ҒТАМР 10.79.21 **DOI 10.47649/vau.25.v79.i4.47**
ӘОЖ 347.4

Е. Нұрмағанбет[1] , Р. Шайхаденов[1] , А. Конысов[2]*

[1]Ш.Есенов атындағы Каспий технологиялар және инжиниринг университеті,
Ақтау қ., Қазақстан Республикасы
[2]А.Байтұрсынұлы атындағы Қостанай өңірлік университеті,
Қостанай қ., Қазақстан Республикасы
*e-mail: akylbek.konyssov@yu.edu.kz

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫ ТЕРГЕУДЕГІ ПРОКУРОРЛЫҚ ҚАДАҒАЛАУ: ҚҰҚЫҚТЫҚ РЕТТЕУ МЕН ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕ

Аңдатпа

Мақала қазіргі құқықтық қатынастар жүйесіндегі өзекті мәселелердің бірі – ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды тергеудегі прокурорлық қадағалау институтының теориялық және тәжірибелік аспектілерін кешенді түрде талдауға бағытталған. Мақаланың мақсаты – цифрлық дәуір жағдайында прокурорлық қадағалау тетіктерін жетілдірудің ғылыми негіздерін айқындау және қылмыстық процестің тиімділігін арттыру бағытындағы ұсыныстар әзірлеу болып табылады. Зерттеу барысында жалпы ғылыми және арнайы-құқықтық әдістер кешені пайдаланылды, оның ішінде жүйелік талдау, салыстырмалы-құқықтық, тарихи-құқықтық, статистикалық және модельдеу әдістері қолданылды. Авторлық тұжырымдар мен қорытындылар Қазақстан Республикасының қолданыстағы қылмыстық заңнамасы мен Германия, Жапония, Қытай, Испания және АҚШ мемлекеттерінің құқықтық реттеу тәжірибесін жан-жақты ғылыми талдау нәтижесінде негізделіп әзірленді. Зерттеу нәтижесінде прокурорлық қадағалаудың ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды тергеудегі рөлі мен шекарасы нақтыланып, цифрлық дәлелдемелермен жұмыс істеудің «chain-of-custody» қағидатына негізделген халықаралық стандарттарын енгізу қажеттілігі дәлелденді. Криптовалюта және өзге де цифрлық активтерге қатысты KYC/AML талаптарын жетілдіру мен ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар бойынша ведомствоаралық өзара іс-қимылды нығайтудың маңыздылығы көрсетілді. Зерттеу нәтижелері құқық қорғау органдарының қызметін жетілдіруге, ақпараттық қауіпсіздік саласындағы ұлттық заңнаманы халықаралық стандарттармен үйлестіруге және ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды тергеудегі прокурорлық қадағалаудың жаңа форматын қалыптастыруға бағытталған.

Негізгі сөздер: прокурорлық қадағалау, ақпараттық технологиялар, киберқылмыс, цифрлық дәлелдеме, құқықтық реттеу, халықаралық стандарттар.

Кіріспе

Қазіргі қоғамдағы цифрлану үдерісі ақпараттық технологиялар инфрақұрылымын экономика, мемлекеттік басқару және әлеуметтік қатынастардың негізгі құрамдас бөлігіне айналдырып, қылмыстық қол сұғушылықтардың жаңа нысандары мен тәсілдерінің қалыптасуына алғышарттар жасады. Аталған қылмыстық құқық бұзушылықтардың трансшекаралық сипатта болуы, дәлелдемелердің динамикалық әрі ұшқыр табиғаты, келтірілетін зиян көлемінің жедел ұлғаюы тергеу қызметінің әдіснамалық және ұйымдастырушылық күрделілігін арттырып, прокурорлық қадағалау тетіктерін жаңаша ғылыми-құқықтық тұрғыда қайта пайымдауды қажет етеді. Осы орайда, халықаралық деңгейде компьютерлік қылмыстарға қарсы іс-қимылдың бірыңғай құқықтық негізін қалыптастыруға бағытталған Будапешт конвенциясы (2001 ж.) мемлекеттер үшін қылмыс құрамдарын үйлестіру, электрондық дәлелдемелерге қол жеткізу рәсімдерін нақтылау және құқық қорғау органдарының шұғыл өзара іс-қимылын қамтамасыз ету тұрғысынан маңызды құрал болып табылады. Конвенцияда көзделген міндеттемелер ұлттық заңнамалар мен қадағалау тәжірибесін трансшекаралық киберқылмыспен тиімді күрес жүргізу талаптарына сәйкестендіруге мүмкіндік береді [1].

Ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды саралаудағы мемлекеттер арасындағы айырмашылықтар қылмыстық құқықтық құрамдардың шекараларын айқындауда әркелкілік тудырып, құқық қолдану тәжірибесінде үйлесім мен бірізділіктің жеткіліксіздігіне әкеледі. Бұл әсіресе қатаң кіру және контенттік бақылау режимдерін енгізген юрисдикциялар, соның ішінде Қытай Халық Республикасының қылмыстық заңнамасы мысалында айқын байқалады. Мәселен, ҚХР Қылмыстық кодексінің 285–287-баптарында «компьютерлік ақпараттық жүйелерге заңсыз қол жеткізу», «жүйенің жұмысын бұзу», «зиянды бағдарламаларды тарату» секілді әрекеттер үшін қатаң жауапкершілік бекітілген, сондай-ақ ұлттық қауіпсіздік пен

әлеуметтік тұрақтылыққа қатер төндіретін цифрлық контентті өндіру мен таратуды бөлек қылмыс ретінде қарастыру үрдісі басым. Бұл өз кезегінде құқықтық саясаттың технологиялық трансформацияларға бейімделу жылдамдығын айқындай отырып, трансшекаралық деректер алмасу, дәлелдемелердің цифрлық сипаты және юрисдикцияны белгілеу сияқты жаңа процессуалдық және дәлелдемелік дилеммалардың пайда болуына себеп болады. [2].

Цифрлық активтер экожүйесінің (блокчейн технологиясы, криптовалюталар және өзге де децентрализденген қаржы құралдары) қарқынды кеңеюі алаяқтық, ақшаны жылыстату және нарықтық манипуляциялар сияқты құқыққа қарсы әрекеттердің тәуекелдерін едәуір арттырды. Dark Web платформалары мен криптовалюта инфрақұрылымына қатысты даулар құқық қорғау органдарынан дәлелдеу стандарттарын қайта қарауды, ал прокурорлық қадағалау тәжірибесінен цифрлық деректердің шығу тегі мен қозғалысын (chain of custody) қатаң бақылауға алу тетіктерін енгізуді талап етеді [3].

Осы тұрғыда Қазақстан Республикасының Қылмыстық кодексі ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды жүйелі түрде жіктей отырып, 205–213-баптарында ақпаратқа заңсыз қол жеткізу, деректерді жою немесе түрлендіру, ақпараттандыру объектілерінің жұмысын бұзу, зиянды бағдарламалық қамтамасыз етуді әзірлеу мен таратудың өзге де нысандары үшін қылмыстық жауаптылық белгілейді. Алайда, дәлелдемелердің цифрлық табиғаты мен олардың жоғары динамикасы тергеу тактикасын, прокурорлық қадағалау тетіктерін ақпараттық технологиялар саласының ерекшеліктеріне бейімдеу қажеттілігін өзекті күйде сақтап отыр [4].

Зерттеудің мақсаты – ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды қылмыстық-құқықтық саралаудың теориялық-әдіснамалық негіздерін айқындау, прокурорлық қадағалаудың тиімді тетіктерін жетілдіру және ұлттық қылмыстық заңнаманы халықаралық стандарттармен үйлестіруге бағытталған ұсыныстар әзірлеу болып табылады. Зерттеу нысаны – ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды қылмыстық-құқықтық саралау мен оларды тергеу үстінен прокурорлық қадағалаудың тетіктері. Зерттеу пәні – қылмыстық құқық бұзушылықтардың құрамдық белгілері, цифрлық дәлелдемелердің жинақталуы мен сақталу ерекшеліктері, юрисдикцияаралық ынтымақтастықтың модельдері мен оларды өңірлік үлгілік реттеулермен үйлестіру тетіктері болып табылады.

