ӘОЖ 343.3/.7
ХҒТАР 10.77.51

А.А. Қалиев[1], К.С. Кужахметова[2]
[1]Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы
[2]Қазақстан Республикасы Ішкі істер министрлігінің Ш. Қабылбаев атындағы Қостанай академиясы, Қостанай қ., Қазақстан Республикасы

АҚПАРАТТЫҚ-ТЕЛЕКОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР АРҚЫЛЫ ЖАСАЛАТЫН АЛАЯҚТЫҚТЫҢ АЛДЫН АЛУДЫҢ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ АСПЕКТІЛЕРІ

Аннотация. Мақалада ақпараттық-телекоммуникациялық технологиялар арқылы жасалатын алаяқтықтың алдын алудың қылмыстық-құқықтық тетіктері талданады. Зерттеудің мақсаты – цифрлық ортада жасалатын алаяқтықтың құқықтық табиғатын айқындау, оның алдын алуда қылмыстық заңнаманың, құқық қолдану практикасының және құқық қорғау органдарының ұйымдастырушылық қызметінің рөлін анықтау. Жұмыста формальды-заңи, салыстырмалы-құқықтық, жүйелік-құрылымдық және доктриналық талдау әдістері пайдаланылды. Авторлар алаяқтықтың дәстүрлі белгілері цифрлық кеңістікте сақталғанымен, алдау тәсілдері, жәбірленушіге ықпал ету нысандары, дәлелдемелердің электрондық сипаты және қылмыстың трансшекаралық элементі оның алдын алуды күрделендіретінін негіздейді. Сонымен бірге құқықтық саралау өлшемдерін нақтылау, цифрлық іздерді бекіту тәртібін жетілдіру, жәбірленушіні ерте қорғау, банктер мен платформалармен өзара іс-қимылды күшейту және ақпараттық-талдамалық қызметті жетілдіру жөнінде ұсыныстар беріледі.

Түйінді сөздер: цифрлық дәлелдеме; фишинг; әлеуметтік инженерия; құқықтық саралау; ақпараттық жүйе; киберқауіпсіздік; санкция; превенция; құқық қолдану.

А.А. Калиев[1], К.С. Кужахметова[2]
[1]Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан
[2]Костанайская академия Министерства внутренних дел Республики Казахстан имени Ш. Кабылбаева, г. Костанай, Республика Казахстан

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье анализируются уголовно-правовые механизмы профилактики мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий. Цель исследования – определить правовую природу цифрового мошенничества и раскрыть роль уголовного законодательства, правоприменительной практики и организационного взаимодействия правоохранительных органов в его предупреждении. Использованы формально-юридический, сравнительно-правовой, системно-структурный и доктринальный методы. Обосновано, что традиционные признаки мошенничества сохраняются и в цифровой среде, однако способы обмана, формы воздействия на потерпевшего, электронный характер доказательств и трансграничный элемент преступления существенно усложняют профилактику. В результате сформулированы предложения по уточнению правовой квалификации, совершенствованию порядка фиксации цифровых следов, ранней защите потерпевшего, усилению взаимодействия с банками и платформами, а также систематизации информационно-аналитической работы.

Ключевые слова: цифровые доказательства; фишинг; социальная инженерия; правовая квалификация; информационная система; кибербезопасность; санкция; превенция; правоприменение.

A.A. Kaliyev[1], K.S. Kuzhakhmetova[2]
[1]The Law Enforcement Academy under the Procesutor General's Office of the Republic of Kazakhstan, Kosshy, the Republic of Kazakhstan
[2]The Kostanay Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Sh. Kabylbayev, Kostanay, the Republic of Kazakhstan

CRIMINAL LAW ASPECTS OF PREVENTING FRAUD COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Abstract. The article examines criminal law mechanisms for preventing fraud committed through information and telecommunication technologies. The purpose of the study is to identify the legal nature of digital fraud and to determine the role of criminal legislation, law enforcement practice, and organizational interaction of law enforcement agencies in its prevention. The research is based on formal legal, comparative legal, systemic, and doctrinal methods. The author argues that although the classic features of fraud remain unchanged in the digital environment, prevention becomes more difficult because of new methods of deception, specific ways of influencing victims, the electronic nature of evidence, and the transnational component of such acts. The study proposes clarifying legal qualification, improving procedures for securing digital traces, strengthening early victim protection, enhancing cooperation with banks and online platforms, and systematizing information-analytical work.

Keywords: digital evidence; phishing; social engineering; legal qualification; information system; cybersecurity; sanction; prevention; law enforcement.

