттың ерекше құрылымдық жеткізгіші үшін дәлелдеменің дербес түрі ретіндегі «цифрлық заттай дәлелдеме» санатын енгізуді негіздей отырып, өзге терминологиялық ракурсты ұсынады [100, 528 б.].

Ұсынылған ғылыми ұстанымдарды салыстыру криминалистикалық фокус объектілеріндегі тұжырымдамалық айырмашылықты анықтауға мүмкіндік береді: егер М.С. Бисалиев назарды гносеологиялық нысанға (қылмыстық процестегі дәлелдеме мәртебесіне) аударса, онда П.С. Пастухов проблеманы онтологиялық мазмұн (машиналық кодтың физикалық-ақпараттық құрылымы) призмасы арқылы қарастырады. Осы айырмашылықты шеше отырып, авторлық ұстанымды тұжырымдау қажет: аталған тұжырымдамалар бәсекелеспейді, қайта екіденгейлі заңдық конструкцияны құрайды. Заң шығарушыға «цифрлық дәлелдеме» ұғымын макродеңгейлік процестік қабық (қатыстылық пен анықтық қасиеттеріне ие электрондық-цифрлық нысандағы ақпарат) ретінде, ал «цифрлық артефактіні» (желілік логтар, IP-мекенжайлар, хэш-сомалар) – ҚР ЦК-нің 21-бабында бекітілген «цифрлық жазбалар» заңды терминімен органикалық түрде корреляцияланатын микродеңгейлік жеткізгіш ретінде енгізу қажет. Мұндай синтез виртуалды іздерді классикалық құжаттармен мәжбүрлі түрде теңестірудің теріс практикасын түпкілікті жоюға мүмкіндік береді.

Ұсынылған тұжырымдаманы институционалдау үшін ҚР Қылмыстық-процестік кодексіне бір-бірімен байланысты бірнеше өзгеріс қатар енгізілуге тиіс. Әуелі ҚР ҚПК-тің 7-бабын мына мазмұндағы 59-тармақпен толықтырған жөн: «Электрондық (цифрлық) дәлелдемелер – ақпараттық жүйелерде, желілік ресурстарда, электрондық құрылғыларда цифрлық формада қалыптастырылған, сақталатын, өңделетін немесе берілетін, қылмыстық іс үшін мәні бар мән-жайларды белгілеу және тексеру үшін қолданылатын деректер (нәрселер)». Бұдан соң нақты деректердің заттай дәлелдемелермен бірге «электрондық (цифрлық) дәлелдемелермен» де белгіленетінін тікелей жазып, ҚР ҚПК-тің 112-бабының 2-бөлігін жаңа редакцияда беру керек. Соңында ҚР ҚПК-тің 118-бабының 1-бөлігіне 6-тармақ қосылып, ол цифрлық ақпаратты физикалық жеткізгішіне қарамастан дербес алып қою мен іске тіркеудің тәртібін бекітуге тиіс.

Бірақ ұғымдық аппаратты құрумен ғана шектелу – жеткіліксіз қадам. Цифрлық дәлелдememен жұмыстың нақты процестік рәсімдері (алу, сақтау, верификация) мен деректі бұрмалаудан қорғаудың заңнамалық кепілдіктері ҚР ҚПК нормаларынан тікелей орын табуы қажет. М.С. Бисалиев пен А.И. Зазулин негіздегендей, цифрлық ақпаратты дәстүрлі «заттай дәлелдемеге» теңеу оның алгоритмдік болмысын бұрмалайды, әрі физикалық объектінің жоқтығын дәлелдеменің жоқтығымен қате шатастыруға жетелейді [16, 45 б.; 114, 65 б.]. IT-

сарапшылардың қазіргі криминалистикалық талаптарын ескере отырып, цифрлық дәлелдемелердің авторлық тұжырымдамасында деректерді «жеделдетілген деградация» деңгейіне қарай екі іргелі санатқа жіктеу керек:

– қуатқа тәуелді, ұшпа деректер (volatile data): құрылғының жедел жадындағы (ОЗУ/RAM), кэштегі, файлдық подкачкалардағы және желілік қосылымдардағы ақпарат. В.Е. Пономарев пен А.И. Зазулин дәлелдегендей, мұндай дерек құрылғы қуат көзінен ажыраған сәтте лезде әрі қайтымсыз деградацияланып, толық жойылады [71, 45 б.; 114, 65 б.]. Осы санаттағы із дәлелдеме алудың ең қысқа «мүмкіндіктер терезесін» талап етеді;

– қуатқа тәуелсіз, тұрақты сақталатын деректер (non-volatile data): қатты дискілердегі (HDD, SSD), флэш-жинақтағыштардағы ақпарат [114, 90 б.]. Бұлардың деградациясы құрылғының пассивті тозуымен не қасақана өшірумен, салыстырмалы түрде баяу жүреді.

Осы технологиялық дихотомияны негізге ала отырып, ҚР ҚПК-нің 111-бабын «электрондық (цифрлық) дәлелдемелер» деген дербес дәлелдеме түрімен толықтыру, әрі ҚР ҚПК-нің 7-бабына мына нақтыланған авторлық анықтаманы енгізу ұсынылады: «Электрондық (цифрлық) дәлелдемелер – ақпараттық жүйелерде, желілік ресурстарда және құрылғыларда тұрақты (non-volatile) немесе энергияға тәуелді ұшпа (volatile) формада қалыптастырылған, сақталатын және өңделетін, қылмыстық іс үшін мәні бар мән-жайларды белгілеуге арналған деректер». Бұл виртуалды іздерді нақты физикалық «темірге» байлаудан бас тартуға және ұшпа деректерді деградацияға ұшырап жойылып кетпей тұрып жедел көшіріп алуға заңнамалық негіз береді.

Электрондық ақпараттың гиперқұбылмалылығын және виртуалды табиғатын ескере отырып, оны алу кезінде деректердің қашықтан жойылуын немесе өзгеруін болдырмау қатаң қамтамасыз етілуі тиіс. Ол үшін дәлелдемелерді жинау және сақтау тәртібіне келесідей заманауи криминалистикалық стандарттарды ҚР ҚПК нормаларына имплементациялау қажет:

Біріншіден, радиоэлектрондық оқшаулау. Мобильді құрылғылар мен электрондық ақпарат тасымалдағыштарды алу сатысында, олардың жадына қашықтан рұқсатсыз қол жеткізу және деректерді қашықтан жою (remote wipe) қаупін толығымен бейтараптандыру маңызды қадам болып саналады. А.А. Рудых, А.В. Маилян және Д.В. Завьялова сияқты криминалист-ғалымдардың зерттеулерінде дәйектелгендей, бұл мақсатта сыртқы радиоэлектрондық сигналдарды өткізбейтін арнайы жабдықтарды – «Фарадей қаптарын» (Faraday bags) міндетті түрде қолдану талап етіледі [60, 181-182 б.; 64, 149 б.; 90, 109 б.]. Сонымен қатар, маманның міндетті түрде қатысуымен құрылғыны желіден толық оқшаулау режиміне («авиарежимге») дереу ауыстыру немесе байланыс сигналдарын басатын арнайы техникалық құралдарды пайдалану қажеттілігін И.А. Орешков нақты негіздейді [34, 133-134 б.]. Аталған криминалистикалық әдістерді қолдану тергеу әрекетінің хаттамасында міндетті түрде тіркелуі тиіс, бұл алынатын цифрлық дәлелдемелердің тұтастығына және қылмыстық іс жүргізу барысындағы өзгермеушілігіне толық кепілдік береді.

Екіншіден, аппараттық бұғаттау (write-blocking) арқылы көшіру. Цифрлық

іздермен жұмыстың алтын қағидасы бір нәрсеге саяды: көшірме түсіру барысында бастапқы (түпнұсқа) тасымалдағышқа тіпті болмашы өзгеріс те енгізілмеуге тиіс. В.Е. Пономарев ғылыми негіздегендей, ақпараттың побиттік көшірмесін (имиджін) жасаған кезде түпнұсқа тасымалдағышқа кез келген модификацияны бөгейтін арнайы аппараттық-бағдарламалық құралдарды – жазба бұғаттағыштарын (write-blockers) – қолдану міндетті [71, 142-143 б.]. Мұндай құрылғылар деректі тек оқу режимінде ұстап, операциялық жүйенің метадеректерді өз бетінше өзгертуіне жол бермейді. Соның арқасында түпнұсқаның криминалистикалық тазалығы бұзылмайды, әрі сот талқысында оның жарамдылығына күмән тудыратын сылтау қалмайды.

Үшіншіден, түпнұсқалықты тексеру, метадеректерді қорғау және «сақтау тізбегі» (Chain of Custody) кепілдігін қамтамасыз ету мәселесі бар. Цифрлық дәлелдеменің тұтастығы мен аутентиктілігін халықаралық деңгейде мойындалған жалғыз криминалистикалық кепілі – оның криптографиялық хэш-сомасын есептеу. IT-сарапшылар мен криминалистердің талаптарына сай (АҚШ-тың FRE 902(14) ережесі, NIST стандарттары), әрі С.З. Шихалиева негіздегендей, цифрлық деректі бұрмалаудан қорғаудың кешенді IT-алгоритмі бірнеше технологиялық және процестік тетікті бір-бірімен ұштастыруы қажет [156, 102-103 б.].

Нақтырақ айтқанда, дәлелдемені алу және көшіру сатысында MD5, SHA-1, SHA-256 (Secure Hash Algorithm) не ГОСТ Р 34.11-2012 сынды сертификатталған хэш-алгоритмдерді пайдалану міндетті. Бұл алгоритмдер қандай көлемдегі деректі болсын тұрақты ұзындықтағы бірегей цифрлық «саусақ ізіне» түрлендіреді [157, 102-103 б.]; мұнда файлдағы бір ғана биттің (нөл не бір) өзгеруі бүкіл хэш-соманы түбегейлі өзгертіп жібереді [71, 134 б.].

Хэштеу тек негізгі файл контентіне ғана емес, оның метадеректеріне де – жасалу мен өзгертілу уақытына, файлдық жүйе атрибуттарына, операциялық жүйенің лог-файлдарына – қолданылуы шарт, өйткені метадеректерді бұрмалаудан қорғау цифрлық артефактінің ішкі құрылымының криминалистикалық тазалығын қамтамасыз етеді.

Мұнда халықаралық цифрлық форензика (digital forensics) тәжірибесінің бір аксиомасын ескерген жөн: дәлелдеменің заңдылығы оның «сақтау тізбегінің» (Chain of Custody) үзілмеуіне тікелей байланысты. Сол себепті ҚР ҚПК нормаларында цифрлық файлдың бастапқы көзден алынған сәтінен сотта бағаланғанға дейінгі бүкіл қозғалысын құжаттап әрі техникалық жағынан растап отыратын үздіксіз процесс регламенттелуге тиіс. Аталған «сақтау тізбегінің» мызғымастығын кепілдендіру және валидациялау үшін үлестірілген тізілімдер (блокчейн) технологиясын енгізу оңтайлы шешім болып табылады. Хэш-сомалар мен метадеректер туралы ақпарат әрбір келесі блок алдыңғы блоктың криптографиялық кодын және нақты уақыт белгісін (time-stamp) қамтитын жүйеге енгізілуі тиіс, бұл сақталған файлдарға кез келген кейінгі өзгерістерді білдірмей енгізу мүмкіндігін техникалық тұрғыдан толық жояды.

Жоғарыда мазмұндалған технологиялық және криминалистикалық кепілдіктерді ескере отырып, ҚР ҚПК-нің 112-бабын («Жол берілмейтін дәлелдемелер») мынадай нормамен толықтыру ұсынылады (бұл тәсіл М.Б.

Набатовтың қылмыстық-процестік заңнамаға қатысты ұқсас бастамасымен [155, 86 б.] және М.С. Бисалиевтің ҚР ҚПК 112-бабын цифрлық іздерге қолдану логикасымен [16, 100 б.] толық үндеседі):

«Цифрлық (электрондық) дәлелдемелер, егер түпнұсқа мен көшірменің бақылау криптографиялық хэш-сомаларында (SHA, MD немесе оларға теңестірілген алгоритмдер бойынша) алшақтықтар болса, іс жүргізу құжаттарында бастапқы хэш-сомасы бекітілмесе немесе олардың қозғалыс және сақтау тізбегінің (Chain of Custody) тұтастығы бұзылса, жол берілмейтін дәлелдемелер болып танылады».

Жаңа ұғымдық аппаратты заңдастыру терең рәсімдік новацияларға деген императивті қажеттілікпен ажырамас байланысты. ҚР ҚПК-тің 199 және 254-баптарымен регламенттелген және заттық объектілерді визуалды қабылдауға бағдарланған қарап-тексеру мен алудың дәстүрлі нысандары лездік қашықтан модификациялануға бейім деректерге мүлдем қолданылмайды. Осы тосқауылды зерттей отырып, А.Н. Колычева виртуалды іздерді алып қоюдың егжей-тегжейлі стандарттарының болмауы оларды дәлелдемелік базадан жаппай алып тастаудың бастапқы себебі ретінде әрекет ететінін тұжырымдайды [126, 106 б.]. Деректерді қорғау тетігін нақтылай отырып, А.А. Толыбаева бастаған авторлар ұжымы дәлелдемелердің қозғалыс тізбегінің (Chain of Custody) криптографиялық тұтастығын қамтамасыз ету үшін «Е-ҚІ» (Электрондық қылмыстық іс) жүйесіне интеграцияланған QR-кодтау (QR-маркировка) модулін енгізуге және метадеректер мен уақыт белгілерін (timestamp) міндетті түрде тіркеуге қатаң талаптар қоюдың баламасыз қажеттілігін дәлелдейді [98, 136 б.]. Рәсімге өзге көзқарас тұрғысынан С.В. Зуев келеді, ол жабдықты физикалық түрде алып қою мүмкіндігін объективті түрде жоққа шығаратын бөлінген бұлттық көздерге қашықтан қол жеткізуді (IT-тергеушінің цифрлық ортадағы қызметі аясында) регламенттеуге басымдық берілуге тиіс екенін әділетті түрде көрсетеді [157, 51 б.].

А.А. Толыбаева мен С.В. Зуевтің көзқарастарын салыстыру іздерді жинау тактикасындағы айқын қайшылықты көрсетеді: бірінші авторлар оқиға орнында физикалық құрылғымен жұмыс істеуді қатаң алгоритмдеуді талап етеді, ал екіншісі аппараттық бөлікпен байланыссыз ақпаратты экстерриториялық қашықтан алу қажеттілігін негіздейді. Авторлық тәсілді негіздей отырып, заң екі модельді де дербес тергеу әрекеттері түрінде инкорпорациялауға міндетті екенін мойындау қажет. Құрылғыны криптографиялық тіркеп-белгілеуді елемеу анықтықтың жоғалуына, ал бұлттық мұрағатты ала алмау қатыстылықтың жоғалуына алып келеді. Қашықтан және локальды тіркеп-белгілеудің мамандандырылған техникалық-құқықтық стандарттарын енгізу осал кодты даусыз заңдық фактіге трансформациялай отырып, ҚР ҚПК-тің 112-бабының (дәлелдемелерге жол берілмеуі) императивті тосқауылын еңсеруге мүмкіндік береді.

Тұжырымдамалық және рәсімдік новацияларды табысты іске асыру барабар институционалдық өзгерістерсіз үзілді-кесілді мүмкін емес. Сотқа дейінгі тергеп-тексерудің дәстүрлі ұйымдастырушылық моделі құқық қолданудың құзыретті субъектісінсіз күрделі алгоритмдерді іске асыруға қабілетсіз.

Криминологиялық талдауға сүйене отырып, К.О. Карабеков цифрлық деликтілерді тергеп-тексеру бойынша тар бейінді құрылымдық бөлімшелерді жаппай құру арқылы ішкі істер органдарын түбегейлі қайта құру қажеттілігін сенімді түрде дәлелдейді [17, 138 б.]. Өз кезегінде, Е.Р. Россинская цифрлық криминалистиканы үдетіп дамыту және тәуелсіз сот-сараптамалық сүйемелдеуді түбегейлі күшейту қажеттілігін негіздей отырып, акцентті ғылыми құрамдас бөлікке ауыстыруды ұсынады [158, 36 б.]. Ұстанымдардағы анықталған алшақтық кадрлық вакуумді еңсерудің әртүрлі жолдарын көрсетеді: К.О. Карабеков шешімді тергеу аппаратын ішкі ұйымдастырушылық қайта құрудан көреді, ал Е.Р. Россинская сыртқы сараптамалық қолдауды сапалы түрде күшейтуді талап етеді. Осы бағыттарды синтездей отырып, маманның (ҚР ҚПК-тің 80-бабы) және сарапшының (ҚР ҚПК-тің 274-бабы) процестік мәртебесі мамандандырылған кибербөлімшелердің қызметіне органикалық түрде интеграциялануға тиіс деген қорытынды жасауға болады. Бұл субъектілерге нақты уақыт режимінде деректердің шифрын ашудың аппараттық-бағдарламалық кешендерін кедергісіз қолдану үшін кеңейтілген процестік кепілдіктер беру қажет.

Қылмыстық-процестік заңнамадағы және институционалдық құрылымдағы ұсынылып отырған тұжырымдамалық новеллалар тәжірибелік қызметкерлер тарапынан абсолютті қолдауға ие. Сауалнамаға қатысқандардың 95%-ы ҚР ҚПК-де жаңа дербес тергеу әрекетін – «бөлінген желілерден және бұлтты қоймалардан компьютерлік ақпаратты алуды» заңнамалық бекіту идеясын жақтады (бұл ретте сауалнамаға қатысушылардың 65%-ы қолданыстағы алу және тінту нормаларының ескіргенін және виртуалды орта үшін мүлдем жарамайтынын ашық мойындады). Сонымен қатар, сараптама тағайындау кезінде дәлелдемелік маңызы бар сұрақтарды тұжырымдауда қиындық көретіндердің жоғары үлесі (70%) және заманауи технологиялармен жабдықталған мамандандырылған кибербөлімшелерді құруды сауалнамаға қатысушылардың 90%-ының қатаң талап етуі – біз бұрын негіздеген терең институционалдық дағдарыс пен құқық қолданушылардың «цифрлық нигилизмін» жеңу үшін кешенді құрылымдық реформалардың баламасыздығын объективті түрде дәлелдейді (Қосымша А).

Жүргізілген талдау нәтижелерін қорыта отырып, реформалау бағыттары қатаң, талдамалық және функционалдық тұрғыдан ажырамас: «дефиниция лар → рәсімдер → институттар» триадасын құрайды деп түйіндеу қажет. Қылмыстық қудалау тетігін жаңғырту олар қатаң синхронды түрде өзгертілген жағдайда ғана тұжырымдамалық тұрғыдан іске асырылуы мүмкін. Цифрлық артефакт санатын заңдастыру оны криптографиялық тіркеп-белгілеудің процестік рәсімінсіз заңдық мағынасынан айырылады, ал ең озық нормативтік рәсім құзыретті институционалдық субъектісіз өлі декларация күйінде қалады. Ұсынылған новациялар кешені сотқа дейінгі тергеп-тексеруді цифрлық ортаға толыққанды гносеологиялық бейімдеу үшін берік нормативтік базаны қалыптастырады. Бұл ретте қолданыстағы консервативті инфрақұрылым базасында осы құқықтық конструкцияларды толық ауқымда іске асырудың объективті қабілетсіздігі құқық қорғау жүйесін озық материалдық-техникалық және технологиялық қамтамасыз ету мәселелерін егжей-тегжейлі зерделеу қажеттілігін туындатады.

Алдыңғы зерттеу кезеңдерінде әзірленген сотқа дейінгі тергеп-тексерудің интегративті моделін іс жүзінде іске асыру тиісті институционалдық-технологиялық инфрақұрылымды қалыптастыру қажеттілігін объективті түрде туындатады. ҚР ҚПК-тің 118-бабында бекітілген заңнамалық конструкция тарихи түрде құқық қолданушыны сезілетін материалдық іздерді тіркеп-белгілеуге бағдарлайды, бұл кибержымқырулардың денесіз табиғатымен сыни қайшылыққа түседі. Релевантты мамандандырылған ортаның болмауы кез келген озық процестік новациялардың гносеологиялық әлеуетін сөзсіз жоққа шығарады, оларды жұмыс істемейтін құқықтық декларацияларға айналдырады. Ұсынылған процестік конструкцияның табысты жұмыс істеуі кадрлық, технологиялық және интеграциялық деңгейлерде жүйелі түрде көрініс табатын терең инфрақұрылымдық дағдарысты шешумен тікелей детерминацияланған.

Құрылатын инфрақұрылымның түп негізі – қылмыстық қудалау органдарының сапалы кадрлық трансформациясы. Дәстүрлі даярлықтың цифрлық ортаның сын-қатерлерінен артта қалғанын саралаған А.Д. Фокин мынадай тұжырымға келеді: классикалық заңгерлік білім цифрлық қоғам жағдайында тергеушіге киберқылмыстардың өзіндік іздік көрінісін дұрыс оқып-түсінуге тұжырымдамалық негіз бермейді, яғни қажеттілікті өтей алмайды [41, 161 б.]. Осы дағдарыстан шығу жолы төңірегінде ғылыми пікірталас өрбіген. Д.В. Завьялова экстенсивті бағытты жақтап, жұмыс істеп жүрген қызметкерлерді қашықтан оқытуға арналған мамандандырылған білім беру бағдарламалары мен қорғалған платформалар құруды ұсынады [90, 134-135 б.]. Е.Р. Россинская мұнымен келіспей, интенсивті құрылымдық қайта құруды алға тартады: мәселе біліктілікті жер-жерінен көтеруде емес, юриспруденция мен IT тоғысында орнықты пәнаралық құзыретті қалыптастыруда; онсыз тергеуші техникалық маманға тәуелді «номиналды тұлға» дәрежесіне дейін тайып кетеді [158, 36 б.]. Екі ұстанымды қатар қойғанда реформаның тереңдігіне қатысты айырма айқындалады: алғашқы автор қайта оқытудың сыртқы құралдарына арқа сүйесе, екіншісі тергеушінің түбегейлі жаңа кәсіби генотипін қалыптастыруды талап етеді. Біздің ойымызша, Е.Р. Россинскаяның объективті дұрыстығын мойындау қажет: құқық қорғау жүйесі деректер базасының архитектурасын, криптография алгоритмдерін және желілік трафикті маршруттауды дербес талдай алатын, өтпелі құзыреттерге (Law & IT) ие жаңа формациядағы тергеп-тексеру субъектілеріне мұқтаж.

Қалыптасқан кадрлық әлеует барабар техникалық қамтамасыз етуді объективті түрде талап етеді, бұл ғылыми-техникалық құралдарды қолдану туралы ҚР ҚПК-тің 126-бабының ұйғарымдарын қайта қарау қажеттілігін туындатады. Қазіргі жағдайда цифрлық технологиялар қосалқы құрал болудан қалады және дәлелдеудің іргелі құрылымдық базисіне айналады. Технологиялық даму векторларын зерттей отырып, А.А. Рудых техникалық қамтамасыз ету криминалдық белсенділікті анықтау тетігінің негізінің өзін құрайтынын әділетті түрде атап көрсетеді [60, 20 б.]. Идеяны дамыта отырып, П.С. Пастухов үлкен деректер массивтерін (Big Data) өңдеуге және жасанды интеллект элементтерін қолдануға мүмкіндік беретін кешенді цифрлық платформаларды енгізудің императивтілігін негіздейді [100, 527 б.]. Осы міндетті іске асыру үшін Р.Б.

Джилкишиевтің зерттеулерінде ұсынылған мамандандырылған бағдарламалық-аналитикалық кешенді (МБАК немесе СПАК) ұлттық тергеу практикасына енгізу орынды. Бұл кешен цифрлық дәлелдемелерді автоматты түрде жинауды, жасанды интеллект алгоритмдерін қолдана отырып ақпаратты аналитикалық өңдеуді және сараптамалық қорытындыларды автоматты түрде қалыптастыруды қамтамасыз етеді [57, 164 б.]. Талдауға өзге көзқарас тұрғысынан өтпелі интеграциялық шинаны және бірыңғай «Data Hub» құрмай кез келген талдамалық алгоритмдер оқшауланған фрагменттер күйінде қалатын қолданыстағы электрондық қылмыстық істің сыни шектеулеріне назар аударатын А.А. Толыбаева басқарған авторлар ұжымы келеді [98, 126 б.]. Ғылыми акценттердегі анықталған алшақтық абстрактілі талдамалық әлеует (П.С. Пастуховтың ұстанымы) пен прагматикалық архитектуралық тапшылық (А.А. Толыбаеваның ұстанымы) арасындағы қақтығысты көрсетеді. Авторлық тәсілді негіздеу қажет деп пайымдау негізді болып табылады: ақпаратты агрегациялаудың платформалық моделіне баламасыз көшу бірыңғай ведомстволық деректер шинасын құруға негізделуге тиіс. Тек осындай архитектура ғана ҚР ҚПК-тің 273-бабы тәртібімен сараптамалық зерттеу жүргізгенге дейін олардың процестік сақталуын және криминалистикалық тұтастығын кепілдендіре отырып, артефактілерді алу және олардың шифрын ашу процестерін автоматтандырады.

Сотқа дейінгі тергеп-тексеру сатысында осындай инновациялық технологияларды (блокчейн-аналитика, Big Data) кешенді қолдану бүгінгі таңда қоғамның қылмысқа қарсы қауіпсіздігін қамтамасыз етудің базалық элементі ретінде әрекет етеді. Жоғары технологиялық тергеу платформасының жұмыс істеуі сенімді секторараралық интеграциялық тетіктерді құрмай физикалық тұрғыдан мүмкін емес, өйткені ҚР ҚК-нің 190-бабы бойынша тергеп-тексеру айқын көрініс тапқан бөлінген сипатқа ие. Өзара іс-қимыл проблемасын саралаған С.М. Голятина мемлекеттік органдардың қатаң құрылымдалған, бірыңғай цифрлық ортасын құруды талап етеді әрі оған банк секторы мен телекоммуникациялық компаниялардың нақты уақыт режимінде міндетті түрде қосылуын шарт етіп қояды [111, 23-27 б.]. Осы орталықтандырылған тәсілге А.С. Камко өзге баламаны қарсы қояды: ол ұзаққа созылатын бюрократиялық рәсімдерді айналып өтіп, деректі жедел алуға жол ашатын, трансұлттық цифрлық алаңдармен құрылатын мемлекеттік-жекешелік әріптестіктің икемді алгоритмдері тиімдірек екенін дәлелдейді [36, 127 б.]. Екі көзқарасты қатар қойғанда интеграция тетігіндегі қағидатты айырма көрінеді: біріншісінде – мемлекет ішіндегі орталықтандырылған бақылау, екіншісінде – орталықсыздандырылған әріптестік. Екі тәсілді де «Төлемдер және төлем жүйелері туралы» ҚРЗ-ның 25-1-бабы призмасы арқылы интеграциялау қажет. Оңтайлы модель ретінде алаяқтық транзакциялар туралы мәліметтерді шоғырландыру үшін тергеу органдарына тікелей шлюз ұсына отырып, Ұлттық Банктің Антифрод-орталығының функционалын дамыту әрекет етеді. Бұл оқшауланған тергеу аппаратының бөлінген қаржылық базаларға легитимді және лездік қол жеткізуін қамтамасыз етеді.