Зерттеу материалдары мен әдістері

Зерттеу материалдары мен әдістері зерттеу нысанның күрделілігі мен көпқырлылығын ескере отырып таңдалды. Зерттеу мәдени-құқықтық әртектілікті қамтитын салыстырмалы-құқықтық және доктриналық талдау әдістеріне негізделіп, құқықтық жүйелер арасындағы ұқсастықтар мен айырмашылықтарды айқындауға бағытталды. Эмпирикалық деректерді жүйелі талдау үшін кейс-стади және нормативтік модельдеу тәсілдері қолданылды. Методологиялық негіз ретінде Будапешт конвенциясының қылмыстық құқық бұзушылықтар таксономиясы алынған, бұл ақпараттық технологиялар саласындағы қылмыстық-құқықтық реттеуді халықаралық стандарттар контексінде зерттеуге мүмкіндік берді. Материалдар корпусына АҚШ-тың Computer Fraud and Abuse Act, Ұлыбританияның Computer Misuse Act, Қытайдың қылмыстық кодексі мен киберқауіпсіздік туралы Заңы, БАӘ-нің №5 Заңы, ТМД елдерінің ұлттық актілері, сот тәжірибесінің деректері және ведомстволық нұсқамалар енгізілді.

Қазақстандық сегментте талдау ҚР ҚК-нің 205-213 баптары бойынша диспозициялық және санкциялық құрылымды, құрам элементтерінің (объект, объективтік және субъективтік жақтар) үйлесімін және прокурорлық уәкілеттіктерді қамтыды.

Салыстырмалы-құқықтық талдау Германия, Испания, Жапония, АҚШ, Ұлыбритания, БАӘ және ТМД елдерінің құқықтық жүйелерін қамтып, типологиялық ұқсастықтар мен айырмашылықтарды анықтауға бағытталды. Негізгі салыстыру нүктесі ретінде ТМД-ның Үлгілік қылмыстық кодексі алынды [5]. Эмпирикалық деңгейде Mt.Gox, Silk Road және Bitfinex істері бойынша кейс-стади жүргізіліп, олардың инциденттік ерекшеліктері (құрал, тәсіл, зиян және дәлелдеу қиындығы) талданды.

Техникалық-құқықтық талдау блокчейн-транзакциялар мен желілік деректерді зерттеу арқылы дәлелдемелік ізді карталауға бағытталды. Сенімділік пен жарамдылықты қамтамасыз ету мақсатында дереккөздердің үштік тексеру әдісі (нормативтік мәтін, доктриналық түсіндірме, эмпирикалық дерек) қолданылды. Репликация мен сыртқы валидтілік Жапонияның статистикалық бақылау тәжірибесімен салыстыру арқылы бағаланды.

Нәтижелер және оларды талқылау

Ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды саралаудың көпөлшемді моделі әзірленді. Аталған модель өзара функционалдық байланыстағы бес негізгі өлшемнен тұрады: қолсұғушылық объектісі (*object*), қылмыстық қолсұғушылық заты немесе материалы

(*asset/data*), қылмыс жасау құралы (*tool*), іске асыру тәсілі (*modus operandi*) және контенттік құрам (*content*). Бұл құрылым Будапешт конвенциясында айқындалған «құпиялылық – тұтастық – қолжетімділік» (confidentiality–integrity–availability) триадасымен әдіснамалық тұрғыдан үйлестіріліп, әрбір қылмыстық құрам бойынша құқыққа қарсы әрекеттің негізгі әсер векторын айқындауға мүмкіндік береді. Модельдің валидтілігі қылмыстық істердің үлгілік материалдары, ашық дереккөздердегі прецеденттер және нормашығармашылық актілер негізінде жүргізілген мазмұндық талдау арқылы тексерілді. Эмпириялық тексерім нәтижелері әзірленген модельдің дәлелдеу логикасын кезеңдік құрылымда жүйелеуге мүмкіндік беретінін және оны прокурорлық қадағалау практикасына бейімделген тексеру парақтары (checklist) форматындағы қолданбалы құрал ретінде пайдалануға болатынын көрсетті.

Модельдің практикалық маңызы үш негізгі аспектіде айқындалды.

Біріншіден, типтік құрам белгілерін өлшемдер бойынша жіктеу тәсілі тергеу органдарына дәлелдемелерді жинау және талдау процесін құрылымдауға мүмкіндік берді. Мұндай тәсіл объектіден тәсілге дейінгі дедуктивтік логиканы қамтамасыз етіп, дәлелдемелік базаны толық әрі жүйелі қалыптастыруға ықпал етеді.

Екіншіден, «құпиялылық – тұтастық – қолжетімділік» триадасы аясында негізгі құқыққа қарсы әсерді айқындау айыптау диспозициясының нақтылығын арттырды. Мысалы, ақпаратқа заңсыз қол жеткізу көбіне құпиялылыққа нұқсан келтірсе, ал деректер мен жүйелерге араласу әрекеттері негізінен тұтастық пен қолжетімділікке қауіп төндіретіні анықталды. Мұндай саралау тәсілі айыптаудың дәлдігі мен құқықтық шекараларын айқындауға мүмкіндік береді.

Үшіншіден, модельдің халықаралық және ұлттық құқықтық үлгілермен (Еуропа Кеңесінің құжаттары, Халықаралық электр байланысы одағының ITU модельдік заңы, ТМД Үлгілік кодексі) салыстырмалы талдануы оның әмбебап сипатын және бейімделгіштік әлеуетін дәлелдеді Осылайша, модельдің құрылымы әртүрлі құқықтық жүйелерде қолдануға бейім екенін және оны қылмыстық-құқықтық саралау мен прокурорлық қадағалау тәжірибесіне енгізудің ғылыми негізін қалыптастыратынын көрсетті.

Зерттеу нәтижесінде әзірленген құқықтық жіктеу моделі ақпараттық технологиялар саласындағы қылмыстарды саралау процесін жүйелеудің стандартталған алгоритмін ұсынады. Бұл модель істің бастапқы белгісінен (мысалы, рұқсатсыз ену, зиянды кодты енгізу және т.б.) бастап уәкілетті құқықтық саралауға дейінгі барлық кезеңдерді біріздендіреді, осылайша тергеу мен айыптау қызметін әдіснамалық тұрғыдан құрылымдайды.

Құқықтық жіктеу моделі архитектурасы ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды саралаудың көпдеңгейлі аналитикалық үлгісін білдіреді және бес өзекті деңгейден тұрады. Бірінші деңгей — арна (вектор), ол қылмыстық әрекеттің жүзеге асырылатын ортасын сипаттайды. Бұл деңгейде қылмыстың жүзеге асу кеңістігі желілік, бағдарламалық, аппараттық немесе гибридті сипатта болуы мүмкін. Екінші деңгей — әрекет типі, ол құқыққа қайшы ықпал ету нысанын айқындайды, атап айтқанда, ену, ұстап қалу, өзгерту немесе бұғаттау сияқты әрекеттер түрінде көрініс табады. Үшінші деңгей — зиян сипаты, келтірілген зардаптың табиғаты мен ауырлығын бейнелей отырып, материалдық, функционалдық немесе беделдік зиян түрлерін қамтиды. Сонымен қатар, бұл деңгей зорлықсыз және зорлық элементтері бар әрекеттердің ара жігін ажыратуға мүмкіндік береді. Төртінші деңгей — арнайы субъект белгілері, қылмыс субъектісінің құқықтық мәртебесін ескере отырып, қызметтік өкілетті тұлғаның, ұйымдасқан топ мүшесінің немесе трансұлттық сипаттағы қатысушының рөлін айқындайды. Бесінші деңгей — объект мәртебесі, құқыққа қарсы ықпал етілген ақпараттық жүйе мен деректердің құқықтық режимін сипаттайды және оларды аса маңызды ақпараттық-коммуникациялық инфрақұрылымға, жеке немесе коммерциялық құпияға, не мемлекеттік құпияға жатқызуға мүмкіндік береді.

Ұсынылып отырған құрылым Будапешт конвенциясының 2–5 баптарында айқындалған компьютерлік жүйелер мен деректерге қарсы қылмыстардың мазмұнымен әдіснамалық тұрғыдан өзара үйлеседі. Мұндай үйлесім киберқылмыстардың құқықтық табиғатын халықаралық стандарттар контекстінде талдауға және оларды екі деңгейлі жіктеу негізінде жүйелеуге мүмкіндік береді.

Бірінші деңгей — «қысқа мағынадағы киберқылмыстар», яғни компьютерлік жүйелер мен деректерге тікелей бағытталған құқыққа қайшы әрекеттер (мысалы, заңсыз қол жеткізу, деректерді бұзу, ақпараттық жүйелердің жұмысын бұғаттау және т.б.). Екінші деңгей — «кең мағынадағы киберқылмыстар», мұнда компьютер немесе өзге де ақпараттық технологиялар құқық бұзушылық жасау құралы ретінде қолданылады (мысалы, онлайн алаяқтық, киберэкстремизм және т.б.).

Осы әдістемелік тәсіл киберқылмыстарды құқықтық саралауда жүйелілік пен бірізділікті қамтамасыз етіп қана қоймай, дәлелдеу процесінің логикасын формализациялау арқылы прокурорлық қадағалаудың тиімділігін арттыруға бағытталған. Нәтижесінде шешім ағашының архитектурасы құқық қолдану тәжірибесінде ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды дәл, салыстырмалы және әділ бағалауға мүмкіндік беретін әмбебап аналитикалық құрал ретінде айқындалады.