DOI: 10.52425/25187252_2026_40_52

Kipicne. Қоғамдық қатынастардың цифрлануы мүліктік қылмыстардың жасалу тәсілдерін түбегейлі өзгертті. Егер бұрын алаяқтық көбіне тікелей байланыс, бетпе-бет сендіру, жалған құжат ұсыну немесе сенімге кіру арқылы жүзеге асырылса, бүгінгі жағдайда оның негізгі бөлігі қашықтан жасалатын ықпал ету тетіктеріне сүйенеді. Бүгінде алдау телефон байланысы, мессенджерлер, жалған интернет-дүкендер, төлем сілтемелері, банктің немесе мемлекеттік органның атынан жасалатын хабарламалар арқылы жүзеге асады. Мұндай жағдайда қылмыстық-құқықтық алдын алу тек санкция белгілеумен шектелмейді; ол құқық нормасының анықтығын, кінәлі әрекетті дер кезінде тануды және жәбірленушіні ерте қорғауды қамтуы тиіс [1, 124 б.].

Цифрлық алаяқтықтың қауіптілігі оның тек жаңа техникалық формаға ие болуында емес, сонымен бірге күнделікті өмірдің қарапайым цифрлық әрекеттерімен астасып кетуінде. Азамат интернет арқылы төлем жасап, курьерлік қызметке жүгініп, банк қосымшасын пайдаланып немесе әлеуметтік желіде хабарлама алмасып отырған кезде қылмыстық тәуекелге ұшырауы мүмкін. Қылмыскер дәл осы үйреншікті цифрлық мінез-құлықты пайдаланады. Сондықтан мәселе жекелеген құқық бұзушылықтарды тіркеумен ғана шектелмейді; сөз азаматтардың цифрлық ортада қалыптасқан сенім моделін қылмыстық мақсатта теріс пайдалану жөнінде болып отыр. Бұл жағдай қылмыстық құқықтың дәстүрлі түсіндіру аппаратын жаңа шындыққа бейімдеуді талап етеді.

Qamqor құқықтық статистика порталындағы деректер интернет-алаяқтық фактілері елдегі қылмыстық ахуалдың ірі сегментіне айналғанын көрсетеді. Сондықтан мәселе тек жекелеген эпизодтармен күресу емес, ақпараттық жүйені пайдаланушыны алдау тәсілдерінің алдын алуға бағытталған тұрақты қылмыстық саясат қалыптастыруда болып отыр. Осы тұрғыдан алғанда қылмыс құрамының объективтік жақтарын дұрыс тану мен оларды ұқсас құрамдардан шектеу алдын алу үшін шешуші мәнге ие [2, 22 б.]. Әсіресе цифрлық ортада жасалатын әрекеттердің көпшілігі бір мезгілде бірнеше құқықтық белгілерге ұқсап көрінеді: бір жағынан, мүлікті иелену бар, екінші жағынан, ақпараттық жүйеге заңсыз араласу элементтері байқалады, үшінші жағынан, жәбірленушінің өз қолымен ақша аударуы орын алады. Осындай күрделі жағдайларда құқықтық саралаудың қателігі тек әділ жаза тағайындауға ғана емес, жалпы профилактиканың тиімділігіне

де кері әсер етеді.

Шетелдік зерттеулер де азаматтық-құқықтық мәміле нысанын бүркеніш ретінде қолданатын, жалған міндеттемелер мен сенім қатынасын пайдаланатын алаяқтықтың қауіптілігі жоғары екенін көрсетеді. Демек, ақпараттық технологиялар арқылы жасалатын алаяқтықты алдын алудың қылмыстық-құқықтық аспектісі құқықтық саралауды, ниетті дәлелдеуді және бастапқы алдауды уақтылы анықтауды біртұтас жүйеде қарастыруды талап етеді [3, 74 р.]. Мұнда аса маңыздысы, цифрлық алаяқтық әрдайым техникалық шабуылдан басталмайды. Көп жағдайда ол әлеуметтік инженериядан, яғни адамның эмоциясына, қорқынышына, сенгіштігіне, асығыстығына немесе беделді институттарға деген сеніміне әсер етуден басталады. Осы себепті цифрлық қылмыстарды тек техникалық қауіп ретінде емес, құқықтық және психологиялық ықпал ету феномені ретінде де қарастырған жөн.