Инфрақұрылымдық шектеулерді зерттеу нәтижелерін қорыта отырып,

«кадрлар → технологиялар → өзара іс-қимыл» қатаң, ажырамас себеп-салдарлық триадасының қалыптасқанын тұжырымдау қажет. Басқаларынан оқшау тек бір элементті ғана дамыту бүкіл цифрлық дәлелдеу тетігінің сөзсіз күйреуіне әкелетін институционалдық теңгерімсіздікті туындатады. Оларды легитимді түрде қолдана алатын IT-тергеушілер болмаған жағдайда озық криминалистикалық бағдарламалардың болуы мүлдем мәнсіз, ал білікті кадрлар банк жүйелеріне лездік интеграциялық қолжетімділіксіз параличке ұшырайды. Синхрондалған инфрақұрылымдық жаңғырту ұсынылған теориялық конструкцияны сот төрелігінің пәрменді құралына трансформациялаудың жалғыз объективті шарты ретінде әрекет етеді. Интегративті модель тиімділігінің институционалдық қамтамасыз ету деңгейіне анықталған тікелей тәуелділігі прогностикалық талдаудың: әзірленген тетіктің қолданылу шектерін және оның қылмыстық сот ісін жүргізу нәтижелілігіне әсер ету дәрежесін объективті бағалаудың қажеттілігін туындатады.

Онлайн алаяқтықты сотқа дейінгі тергеп-тексерудің ұсынылып отырған интегративті моделінің тиімділігін прогностикалық бағалау құқық қолданудың жүйелі коллизиялары мен әзірленген компенсаторлық процестік тетіктерін сыни салыстыруға объективті түрде негізделеді. Қолданыстағы консервативті дәлелдеу тетігі экстерриториялық виртуалды ортада істің мән-жайларын жан-жақты, толық және объективті зерттеуді (ҚР ҚПК-тің 24-бабы) тұжырымдамалық түрде қамтамасыз етуге қабілетсіз екені анықталды. Осы дағдарысты еңсеру жолдарын бағалай отырып, А.А. Толыбаева бастаған авторлар ұжымы қалыптасқан тергеу тығырығын шешу сот ісін жүргізудің кешенді интеграцияланған модельдерін енгізу арқылы түйінді институционалдық деформацияларды жоюды талап ететінін дәлелдейді [98, 127 б.]. Бұл құрылымдық-институционалдық тәсілмен П.С. Пастухов тұжырымдамалық пікірталасқа түсіп, экономикалық-технологиялық өлшемшартты негіздейді: кез келген жаңа процестік модельдің тиімділігі тек оның дәлелдеудің транзакциялық шығындарын барынша азайту және тергеп-тексеру субъектілері арасындағы үздіксіз ақпараттық байланысты қамтамасыз ету қабілеті арқылы ғана бағалануға тиіс [100, 527 б.]. Келтірілген пікірлерді талдау бағалау өлшемшарттарындағы айырмашылықты көрсетеді: бірінші авторлар тобы процесті архитектуралық қайта құрылымдауға назар аударады, ал екінші автор операциялық тиімділік пен IT-байланыстылыққа шоғырланады. Біздің ойымызша, ұсынылған интегративті модель екі тәсілді де органикалық түрде синтездейді. Архитектуралық қайта құрылымдау легитимді каркас жасайды, ал технологиялық байланыстылық қылмыстық қудалаудың нәтижелілігін бұғаттайтын іргелі деформацияларды мақсатты түрде жоя отырып, процестік шығындарды барынша азайтады.

Әзірленген архитектураны іс жүзінде енгізу күтілетін жүйелі эффектілер каскадын қалыптастыра отырып, қылмыстық-процестік заңның түйінді институттарына тікелей проекцияланады. Осы эффектілерді талдай отырып, К.О. Карабеков тек іздерді өте ерте автоматтандырылған тіркеп-белгілеу есебінен ғана қол жеткізілетін кибержымқырулар латенттілігінің сыни деңгейін басымдықпен төмендетуді негізді түрде атап көрсетеді, бұл азаматтық-құқықтық даудың болуы желеуімен өтініштерді тіркеуден негізсіз бас тартудың зиянды практикасын

жоққа шығарады [17, 152 б.]. Өз кезегінде, А.В. Кулаевский субъектінің анықталмауына байланысты іс жүргізу мерзімдерінің жүйелі түрде үзілуін жоққа шығаратын артефактіге орталықтандырылған тәсілмен анықталған адамдар үлесінің еселеп артуы тікелей детерминацияланғанына назар аудара отырып, фокусты тергеу динамикасына ауыстырады [153, 111-112 б.]. Қағидатты түрде өзге телеологиялық ұстанымдар тұрғысынан В.В. Поляков келеді, ол әдістеменің нәтижелілігін тек реституция призмасы арқылы ғана бағалауды ұсынады: процестік әрекеттерді синхрондау материалдық залалдың іс жүзінде өтелуіне кепілдік бере отырып, бөлінген электрондық мүлікке уақтылы тыйым салуды қамтамасыз етеді [154, 83 б.]. Ұсынылған ғылыми көзқарастарды салыстыру мақсатты басымдықтардың айқын дифференциациясын көрсетеді: латенттілік превенциясы (К.О. Карабеков), процестік атрибуция (А.В. Кулаевский) және материалдық өтемақы (В.В. Поляков). Авторлық тәсілді негіздей отырып, мынаны тұжырымдау қажет: бұл метрикалар бәсекелеспейді, керісінше терең синергетикалық эффектіге ие. Озып әрекет ететін ерте тіркеп-белгілеу жасырын субъектінің атрибуциясын гносеологиялық тұрғыдан мүмкін етеді, ол өз кезегінде бүкіл сотқа дейінгі іс жүргізудің жалпы нәтижелілігін өзара күшейте отырып, активтерді шығарудың технологиялық жолын кесу үшін легитимді базаны қамтамасыз етеді.

Сипатталған синергияға қол жеткізу толығымен модельдің электрондық ортаның гиперқұбылмалы табиғаты мен тарихи түрде сезілетін физикалық объектілердің (ҚР ҚПК-тің 118-бабы) төңірегінде құрылған архаикалық материалдық бағдарланған процестік нысан арасындағы іргелі алшақтықты жою қабілетіне негізделеді. А.И. Зазулин тұжырымдағандай, ақпараттық технологияларды терең интеграциялау статикалық қағаз жүйесінен криминалдық ортаның сын-қатерлеріне барабар ден қоюға қабілетті тергеп-тексерудің икемді және бейімделгіш моделіне институционалдық көшуді қамтамасыз етеді [114, 56 б.]. Осы тезисті дамыта отырып, Головин А.Ю. мен В.О. Давыдов дәл осы қол жеткізілетін процестік бейімделгіштік желілік анонимділік жағдайында дәлелдемелік базаның сапасын түбегейлі арттыру үшін баламасыз шартты қалыптастыратынын атап көрсетеді [159, 31-32 б.]. Ғалымдардың пікірлерін заң ұйғарымдарымен синтездей отырып, мынадай қорытынды жасау қажет: ұсынылған конструкцияның икемділігі алынған электрондық деректерді ҚР ҚПК-тің 112-бабында көзделген таза формальды негіздер бойынша жол берілмейтін дәлелдемелер деп танудың процестік тәуекелдерін сыни түрде барынша азайта отырып, виртуалды ақпаратпен жұмыс істеу үшін мінсіз құқықтық жағдайлар жасайды.

Жүргізілген кешенді зерттеу нәтижелерін қорыту оның үш өзара байланысты ережеде тұжырымдамаланатын ғылыми жаңалығын нақты құрылымдауға мүмкіндік береді: Біріншіден, превентивті, инициациялық, процестік және жолын кесу ден қою тетіктерін органикалық және ажырамас түрде біріктіретін онлайн алаяқтықты сотқа дейінгі тергеп-тексерудің көпдеңгейлі интегративті моделі әзірленді. Екіншіден, артефактіге орталықтандырылған тәсілде – классикалық іздестіру әдістерінен цифрлық іздердің сөзсіз басымдығы мен гносеологиялық бастапқылығын тануда

тұжырымдамалық түрде құрылған жаңа процестік парадигма ғылыми негізделді. Үшіншіден, құбылмалы артефактілердің бастапқы ақпараттық сақталуын қамтамасыз етудің түйінді процестік элементі ретінде әрекет ететін жеделдетілген ден қою алгоритмі шығарылды және дәлелдеу құрылымына интеграцияланды.

Баяндалғанды түйіндей отырып, ағымдағы тараудың қорытынды бағдарламалық түйінін тұжырымдау қажет: әзірленген интегративті модель сотқа дейінгі тергеп-тексеруді ауқымды жаңғырту үшін берік, ғылыми негізделген жүйелі базаны қалыптастырады. Ол жаһандық цифрландырудың сын-қатерлеріне толық барабар қылмыстық-процестік реттеу тиімділігінің сапалы өсуін қамтамасыз етеді. Сонымен бірге, ұсынылған артефактіге орталықтандырылған парадигманы толыққанды құқық қолдануда іске асыру оқшауланған ұлттық контурда объективті түрде мүмкін емес. Бөлінген қашықтықтан қаржылық айналым мен криптографиялық іздердің трансшекаралық, экстерриториялық табиғаты мемлекетаралық ынтымақтастықтың консервативті алгоритмдерін түбегейлі қайта қарауды талап етеді. Шетелдік цифрлық платформаларға анықталған технологиялық тәуелділік халықаралық ведомствоаралық өзара іс-қимылдың қағидатты түрде жаңа, орталықсыздандырылған тетіктерін дербес, тереңдетіп талдау қажеттілігін туындатады.

3.2 Онлайн алаяқтық қылмыстарын сотқа дейінгі тергеп-тексеруде халықаралық тәжірибе мен цифрлық технологияларды интеграциялау

Ұлттық заңнаманы жаңғыртудың логикалық жалғасы ретінде экстерриториялық кибержымқыруларды тергеп-тексеру кезінде құқық қорғау жүйесінің институционалдық оқшауланууын еңсеру қажеттілігі әрекет етеді. Тек мемлекетішілік шекараларда тұйықталған құқық қолдану моделі цифрлық қылмыстылықтың трансұлттық және бөлінген архитектурасының алдында тұжырымдамалық тұрғыдан дәрменсіз.

Трансұлттық юрисдикциялық оқшауланууды еңсерудің объективті қажеттілігі озық шетелдік тәжірибені терең талдауды талап етеді. Әлемдік құқық қолдану практикасы көрсетіп отырғандай, киберқылмыстылық бөлінген желілік архитектураға және анонимизациялау әдістеріне сүйенеді, бұл аумақтық тергеп-тексерудің және дипломатиялық құқықтық көмектің классикалық тетіктерін сыни тұрғыдан осал әрі архаикалық етеді [160, 118 б.]. Қазіргі заманғы қылмыстық сот ісін жүргізу іздерді локальды тіркеп-белгілеуден экстерриториялық алгоритмдік құдалауға көшуге міндетті. Тиісінше, онлайн алаяқтыққа қарсы іс-қимылдың ұлттық гибридті моделін құрастыру шетелдік IT-корпорациялардың деректеріне тікелей қол жеткізуді және қаржы секторын тергеу процесіне интеграциялауды қамтамасыз ететін халықаралық нормативтік конструкцияларды имплементациялаусыз мүмкін емес.

Антикриминалдық инфрақұрылым құрудың халықаралық тәжірибесіне үңілген А.Л. Осипенко бастапқы модель ретінде орталықтандырылған талдамалық жүйелерді бөліп көрсетеді; олардың негізгі жұмысы желілік

қатерлер жайлы макродеректі енжар жинауға және қаржы реттеушілерінің статистикалық базаларын құруға саяды [150, 109-110 б.]. Д.В. Завьялова бұған қарсы уәж айтады: ауыр, орталықтандырылған құрылымдар тиімділігін объективті түрде жоғалтты, ал олардың орнын шабуылдың жолын белсенді кесіп, жедел деанонимизация жүргізуге қауқарлы икемді ведомствоаралық платформалар мен тар бейінді бөлімшелер басуға тиіс. Екі ұстанымды салғастырғанда функцияны бағалаудағы айырма ашылады: А.Л. Осипенко енжар талдамалық бақылауды бірінші орынға қойса, Д.В. Завьялова проактивті, орталықсыздандырылған ден қоюды басым санайды [90, 155-156 б.]. Біздің ойымызша, классикалық юрисдикциялық тосқауылдардан тыс деректермен шұғыл трансшекаралық алмасуды қамтамасыз ететін өзара іс-қимылдың жаһандық желілерінің (24/7 форматындағы) жұмыс істеуінде өзінің жоғары көрінісін табатын желілік тәсілдің баламасыздығын мойындау қажет. Интеграцияның бұл векторы халықаралық құқықтың императивті нормаларында, атап айтқанда Компьютерлік қылмыстар туралы конвенцияның (2001 ж.) 35-бабында және БҰҰ-ның Киберқылмыстылыққа қарсы перспективалық конвенциясының (2025 ж.) 41-бабында тікелей бекітілген.

Будапешт конвенциясының ережелерін, оның ішінде деректерге трансшекаралық қол жеткізу тетіктерін ҚР ұлттық заңнамасына терең имплементациялау тергеп-тексерулердің тиімділігін арттыру үшін айтарлықтай әлеуетке ие [161, 90 б.]. Желілік халықаралық модельдердің анықталған басымдығы барабар жоғары технологиялық мемлекетішілік іргетастың болуын объективті түрде талап етеді. Тергеу аппараты банктік ақпаратқа тікелей қол жеткізуден айырылған және консервативті қағаз сұрау салуларды іске асыруға мәжбүр болатын дәстүрлі жүйе цифрлық іздердің қайтымсыз жоғалуына және жымқырылған активтердің шығарылуына фатальды түрде әкелетін сыни процестік кешігуді туындатады. Осы инфрақұрылымдық алшақтықты еңсеру жолдарын бағалай отырып, А.А. Толыбаева бастаған авторлар ұжымы қашықтықтан жымқыруларды анықтаудың тиімділігі тек қаржы институттары мен қылмыстық қудалау органдарының жіксіз технологиялық интеграциясы жағдайында ғана түбегейлі артатынын дәлелдейді [98, 138 б.]. Процесс механикасына өзге көзқарас тұрғысынан фокусты жалпы институционалдық архитектурадан нақты технологиялық инструментарийге ауыстыратын С.М. Голятина келеді: табысты тергеп-тексерудің іргетасы ретінде нақты уақыт режимінде (real-time) банктік базалармен ажырамас байланыста желілік аномалияларды мониторингтеудің автоматтандырылған жүйелерін қолдану әрекет етеді [111, 106 б.]. Өз кезегінде, Д.О. Буйнов ақпаратпен мемлекетаралық алмасу үшін крипто-транзакцияларды қадағалаудың озық талдамалық құралдарын міндетті түрде пайдалануды және қорғалған криптографиялық хаттамаларды енгізуді талап ете отырып, бұл технологиялық талапты күрделендіреді [162, 136 б.]. Келтірілген пікірлерді талдау проблеманың көпдеңгейлілігін көрсетеді: макроинтеграциядан (А.А. Толыбаева) операциялық мониторингке (С.М. Голятина) және криптографиялық қорғауға (Д.О. Буйнов) дейін. Біздің ойымызша, бұл тәсілдерді синтездеу қажет: жоғары нәтижелілікке қаржы секторының технологиялық сүзгілері мен халықаралық алмасудың

стандартталған хаттамалары (БҰҰ-ның Киберқылмысқа қарсы конвенциясының 40-бабына сәйкес) дәлелдемелерді жинаудың процестік тетігімен ажырамас байланыста болған кезде ғана объективті түрде қол жеткізіледі.

Талданған ұлтүстілік тәжірибе мен доктриналық көзқарастардың синтезі онлайн алаяқтыққа қарсы іс-қимылдың гибридті моделінің негізделген авторлық тұжырымдамасын қалыптастыруға мүмкіндік береді. Оқшауланған антифрод-орталықтар, жаһандық құқық қорғау желілері немесе мамандандырылған кибербөлімшелер болсын, қарастырылған институционалдық конструкциялардың ешқайсысы таза күйінде қылмыстық қудалаудың абсолютті тиімділігіне кепілдік бере алмайтыны анықталды. Банк құрылымдарының технологиялық алгоритмдері ҚР ҚПК-тің 122-бабымен регламенттелген алынатын цифрлық іздерді легитимациялаудың қатаң рәсімінсіз таза превентивті құрал күйінде қалады. Сонымен бір уақытта экстерриториялық құқық қорғау желілерінің жұмыс істеуі синхрондалған мемлекетішілік үйлестіру мен аппараттың дайындығы болмаған кезде толығымен параличке ұшырайды. Демек, әзірленген гибридті модель озық цифрлық қадағалау практикаларын, мемлекеттік және жекеше секторлардың қатаң институционалдық үйлестіруін органикалық түрде интеграциялауға, сондай-ақ ұлттық қылмыстық-процестік реттеудің ерекшелігін императивті түрде ескеруге міндетті.

Баяндалғанды түйіндей отырып, қорытынды тұжырымдамалық түйін жасау қажет: онлайн алаяқтықты сотқа дейінгі тергеп-тексерудің нәтижелілігі технологиялық, қаржылық және халықаралық құқық қорғау ресурстарының жүйелі интеграциялану дәрежесімен тікелей математикалық және процестік корреляцияда болады. Озық тәжірибе тек автоматтандырылған, орталықсыздандырылған деректер алмасуды және икемді институционалдық құрылымдарды енгізген кезде ғана киберқылмыстардың ашылуын еселеп арттыру мүмкіндігін сөзсіз растайды. Процестік табыстың жүйенің аппараттық-бағдарламалық жарақтандырылуына анықталған объективті тәуелділігі қазіргі заманғы тергеу практикасында қолданылатын нақты цифрлық технологияларды, шифрды ашудың криминалистикалық алгоритмдерін және мамандандырылған бағдарламалық кешендерді пәндік талдау қажеттілігін туындатады.

Онлайн алаяқтықтарды (ҚР ҚК-нің 190-бабы) жасау ортасын ауқымды цифрландыру қылмыстық сот ісін жүргізудің дәстүрлі матрицасының гносеологиялық дәрменсіздігін айқындайды. ҚР ҚПК-тің 118-бабында тарихи бекітілген құқық қолданушының материалдық түрде тіркеп-белгіленген іздерді іздестіруге бағдарлануы виртуалды дәлелдемелердің денесіз табиғатымен еңсерілмейтін қақтығысқа түседі. Осы дағдарысты талдай отырып, А.С. Шаталов бүгінгі таңда онлайн алаяқтықты ашудың тиімділігі жоғары технологиялық ақпараттық жүйелерді қолданумен қатаң детерминацияланғанын тұжырымдайды [163, 10 б.]. Технологиялық императивті дамыта отырып, А.А. Рудых инновациялардың мәртебесін қайта қарауға деген объективті қажеттілікті негіздейді: цифрлық құралдар қосалқы криминалистикалық техниканың архаикалық рөлін жоғалтуға және бүкіл дәлелдеу тетігінің іргелі өзегіне айналуға тиіс [60, 217 б.]. Бұл пікірлер доктриналық бағадағы алшақтықты аңғартады: алғашқы автор процестің сыртқы технологиялық тәуелділігін атап көрсетсе,

екіншісі дәлелдеу құралдары жүйесінде IT-құралдардың мәртебесін ішкі, тұжырымдамалық деңгейде қайта қарауды талап етеді. Біздіңше, бұл тұста А.А. Рудыхтың ұстанымы дұрыс: ғылыми-техникалық құралдарды қолдану тәртібі (ҚР ҚПК-тің 126-бабы) процестік жағынан қайта қаралуға тиіс. Технологиялар заңдық маңызы бар ақпаратты алудағы басты жүкті өз мойнына алады, әрі дәлелдемені бағалауды (ҚР ҚПК-тің 125-бабы) субъективті ықтимал болжамдар аясынан нақты аппараттық-бағдарламалық есептеулер жазықтығына көшіреді.

Дәлелдеу тетігін трансформациялау бөлінген криминалдық желілерді деанонимизациялау үшін қолданылатын цифрлық инструментарийді функционалдық жүйелеуді талап етеді. Сыртқы барлау құралдарын зерттей отырып, Д.В. Завьялова шашыраңқы желілік артефактыларды агрегациялауды автоматтандыратын ашық көздерді талдау (OSINT) жүйелерінің басым рөлін бөліп көрсетеді. Автор Maltego, Intelligence X және Recon-ng сияқты мамандандырылған бағдарламалық құралдарды қолдануды ұсынады, бұл іздеуді толық автоматтандыруға және уақытты едәуір үнемдеуге мүмкіндік береді [90, 92 б.]. Сыртқы мониторингпен тұжырымдамалық пікірталасқа терминалдық құрылғылардан алынатын латентті іздерді легитимациялауға мүмкіндік беретін терең ішкі талдау құралдарының: компьютерлік форензика мен криптографиялық трейсингтің сыни құндылығын дәлелдейтін К.А. Мира түседі [61, 112 б.]. Әдістер палитрасын толықтыра отырып, Д.В. Бахтеев адамның қабылдауына қолжетімсіз Big Data массивтеріндегі жасырын корреляцияларды анықтау үшін жасанды интеллект жүйелерін қолдануды негіздей отырып, акцентті когнитивтік деңгейге ауыстырады [133, 352 б.].

Ұстанымдарды салыстыру технологиялық фокусты оқшаулаудағы айырмашылықты айқындайды: сыртқы деректер бойынша барлау (Д.В. Завьялова), жасырын іздерді тереңінен алу (К.А. Мира) және массивті талдамалық сүзгілеу (Д.В. Бахтеев). Авторлық тәсілді негіздей отырып, бұл функцияларды процестік өріс шеңберінде синтездеу қажет. Биллингтік деректерді оқшауланған талдау (ҚР ҚПК-тің 244-бабы) немесе ақпаратты жасырын алу (ҚР ҚПК-тің 245-бабы) өздерін сарп етті. Тек нейрожелілік сүзгілерді кешенді қолдану ғана анонимді аватар мен нақты физикалық субъект арасындағы байланысты белгілеудің мінсіз алгоритмдік дәлдігіне кепілдік бере отырып, тергеудің құқық қолданушының психофизиологиялық шектеулеріне тәуелділігін түбегейлі төмендетеді.

Жоғары технологиялық аналитика қылмыскерді сәйкестендіруді қамтамасыз етіп қана қоймайды, сонымен қатар тергеп-тексеруді АҚШ Федералдық тергеу бюросы «Level Up» операциясы шеңберінде іске асырғанындай проактивті фазаға ауыстыра отырып, жәбірленушінің мәртебесін түбегейлі трансформациялайды. Бұл стратегияның тетігі латентті жәбірленушілерді предиктивті түрде анықтау үшін Интернет-қылмыстарға шағымдарды қабылдау орталығы (IC3) арқылы шағымдар массивтерін агрегациялауда және криптовалюталық транзакциялар ағындарын (Financial Fraud Kill Chain) қадағалауда жатыр [164]. Тергеп-тексеру процесі инверсияланады: Федералды тергеу бюросының мамандандырылған кибербөлімшелері автоматтандырылған алгоритмдердің (транзакциялар

хэштерін және криптовалюталық әмияндардың мекенжайларын талдау) көмегімен алаяқтық инвестициялық схемаларға (pig butchering) тартылған азаматтарды сәйкестендіреді және жәбірленушілер жымқыру фактісін сезініп, сыни активтерінен айырылғанға дейін ресми полициялық хабарламаны инициациялайды. Мұндай тәсілдің заңдық маңызы бастапқы цифрлық дәлелдемелерді жинау және қаскөйлердің коммуникация іздерін тіркеп-белгілеу қылмыстық пиғылдың ерте сатысында (транзакциялар аяқталғанға дейін) жүзеге асырылатындығында, ал банк секторымен үйлестіру көпмиллионды сомаларды шұғыл бұғаттауға мүмкіндік беретіндігінде көрініс табады. Бұл тәжірибе кибержымқыруларға табысты қарсы іс-қимыл жасау үшін ұлттық тергеу әдістемесі желілік трафик аномалияларын мониторингтеу негізіндегі превентивті цифрлық сәйкестендіру және жәбірленушілерді проактивті іздестіру алгоритмдерімен толықтырылуға тиіс екенін дәлелдейді.

Алайда ең озық инструментарийді оқшауланған түрде қолдану өткір әдіснамалық коллизияны – дәлелдемелік тізбекті бұзатын құқық қолданудың фрагменттілігін туындатады. Осы осалдықты бағалай отырып, С.М. Голятина тергеу, банк секторы және провайдерлер арасындағы перманентті интеграциялық байланыстың болмауы деректерді тексеру сатысында тергеп-тексеруді бұғаттайтын сыни ақпараттық алшақтықтарды жасайтынын әділетті түрде тұжырымдайды [111, 106 б.]. Осы инфрақұрылымдық параличті еңсеру үшін П.С. Пастухов процестік шешімдер мен электрондық құжат айналымының жіксіз синхрондалуын қамтамасыз етуге қабілетті бірыңғай ақпараттық-талдамалық платформаны енгізуді ұсынады [110, 530 б.]. Өз кезегінде, 3.1-бөлімде біз негіздегеніміздей, шашыраңқы базаларды физикалық түрде біріктіретін интеграциялық торапты («Data Hub») құру осы проблеманың практикалық архитектуралық шешімі болуға тиіс. Ұсынылған тәсілдерді талдау шоғырландыру ауқымындағы айырмашылықты көрсетеді: П.С. Пастухов тергеуші үшін процестік бағдарламалық қабық құруды негіздейді, ал А.А. Толыбаева жаһандық ведомствоаралық деректер базасын құрастыруды талап етеді. Біздің ойымызша, тергеп-тексерудің платформалық моделі жай ғана бағдарламалық интерфейс ретінде емес, жаңа процестік орта ретінде жұмыс істеуге тиіс. Бұл орта қатаң бірізділікпен құрылады: бірыңғай цифрлық контурда активтерге дереу электрондық тыйым сала отырып (ҚР ҚПК-тің 161-бабы), телеметрияны автоматтандырылған жинаудан бастап талдамалық шифрды ашуға және кінәлі адамды заңдық сәйкестендіруге (ҚР ҚПК-тің 113-бабы) дейін.

Цифрлық орта жағдайында активтерге дереу тыйым салу функциясын іске асыру құқық қорғау органдарына экстраординарлық өкілеттіктер беруді талап етеді, бұл Сингапурдың 2025 жылғы Алаяқтықтан қорғау туралы заңымен (Protection from Scams Act 2025) айқын көрсетіледі. Заңның қолданылу тетігі уәкілетті полиция офицерлері банк мекемелерінің атына тікелей шығаруға құқылы арнайы «шектеу ордерлерін» (Restriction Orders) енгізуде жатыр [165]. Процесс сотқа дейінгі тергеп-тексеру сатысында немесе тіпті қылмыстық істі формальды түрде қозғағанға дейін іске қосылады: жәбірленуші қаскөйлердің манипулятивті психологиялық ықпалында екендігіне негізді күдік болған кезде, полиция банкке директивті түрде кез келген транзакцияларды бұғаттауды және

несие қаражатын беруді 30 күнге дейінгі мерзімге тоқтата тұруды ұйғарады. Бұл превентивті шараның заңдық маңызы мынада: ол банктерге клиенттің өз қаражатын бұғаттағаны үшін оның алдындағы азаматтық-құқықтық жауаптылықтан толық иммунитет бере отырып, олардың әрекеттерін декриминализациялайды және активтерді сақтау процесін сот санкциясын алудың ауыр рәсімінен шығарады. Осы тәжірибені рецепциялау отандық құқық қолдану үшін сыни маңызға ие: тергеушіге сингапурлық шектеу ордері моделі бойынша шоттарды соттан тыс шұғыл бұғаттау құқығын беру қаражатты офшорлық юрисдикцияларға қайтымсыз шығарғанға дейін кибералаяқтықтың қаржылық тізбегін үзуге мүмкіндік береді.