Еуропа Кеңесінің Киберқылмыс жөніндегі конвенциясы (Будапешт, 2001 ж.) халықаралық-құқықтық кеңістікте киберқылмыстарды жүйелеудің негізгі таксономиясын айқындайтын базалық акт болып табылады. Конвенцияның құрылымы компьютерлік жүйелер мен деректерге қарсы қылмыстарды (2–5-баптар), компьютерді пайдалана отырып жасалатын алаяқтық пен жалғандықты, контентке қатысты құқықбұзушылықтарды (әсіресе балалар порнографиясына байланысты құрамдарды), сондай-ақ зияткерлік меншік пен қоғамдық қауіпсіздікке қарсы бағытталған әрекеттерді (кибертерроризм элементтері) қамтиды. Бұл жүйе киберқылмыстардың негізгі объектілерін — жүйе, деректер, контент және қауіпсіздік — нақты бөліп көрсетуге және олардың құқықтық қорғалуының деңгейін саралауға мүмкіндік береді.

Халықаралық электр байланысы одағының (ITU) үлгілік заңы Будапешт конвенциясының негізін кеңейте отырып, кибертерроризм ұғымын кейбір құрамдарда мақсаттық белгі ретінде енгізудің нормативтік тәсілдерін ұсынады. Мысалы, «террористік мақсаттағы рұқсатсыз қол жеткізу» немесе «инфрақұрылымға бағытталған шабуыл» сияқты құрамдарда құқықбұзушылықтың мақсаттық сипаттамасы қылмыстық-құқықтық салмаққа ие болады. Мұндай тәсіл құқық бұзушылықтың ниеті мен салдарын ажыратуға, сондай-ақ жауаптылықты саралаудың дәлдігін арттыруға бағытталған.

ТМД Үлгілік қылмыстық кодексі посткеңестік құқықтық жүйелердің ерекшеліктерін ескере отырып, рұқсатсыз қол жеткізу, ақпаратты модификациялау, компьютерлік диверсия, зиянды бағдарламаларды тарату және осындай құралдарды әзірлеу немесе өткізу сияқты құрамдарды жүйелейді. Бұл кодекс посткеңестік кеңістіктегі құқықтық техниканы унификациялау мен ұлттық заңнамаларды үйлестірудің үлгісі ретінде қызмет етеді.

Осы үш халықаралық бастама өзара толықтырушы сипатқа ие: Будапешт конвенциясы — халықаралық стандарттарды айқындайтын нормативтік өзек; ITU үлгілік заңы — мақсаттық белгілер мен терроризмге қатысты квалификациялау тәсілдерін нақтылаушы акт; ал ТМД Үлгілік кодексі — посткеңестік құқықтық кеңістікте аталған стандарттарды бейімдеу және құқықтық нормаларды унификациялау тетігі ретінде көрініс табады.

Германияның қылмыстық құқығында компьютерлік қылмыстардың жүйеленуі ұзақ мерзімді эволюция нәтижесінде бірнеше ірі блоктар бойынша қалыптасқан: экономикалық қылмыстық құқық (манипуляциялар, диверсия, тыңшылық, рұқсатсыз қол жеткізу), зияткерлік меншік, мемлекеттік ақпараттық қауіпсіздік және қылмыстық-процестік реттеу. Неміс құқықтық доктринасы «деректерді» құқықпен қорғалатын дербес құқықтық игілік ретінде таниды және электрондық өңдеуді тек құрал емес, қорғау нысаны ретінде қарастырады. Бұл ұстаным зерттеуде ұсынылған саралау моделіндегі «asset/data» өлшемінің дербес маңыздылығын негіздейді [6].

Қытай Халық Республикасының Қылмыстық кодексі (285–288-баптар) ақпараттық жүйелерге рұқсатсыз ену, жүйенің қалыпты жұмысына кедергі келтіру, деректерді заңсыз өзгерту және вирустарды тарату әрекеттерін жеке құрамдар ретінде нақтылайды [2]. Зардаптың ауырлығы жаза түрі мен шегін айқындауда негізгі критерий болып табылады. 2016 жылғы «Киберқауіпсіздік туралы» заң және оған ілеспе нормативтік актілер деректерді ҚХР аумағында сақтау, нақты сәйкестендіру (real-name identification) және цифрлық платформалардың жауаптылығын арттыру қағидатын бекітеді [7]. Мұндай тәсіл профилактикалық бағытты институционалдандырып, жеке деректерді қорғау мен сөз бостандығы арасындағы теңгерім мәселесін өзектендіреді.

Испанияның Қылмыстық кодексі дәстүрлі қылмыс құрамдарын цифрлық кеңістікке бейімдеп, зияткерлік меншікке, коммерциялық құпияға және шектеулі қолжетімді ақпаратқа қарсы әрекеттерді киберқылмыстар санатына енгізу арқылы құқықтық регламентацияны кеңейтеді [8]. Жапонияның құқықтық жүйесі киберқылмыстарды статистикалық және практикалық тұрғыдан екі негізгі топқа бөліп, қолдануға ыңғайлы типологияны қалыптастырған [9].

АҚШ-тың 1984 жылдан бастап бірнеше рет жаңартылған Computer Fraud and Abuse Act (CFAA) заңы рұқсатсыз қол жеткізу, компьютерлік алаяқтық, тыңшылық, қорғалған компьютерлерге зиян келтіру және бопсалау әрекеттерін қамтитын кең ауқымды құқықтық шеңберді айқындайды [10]. Санкция деңгейі келтірілген залалдың мөлшері мен ұлттық қауіпсіздік инфрақұрылымына төнген

қатердің дәрежесіне байланысты сараланады. Cybersecurity and Infrastructure Security Agency (CISA) маңызды инфрақұрылымды қорғаудың институционалдық тетігі ретінде қызмет атқарады [11].

Ұлыбританияның Computer Misuse Act (1990) және Terrorism Act (2000) актілері ақпараттық жүйелердің жұмысына заңсыз араласу әрекеттерін терроризммен байланыстырып, күшейтілген жауапкершілік режимін белгілейді [12].

Біріккен Араб Әмірліктерінің №5 заңы (2012) үш негізгі құрамдық блоктан тұрады: рұқсатсыз ену, фишинг және электрондық құжаттарды қолдан жасау; қаржы, бедел және тыңшылыққа қатысты ауыр құрамдар; сондай-ақ ұлттық қауіпсіздік пен мемлекеттік мүдделерге бағытталған әрекеттер [13].

Осы салыстырмалы талдау нәтижесінде әзірленген модельде «мақсат белгісі» (терроризм, тыңшылық, диверсия және т.б.) құрамның квалификациялаушы элементі ретінде қарастырылуы қажет деген тұжырым қалыптасты. Мұндай тәсіл киберқылмыстарды саралауда объективтік және субъективтік белгілердің өзара үйлесімділігін қамтамасыз етіп, прокурорлық қадағалаудың дәлдігі мен тиімділігін арттыруға мүмкіндік береді.

Қазақстан Республикасының Қылмыстық кодексі ақпараттық технологиялар саласындағы қылмыстарды жүйелі түрде тоғыз дербес құрамға бөледі (205–213-баптар). Оларға: ақпараттық жүйелерге рұқсатсыз қол жеткізу; ақпаратты заңсыз жою немесе түрлендіру; ақпараттандыру объектілерінің жұмысын бұзу; ақпаратты заңсыз иелену; ақпарат беруге мәжбүрлеу; зиянды бағдарламалық өнімдер мен құралдарды пайдалану немесе тарату; қолжетімділігі шектелген электрондық ресурстарды заңсыз тарату; құқыққа қайшы интернет-қызметтерін ұсыну; сондай-ақ ұялы байланыстың сәйкестендіру кодтары мен құрылғыларына заңсыз әсер ету әрекеттері жатады [14].

Бұл құрамдардың ерекшелігі – олардың аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектілеріне қатысты жасалған жағдайларда жауаптылықтың күшейтілуі. Мұндай жағдайларда әрекеттер квалификацияланған құрамдар ретінде сараланып, жаза деңгейі инфрақұрылымның әлеуметтік және экономикалық маңыздылығына сәйкес дифференцияланады.

Ұсынылып отырған құрылымдық модельде объектінің мәртебесі бастапқы классификациялық түйін ретінде алынады. Одан кейін «құпиялылық–тұтастық–қолжетімділік» қағидаты бойынша құқыққа қарсы әсер векторы айқындалып, дәлелдемелік логика қауіп деңгейімен сәйкестендіріледі. Бұл тәсіл қылмыстық-құқықтық саралаудың нақтылығын арттырып, прокурорлық айыптау процесінің дәлдігі мен негізділігін қамтамасыз етеді.

