

ҚЫЛМЫСТЫҚ ЖӘНЕ ҚЫЛМЫСТЫҚ-ПРОЦЕСТІК ҚҰҚЫҚ / УГОЛОВНОЕ И УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ПРАВО / CRIMINAL AND CRIMINAL PROCEDURE LAW

УДК 343.34: 004

БИЕБАЕВА Ардақ Әлімханқызы

Заң ғылымының кандидаты, қауымдастырылған профессор, Қазақстан Республикасы Жоғарғы Сотының жанындағы Сот төрелігі академиясының Қылымыстық-құқықтық пәндердің ғылыми-білім беру орталығының профессоры

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ КИБЕРҚЫЛМЫСТАРҒА ҚАРСЫ ЗАҢНАМАСЫНЫҢ ЗАМАНАУИ ЖАЙ-КҮЙІНЕ ЖӘНЕ ДАМУ ПЕРСПЕКТИВАЛАРЫНА ШОЛУ

Аннотация. Мақалада киберқылмыстарға қарсы іс-қимылдың халықаралық-құқықтық және ұлттық-құқықтық негіздері қарастырылады. Автор киберқылмыстар үшін қылмыстық жауаптылық туралы ұлттық заңнаманы талдауды цифрлық ортаны позитивті тұрғыдан реттейтін заңнаманы шолуға негіздейді. Зерттеу нәтижесінде автор ақпараттық-коммуникациялық технологияларды реттейтін нормативтік-құқықтық базаның тұрақсыздығының себептерін айқындайды, ақпараттық заңнаманы кодификациялаудың артықшылықтарын көрсетеді, ұлттық қылмыстық заңнамадағы киберқылмыстарды зиянды әсер ету тәсілдері мен бағытына қарай топтастырады, дәстүрлі қылмыстарды телекоммуникация желілерін пайдалана отырып жасау жағдайларын саралаудың қалыптасқан практикасына қатысты сыни пікір айтады, киберқылмыстар туралы заңнаманың көмегімен киберқауіпсіздікті қамтамасыз ету перспективаларын болжайды.

Түйін сөздер: киберқауіпсіздік, киберқылмыстар, ақпараттық-коммуникациялық технологиялар, ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникация желілері, қылмыстық заңнама, криминализация.

БИЕБАЕВА Ардақ Алимхановна

Кандидат юридических наук, ассоциированный профессор, профессор Научно-образовательного центра уголовно-правовых дисциплин Академии правосудия при Верховном Суде Республики Казахстан

ОБЗОР СОВРЕМЕННОГО СОСТОЯНИЯ И ПЕРСПЕКТИВ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ КАЗАХСТАН ПРОТИВ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В статье рассматриваются международно-правовые и национально-правовые основы противодействия киберпреступлениям. Анализ национального законо-

дательства об уголовной ответственности за киберпреступления автор основывает на обзоре законодательства, регулирующего цифровую среду в позитивном ключе. В результате исследования автор выявляет причины нестабильности нормативно-правовой базы, регулирующей информационно-коммуникационные технологии, демонстрирует преимущества кодификации законодательства от информатизации, группирует киберпреступления в национальном уголовном законодательстве по способам и направлениям вредного воздействия, высказывает критическое замечание относительно сложившейся практики квалификации случаев совершения традиционных преступлений с использованием сетей телекоммуникаций, прогнозирует перспективы обеспечения кибербезопасности с помощью законодательства о киберпреступлениях.

Ключевые слова: кибербезопасность, киберпреступления, информационно-коммуникационные технологии, информационные ресурсы, информационные системы, сеть телекоммуникаций, уголовное законодательство, криминализация.