Іргелі ғылыми жаңалық мынада: технологиялық интеграция сотқа дейінгі тергеп-тексеруді құбылмалы айғақтарды қолмен іріктеудің архаикалық процесінен предиктивті және ретроспективті аппараттық-бағдарламалық талдаудың бірыңғай, жоғары автоматтандырылған жүйесіне қайтымсыз түрде трансформациялайды. Платформалық модельді енгізу дәлелдемелік тізбектің үздіксіздігін және машиналық кодтың орны толмас жоғалуын барынша азайтуды қамтамасыз етеді. Жоғарыда аталғандар үлкен деректерді талдауды автоматтандыру және тәуекелдерді предиктивті болжау үшін қылмыстық сот ісін жүргізуге жасанды интеллект алгоритмдері мен машиналық оқыту элементтерін интеграциялаудың императивті қажеттілігін туындатады. Ұсынылған архитектура қылмыстық сот ісін жүргізудің электрондық форматына жаһандық көшу үшін берік инструменталдық және құқықтық база жасайды. Сонымен бірге, транзакцияларды толық алгоритмдік деанонимизациялау юрисдикциялық шектерге объективті түрде тап болады. Платформалық тәсілді тек ұлттық құқықтық жүйе шекарасында ғана толық ауқымда іске асыру жымқырылған активтер қозғалысының трансұлттық векторын бейтараптандыруға қабілетсіз. Ұлттық цифрлық контурдың анықталған шектеулілігі дәлелдемелік ақпаратпен жеделдетілген мемлекетаралық алмасу хаттамаларын әзірлеу және экстерриториялық құқықтық өзара іс-қимыл тетіктерін жетілдіру қажеттілігін туындатады.

Шетелдік құқық қорғау органдарының тиімді практикаларын, оның ішінде бірлескен тергеу топтарын (JITs) құрудың озық тәжірибесін және MLATs құралдарын пайдалануды белсенді түрде қабылдау қалыптасқан юрисдикциялық тосқауылдарды еңсеруге мүмкіндік береді [166, 428 б.]. Ұлттық технологиялық интеграция барабар мемлекетаралық өзара іс-қимылды құрмай, киберқылмыстылық қатерлерінің толық көлемде жолын кесуге объективті түрде қабілетсіз. Базалық проблема ретінде ҚР ҚПК-тің 559-бабымен регламенттелген халықаралық құқықтық көмектің консервативті институтының желілік жымқырулардың гипердинамикалық трансұлттық табиғатына толық сәйкессіздігі әрекет етеді. Оған қоса, М.С. Бисалиев атап көрсеткендей, мұндай ретте трансшекаралық инциденттерді нақты мемлекетке не тұлғаға телу – атрибуция – проблемасын шешуге тура келеді [16, 16 б.]. Р.Б. Джилкишиев негіздегендей, бюрократиялық бөгеттерді айналып өтіп, шетелдік провайдерлерден ақпаратты жедел алудың бір жолы – Интерполдың I-24/7 жаһандық коммуникациялық желісі секілді тәулік бойы істейтін байланыс

арналарын ұлттық тергеу практикасына тікелей қосу [57, 89 б.]. Осы нормативтік дағдарысты саралаған А.Г. Волеводз сұрау салуды жіберудің классикалық рәсімі дипломатиялық формальдылыққа тұнып тұрғанын, ал бұл шетелдік провайдерлерден банктік мәлімет пен деректі жедел алуды тұсаулайтынын көрсетеді [167, 14-15 б.]. Институционалдық талдауды тереңдете отырып, И.М. Нурбеков көпдеңгейлі келісу рәсімі және ұлттық құқықтық режимдердегі (егемендіктегі) айырмашылықтарға қатаң тәуелділік ҚР ҚПК-тің 122-бабы тәртібімен дәлелдемелерді жинауды көп айлық бюрократиялық процеске айналдыратынын тұжырымдайды [136, 133-134 б.]. Саяси-құқықтық тәсілмен өткір пікірталасқа Д.В. Завьялова түседі, ол дәстүрлі тапсырмаларды (ҚР ҚПК-тің 561 және 565-баптары) орындау мерзімдерінің цифрлық іздердің құбылмалығына сәйкессіздігі олардың шетелдік серверлерде қайтымсыз жоғалуына сөзсіз әкелетінін дәлелдей отырып, фокусты цифрлық ортаның физикалық қасиеттеріне ауыстырады [90, 156 б.].

Сипатталған нормативтік параличті еңсеру үшін Еуропалық Одақта электрондық дәлелдемелер туралы пакет (e-Evidence Package) шеңберінде іске асырылған тікелей трансшекаралық қол жеткізу тетігі тұжырымдамалық мәнге ие. Тетік процестік айналымға электрондық дәлелдемелерді ұсыну және сақтауға арналған еуропалық ордерлерді (European Production and Preservation Orders) енгізетін ЕО-ның 2023/1543 Регламентіне негізделеді, олар тергеу судьялары мен прокурорларына өзара құқықтық көмектің классикалық арналарын (MLAT) айналып өтіп, шетелдік IT-корпорацияларға орындалуы міндетті сұрау салуларды тікелей жіберуге мүмкіндік береді [168]. Процесс орталықсыздандырылған қорғалған платформа (e-EDES) арқылы инициацияланады, бұл ретте провайдерлерге деректерді сақтау (60 күнге дейін) немесе сәйкестендіру логтары мен контентті 10 күн ішінде, ал өмірге немесе сыни инфрақұрылымға қатер төнумен ұштасқан шұғыл жағдайларда – 8 сағат ішінде ұсынудың императивті міндеті жүктеледі [169]. Бұл модельдің заңдық маңызы юрисдикция парадигмасын түбегейлі өзгертуінде жатыр: серверлердің аумақтық байланыстырылуы өзінің бұғаттаушы мәнін жоғалтады, ал цифрлық іздерді беру міндеті ЕО аумағында қызметтер көрсету фактісіне байланыстырылады. ҚР ҚПК-ге тікелей қолданылатын осындай экстерриториялық құралды енгізу құбылмалы деректерді олар алгоритмдік жойылғанға дейін процестік тіркеп-белгілеуді қамтамасыз ете отырып, қағаз сұрау салулар мен желілік алаяқтық гипердинамикасының кеңістіктік-уақыттық сәйкессіздігін жоюға мүмкіндік береді.

Ұсынылған ғылыми ұстанымдарды талдау ақаудың бастапқы себебін локализациялаудағы айырмашылықты көрсетеді: алғашқы екі автор оны дипломатияның саяси-бюрократиялық тосқауылдарынан көреді, ал Д.В. Завьялова іргелі кеңістіктік-уақыттық сәйкессіздікті диагностикалайды [90, 156 б.]. Біздің ойымызша, аталған факторлар кумулятивті түрде әрекет етеді: іс-әрекетті қылмыс деп өзара тану талаптары мен ауыр дипломатиялық арналар уақытты жасанды түрде созады, бұл деректердің секунд үлесінде орын ауыстыруы жағдайында дәлелдеудің архаикалық қағаз моделін құбылмалы іздердің ресми түрде алынғанға дейінгі процестік сақталуын қамтамасыз етудің

гносеологиялық қабілетінен айырады.

Анықталған нормативтік параличті еңсеру мемлекетаралық ынтымақтастық тетіктерін тұжырымдамалық қайта қараудың императивті қажеттілігін туындатады. Оңтайландыру жолдарын зерттей отырып, В.А. Шестак пен А.С. Чеботарь деректерге шұғыл жедел қол жеткізудің процестік басымдығы ұзаққа созылатын формальды келісулерден басым болуға тиіс деп мәлімдей отырып, уақыт шығындарын барынша азайту қажеттілігіне назар аударады [170, 307 б.]. Қағидатты түрде өзге ұстанымдар тұрғысынан нақты уақытқа жақындатылған режимде (real-time) жұмыс істейтін өзара іс-қимылдың архаикалық реактивті моделінен проактивті желілік моделіне идеологиялық көшу пайдасына ескі нысандарды жаңғыртудан толық бас тарту қажеттілігін дәлелдейтін А.А. Толыбаева бастаған авторлар ұжымы келеді [98, 138 б.]. Ғылыми көзқарастарды салыстыру тұжырымдамалық алшақтықты көрсетеді: егер В.А. Шестак пен А.С. Чеботарь қолданыстағы реактивті модельге басымдық бере отырып, оны жеделдетуді ұсынса, А.А. Толыбаева ақпарат алмасудың мүлдем жаңа, перманентті (проактивті) нысанын енгізуді талап етеді. Авторлық тәсілді негіздей отырып, А.А. Толыбаева ұстанымының баламасыздығын мойындау қажет. Постфактум сұрау салуды жіберуді жай ғана процестік жеделдету активтерді лездік шығарудың орнын толтыруға қабілетсіз; жоғары технологиялық жымқыруларды нәтижелі тергеп-тексеруге киберқылмысты жасау сәті мен үздіксіз автоматтандырылған желі арқылы транзакциялық деректерді іс жүзінде алу арасындағы алшақтықты түбегейлі қысқартқан кезде ғана қол жеткізуге болады.

Проактивті модельді іс жүзінде іске асыру терең технологиялық интеграцияны талап етеді, оның векторлары да ғылыми пікірталас тудырады. Ақпарат алмасу инструментарийін бағалай отырып, П.С. Пастухов базалық шешім ретінде ведомствоаралық құқықтық сұрау салуларды верификациялау және өңдеу рәсімдерін автоматтандыруды технологиялық тұрғыдан қамтамасыз етуге қабілетті қорғалған халықаралық цифрлық платформаларды енгізуді ұсынады [110, 535-536 б.]. Өз кезегінде, К.К. Клевцов пен В.Ф. Васюков орталық дипломатиялық ведомстволарды айналып өтіп, лог-файлдарға шұғыл қол жеткізуді алу үшін трансұлттық провайдерлермен тікелей тергеу органдарының көлденең желілік байланыстарын (тәулік бойғы байланыс желілері форматында) дамытудың сыни маңыздылығын көрсете отырып, өзара іс-қимыл векторын ауыстыру қажеттілігін негіздейді [171, 44-45 б.]. Тәсілдердің анықталған айырмашылығы айқын: П.С. Пастухов мемлекетаралық (егеменді) платформалық архитектураны құрастырады, ал тең авторлар тікелей қол жеткізудің мемлекеттік-жекешелік (корпоративтік) желісін қалыптастыруды талап етеді. Екі институционалдық конструкция бір-бірін жоққа шығармайды, қайта толықтырады. Қылмыстық-процестік заң екі контурлы жүйені: мемлекеттер арасындағы цифрлық дәлелдемелерді платформалық верификациялауды (мемлекетаралық контур) және трансұлттық IT-корпорациялардың серверлеріне тікелей басымдықпен қол жеткізу тетіктерін (корпоративтік контур) легитимдеуге тиіс. Бұл синтез консервативті қағаз-бюрократиялық рәсімнен трансшекаралық құқықтық өзара іс-қимылдың озық

цифрлық желілік архитектурасына сөзсіз тұжырымдамалық көшуді қамтамасыз етеді.

Ғылыми жаңалық мынада: жеделдетілген халықаралық өзара іс-қимыл ынтымақтастықтың қағидатты түрде жаңа құқықтық институционалдық моделі болып табылады. Бұл конструкция іргелі түрде үш міндетті элементке негізделеді: транзакциялық және коммуникациялық деректермен алмасуды өтпелі автоматтандыру; құбылмалы іздерді шұғыл сақтау кезінде юрисдикциялық процестік тосқауылдарды толықтай барынша азайту; әртүрлі мемлекеттердің құқық қорғау органдарының ақпараттық жүйелерін бірыңғай контурға терең, криптографиялық қорғалған технологиялық интеграциялау. Құқықтық көмекті цифрландыру электрондық дәлелдемелік базаның сақталуына және сотқа дейінгі іс жүргізу нәтижелілігінің еселеп өсуіне кепілдік бере отырып, онлайн алаяқтыққа тиімді қарсы іс-қимыл жасаудың императивті шарты ретінде әрекет етеді. Бұл ретте мәлімделген архитектураның объективті ауқымдылығы және ұлттық қылмыстық сот ісін жүргізуге платформалық шешімдерді имплементациялау үшін орасан зор ресурс шығындарына деген қажеттілік әзірленген тетіктердің экономикалық орындылығы мен ұйымдастырушылық тиімділігін пәндік бағалау қажеттілігін туындатады.

Алайда, мәлімделген артефактіге орталықтандырылған модельді практикаға кезең-кезеңмен енгізу тетігі таза процестік шеңберден шығып, ауқымды макроэкономикалық және институционалдық шығындарды талап ететін күрделі мемлекеттік инвестициялық процесті білдіреді. Құқық қолданудың қазіргі заманғы жағдайында қылмыстық сот ісін жүргізуді цифрландыру криминалистикалық мүкәммалды жай ғана техникалық жаңартуды емес, күрделі мемлекеттік инвестициялық процесті білдіреді. Осы жаңғырту шеңберінде қаржы ағындарын бөлу өткір доктриналық пікірталас тудырады. Д.В. Завьялова күрделі салымдардың абсолютті басымдығы ретінде техникалық инфрақұрылымды дамыту: интеграцияланған платформаларды әзірлеуді үздіксіз қаржыландыру, серверлік жабдықты сатып алу және жүйелерді алгоритмдік жаңарту әрекет етуге тиіс екенін дәлелдейді [90, 95 б.]. Бұл тәсілден айырмашылығы, Е.Р. Россинская когнитивтік фактордың бастапқылығын негіздейді: цифрлық криминалистиканы озып ауқымды қаржыландырусыз және тергеу аппаратын үздіксіз қайта даярлаусыз техникаға инвестициялар құю мәнсіз [158, 36 б.]. Ұсынылған ғылыми ұстанымдарды салыстыру іргелі алшақтықты көрсетеді: ішкі адами капиталды арттыруға қарсы сыртқы инфрақұрылымдық масштабтау. Біздің ойымызша, бұл векторлар қатаң симметриялық теңгерімді талап етеді. 2023-2029 жылдарға арналған Цифрлық трансформациялау тұжырымдамасы талап ететіндей, бейінді IT-тергеушілер пулын қалыптастырмай озық ғылыми-техникалық құралдарды (ҚР ҚПК-тің 126-бабы) оқшауланған түрде сатып алу қымбат тұратын аппараттық-бағдарламалық кешендерді сөзсіз жұмыс істемейтін, өлі активке айналдырады.

Кешенді қаржыландырудың анықталған қажеттілігі дәстүрлі бюджеттік модельдің сыни дәрменсіздігін көрсетеді. Тарихи қалыптасқан тетік процестік шығындарды және тергеп-тексеру органдарын ұстауға арналған шығыстарды тек мемлекеттік қаражат есебінен ғана жабуды ұйғарады (ҚР ҚПК-тің 177-бабы).

Алайда цифрлық инфрақұрылымның ресурстық сыйымдылығының бұрын-соңды болмаған ауқымы таза бюджеттік қаржыландыруды өміршең емес етеді. Тапшылықты еңсеру жолдарын зерттей отырып, Д.В. Завьялова мемлекеттік-жекешелік өзара іс-қимыл тетіктеріне негізделген әртараптандырылған тәсілдің баламасыздығын көрсетеді [90, 148 б.]. Авторлық ұстаным осы вектормен толық ынтымақтасады: тергеу аппаратын сыртқы базалармен интеграциялау қаржы нарығы субъектілері мен телекоммуникация компаниялары тарапынан тікелей бірлесіп инвестициялауды талап етеді. Корпоративтік сектор өз желілеріндегі репутациялық және алаяқтық тәуекелдерді барынша азайтудан тікелей пайда алушы ретінде әрекет ететіндіктен, оның бірыңғай антифрод-орталықтардың жұмысына технологиялық және қаржылық қатысуы («Төлемдер және төлем жүйелері туралы» ҚРЗ-ның 25-1-бабы негізінде) заңдық және макроэкономикалық тұрғыдан негізделген, бұл мемлекеттің күрделі шығындарының бір бөлігін легитимді түрде қайта бөлуге мүмкіндік береді.

Ауқымды инвестицияларды тартуды негіздеу толығымен ұсынылған модельдің жоғары рентабельділік өлшемшарттарына сүйенеді. Бұрын анықталған процестік үнемдеу және реституция параметрлеріне сүйене отырып, өтелімділік өлшенетін екі фактордың синергиясы есебінен қол жеткізілетінін атап өту қажет. Бастапқы тікелей эффект қайтымсыз залал көлемін түбегейлі төмендететін және активтерге электрондық тыйым салудың нақты орындалуын қамтамасыз ететін криминалдық транзакциялардың алгоритмдік жолын кесуден көрініс табады (ҚР ҚПК-тің 161-бабы). Қайталама макроэкономикалық эффект құқық қорғау машинасының өзінің операциялық шығындарын жүйелі түрде барынша азайтудан көрінеді: қылмыстық сот ісін электрондық форматта жүргізуге толық көшу (ҚР ҚПК-тің 42-1-бабы) қағаз іс жүргізуге, логистика мен бюрократиялық әкімшілендіруге кететін көпмиллионды мемлекеттік шығындарды біржолата жояды. Бұл арақатынас технологияларға құйылатын бастапқы күрделі салымдар ұзақ мерзімді перспективада қылмыстық әділет жүйесіне түсетін жиынтық қаржылық жүктемені ұдайы төмендететінін сенімді түрде дәлелдейді.

Мәлімделген экономикалық көрсеткіштерге қол жеткізу тергеу аппаратын терең құрылымдық қайта құрусыз мүлдем мүмкін емес. Архаикалық бюрократиялық каркасқа салынған технологиялық жаңғырту институционалдық параличті сөзсіз туындатады. Ұйымдастырушылық ортаны бағалай отырып, К.О. Карабеков автономды, тар бейінді кибербөлімшелерді құру пайдасына штаттарды дәстүрлі бөлуден толық бас тартудың объективті қажеттілігін дәлелдейді [17, 143-144 б.]. Авторлық тәсілді негіздей отырып, бұл тезисті дамыту қажет: жаңа модель қатаң функционалдық бөлуді енгізуді талап етеді. Құқық қорғау органдары тек фактілерді процестік тіркеп-белгілеуге, қаржы институттары – транзакциялық телеметрияны шұғыл беруге, ал технологиялық корпорациялар – алмасу архитектурасын қорғауға шоғырлануға тиіс. Тек осындай жіксіз, гибридті операциялық орта шеңберінде ғана цифрлық шешімдер 2024-2028 жылдарға арналған Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасында тікелей бекітілетін ұзақ мерзімді жүйелі эффектілерді: қылмыстардың жасанды латенттілігін жоюды және азаматтық қоғамның сенімін

қалпына келтіруді генерациялауға қабілетті.

Онлайн алаяқтықты сотқа дейінгі тергеп-тексеру тетігіне платформалық цифрлық технологияларды жүйелі түрде енгізу экономикалық тұрғыдан рентабельді, ұйымдастырушылық жағынан қажетті және ғылыми негізделген қадам ретінде әрекет етеді. Материалдық-құқықтық новеллаларды, артефактіге орталықтандырылған процестік алгоритмдерді, деанонимизациялаудың технологиялық құралдарын және өзара іс-қимылдың салааралық тетіктерін органикалық түрде синтездейтін диссертация шеңберінде әзірленген кешенді парадигма киберқылмыстылыққа қарсы іс-қимылдың монолитті жүйесін қалыптастырады. Теориялық ережелердің, нормативтік ұсыныстардың және қолданбалы әдістемелердің қалыптастырылған жиынтығы зерттеудің қорытынды нәтижелерін тұжырымдамалық қорытуға көшу қажеттілігін логикалық түрде туындатады.

Онлайн алаяқтықты сотқа дейінгі тергеп-тексерудің кешенді парадигмасын қалыптастыруды аяқтау талданатын проблематиканы технологиялық, институционалдық және халықаралық компоненттердің макродеңгейлік синтезіне шығаруды баламасыз түрде талап етеді. Дәлелдемелерді жинаудың қолданыстағы тетігі (ҚР ҚПК-тің 122-бабы) және құқықтық көмек көрсетудің консервативті рәсімдері (ҚР ҚПК-тің 559-бабы) киберқылмыстылықтың экстерриториялық анонимділігіне тұжырымдамалық түрде қарсы тұруға қабілетсіз. Осы институционалдық дағдарысты еңсеру векторларын зерттей отырып, Д.В. Завьялова цифрлық кеңістіктегі қудалаудың нәтижелілігіне тек әртүрлі юрисдикциялардағы құқық қорғау органдарының шашыраңқы күш-жігерін деректермен алмасудың бірыңғай трансұлттық жүйесіне шоғырландыру есебінен ғана қол жеткізіледі деп мәлімдейді [90, 158-159 б.]. Макроюрисдикциялық тәсілден айырмашылығы, П.С. Пастухов ішкі технологиялық фактордың абсолютті басымдығын дәлелдейді: дәл осы өтпелі аппараттық-бағдарламалық кешендерді және зияткерлік жүйелерді (Big Data) енгізу дәлелдеудің архаикалығын еңсеруге және ҚР ҚПК-тің 126-бабы бойынша ғылыми-техникалық құралдарды қолдану шеңберінде құбылмалы іздердің орасан зор массивтерін дереу тіркеп-белгілеуге мүмкіндік береді [100, 538 б.]. Талдауға үшінші, темпоральды метриканы Р.И. Оконенко енгізеді, ол қатерді анықтау мен іс жүзіндегі құқықтық ден қою арасындағы сыни алшақтықты қысқарту есебінен шетелдік серверлерде электрондық дәлелдемелердің орны толмас жоғалуын тұжырымдамалық түрде барынша азайтатын өзара іс-қимылды технологиялық жеделдету түйінді болып табылатынын талап етеді [172, 118 б.].

Ұсынылған ұстанымдарды талдау жаңғыртудың құрылым құраушы драйверін айқындаудағы айырмашылықты көрсетеді: сыртқы юрисдикциялық интеграция (Д.В. Завьялова), ішкі технологиялық трансформация (П.С. Пастухов) немесе құқықтық рәсімдерді темпоральды жеделдету (Р.И. Оконенко). Біздің ойымызша, көрсетілген бағыттардың кез келгенін оқшауланған түрде іске асыру объективті түрде дәрменсіз. Проблеманы шешу мемлекеттік қылмыстық қудалау мен жекеше қаржы секторы арасындағы жасанды тосқауылдарды жоятын синергетикалық жүйені қалыптастыруда жатыр. Технологиялық инновациялар юрисдикцияларды біріктіретін және уақытты қысқартатын

факультативтік емес, іргелі құрал ретінде әрекет етеді. Зерттеу шеңберінде ұсынылған экономикалық-ұйымдастырушылық архитектура технологиялық, құқықтық және институционалдық факторлар бір-бірінің әлеуетін еселеп күшейте отырып, ажырамас процестік өзара байланыста жұмыс істеуге міндетті екенін дәлелдейді.

3.3 Онлайн алаяқтық қылмыстарына қарсы іс-қимыл саласындағы Қазақстан Республикасының заңнамасын жетілдіру

Инновациялық криминалистикалық және процестік модельдерді жобалау материалдық құқықтың іргелі осалдығын логикалық түрде көрсетеді: цифрлық қаржы технологияларын енгізу мен оларды қылмыстық-құқықтық регламенттеу арасындағы айқын заңнамалық артта қалушылық. Қазақстан Республикасының қылмыстық заңнамасы алаяқтық үшін жауаптылықты белгілей отырып (ҚР ҚК-нің 190-бабы), тарихи тұрғыдан қолсұғушылықтың классикалық нысандарына сүйенеді. Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасы құқықтық реттеу тек реактивті сипатқа ие екенін ресми түрде тіркеп-белгілейді. Осы артта қалушылықтың табиғатын бағалай отырып, Г.Р. Григорян ақпараттық қатынастардың даму қарқыны нормашығармашылықтан еңсерілмейтіндей озып кетіп, заңды превентивті функциясынан айыратынын тұжырымдайды [15, 5 б.]. Бұл заңнамалық артта қалушылықты еңсеру үшін нормашығармашылық процестің өзін автоматтандыру және жаңа заңдардың салдарын предиктивті болжау үшін жасанды интеллект (AI) пен үлкен деректерді (Big Data) қолдану перспективалы болып табылады [173, 31 б.].

Талдауды дамыта отырып, К.О. Карабеков дәл осы мемлекет реакциясының кешігуі құқық қолданудың жүйелі тиімсіздігінің басты детерминанты ретінде әрекет ететінін мәлімдейді, өйткені қылмыстық құдалау органдары жаңа қатерлермен күресудің өзекті құқықтық құралдарынан айырылады [17, 93-94 б.]. Сонымен бір уақытта А.Қ. Қамбаров жаңа криминалдық схемалар консервативті нормалардың қолданысынан шығып қалатын ауқымды «құқықтық белгісіздік аймағының» қалыптасуын негіздей отырып, проблеманы темпоральды жазықтықтан құрылымдық жазықтыққа ауыстырады [174, 14 б.]. Осы ұстанымдарды салыстыру салдарларды бағалаудағы айырмашылықты көрсетеді: егер О.С. Капинус пен М.А. Костюченко қатерді қарқынды жоғалтудан (уақытша құлдырау) көрсе [15, 5-6 б.; 175, 59-60 б.], онда А.Қ. Қамбаров абсолютті құқықтық вакуумның пайда болуын (мәндік құлдырау) диагностикалайды. Біздің ойымызша, аталған ақаулар синергетикалық түрде әрекет етеді. Криминализациялаудың хронологиялық артта қалуы мағыналық бостықты объективті түрде туындатады, бұл ретте жоғары технологиялық жымқырулар формальды түрде жалпы тыйым салулардың аясына түскенімен, іс жүзінде іс-әрекеттің қағидатты түрде өзге архитектурасына байланысты олармен қамтылмайды.

Анықталған нормативтік инерттілік қолсұғушылықтың базалық объектісі цифрлық кредиттік өнімдер болатын қылмыстылықтың сапалы жаңа

сегменттерінің қалыптасуын катализдейді. Қашықтықтан көрсетілетін қаржылық сервистер қылмыс жасау тетігінің өзін трансформациялайды. Осы трансформацияны талдай отырып, Р.А. Тагиров банктік мәмілелерді толық автоматтандыру пайдакүнемдік іс-әрекеттерді тек қашықтықтағы жазықтыққа ауыстыратынын көрсете отырып, назарды кеңістіктік аспектіге аударады [176, 151 б.]. Бұл тәсілден айырмашылығы, А.Б. Курумбаева мен Б.Б. Кощегулов трансформацияның терең сапалық сипатқа ие екенін дәлелдейді: адам санасына классикалық вербалды ықпал ету толығымен скорингтік алгоритмдермен виртуалды манипуляция жасаумен алмастырылады [21, 50-51 б.].

Бұл доктриналық ұстаным біз бұрын талдаған сот практикасымен (атап айтқанда, №5516-22-00-1/28 [143] және №3528-23-00-1/20 [48] қылмыстық істермен) расталады. Анықталғандай, қаскөйлер жәбірленушімен байланысты вербалды алдау үшін емес, тек биометриялық жүйелерді («Face ID») техникалық айналып өту үшін пайдаланады. Мұның өзі алаяқтықтың объективтік жағында эволюциялық ығысу болғанын күмәнсіз аңғартады: ықпал енді адам санасына емес, қаржы институттарының қауіпсіздік алгоритмдеріне бағышталады, ал бұл қылмыстық заңды соған сәйкес бейімдеуді қажет етеді.