Сонымен бірге цифрлық ортадағы алаяқтықтың ерекшелігі оның анонимдік дәрежесінің жоғары болуында. Қылмыскер басқа елдің нөмірін, жалған аккаунтты, үшінші тұлғаның банктік деректерін немесе уақытша серверлерді пайдалана алады. Бұл құқық қорғау органдары үшін кінәлі тұлғаны анықтау ғана емес, қылмыс тізбегін дәлелдеу міндетін де күрделендіреді. Сондықтан алдын алу жұмысы тек қылмыс жасалғаннан кейін әрекет ететін репрессивтік жүйе емес, ерте байқау, тәуекелді модельдеу және қорғау шараларын уақытылы қосатын көпдеңгейлі құқықтық механизм болуы қажет.

Материалдар мен әдістер. Зерттеу барысында отандық ғылыми әдебиет, қазақстандық құқық қолдану практикасы, Қазақстан Республикасы Жоғарғы Сотының 2017 жылғы 29 маусымдағы № 6 «Алаяқтық туралы істер бойынша сот практикасы туралы» нормативтік қаулысы, сондай-ақ цифрлық ортадағы мүліктік қылмыстарға арналған шетелдік еңбектер талданды[1]. Формальды-заңи әдіс алаяқтық құрамының белгілерін нақтылауға, салыстырмалы-құқықтық әдіс интернет-алаяқтықты интернет-ұрлықтан және өзге де цифрлық жымқырулардан ажырату өлшемдерін айқындауға мүмкіндік берді [4, 69 б.]. Әдістердің үйлесімді қолданылуы зерттеудің сипаттамалық деңгеймен шектелмей, түсіндірмелік сипат алуына мүмкіндік берді. Яғни назар тек норманың мәтініне емес, сол норманың цифрлық қатынастар жағдайында қалай қолданылатынына аударылды

Құқық қолдану тәжірибесін зерделеу үшін банктік карталар шоттарынан ақша қаражатын алумен байланысты істерді саралау проблемаларына арналған отандық жарияланымдар пайдаланылды. Бұл материалдар жәбірленушінің ерік білдіруі бұрмаланған жағдайда алдаудың мазмұнын, электрондық реквизиттердің рөлін және қылмыстың аяқталу сәтін дұрыс анықтаудың маңызын көрсетуге мүмкіндік береді [5, 16 б.]. Әсіресе цифрлық ортада жәбірленушінің еркі мен оның сыртқы әрекетінің арақатынасы күрделі сипат алады. Мысалы, азамат ақша аударымын өзі растауы мүмкін, бірақ бұл растау шынайы еркінен емес, жалған ақпараттың ықпалынан туындайды. Мұндай жағдайда сырттай қарағанда ерікті әрекет болып көрінгенімен, мазмұны бойынша ол алдаудың нәтижесі ретінде бағалануға тиіс.

Сонымен қатар ақпараттық технологиялар саласындағы қылмыстарды анықтау және жолын кесудегі ақпараттық-талдамалық жұмыстың маңызын ашатын еңбектер қарастырылды. Мұндай тәсіл алдын алу ұғымын тар салалық жазалау шарасынан шығарып, оны құқықтық нормалар, цифрлық мониторинг, ведомствоаралық өзара іс-қимыл және тәуекелді ерте байқау құралдары арқылы іске асатын кешенді қызмет ретінде түсіндіруге негіз береді [6, 95 б.]. Қазіргі жағдайда қылмыстық-құқықтық профилактика тек құқық қорғау органының құзыретімен шектелмейді. Банктер, байланыс операторлары, цифрлық платформалар, төлем сервистері, киберқауіпсіздік құрылымдары және мемлекеттік органдар бірлескен профилактикалық контур

[1] Алаяқтық туралы істер бойынша сот практикасы туралы: Қазақстан Республикасы Жоғарғы Сотының 2017 ж. 29 маусымдағы № 6 нормативтік қаулысы [Электрондық ресурс] – Айналыс режимі: https://adilet.zan.kz/kaz/docs/P170000006S (жүгінген күні: 03.06.2026).

құруы керек. Зерттеудің әдістемелік негізі осы ортақ жауапкершілік идеясын да ескереді.

Зерттеуде талдау бірліктері ретінде алаяқтық тәсілі, жәбірленушіге ықпал ету механизмі, мүлікті иеленудің құқықтық формасы, электрондық іздердің сипаты және әрекеттің аяқталу сәті алынды. Осындай құрылым зерттеу нысанын шашыратпай, негізгі құқықтық түйіндерді іріктеп қарауға мүмкіндік берді. Сонымен бірге виктимологиялық тәсіл пайдаланылды. Бұл тәсіл қылмыскердің әрекетін ғана емес, жәбірленушінің цифрлық ортадағы осал мінез-құлқын, қауіп сигналдарын қабылдау қабілетін және алдын алу шараларына жауап беру ерекшеліктерін бағалауға мүмкіндік береді. Өйткені цифрлық алаяқтықта зиян келтіру көбіне шабуыл мен жәбірленуші реакциясының қиылысында пайда болады.