BIEBAEVA Ardak Alimkhanovna

Candidate of Law, associate Professor, Professor of the Scientific and Educational Center of Criminal Law Disciplines of the Academy of Justice at the Supreme Court of the Republic of Kazakhstan

REVIEW OF THE CURRENT STATE AND PROSPECTS FOR THE DEVELOPMENT OF LEGISLATION OF THE REPUBLIC OF KAZAKHSTAN AGAINST CYBERCRIME

Annotation. *The article examines the international legal and national legal foundations of countering cybercrime. The author's analysis of national cybercrime legislation is based on a review of legislation governing the digital environment in a positive manner. In the result of the study, the author identifies the causes of instability of the regulatory framework governing information and communication technologies, demonstrates the advantages of codifying informatization legislation, groups cybercrimes in the national criminal legislation depending on the ways and directions of harmful effects, comments critically on the established practice of classifying traditional crimes committed through telecommunications networks, predicts the prospects for ensuring cybersecurity through cybercrime legislation.*

Keywords: *cybersecurity, cybercrimes, information and communication technologies, information resources, information systems, telecommunications network, criminal legislation, criminalization.*

Kіріспе

Электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, оларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясаттың негізгі бағыттары Қазақстанның ақпараттық-коммуникациялық технологиялар (АКТ) саласында-

ғы құқыққа қайшы әрекеттерден төнетін қатерлерді барабар түсінетіндігінің және бағалайтындығының айқын дәлелі болып табылады. Ұлттық қауіпсіздіктің ажырамас бөлігі болып табылатын ақпараттық қауіпсіздік елдің орнықты дамуы мен ақпараттық тәуелсіздігін, сондай-ақ адам мен азаматтың құқықтары мен мүдделерін қор-

ғауды қамтамасыз ететін аса маңызды фактор болып табылады [1].

Қазіргі заманғы әдебиеттерде ХХІ ғасырдың екінші онжылдығында ақпараттық қауіпсіздік парадигмасы киберқауіпсіздік парадигмасына ұласқаны туралы айтылады [2]. Бұл үрдіс біздің елімізге де тән: ҚР Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысымен бекітілген Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») [3] киберқауіпсіздікті ақпараттық қауіпсіздіктің құрамдас бөлігі ретінде қарастырылған болатын.

Осы Тұжырымдаманы іске асырудың нәтижесінде еліміз бірқатар оң нәтижелерге қол жеткізді. 2023 жылы Қазақстан ұлттық киберқауіпсіздік индексі бойынша әлемдік рейтингте 176 елдің ішінен 78-ші орынды иеленді. Ел индексі мүмкін болатын ең жоғары 100 проценттен 48,05 процентті құрады. Сол рейтингте халықтың цифрлық даму деңгейі 60,18 процентке жетті.

ҚР Үкіметінің 2023 жылғы 28 наурыздағы №269 қаулысымен 2023–2029 жылдарға арналған Цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамытудың жаңа тұжырымдамасы бекітілді [5]. Бұл бағдарламалық құжат орта мерзімді перспективада шешілуге жататын киберқауіпсіздіктің негізгі мәселелері ретінде мыналарды айқындайды: Қазақстанның цифрлық кеңістігіне кибершабуылдардың өсуі; халықтың, АКТ саласы қызметкерлерінің және ұйымдар басшыларының киберқауіпсіздік мәселелері жөніндегі цифрлық (құқықтық) сауаттылығының төмендігі; дербес деректерді қорғауды күшейту қажеттігі.

Материалдар мен әдістер

Тақырыпты ашу барысында ақпараттық қауіпсіздікті қамтамасыз ету саласындағы халықаралық-құқықтық актілер, қоғам өмірінің түрлі салаларында цифрлық технологиялардың мүмкіндіктерін пайдаланудың

негізгі бағыттарын айқындайтын бағдарламалық құжаттар, Қазақстан Республикасының ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қауіпсіз пайдалану және қорғау саласындағы қоғамдық қатынастарды реттейтін заңнамалық актілері, киберқылмыстар туралы заңнамасы, тақырып төңірегіндегі ғылыми еңбектер зерделенді. Автор құқықтық болмысты танудың тарихи, салыстырмалы-құқықтық, формальды-құқықтық, жүйелі-құрылымдық талдау әдістерінің көмегіне жүгінді.

Нәтижелер, талқылау

1. Киберқылмыстарға қарсы іс-қимылдың халықаралық-құқықтық негіздері.

Киберқылмыстарға қарсы іс-қимылдың халықаралық-құқықтық негіздері туралы сөз қозғағанда Қазақстанның 2000 жылы Окинавада қабылданған ақпараттық технологияларды қылмыстық мақсаттарда қолдануға қарсы іс-қимылды құқықтық реттеу саласындағы алғашқы халықаралық құжат болып табылатын Жаһандық ақпараттық қоғам хартиясын (Okinawa Charter on Global Information Society) ратификацияламағанын атап өту керек. Соған қарамастан, ақпараттық қауіпсіздік мәселелері бойынша мемлекетішілік бағдарламалық құжаттарды әзірлегенде біздің еліміз Окинава Хартиясының қылмыстылықтан таза киберкеңістік қалыптастыру туралы негізгі қағидаларын ескереді.