Тергеуді жоспарлау матрицасы — ақпараттық технологиялар саласындағы қылмыстарды тергеу үдерісін құрылымдауға арналған кешенді аналитикалық құрал. Оның мазмұндық құрылымы мына бағыттармен айқындалады:

1.Объект. Тергеудің бастапқы кезеңінде нысанның аса маңызды ақпараттық-коммуникациялық инфрақұрылым мәртебесі анықталады. Бұл мәртебе меншік иесінің (оператордың) ресми деректері мен техникалық құжаттамалар арқылы дәлелденеді. «Құпиялылық–тұтастық–қолжетімділік» қағидаты тұрғысынан кез келген компонентке ықпал ету мүмкіндігі бағаланады. Объектінің ақпараттық-коммуникациялық инфрақұрылым мәртебесі анықталған жағдайда, ол құқықтық тұрғыдан бағалау кезінде ауырлататын мән-жай ретінде қаралады.

2.Asset/Data (деректер). Тергеу барысында ықпал етілген деректердің нақты түрі белгіленеді. Негізгі дәлелдемелерге резервтік көшірмелер, хеш-суммалар, журналдар мен өзге де цифрлық іздер жатады. Бұл бағыт «құпиялылық–тұтастық–қолжетімділік» қағидаты компоненттері бойынша зардаптың сипатын анықтауға және келтірілген залалдың көлемін ғылыми негізде есептеуге мүмкіндік береді.

3.Tool (құрал). Қылмыстық құқық бұзушылық жасау кезінде пайдаланылған техникалық немесе бағдарламалық құралдың сипаттамасы талданады. Құралдың сигнатуралары мен артефактілері анықталып, оның жүйенің тұтастығы мен қолжетімділігіне әсер ету дәрежесі бағаланады. Мұндай құралдың қолданылуы құқықтық тұрғыдан «арнайы құрал пайдалану» ретінде бағаланады.

4.Modus (тәсіл). Қылмыстық құқық бұзушылық жасау тәсілі (рұқсатсыз ену, ақпаратты ұстап қалу, өзгерту, бұғаттау және т.б.) SIEM, IDS, IPS және өзге де оқиға тіркеу жүйелерінің деректері негізінде бекітіледі. Бұл тәсіл «құпиялылық–тұтастық–қолжетімділік» қағидаты бойынша әсер векторын дәл анықтап, қылмыстық кодекстің тиісті бабын нақты таңдауға мүмкіндік береді.

5.Content (контент). Заңсыз контенттің (мысалы, балалар порнографиясы, экстремистік материалдар, авторлық құқықты бұзатын файлдар) бар-жоғы сараптамалық зерттеу арқылы анықталады. Бұл компонент, негізінен, құпиялылыққа қатысты зардаптарды айқындайды және кей жағдайларда өзге құрамдармен (зияткерлік меншікке қол сұғу, адамгершілікке қарсы қылмыстар) тоғысуы мүмкін.

Ұсынылып отырған мазмұндық тәсіл тергеу кезеңінде дәлелдемелік олқылықтардың алдын алуға және оларды уақтылы жоюға мүмкіндік береді. Сонымен бірге «құпиялылық–тұтастық–қолжетімділік» қағидаты әсерінің сапалық және сандық параметрлерін жүйелі айқындау арқылы іс материалдарын құрылымдау мен құқықтық саралаудың дәлдігін арттырады. Бұл тәсіл ақпараттық технологиялар саласындағы қылмыстар бойынша прокурорлық қадағалаудың тиімділігін күшейтетін қолданбалы ғылыми нәтиже болып табылады.

Зерттеу нәтижелері криптовалюта айналымына байланысты құқық бұзушылықтарды дербес қылмыстық-құқықтық категория ретінде танудың ғылыми және практикалық негізін көрсетті. Криптовалютаның технологиялық өзегі — блокчейн немесе бағытталған граф құрылымы, консенсус алгоритмдері, ашық кілт инфрақұрылымы (PKI) және тізбекті хештеу тетігі — транзакциялардың ашық әрі псевдонимді сипатын айқындайды. Бұл ерекшелік дәстүрлі дәлелдемелік құралдардың жеткіліксіздігін аңғартып, цифрлық іздерді тіркеу мен тексерудің жаңа әдістерін енгізуді талап етеді [15].

Криптовалютаның ұғымдық тұрақтануы мен нарықтық дамуы оны қосарлы құқықтық феномен ретінде сипаттайды: экономикалық актив әрі азаматтық айналым объектісі бола отырып, ол қылмыстық құрал немесе кіріс көзіне айналуы мүмкін [16]. Mt. Gox, Silk Road, Bitfinex істері криптовалюталық құқық бұзушылықтардың трансұлттық және жасырын сипатын дәлелдеп, биржалық инфрақұрылым мен миксерлердің рөлін айқындады. Еуропалық зерттеулер виртуалды валюталардың терроризмді қаржыландыру мен ұйымдасқан қылмыс саласында қолданылу тәуекелін атап өтіп, реттеу мен бақылауды күшейту қажеттігін негіздеді.

Осы эмпириялық база негізінде әзірленген модель криптоактивтерге қатысты қылмыстық әрекеттердің *toolchain*және *modus* элементтерін нақтылап, дәлелдемелердің тізбектілігін (*chain of custody*) қамтамасыз етуге бағытталды. Бұл мақсатта блокчейн-хештер, түйін операторларының журналдары, VASP субъектілерінің KYC/AML деректері мен платформалық API жазбалары кешенді түрде пайдаланылды [17]. Мұндай тәсіл криптовалюталық операцияларды тергеуде цифрлық дәлелдемелердің сенімділігі мен трассабельдігін арттыруға мүмкіндік береді.

Талдау нәтижесінде үш негізгі нормативтік-құқықтық ұсыныс әзірленді:

1.Mixing/tumbling, privacy-coin және Defi-манипуляциялар сияқты әрекеттерге арналған дербес қылмыстық құрамдарды енгізу қажеттілігі. Бұл шаралар криптоэкономикадағы ақшаны жылыстату мен ағынды жасыру механизмдерін құқықтық тұрғыдан нақтылауға бағытталады [18];

2.VASP субъектілеріне қатысты KYC/AML және міндетті хабарлау (SAR/STR) талаптарын қатаңдату және нақтылау, бұл криптовалюталық платформалар мен құқық қорғау органдарының өзара іс-қимылын институционалдық деңгейде күшейтеді;

3.Цифрлық дәлелдемелердің chain-of-custody стандарты мен таймстамп, хеш-пег, мульти-қолтаңба сияқты механизмдерді процессуалдық тұрғыда бекіту, бұл дәлелдемелердің түпнұсқалығы мен тұтастығын қамтамасыз етеді [19].

Осылайша, зерттеу криптовалюталық экожүйені құқықтық реттеуді жетілдіру және цифрлық дәлелдемелерді жинау, сақтау, бағалау тетіктерін жаңғыртудың тұжырымдамалық негізін қалыптастырды.

Алдыңғы зерттеулерде ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар негізінен нормативтік регламентация мен техникалық феноменология тұрғысынан жеке талданған. Бұл зерттеу аталған аспектілерді біріктіріп, «evidence-by-design» тәсілі арқылы олардың өзара сабақтастығын тұтас концептуалдық модель шеңберінде жүйелендірді. Модельдің әрбір өлшемі (объект, дерек, құрал, тәсіл, контент) нақты дәлелдемелік артефактпен сәйкестендіріліп, «құпиялылық–тұтастық–қолжетімділік» векторы залал түрімен кодификацияланады, ал объектінің мәртебесі қылмыстық-құқықтық бағалау деңгейімен тікелей сәйкестенеді.

«Зерттеудің ғылыми жаңалығының маңызды қыры — криптовалюталық экожүйені дербес қылмыстық-құқықтық домен ретінде қарастыру және оны нормативтік-концептуалдық модель арқылы жүйелендіру болып табылады. Мұндай тәсіл бұрынғы фрагменттік талқылауларды біртұтас аналитикалық және реттеушілік құрылымға біріктіріп, ақпараттық және қаржылық технологиялар түйісінде туындайтын жаңа қылмыстық әрекеттердің құқықтық табиғатын кешенді бағалауға мүмкіндік берді. Бұл ретте, алғаш рет кең аудиторияға криптовалюта концепциясын таныс еткен Andy Greenberg-дің “Crypto Currency” мақаласында көрсетілген криптовалютаның технологиялық және институционалдық ерекшеліктері - децентрализация, мемлекет-банктер жүйесінен тәуелсіздігі, ашық-кодты негізде құрылуы - заңнамалық саралау үшін жаңа құқықтық шеңберді қажет ететіндігін дәлелдейтін бастапқы теоретикалық негіз ұсынады [20].