Нәтижелер, талқылау. Ақпараттық-телекоммуникациялық технологиялар арқылы жасалатын алаяқтықтың қылмыстық-құқықтық ерекшелігі алдау тәсілінің техникалық тұрғыдан күрделенуі, бірақ құқықтық мәнінің сақталуы болып табылады. Яғни кінәлі тұлға жәбірленушінің санасына жалған ақпарат енгізу арқылы оның мүлікке қатысты еркін өзгертіп, сол арқылы мүліктік зиян келтіреді. Цифрлық кеңістікте бұл ықпал автоматтандырылған хабарламалар, клон-сайттар, deepfake дыбыс, жалған сервистік сілтемелер және аккаунттарды иемдену схемалары арқылы жүзеге асуы мүмкін. Мұндай өзгеріс классикалық алаяқтықтың мазмұнын жоймайды, бірақ оның жасалу ауқымын, жасырынуын және трансшекаралық сипатын күшейтеді [7, 18 б.].

Осы орайда маңызды мәселе мынада: цифрлық алаяқтықтың сыртқы белгілері көбіне техникалық шабуылға ұқсайды, бірақ оның түпкі өзегі адамды жаңылыстыру болып қала береді. Мәселен, жалған банк қызметкері ретінде хабарласу кезінде қылмыскер жәбірленушінің шотына тікелей бұзып кірмейді, қайта оны өзі құпия кодты айтуға, қосымшаны орнатуға немесе ақшаны «қауіпсіз шотқа» аударуға көндіреді. Демек, қылмыстық-құқықтық бағалау барысында негізгі назар техникалық құралдың өзіне емес, сол құрал арқылы жүзеге асқан алдау механизміне аударылуы тиіс. Егер бұл айырмашылық ескерілмесе, құқық қолдану тәжірибесінде біркелкілік бұзылады.

Қылмыстық-құқықтық алдын алудың бірінші бағыты заңи айқындық болып табылады. Қолданушыны алдау, жалған төлем интерфейстерін жасау немесе дербес деректерді иелену арқылы қаражатқа қол жеткізу жағдайларында қылмысты алаяқтық, ұрлық немесе ақпараттық қауіпсіздікке қарсы өзге қылмыс ретінде саралау мәселесі жиі туындайды. Шетелдік виктимологиялық зерттеулер көрсеткендей, фишинг пен зиянды бағдарламалар көбіне жәбірленушінің әлеуметтік сенімін, күнделікті онлайн мінез-құлқын және қорғаныш дағдыларының әлсіздігін пайдаланады, сондықтан құқықтық бағалау қылмыс тәсілімен қатар жәбірленушінің ерік білдіруіне әсер ету механизмін де есепке алуы тиіс [8, 82 б.].

Заңи айқындықтың маңызы сол, ол тек сот пен тергеушіге бағыт-бағдар бермейді, сонымен бірге жалпы алдын алу әсерін де күшейтеді. Норма неғұрлым нақты болса, соғұрлым құқық қолданушы алаяқтықтың белгілерін ерте таниды, ал азаматтар да қауіпті мінез-құлықты тезірек ажыратады. Керісінше, құқықтық шекаралар көмескі болса, бірдей әрекеттер әртүрлі сараланып, құқықтық сенім әлсірейді. Осы себепті цифрлық ортадағы алдаудың нысандары бойынша ресми түсіндірмелерді жүйелеу маңызды.

Алдын алудың екінші бағыты қылмыстық саясатты ұйымдастырушылық-техникалық шаралармен ұштастыру болып табылады. Фишинг шабуылдарының эволюциясын зерттеген еңбектер пайдаланушыларға ескерту мәтінін көбейту жеткіліксіз екенін, интерфейс қауіпсіздігі, көпфакторлы тексеру, домендерді жедел бұғаттау және жалған байланыс арналары туралы жедел хабарлау секілді ұйымдастырушылық шешімдердің құқықтық превенциямен бірге қолданылуы қажет екенін дәлелдейді [9, 74 б.]. Аталған ғылыми тұжырым ерекше назар аударуға лайық. Себебі құқықтық норма азаматты қорғайды, бірақ ол қорғау нақты цифрлық архитектурамен бекітілмесе, оның әсері әлсіз болады. Азамат қаншалықты сақ болса да, егер жалған сайт

түпнұсқаға айнытпай ұқсаса немесе жалған қоңырау ресми нөмірден түскендей көрінсе, қателесу ықтималдығы жоғары.