Сонымен қатар, Қазақстан Еуропа Кеңесінің киберқылмыстарға қарсы күрестегі халықаралық ынтымақтастықтың жедел және тиімді жүйесін құруға бағытталған 2001 жылғы 23 қарашадағы Киберқылмыстар туралы Будапешт конвенциясына (Convention on cybercrime) да қосылған жоқ. Дегенмен, ұлттық заңнамамыз қоғамдық қауіпті әрекеттерді криминализациялау бөлігінде Будапешт Конвенциясының бірқатар талаптарына жауап береді.

Өңірлік деңгейдегі халықаралық-құқықтық актілерге келетін болсақ, Қазақстан

2009 жылғы 16 маусымда Екатеринбург қаласында жасалған Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімнің [6] қатысушысы болып табылады.

Шанхай Келісімінің негізгі мақсаты халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастықтың құқықтық және ұйымдастырушылық негіздерін құру болып табылатындықтан, бұл құжатта ақпараттық технологиялар саласындағы қоғамдық қауіпті әрекеттерді криминализациялау мәселелеріне назар аударылмайды. Алайда, Келісімнің 2-бабында халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі қатерлер арасында «ақпараттық қылмыстылық» аталады, өз кезегінде ол «ақпараттық кеңістікте заңға қайшы келетін мақсаттарда ақпараттық ресурстарды пайдалану және (немесе) оларға әсер ету» деп анықталады.

Қазақстан ратификациялаған өңірлік деңгейдегі келесі құжат – 2018 жылғы 28 қыркүйекте Душанбеде жасалған Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстарға қарсы күрестегі ынтымақтастығы туралы келісім [7]. 2001 жылғы Минск келісімінің орнына қабылданған бұл құжат ақпараттық технологиялардың қазіргі заманғы даму деңгейіне бейімделген және осы саладағы қылмыстарға қарсы күрестің тиімділігін арттыру мақсатын көздейді.

2. Киберқылмыстарға қарсы іс-қимылдың ұлттық-құқықтық негіздері

2.1. Қазақстан Республикасының цифрлық ортаны реттейтін заңнамасы

Белгілі бір әрекеттерді криминализациялау немесе декриминализациялау мақсаттары үшін осы құбылыстың мәні мен оның қасиеттері туралы үйлесімді идеялар жүйесінің болуы маңызды. Сондықтан, ки-

берқылмыстар туралы заңнаманы талдауға кіріспес бұрын, ақпаратты жинау, өңдеу, сақтау және тарату, сондай-ақ ақпараттық-коммуникациялық желілерді пайдалану саласындағы қоғамдық қатынастарды позитивті тұрғыдан реттейтін заңнамалық актілерге қысқаша тоқталып өту қажет.

Қазақстанда Интернет 1994 жылы пайда болды. Елде интернет қолданушылар санының экспоненциалды өсуі байқалады. Ақпараттық технологиялардың біртіндеп өмір шындығына айналуы қоғамдық қатынастардың осы саласын құқықтық реттеудің объективті қажеттілігін тудырды.

Осы бағытта қабылданған алғашқы нормативтік құқықтық актілердің қатарында азаматтардың ақпаратқа құқығын қамтамасыз етуге, елдің әлеуметтік-экономикалық даму талаптарына жауап беретін ақпараттық әлеуеттің қажетті деңгейін құруға және дамытуға, әлемдік ақпараттық кеңістікке интеграциялауға бағытталған «Қазақстан Республикасында бірыңғай ақпараттық кеңістікті қалыптастыру туралы» ҚР Президентінің 1997 жылғы 9 желтоқсандағы №3787 Жарлығын атап өткен жөн.

Ақпараттандыру объектілерін құру, дамыту және пайдалану кезінде, сондай-ақ АКТ саласын дамытуды мемлекеттік қолдау кезінде туындайтын қоғамдық қатынастарды реттейтін арнайы заңнамалық акт «Ақпараттандыру туралы» ҚР Заңы болып табылады.