Осы тұстағы көзқарастарды қатар қойғанда қағидатты алшақтық көрінеді: Р.А. Тагиров өзгерісті коммуникация тәсілінен (қашықтықтан жасалуынан) іздесе, тең авторлар алдау объектісінің өзі ауысқанын – адамның орнын алгоритм басқанын – диагностикалайды. Авторлық ұстанымды негіздей келе, ҚР ҚК-нің 190-бабымен ашық қайшылыққа түсетін осы сапалық трансформацияның бастапқы, түпкі сипатын мойындаған жөн. Заңның «ақпараттық жүйені пайдаланушыны алдау» туралы қолданыстағы тұжырымдамасы тұжырымдамалық тұрғыдан ақаулы: қазіргі заманғы кредиттік өнімдерде қылмыскер легитимді емес деректерді енгізу арқылы пайдаланушыны емес, капиталды маршруттаудың соқыр құралы ретінде әрекет ететін автоматтандырылған платформаның өзін алдайды.

Дәстүрлі құқықтық конструкциялардың ақаулығы электрондық қызметтерін заңдастыру «Микроқаржылық қызмет туралы» ҚРЗ-ның 3-бабымен бекітілген МҚҰ сегментінде неғұрлым бедерлі түрде көрініс табады. Нарықты либерализациялау жалған қарыздарды жаппай ресімдеуді туындатты. Осы сегментті зерттей отырып, А.Б. Сабырбаева қашықтан қызмет көрсету форматы «қылмыскер – жәбірленуші» дәстүрлі бинарлық моделінің түпкілікті бұзылуына әкеле отырып, визуалды байланысты барынша азайтатынын тұжырымдайды [103, 162 б.]. Проблемаға өзге ұстанымдар тұрғысынан К.О. Карабеков келеді, ол ескі модельдің жай ғана бұзылмайтынын, оның алданған ұйым мен компрометацияланған азамат шашыраңқы элементтерді құрайтын күрделі көпсубъектілі конструкциямен алмастырылатынын негіздейді [17, 43-44 б.]. М.С. Бисалиев атап өткендей, мұның базалық себебі ретінде үшінші тұлғалардың дербес деректерін құқыққа сыйымсыз пайдалану әрекет етеді [16, 160 б.]. А.Б. Сабырбаеваның (бинарлықты жоғалтуға фокус) және К.О. Карабековтың (көпсубъектілікті қалыптастыруға фокус) көзқарастары арасындағы анықталған тұжырымдамалық алшақтық құрылымдық синтезді талап етеді.

Осы синтез шеңберінде алғаш рет құқықтық табиғаты: қылмыскердің,

қаржы институтының және дербес деректер субъектісінің өзара іс-қимылының күрделі құқықтық конструкциясын құрайтын қолсұғушылықтың қособъектілігіне негізделетін микрокредиттік алаяқтықтың криминалдық ерекшелігі негізделді. Бұл іс-әрекетті жасау кезінде залал бір мезгілде екі дербес қорғалатын игілікке келтіріледі. Негізгі объект рөлін меншік қатынастары атқарады, әрі тікелей мүліктік залал тек МҚҰ-ға ғана келеді: айналымдағы активінен қайтару мүмкіндігінсіз айырылатын да, сол себепті бастапқы мүліктік жәбірленуші саналатын да – осы ұйым. Қосымша объект ретінде азаматтың ақпараттық және конституциялық құқықтары – жеке өмірге қолсұғылмаушылық пен дербес деректерді қорғауға берілген кепілдіктер (соның ішінде ҚР ҚК-нің 147-бабымен қорғалатын мүдделер) – көрініс табады. Демек, цифрлық дәлелдемені алу мен өңдеу барысында азаматтардың конституциялық құқығын сақтаудың қатаң құқықтық тетіктерін әзірлеу құқықтық мемлекет үшін аса мәнді міндетке айналады [177, 44-45 б.]. Қаскөйдің бөтен дербес деректерді пайдалануы, электрондық цифрлық қолтаңбаны (ЭЦҚ) заңсыз генерациялауы және иесінің білуінсіз биометрияны ауыстыруы жеке тұлғаға елеулі беймәтериалдық және құқықтық зиян (цифрлық бірегейліктің компрометациясы, деректерді заңсыз өңдеу, кредиттік тарихты бұрмалау) келтіреді.

Осылайша, МҚҰ-ны меншікті жымқыру бөлігінде негізгі жәбірленуші деп тану ешқандай жағдайда азаматты қылмыстық процестен шығаруды білдірмейді. Керісінше, қособъектілік тұжырымдамасы келтірілген зиянның екі қатарлас деңгейінің: мүліктік (МҚҰ-ға қатысты) және ақпараттық-конституциялық (жеке тұлғаға қатысты) бар екендігін тануды императивті түрде талап етеді. Азамат оның заңмен қорғалатын ақпараттық құқықтарына қолсұғушылықтан жәбірленуші деп танылуға тиіс, бұл осы құқықтық қатынастардың барлық қатысушыларын кешенді қылмыстық-құқықтық қорғауды қамтамасыз етеді.

Тұжырымдалған аномальді триада тұжырымдамасы зерттеудің ағымдағы сатысының ғылыми жаңалығын негіздеуге мүмкіндік береді: микрокредиттік онлайн алаяқтық барабар материалдық-құқықтық базамен мүлдем қамтамасыз етілмеген дербес, жоғары технологиялық сегментке бөлінеді. Қылмыстық заңның (ҚР ҚК-нің 190-бабы) осы іс-әрекеттің күрделі субъектілік құрылымын жүйелі түрде елемеуі тергеп-тексеруді инициациялау сатысында құқық қолданудың жойқын салдарларына әкеп соғады. Формальды түрде генерацияланған электрондық кредиттік шарттың болуы криминалдық деликтіні легитимді мәміле көрінісіне жасанды түрде трансформациялайды. Бұл құқық қорғау органдарына азаматтық-құқықтық даудың бар екендігіне сілтеме жасай отырып, арыздарды тіркеуден бас тарта отырып, ҚР ҚПК-тің 179-бабының ұйғарымдарын жаппай қолдануға мүмкіндік береді. Нәтижесінде сот төрелігінің терең деформациясы орын алады: жасанды аса жоғары латенттілік генерацияланады, деректердің жылыстауының құрбаны құқықтық жүйемен жосықсыз борышкер ретінде негізсіз қарастырылады, ал шынайы қолсұғушылық қылмыстық қудалау шегінен шығарылады.

Жүргізілген материалдық-құқықтық диагностиканың нәтижелерін қорыта отырып, қатаң бағдарламалық қорытындыны тұжырымдау қажет. Үдемелі заңнамалық артта қалушылық кибержымқыруларға қатысты қылмыстық заңның

қолданыстағы редакциясының реттеушілік әлеуетінің сарқылуын қатаң түрде туындатады. Материалдық құқықтың тұжырымдамалық олқылықтары және олар туындатқан құқық қолдану практикасының жүйелі бұрмаланулары дағдарысты еңсеру тек процестік немесе әкімшілік шаралармен ғана мүмкін еместігін бұлтартпастай дәлелдейді. Қалыптасқан құқықтық белгісіздік бейінді материалдық-құқықтық новацияларды әзірлеу және цифрлық транзакциялық сегменттің ерекшелігін барабар көрсететін мамандандырылған қылмыс құрамдарын құрастыру бойынша императивті ғылыми-практикалық қажеттілікті туындатады.

Бұрын анықталған процестік-инфрақұрылымдық дағдарыс материалдық құқықтың терең гносеологиялық және нормативтік сәйкессіздігімен объективті түрде ушыға түседі. Базалық проблема ретінде ҚР ҚК-нің 190-бабының консервативті конструкциясы мен микрокредиттеу саласындағы кибержымқыруларды жасаудың іс жүзіндегі трансұлттық моделі арасындағы заңнамалық артта қалушылық әрекет етеді. Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасында бекітілген ресми криминологиялық статистика азаматтарды жаппай қашықтан тартуға негізделген микрокредиттік схемалардың басым үлесін тіркеп-белгілейді. Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасында тіркеп-белгіленген микрокредиттік схемалардың басымдығы сипатталған қособъектілік тұжырымдамасының өзектілігін эмпирикалық түрде растайды. Зерттеушілер негізді түрде атап өткендей, саралаудың қолданыстағы нормативтік моделі нақты жәбірленушіні (микроқаржы ұйымын) кредиттік құқықтық қатынастардың номиналды субъектісімен алмастыра отырып, бұл фактіні елемеуді жалғастырады.

Қалыптасқан тұжырымдамалық тұйықтықты еңсеру векторлары кибержелінің транзиттік элементтерінің рөлін қылмыстық-құқықтық бағалау бөлігінде өткір ғылыми пікірталас тудыратын материалдық-құқықтық новациялар кешенін енгізуді объективті түрде талап етеді. Үшінші тұлғаларды криминалдық схемаға тарту тетігін зерттеген А.М. Ахатова өз банктік деректемесін ұсынған адамдарды көбіне сыбайлас қатысу институтының призмасынан қарайды әрі оларды негізгі жымқырудың көмектесушісі ретінде саралау керектігін негіздейді [178, 1079-1080 б.]. Мұндай біріңғай тәсілге В.А. Машлякевич қарсы шығып, сыбайлас қатысуды механикалық түрде таға салу әдіснамалық жағынан қате екенін дәлелдейді. «Қылмыс делдалдары» санатын талдай келе, бұл автор ондай адамдардың басым көпшілігі өз шоты арқылы өтетін транзакциялардың нақты көлемі мен криминалдық астарын түсінбей, «бейхабар» күйде пайдаланылатынын, ал бұл алаяқтыққа бірлескен пиғылдың болуын мүлде жоққа шығаратынын сенімді көрсетеді [79, 58-59 б.].

Екі ұстанымды қатар қойғанда догматикалық бағаның ашық қайшылығы байқалады: алғашқы автор объективтік жақтың – жымқырылған активті шығаруды іс жүзінде қамтамасыз етудің – салмағын бірінші орынға шығарса, екіншісі проблеманы субъективтік жақ жазықтығына, яғни бірлескен хабардарлық пен пиғылдың жоқтығына, ойыстырады. Авторлық ұстанымды қалыптастыра келе, бұл екі тәсіл де күрделі цифрлық шынайылықты тек жарым-

жартылай қамтитынын айту керек. Шешім жауаптылық негіздерінің догматикалық аражігін қатаң ажыратудан табылады. Кредиттік қаражатты жымқыруға тікелей пиғыл дәлелденсе, адам онлайн алаяқтықтың толыққанды сыбайласы ретінде жауап береді (ҚР ҚК-нің 190-бабы). Ал дроппердің пайдакүнемдік ниеті жымқырудың түпкі мақсатын аңғармастан, электрондық төлем құралының аутентификациялық деректерін формальды түрде беріп, соның есесіне біржолғы сыйақы алумен ғана шектелсе, сыбайлас қатысу институтын (ҚР ҚК-нің 28-бабы) қолдануға болмайды.

Мұндай әрекет төлем жүйелерінің белгіленген жұмыс тәртібіне қол сұғатын дербес қылмыс құрамын түзеді әрі оқшау күйінде – ҚР ҚК-нің 232-1-бабының арнайы нормасымен сараланады. Осы доктриналық конструкция шот иесін микроқаржы ұйымы алдындағы заңды азаматтық-құқықтық борышкер деп қате танитын жағымсыз құқық қолдану фикциясын біржола ыдыратуға мүмкіндік береді. Оның логикалық жалғасы ретінде тағы бір өткір мәселе туындайды: ҚР ҚК-нің 232-1-бабы бойынша тартылатын адамдардың материалдық жауаптылығының шегін айқындау. Сот практикасы көрсеткендей, бұл санаттағы істерде жәбірленушілер азаматтық талап шеңберінде келтірілген материалдық залалдың толық сомасын тікелей номиналды шот иелерінен (дропперлерден) өндіруді талап етіп жатады. Сонымен бірге, мұндай адамдардың іс жүзіндегі рөлі негізгі алаяқтық схеманы іске асыруға тікелей қатыспай, сыйақы үшін төлем құралдарына қол жеткізуді ұсынумен ғана шектеледі. Оларға жымқырылған қаражаттың толық көлемін ортақтасып өтеу міндетін жүктеу әділеттілік және қылмыстық жауаптылықты дараландыру қағидатымен объективті қайшылыққа түседі.

Осыған байланысты, қылмыстық және азаматтық заңнаманы біркелкі қолдануды қамтамасыз ету мақсатында ҚР Жоғары Сотының №6 Нормативтік қаулысында тиісті ресми түсіндірмелерді әзірлеу мақсатқа сай деп саналады. Атап айтқанда, ҚР ҚК-нің 232-1-бабы бойынша сотталған адамдар негізгі алаяқтық фактісімен келтірілген залалды толық өтеу міндетінен босатылуға жатады деген ережені бекіту ұсынылады. Сонымен бір мезгілде, ҚР ҚК-нің 3-бабының 2 және 38-тармақтарына сәйкес, дроппердің әрекеттерін саралау кезінде ол заңсыз алған материалдық сыйақының (мүліктік пайданың) мөлшерін айқын айқындау қажет: 200 айлық есептік көрсеткіштен асатынын айтарлықтай мөлшер ретінде, ал 500 АЕК-тен асатынын – ірі мөлшер ретінде бағалау ұсынылады.

Кредиттік ұйымды алаяқтықтан тиісті жәбірленуші, ал дропперді ақпараттық қауіпсіздікке қарсы дербес қылмыстың субъектісі деп тану тергеуді көлеңкелі капиталдардың шынайы бенефициарларын іздеуге бағдарлай отырып, оны легитимді арнаға қайтарады.

Қалыптасқан тұжырымдамалық тұйықтықты еңсеру векторлары өткір ғылыми пікірталас тудыратын материалдық-құқықтық новациялар кешенін енгізуді объективті түрде талап етеді. Жаңғырту жолдарын талдай отырып, А.Б. Курумбаева мен Б.Б. Кощегулов мұны қазіргі заманғы ақпараттық жүйелерде алдау адам психикасына емес, аппараттық-бағдарламалық кешеннің математикалық алгоритмдеріне бағытталғанымен дәлелдей отырып,

алаяқтықтың объективтік жағын бейімдеу қажеттілігін талап етеді [21, 50-51 б.]. Қаржы институттарын келтірілген залал субъектілері деп сөзсіз тани отырып, кредиттік-қаржылық саланы дербес объект ретінде оқшаулауды ұсына отырып, іс-әрекет тәсілін емес, қорғау объектісін өзгертудің орындылығын дәлелдейтін М.А. Костюченко өзге ұстанымды ұстанады [175, 47-48 б.]. Ұсынылған ғылыми тәсілдерді салыстыру айқын қайшылықты көрсетеді: алғашқы авторлар ақауды қылмыс жасау тәсілінде (объективтік жағы) локализациялайды, ал екіншісі проблеманы қолсұғушылық объектісін дұрыс анықтамаудан көреді. Бұл тәсілдерді синтездеу қажет деп саналады. ҚР ҚК-нің 190-бабы 2-бөлігі 4-тармағының қолданыстағы нормасы тек жеке тұлғаның мүдделерін ғана қорғайтын «ақпараттық жүйені пайдаланушыны» алдағаны үшін жауаптылықты белгілейді. Алайда микрокредиттік жымқыру тетігінде қылмыскер ұйымның өзінің активтеріне (қолсұғушылық объектісі) залал келтіре отырып, дәл қаржы платформасының скорингтік алгоритмін (жасау тәсілі) алдайды.

Анықталған доктриналық және нормативтік қайшылықтарды синтездеу МҚҰ бастапқы жәбірленуші тұлға ретінде құрастыру тұжырымдамасынан көрініс табатын зерттеудің ғылыми жаңалығын негіздеуге мүмкіндік береді. Бұл тұжырымның практикалық құны айқын: микрокредиттік кибержымқыруды саралағанда оны соттар да, қылмыстық қудалау органдары да тікелей басшылыққа ала алады. Тұжырымдаманы іске асыру мақсатында ҚР ҚК-нің 190-бабының 2-бөлігін мына жаңа саралаушы белгімен толықтыру ұсынылады: «қаржы ұйымының ақпараттық жүйесіне көрінеу жалған компьютерлік деректерді енгізу арқылы жымқыру». Бұл новелланың заңдық логикасы пайдаланушы (компрометацияланған деректердің азаматы) мен жүйе әкімшісінің (капитал иесінің) қатаң догматикалық аражігін ажыратуға негізделеді.

Сонымен бірге, ұсынылған саралаушы белгіні ҚР ҚК-нің 190-бабына енгізу виртуалды децепцияны ҚР ҚК-нің 7-тарауымен регламенттелген ақпараттандыру және байланыс саласындағы аралас қылмыстық құқық бұзушылықтардан қатаң догматикалық шектеуді талап етеді.

Біз ұсынып отырған «қаржы ұйымының ақпараттық жүйесіне көрінеу жалған компьютерлік деректерді енгізу арқылы жымқыру» конструкциясы ақпараттандыру объектісіне көрінеу жалған ақпаратты енгізуді криминализациялайтын ҚР ҚК-нің 206-бабының нормаларымен, сондай-ақ ҚР ҚК-нің 205 (Ақпаратқа құқыққа сыйымсыз қол жеткізу) және 207-баптарымен (Ақпараттандыру объектісінің жұмысын бұзу) жасанды бәсекелестік тәуекелін өзінде тасиды.

Осы коллизияны шешу үшін біз мынадай аражігін ажырату өлшемшартын ұсынамыз. Микрокредиттеу саласындағы онлайн алаяқтық кезінде жалған деректерді енгізу (мысалы, бөтен дербес деректерді пайдалану немесе жалған адамның «Face ID» өтуі) қаржы ұйымы интерфейсінің штаттық, қалыпты функционалдық параметрлері шеңберінде жүзеге асырылады. Жүйенің алгоритмі (скоринг) бұзуға, модификациялауға немесе технологиялық қиратуға ұшырамайды; ол штаттық режимде жұмыс істейді, бірақ легитимді түрде енгізілген, алайда мазмұны бойынша жалған ақпарат негізінде кредит беру туралы қате шешім қабылдайды. Мұнда кінәлінің мақсаты ретінде тек мүлікті

жымқыру ғана әрекет етеді.

Бұған қарама-қарсы, ҚР ҚК-нің 7-тарауындағы қылмыстар (компьютерлік саботаж) қауіпсіздік контурларын технологиялық еңсерумен сипатталады. ҚР ҚК-нің 205, 206 және 207-баптары бойынша объективтік жақ рұқсатсыз қол жеткізуді, хакерлік бұзуды, жүйенің бастапқы бағдарламалық кодын өзгертуді немесе серверлердің лог-файлдарын жоюды ұйғарады. Бұл жағдайда пиғыл ақпараттық инфрақұрылымның өзінің дербес игілік ретіндегі тұтастығын, құпиялылығын және қолжетімділігін бұзуға бағытталған.

Демек, ҚР Жоғарғы Соты Пленумының қаулысында мынадай түсіндірмені бекіту қажет: егер қаржы ұйымының қаражатын жымқыру стандартты пайдаланушы интерфейсін пайдалану арқылы (әлеуметтік инженерия, бөтен биометриялық немесе сауалнамалық деректерді ұсыну арқылы) жасалса, іс-әрекет ҚР ҚК-нің 7-тарауы бойынша қосымша саралаусыз, тек ҚР ҚК-нің 190-бабының тиісті бөлігі бойынша ғана сараланады. Егер жымқыру қорғау жүйелерін технологиялық бұзумен, банктің дерекқорларын құқыққа сыйымсыз модификациялаумен немесе ақпаратты жоюмен ұштасса, жасалған әрекет кибералаяқтық пен компьютерлік қылмыстардың идеалды жиынтығын құрайды.

Аралас құрамдардың аражігін ажыратумен қатар, ресми соттық түсіндіру деңгейінде кибержымқырулардың сатылылығын регламенттеудің өткір қажеттілігі туындады. Құқық қолдану практикасы бастапқы алдау ақша қаражатын тікелей иемденуге емес, құпия аутентификациялық ақпаратты (мобильді банкингтің CVV-кодтарын, PIN-кодтарын, SMS-парольдерін) алуға бағытталған жағдайлармен үнемі тап болады. Осыған байланысты ҚР Жоғары Сотының №6 қаулысын тікелей түсіндірмемен толықтыру мақсатқа сай: банктік және өзге де дербес шоттарға қол жеткізу кодтарын алдау немесе сенімді теріс пайдалану арқылы иемдену алаяқтыққа оқталу (оқталу) ретінде дербес сараласуға жатады, өйткені бұл әрекеттер электрондық активтерді кейіннен жасырын жымқыру үшін тікелей жағдайлар жасайды.

Ұсынылған материалдық-құқықтық реформаның практикалық салдарлары тұрақтандырушы сипатқа ие және салалық заңнамамен органикалық түрде синхрондалады. Нақтырақ айтсақ, «Микроқаржылық қызмет туралы» ҚРЗ-ның 3-2-бабы кредиттің алаяқтық жолмен ресімделгені анықталған кезде МҚҰ-ны клиенттің берешегін есептен шығаруға міндеттейді. Қаржы институтын залалдың тиісті субъектісі деп тану оған қылмыстық сот ісі шеңберінде шығынды тікелей киберқылмыскерден өндіруді талап етуге заңды құқық береді, әрі жалған міндеттеме бойынша жеке тұлғаларды ынтымақты жауаптылыққа негізсіз тартудың жолын кеседі.

Осы олқылықты жою прокурор мен тергеу судьясының өкілеттігін кеңейтуді объективті түрде қажет етеді. Мұның өзектілігі толық цифрландыру жағдайында анықтау және алдын ала тергеу органдарының процестік қызметінің заңдылығына жүргізілетін қадағалауды күшейту қажеттілігінен туындайды [179, 113 б.]. Осыған орай ҚР ҚПК-тің 193-бабын 19-1-бөлікпен толықтырып, прокурорға мынадай құзырет беру ұсынылады: «сотқа дейінгі тергеп-тексеру сатысында қылмыстық іс бойынша кредиттік ұйымды жәбірленуші деп тану және атына кредиттер заңсыз ресімделген адамдардан кредиттік міндеттемелерді

алып тастау туралы тергеу сотына өтінішхат енгізу». Тиісінше, ҚР ҚПК-тің 55-бабының 2-бөлігін тергеу судьясына: «прокурордың ұсынуы бойынша кредиттік ұйымды жәбірленуші деп тану және кредиттік құқықтық қатынастарға заңсыз тартылған адамдардан кредиттік міндеттемелерді алып тастау туралы мәселені қарау» өкілеттігін беретін 5-1-тармақпен толықтыру қажет. Мұндай конструкция жалған қарыздармен негізсіз ауыртпалық түскен азаматтардың құқықтарын қорытынды сот үкімі шығарылғанға дейін-ақ қалпына келтіреді.

Мамандандырылған саралаушы белгілерді алаяқтық туралы норманың конструкциясына енгізу іс-әрекеттің іс жүзіндегі цифрлық моделі мен оны заңдық бағалау арасындағы пайда болған гносеологиялық олқылықты жояды. Дәл саралау институттарды қудалауды дербес инициациялауға ынталандыра отырып және жасанды латенттілікті түбегейлі төмендете отырып, қылмыстық заңның трансұлттық қаржылық ортаның шынайылығына терең бейімделуін қамтамасыз етеді. Анықталған заңдылықтар қаржы секторының мүдделерін қорғау және ұсынылған материалдық-құқықтық новеллаларды іске асыру оларды дәлелдеудің тиісті рәсімдік тетігімен қатаң синхрондаусыз объективті түрде мүмкін емес екенін сенімді түрде дәлелдейді. Бұл факт тергеп-тексерудің бейімделген процестік қамтамасыз етілуін егжей-тегжейлі әзірлеу қажеттілігін туындатады.

Онлайн алаяқтық туралы істер бойынша МҚҰ жәбірленушілер деп тануды негіздейтін жаңа материалдық-құқықтық конструкцияны енгізу өзінің қатаң процестік қамтамасыз етілуін императивті түрде талап етеді. ҚР ҚПК нормаларына негізделетін сотқа дейінгі іс жүргізудің қолданыстағы моделі тарихи тұрғыдан тұлғааралық физикалық өзара іс-қимылдарға бағдарланған және қашықтықтан кредиттеудің цифрлық ерекшелігін объективті түрде ескермейді. Заң жәбірленушіні қылмыспен мүліктік немесе өзге де зиян келтірілген тұлға ретінде айқындайды, алайда құқық қолдану практикасы жүйелі іркілісті көрсетеді: тергеу қаржылық шығындардың нақты субъектісі – кредиттік ұйымның өзін толығымен елемей, дербес деректері компрометацияланған жеке тұлғаны формальды түрде жәбірленуші деп таниды. Осы құқықтық бұрмалаудың табиғатын бағалай отырып, М.С. Бисалиев қаржы институтының дербес жәбірленуші ретіндегі процестік мәртебесін нормативтік бекітудің болмауы абсолютті құқықтық белгісіздікті туындататынын және сот ісін жүргізуге қатысушылардың рөлдерін фатальды түрде бұрмалайтынын тұжырымдайды [16, 104-105 б.]. Проблемаға өзге ұстанымдар тұрғысынан А.И. Зазулин келеді, ол субъективті мәртебелік олқылық объективті санаттардың неғұрлым терең тапшылығының салдары ғана болып табылатынын дәлелдейді: құқық қолданушы виртуалды іздерді бағалау үшін заңды инструментарийден айырылған, бұл тұтастай алғанда тергеп-тексеруді бұғаттайды [114, 14 б.]. Өз кезегінде, Р.И. Оконенко электрондық дәлелдемелерді тікелей заңдастыра отырып, барлық цифрлық сегмент үшін тұтас ұғымдық аппаратты қалыптастыруды талап етіп, жаһандық инфрақұрылымдық тәсілді табанды түрде ұстанады [172, 141 б.]. Ұсынылған ғылыми ұстанымдарды талдау зерттеу деңгейлерінің айырмашылығын көрсетеді: егер М.С. Бисалиев субъективтік жаққа (қатысушылардың мәртебесіне) фокусталса, А.И. Зазулин қолданбалы

инструменталдық тапшылықты бөліп көрсетсе, онда Р.И. Оконенко макрожүйелік тұжырымдамалық проблеманы тұжырымдайды. Біздің ойымызша, аталған ақаулар оқшауланған түрде әрекет етпейді, қайта бірыңғай гносеологиялық вакуумды құрайды: МҚҰ мәртебесін легитимдеу цифрлық дәлелдеменің беймәтериалдық табиғатын бір мезгілде нормативтік танусыз тұжырымдамалық тұрғыдан мүмкін емес. Демек, ҚР ҚПК-ге мамандандырылған ұғымдық аппаратты енгізу жаңа корпоративтік жәбірленушіні де, дәлелдеудің ерекше объектісін де синхронды түрде айқындай отырып, кешенді сипатқа ие болуға тиіс.