Осыдан келіп, қылмыстық-құқықтық алдын алудың техникалық өлшемі құқықтық кеңістікпен ажырамас байланыста қаралуы тиіс деген қорытынды шығады. Банктер тарапынан күмәнді транзакцияларды уақытша тоқтату, платформа әкімшілігінің жалған аккаунттарды жылдам бұғаттауы, байланыс операторларының жалған қоңырау трафигін сүзгіден өткізуі және азаматқа нақты қауіп сигналы бар интерфейс ұсынуы құқықтық профилактиканың шынайы мазмұнын толықтырады. Мұнда алдын алу тек «сақ болыңыз» деген ескертумен шектелмеуі керек, ол пайдаланушы қате жасауға үлгермейтіндей етіп құрылған орта қалыптастыруы тиіс.

Кешенді алдын алудың үшінші бағыты тәуекелге бағдарланған құқық қолдану болып табылады. Құқық қорғау органдары, банктер және цифрлық платформалар азаматтардың онлайн мінез-құлқындағы типтік қауіпті сценарийлерді ерте анықтауға бағытталған бірыңғай профилактикалық модельдерді әзірлеуі керек. Зерттеулер тәуекелі жоғары топтар өзін қорғау стратегияларын білсе де, оларды тұрақты түрде қолданбайтынын көрсетеді. Сондықтан қылмыстық-құқықтық алдын алу қорқыту әсеріне ғана сүйенбей, мінез-құлықтық профилактикамен, ақпараттық науқандармен және процестік жедел әрекет ету тәртібімен толықтырылуға тиіс [10, 540 б.].

Мысалы, азамат түнгі уақытта бұрын пайдаланбаған құрылғы арқылы бірден бірнеше аударым жасауға әрекет етсе немесе қысқа мерзім ішінде бірнеше күмәнді сілтемеге өтсе, мұндай мінез-құлық тәуекел индикаторы ретінде танылуы мүмкін. Осындай индикаторлар банктік жүйелерде, онлайн-платформаларда және құқық қорғау органдарының талдамалық базаларында бірдей ескерілсе, зиян келтірудің алдын алу ықтималдығы артады. Сонымен қатар адамның құқығын шектемеуі керек, бірақ пропорционалды және заңды бақылау құралдары арқылы үлкен шығынның алдын алуға болады.

Тағы бір маңызды бағыт цифрлық дәлелдемелермен жұмыс істеудің сапасын арттыруға қатысты. Цифрлық алаяқтық істерінде дәлел көбіне тұрақсыз, тез өшірілетін және бірнеше сервисте шашыраңқы түрде сақталатын сипатқа ие. Скриншоттар, чаттар, логтар, төлем тарихы, IP-мекенжайлар, құрылғы ізі, электрондық пошта тақырыптары, домен туралы мәліметтер сияқты деректердің әрқайсысы жеке алғанда жеткіліксіз болуы мүмкін, бірақ жиынтығында алдау схемасын қалпына келтіруге мүмкіндік береді. Сондықтан цифрлық дәлелдемелерді жинау, бекіту және бағалау тәртібінің бірыңғай стандарты қылмыстық-құқықтық алдын алу үшін де қажет. Өйткені қылмыскер жазасыз қалатын болса, профилактика әлсірейді.

Виктимологиялық профилактика да ерекше назар аударуды талап етеді. Цифрлық алаяқтық құрбандары әрдайым құқықтық сауаты төмен немесе техниканы білмейтін адамдар емес. Кейде жәбірленуші ақпараттандырылған, сақ, тәжірибелі қолданушы болуы мүмкін. Бірақ алаяқтық қысым, асығыстық, қорқыныш немесе беделді органның атын пайдалану арқылы іске асқанда, рационалды шешім қабылдау әлсірейді. Осыған байланысты халықты оқыту тек жалпы ережелер тізбегі ретінде емес, нақты мінез-құлықтық сценарийлерге негізделген бағдарлама ретінде құрылуы керек. Мысалы, «банк ешқашан код сұрамайды» деген сөйлемді қайталау жеткіліксіз; азаматқа күмәнді қоңырау түскен сәтте не істеу керектігінің қадамдық алгоритмі қажет.

Мәтінде айтылған ұсыныстарды жүйелеу үшін төмендегі кестені келтіреміз.