Бас-аяғы 12 жылдың ішінде Қазақстан осындай үш заң қабылдап үлгерді: 2003 жылы; 2007 жылы; және қазір қолданыстағы 2015 жылғы 24 қарашадағы «Ақпараттандыру туралы» ҚР Заңы [8].

Осы орайда «қысқа тарихи кезең ішінде бірнеше аттас заңнамалық актілердің қабылдануының себебі неде?» деген орынды сұрақ туындайды.

Профессор М.К. Сүлейменовтің пікірінше, оның себептерінің бірі – цифрлан-

дыру саласындағы заң жобаларын әзірлеу процесіне IT мамандарының белсенді тар-тылуы. Бұл болса, заңдарға технологияны жетік меңгерген адамдардың тар аясына ғана белгілі терминдердің кеңінен енгізілуіне алып келді. Профессор цифрлық техно-логия ілгерілеген сайын үнемі өзгеріп оты-ратын бұл «түсініксіз терминдерді» «олар ештеңені реттемейтіндіктен», «құқықтық тұрғыдан пайдасыз» деп атайды және мұн-дай анықтамалар «заңда емес, анықтама-лықта немесе энциклопедияда (википедия-да) орын тебуі керек» екенін көрсетеді [9].

Заңгер И.Ю. Лоскутов осы саладағы бірқатар іргелі құқықтық ұғымдардың дұ-рыс қалыптаспауының себебін ақпараттық қатынастарды реттеудің құқықтық негізде-рінің асығыс әзірленуімен түсіндіреді. «Құ-қықтық тетіктер реттелетін қоғамдық қаты-настар жеткілікті түрде зерттеліп, оларды реттеу құралдары толық сынамадан өткен кезде ғана енгізілуі және тиімді болуы мүм-кін» [10], - деп жазады ол.

Өз тарапымыздан ақпараттандыру тура-лы заңнаманың тұрақсыздығының объектив-ті себебі ретінде құқықтық реттеу объектісі-нің күрделілігін (ақпаратты өңдеудің үздіксіз жаңартылып отыратын құралдарының техни-калық сипаттамалары, оларды қолдану сала-ларының күн санап кеңейуі, әртүрлі машина-лық тасымалдағыштарда сақталатын ақпарат көлемінің ұлғаюы) атағымыз келеді.

Сонымен, электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен те-лекоммуникация желілерін қорғауға және қауіпсіз пайдалануға байланысты қоғамдық қатынастарды реттейтін нормативтік-құ-қықтық базаның тұрақсыздығының объек-тивтік және субъективтік сипаттағы себеп-тері мыналар:

- біріншіден, құқықтық реттеу объекті-сінің күрделілігі мен құбылмалылығы;
- екіншіден, реттеу объектісінің жеткі-ліксіз зерттелгендігі;

- үшіншіден, заңнамалық актілерде мә-селенің құқықтық емес, технологиялық ас-пектілеріне баса назар аударылуы.

Әлемнің көптеген елдеріндегідей, қазір-гі уақытта Қазақстанда ақпараттандыру про-цестерін енгізу мен дамытуды тиісті дәре-жеде реттейтін нормативтік-құқықтық база қалыптаспаған. АКТ мен цифрландыруды дамыту саласында көптеген ұқсас құжаттар-дың кездесуі қайталауды және екіұшты қа-былдауды тудырады. Қазақстандағы цифр-лық ортаны құқықтық реттеу тұрғысындағы ең күрделі мәселе – қоғамдық қатынастар-дың нақты осы саласын құқықтық реттеудің заңнамада айқындалған және ғылыми докт-ринамен расталған қағидаттары мен ұста-нымдары жүйесінің болмауы.

Еліміздің 2023-2029 жылдарға арнал-ған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырым-дамасында АКТ нарығын «қатарлас, уақты-лы, кейде озыңқы заңнамалық, нормативтік қамтамасыз ету және реттеу» [5] қажеттігі туралы айтылған.