Зерттеудің айрықша ғылыми жаңалығының бірі — прокурорлық қадағалауды орталықтандыру қағидатынұсыну және оны іске асырудың құралдық негізін қалыптастыру болып табылады. Тергеу мен айыптаудың дәлелдемелік логикасын біріздендіру мақсатында стандартталған чек-парақтар мен процессуалдық тәуекел картасы әзірленді. Бұл тетіктер прокурордың ақпараттық технологиялар саласындағы істер бойынша процестік шешім қабылдау сапасын арттырып, дәлелдемелерді бағалау мен құқықтық саралау кезінде тәуекелге негізделген қадағалау моделін қалыптастыруға мүмкіндік береді.

Әдіснамалық тұрғыдан зерттеу шеңберінде кейбір эмпирикалық кейстердің талдауы ашық дереккөздермен шектелді, бұл құпия материалдарға қолжетімсіздік салдарынан жекелеген тұжырымдардың индуктивтік деңгейде қалуына әкелді [21]. Мұндай шектеу ақпараттық қауіпсіздік пен қылмыстық іс жүргізу құпиясын сақтау талаптарымен айқындалады.

Халықаралық құқықтың жоғары динамикасы мен киберреттеу тетіктерінің жиі жаңартылуы зерттеу моделін мерзімді қайта қарауды және жаңартуды талап етеді. Бұл қажеттілік, әсіресе, Будапешт конвенциясы мен оған қосымша хаттамалардың эволюциясымен, сондай-ақ трансұлттық киберқылмыстарды тергеудегі юрисдикциялық үйлестірудің күрделенуімен тікелей байланысты.

Криптоактивтер экожүйесіндегі технологиялық инновациялар — L2 протоколдары, zk-технологиялар және cross-chain бридждер — дәлелдемелерді жинау мен тексерудің дәстүрлі тәсілдеріне жаңа әдіснамалық талаптар қояды. Бұл үрдіс дәлелдемелік әдістердің үздіксіз эволюциясын, соның ішінде блокчейн транзакцияларын верификациялау мен смарт-келісімшарттарды саралау тетіктерін жетілдіруді қажет етеді.

Қолданбалы тұрғыда зерттеу ақпараттық-коммуникациялық инфрақұрылым (АКИ) істерінде инфрақұрылым операторларын процессуалдық стандарттардың міндетті қатысушылары ретінде тану қажеттігін негіздейді. Мұндай тәсіл дәлелдемелердің сақталуы мен қолжетімділігін қамтамасыз етуге бағытталған.

Құпиялылық пен қауіпсіздік арасындағы теңгерімді сақтау мақсатында «минималды өңдеу» және «дәлелдемеге бағытталған өңдеу» қағидаларын нормативтік деңгейде бекіту ұсынылады [22]. Мұндай тәсіл Ұлыбританияның Terrorism Act 2000 (Article 1–18) актісінде террористік әрекеттерге қатысты деректерді жинау, сақтау және пайдалану тәртібі бойынша көзделген құқықтық талаптарға ұқсас, яғни тергеу мүдделерін қамтамасыз етумен қатар жеке деректерді қорғаудың институционалдық тетіктерін нығайтуға мүмкіндік береді. Аталған қағидалар прокурорлық және тергеу тәжірибесінде деректермен жұмыс істеудің құқықтық айқындылығын арттырып, жеке деректерді қорғау жүйесін жетілдіруді қамтамасыз етеді.

Зерттеу нәтижелері ақпараттық технологиялар саласындағы қылмыстарды тергеу мен прокурорлық қадағалау жүйесін жетілдірудің негізгі стратегиялық бағыттарын айқындады.

Біріншіден, ұлттық типологияны жаңғырту ұсынылады. Бұл ретте Будапешт конвенциясының 2–5-баптарына сәйкес келетін базалық құрамдарға техникалық және процессуалдық индикаторларды енгізу қажет. Мысалы, «жүйеге заңсыз араласу» құрамында SIEM/IDS журналдарының мәртебесі мен форензикалық тұтастық талаптарын белгілеу құқықтық саралаудың нақтылығын арттырып, дәлелдемелердің сенімділігін күшейтеді.

Екіншіден, виртуалды активтер қызметін көрсетуші провайдерлер (VASP) мен онлайн-платформалардың жауапкершілік шеңберін кеңейту қажет. Бұл бағытта KYC/AML рәсімдерін, журнал жүргізу мен инциденттер туралы міндетті хабарлау жүйесін, сондай-ақ санкциялық режим мен тәуекелге негізделген қадағалау тетіктерін енгізу Еуропалық Одақтың 2016 жылғы регламенттерімен үйлесіп, криптоактивтер нарығын құқықтық тұрақтандыруға ықпал етеді.

Үшіншіден, chain-of-custody (дәлелдемелер тізбегін сақтау) стандартын жетілдіру қажет. Дәлелдемелердің түпнұсқалығын қамтамасыз ету үшін таймстамптау, хеш-пег технологияларын пайдалану, тәуелсіз куәландыру тетіктерін енгізу және зертханалар қызметін ISO/IEC 17025 стандартымен үйлестіру ұсынылады. Бұл сотта дәлелдемелердің мойындалуын және процессуалдық адалдықты қамтамасыз етеді.

Төртіншіден, институционалдық деңгейде ұлттық үйлестіру орталығын дамыту қажет. Мұндай құрылым АҚШ-тағы Cybersecurity and Infrastructure Security Agency (CISA) үлгісі бойынша ведомствоаралық өзара іс-қимылды, ақпарат алмасуды және инциденттерге жедел әрекет етуді қамтамасыз етуі тиіс.

Бесіншіден, прокурорлық қадағалаудың әдістемелік негізін жетілдіру мақсатында стандартталған чек-парақтар әзірленді. Олар тоғыз типтік құрам бойынша минималды дәлелдеме талаптарын,

«құпиялылық–тұтастық–қолжетімділік» әсер картасын және ақпараттық-коммуникациялық инфрақұрылым мен криптоарналарға арналған модульдерді қамтиды. Бұл құралдар дәлелдеу логикасын құрылымдауға және прокурорлық қадағалаудың тиімділігін арттыруға мүмкіндік береді.

Зерттеу барысында модельдің қолданбалы жарамдылығын бағалау мақсатында үш типтік эмпирикалық сценарий талданды. Әр сценарий ақпараттық технологиялар саласындағы қылмыстардың нақты түріне, олардың техникалық артефактыларына және «құпиялылық–тұтастық–қолжетімділік» триадасына әсер векторына негізделді.

Сценарий А — рұқсатсыз қол жеткізу (ақпараттық-коммуникациялық инфрақұрылым контексінде). Қылмыстық әрекет сыртқы желілік шабуыл арқылы жүзеге асқан. Тергеу барысында WAF/IDS журналдары, VPN-іздері және брутфорс артефактылары негізгі дәлелдемелік дереккөздер ретінде қолданылды. «Құпиялылық–тұтастық–қолжетімділік» триадасының «құпиялылық» компонентіне тікелей әсер етілгені анықталды. Ақпараттық-коммуникациялық инфрақұрылым объектісінің мәртебесі ауырлататын мән-жай ретінде танылып, SIEM және NetFlow деректерінің үйлесімді талдауы айыптау диспозициясының дәлдігін қамтамасыз етті.

Сценарий В — деректерге араласу және жүйенің жұмыс істеуіне кедергі келтіру (бұлттық инфрақұрылым). Қылмыстық әрекет инсайдерлік сипатта болған. Негізгі дәлел көздері ретінде идентификация және қолжетімділікті басқару (IAM) журналдары, өзгерістерді басқару жазбалары және оркестрация логтары пайдаланылды. «Құпиялылық–тұтастық–қолжетімділік» триадасының векторы тұтастық пен қолжетімділікке бағытталған. Immutable-log (өзгермейтін журнал) архитектурасын қолдану дәлелдемелердің сенімділігін арттырып, процессуалдық дауларды қысқартуға мүмкіндік берді.

Сценарий С — криптовалюталық алаяқтық (дезентрализденген биржа және миксерлер арқылы). Фишингтік шабуыл және криптовалюталық миксерлерді пайдалану арқылы жасалған күрделі алаяқтық тізбегі талданды. Дәлелдемелер блокчейн-транзакцияларын трассалау, VASP субъектілерінің KYC деректері және браузерлік форензика нәтижелері негізінде қалыптастырылды. «Құпиялылық–тұтастық–қолжетімділік» триадасының әсері құпиялылық пен тұтастық компоненттерін қамтыды. Транзакциялық графты биржа және кастодиан операторларының жауаптарымен валидациялау айғақтардың соттағы дәлелдік күшін күшейтті.