Бағыт	*Негізгі проблема*	*Ұсынылатын шешім*
Құқықтық саралау	Алаяқтықты интернет-ұрлықтан және өзге цифрлық жымқырудан ажырату қиындығы	Жоғарғы Соттың нормативтік қаулылары негізінде бірыңғай өлшемдер қалыптастыру

Дәлелдеме айналымы	Электрондық іздердің тез жойылуы және фрагменттілігі	Цифрлық дәлелдемені жинау мен бекітудің стандартталған тәртібін енгізу
Ведомствоаралық өзара іс-қимыл	Банк, платформа және құқық қорғау органының ақпарат алмасуы баяу	Жедел хабарлау хаттамалары мен тәуекел индикаторларын ұйымдастырушылық деңгейде біріктіру
Виктимологиялық профилактика	Азаматтардың әлеуметтік инженерияға осалдығы	Арнайы виктимологиялық бағдарлама мен мінез-құлықтық ескертулер жүйесін қолдану

1-кесте. Ақпараттық-телекоммуникациялық технологиялар арқылы жасалатын алаяқтықтың қылмыстық-құқықтық және ұйымдастырушылық-криминологиялық алдын алу бағыттары

Кестеде көрсетілген бағыттар бір-бірінен оқшау жұмыс істемейді. Құқықтық саралау нақтыланбайынша, процестік әрекет ету де әлсіз болады. Ведомствоаралық өзара іс-қимыл жолға қойылмайынша, цифрлық дәлелдемелер толық жиналмайды. Ал азаматтың мінез-құлқына бағытталған профилактикасыз техникалық қорғаныс та жеткілікті нәтиже бермейді. Сондықтан цифрлық алаяқтықпен күресте кешенді, өзара байланысқан алдын алу жүйесін қалыптастыру тиімді бағыт ретінде көрінеді.

Қорытынды. Ақпараттық-телекоммуникациялық технологиялар арқылы жасалатын алаяқтықтың алдын алу қылмыстық құқықтың тек жазалау функциясымен шектелмейді. Оның тиімділігі қылмыстық заң нормаларының айқындығына, цифрлық дәлелдемелерді бекітудің сенімді тәртібіне, құқық қолдану органдарының жедел үйлесімділігіне және жәбірленушіні ерте қорғау тетіктеріне тәуелді. Қазақстан жағдайында мұндай профилактика қылмыстық кодекстегі алаяқтық құрамын қазіргі цифрлық тәсілдерге бейімдеп түсіндіруді, сот тәжірибесін біріздендіруді және ақпараттық жүйелерді пайдаланушыны алдау фактісін дәлелдеудің бірыңғай өлшемдерін қалыптастыруды қажет етеді.

Зерттеу нәтижелері цифрлық алаяқтықтың басты құқықтық өзегі өзгермегенін, яғни негізгі белгі әлі де алдау арқылы жәбірленушінің еркіне ықпал ету екенін көрсетті. Өзгерген нәрсе оның сыртқы формасы, таралу жылдамдығы, жасырыну деңгейі және трансшекаралық сипаты. Осыған байланысты құқықтық реакция да тек дәстүрлі қылмыс үлгісіне сүйенбеуі керек. Қылмыстық-құқықтық алдын алу енді заңи, техникалық, процестік және виктимологиялық компоненттерді біріктіретін көпқабатты жүйе ретінде құрылуға тиіс.

Цифрлық ортадағы алаяқтықтың қауіптілігі оның қылмыс ретінде тез бейімделуінде. Қылмыскерлер жаңа сервистерді, коммуникация арналарын, беделді ұйымдардың атын, тіпті адамның дауысын имитациялайтын технологияларды да пайдаланады. Сондықтан алдын алу саясаты да икемді болуы керек. Ол тек жасалған әрекетке жауап бермей, келесі ықтимал схемаларды да есепке алуы тиіс. Бұл тұрғыдан алғанда тәуекелге негізделген құқық қолдану моделі, күмәнді транзакциялар туралы жедел хабарлау, банктер мен платформалар арасындағы ақпарат алмасуды жеделдету аса өзекті.

Сонымен бірге, цифрлық алаяқтықпен күресте азаматтың рөлі ерекше. Жәбірленушіні тек әлсіз тарап ретінде емес, қорғау механизміне белсенді қатысушы субъект ретінде қарау қажет. Азаматтардың цифрлық құқықтық сауаттылығын көтеру профилактиканың қосымша емес, негізгі бағыты болуы тиіс. Бірақ бұл жұмыс жай ғана ескерту материалдарымен шектелмеуі керек. Ол шынайы сценарийлерге негізделген, түсінікті, жиі қайталанатын және нақты әрекет алгоритмін ұсынатын жүйе болғаны жөн.