Қазіргі уақытта Қазақстанда ақпарат-тандыру, байланыс, дербес деректер, мем-лекеттік көрсетілетін қызметтер, элект-рондық құжаттар, электрондық-цифрлық қолтаңба және т.б. саласындағы бытыраң-қы нормативтік құқықтық актілерді бірік-тіретін бірыңғай кодификацияланған заң – Цифрлық кодексті әзірлеу бойынша жұ-мыстар жүргізілуде. Ақпараттық заңнама-ны кодификациялау үрдісі Орта Азия өңірі-нің басқа елдеріне де тән (мысалы, Қырғыз Республикасы, Тәжікстан).

Бұл ретте елімізде АКТ саласын рет-тейтін кодификацияланған нормативтік құ-қықтық акт қабылдау үшін құқықтық негіз де, доктриналық база да жоқ, білікті заң-гер-мамандар тапшы деп санайтын отан-дық ғалымдардың пікіріне де назар аудар-а кеткіміз келеді [11].

Қалай болғанда да, бүгінгі күні «Ашық НҚА» порталында Қазақстан Республикасының Цифрлық кодексі жобасына реттеушілік саясаттың консультативтік құжаты орналастырылды.

Цифрлық кодекстің реттеу пәнін, басқалармен қатар, адамның цифрлық құқықтары, электрондық үкімет, цифрлық активтер, блокчейн технологиялары, цифрлық майнинг, жасанды интеллект және т.б. құрауы тиіс.

Қазақстанның жаңа Цифрлық кодексінде терминология оңтайландырылып, техникалық ұғымдардың артық бөлігі алынып тасталуы тиіс. Кодексте ұзақ уақыт бойы өзгермейтін және реттеудің негізгі тәсілдерін анықтайтын кемел нормалар бекітіледі деп күтілуде.

Цифрлық кодекспен қатар реттеуші құжаттардың жаңа нысандары (ұсынымдық стандарттар, гайдлайндар және т.б.) әзірленетін болады, заңнамалық актілермен салыстырғанда оларды жедел түзетіп, үнемі өзекті күйге келтіріп отыруға болады. Мұндай ұстаным ақпараттық технологияларды кедергісіз дамыту мүмкіндігі және азаматтардың, бизнес пен мемлекеттің құқықтары мен мүдделерін қорғау арасындағы тепе-теңдікті сақтаудың құқықтық негіздерін қалайды деген үміттеміз.

2.2. Қазақстан Республикасының қылмыстық заңнамасындағы киберқылмыстар үшін жауаптылық

Қазақстанда ақпараттық технологиялар саласындағы қоғамдық қауіпті әрекеттер алғаш рет 1997 жылғы Қылмыстық кодексте криминализацияланды. Компьютерлік ақпаратқа заңсыз кіру, ЭЕМ үшін зиянды бағдарламаларды жасау, пайдалану және тарату үшін жауаптылық көздейтін норма (227-бап) ҚК-нің Экономикалық қызмет саласындағы қылмыстарға арналған тарауында орналасқан болатын. Ақпаратты жою, бұғаттау, өзгерту немесе көшіру, ЭЕМ-нің,

ЭЕМ жүйесінің немесе олардың желісінің бұзылуы түріндегі салдардың туындауы заңда аталған әрекеттерді қылмыс деп танудың міндетті шарты ретінде көрсетілді.

1997 жылғы Қылмыстық кодекс қолданыста болған кезең ішінде ақпараттық технологияларды қолдану аясы айтарлықтай артты, қоғамдық қатынастардың осы саласын реттеудегі кемшіліктердің беті ашылды, теориялық және терминологиялық қайшылықтар анықталды.

Сондықтан 2014 жылғы 23 сәуірдегі ҚР Заңымен 1997 жылғы Қылмыстық кодекс «Ақпараттық технологиялардың қауіпсіздігіне қарсы қылмыстар» деп аталатын жаңа 7-1-тараумен толықтырылды. Осы заңнамалық актідегі қылмыстық заңмен жазаланатын әрекеттер аясы еліміздің 2014 жылғы қолданыстағы Қылмыстық кодексіндегі тізбеге өте ұқсас болатын.

БҰҰ-ның Есірткі және қылмыстылық жөніндегі басқармасы зиянды әсер ету тәсілдері мен бағытын ескере отырып, киберқылмыстарды үш топқа жіктейді: 1) компьютерлік деректердің немесе жүйелердің құпиялылығына, тұтастығына және қолжетімділігіне қарсы бағытталған әрекеттер; 2) компьютерді жеке не қаржылық пайда алу немесе жеке не қаржылық зиян келтіру мақсатында пайдалануды көздейтін әрекеттер; 3) компьютерлік деректердің мазмұнына байланысты әрекеттер [12].