Үш сценарийдің салыстырмалы талдауы ақпараттық қылмыстарды дәлелдеу процесінде техникалық журналдардың, блокчейн-артефактылардың және бұлттық инфрақұрылым жазбаларының маңызын айқындап, прокурорлық қадағалауда дәлелдемелік тізбекті формалдандырудың тиімді әдістерін негіздеді.

Зерттеу көпөлшемді модельді «құпиялылық–тұтастық–қолжетімділік» векторларымен және дәлелдемелік артефакт-картамен интеграциялау арқылы ақпараттық қылмыстарды саралаудың жаңа ғылыми тәсілін ұсынды. Криптоэкожүйеге арналған дербес құрамдар пакетін нормативизациялау және прокурорлық қадағалау үшін стандартталған чек-парақтар мен тәуекел картасын әзірлеу — модельдің түбегейлі жаңалықтарының бірі болып табылады.

Модель тергеу мен айыптау стратегиясын жоспарлауды жетілдіруге, дәлелдемелерді жинау–сақтау–ұсыну циклін стандарттауға, ведомствоаралық үйлестіруді күшейтуге және соттағы дәлелдің тұрақтылығын арттыруға бағытталған. Зерттеу нәтижелері zero-knowledge және privacy-preserving технологиялар жағдайында дәлелдемелік стандарттарды бейімдеу, AI-негізделген контенттің түпнұсқалығын процессуалдық тұрғыдан дәлелдеудің үлгілерін әзірлеу, cross-border e-evidence аясында модельдік өтініш-пакеттер дайындау, АКИ-дің юрисдикциялық режимін технологиядан бейтарап нормалармен нақтылау және киберқылмыс залалын эконометрикалық тұрғыда бағалау әдістемесін сынақтан өткізу сияқты практикалық бағыттарды қамтиды.

Ұсынылған көпөлшемді модель халықаралық стандарттар мен ұлттық құқықтық ерекшеліктерді интеграциялай отырып, киберқылмыстарды саралаудың жүйелі әрі дәлелдемеге бағдарланған тәсілін ұсынады. Будапешт конвенциясының қағидаттары, ITU және ТМД үлгілік шешімдері, сондай-ақ Германия, Қытай, Испания, Жапония, АҚШ, Ұлыбритания, БАӘ тәжірибесі модельдің әмбебап бейімделу әлеуетін дәлелдейді.

Қазақстан жағдайында тоғыз құрамдық архитектураны ақпараттық-коммуникациялық инфрақұрылымның фокус процессуалдық стандарттармен және цифрлық дәлелдеме инфрақұрылымымен толықтыру қылмыстық-құқықтық ықпал ету тиімділігін арттырады [14]. Криптоактивтер саласындағы нормативизация және VASP субъектілеріне қойылатын талаптарды нақтылау құқықтық айқындық пен тәуекелдерді төмендетуге бағытталған маңызды институционалдық қадам болып табылады.

Қорытынды

Зерттеу нәтижелері ақпараттық технологиялар саласындағы қылмыстарды қылмыстық-құқықтық тұрғыдан саралаудың көпөлшемді моделін қолдану осы санаттағы құқықбұзушылықтардың құқықтық табиғатын неғұрлым жүйелі және дәл бағалауға мүмкіндік беретінін көрсетті. Бұл тәсіл қылмыс объектісін, затын, тәсілін және контентін өзара байланысты өлшемдер ретінде қарастырып, дәлелдемелерді жинау мен талдаудың логикалық құрылымын қалыптастыруға мүмкіндік береді. Мұндай әдістемелік негіз ақпараттық қылмыстарды тергеу мен прокурорлық қадағалаудың тиімділігін арттыруда қолданбалы мәнге ие.

Салыстырмалы-құқықтық талдау нәтижесінде Будапешт конвенциясының нормалары, АҚШ-тың Computer Fraud and Abuse Act (CFAA) ережелері және Қытай Халық Республикасының киберқауіпсіздік заңнамасы ұлттық құқықтық тәжірибеге бейімдеуге болатын бірқатар үлгілік шешімдерді ұсынатыны анықталды. Бұл халықаралық тәжірибе ақпараттық құқықбұзушылықтармен күресте бірыңғай стандарттарды қалыптастыру мен трансшекаралық ынтымақтастықты күшейтудің маңызын дәлелдейді.

Зерттеу барысында Қазақстан Республикасының Қылмыстық кодексінің 205–213-баптары ақпараттық технологиялар саласындағы базалық құрамдарды қамтитыны анықталды, алайда криптовалюта және блокчейн негізіндегі жаңа құқықбұзушылықтардың пайда болуы құқықтық реттеуді жаңғыртуды қажет етеді. Осыған байланысты ұлттық қылмыстық заңнамада цифрлық активтер мен виртуалды экожүйелерге қатысты арнайы нормалар енгізу ұсынылады. Бұл жаңа құқықтық құбылыстарды нақты айқындап, құқыққолдану тәжірибесіндегі түсінбеушіліктерді азайтады.

Зерттеу нәтижелері көрсеткендей, электрондық дәлелдемелермен жұмыс істеу іс жүзінде ең әлсіз буын болып отыр. Сондықтан процессуалдық деңгейде дәлелдемелерді жинау, сақтау және ұсыну стандарттарын (forensic protocols, chain-of-custody талаптары) біріздендіру қажет. Мұндай регламенттер тергеу мен сот тәжірибесінде дәлелдемелердің түпнұсқалығын қамтамасыз етуге мүмкіндік береді.

Прокурорлық қадағалау институтының тиімділігін арттыру мақсатында ақпараттық қылмыстар бойынша типтік дәлелдеме карталары мен тәуекелге негізделген чек-парақтар әзірлеу ұсынылады. Бұл құралдар айыптау дәлелдемелерінің логикалық және процессуалдық тұрақтылығын арттыруға, сондай-ақ тергеу сапасын бағалаудың бірыңғай критерийлерін енгізуге мүмкіндік береді.

Кадрлық және институционалдық аспектілер тұрғысынан құқық қорғау органдарының мамандануын күшейту, киберсараптама инфрақұрылымын дамыту және халықаралық тәжірибе алмасуды жүйелеу қажеттілігі айқындалды. Бұл қадамдар ақпараттық қылмыстарды анықтау мен дәлелдеудің практикалық деңгейін жаңа сапаға көтереді.

Болашақ зерттеулер бағытында цифрлық құқықтың динамикасына сәйкес қылмыстық-құқықтық нормалардың бейімделгіштігін модельдеу, сондай-ақ ақпараттық-коммуникациялық инфрақұрылымдарға жасалатын шабуылдардың әлеуметтік және экономикалық салдарын сандық тұрғыда бағалау өзекті болып табылады.

Жалпы алғанда, жүргізілген зерттеу нәтижелері ақпараттық технологиялар саласындағы қылмыстарды қылмыстық-құқықтық тұрғыдан саралауда жүйелі, дәлелдемеге бағдарланған тәсілдің тиімділігін дәлелдеді. Ұсынылған тұжырымдар ұлттық құқықтық саясат пен прокурорлық қадағалау тәжірибесін жетілдіруге нақты үлес қосуға бағытталған және киберқылмыстарға қарсы іс-қимылдың ғылыми-негізделген стратегиясын қалыптастыруға мүмкіндік береді.

ӘДЕБИЕТТЕР ТІЗІМІ

1 Компьютерлік қылмыс туралы конвенция. Будапешт, 23 қараша 2001 ж. 2-5. Европалық келісімдер сериясы - № 185. [Электрондық ресурс] – URL: https://online.zakon.kz/Document/?doc_id=30170556 (қаралу уақыты 01.01.2025).

2 Қытай Халық Республикасының Қылмыстық кодексі. 1979 жылғы 1 шілдеде бесінші ҚҰП екінші сессиясында қабылданды. 1997 жылғы 14 наурыздағы сегізінші ҚҰП бесінші сессиясында түзетулер енгізілді. Б. 285-288. [Электрондық ресурс] – URL: https://ru.china-embassy.gov.cn/rus/zfhz_0/zgflyd_ (қаралу уақыты 01.01.2025).

3 Н.Билтон. Киберпреступник №1. История создателя подпольной сетевой империи / [пер. с англ.]. – Москва : Эксмо, 2017. – 448 с.

4 Қазақстан Республикасының Қылмыстық кодексі 03.07.2024 ж. № 226-V ҚРЗ. (31.08.2024 ж. жағдай бойынша өзгерістер мен толықтырулармен). [Электрондық ресурс] – URL: https://adilet.zan.kz/kaz/docs/K1400000226 (қаралу уақыты: 01.01.2025).