Осыған байланысты ұсыныстарды екі деңгейге бөліп қарастыру орынды. Қылмыстық-құқықтық деңгейге алаяқтық пен цифрлық ортадағы өзге жымқыру нысандарын ажыратудың ресми түсіндірмелерін нақтылау және қылмыстық процесте электрондық іздерді сақтау мен ұсыну стандарттарын біріздендіру жатады. Ал банктер мен онлайн-платформалар үшін күмәнді транзакциялар туралы шұғыл хабарлау міндеттемесін күшейту, халықтың цифрлық құқықтық сауаттылығын арнайы виктимологиялық бағдарлама ретінде жүргізу, ведомствоаралық жедел байланыс арналарын автоматтандыру және тәуекел индикаторларының ортақ базасын қалыптастыру ұйымдастырушылық, криминологиялық және виктимологиялық алдын алу шаралары ретінде қарастырылуы тиіс. Бұл шаралар қылмыстық-құқықтық алдын алудың нәтижелілігін қамтамасыз ететін қосымша емес, онымен өзара байланысты элементтер болып табылады.

Сондықтан кешенді тәсіл цифрлық алаяқтықтың таралуын тежеуге және қылмыстық-құқықтық алдын алуды нақты нәтижеге бағыттауға мүмкіндік беретін маңызды алғышарт болып табылады. Қатаң қылмыстық-құқықтық ықпал ету шаралары өздігінен жеткілікті нәтиже бермейді. Сол сияқты техникалық сүзгілеу құралдарын жеке қолдану да цифрлық алаяқтықтың алдын алуды толық қамтамасыз ете алмайды. Ағартушылық шаралары да құқықтық және процестік тетіктермен ұштаспаса, тұрақты нәтиже бермейді. Нақты нәтиже құқықтық анықтық, технологиялық қорғаныс, процестік жеделдік және азаматтың саналы мінез-құлқы өзара ұштасқанда күшейеді. Қазіргі цифрлық қоғамда қылмыстық-құқықтық алдын алу осындай тұтас, бейімделгіш және тәжірибеге бағытталған сипатқа ие болғаны орынды.

Пайдаланылған әдебиеттер тізімі:

1. Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры / В.С. Овчинский. – М.: Норма: ИНФРА-М, 2018. – 352 с.

2. Жолжаксынов, Ж.Б. Хищение посредством использования информационно-коммуникационных технологий в уголовном законодательстве Республики Казахстан / Ж.Б. Жолжаксынов, Е.Б. Жунусов // Хабаршы – Вестник Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова. – 2021. – № 2 (72). – С. 20-25.

3. Togaibayeva, S.S. Features of the Commission of Fraud, Coupled with the Failure to Comply with the Provisions of a Civil Contract / S.S. Togaibayeva, et al. // Journal of Politics and Law. – 2019. – № 12 (3). – Pp. 69-79.

4. Хамит, Е.Е. «Фишинг» арқылы жасалатын интернет-жымқыруларды саралаудың ерекшеліктері / Е.Е. Хамит // Құқық қорғау органдары академиясының Жаршысы. – 2023. – № 3 (29). – 67-74 б.

5. Еспергенова, Е.В. Некоторые вопросы квалификации преступлений, связанных с хищением денежных средств со счетов банковских карт / Е.В. Еспергенова // Хабаршы – Вестник Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова. – 2021. – № 2 (72). – С. 14-19.

6. Коржумбаева, Т.М. Ақпараттық технологиялар саласындағы қылмыстарды анықтау, алдын алу және жолын кесудегі ақпараттық-талдамалық жұмыстың ерекшеліктері / Т.М. Коржумбаева, С.М. Әбіжанов // Құқық қорғау органдары академиясының Жаршысы. – 2023. – № 3 (29). – 93-102 б.

7. Wall, D.S. Cybercrime: The Transformation of Crime in the Information Age / D.S. Wall. – Cambridge: Polity Press, 2024. – 356 p.

8. Jansen, J. Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization / J. Jansen, R. Leukfeldt // International Journal of Cyber Criminology. – 2016. – Vol. 10 (1). – Pp. 79-91.