Аталған жіктемедегі киберқылмыстардың барлық топтары Қазақстанның қолданыстағы қылмыстық заңнамасында кеңінен ұшырасады:

1) Ақпараттық-коммуникациялық технологиялардың арқасында пайда болған «жаңа» қылмыстарды қамтитын «компьютерлік деректердің немесе жүйелердің құпиялылығына, тұтастығына және қолжетімділігіне қарсы бағытталған әрекеттерге» 212-бапта көзделген әрекетті қоспағанда, 2014 жылғы ҚК-нің 7-тарауына енгізілген

қылмыстық құқық бұзушылықтар жатқызылуы тиіс. Әдебиетте киберқылмыстардың бұл тобын «машиналарға қарсы киберқылмыстар» деп те атайды [13].

2) «Компьютерді жеке не қаржылық пайда алу немесе жеке не қаржылық зиян келтіру мақсатында пайдалануды көздейтін әрекеттердің екінші тобына біз олардың жасалуына қандай да бір дәрежеде ақпараттық-коммуникациялық технологиялар ықпал ететін дәстүрлі қылмыстарды қосамыз: ҚК-нің 105-баб. 2-бөл. 4)-тарм.; 131-баб. 2-бөл.; 132-баб. 2-бөл.; 134-баб. 3-бөл. 1-1)-тарм.; 147-баб. 3 және 5-тарм.; 148-баб. 2-бөл.; 188-баб. 2-бөл. 4)-тарм.; 190-баб. 2-бөл. 4)-тарм.; 195-баб. 3-бөл. 3)-тарм.; 272-баб. 4-бөл.; 316-баб. 3-бөл. 5)-тарм.; 375-баб. 2-бөл.; 376-бабы; 378-баб. 2-бөл.; 380-баб. 2-бөл. 4)-тарм. Оларды әдебиетте «машиналар арқылы жасалатын киберқылмыстар» деп те атайды.

Екінші топқа кіретін әрекеттердің саны күн сайын артып келеді және олар қылмыстық заңның әртүрлі тарауларынан орын тепкен. Киберқылмыстардың екінші тобы үшін жауаптылық белгілейтін қылмыстық-құқықтық нормалар санының өсуі жалпы әлемдік үрдіс болып табылады.

Қарастырылып отырған топтағы киберқылмыстардың басым бөлігінде «БАҚ-ты, телекоммуникация желілерін, оның ішінде Интернет желісін пайдалану» неғұрлым қатаң жауаптылыққа әкеліп соғатын ауырлаушы мән-жай ретінде ескерілген.

Осы орайда «кінәлі адамдардың әрекеттерін ҚК-нің 7-тарауының тиісті бабы бойынша қосымша саралау керек пе?» деген сұрақ туындайды. Құқық қолдану практикасында кінәлі адамдардың әрекеттері жиынтық бойынша сараланып жүр. Мысалы, «скиммердің» көмегімен ақпараттық жүйеге заңсыз кіру жолымен ұрлық жасаған Қазақстан, Әзірбайжан, Грузия және Молдова азаматтарынан тұратын ұйымдас-

қан қылмыстық топтың мүшелері ақпараттық жүйеге заңсыз кіру және телекоммуникация желісі бойынша берілетін ақпаратты өзгерту жолымен жасалған ұрлық үшін де (ҚК-нің 188-баб. 2-бөл. 4-тарм.), сондай-ақ ақпараттық жүйеге құқыққа сыйымсыз қол жеткізгені үшін де (ҚК-нің 205-бабы) және ақпаратты заңсыз иемденгені үшін де (ҚК-нің 208-бабы) қылмыстық жауаптылыққа тартылған [14].

Біздің ойымызша, қалыптасқан жаңсақ тәжірибе әділеттік принципін өрескел бұзды және кінәлінің бір әрекет үшін екі рет жауап беруіне алып келеді.

Келтірілген мысалда қылмыстық-құқықтық әдебиетте «ескерілген жиынтық» деген шартты атаумен белгілі жағдай орын алып тұр. «Ескерілген жиынтық» кезінде қылмыстық заңның бабында бір қылмыс басқа бір қылмысты жасаудың құралы немесе тәсілі ретінде көрсетіледі.