МҚҰ-ның процестік мәртебесін іске асыру электрондық дәлелдемелік ақпаратты тіркеп-белгілеу тосқауылдарын еңсеру қажеттілігімен ажырамас байланысты. Дәлелдемелерді жинаудың дәстүрлі тетіктері автоматтандырылған скорингтік жүйелермен генерацияланатын ұшпа компьютерлік деректерді (лог-файлдарды, транзакциялық хэштерді, IP-мекенжайларды) сақтау міндеті алдында мүлдем дәрменсіз болып шығады. Құбылмалы іздерді құтқару тактикасын талдай отырып, А.Н. Колычева темпоральды фактор абсолютті басымдыққа ие деп мәлімдейді: деректерді аса жылдам тіркеп-белгілеу оларды сақтаудың баламасыз шарты ретінде әрекет етеді, өйткені кез келген процестік кідірістер айғақтардың орны толмас жоғалуына әкеледі [126, 27-28 б.]. Баламалы тәсілді А.А. Толыбаева бастаған авторлар ұжымы ұсынады, ол технологиялық басымдықты дәлелдейді: тіркеудің автоматтандырылған жүйелерін пайдалануды нормативтік бекітусіз және алынатын массивтің қатаң криптографиялық тұтастығын қамтамасыз етусіз жылдамдықтың маңызы жоқ [98, 134 б.]. Ұсынылған көзқарастарды салыстыру процестік жеделдік талабы мен техникалық мінсіздік императиві арасындағы тұжырымдамалық қақтығысты көрсетеді. Авторлық тәсілді негіздей отырып, бұл ұстанымдарды бірыңғай процестік алгоритмге синтездеу қажет. Жеделдік пен криптографиялық тұтастық тікелей шлюзді құру арқылы процестік тұрғыдан интеграциялануға тиіс: Ұлттық Банктің Антифрод-орталығын СДТБТ ақпараттық жүйесімен платформалық интеграциялау цифрлық артефактыларды қылмыстық іс материалдарына автоматты және легитимді түрде трансляциялауды жүзеге асыруға мүмкіндік береді. Бұл ұсыныстың практикалық маңызы оның ҚР Бас прокуратурасы мен Ұлттық Банкінің қызметіне дереу енгізу үшін ұсынылуында жатыр. Осындай алгоритммен ақпаратты СДТБТ-да дер кезінде тіркеп-белгілеу іздерді деградациядан аман алып қалумен шектелмейді; ол бүкіл дәлелдеу процесінің нәтижелілігін арттыратын тікелей катализаторға да айналады.

Дегенмен тергеу органдары мен банктердің антифрод-жүйелерін ұштастырудың осы құқықтық идеясы нақты технологиялық хаттамалармен әрі банк құпиясын қорғаудың қатаң кепілдіктерімен қатар жүруге тиіс. Тергеу органдары мен екінші деңгейдегі банктердің антифрод-жүйелерін тиімді интеграциялау үшін озық халықаралық АТ-шешімдерінің сәулеттік тәжірибесін имплементациялаған жөн – атап айтқанда, Еуропалдың «SIRIUS» платформасын (құқық қорғау органдарына арналған электрондық дәлелдемелерді трансшекаралық алу платформасы) және шетелдік қаржылық барлаудың STRO жүйесін (күмәнді транзакцияларды тіркеу жүйесі) [174, 148-149 б.].

Технологиялық тұрғыдан бұл ведомствоаралық өзара іс-қимыл бірыңғай интеграциялық торап («Data Hub») арқылы жүзеге асырылуы тиіс. Мұндай экожүйеде ақпарат алмасу процесі автоматтандырылған жүйелер арасында қауіпсіз REST API хаттамаларын қолдану арқылы, деректерді машиналық оқуға болатын JSON немесе XML форматтарында шифрлап беру негізінде құрылуы шарт [98, 126 б.]. Бұл ретте тергеушілердің банк деректеріне қол жеткізу шектері бағдарламалық деңгейде қатаң шектеледі: құқық қорғау органдары азаматтардың барлық шоттарына жаппай рұқсат алмайды; оларға тек антифрод-жүйелермен алаяқтық маркері берілген немесе қылмыстық іс аясында СДТБТ ресми тіркелген нақты транзакциялар бойынша ғана нүктелі ақпарат беріледі. Банк құпиясы мен дербес деректерді қорғаудың ұлттық заңнамалық талаптарын бұлжытпас орындау мақсатында жүйеге кіру міндетті түрде көпфакторлы аутентификациямен қорғалып, әрбір тергеушінің сұранымы (оның негіздемесі, уақыты және көлемі) қорғалған лог-файлдарда (өзгертілмейтін цифрлық аудит журналдарында) автоматты түрде тіркелуі қажет. Бұл тетік, бір жағынан, қылмыстық іс бойынша деректерді лезде алуды қамтамасыз етіп, ұзаққа созылатын бюрократиялық кедергілерді жойса, екінші жағынан, деректердің рұқсатсыз шығып кетуін болдырмайды және банк клиенттерінің конституциялық құқықтарының бұзылмауына толық технологиялық кепілдік береді

Тіркеп-белгілеудің технологиялық стандарттары сотқа дейінгі іс жүргізуді инициациялаудың архаикалық нормаларымен объективті түрде қақтығысқа түседі. ҚР ҚПК-тің 179-бабында бекітілген қылмыстық құқық бұзушылықтар туралы арыздарды қараудың консервативті рәсімі трансұлттық желілерде жымқырылған активтерді шығарудың гипердинамикасымен апатты түрде сәйкес келмейді. Осы процестік диссонансты салыстырмалы-құқықтық аспектіде зерттей отырып, А.Б. Сабырбаева Өзбекстан Республикасының қылмыстық іс жүргізу заңнамасы мысалында қатаң регламенттелген тергеуге дейінгі тексеру жоғары технологиялық деликттерді ашу жолында еңсерілмейтін бюрократиялық тосқауыл ретінде әрекет ете отырып, айғақтарды жинау процесін жасанды түрде тежейтінін тұжырымдайды [103, 162 б.].

Осы тосқауылды еңсеру құралы ретінде қаржы мониторингі жүйелері генерациялайтын деректердің құқықтық маңызын тұжырымдамалық түрде қайта қарау ұсынылады. Сөз билік өкілеттіктерін жекеше құрылымдарға жол берілмейтіндей беру (аутсорсинг) туралы емес, цифрлық аномалиялардың объективті криминалистикалық маңыздылығын тану туралы болып отыр. Қашықтықтан децепция жағдайында дәл МҚҰ және екінші деңгейлі банктер қауіпсіздік қызметтерінің (антифрод-жүйелерінің) автоматтандырылған есептері ерікті азаматтық-құқықтық мәміле елесін бұзатын объективті техникалық индикатор ретінде әрекет етеді.

Осыған байланысты ҚР ҚПК-тің 179-бабын қолдану тәртібін регламенттейтін нормативтік ұйғарымдарды аса маңызды императивті ерекшелікпен толықтыру ұсынылады. Жәбірленушінің арызы объективті компрометация маркерлерімен (антифрод-жүйелердің сигналдарымен) сүйемелденетін немесе расталатын жағдайларда, «азаматтық-құқықтық даудың» бар екендігі уәждері бойынша арыздарды тіркеуге тыйым салу қолданылмауға

тиіс.

Қылмыстық қудалау шектерін негізсіз кеңейту тәуекелін болдырмау үшін болуы криминалдық пиғылды презюмпциялайтын және СДТБТ-да дереу тіркеуді талап ететін объективті техникалық триггерлердің түпкілікті тізбесін бекіту қажет:

– бірыңғай немесе алмастырылған желілік тораптан кредиттеуге сұрау салуларды жаппай автоматтандырылған генерациялау;

– тікелей қаржылық транзакцияны авторизациялау кезінде маршруттауды ауыстыру алгоритмдерін (VPN/Proxy/TOR) қолданудың техникалық расталған фактісі;

– бастамашы құрылғысы геолокациясының авторизацияланған пайдаланушының верификацияланған биометриялық параметрлерімен сыни сәйкессіздігі.

Мұндай триггерлердің болуы, тіпті егер сырттай транзакция легитимді мәміле белгілеріне ие болса да, техникалық іркілісті немесе азаматтық дауды киберқылмыстан ажыратуға мүмкіндік береді. Тек осындай нормативтік ерекшелік «72 сағат» алгоритмін процестік кідірістерсіз іске қосуға мүмкіндік береді.

ҚР ҚПК-ні жаңғыртудың тұжырымдалған векторы салыстырмалы-құқықтық конвергенция қағидаттарымен объективті түрде корреляцияланады. Халықаралық стандарттар, оның ішінде БҰҰ Киберқылмысқа қарсы конвенциясының ұйғарымдары компьютерлік деректерді шұғыл жинаудың процестік алгоритмдерін белгілеу қажеттілігін императивті түрде бекітеді. Осы аспектіні талдай отырып, Д.В. Завьялова озық шетелдік құқықтық тәртіптерде қаржы институттарын жәбірленушілер деп тану және төлем жүйелерінің ерекшелігін қатаң нормативтік есепке алу өзінің қолданбалы тиімділігін дәлелдеп қойғанына назар аударады [90, 46-47 б.]. Осы доктриналық пікірді есепке алу ұсынылып отырған ұлттық өзгерістер жасанды конструкциялар болып табылмайтынын, қайта тиімді трансшекаралық өзара іс-қимыл үшін берік іргетас құра отырып, жаһандық трендтерге органикалық түрде үйлесетінін растайды.

Жүргізілген талдаудың нәтижелерін қорыта отырып, қатаң тұжырымдамалық логиканы құру қажет: МҚҰ-ның нақты залал субъектісі ретіндегі мәртебесін легитимдейтін материалдық-құқықтық реформа жаңа дефинацияларды, тіркеп-белгілеудің электрондық стандарттарын және тергеп-тексеруді жеделдетіп инициациялау алгоритмдерін енгізу түріндегі симметриялық рәсімдік бейімдеуді баламасыз түрде талап етеді. Анықталған заңдылықтар қылмыстық-процестік нысан желілік жымқырулардың қаржылық ерекшелігін терең көрсетуге тиіс екенін дәлелдейді, өйткені дәлелдеудің консервативті рәсімдерін жаңғыртусыз материалдық құқықты іске асыру тек декларативті болып қалады. Сонымен бірге әзірленген процестік институттардың табысты жұмыс істеуі объективті түрде тек ҚПК шеңберімен ғана шектеле алмайды. Бұл факт аралас реттеушілік заңнаманы жетілдіру жолдарын кешенді талдау және өзара іс-қимылдың қағидатты түрде жаңа ведомствоаралық алгоритмдерін құрастыру қажеттілігін туындатады.

Онлайн алаяқтықтың кешенді және жоғары технологиялық табиғаты оны

тергеп-тексеру тетігін таза қылмыстық-процестік реттеудің тар шеңберінен объективті түрде шығарады. Банк операцияларының құпиясына кепілдік беретін «Қазақстан Республикасындағы банктер және банк қызметі туралы» ҚРЗ-ның 50-бабы [180] базалық тосқауыл ретінде әрекет етеді. Қаржылық ақпаратты ашудың қатаң формализацияланған тәртібі кибержымқыруларды жасаудың трансұлттық жылдамдығымен сыни қайшылыққа түседі. Осы диссонансты талдай отырып, С.М. Голятина деректерді алудың қолданыстағы рәсімдері дәлелдемелік базаның орны толмас жоғалуына әкеле отырып, қылмыстардың динамикасына тұжырымдамалық түрде сәйкес келмейтінін тұжырымдайды [111, 101-102 б.]. Бұл проблеманы шешу ғылыми пікірталас тудырады. Р.Б. Джилкишиев мерзімдерді 48 сағатқа дейін қысқарта отырып, тергеудің цифрлық транзакцияларға соттың санкциясынсыз, басымдықпен қол жеткізу тетіктерін енгізу арқылы құпияны түбегейлі жұмсартудың өткір қажеттілігін дәлелдейді [57, 155 б.]. Олармен қағидаттық пікірталасқа М.С. Бисалиев түседі, ол мәліметтердің бақылаусыз компрометациялануына жол берілмейтінін әділетті түрде атап өтеді және дербес деректерді қорғаудың технологиялық кепілдіктерінің тергеу жеделдігінен басымдығын талап етеді [16, 63-64 б.].

Кибералаяқтықты тергеп-тексеру жағдайында қатаң банк құпиясы режимін еңсерудің ымыралы және жоғары тиімді құралы ретінде қаржы мониторингі тетіктерін интеграциялайтын Индонезияның құқық қолдану практикасы әрекет етеді. Тетік қаскөйлердің әрекеттерін құқықтық қайта саралауда және e-commerce платформаларындағы алаяқтық кезінде электрондық дәлелдемелерді жинау үшін негізгі процестік драйвер ретінде Кірістерді заңдастыруға (жылыстатуға) қарсы іс-қимыл туралы заңды (Law No. 8 of 2010 Concerning the Crime of Money Laundering) қолдануда жатыр [181]. Дәлелдемелерді жинау процесі айтарлықтай трансформацияланады: Орталық банктің жоғары инстанциялары арқылы банк құпиясына қол жеткізуді ұзақ иерархиялық келісудің орнына, полицияның аумақтық органының басшысы реттеушінің жергілікті өкіліне тікелей сұрау салу жібереді. Жылыстатуға қарсы заңнаманы кибержымқыруларға қолданудың заңдық маңызы арнайы нормаға (Заңның 73-бабы) сәйкес қосымша материалдандыруды талап етпейтін дәлелдемелердің дербес түрі деп танылатын цифрлық дәлелдемелерді (транзакциялар тарихын, аутентификация журналдарын, биллингтерді) жедел, легитимді алуда жатыр. Отандық сотқа дейінгі тергеп-тексеруді жетілдіру үшін бұл тәжірибе онлайн алаяқтықтың цифрлық маркерлері болған кезде тергеудің екінші деңгейдегі банктердің дерекқорларына оңайлатылған, басымдықпен қол жеткізу құқығын бекітетін ҚР жылыстатуға қарсы заңнамасына түзетулер енгізудің орындылығын көрсетеді.

Ұсынылған ұстанымдарды талдау тергеу жылдамдығының императиві мен ақпараттық қауіпсіздік презумпциясы арасындағы қақтығысты көрсетеді. Біздің ойымызша, бұл тәсілдерді синтездеу қажет: институционалдық кідірісті еңсеру аралас заңнамаға транзакциялық деректерге соттан тыс шұғыл қол жеткізу тетігін енгізуді талап етеді, ол міндетті кейінгі прокурорлық бақылаумен және сұрау салулардың қатаң цифрлық есептілігімен қатаң теңестірілуге тиіс. Мұндай теңгерім жеке өмірге қолсұғылмаушылықтың конституциялық кепілдіктерін бұзбай, активтерді шығарудың жолын кесуге мүмкіндік береді.

Уақытша кідірісті еңсеру автоматтандырылған ақпараттық алмасудың жаңа салааралық тетіктерін құруды баламасыз түрде талап етеді. «Төлемдер және төлем жүйелері туралы» ҚРЗ-ның қолданыстағы 25-1-бабы алаяқтық транзакциялар бойынша деректер алмасу орталығының жұмыс істеуін формальды түрде бекітеді, алайда сұрау салуларды қолмен немесе жартылай автоматты түрде өңдеуді сақтау өткізу қабілетінің объективті шектелуін қамтиды. Осы инфрақұрылымдық алшақтықты зерттей отырып, А.С. Камко назарды құрылымдық ақаулыққа аударады: құқық қорғау органдары, екінші деңгейдегі банктер және цифрлық платформалар арасындағы тұрақты көлденең өзара іс-қимыл арналарының болмауы жедел ден қоюды жасанды түрде бұғаттайды [36, 152-153 б.]. Проблемаға өзге ұстанымдар тұрғысынан И.А. Орешков келеді, ол жоғары латенттіліктің бастапқы себебі ретінде арналардың болмауы ғана емес, қайта қаржы нарығы субъектілерінің компрометация маркерлерін үздіксіз беру үшін «нақты уақыт» (real-time) технологиялық модельдерін қолдану жөніндегі нормативтік міндетінің болмауы әрекет ететінін дәлелдейді [115, 58 б.]. Ғылыми көзқарастарды салыстыру проблеманы локализациялаудағы айырмашылықты көрсетеді: А.С. Камко құрылымдық байланыстардың тапшылығын диагностикалайды, ал И.А. Орешков технологиялық динамиканың тапшылығын айқындайды. Анықталған қайшылықты шеше отырып, технологиялық жеделдетусіз құрылымдық интеграцияның мағынасы жоқ екенін негіздеу қажет. Демек, бейінді заңнама клиенттің келісімінсіз сыни маңызды деректермен лезде ведомствоаралық алмасуды жүзеге асыру құқығын бере отырып, орталықтандырылған антифрод-платформалардың жұмысын легитимдейтін императивті нормамен толықтырылуға тиіс. Автоматтандырылған алмасу жүйелерін енгізу аномальді транзакцияны тіркеп-белгілеу мен қаражатты процестік бұғаттау арасындағы ажырамас байланысты қалыптастырады.

Мұндай архитектураны мемлекеттік деңгейде құру Қытай Халық Республикасында «Телекоммуникациялық және желілік алаяқтыққа қарсы іс-қимыл туралы» (Anti-Telecom and Online Fraud Law) Заңды қабылдау арқылы табысты апробацияланды. Заңның тетігі тежемелік пен тепе-теңдіктің қатаң жүйесін белгілеуге негізделеді, бұл ретте интернет-қызметтер провайдерлеріне, байланыс операторларына және қаржы институттарына олардың тәуекелдерді бақылаудың ішкі жүйелерін Үлкен деректердің ұлттық антифрод-платформасымен интеграциялау бойынша императивті міндет жүктеледі [182]. Процестік аспектіде бұл банктер мен IT-компаниялардың алдын ала сот санкциясынсыз сыни дәлелдемелік телеметрияны (IP-мекенжайларды, MAC-мекенжайларды, терминалдардың локацияларын) өздігінен жинай отырып, күдікті транзакцияларға автоматты режимде мониторингті жүзеге асыруға, ауыстырылған нөмірлерден (spoofed numbers) шалынған қоңырауларды бұғаттауға және аномальді аккаунттарға қызмет көрсетуді тоқтатуға міндетті екенін білдіреді. Мұндай нормативтік конструкцияның заңдық маңызы орасан зор: ол алаяқтық трафикті ұстап қалу бойынша шаралар қабылдамағаны үшін бизнеске тікелей әкімшілік және қаржылық жауаптылықты жүктей отырып, жекеше сектордың цифрлық дәлелдемелерді нақты уақыт режимінде жинауын легитимдейді. Осы модельді зерделеу жекеше технологиялық компанияларды

ақпаратты пассивті сақтаушылардан оларға криминалистикалық маңызды ақпаратты автоматтандырылған түрде тіркеп-белгілеу міндеті жүктелген алаяқтыққа қарсы іс-қимылдың активті субъектілеріне конвертациялау мақсатында ұлттық әкімшілік және салалық заңнаманы қайта қарау қажеттілігі туралы қорытынды жасауға мүмкіндік береді.

Құрылатын қорғау жүйесінің ажырамас контуры ретінде киберқылмыстылықтың базалық инфрақұрылымын құрайтын цифрлық активтер мен коммуникациялық сервистердің айналымын қатаң нормативтік реттеу әрекет етеді. Ұлттық заңнамада фрагменттік құралдар қазірдің өзінде қамтылған: «Қазақстан Республикасындағы цифрлық активтер туралы» ҚРЗ-ның 12-1-бабы қамтамасыз етілмеген активтердің айналымы режимін енгізеді, «Қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл туралы» ҚРЗ-ның 16-бабы күдікті криптоәмияндар тізілімін регламенттейді, ал «Байланыс туралы» ҚРЗ-ның 15-4-бабы алаяқтық нөмірлерді бұғаттауға міндеттейді. Алайда, бұл нормаларды іске асыру тетігі түпкі пайдаланушыларды толық сәйкестендірудің болмауымен салдандырылады. Осы олқылықты бағалай отырып, А.А. Рудых байланыс операторлары мен хостинг провайдерлеріне қойылатын толыққанды реттеушілік талаптардың болмауы анонимді криминалдық қызмет үшін қолайлы пассивті «сұр аймақты» құрайтынын тұжырымдайды [60, 168-169 б.].

Ведомствоаралық өзара іс-қимыл шеңберінде байланыс саласындағы уәкілетті мемлекеттік органдар қатаң бөгеттік бақылау алгоритмін іске асыруға міндетті.

Біріншіден, тіркелмеген немесе телнұсқаланған IMEI-кодтарымен жұмыс істейтін мобильді құрылғыларды бұғаттау тәртібін қайта қарау және қатаңдату талап етіледі.

Екіншіден, ұлттық байланыс операторларына қазақстандық ішкі нөмірлеуге бүркемеленетін SIP-шақыруларды сөзсіз кері қаға отырып, шетелден келіп түсетін фродуленттік SIP-телефониялық трафикті синхронды түрде бұғаттау бойынша императивті техникалық міндет жүктелуге тиіс.

Пассивті ортаны тұжырымдауға баламалы тәсілді бірқатар ғалымдар ұсынады, олар агрессивті нормашығармашылықтың қажеттілігін: мүлдем барлық цифрлық сервистерді (оның ішінде мессенджерлер мен криптобиржаларды) пайдаланушыларды сөзсіз биометриялық және құжаттық сәйкестендіруге қатаң императивті талаптар енгізуді [115, 165-166 б.] және операторларға лог-файлдарды ұзақ уақыт (12 айға дейін) сақтау және тергеуге дереу ұсыну бойынша тікелей міндет белгілеуді негіздейді [57, 93-94 б.]. Осы тәсілдерден көрініп тұрғандай, талап етілетін араласу тереңдігінде айырмашылық бар: Б.Э. Шавалеев проблеманы инфрақұрылымдық олқылықтар деңгейінде тіркеп-белгілейді, ал Р.Б. Джилкишиев цифрлық орта субъектілеріне толық активті бақылау орнатуды талап етеді. Біздің ойымызша, қатаң шаралардың баламасыздығын тану қажет. Цифрлық сервистер олардың иелері үшін жария-құқықтық міндеттерді императивті түрде бекіту арқылы құқықтық анонимділік жай-күйінен шығарылуға тиіс. Тек өтпелі биометриялық сәйкестендіру ғана тергеу аппаратын процестік дәлелдеу үшін қажетті

релевантты артефактылармен қамтамасыз етуге қабілетті.

Салааралық коллизияларды зерттеу нәтижелерін қорыта отырып, бағдарламалық тезисті тұжырымдау қажет: онлайн алаяқтыққа қылмыстық-процестік қарсы іс-қимылдың тиімділігі аралас реттеушілік заңнаманың жай-күйіне абсолютті тәуелділікте болады. Егер қаржылық, ақпараттық және әкімшілік құқық нормалары ведомстволық тосқауылдарды сақтай отырып, оқшауланған түрде жұмыс істейтін болса, жобаланған процестік реформалар өзінің эвристикалық әлеуетін кепілді түрде жоғалтады. Құқықтық тетіктерді, технологиялық антифрод-сүзгілерді және әкімшілік тыйым салуларды терең тұжырымдамалық интеграциялау қаскөйлерді уақыт факторынан және технологиялық анонимділіктен айырудың жалғыз шарты ретінде әрекет етеді. Әзірленген қылмыстық-құқықтық, процестік және салааралық новеллалар кешенін практикалық іске асыру цифрлық ортаны қорғаудың монолитті ұлттық жүйесін қалыптастырады.

Әзірленген шаралар кешенін практикалық іске асыру егжей-тегжейлі заңжобалық жол картасын қалыптастыруды баламасыз түрде талап етеді. Жаңғырту іргелі кодификацияланған актілерді қозғайтындықтан, фрагменттік құқық қолдануға жол берілмейді. Атап айтқанда, бастапқы сатыда скорингтік жүйелерді алдауды криминализациялау және заңды тұлғаларды жәбірленушілер деп тану бөлігінде ҚР ҚК-нің 190-бабын, сондай-ақ цифрлық артефактыларды дереу тіркеп-белгілеу рәсімдерін заңдастыру үшін ҚР ҚПК-тің 120 және 122-баптарын өзгерту талап етіледі. Осы реформалау векторларын бағалай отырып, А.Д. Фокин мемлекеттік ден қоюдың құқықтық және криминалистикалық шараларын қатаң синхрондайтын прогностикалық модельді құру қажеттілігін дәлелдейді [41, 18-19 б.]. Өз кезегінде, А.А. Толыбаева бастаған авторлар ұжымы процесті жүйелі түрде бейімдеусіз нормаларды нүктелі түрде қолдануды жоққа шығаратын реформалардың көпдеңгейлі иерархиясын құру талабын алға тартады [98, 130 б.]. Келтірілген пікірлерді талдау акценттерді қоюдағы айырмашылықты көрсетеді: А.Д. Фокин салааралық прогностикалық синхрондауды (құқық және криминалистика) басты орынға қояды, ал А.А. Толыбаева қатаң процесішілік құрылымдық иерархияны талап етеді. Біздің ойымызша, аталған тәсілдер үш кезеңдік алгоритмге интеграциялануға тиіс. ҚР ҚК мен ҚР ҚПК-нің бастапқы кодификациялық реформасы аралас реттеуді қайталама синхрондаусыз, атап айтқанда «Төлемдер және төлем жүйелері туралы» ҚРЗ-ның 25-1-бабы тәртібімен күдікті операцияларды бұғаттау бойынша Ұлттық Банкке құзырет берусіз объективті түрде өміршең емес, бұл түпкі нәтижесінде егжей-тегжейлі ведомстволық криминалистикалық әдістемелерді бекітумен бекемделеді.

Бекітілген заңнамалық новеллалар озат институционалдық қайта құруларды жүргізусіз сөзсіз декларативтік ұйғарымдар мәртебесіне ие болады. ҚР ҚПК-тің 58-бабында бекітілген сотқа дейінгі тергеп-тексеру субъектілерінің өкілеттіктерін кеңейту құқық қолдану аппаратының өзін сапалы түрде өзгертуді талап етеді. Осы тосқауылды зерттей отырып, К.О. Карабеков бейінді жоғары технологиялық бөлімшелерді («Киберпол» мақсатты тобының моделі бойынша) құрудың және тергеу кадрларының гибридтік IT-құзыреттерді иемденуі үшін

оларды қарқынды қайта даярлаудың императивті қажеттілігін негіздейді [17, 138 б.]. Ішкі ведомстволық тәсілмен өткір пікірталасқа М.С. Бисалиев түсіп, қаржылық реттеушілермен және ИТ-сектормен тікелей ведомствоаралық өзара іс-қимылдың қатаң тетіктерін құрусыз кез келген, тіпті ең озық тергеу бөлімшелерінің оқшауланған жұмысы тұжырымдамалық тұрғыдан дәрменсіз екенін үзілді-кесілді мәлімдейді [16, 130-131 б.]. Ұсынылған көзқарастарды салыстыру айқын тұжырымдамалық айырмашылықты көрсетеді: бірінші автор проблеманы шешуді тергеу органдарының ішкі кадрлық-құрылымдық қайта құрылуында локализациялайды, ал екіншісі шығу жолын сыртқы автоматтандырылған ақпараттық контурларды қалыптастырудан көреді. Авторлық тәсілді негіздей отырып, осы бағыттардың бөлінбестігін тану қажет. Институционалдық дайындық тек жоғары білікті тергеу кадрларының және СДТБТ мен Антифрод-орталық арасында автоматтандырылған деректер алмасудың бірыңғай архитектурасын құрудың симбиозымен ғана қамтамасыз етіледі.