9. Hong, J. The State of Phishing Attacks / J. Hong // Communications of the ACM. – 2012. – Vol. 55 (1). – Pp. 74-81.

10. Drew, J.M. Online Victimization Risk and Self-Protective Strategies: Developing Police-Led Cyber Fraud Prevention Programs / J.M. Drew, L. Farrell // Police Practice and Research. – 2018. – Vol. 19 (6). – Pp. 537-549.

References:

1. Ovchinskij, V.S. Kriminologija cifrovogo mira: uchebnik dlja magistratury / V.S. Ovchinskij. – M.: Norma: INFRA-M, 2018. – 352 s.

2. Zholzhaksynov, Zh.B. Hishhenie posredstvom ispol'zovanija informacionno-kommunikacionnyh tehnologij v ugolovnom zakonodatel'stve Respubliki Kazahstan / Zh.B. Zholzhaksynov, E.B. Zhunusov // Habarshy – Vestnik Karagandinskoj akademii MVD Respubliki Kazahstan im. B. Bejsenova. – 2021. – № 2 (72). – S. 20-25.

3. Togaibayeva, S.S. Features of the Commission of Fraud, Coupled with the Failure to Comply with the Provisions of a Civil Contract / S.S. Togaibayeva, et al. // Journal of Politics and Law. – 2019. – № 12 (3). – Pp. 69-79.

4. Hamit, E.E. «Fishing» arқyly zhasalatyn internet-zhymқyrulardy saralaudyң erekshelikteri / E.E. Hamit // Құқyқ қorғau organdary akademijasynyң Zharshysy. – 2023. – № 3 (29). – 67-74 b.

5. Espergenova, E.V. Nekotorye voprosy kvalifikacii prestuplenij, svjazannyh s hishheniem denezhnyh sredstv so schetov bankovskih kart / E.V. Espergenova // Habarshy – Vestnik Karagandinskoj akademii MVD Respubliki Kazahstan im. B. Bejsenova. – 2021. – № 2 (72). – S. 14-19.

6. Korzhumbaeva, T.M. Aқparattyқ tehnologijalar salasyndaғy қylmystardy anyқtau, aldyn alu zhәne zholyn kesudegi aқparattyқ-taldamalyқ zhymystyң erekshelikteri / T.M. Korzhumbaeva, S.M. Әbizhanov // Құқyқ қorғau organdary akademijasynyң Zharshysy. – 2023. – № 3 (29). – 93-102 b.

7. Wall, D.S. Cybercrime: The Transformation of Crime in the Information Age / D.S. Wall. – Cambridge: Polity Press, 2024. – 356 p.

8. Jansen, J. Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization / J. Jansen, R. Leukfeldt // International Journal of Cyber Criminology. – 2016. – Vol. 10 (1). – Pp. 79-91.

9. Hong, J. The State of Phishing Attacks / J. Hong // Communications of the ACM. – 2012. – Vol. 55 (1). – Pp. 74-81.

10. Drew, J.M. Online Victimization Risk and Self-Protective Strategies: Developing Police-Led Cyber Fraud Prevention Programs / J.M. Drew, L. Farrell // Police Practice and Research. – 2018. – Vol. 19 (6). – Pp. 537-549.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Асқар Абужанұлы Қалиев – Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау органдарының академиясы Қазіргі заманғы сын-тегеуріндерге қарсы іс-қимыл және цифрлық технологияларды енгізу орталығының Кибертехнология және жасанды интеллект кафедрасының меңгерушісі, e-mail: askar909@mail.ru.

Калиев Аскар Абужанович – заведующий кафедрой кибертехнологий и искуственного интеллекта Центра противодействия современным вызовам и внедрения цифровых технологий Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, e-mail: askar909@mail.ru.

Kaliev Askar Abuzhanovich – Head of the Department of Cyber Technologies and Artificial Intelligence at the Center for Countering Modern Challenges and Introducing Digital Technologies at the Law Enforcement Academy under the Procesutor General's Office of the Republic of Kazakhstan, e-mail: askar909@mail.ru.

Калдығұл Сирғалиқызы Кужахметова – Ш. Қабылбаев атындағы Қазақстан Республикасы Ішкі істер министрлігі Қостанай академиясының докторанты, заң ғылымдарының магистрі, e-mail: kalda83@mail.ru.

Кужахметова Калдыгул Сиргалиевна – докторант Костанайской академии Министерства внутренних дел Республики Казахстан имени Ш. Кабылбаева, магистр юридических наук, e-mail: kalda83@mail.ru.

Kuzhakhmetova Kaldygul Sirgalievna – Doctoral Student at the Kostanay Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Sh. Kabylbayev, Master of Law, e-mail: kalda83@mail.ru.