ҚК-нің 13-бабының 2-бөлігін басшылыққа ала отырып, заңда бір қылмыстық құқық бұзушылық басқа бір қылмыстық құқық бұзушылықтың саралаушы белгісі ретінде ескерілген жағдайларға қатысты ҚР Жоғарғы Соты: «Егер іс бойынша қолдануға жататын қылмыстық заңның нормасы, қылмыстық құқық бұзушылықтар жиынтығын көрсете келе, жасалған қылмыстық құқық бұзушылықтардың әрқайсысының барлық белгілерін толық қамтыса және олардың әрқайсысынан қоғамдық қауіпті зардаптардың келтірілуін көздесе, онда жасалған әрекет тұтастай алғанда осы саралаушы белгілері бар неғұрлым ауыр қылмыстық құқық бұзушылықты жасағаны үшін жауаптылықты көздейтін ҚК-нің тиісті бабы бойынша саралауға жатады» деп түсіндіреді [15].

Демек, ҚК-нің 188-баб. 2-бөл. 4)-тармағында ҚК-нің 205-бабында көзделген дербес қылмыстық құқық бұзушылық ұрлықты жасаудың тәсілі ретінде ескерілгендіктен, жасалған әрекет қылмыстық заңның неғұр-

лым ауыр қылмыстық құқық бұзушылық үшін жауаптылық көздейтін бабы бойынша ғана саралануы тиіс. Бұл ретте жеңілірек қылмыстық құқық бұзушылық үшін жауаптылық көздейтін бап бойынша қосымша саралау қажет емес.

3) Компьютерлік деректердің мазмұнына байланысты әрекеттер тобына (оларды әдебиетте «машинадағы киберқылмыстар» деп атайды) біз ҚК-нің келесі баптарында көзделген қылмыстық құқық бұзушылықтарды жатқызамыз: 161-баб. 2-бөл.; 174-баб. 1-бөл.; 179-баб. 2-бөл.; 180-баб. 2-бөл.; 183-бап; 256-баб. 2-бөл.; 274-баб. 2-бөл. 3)-тарм.; 299-1-баб. 2-бөл. 4)-тарм.; 402-баб. 1-бөл.; 409-баб. 3-бөл. 4)-тарм.

Киберқылмыстардың соңғы тобы алдыңғы екеуінен қылмыстық құқық бұзушылық жасау құралы ретінде «бұқаралық ақпарат құралдарының немесе телекоммуникация желілерінің» өздері емес, оларда орналастырылған контенттің мазмұны пайдаланылатынымен ерекшеленеді. Осы қисын бойынша ҚК-нің 212-бабында көзделген «Құқыққа қайшы мақсаттарды көздейтін интернет-ресурстарды орналастыру үшін қызметтер ұсыну» әрекетін де осы топқа қосқан орынды.

Қазақстан Республикасының ұлттық заңнамасы шеңберіндегі қылмыстық заңмен қудаланатын әрекеттер аясына жасалған шолу қоғамдық қауіпті әрекеттерді криминализациялау мәселесінде ол Будапешт Конвенциясының талаптарының басым бөлігіне жауап беретіндігін айғақтайды.

Алайда ұлттық қылмыстық заңнамада Қорқытып алу (ҚК-нің 194-бабы), Авторлық және (немесе) сабақтас құқықтарды бұзу (ҚК-нің 198-бабы), Порнографиялық материалдарды немесе заттарды заңсыз тарату (ҚК-нің 311-бабы), Кәмелетке толмағандардың порнографиялық бейнелері бар материалдарды немесе заттарды дайындау және олардың айналымы не оларды порног-

рафиялық сипаттағы ойын-сауық іс-шараларына қатысу үшін тарту (ҚК-нің 312-бабы) сияқты қылмыстық құқық бұзушылықтарды телекоммуникация желілерін пайдалана отырып жасағаны үшін жауаптылықты қатаңдату мүмкіндігі көзделмеген.