Ұсынылған қайта құрулардың архитектурасында абсолютті басымдық «Микроқаржылық қызмет туралы» ҚРЗ-ның 3-бабымен реттелетін МҚҰ сегментіне беріледі. Бұл сектор онлайн-жымқырулардың неғұрлым деструктивті схемаларын шоғырландыра отырып, криминалдық белсенділіктің эпицентрі ретінде әрекет етеді. Сегменттің ерекшелігін талдай отырып, А.А. Агарко проблеманың өзегі өздерінің хабарынсыз мәмілелерге қашықтықтан тартылатын азаматтардың дербес деректерін жаппай компрометациялау болып табылатынын дәлелдей отырып, назарды қылмыстың микродеңгейлік механикасына аударады [142, 10 б.]. Қағидаттық өзге ұстанымдар тұрғысынан проблеманы макроэкономикалық деңгейде бағалайтын П.А. Гоибназарзода әрекет етеді: кредиттік алаяқтық жекелеген адамдарға ғана емес, сонымен қатар тұтастай алғанда мемлекеттің қаржы жүйесінің іргелі тұрақтылығына қатер төндіретін орасан зор жиынтық мүліктік нұқсанды генерациялайды [25, 218 б.]. Анықталған ұстанымдардың алшақтығы айқын: А.А. Агарко қолсұғушылық инструментарийін (субъект деректерінің жылыстауын) зерттейді, ал П.А. Гоибназарзода кредиттік институттар үшін жаһандық экономикалық салдарларды диагностикалайды. Бұл тәсілдерді синтездей отырып, авторлық ұстанымды қалыптастыра отырып, мынаны тұжырымдау қажет: макроэкономикалық қатерді бейтараптандыру микродеңгейлік инструментарийді бұлтартпай бұғаттау арқылы ғана мүмкін болады. Алданған МҚҰ мәртебесін толыққанды жәбірленушіге трансформациялау азаматтарды жалған қарыздардан босату туралы «Микроқаржылық қызмет туралы» ҚРЗ-ның 9-2-бабын бір мезгілде қолдана отырып, әлеуметтік әділеттілікті қалпына келтіріп қана қоймайды, сонымен қатар осы қаржы институтына бағдарланған криминалдық схемалардың экономикалық рентабельділігінің өзін бұзады.

Қаралып отырған жол картасын енгізу қатаң экономикалық верификациялауға жатады. Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024-2028 жылдарға арналған тұжырымдамасында бекітілген ресми статистика сыни теңгерімсіздікті көрсетеді: өтеу деңгейі 6,3% болған кезде залал ондаған миллиард теңгемен есептеледі [3]. Реформалардың рентабельділік

өлшемшарттарын бағалай отырып, П.С. Пастухов жаңғыртудың экономикалық дәрменділігі қылмыстық-процестік дәлелдеудің транзакциялық және операциялық шығындарын түбегейлі барынша азайту қабілетімен айқындалады деген ұстанымды негіздейді [99, 533 б.]. Таза процестік үнемдеуге қарама-қарсы В.В. Поляков реституцияның абсолютті басымдығының телеологиялық қағидатын алға тартады: тиімділік бұғаттау рәсімдерінің жеделдігі есебінен заңды экономикаға қайтарылған көлеңкелі капиталдардың көлемімен ғана айқындалады [154, 141-142 б.]. Ғалымдардың пікірлерін салыстыру метрикалар қақтығысын айғақтайды: ішкі процестік ресурстарды үнемдеу өлшемшарты (П.С. Пастухов) жымқырылған активтерді сыртқы қайтару өлшемшартына (В.В. Поляков) қарсы. Демек, цифрландыру жағдайында бұл метрикалар берік себеп-салдарлық байланысты құрайды деп қорытынды жасау қажет. Цифрлық дәлелдемелерді легитимдеу (ҚР ҚПК-тің 42-1-бабы) және істерді ресурсты көп қажет ететін тоқтата тұру фактілерін барынша азайту (ҚР ҚПК-тің 45-бабы) арқылы ішкі шығындарды қысқарту бөлінген мүлікке дереу тыйым салу үшін сыни қажетті (ҚР ҚПК-тің 161-бабы) жүйелік әлеуетті босатады.

Материалдық-құқықтық және процестік аспектілердің жүргізілген синтезінің нәтижелерін қорыта отырып, мынаны тұжырымдау қажет: кибержымқыруларды сотқа дейінгі тергеп-тексеру дағдарысын еңсеру жүйелі халықаралық конвергенциясыз мүмкін емес. Транзакцияларды банктік ордерлермен соттан тыс бұғаттау институтын енгізуді және провайдерлердің серверлеріне экстерриториялық қол жеткізуді қоса алғанда, озық шетелдік практикаларды синтездеу ҚР ҚПК-ні жаңғырту үшін негізделген траекторияны қалыптастырады. Ұсынылған аналитикалық парадигманы толық ауқымды енгізу орны толмас цифрлық шығындарды инертті хаттамалаудан криминалдық транзакциялардың жолын кесудің және цифрлық дәлелдемелерді сенімді тіркеп-белгілеудің проактивті, жоғары автоматтандырылған архитектурасына тұжырымдамалық өтуді қамтамасыз етеді.

Қорытынды

Онлайн алаяқтық тетіктерін талдауға және оған қарсы іс-қимылдың құқықтық негіздерін әзірлеуге арналған жүргізілген диссертациялық зерттеуді қорытындылай отырып, бірқатар іргелі қорытындыларды тұжырымдау қажет. Репрезентативті эмпирикалық базаға және компаративистік талдау нәтижелеріне сүйене отырып, жұмыста Қазақстан Республикасының қылмыстық және қылмыстық-процестік заңнамасын жоғары технологиялық криминалдық белсенділік жағдайларына терең бейімдеудің объективті қажеттілігі дәлелденді. Осыған байланысты, зерттеу нәтижелерін келесі тұжырымдамалық қағидаларға топтастыруға болады:

1) Ақпараттық-коммуникациялық технологияларды енгізу тіркелетін қылмыстар санының ауқымды өсуін ғана емес, алаяқтықтың мәнінің жүйелі трансформациясын туындатты. Тікелей физикалық байланыс пен тікелей алып қоюға негізделген классикалық жеке-материалдық парадигмадан күрделі жүйелі-виртуалды парадигмаға өту жүзеге асты. Сапалық өзгеріс мыналардан көрініс табады:

– «байланыс → алдау → мүлікті беру» жымқырудың классикалық формуласы қашықтықтан алгоритмдермен алмастырылады. Ендігі жерде ықпал ету жанама түрде жүзеге асырылады, соның нәтижесінде құрбан транзакцияны өзі жасайды, немесе қылмыскер физикалық өзара іс-қимылды толығымен жоққа шығара отырып, банктердің скорингтік және биометриялық жүйелерімен тікелей манипуляция жасайды (деректерді жасырын жинау → құпия инициациялау);

– жеке қылмыскер қатысушылары аумақтық жағынан алшақталған, анонимді және көбінесе жеке таныс емес үлестірілген криминалдық құрылыммен (әлеуметтік инженерлер, техникалық мамандар, дропперлер) алмасты.

Онлайн алаяқтықтың ситуациялық проблема емес, орнықты жүйелі феномен екенін дәлелдеу үшін оның генезисі технологиялардың ауысуы ықпалымен криминалдық практикалардың үздіксіз эволюциясы арқылы ашылады:

– пайда болу сатысы (1990-2013 жж.) – ақпараттық технологияларды (базалық желілер, ДК) қылмыскерлер тек қосалқы құрал ретінде ғана пайдаланды. Алдау дәстүрлі сипатты сақтап қалды және құрбанмен физикалық байланысты талап етті;

– қалыптасу сатысы (2014-2018 жж.) – онлайн-банкинг пен мобильді интернеттің жаппай таралуы алдау практикасының біржолата қашықтықтан форматқа ауысуына әкелді. Ақпараттық жүйелер адам психикасымен қатар манипуляциялар объектісіне айналды;

– институционалдану сатысы (2019 жылдан бастап қазіргі уақытқа дейін) – цифрлық платформалардың терең енуі кибералаяқтықты орнықты криминалдық институтқа айналдырды. Қазіргі заманғы қолсұғушылықтар автоматтандырылған, гибридтік сипатқа ие және жаһандық көлеңкелі инфрақұрылым мен жаппай әлеуметтік инженерияға арқа сүйейді.

2) Қылмыстық құқықтың классикалық санаттық аппараты виртуалды ортаға тұжырымдамалық тұрғыдан бейімделмеген болып шыққандықтан, терминологиялық жаңартудың объективті қажеттілігі туындады;

«Цифрлық децепция» ұғымын енгізу дәстүрлі алдаудан іргелі алшақтықты көрсетеді. Бұл жалған ақпаратты беру ғана емес, тек виртуалды кеңістік құралдарымен, қашықтықтан және жеке байланыссыз іске асырылатын, жәбірленушінің ерік білдіруін немесе ақпараттық жүйе алгоритмдерін когнитивтік бұрмалаудың күрделі тетігі. Цифрлық децепция қазіргі заманғы жымқырудың гибридтік технологиялық-психологиялық табиғатын атап көрсетеді.

Бұрын ғылымда біржақты тәсілдер басым болды: бір зерттеушілер онлайн алаяқтықты жүйелерге техникалық араласуға саяды деп есептесе, басқалары интернет тек байланыс құралы ретінде әрекет ететін кәдімгі жымқыруға саяды деп санады. Диссертацияда тұжырымдалған ұғым іс-әрекетті гибридтік криминалдық феномен ретінде айқындай отырып, осы алшақтықты еңсереді. Дефиницияның ғылыми жаңалығы классикалық белгілердің (баю мақсаты, алдау жолымен мүлікті иемдену) және ерекше технологиялық детерминанттардың (тек цифрлық ортада жасалуы, қашықтық сипаты, құрбанның еркін немесе алгоритмдерді бұрмалау үшін АКТ пайдалану) органикалық бірігуінде жатыр

3) Тергеуші тергеп-тексерудің дұрыс әдістемесін таңдай алуы үшін қылмыстарды сауатты түрде саралау қажет. Бір өлшемді жіктеу өзінің әлеуетін сарқылғандықтан, төрт базалық өлшемшартты қамтитын кешенді модель әзірленді:

– технологиялық, ол қылмыс тәсілінің пайдаланылатын аппараттық-бағдарламалық құралдарға тәуелділігін көрсетеді, олар бүгінде байланыс құралы ғана емес, банктік скорингтік жүйелерді тікелей айналып өтудің автономды құралы ретінде әрекет етеді;

– объектілік, ол жымқыру затының кеңеюін ескереді, оның орбитасына енді цифрлық құқықтар, криптовалюталар және электрондық әмияндар кіреді;

– құрылымдық, ол қылмыстардың дербес және жасырын әрекет ететін, рөлдері терең бөлінген (техникалық мамандар, әлеуметтік инженерлер, дропперлер) үлестірілген желілік құрылымдармен жасалатынын тіркеп-белгілейді;

– трасологиялық, ол материалдық цифрлық іздерді (логтар, IP), идеалды (құрбанның жадындағы) және ерекше гибридтік іздерді (желідегі мінез-құлық паттерндері, пернетақталық қолтаңба) бөліп көрсете отырып, іздік көрініс жіктейді.

Жіктеу моделінің басты инновациясы – жоғарыда көрсетілген факторлардың комбинациясына тәуелді болатын және тергеуші үшін тактикалық-ұйымдастырушылық алгоритмдерді таңдауды тікелей талап ететін күрделіліктің интегративтік өлшемшартын енгізу:

– Төменгі деңгей – іс-әрекетті ел ішінде қарапайым байланыс құралдарының көмегімен жалғыз адам жасайды. Дәлелдеу үшін жергілікті операторларға стандартты сұрау салулар жеткілікті;

– Орташа деңгей – ел ішінде ішінара анонимизациясы бар адамдар тобы әрекет етеді. Бұл ұзаққа созылатын жасырын тергеу әрекеттерін және күрделі IT-сараптамаларды талап етеді;

– Жоғары деңгей – терең шифрлауды, криптовалюталарды және шетелдік серверлерді қолдана отырып, трансұлттық желілер жұмыс істейді. Мұндай істер тоқтата тұрудың барынша жоғары тәуекеліне ие және халықаралық құқықтық көмек туралы шұғыл сұрау салуларды талап етеді.

Бұл ереже жұмыстың қолданбалы құндылығын көрсетеді. Ұсынылған көпфакторлы жіктеу құқық қолданушы үшін жай ғана теория емес, практикалық компас ретінде қызмет етеді. Ол сотқа дейінгі тергеп-тексеру органдарына ақпаратты бастапқы тексеру сатысының өзінде-ақ ресурстық шығындарды болжауға, дәлелдемелерді жоғалту тәуекелдерін бағалауға және бірден іс-қимылдардың барабар алгоритмін таңдауға мүмкіндік береді;

4) Қашықтықтан микрокредиттеу саласында классикалық «қылмыскер – жәбірленуші» бинарлық моделі толығымен бұзылады. Оның орнына қолсұғушылықтың қос объектілілігіне негізделетін қылмыстық «аномальді триада» деп аталатын модель келеді. Мұндай іс-әрекетті жасау кезінде бір мезгілде екі дербес игілікке залал келтіріледі:

– Негізгі объект (меншік қатынастары) – тікелей мүліктік залал тек өзінің айналымдағы активтерінен айырылатын МҚҰ келтіріледі;

– Қосымша объект (ақпараттық және конституциялық құқықтар) – дербес немесе биометриялық деректері заңсыз пайдаланылған (цифрлық бірегейлікті компрометациялау, ЭЦҚ-ны заңсыз генерациялау, кредиттік тарихты бұрмалау) жеке тұлғаға айтарлықтай беймәтериалдық нұқсан келтіріледі.

Қолданыстағы құқық қолдану практикасы жүйелі іркілісті көрсетеді: формальды түрде легитимді электрондық шарттың болуы МҚҰ-ны қорғалатын объектінің шеңберінен шығара отырып, тергеу фокусын жасанды түрде ығыстырады. Нәтижесінде алданған азаматтар қате түрде сыбайлас қатысушылар немесе азаматтық-құқықтық борышкерлер деп танылады, ал кредиттік ұйым жәбірленуші тарап деп танылмайды. Қайтару келешегінсіз нақты капиталды жоғалтатындықтан, дәл қаржы институты бастапқы мүліктік жәбірленуші ретінде әрекет етеді. Азамат болса өзінің ақпараттық құқықтарына қолсұғушылық бөлігінде жәбірленуші деп танылуға тиіс.

ҚР ҚК-нің 190-бабы 2-бөлігінің 4-тармағының қолданыстағы нормасы тұжырымдамалық тұрғыдан ескірген. Қазіргі заманғы кредиттік өнімдерде қылмыскер адамды (пайдаланушыны) емес, қайта автоматтандырылған платформаның өзін және оның скорингтік немесе биометриялық алгоритмдерін алдайды (мысалы, бөтен фотосуреттердің көмегімен «Face ID» жүйесін айналып өтіп). Осыған байланысты арнайы саралаушы белгіні: «қаржы ұйымының ақпараттық жүйесіне көрінеу жалған компьютерлік деректерді енгізу жолымен жымқыру» деп енгізу қажеттілігі негізделген. Бұл тұжырым фокусты адамды алдаудан жүйені технологиялық алдауға ауыстырады.

Бұл новелланы енгізу онлайн алаяқтықты компьютерлік саботаж бен хакерліктен (ҚР ҚК-нің 205-207-баптары) нақты ажыратуға мүмкіндік береді. Алаяқтық кезінде МҚҰ жүйесі штаттық режимде жұмыс істейді және бастапқы

кодты бұзуға ұшырамайды; ол легитимді түрде енгізілген, бірақ мазмұны бойынша жалған ақпарат негізінде қарыз беру туралы қате шешім ғана қабылдайды.

Ұсынылған реформа салалық заңнамамен («Микроқаржылық қызмет туралы» Заңның 3-2-бабы) органикалық түрде синхрондалады. МҚҰ кінәсіз азаматтың жалған қарызын есептен шығарады және қылмыстық сот ісін жүргізу шеңберінде ұсталған киберқылмыскерден тікелей залалды өтеуді талап етуге легитимді құқық алады. Бұл ереже заңнаманың жай ғана косметикалық түзетулерді емес, қайта трансұлттық қаржы ортасының шынайылығына терең бейімделуді қажет ететінін дәлелдейді. Жалған онлайн-кредиттер проблемасын шешу тек МҚҰ-ны жәбірленуші деп тану және ҚР ҚК-ге алгоритмдік тұрғыдан дәл қылмыс құрамын енгізу арқылы ғана мүмкін болады;

5) Аралас құрамдарды ажыратумен қатар, кибержымқырулардың сатылылығын ресми соттық түсіндіру деңгейінде регламенттеудің өткір қажеттілігі туындады. Құқық қолдану практикасы бастапқы алдау ақшалай қаражатты тікелей иемденуге емес, құпия аутентификациялық ақпаратты (CVV-кодтарды, PIN-кодтарды, мобильді банкингтің SMS-парольдерін) алуға бағытталған жағдайлармен үнемі бетпе-бет келеді. Осыған байланысты ҚР Жоғары Сотының №6 нормативтік қаулысын тікелей түсіндірмемен толықтыру орынды: алдау немесе сенімді теріс пайдалану жолымен банктік және өзге де дербес шоттарға қол жеткізу кодтарын иемдену алаяқтыққа оқталу ретінде дербес сараланауға жатады, өйткені бұл әрекеттер кейіннен электрондық активтерді жасырын жымқыру үшін тікелей жағдай жасайды.

Қаржы институтын бастапқы жәбірленуші деп тану дербес деректері заңсыз компрометацияланған жеке тұлғалардың құқықтарын қорғаудың айналы процестік тетігін объективті түрде талап етеді. Қылмыстық сот ісін жүргізудің қолданыстағы моделі алданған азаматтарды түпкілікті сот үкімі шығарылғанға дейін азаматтық-құқықтық борышкерлер мәртебесінде қалдырады, бұған құқықтық мемлекетте жол берілмейді. Бұзылған құқықтарды сотқа дейін қалпына келтіру тұжырымдамасын іске асыру мақсатында прокуратура органдары мен тергеу соттарына жаңа құзыреттер беру қажеттілігі негізделген. ҚР ҚПК-не, атап айтқанда, 55 және 193-баптарына прокурорға сотқа дейінгі тергеп-тексеру сатысында тергеу сотына тиісті өтінішхат енгізуге мүмкіндік беретін арнайы құқықтық институтты енгізу ұсынылады. Бұл тетік тергеу судьясына кредиттік ұйымды жәбірленуші деп тану және цифрлық бірегейлігін алаяқтар пайдаланған азаматтардан жалған кредиттік міндеттемелерді мерзімінен бұрын алып тастау туралы мәселені қарау бойынша тікелей өкілеттік беруді көздейді. Мұндай процестік конструкция сот ісін жүргізудің ең ерте сатыларында киберқылмыстылықтың теріс әлеуметтік-экономикалық салдарларын нивелирлей отырып, жеке тұлғалардың құқықтарының жедел реституциясын қамтамасыз етеді. Атап айтқанда, ҚР ҚПК-тің 193-бабы 19-1-бөлігін қосу арқылы келесідей нұсқа ұсынамыз:

«Сотқа дейінгі тергеп-тексеру сатысында қылмыстық іс бойынша несие беруші органды жәбірленуші ретінде тану және несие рәсімделген тұлғалардан несиелік шығындарды алып тастау жөнінде тергеу соттарына өтінішхат

келтіреді».

ҚР ҚПК-тің 55-бабының 2-бөлігінің 5-1-тармағын қосу арқылы келесідей нұсқа ұсынамыз:

«Прокурордың ұсынуымен қылмыстық іс бойынша несие беруші органды жәбірленуші ретінде тану және несие рәсімделген тұлғалардан несиелік шығындарды алып тастау туралы мәселені қарайды»;

6) Қылмыстық процестің (ҚР ҚПК-нің базалық ұйғарымдарына сүйенетін) дәстүрлі архитектурасы тарихи түрде субъект-центристік логикада құрылған. Бұл модель шеңберінде күдіктінің жеке басын бастапқы анықтау басты орынға қойылады, содан кейін тергеу оның кінәсінің сезілетін материалдық дәлелдемелерін іздеуге көшеді. Алайда қылмыстылық желілік, анонимді және экстерриториялық сипатқа ие болған цифрландыру жағдайында бұл классикалық алгоритм толығымен салданған болып шықты. Құқық қолданушының ескі схема бойынша әрекет ету және технологиялардан бөлек жеке тұлғаны іздеу әрекеттері субъектінің анықталмауына байланысты істердің жаппай тоқтатыла тұруына әкеледі.

Осы институционалдық дағдарысты еңсеру үшін диссертация тергеп-тексеру векторын «із → субъект» бағытына түбегейлі ауыстыру қажеттілігін негіздейді. Ұсынылған инновациялық модельде танымның бастапқы объектісі ретінде цифрлық артефакт (машиналық код, желілік логтар, IP-мекенжайлар, транзакциялардың хеш-сомалары) әрекет етеді. Денесіз цифрлық артефакт қылмыстың жасырын субъектісіне гносеологиялық өтуді жүзеге асыруға мүмкіндік беретін баламасыз бастапқы нүкте деп танылады. Сотқа дейінгі іс жүргізудің бүкіл логикасы жаңа императивті формула бойынша қайта құрылады: «цифрлық із → тіркеп-белгілеу → талдау → субъектіні анықтау → жолын кесу».

Цифрлық дәлелдемелердің басты ерекшелігі – олардың гиперқұбылмалылығы (өзгергіштігі, тез жойылу немесе деградациялану қабілеті). Егер тергеуші алғашқы сағаттарды жеке басын анықтауға (кінәліні дербестендіруге) жұмсайтын болса, ол цифрлық деректерді орны толмастай жоғалтады. Сондықтан артефакт-центристік модель қатаң процестік басымдықты белгілейді: бастапқы сатының басты міндеті цифрлық іздердің криптографиялық тұтастығын қамтамасыз ете отырып, оларды дереу жедел тіркеп-белгілеу болып табылады. Тек сенімді сақталған және заңды түрде бекітілген артефакт қана бұдан былай қылмыскерлердің бүкіл үлестірілген желісін деанонимизациялау кілтіне айнала алады.

Қолданыстағы ҚПК виртуалды ақпаратты материалдық объектілердің (заттай дәлелдемелердің немесе қағаз жүзіндегі «өзге де құжаттардың») архаикалық шеңберіне күштеп сыйғызады. Бұл тергеуді фиктивті рәсімдерді жүргізуге: шынайы криминалистикалық маңызды деректер бұлтты серверлерге үлестірілген кезде, физикалық «пластик пен металды» (смартфондарды, қатты дискілерді) алып қоюға мәжбүр етеді. Осы нормативтік вакуумды еңсеру үшін авторлық анықтама енгізілді. Цифрлық дәлелдеме криминалдық оқиғаны объективті түрде көрсететін және сезілетін физикалық жеткізгішке мүлдем тәуелді емес, тұтастықтың, қайта жаңғыртылушылықтың және атрибуцияланудың математикалық қасиеттеріне ие дербес ақпараттық құрылым

ретінде қарастырылады. Бұл ақпаратты нақты «темірге» қарапайым байланыстырудан түпкілікті бас тартуды қамтамасыз етеді және желіден деректерді легитимді түрде алып қоюға мүмкіндік береді.

Ұсынылған тұжырымдаманы институционализациялау мақсатында ҚР ҚПК-не өзара байланысты өзгерістер кешенін енгізу талап етіледі. Біріншіден, ҚР ҚПК-нің 7-бабын мынадай мазмұндағы 59-тармақпен толықтыру орынды: «Электрондық (цифрлық) дәлелдемелер – ақпараттық жүйелерде, желілік ресурстарда, электрондық құрылғыларда цифрлық формада қалыптастырылған, сақталатын, өңделетін немесе берілетін, қылмыстық іс үшін мәні бар мән-жайларды белгілеу және тексеру үшін қолданылатын деректер (нәрселер)». Екіншіден, нақты деректер заттай дәлелдемелермен қатар «электрондық (цифрлық) дәлелдемелермен» де белгіленетінін тікелей бекіте отырып, ҚР ҚПК-нің 112-бабының 2-бөлігін жаңа редакцияда жазу қажет. Ақырында, ҚР ҚПК-нің 118-бабының 1-бөлігін цифрлық ақпаратты оның физикалық жеткізгішіне тәуелсіз алып қоюдың және қоса тіркеудің дербес тәртібін заңдастыратын 6-тармақпен толықтырған жөн;

7) «Цифрлық іздердің жеделдетіліп деградациялануы» тұжырымдамасы дәлелдемелерді жоғалтудың іргелі себебін түсіндіреді. Екі жылдамдықтың сыни асимметриясымен негізделген тар «мүмкіндіктер терезесі» ұғымы енгізілді:

– орта жылдамдығы – цифрлық іздер (логтар, IP-мекенжайлар, транзакциялар) гиберқұбылмалыққа ие. Олар қылмыскерлердің активті қарсы іс-қимылының (автоматты тазарту скрипттері, шифрлау), сондай-ақ деректерді циклді түрде өшіретін серверлердің өздерінің пассивті архитектурасының әсерінен секундтың үлесінде жоғалады;

– тергеудің инерттілігі – дәстүрлі қылмыстық процесс өте бюрократияланған. Тергеуші прокурордың қажетті санкцияларын алып, қағаз жүзіндегі сұрау салуларды жібергенше, технологиялық орта іздік көріністі кепілді түрде жойып үлгереді. Бұл тұжырымдама кибержымқыруды монетизациялау құқық қорғау жүйесінің айғақтарды легитимді жинауды процестік түрде инициациялауға үлгеруінен жүздеген есе тез алгоритмдік түрде жүзеге асырылатыны туралы фактіні ғылыми негіздейді.

Егер алдыңғы тармақ технологиялық тосқауылды сипаттаса, онда «цифрлық нигилизм» феномені деструктивті адами факторды сипаттайды. Цифрлық нигилизм – бұл ұшпа деректермен бетпе-бет келетін, бірақ әдеттегідей заттық әлем санаттарымен ойлауды жалғастыратын құқық қолданушының қорғаныс реакциясы мен когнитивтік диссонансы. Практикада бұл артефактылардың технологиялық ерекшелігін жүйелі және саналы түрде елемеуден көрініс табады: тергеушілер алып қойылатын файлдардың міндетті криптографиялық хеш-сомаларын есептемейді, жасырын жүйелік метадеректерді елемейді және машиналық кодпен күрделі жұмысты скриншоттарды қарапайым басып шығарумен және қарапайым қағаз актілерін жасаумен алмастыруға тырысады. Цифрлық нигилизмнің нәтижесі соттардың мұндай дәлелдемелерді жаппай жол берілмейтін деп тануы болып табылады, өйткені қағаз хаттама виртуалды кодтың тұтастығына кепілдік бере алмайды.