5 Модельный Уголовный кодекс для государств - участников Содружества Независимых Государств от 17 февраля 1996 года. Ст. 286-292. [Электрондық ресурс] – URL: https://online.zakon.kz/Document/?doc_id=30074120 (қаралу уақыты: 11.01.2025)

6 Momsen C. Relevance of Data Security and Data Protection in Companies from the Perspective of Criminal Law // *Handbook Industry 4.0*. Berlin: Springer, 2022. P. 41–71. [Электрондық ресурс] – URL: https://www.springerprofessional.de/en/relevance-of-data-security-and-data- (қаралу уақыты: 11.01.2025)

7 Қытай Халық Республикасының киберқауіпсіздік туралы заңы 2017 жылғы 1 маусымдағы [Электрондық ресурс] – URL: http://www.npc.gov.cn/npc/index.html (қаралу уақыты 01.01.2025).

8 Испанияның Қылмыстық кодексі (Ley Orgánica 10/1995, de 23 de noviembre, Código Penal). 25.11.1995 ж. қабылданған, 2017 жылға дейінгі өзгерістер мен толықтыруларымен. Б. 270-598. [Электрондық ресурс]. — URL: https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf (қаралу уақыты: 01.01.2025).

9 Морозов Н.А. Борьба с компьютерной преступностью в Японии. Общество и право. 2014. № 2 (48) — С.141-145.

10 Computer Fraud and Abuse Act of 1984. 98th Congress (1983-1984). [Электрондық ресурс] – URL: https://www.congress.gov/bill/98th-congress/senate-bill/2864/text (қаралу уақыты 01.01.2025).

11 Cybersecurity and Infrastructure Security Agency Act of 2018 [Public Law 115–278] [This law has not been amended] [Электрондық ресурс] – URL: https://www.govinfo.gov/content/pkg/COMPS-15296/pdf/COMPS-15296.pdf (қаралу уақыты 01.09.2025).

12 Computer Misuse Act 1990 (United Kingdom): with the latest amendments and additions up to 2017, Articles 1–13 [Электрондық ресурс] – URL: https://www.legislation.gov.uk/ukpga/1990/18/contents (қаралу уақыты 11.02.2025).

13 Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes, Article 1-51. [Электрондық ресурс] – URL: https://www.wipo.int/wipolex/en/legislation/details/13909 (қаралу уақыты 01.02.2025).

14 Қазақстан Республикасының Қылмыстық кодексі 03.07.2024 ж. № 226-V ҚРЗ. (31.08.2024 ж. жағдай бойынша өзгерістер мен толықтырулармен). [Электрондық ресурс] – URL: https://adilet.zan.kz/kaz/docs/K1400000226/k14226_.htm (қаралу уақыты: 01.02.2025).

15 Рисс В.И. К вопросу о коллективных валютах или частных деньгах. сборник статей победителей VIII Международной научно-практической конференции: в 3 частях. Том Часть 2. Экономика, управление и право: инновационное решение проблем. Пенза. – 2017. С. 21-23.

16 Что такое волатильность криптовалют? Просто и понятно // Bitfin.info. — 19.07.2018. [Электрондық ресурс] – URL: https://bitfin.info/4663-chto-takoe-volatilnost/ (қаралу уақыты: 21.02.2025).

17 Мащенко П.Л., Пилипенко М.О. Технология блокчейн и ее практическое применение. Наука, техника и образование. - 2017. - № 2 (32). - С. 61–64.

18 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 [Электрондық ресурс]. – URL: https://www.law.cornell.edu/uscode/text/18/1030?utm (қаралу уақыты: 21.02.2025).

19 Пол В., Майкл К. Эпоха криптовалют: как биткоин и цифровые деньги бросают вызов мировому экономическому порядку. Святого Мартина: - 2015. – 357 с.

20 Greenberg A. Crypto Currency. Forbes. 20.04.2011. [Электрондық ресурс]. - URL: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin (қаралған күні: 01.02.2025).

21 Котенко М.А. Криминал вокруг криптовалют, самые громкие около-криптовалютные преступления! // Цифровой суверенитет и кибербезопасность: Материалы Четвертого международного транспортно-правового форума. [Электрондық ресурс] — URL: https://ui-miit.ru/files/docs/forum_tssik_sbornik_2022.pdf (қаралу уақыты: 01.09.2025).

22 Terrorism Act 2000. UK Public General Acts. 2000 c. 11. Article 1-18. [Электрондық ресурс] – URL: https://www.legislation.gov.uk/ukpga/2000/11/contents (қаралу уақыты: 01.02.2025).

ПРОКУРОРСКИЙ НАДЗОР ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ И МЕЖДУНАРОДНЫЙ ОПЫТ

Аннотация

Статья посвящена комплексному анализу теоретических и практических аспектов института прокурорского надзора при расследовании уголовных правонарушений в сфере информационных технологий относящейся к — одной из актуальнейших проблем современной системы правовых отношений. Цель статьи заключается в определении научных основ совершенствования механизмов прокурорского надзора в условиях цифровой эпохи и выработке предложений, направленных на повышение эффективности уголовного процесса. В ходе исследования использован комплекс общенаучных и специально-правовых методов, включая системный анализ, сравнительно-правовой, историко-правовой, статистический и моделирующий подходы. Авторские выводы и положения основаны на всестороннем научном анализе действующего уголовного законодательства Республики Казахстан, а также правового регулирования в Германии, Японии, Китае, Испании и США. В результате исследования уточнены роль и границы прокурорского надзора при расследовании уголовных правонарушений в

сфере информационных технологий, обоснована необходимость внедрения международных стандартов работы с цифровыми доказательствами, основанных на принципе «chain of custody». Отмечена значимость совершенствования требований KYC/AML в отношении криптовалют и иных цифровых активов, а также укрепления межведомственного взаимодействия по делам данной категории. Полученные результаты направлены на совершенствование деятельности правоохранительных органов, гармонизацию национального законодательства в сфере информационной безопасности с международными стандартами и формирование нового формата прокурорского надзора при расследовании уголовных правонарушений в сфере информационных технологий.

Ключевые слова: прокурорский надзор, информационные технологии, киберпреступность, цифровые доказательства, правовое регулирование, международные стандарты.

PROSECUTOR'S SUPERVISION IN THE INVESTIGATION OF CRIMINAL OFFENSES IN THE FIELD OF INFORMATION TECHNOLOGY: LEGAL REGULATION AND INTERNATIONAL EXPERIENCE

Abstract

This scientific study is devoted to a comprehensive analysis of the theoretical and practical aspects of prosecutorial supervision in the investigation of criminal offenses in the field of information technology — one of the most pressing issues in the modern legal system. The purpose of the article is to determine the scientific foundations for improving prosecutorial oversight mechanisms in the digital era and to develop proposals aimed at enhancing the effectiveness of criminal proceedings. The research employed a set of general scientific and special legal methods, including system analysis, comparative-legal, historical-legal, statistical, and modeling approaches. The author's findings and conclusions are based on a comprehensive scientific study of the current criminal legislation of the Republic of Kazakhstan, as well as the legal regulation practices of Germany, Japan, China, Spain, and the United States. As a result of the study, the role and boundaries of prosecutorial supervision in the investigation of criminal offenses in the field of information technology were clarified, and the necessity of implementing international standards for handling digital evidence based on the "chain of custody" principle was substantiated. The importance of improving KYC/AML requirements for cryptocurrencies and other digital assets, as well as strengthening interagency cooperation in investigating such crimes, was emphasized. The research findings aim to improve law enforcement agency performance, harmonize national information security legislation with international standards, and shape a new format for prosecutorial supervision in the investigation of criminal offenses in the field of information technology.

Keywords: prosecutorial supervision, information technologies, cybercrime, digital evidence, legal regulation, international standards.

REFERENCES

1 Kömpüterlık qylmys turaly konvensia. Budapeşt, 23 qaraşa 2001 j. 2-5. Europalyq kelısımder seriasy - № 185. *[Convention on Cybercrime. Budapest]*, – No. 185. - Available at: - URL: https://online.zakon.kz/Document/?doc_id=30170556 [in Kazakh] (accessed 01.01.2025).

2 Qytai Halyq Respublikasynyñ Qylmystyq kodeksı. *[Criminal Code of the People's Republic of China]*.1979 jylğy 1 şıldede besınşı QŪP ekınşı sesiasynda qabyldandy. 1997 jylğy 14 nauryzdağy segızınşı QŪP besınşı sesiasynda tüzetuler engızıldı. P.285–288. - Available at: - URL: https://ru.china-embassy.gov.cn/rus/zfhz_0/zgflyd [in Kazakh] (accessed 01.01.2025).

3 N.Bilton. Kiberprestupnik №1. İstoria sozdatelä podpölnoi setevoi imperii. *[The Story of the Creator of an Underground Network Empire]* / [per. s angl.]. – Moskva : Eksmo, 2017. – 448 p. [in Russian].