Қазіргі заманғы сын-тегеуріндер мен қатерлерді ескере отырып, жақын болашақта ұлттық қылмыстық заңнамамыз жасанды интеллектіні қылмыстық мақсаттарда қолданғаны үшін жауаптылықты көздейтін құқық бұзушылықтың жекелеген құрамымен толықтырылады деп күтілуде. Бұл туралы ҚР Президентінің 2021 жылғы 15 қазандағы № 674 Жарлығымен бекітілген «Қазақстан Республикасының 2030 жылға дейінгі құқықтық саясатының тұжырымдамасында» айтылған [16].

Қорытынды

Қазақстан Республикасына ұлттық заңнамалар арасындағы ұғымдық біркелкілікті қамтамасыз етуге, ақпараттық-коммуникациялық технологиялар саласындағы қоғамдық қауіпті әрекеттер туралы қылмыстық-құқықтық нормаларды үйлестіруге ықпал ететін жаһандық деңгейдегі халықаралық-құқықтық актілерге қосылу мүмкіндігін қарастыру керек.

Ақпараттық-коммуникациялық технологиялар саласындағы бытыраңқы нормативтік құқықтық актілерді біріктіретін бірыңғай кодификацияланған нормативтік құқықтық актіні әзірлеу және қабылдау қажеттігі күмән тудырмайды. Алайда бұл істе асығыстық танытып, сапасыз заң қабылдауға жол беруге болмайды.

Қылмыстық заңнамада дәстүрлі қылмыстарды заманауи ақпараттық-коммуникациялық технологияларды пайдалана отырып жасағаны үшін, сондай-ақ, ақпараттық жүйеде немесе желіде орналастырылатын және таратылатын контенттің мазмұны үшін қатаңырақ жауаптылық көздейтін нормалар санының одан күтілуде.

Пайдаланылған қайнар көздер тізімі

1. «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы» 2012 жылғы 6 қаңтардағы ҚР Заңы. <https://adilet.zan.kz/kaz/docs/Z1200000527>
2. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение. // <https://cyberleninka.ru/article/n/kiberprestupnost-globalnaya-problema-i-ee-reshenie/viewer>
3. «Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы» Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысы (күшін жойған). <https://adilet.zan.kz/kaz/docs/P1700000407>
4. Цифровизация Казахстана. Часть I. В мире и Казахстане. <https://the-tenge.kz/articles/digital-kazakhstan-11>
5. «2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасын бекіту туралы» Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы №269 қаулысы. <https://adilet.zan.kz/kaz/docs/P2300000269>
6. «Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді ратификациялау туралы» 2010 жылғы 1 маусымдағы ҚР Заңы. https://adilet.zan.kz/kaz/docs/Z100000286_
7. «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімді ратификациялау туралы» 2019 жылғы 9 желтоқсандағы ҚР Заңы. <https://adilet.zan.kz/kaz/docs/Z1900000277>
8. «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы ҚР Заңы. <https://adilet.zan.kz/kaz/docs/Z1500000418>
9. Сулейменов М.К. Цифровизация и совершенствование гражданского законодательства. <https://www.zakon.kz/5009131-tsifrovizatsiya-i-sovershenstvovanie.html>
10. Лоскутов И.Ю. Преступления в сфере информационных технологий в проекте новой редакции Уголовного кодекса Республики Казахстан. <https://online.zakon.kz/Document/>
11. Идрышева С.К. О Цифровом кодексе Казахстана // Право и государство, 2022, № 3 (96), с.72-87.
12. Основные виды киберпреступности. Вена, 2019. https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_2_General_Types_of_Cybercrime_RU.pdf
13. Wall David S. Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017). Available at SSRN: <https://ssrn.com/abstract=3005872> or <http://dx.doi.org/10.2139/ssrn.3005872>
14. Актауский городской суд приговорил к лишению свободы членов преступной группы. // https://online.zakon.kz/Document/?doc_id=39550449#pos=3;-80
15. ҚР Жоғарғы Сотының 2006 жылғы 25 желтоқсандағы №11 Нормативтік қаулысы «Қылмыстық құқық бұзушылықтардың бірнеше рет жасалуын және жиынтығын саралау туралы». // https://adilet.zan.kz/kaz/docs/P06000011S_
16. «Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасын бекіту туралы» Қазақстан Республикасы Президентінің 2021 жылғы 15 қазандағы №674 Жарлығы. <https://adilet.zan.kz/kaz/docs/U2100000674>