Егер деректердің процестік мәртебесі мен тергеушінің өзінің ойлауы

өзгермесе, тергеуді технологиялық жарақтандыру өздігінен мағынасыз болады. «Цифрлық нигилизмді» еңсеру және цифрлық дәлелдемелерді физикалық жеткізгіштерден бөлек заңдастыру құқық қорғау жүйесінің электрондық қылмыстық сот ісін жүргізуге өтуі және онлайн алаяқтықпен тиімді күресу үшін іргелі заңдық шарттар ретінде әрекет етеді;

8) Дәстүрлі фрагменттік қарсы іс-қимылдың өзін сарқығаны дәлелденді, сол себепті кибержымқыруларды тергеп-тексеру үшін қатаң, иерархиялық және ажырамас процестік конструкция ұсынылды. Онда әрбір кезең алдыңғысының табыстылығымен қатаң детерминацияланған:

– превентивті деңгей жәбірленушінің формальды түрде жүгінуіне дейін-ақ криминалдық белсенділік маркерлерін анықтауға мүмкіндік беретін банктік антифрод-жүйелермен цифрлық ортаға үздіксіз автоматтандырылған криминалистикалық мониторинг жүргізуден тұрады;

– инициациялық деңгей электрондық хабарламаларды СДТБТ-да жедел тіркеу арқылы цифрлық сигналды (аномалияны) легитимді процеске лезде трансформациялауды қамтамасыз етеді;

– артефактілік деңгей құбылмалы цифрлық іздерді (логтарды, IP-мекенжайларды) олардың криптографиялық тұтастығы мен өзгермеушілігін міндетті түрде қамтамасыз ете отырып, шұғыл процестік-технологиялық тіркеп-белгілеу орын алатын жүйенің өзегі ретінде әрекет етеді;

– атрибутивтік деңгей алынған артефактылар мен үлестірілген желілік профильдерді талдау негізінде жасырын қылмыскердің шынайы жеке басын динамикалық түрде анықтауға (деанонимизациялауға) бағытталған;

– жолын кесу деңгейі жәбірленушілерге залалды нақты өтеу үшін транзакцияларды технологиялық бұғаттауды және шығарылған активтерді жедел қамауға алуды қамтамасыз ететін модельдің мағыналық шыңы болып табылады.

Бұл модель тек бір тұтас ретінде жұмыс істейді: ерте анықтаудың болмауы инициацияны құнсыздандырады, тіркеп-белгілеу қателері заңдық атрибуцияны бұғаттайды, ал активтерді қайтарусыз жеке басты анықтау тергеуді практикалық мағынасынан айырады.

Бұл архитектураны іске асыру үшін орталық кедергі уақыт болып табылады. Цифрлық ортаның гиперқұбылмалылығына байланысты (деректер серверлерден секундтың үлесінде автоматты немесе мақсатты түрде жойылуы мүмкін) «72 сағат» алгоритмін енгізу негізделген. Ол сотқа дейінгі іс жүргізудің бастапқы сатысын түбегейлі қысқартатын және барлық өзге рәсімдерден гөрі іздерді криптографиялық бекіту бойынша жоғары технологиялық кезек күттірмейтін тергеу әрекеттерінің абсолютті басымдығын белгілейтін императивті хронологиялық сүзгі ретінде әрекет етеді.

Шұғыл алгоритмді легитимдеу және практикалық қамтамасыз ету үшін аса маңызды нормативтік новелла – күдіктіні ұстап алудың айрықша жағдайларын 72 сағатқа дейін кеңейту ұсынылды. Үлестірілген трансұлттық кибертоптың қатысушысын анықтау және ұстап алу кезінде оның немесе оның сыбайлас қатысушыларының шифрланған іздерді қашықтықтан жойып үлгеруінің немесе активтерді шұғыл шығаруының сыни тәуекелі туындайды. Ұсынылып отырған

негіз жазалау шарасы ретінде емес, қатаң процестік дедлайн ретінде енгізіледі: дәл осы уақыт аралығы қашықтағы серверлерде машиналық кодты қауіпсіз шығарып алу бойынша кезек күттірмейтін жоғары технологиялық іс-шараларды жүргізу үшін тергеуге беріледі.

Әзірленген архитектура жедел, технологиялық және процестік қызмет арасындағы жасанды ведомстволық тосқауылдарды толығымен жояды. «72 сағат» алгоритмін және ұстап алудың жаңа нормасын енгізу ақырында трансұлттық онлайн алаяқтықтың гипердинамикасына толығымен барабар болатын, тергеудің алғашқы секундтарынан бастап цифрлық дәлелдемелердің сенімді сақталуын қамтамасыз ететін процестік жауапты қалыптастырады;

9) Зерттеу құқық қорғау жүйесінің айғақтар тапшылығымен ғана емес, қайта ерекше криминалистикалық-процестік жай-күймен – технологиялық ұсталмайтындықпен бетпе-бет келетінін көрсетеді. Криминалдық инфрақұрылым цифрлық пакеттердің өтуінің шынайы маршруттарын техникалық тұрғыдан жасыратын көпдеңгейлі желілік анонимизацияны (VPN, TOR пияздық маршрутизаторларын, прокси-серверлерді) және терең өтпелі шифрлауды активті түрде қолданады. Бұл технологиялық бүркемелеу юрисдикциялық тосқауылдармен бекемделеді: шет мемлекеттердің жеке өмірді қорғау туралы қатаң ұлттық заңдары (zero-log саясатына дейін) криминалдық трафик үшін мүлдем легитимді қалқан ретінде әрекет етеді. Нәтижесінде іздердің техникалық көрінбеуі ұлттық тергеу үшін олардың абсолютті процестік қолжетпестігіне трансформацияланады.

Қазіргі заманғы онлайн алаяқтық айқын көрінетін «мультиюрисдикциялық» сипатқа ие: құрбанға когнитивтік ықпал ету, серверлік маршрутизациялау және активтерді шығару әртүрлі мемлекеттердің аумақтары арасында перманентті түрде үлестірілген. Құқық қолданушының халықаралық құқықтық көмектің консервативті институтын (ҚР ҚПК-нің 559-бабы тәртібімен) пайдалану әрекеттері фатальды «рәсімдік асимметрияға» әкеледі. Оның мәні қағаз жүзіндегі дипломатиялық сұрау салуларды орындау мерзімдерінің (айлар мен жылдарға созылатын) гиперқұбылмалы виртуалды іздердің өмір сүру уақытынан өлшеусіз асып түсуінде. Деректер циклді түрде қайта жазылатын және шетелдік хостингтерде автоматты түрде жойылатын жағдайларда, дәстүрлі дипломатиялық тетік ішінде дәлелдемелер орны толмастай жойылатын заңды хронологиялық тосқауылға айналады.

Ұлттық тергеудің оқшауланuын еңсеру үшін институционалдық гибридтік модель әзірленді. Оның ішкі контуры мемлекет пен жекеше қаржы секторы арасындағы ведомстволық қабырғаларды толығымен бұзуды талап етеді. СДТБТ-нің ақпараттық жүйесін Ұлттық Банк пен екінші деңгейдегі банктердің антифрод-жүйелерімен өтпелі интеграциялаудың (платформалық тәсіл) объективті қажеттілігі негізделді. Бұл шығарылған электрондық активтердің криптографиялық жасырылуына дейін олардың шұғыл бұғатталуын қамтамасыз ете отырып, цифрлық аномалиялар мен компрометация маркерлерін қылмыстық іс материалдарына лезде трансляциялауға мүмкіндік береді.

Гибридтік модельдің сыртқы контуры халықаралық көмектің архаикалық реактивті формасынан проактивті автоматтандырылған мемлекетаралық желілік

деректер алмасуға түбегейлі идеологиялық өтуді талап етеді. Сөз орталық дипломатиялық инстанцияларды айналып өтіп, әртүрлі елдердің құқық қорғау органдарын біріктіретін және трансұлттық корпорация-провайдерлердің лог-файлдарына тікелей басым қол жеткізуді ұсынатын криптографиялық қорғалған цифрлық платформалар мен 24/7 форматындағы тәулік бойғы көлденең желілерді құру туралы болып отыр.

Егер тергеу ақпараттық оқшауланууда қалатын болса, ҚР ҚПК-нің ешқандай ішкі реформалары және ең озық криминалистикалық тактикаларды енгізу нәтиже бермейді. Тек ұлттық қылмыстық-процестік әрекеттерді жекеше қаржы секторымен және деректерді шұғыл алмасудың жаһандық желілерімен терең, ажырамас интеграциялау ғана трансұлттық киберқылмыстылықты оның басты артықшылықтарынан – уақыт факторы мен технологиялық анонимділіктен айыруға қабілетті.

Ережелердің дұрыстығы мен негізділігі ғылыми танымның жалпыға бірдей диалектикалық, формальды-заңдық, статистикалық және компаративистік әдістерін кешенді қолданумен қамтамасыз етілген. Зерттеудің эмпирикалық базасы 2020-2026 жылдар кезеңінде онлайн алаяқтық туралы істер бойынша Қазақстан Республикасының соттары шығарған 127 сот үкімінен тұратын репрезентативті массивке, сондай-ақ ҚР БП Құқықтық статистика жөніндегі комитетінің статистикалық деректерін және 2024-2028 жылдарға арналған Қоғамдық қауіпсіздікті қамтамасыз ету тұжырымдамасының көрсеткіштерін терең талдауға сүйенеді.

Одан әрі зерттеулердің перспективалары жасырын цифрлық корреляцияларды автоматтандырылған түрде талдау үшін жасанды интеллект (Big Data) жүйелерін енгізу мүмкіндіктерін тереңдетіп салааралық зерделеу, сондай-ақ нақты уақыт режимінде цифрлық дәлелдемелермен лезде трансшекаралық алмасуды қамтамасыз ету үшін унификацияланған криптографиялық қорғалған платформалардың архитектурасын әзірлеу жазықтығында жатыр.

Пайдаланылған әдебиеттер тізімі

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

2 Президент Бас прокуратурада жиын өткізді // Қазақстан Республикасы Президентінің ресми сайты (Ақорда). https://www.akorda.kz/kz/prezident-bas-prokuraturada-zhiyn-otkizdi-2604726

3 Қоғамдық қауіпсіздікті қоғаммен әріптестік жасап қамтамасыз етудің 2024–2028 жылдарға арналған тұжырымдамасын (құқық бұзушылық профилактикасы саласында) бекіту туралы: Қазақстан Республикасы Үкіметінің 2023 жылғы 29 желтоқсандағы № 1233 қаулысы. https://adilet.zan.kz/kaz/docs/P2300001233

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

5 Қазақстан Республикасының Қылмыстық-процестік кодексі: 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. https://adilet.zan.kz/kaz/docs/K1400000231

6 Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің статистикалық есептері. https://qamqor.gov.kz/crimestat/statistics

7 Қазақстан Республикасының Азаматтық кодексі (Жалпы бөлім): 1994 жылғы 27 желтоқсандағы № 268-XIII. https://adilet.zan.kz/kaz/docs/K940001000_#z465

8 Жедел-іздестіру қызметі туралы: Қазақстан Республикасының 1994 жылғы 15 қыркүйектегі № 154-XIII Заңы. https://adilet.zan.kz/kaz/docs/Z940004000_

9 Микроқаржылық қызмет туралы: Қазақстан Республикасының 2012 жылғы 26 қарашадағы № 56-V Заңы. https://adilet.zan.kz/kaz/docs/Z1200000056

10 Төлемдер және төлем жүйелері туралы: Қазақстан Республикасының 2016 жылғы 26 шілдедегі № 11-VI ҚРЗ Заңы. https://adilet.zan.kz/kaz/docs/Z1600000011

11 Қазақстан Республикасындағы цифрлық активтер туралы: Қазақстан Республикасының 2023 жылғы 6 ақпандағы № 193-VII ҚРЗ Заңы. https://adilet.zan.kz/kaz/docs/Z2300000193

12 Алаяқтық туралы істер бойынша сот практикасы туралы: Қазақстан Республикасы Жоғарғы Сотының 2017 жылғы 29 маусымдағы № 6 нормативтік қаулысы. https://adilet.zan.kz/kaz/docs/P170000006S

13 Компьютерлік қылмыс туралы конвенция (Еуропалық шарттар сериясы (CETS/ETS) № 185). https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=185

14 Біріккен Ұлттар Ұйымының киберқылмысқа қарсы конвенциясы: ақпараттық-коммуникациялық жүйелерді пайдалану арқылы жасалатын жекелеген қылмыстарға қарсы күресте халықаралық ынтымақтастықты нығайту және ауыр қылмыстарға қатысты электрондық нысандағы дәлелдемелермен алмасу туралы. https://www.un.org/ru/documents/treaty/A-RES-79-243

15 Капинус О.С. Цифровизация преступности и уголовное право // Baikal Research Journal. – 2022. – Т. 13, № 1. – С. 1–7. – DOI 10.17150/2411-6262.2022.13(1).22.

16 Бисалиев М.С. Международно-правовые аспекты защиты личной информации в глобальном и национальном информационном пространстве: дис. ... доктора философии (PhD): 8D04201 / Казахский национальный университет имени аль-Фараби. – Алматы, 2025. – 186 с.

17 Карабеков К.О. Киберпреступность в Российской Федерации и Республике Казахстан: состояние и меры предупреждения: дис. ... к.ю.н.: 5.1.4 / Омская академия МВД России. – Омск, 2025. – 217 с.

18 Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... к.ю.н.: 12.00.08 / Российский университет дружбы народов. – М., 2019. – 211 с.

19 Тамбиев С.А. Криминологические аспекты противодействия преступности в цифровом пространстве // Журнал прикладных исследований. – 2022. – Т. 9, № 1. – С. 63–66.

20 Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д.ю.н.: 12.00.08 / Университет прокуратуры РФ. – М., 2021. – 557 с.

21 Курумбаева А.Б., Кощегулов Б.Б. Некоторые вопросы квалификации мошенничеств, совершаемых с использованием информационных систем // Вестник Карагандинского университета. Серия: Право. – 2022. – № 3(107). – С. 46–53.

22 Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: дис. ... к.ю.н.: 12.00.08. – Самара, 2021. – 243 с.

23 Объем операций через Интернет/мобильный банкинг в 2017 году в РК вырос в три раза. https://inbusiness.kz/ru/last/obem-operacij-cherez-internet-mobilnyj-banking-v-2017-godu-

24 О процессе цифровизации в финансовом секторе рассказали в Национальном Банке Казахстана. https://nationalbank.kz/file/download/14477

25 Гоибназарзода П.А. Уголовная ответственность за мошенничество в сфере кредитования по законодательству Российской Федерации и Республики Таджикистан: дис. ... к.ю.н.: 5.1.4 / Московский университет МВД России им. В.Я. Кикотя. – М., 2025. – 259 с.

26 Объем безналичных операций по платежным карточкам впервые превысил показатели по снятию наличных денег. https://nationalbank.kz/ru/news/informacionnye-soobshcheniya/8803

27 Энгельгардт А.А. Вопросы квалификации мошенничества в сфере компьютерной информации // Право. Журнал Высшей школы экономики. – 2016. – № 4. – С. 86–95.

28 Apsimet N.M., Smanova A.B., Utegenova G.A. The role of the Internet in the evolution of fraud: a historical aspect // Bulletin of the L.N. Gumilyov Eurasian National University. Law Series. – 2024. – № 1(146). – P. 247–257.

29 Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-

правовые меры борьбы: дис. ... к.ю.н.: 12.00.08 / Дальневосточный государственный университет. – Владивосток, 2005. – 234 с.

30 Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. – 2012. – № 1. – С. 9–22.

31 Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д.ю.н.: 12.00.08. – М., 2018. – 427 с.

32 Зотина Е.В. Уголовно-правовой аспект предупреждения мошенничества с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии // Вестник Казанского юридического института МВД России. – 2024. – Т. 15, № 3(57). – С. 73–82.

33 Энгельгардт А.А. О понимании мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. – 2016. – № 8. – С. 84–90.

34 Орешков И.А. Использование современных информационных технологий при расследовании преступлений в сфере экономики: дис. ... к.ю.н.: 5.1.4 / Московский университет МВД России им. В.Я. Кикотя. – М., 2024. – 233 с.

35 Шумихин В.Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. Юридические науки. – 2014. – № 2(24). – С. 229–233.

36 Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. ... к.ю.н.: 12.00.08 / Дальневосточный федеральный университет. – Владивосток, 2020. – 228 с.

37 Полстовалов О.В., Галяутдинов Р.Р. Организованные формы онлайн-мошенничества: виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения // Юридические исследования. – 2023. – № 11. – С. 120–127.

38 №5532-25-00-1/20 қылмыстық ісі бойынша Павлодар облысы Ақтоғай аудандық сотының 2025 жылғы 23 желтоқсандағы үкімі. https://office.sud.kz/

39 Подольный Р.Н. Методологические основы расследования преступлений, совершенных с применением цифровых технологий: дис. ... д.ю.н.: 5.1.4. – М., 2025. – 255 с.

40 Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. ... к.ю.н.: 12.00.08. – Саратов, 2011. – 262 с.

41 Фокин А.Д. Теоретико-прикладные основы методики расследования мошенничества в сфере оборота жилых помещений, совершаемого с использованием информационно-телекоммуникационных технологий: дис. ... к.ю.н.: 5.1.4. – М., 2025. – 225 с.

42 №3572-21-00-1/9 қылмыстық ісі бойынша Қарағанды қаласы Октябрь ауданының №2 аудандық сотының 2021 жылғы 16 сәуірдегі үкімі. https://office.sud.kz/

43 №3511-23-00-1/5 қылмыстық ісі бойынша Қарағанды қаласы Қазыбек би аудандық сотының 2023 жылғы 05 маусымдағы үкімі. https://office.sud.kz/

44 Комлев Ю.Ю. От цифровизации социума и киберпреступности к подготовке киберполицейских // Вестник экономики, права и социологии. – 2025.

– № 2. – С. 139–143.

45 Әпсімет Н.М., Алимкулов Е.Т., Нурутдинова А.Ж. Әлеуметтік желілер мен цифрлық технологияның онлайн алаяқтықтың таралуына әсері // Қазақстан Республикасы ІІМ М. Есболатов ат. Алматы академиясының ғылыми еңбектері. – 2024. – № 1(78). – 18–26 б.

46 Майоров А.В. Виктимология цифровой преступности: концепция научного направления // Виктимология. – 2024. – Т. 11, № 1. – С. 7–12.

47 Жмуров Д.В. Техногенные предпосылки кибервиктимизации // Виктимология. – 2023. – Т. 10, № 2. – С. 138–146.

48 №3528-23-00-1/20 қылмыстық ісі бойынша Қарағанды облысы Шахтинск қалалық сотының 2023 жылғы 11 маусымдағы үкімі. https://office.sud.kz/

49 №7141-25-00-1/1908 қылмыстық ісі бойынша Астана қаласының Қылмыстық істер жөніндегі ауданаралық сотының 2025 жылғы 05 қыркүйектегі үкімі. https://office.sud.kz/

50 №5511-22-00-1/31 қылмыстық ісі бойынша Өскемен қаласы №2 сотының 2022 жылғы 24 мамырдағы үкімі. https://office.sud.kz/

51 №3570-20-00-1/149 қылмыстық ісі бойынша Қарағанды қаласы Октябрь аудандық сотының 2020 жылғы 11 желтоқсандағы үкімі. https://office.sud.kz/

52 Apsimet N.M., Zhanibekov A.K. The impact of online fraud on the psychosocial development of adolescents: predictive and preventive strategies for creating a safe environment // Trends in the development of criminal policy in the context of globalization: materials of the international scientific and practical conference. – Almaty: Kazakh University, 2024. – P. 5–12.

53 Головин А.Ю. Базовые криминалистические классификации преступлений // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 2-2. – С. 31–40.

54 Стояновский М.В. Об основании криминалистической классификации преступлений // Вестник Воронежского государственного университета. Серия: Право. – 2012. – № 1(12). – С. 469–478.

55 Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. ... д.ю.н.: 12.00.09 / Воронежский государственный университет. – Воронеж, 2001. – 387 с.

56 Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дис. ... к.ю.н.: 12.00.09 / Волгоградская академия МВД России. – Волгоград, 2008. – 216 с.

57 Джилкишиев Р.Б. Расследование преступлений в сфере информационных технологий: дис. ... доктора философии (PhD): 8D12301 / Костанайская академия МВД РК им. Ш. Кабылбаева. – Костанай, 2025. – 186 с.

58 Поляков В.В., Шебалин А.В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2013. – № 13-1. – С. 123–125.

59 Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... к.ю.н.: 12.00.12. – М., 2016. – 249 с.

60 Рудых А.А. Информационно-технологическое обеспечение раскрытия и расследования преступлений: дис. ... к.ю.н.: 12.00.12. – Иркутск, 2019. – 239 с.

61 Мира К.А. Установление механизма хищений чужого имущества с использованием информационных технологий: дис. ... к.ю.н.: 12.00.12. – М., 2022. – 245 с.

62 Әпсімет Н.М., Алимкулов Е.Т. Киберқауіптер және жеке деректерді қорғау: онлайн алаяқтықтың заманауи әдістерін талдау // Жаһандану жағдайында қылмыстық саясатты жетілдіру тенденциялары (XIII жыл сайынғы Баймурзин оқулары): халықар. ғыл.-тәж. конф. материалдары. – Алматы, 2023. – 87–95 б.

63 Перетолчин А.П. Мошенничество с использованием электронных средств платежа: уголовно-правовая характеристика и проблемы квалификации: дис. ... к.ю.н.: 12.00.08. – М., 2022. – 238 с.

64 Маилян А.В. Совершенствование методики расследования хищений, совершаемых с использованием электронных средств платежа: дис. ... к.ю.н.: 5.1.4. – Казань, 2024. – 222 с.

65 Щербаченко А.К. Раскрытие, расследование и предупреждение мошенничеств, совершенных группой лиц: дис. ... д.ю.н.: 12.00.12. – Ростов-на-Дону, 2021. – 431 с.

66 Корпеев А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному праву России: дис. ... к.ю.н.: 12.00.08. – Волгоград, 2008. – 198 с.

67 №7550-21-00-1/516 қылмыстық ісі бойынша Алматы қаласы Бостандық ауданының №2 аудандық сотының 2022 жылғы 03 қазандағы үкімі. https://office.sud.kz/

68 Майлис Н.П. Цифровая трасология: современное состояние и пути решения проблем // Роль права в обеспечении благополучия человека: сб. докл. XXII Междунар. науч.-практ. конф.: в 5 ч. – М., 2022. – Ч. 4. – С. 490–494.

69 Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. ... д.ю.н.: 12.00.09. – Волгоград, 2008. – 561 с.

70 Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. – Волгоград: Волгоградская акад. МВД России, 2008. – 401 с.

71 Пономарев В.Е. Технико-криминалистическое обеспечение выявления и закрепления электронных доказательств: дис. ... к.ю.н.: 5.1.4. – Краснодар, 2025. – 218 с.

72 Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: дис. ... к.ю.н.: 12.00.09. – М., 2009. – 252 с.

73 Цветкова А.Д. Криминалистическое исследование компьютерного (клавиатурного) почерка // Электронное приложение к Российскому юридическому журналу. – 2022. – № 2. – С. 55–65.

74 Apsimet N.M., Alimkulov Ye.T., Duisenbayeva G.Zh. The collection of digital traces in the investigation of online crimes // Bulletin of the L.N. Gumilyov Eurasian National University. Law Series. – 2024. – № 4(149). – P. 170–185.

75 Гаврилин Ю.В. О понятии и содержании государственной научно-

технической политики в области криминалистического обеспечения правоохранительной деятельности // Труды Академии управления МВД России. – 2022. – № 2(62). – С. 96–102.

76 Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2001. – 496 с.

77 Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М.: Новый юрист, 1998. – 256 с.

78 Осипенко А.Л. О правовом регулировании действий оперативно-розыскных органов при раскрытии трансграничных преступлений в сети Интернет // Оперативник (сыщик). – 2011. – № 2. – С. 18–23.

79 Машлякевич В.А. Расследование мошенничеств, совершаемых с использованием средств телефонной связи: дис. ... к.ю.н.: 5.1.4 / Барнаульский юридический институт МВД России. – Барнаул, 2024. – 240 с.

80 Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. – М.: Проспект, 2023. – 136 с.

81 Гостевский Д.Ю. Технико-криминалистическое обеспечение производства следственных действий: дис. ... к.ю.н.: 12.00.09. – Люберцы, 2010. – 199 с.

82 Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя // Пермский юрид. альманах. – 2019. – № 3. – С. 598–609.

83 Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. – М.: ИНФРА-М, 2022. – 227 с.

84 №1-577/2022 қылмыстық ісі бойынша ШҚО Өскемен қаласы №2 сотының 2022 жылғы 08 желтоқсандағы үкімі. https://office.sud.kz/

85 №7560-21-00-1/25 қылмыстық ісі бойынша Алматы қаласы Жетісу ауданының №2 аудандық сотының 2021 жылғы 24 ақпандағы үкімі. https://office.sud.kz/

86 Шульга А.В. Объект и предмет преступлений против собственности в условиях рыночных отношений и информационного общества: автореф. дис. ... д.ю.н.: 12.00.08. – Волгоград, 2008. – 61 с.

87 Безверхов А.Г. Уголовно-правовая охрана собственности в условиях рыночной экономики // Уголовное право в эпоху финансово-экономических перемен: материалы IX Рос. Конгресса уголовного права. – М.: Юрлитинформ, 2014. – С. 114–118.

88 Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. – 2013. – № 5(10). – С. 55–65.

89 Лопашенко Н.А. Преступления против собственности: теоретико-прикладное исследование. – М.: ЛексЭст, 2005. – 408 с.

90 Завьялова Д.В. Расследование преступлений в сфере компьютерной информации: отечественный и зарубежный опыт: дис. ... к.ю.н.: 12.00.12. – М., 2021. – 242 с.

91 Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. ... к.ю.н.: 12.00.12 / Байкальский государственный университет. – Иркутск, 2017. – 211 с.

92 Зуев С.В., Зазулин А.И. Цифровой УПК: новая концепция развития права // Правопорядок: история, теория, практика. – 2024. – № 1(40). – С. 67–77.

93 Гаврилин Ю.В., Победкин А.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. – 2018. – № 3(47). – С. 106–113.

94 Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. Международный опыт. – М.: Норма, 2004. – 432 с.

95 Россинская Е.Р. Система теории цифровизации судебно-экспертной деятельности // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 3. – С. 20–32.

96 Маликов С.В. Пробелы уголовного законодательства о преступлениях в сфере компьютерной информации // Институциональные основы уголовного права РФ. – Краснодар: Кубанский государственный университет, 2024. – С. 504–513.

97 Shaisultanov S., Akimzhanov T., Abdrakhmanov B., Bazarlinova A. Combating Internet Fraud through Operative-Search Measures // Revista de Direito, Estado e Telecomunicaçõ̃es. – 2024. – Vol. 16, No. 2. – P. 257–275.

98 Tolybayeva A., Issayeva A., Zhumagulova Sh., Ashimova E., Baitukayeva D.U. Problems of electronic criminal procedure in Kazakhstan and comparative analysis of foreign digital investigation models // Journal of actual problems of jurisprudence. – 2025. – № 4(116). – P. 125–140.

99 Mukhamadieva G.N., Zhanibekov A.K., Apsimet N.M., Alimkulov Y.T. Integration of Artificial Intelligence into Criminal Procedure Law and Practice in Kazakhstan // Laws. – 2025. – Vol. 14, No. 6. – Art. 98. – P. 1–33.

100 Пастухов П.С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Вестник Пермского университета. Юридические науки. – 2023. – № 62. – С. 522–540.

101 Абрамова Л.Л. Фактические основания для начала предварительного расследования: эволюция нормативного регулирования, теория и практика: дис. ... к.ю.н.: 12.00.09. – Омск, 2022. – 267 с.

102 Подваркова М.Ю. Некоторые проблемы разграничения гражданско-правовых отношений и уголовно наказуемого деяния, разграничения мошенничества со смежными составами преступлений против собственности, совершаемых путем обмана и злоупотребления доверием // Имущественные отношения в Российской Федерации. – 2019. – № 7. – С. 76–82.