4 Qazaqstan Respublikasynyñ Qylmystyq kodeksı. *[Criminal Code of the Republic of Kazakhstan dated]*. 03.07.2024 j. № 226-V QRZ. (31.08.2024 j. jağdai boiynşa özgerıster men tolyqtyrularmen). - Available at: – URL: https://adilet.zan.kz/kaz/docs/K1400000226/k14226_.htm [in Kazakh] (accessed 01.01.2025).

5 Modelnyi Ugolovnyi kodeks dlä gosudarstv - uchastnikov Sodrujestva Nezavisimyh Gosudarstv ot 17 fevralä 1996 goda. [Model Criminal Code for the Member States of the Commonwealth of Independent States of 17 February 1996. Articles 286–292.]St. 286-292. - Available at: – URL: https://online.zakon.kz/Document/?doc_id=30074120 [in Russian]. (accessed 11.01.2025).

6 Momsen, C. Relevance of Data Security and Data Protection in Companies from the Perspective of Criminal Law // Handbook Industry 4.0. Berlin: Springer, 2022. P. 41–71. - Available at: – URL: https://www.springerprofessional.de/en/relevance [in English] (accessed 11.01.2025).

7 Qytai Halyq Respublikasynyñ kiberqauıpsızdık turaly zañy [Cybersecurity Law of the People's Republic of China]2017 jylğy 1 mausymdağy., 2017. - Available at: – URL: http://www.npc.gov.cn/npc/index.html [in Kazakh] (accessed 01.01.2025).

8 İspanianyñ Qylmystyq kodeksı [Criminal Code of Spain] (Ley Orgánica 10/1995, de 23 de noviembre, Código Penal). 25.11.1995 j. qabyldanğan, 2017 jylğa deiıngı özgerıster men tolyqtyrularymen. B.270-598. P. 270-598. - Available at: – URL: https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf [in Kazakh] (accessed 01.01.2025).

9 Morozov N.A. Börba s kömpüternoi prestupnöstü v İaponii. [Combating Computer Crime in Japan]. Obşestvo i pravo. 2014. № 2 (48) —P. 141–145. [in Russian].

10 Computer Fraud and Abuse Act of 1984. 98th Congress (1983–1984). - Available at: – URL: https://www.congress.gov/bill/98th-congress/senate-bill/2864/text [in English] (accessed 01.01.2025).

11 Cybersecurity and Infrastructure Security Agency Act of 2018 [Public Law 115–278]. [This law has not been amended]. - Available at: – URL: https://www.govinfo.gov/content/pkg/COMPS-15296/pdf/COMPS-15296.pdf [in English] (accessed 01.01.2025).

12 Computer Misuse Act 1990 (United Kingdom), with the latest amendments and additions up to 2017. Articles 1–13. - Available at: – URL: https://www.legislation.gov.uk/ukpga/1990/18/contents [in English] (accessed 11.02.2025).

13 Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes, United Arab Emirates. Articles 1–51. - Available at: – URL: https://www.wipo.int/wipolex/en/legislation/details/13909 [in English] (accessed 01.02.2025).

14 Qazaqstan Respublikasynyñ Qylmystyq kodeksı. [Criminal Code of the Republic of Kazakhstan]. 03.07.2024 j. № 226-V QRZ. (31.08.2024 j. jağdai boiynşa özgerıster men tolyqtyrularmen). - Available at: – URL: https://adilet.zan.kz/kaz/docs/K1400000226/k14226_.htm [in Kazakh] (accessed 01.02.2025).

15 Riss V.İ. K voprosu o kolektivnyh valütah ili chastnyh dengah. [On the Issue of Collective Currencies or Private Money]. sbornik statei pobeditelei VIII Mejdunarodnoi nauchno-prakticheskoi konferensii: v 3 chastäh. Tom Chäst 2. Ekonomika, upravlenie i pravo: innovasionnoe reşenie problem. Penza. – 2017. P. 21-23. [in Russian].

16 Chto takoe volatilnöst kriptovalüt? Prosto i ponätno. [What is Cryptocurrency Volatility? Simple and Clear]. Bitfin.info. — 19.07.2018. - Available at: – URL: https://bitfin.info/4663-chto-takoe-volatilnost/ [in Russian]. (accessed 21.02.2025).

17 Maşenko P.L., Pilipenko M.O. Tehnologia blokchein i ee prakticheskoe primenenie. [Blockchain Technology and Its Practical Application]. Nauka, tehnika i obrazovanie. - 2017. - No. 2 (32). P. 61–64. [in Russian].

18 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. [Computer Fraud and Abuse Act (CFAA)] - Available at: – URL: https://www.law.cornell.edu/uscode/text/18/1030?utm [in English] (accessed 21.02.2025).

19 Pol V., Maikl K. Epoha kriptovalüt: kak bitkoin i sifrovye dengi brosaiut vyzov mirovomu ekonomicheskomu porädku. The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order]. Svätogo Martina: - 2015. –357 p. [in Russian].

20 Greenberg, A. Crypto Currency. Forbes. 20.04.2011. - Available at: – URL: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html [in English] (accessed 01.02.2025).

21 Kotenko M.A. Kriminal vokrug kriptovalüt, samye gromkie okolo-kriptovalütnye prestuplenia [Crime Around Cryptocurrencies: The Most High-Profile Crypto-Related Crimes] // Sifrovoi suverenitet i kiberbezopasnöst: Materialy Chetvertogo mejdunarodnogo transportno-pravovogo foruma. - Available at: – URL: https://ui-miit.ru/files/docs/forum_tssik_sbornik_2022.pdf [in Russian]. (accessed 01.02.2025).

22 Terrorism Act 2000. UK Public General Acts. 2000 c. 11. Articles. P.1–18. - Available at: – URL: https://www.legislation.gov.uk/ukpga/2000/11/contents [in English] (accessed 01.02.2025).

Information about the authors:

Ermek Nurmaganbet - Candidate of Juridical Sciences, PhD, Professor of the Department of Law, Caspian University of Engineering and Technology named after Sh.Yessenov, Aktau, Republic of Kazakhstan

E-mail: yermek.nurmaganbet@yu.edu.kz

ORCID: https://orcid.org/0000-0001-6248-2429

Renat Shaikhadenov - PhD, Associate Professor of the Department of Law, Caspian University of Engineering and Technology named after Sh.Yessenov, Aktau, Republic of Kazakhstan

E-mail: Renat.shaikhadenov@yu.edu.kz

ORCID: https://orcid.org/0000-0001-8056-9798

Akylbek Konyssov – **corresponding author**, Master of Laws, PhD Student, Ahmet Baitursynov Kostanay Regional University, Kostanay, Republic of Kazakhstan

E-mail: akylbek.konyssov@yu.edu.kz

ORCID: https://orcid.org/0009-0002-3476-1986

Информация об авторах:

Ермек Нурмаганбет – к.ю.н., PhD, профессор кафедры «Правоведение», Каспийский университет инжиниринга и технологий имени Ш. Есенова, г. Актау, Республика Казахстан

E-mail: yermek.nurmaganbet@yu.edu.kz

ORCID: https://orcid.org/0000-0001-6248-2429

Ренат Шайхаденов – PhD, ассоциированный профессор кафедры «Правоведение», Каспийский университет инжиниринга и технологий имени Ш. Есенова, г. Актау, Республика Казахстан

E-mail: Renat.shaikhadenov@yu.edu.kz
ORCID: https://orcid.org/0000-0001-8056-9798
Акылбек Конысов – **основной автор**, м.ю.н., докторант PhD, Костанайский региональный университет имени Ахмета Байтурсынова, г. Костанай, Республика Казахстан
E-mail: akylbek.konyssov@yu.edu.kz
ORCID: https://orcid.org/0009-0002-3476-1986

Авторлар туралы ақпарат:
Ермек Нұрмағанбет – з.ғ.к., PhD, «Құқықтану» кафедрасының профессоры, Ш. Есенов атындағы Каспий технологиялар және инжиниринг университеті, Ақтау қ., Қазақстан Республикасы
E-mail: yermek.nurmaganbet@yu.edu.kz
ORCID: https://orcid.org/0000-0001-6248-2429
Ренат Шайхаденов – PhD, «Құқықтану» кафедрасының қауымдастырылған профессоры, Ш. Есенов атындағы Каспий технологиялар және инжиниринг университеті, Ақтау қ., Қазақстан Республикасы
E-mail: Renat.shaikhadenov@yu.edu.kz
ORCID: https://orcid.org/0000-0001-8056-9798
Акылбек Конысов – **негізгі автор,** з.ғ.м., докторант PhD, Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті, Қостанай қ., Қазақстан Республикасы
E-mail: akylbek.konyssov@yu.edu.kz
ORCID: https://orcid.org/0009-0002-3476-1986