103 Сабырбаева А.Б. Производство доследственной проверки по делам о мошенничестве: тактические особенности, проблемы и способы их решения // Yurisprudensiya. – 2022. – № 3. – С. 160–166.

104 Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения // Российско-

Азиатский правовой журнал. – 2022. – № 2. – С. 49–55.

105 Капустюк П.А., Грибунов О.П., Старичков М.В., Шаевич А.А., Третьякова Е.И. Расследование мошенничества в сфере компьютерной информации: учебное пособие. – Иркутск: ФГКОУ ВО ВСИ МВД России, 2018. – 48 с.

106 №5522-20-00-1/199 қылмыстық ісі бойынша Павлодар облысы Екібастұз қалалық сотының 2021 жылғы 02 сәуірдегі үкімі. https://office.sud.kz/

107 №7511-22-00-1/725 қылмыстық ісі бойынша Алматы қаласы Алмалы аудандық сотының 2022 жылғы 02 қарашадағы үкімі. https://office.sud.kz/

108 №5522-21-00-1/146 қылмыстық ісі бойынша Павлодар облысы Екібастұз қалалық сотының 2021 жылғы 06 желтоқсандағы үкімі. https://office.sud.kz/

109 Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. – 2015. – № 3(90). – С. 145–149.

110 №7135-23-00-1/179 қылмыстық ісі бойынша Астана қаласының Қылмыстық істер жөніндегі ауданаралық сотының 2023 жылғы 26 мамырдағы үкімі. https://office.sud.kz/

111 Голятина С.М. Методика расследования хищений электронных денежных средств: дис. ... к.ю.н.: 12.00.12 / Волгоградская академия МВД России. – Волгоград, 2022. – 196 с.

112 Грудинин И.А. Средства доказывания в уголовном судопроизводстве: система, содержание, гносеологические аспекты: дис. ... к.ю.н. – Хабаровск, 2012. – 190 с.

113 Гущин А.Н. Проблемы использования результатов оперативно-розыскной деятельности в доказывании по уголовным делам: дис. ... к.ю.н.: 12.00.09. – Саратов, 2002. – 180 с.

114 Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. ... к.ю.н.: 12.00.09. – Екатеринбург, 2018. – 268 с.

115 Шавалеев Б.Э. Мошенничество с использованием электронных средств платежа: уголовно-правовой и криминологический аспекты: дис. ... к.ю.н.: 12.00.08. – Казань, 2024. – 216 с.

116 Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Актуальные проблемы российского права. – 2010. – № 4. – С. 201–205.

117 Глазатова С.В., Бурцева Е.В., Медведева С.В. Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // Российский следователь. – 2021. – № 2. – С. 7–10.

118 Бастрыкин А.И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. – 2017. – Т. 11, № 1. – С. 5–12. – DOI 10.17150/2500-4255.2017.11(1).5-12.

119 Пудовкин А.А. Уголовно-правовые и криминологические особенности мошенничества: дис. ... к.ю.н. – СПб., 2007. – 114 с.

120 Евдокимов К.Н. Основные причины компьютерной преступности в современной России // The Journal of Siberian and Far Eastern Studies. – 2015. – № 8. – С. 62–67.

121 Макарова Н.Ю. Методика расследования мошенничества, совершенного в сфере малоэтажного строительства: дис. ... к.ю.н.: 12.00.12. – Санкт-Петербург, 2014. – 183 с.

122 Дорохов В.Я. Понятие доказательства в советском уголовном процессе // Советское государство и право. – 1964. – № 9. – С. 108–117.

123 Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. – Воронеж: Воронежский государственный университет, 2001. – 176 с.

124 Әпсімет Н.М., Алимкулов Е.Т. Цифрлық іздер дәлелді базаның негізі ретінде // «Қазіргі уақыттағы криминалдық қауіптер және жеке адамның, қоғамның антикриминалдық қауіпсіздігінің бағыттары»: халықар. ғыл.-тәж. конф. материалдары. – Алматы, 2024. – 75–79 б.

125 Қазақстан Республикасының Цифрлық кодексі: 2026 жылғы 9 қаңтардағы № 255-VIII ҚРЗ. https://adilet.zan.kz/kaz/docs/K2600000255

126 Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... к.ю.н.: 12.00.12 / Академия управления МВД России. – М., 2018. – 199 с.

127 Калиев А.А. Отдельные аспекты расследования интернет-мошенничества // Вестник Института законодательства и правовой информации Республики Казахстан. – 2025. – Т. 80, № 2. – С. 294–302.

128 Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: дис. ... к.ю.н.: 12.00.12 / Кубанский государственный аграрный университет им. И.Т. Трубилина. – Краснодар, 2021. – 207 с.

129 Аубакирова А.А. Фиксация доказательств в криминалистике и судопроизводстве: дис. ... к.ю.н.: 12.00.09. – Алматы, 1999. – 199 с.

130 Шихалиева С.З. Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме // Правовое государство: теория и практика. – 2025. – № 1(79). – С. 256–264.

131 Apsimet N., Alimkulov Y., Konysbay B., Zhanibekov A., Muratova A. Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international practice // IDP. Revista de Internet, Derecho y Política. – 2026. – No. 44. – P. 1–14.

132 Балакшин В.С. Доказательства в теории и практике уголовно-процессуального доказывания: важнейшие проблемы в свете УПК Российской Федерации: дис. ... д.ю.н.: 12.00.09 / Уральская государственная юридическая академия. – Екатеринбург, 2005. – 533 с.

133 Бахтеев Д.В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений: дис. ... д.ю.н.: 5.1.4 / Уральский государственный юридический университет. – Екатеринбург, 2022. – 504 с.

134 Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2(89). – С. 193–202.

135 Семикаленова А.И. Судебная компьютерно-техническая экспертиза: проблемы компетенций экспертов // Вестник криминалистики. – 2020. – № 2(74). – С. 70–74.

136 Нурбеков И.М. Взаимодействие правоохранительных и компетентных органов при расследовании компьютерных преступлений международного характера: дис. ... к.ю.н.: 12.00.09 / Московский государственный университет им. М.В. Ломоносова. – М., 2010. – 301 с.

137 Терентьева Л.В. Принципы установления территориальной юрисдикции государства в киберпространстве // Lex russica. – 2019. – № 7(152). – С. 119–129.

138 Матвеева Я.М., Оленников С.М. Конкуренция уголовно-правовых юрисдикций и компьютерные преступления // Петербургский юрист. – 2017. – № 2. – С. 31–36.

139 Толпекин К.А. Международные, национальные и интеграционные нормы ЕАЭС об использовании информационных приемов цифровой криминалистики в противодействии киберпреступлениям // Международное сотрудничество евразийских государств: политика, экономика, право. – 2017. – № 4. – С. 87–96.

140 Maras Marie-Helen. Cybercriminology. – Oxford University Press, 2016. – 448 p.

141 Осипенко А.Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. – 2016. – № 3. – С. 83–90.

142 Агарко А.А. О проблеме противодействия онлайн мошенничеству в современном Казахстане // Вестник Торайгыров университета. Серия: Юридическая. – 2025. – № 1. – С. 6–15.

143 №5516-22-00-1/28 қылмыстық ісі бойынша Павлодар облысы Ақсу қалалық сотының 2022 жылғы 17 шілдедегі үкімі. https://office.sud.kz/

144 Apsimet N.M. Crimes involving deepfake in online fraud and the challenges of proving them // Bulletin of the Institute of Legislation and Legal Information of the RK. – 2025. – Vol. 80, № 3. – P. 357–368.

145 Комов А.В. Использование компьютерных (цифровых) следов при выявлении, раскрытии и расследовании преступлений: дис. ... к.ю.н.: 5.1.4 / Московский университет МВД России им. В.Я. Кикотя. – М., 2025. – 279 с.

146 Семикаленова А.И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина. – 2019. – № 5(57). – С. 115–120.

147 Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитеті. Ситуациялық орталық. https://qamqor.gov.kz/stats/d/adfgwzb/svedenija-po-prestupnosti-dlja-gp?var-q_srzID_old=1119530&var-q_srzID=1119529&var-q_regID=19&var-

year_old=2025&var-year_new=2026&kiosk=true&orgId=1&from=now-6h&to=now&timezone=Asia%2FAlmaty

148 Майорова Е.И., Улейчик В.В., Яковлева Л.В. Проблемы отграничения мошенничества от гражданско-правовых споров // Проблемы предварительного следствия и дознания: сборник научных трудов. – М.: ВНИИ МВД России, 2021. – Т. 30. – С. 42–53.

149 Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теории информационно-компьютерного обеспечения криминалистической деятельности: монография. – М.: Проспект, 2022. – 256 с.

150 Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. – Омск: Омская академия МВД России, 2009. – 480 с.

151 Қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға), терроризмді қаржыландыруға және жаппай қырып-жою қаруын таратуды қаржыландыруға қарсы іс-қимыл туралы: Қазақстан Республикасының 2009 жылғы 28 тамыздағы № 191-IV Заңы. https://adilet.zan.kz/kaz/docs/Z090000191_

152 Давыдов В.О., Тишутина И.В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 3. – С. 20–27.

153 Кулаевский А.В. Алгоритмизация деятельности следователя по установлению лица, совершившего дистанционное мошенничество: дис. ... к.ю.н.: 5.1.4 / Алтайский государственный университет. – Барнаул, 2025. – 250 с.

154 Поляков Н.В. Особенности методики расследования незаконного обналичивания и транзитирования денежных средств: дис. ... к.ю.н.: 12.00.12 / Сибирский юридический институт МВД России. – Красноярск, 2021. – 241 с.

155 Набатов М.Б. Реализация права на защиту в уголовном процессе в условиях применения цифровых технологий: дис. ... к.ю.н.: 5.1.4 / Московская государственная юридическая академия им. О.Е. Кутафина. – М., 2023. – 241 с.

156 Шихалиева С.З. Судебные экспертизы объектов в цифровой форме: прогнозирование и профилактика экспертных ошибок: дис. ... к.ю.н.: 5.1.4 / Московская государственная юридическая академия им. О.Е. Кутафина. – М., 2025. – 246 с.

157 Зуев С.В., Зазулин А.И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. – 2024. – № 2(41). – С. 48–54. – DOI 10.47475/2311-696X-2024-40-1-48-54.

158 Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. – 2019. – № 5. – С. 31–44.

159 Головин А.Ю., Давыдов В.О. Криминалистическая категория «информационное обеспечение расследования преступлений» // Актуальные проблемы криминалистики и судебной экспертизы: материалы междунар. науч.-практ. конф. – 2020. – С. 30–33.

160 Әпсімет Н.М. Онлайн алаяқтықты сотқа дейінгі тергеуде инновациялық технологияларды қолдану қоғамның қылмысқа қарсы қауіпсіздігінің элементі ретінде // Жаңа ғаламдық ақиқаттағы Қазақстанның құқық қорғау жүйесі: ахуал, реформа, даму: халықар. ғыл.-тәж. конф. материалдары. – Алматы, 2024. – 114–

124 б.

161 Apsimet N.M., Muratova A.Zh. On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud // Вестник Карагандинского университета. Серия: Право. – 2025. – № 1(117). – С. 87–97.

162 Буйнов Д.О. Теория и практика собирания и экспертного исследования цифровых следов по уголовным делам в сфере экономической деятельности: дис. ... к.ю.н.: 5.1.4 / Московская государственная юридическая академия им. О.Е. Кутафина. – М., 2023. – 229 с.

163 Шаталов А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции // Вестник Сибирского юридического института МВД России. – 2018. – № 3(32). – С. 7–15.

164 Federal Bureau of Investigation. Internet Crime Report 2024. – 2024. https://www.ic3.gov

165 Protection from Scams Act 2025. – Parliament of Singapore, 2025. https://sso.agc.gov.sg/Act/PSA2025

166 Әпсімет Н.М., Алимкулов Е.Т., Муратова А.Ж. Эффективные практики зарубежных правоохранительных органов в расследовании онлайн мошенничества // Ученые труды Алматинской академии МВД Республики Казахстан имени М. Есбулатова. – Алматы, 2024. – № 4(81). – С. 425–433.

167 Волеводз А.Г. Международное сотрудничество в сфере уголовного судопроизводства – уроки истории и некоторые проблемы реформирования // Международное уголовное право и правосудие. – 2014. – № 4. – С. 13–17.

168 Eurojust and Europol. Common Challenges in Cybercrime 2024 Review by Eurojust and Europol. – Publications Office of the European Union, 2025. – DOI 10.2813/3243780.

169 European Union Agency for Law Enforcement Cooperation and European Union Agency for Criminal Justice Cooperation. SIRIUS EU Electronic Evidence Situation Report 2024. – 2024. https://www.europol.europa.eu/

170 Шестак В.А., Чеботарь А.С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. – 2023. – № 8. – С. 305–310.

171 Клевцов К.К., Васюков В.Ф. Получение электронной информации по уголовным делам в рамках международного сотрудничества // Вестник Санкт-Петербургского университета. Право. – 2021. – Т. 12, № 1. – С. 36–51.

172 Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. ... к.ю.н.: 12.00.09 / Московская государственная юридическая академия им. О.Е. Кутафина. – М., 2016. – 158 с.

173 Mukhamadieva G.N., Alimkulov E.T., Zhanibekov A.K., Sharipova A.B., Apsimet N.M. Automation of lawmaking: prospects for the implementation of artificial intelligence technology // Bulletin of Al-Farabi Kazakh National University. Law

Series. – 2025. – № 2(114). – С. 28–37. – DOI 10.26577/JAPJ202511423.

174 Қамбаров А.Қ. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар (қылмыстық-құқықтық және криминологиялық аспектілері): философия докторы (PhD) дәрежесін алу үшін дайындалған диссертация / Alikhan Bokeikhan University. – Семей, 2024. – 171 б.

175 Костюченко М.А. Кредитные преступления (ст.ст. 176, 177 УК РФ): характеристика и предупреждение: дис. ... к.ю.н.: 12.00.08 / Всероссийский государственный университет юстиции (РПА Минюста России), Иркутский институт (филиал). – Иркутск, 2020. – 253 с.

176 Тагиров Р.А. Первоначальный этап расследования мошенничества в сфере кредитования: дис. ... к.ю.н.: 12.00.12 / Башкирский государственный университет. – Уфа, 2022. – 236 с.

177 Әпсімет Н.М., Алимкулов Е.Т. Онлайн қылмыстарды тергеу кезінде конституциялық құқықтарды қорғау // «Сот және құқық қорғау жүйесін дамытудың тұжырымдамалық бағыттары: республикалық және халықаралық-құқықтық тәжірибе»: халықар. ғыл.-тәж. конф. материалдары. – Алматы: әл-Фараби атындағы КазҰУ, 2024. – 41–47 б.

178 Ахатова А.М. Дроп как соучастник преступлений, совершенных с использованием информационно-телекоммуникационных сетей: проблемы уголовно-правовой оценки и правоприменения // Вестник Удмуртского университета. Серия: Экономика и право. – 2024. – Т. 34, № 6. – С. 1075–1083.

179 Mukhamadieva G.N., Alimkulov Y.T., Zhanibekov A.K., Sharipova A.B., Apsimet N.M. The problems of regulating the powers of the prosecutor to supervise the procedural activities of the bodies of inquiry and preliminary investigation // Bulletin of Al-Farabi Kazakh National University. Law Series. – 2024. – № 3(111). – P. 110–118.

180 Қазақстан Республикасындағы банктер және банк қызметі туралы: Қазақстан Республикасының 2026 жылғы 16 қаңтардағы № 258-VIII ҚРЗ. https://adilet.zan.kz/kaz/docs/Z2600000258

181 Widhaningroem W., Widowaty W. The application of regulations in prosecuting cyber crime in identity theft on e-commerce platforms in Indonesia // Formosa Journal of Social Sciences. – 2024. – Vol. 3, no. 3. – P. 441–456. – DOI 10.55927/fjss.v3i3.9797.

182 Anti-Telecom and Online Fraud Law of the People's Republic of China. – National People's Congress, 2022. https://en.moj.gov.cn/2023-12/15/c_948363.htm

Қосымша А

САУАЛНАМА
Құрметті сауалнамаға қатысушы!

Сізден онлайн алаяқтық (киберқылмыстар) фактілерін анықтау, саралау және тергеп-тексеру мәселелеріне арналған сауалнамаға қатысуыңызды сұраймыз. Сіздің білікті жауаптарыңыз Қазақстан Республикасының Қылмыстық-процестік кодексі нормаларын және криминалистикалық тактиканы жетілдіру бойынша ғылыми негізделген ұсынымдар әзірлеуге көмектеседі. Сауалнама анонимді сипатта жүргізіледі, нәтижелер жалпыланған түрде пайдаланылады.

Өз пікіріңізбен сәйкес келетін жауап нұсқасын қоршап немесе астын сызып көрсетіңіз, қажет болған жағдайда өз нұсқаңызды жазыңыз.

I БЛОК. САУАЛНАМАҒА ҚАТЫСУШЫ ТУРАЛЫ ЖАЛПЫ МӘЛІМЕТТЕР

1. Сіздің лауазымыңыз:
а) тергеуші / аға тергеуші;
ә) анықтаушы;
б) жедел уәкіл (оның ішінде киберқылмысқа қарсы күрес бөлімшелерінің);
в) прокурор;
г) судья;
ғ) басқа (көрсетіңіз): _____.

2. Сіздің практикалық жұмыс өтіліңіз:
а) 1 жылға дейін;
ә) 1 жылдан 5 жылға дейін;
б) 5 жылдан 10 жылға дейін;
в) 10 жылдан жоғары.

3. Интернет-алаяқтықты (киберқылмыстарды) тергеп-тексеру саласындағы өзіңіздің кәсіби дайындығыңыздың деңгейін бағалаңыз (1 – төмен, 5 – жоғары):

	1	**2**	**3**	**4**	**5**
Кәсіби дайындық деңгейі	☐	☐	☐	☐	☐

II БЛОК. ЗАҢНАМАНЫ БАҒАЛАУ ЖӘНЕ ОНЛАЙН АЛАЯҚТЫҚТЫҢ ТҮРЛЕРІ

4. Сіздің ойыңызша, Қазақстан Республикасының қолданыстағы қылмыстық-процестік заңнамасы (ҚР ҚПК) киберқылмыстарды тергеп-тексеруге толық көлемде бейімделген бе?
а) иә, толық көлемде бейімделген;
ә) жалпы бейімделген, бірақ нақтылауды талап етеді;
б) жеткіліксіз бейімделген, елеулі өзгерістер қажет;
в) жауап беруге қиналамын.

5. Сіздің тәжірибеңіз бойынша интернет-алаяқтықтың қандай түрлері жиі кездеседі?
а) фишинг (дербес деректерді / карта деректемелерін ұрлау);
ә) сауда алаңдарындағы жарнамаларды пайдалану арқылы алаяқтық (OLX, Kolesa және т.б.);
б) жалған инвестициялық платформаларды пайдалану арқылы алаяқтық;
в) қоңыраулар / SMS арқылы алаяқтық (вишинг / смишинг);
г) әлеуметтік желілер / мессенджерлер арқылы алаяқтық (аккаунттарды бұзу);
ғ) басқа (көрсетіңіз): _____.

III БЛОК. ЭЛЕКТРОНДЫҚ ДӘЛЕЛДЕМЕЛЕР, САРАПТАМАЛАР ЖӘНЕ ӨЗАРА ІС-ҚИМЫЛ

6. Электрондық дәлелдемелерді (бұлтты қоймалардағы ақпарат, лог-файлдар, трафик деректері және т.б.) құжаттау мен алу кезінде қандай негізгі проблемаларға тап боласыз?

а) шетелдік провайдерлерден / сервистерден ақпарат алудың күрделілігі;

ә) электрондық дәлелдемелердің өзгермейтіндігін сақтау проблемасы;

б) тиісті криминалистикалық құралдардың / бағдарламалық қамтылымның (БҚ) болмауы;

в) электрондық дәлелдемелерді алу рәсімінің құқықтық реттелуінің жеткіліксіздігі;

г) қажетті құзыреттерге ие маман-криминалистердің жетіспеушілігі;

ғ) проблемалар жоқ.

7. Интернет-алаяқтықты тергеп-тексеру кезінде криминалистикалық немесе сот сараптамаларын қаншалықты жиі тағайындайсыз?

а) тұрақты түрде (әрбір іс бойынша дерлік);

ә) мезгіл-мезгіл (күрделі жағдайларда);

б) сирек (аса қажет болған жағдайда ғана);

в) тағайындамаймын.

8. Киберқылмыстарды тергеп-тексеру кезінде банк және телекоммуникациялық ұйымдармен (екінші деңгейдегі банктер (ЕДБ), байланыс операторлары) өзара іс-қимылдың тиімділігін бағалаңыз (1 – төмен, 5 – жоғары):

	1	**2**	**3**	**4**	**5**
Өзара іс-қимылдың тиімділігі	☐	☐	☐	☐	☐

9. Сіздің ойыңызша, заманауи технологиялармен және БҚ-мен жарақтандырылған киберқылмыстарды тергеп-тексеру жөніндегі мамандандырылған бөлімшелерді (бөлімдерді) құру қажет пе?

а) иә, бұл аса қажет;

ә) қалаулы, бірақ шешуші емес;

б) жоқ, қазіргі ресурстар жеткілікті;

в) жауап беруге қиналамын.

10. Сіздің ойыңызша, интернет-алаяқтықты тергеп-тексерудің тиімділігін арттыру үшін қандай шаралар неғұрлым басым болып табылады? (әр жол бойынша бір ұяшықты белгілеңіз)

	Аса қажет	**Маңызды**	**Екінші кезектегі**
Халықаралық-құқықтық ынтымақтастықты жақсарту	☐	☐	☐
ҚР ҚПК-ге өзгерістер мен толықтырулар енгізу	☐	☐	☐
Қызметкерлердің біліктілігін тұрақты арттыру	☐	☐	☐
Бөлімшелерді заманауи жабдықпен және БҚ-мен жарақтандыру	☐	☐	☐
Жеке сектормен (IT-компаниялармен, банктермен) өзара іс-қимылды күшейту	☐	☐	☐

IV БЛОК. САРАЛАУ, ПРОЦЕСТІК МӘСЕЛЕЛЕР ЖӘНЕ ЦИФРЛЫҚ ІЗДЕРМЕН ЖҰМЫС

11. СДТБТ-нде тіркеу сатысында онлайн алаяқтықты азаматтық-құқықтық міндеттемелерді орындамаудан ажырату кезінде қиындықтарға тап боласыз ба?

а) иә, үнемі (бастапқы қасақаналықты дәлелдеуде қиындықтар туындайды);

ә) иә, кейде;

б) жоқ, ажырату қиындық тудырмайды.

12. Сіздің практикаңызда кибералаяқтық бойынша материалдар азаматтық-құқықтық даудың болуы сылтауымен қаншалықты жиі номенклатуралық іске есептен шығарылады (немесе ҚР ҚПК-нің 35-бабы бойынша қысқартылады)?

а) өте жиі (бұл жүйелі практика);

ә) мезгіл-мезгіл;

б) сирек;

в) ешқашан.

13. Сіздің ойыңызша, интернет-алаяқтық кезіндегі жоғары латенттіліктің басты себебі неде?

а) жекелеген жәбірленуші үшін келтірілген залал сомасының елеусіздігі;

ә) азаматтардың істің табысты ашылуына және қаражаттың қайтарылуына сенбеуі;

б) жәбірленушінің алдау фактісін түсінбеуі (мұны техникалық ақау деп санауы);

в) басқа (көрсетіңіз): _____.

14. Кибералаяқтық істері бойынша тергеп-тексеру мерзімдерінің жаппай үзілуінің негізгі себебі неде?

а) қылмыскерлердің анонимдендіру құралдарын (VPN, proxy, нөмірлерді ауыстыру) пайдалануы;

ә) цифрлық активтерді шығару және транзиттеу үшін «дропперлерді» пайдалану;

б) субъектілердің Қазақстан Республикасынан тыс жерде болуы;

в) банктер мен провайдерлердің сұрау салуларды орындау мерзімдерінің ұзақтығы;

г) басқа (көрсетіңіз): _____.

15. Интернет-провайдерлерден, ұялы байланыс операторларынан және банктерден жауаптар (биллингтер, IP-мекенжайлар, логтар) алудың жеделдігін қалай бағалайсыз?

а) ақпарат жедел түседі (1-3 тәулік);

ә) мерзімдер созылады (10-нан 30 тәулікке дейін), бұл процестік қарқынның жоғалуына әкеледі;

б) мерзімдер аса созылады (30 тәуліктен астам), бұл цифрлық іздердің түбегейлі жоғалуына әкеледі (серверлер логтарды жояды).

16. Сот компьютерлік-техникалық сараптамасын тағайындау кезінде сарапшыға қойылатын сұрақтарды тұжырымдау кезінде қиындықтарға тап боласыз ба?

а) иә, арнайы техникалық білім жеткіліксіз;

ә) иә, дәл дәлелдемелік мәні бар сұрақтарды таңдау қиын;

б) жоқ, шаблондарды пайдаланамын немесе әрдайым маманмен кеңесемін;

в) қиындықтар жоқ.

17. Тінту / алу барысында компьютерлік техника мен смартфондарды алу кезінде IT-маманның қатысуын міндетті деп санайсыз ба?

а) иә, міндетті (деректерді бұғаттау, шифрлау немесе қашықтан жою қаупі бар);

ә) қалаулы, бірақ тергеуші-криминалистің күшімен де болады;

б) жоқ, тергеушінің жеткілікті дағдылары бар.

18. Сіздің практикаңызда қылмыскерлердің өздерінен алынған құрылғылардағы ақпаратты қашықтан (дистанциялық) жою жағдайлары кездесті ме?

а) иә, кездесті;

ә) жоқ, кездескен жоқ;

б) жауап беруге қиналамын.

V БЛОК. ХАЛЫҚАРАЛЫҚ ЫНТЫМАҚТАСТЫҚ, ЗАҢНАМАНЫ ЖЕТІЛДІРУ ЖӘНЕ ҰСЫНЫСТАР

19. Киберқылмыстарды тергеп-тексеру кезінде халықаралық тергеу тапсырмаларын (құқықтық көмек көрсету туралы сұрау салуларды) жіберу қажеттілігіне қаншалықты жиі тап боласыз?

а) әрбір қылмыстық іс бойынша дерлік;

ә) шамамен істердің 50%-ында;

б) сирек;

в) ешқашан.

20. Халықаралық өзара іс-қимыл кезіндегі басты кедергі не болып табылады?

а) шетел мемлекеттерінің сұрау салуларды орындау мерзімдерінің ұзақтығы;

ә) ресімдеудің күрделі бюрократиялық рәсімі;

б) шетелдік IT-компаниялардың (әлеуметтік желілердің, криптобиржалардың) деректерді беруден бас тартуы;

в) басқа (көрсетіңіз): _____.

21. ҚР ҚПК-де жаңа дербес тергеу әрекетін – «бөлінген желілерден / бұлтты қоймалардан компьютерлік ақпаратты алуды (шығарып алуды)» бекіту идеясын қолдайсыз ба?

а) иә, алу мен тінту туралы қолданыстағы нормалар ескірген және виртуалды ортаға жарамайды;

ә) иә, бірақ ҚР ҚПК-нің қолданыстағы баптарына толықтырулар енгізу жеткілікті;

б) жоқ, қолданыстағы ҚР ҚПК әбден жеткілікті.

22. Интернет-алаяқтықты тергеп-тексеруді оңтайландыру бойынша Сіздің жеке ұсыныстарыңыз:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Қатысқаныңыз үшін алғыс айтамыз!