DOI 10.31489/2021 L3/104-112

ӘОЖ 343.2/.7(4/9)

А.Р. Бижанова[1*], Г.Б. Мейрбекова[1], Г.Ә. Жүнісова[2]

[1]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан
[2]ҚР ІІМ М. Есболатов атындағы Алматы академиясы, Қазақстан
(E-mail: Aike_74@mail.ru; Scopus author ID: 57209296000,
meirbekova67@mail.ru, zunisovagulmira2@gmail.com)

Ақпараттандыру мен байланыс саласындағы қылмыстық құқық бұзушылықтардың ұғымы жайлы

Компьютерлік ақпарат пен технологиялардың, оның ішінде қылмыстық-құқықтық құралдардың қауіпсіздігін қамтамасыз ету проблемасы бүгінде әлемнің көптеген дамыған елдеріндегі ең өткір мәселелердің бірі болып табылады. Әсіресе компьютерлерді, олардың жүйелері мен желілерін өнеркәсіп пен бизнесте жиі пайдаланылуда. Кәсіпорындар әртүрлі компьютерлік шабуылдар мен бұзылуларға байланысты үлкен шығындарға ұшырайды. Ғаламдық компьютерлік желі Интернет академиялық ресурстан коммерциялық ортаға айналды, мұнда қауіпсіздікті қамтамасыз ету және дамып келе жатқан қатынастарға ықтимал шабуылдардың алдын алу маңызды болып табылады. Зерттеудің мақсаты отандық және шетел заңнамаларымен киберқылмыстардың құқықтық реттелуін қарастыру, терминологиялық мәселелерді шешу болып табылады. Зерттеу нәтижесінде ақпараттық технология саласындағы қылмыстық құқық бұзушылықтар ұғымы нақтыланатын болады. Авторлар мақалада елімізде орын алған киберқылмыстылықтың қазіргі күйіне, қауіптілік деңгейіне тоқталған. ҚР ҚК-нің 7-тарауындағы қылмыстық құқық бұзушылықтардың ақпараттық технология салаларын қамтитынын ескере отырып, тараудың атауын өзгерту ұсынылған.

Кілт сөздер: ақпараттық технология, компьютерлік ақпарат, компьютерлік қылмыстар, ақпараттандыру және байланыс салаларындағы қылмыстық құқық бұзушылықтар, ақпараттық технология саласындағы қылмыстық құқық бұзушылықтар.

Кіріспе

XXI ғасыр жаһандану және ақпараттандыру ғасырымен ерекшеленеді. Компьютерлік технологиялар мен байланыс құралдарының қарқынды дамуы бүкіл әлемдегі прогрестің басты қозғалтқышы болды. Адамзат жаңа дәуірге — көрінбейтін мүмкіндіктерді ашатын жаһандық ақпараттық қоғамға аяқ басты. Интернет медицина, көлік, білім беру, өндіріс, банк саласы және т.б. болсын, адам өмірінің барлық салаларына еніп кетті [1].

Бұл үрдісті жаңғырту шаралары жөнінде Қазақстан Президентінің 2017 жылғы 31 қаңтардағы Қазақстан халқына Жолдауында, сандық технологиялардың көмегімен жаңа индустрияларды дамыту қажеттігі айтылған болатын [2]. Сонымен қатар, 2022 жылға дейінгі киберқауіпсіздік тұжырымдамасын («Қазақстан киберқалқаны») іске асыру жөніндегі іс-шаралар жоспары бекітілді [3].

Қазақстан Республикасы расында да әлемдік қоғамдастықпен ынтымақтаса отырып, экономикалық салада басқа елдермен біршама ілгерілей бастады. Интернет пен цифрлық технологиялардың таралуы жаһандану құрылымын түбегейлі өзгертті және өзара іс-қимылдың жаңа арналарын құрды. Өнімді өндіру, тарату құнын төмендететін сандық технологиялар жаһандану процесінде маңызды рөл атқарып отыр. Олардың көмегімен виртуалды қызметтер мен өнімдер жасалатын болды, сондай-ақ нақты тауарларға сұраныс артты.

Әлеуметтік желілер мен әртүрлі интернет-платформаларға келер болсақ, олар ақпарат алмасу мен саудаға арналған негізгі алаңға айналды. Компьютерлендіру шын мәнінде үлкен нәтижелер берді.

Дегенмен де ақпараттық технологияларды пайдалану үрдісі басқа қырынан танылды алды, ол осы салаларға қылмыстық зардаптардың төну қаупін тудырды. Мысалы, ақпаратты технологияны қолданудың бала тәрбиесіне және өмірі мен денсаулығына кері әсері байқалды. Бұл жайлы мемлекет басшысы Қасым-Жомарт Тоқаевтың 2020 жылғы 1 қыркүйектегі Қазақстан халқына арнаған «Жаңа жағдайдағы Қазақстан: іс-қимыл кезеңі» атты Жолдауында: «Бүкіл әлемде адамзаттың, әсіресе жас

*Хат-хабарларға арналған автор. E-mail: *Aike_74@mail.ru*

балалардың интернеттегі ғайбаттаулардың құрбанына айналғанын, сәйкесінше, балаларды кибербуллингтен қорғайтын заңнамалық мәселелерді шешу қажеттілігі туындады», — деп атап көрсетілді [4].

Ақпараттық технология қоғамдық қатынастың түрлі салаларында қылмыстық ізін қалдыра бастады. Нәтижесінде ол азаматтардың, заңды тұлғалардың заңды мүдделері мен құқықтарына, экономиканың өмірлік маңызды салаларын компьютерлендірудің елеулі деңгейіне жеткен кез келген елдің әлеуетті — ұлттық қауіпсіздігіне қауіп төндіреді.

Деректерге сүйенсек, 2019 жылы Қазақстанда ақпараттық қауіпсіздікті бұзу бойынша 21 мыңнан астам инцидент анықталған екен. Ботнеттер-кибершабуылмен байланысты 17,7 мың оқиға, фишинг жайлы 883 жағдай тіркелгені белгілі [5].

ҚР аумағында компьютерлік техника мен коммуникация құралдары қол сұғу объектілері ретінде ғана емес, сонымен қатар қылмыстық іс-әрекет құралы ретінде (АҚШ, Канада, Еуропа және т.б. елдерде компьютерлік ақпаратқа заңсыз қол жеткізу, электрондық транзакция арқылы ақша қаражатын жымқыру іс-тәжірибеде жиі кездеседі) пайдаланылады [6]. Соңғы уақытта киберқылмыстар жасау, оның ішінде интернет-пайдаланушыларға қатысты алаяқтық жағдайлары да жиілеп кетті. Мысалы, 2020 жылы осындай 14 мың қылмыс, ал ағымдағы жылдың қаңтарында — 1 700-ден астам қылмыс тіркелген [7].

ҚР Ішкі істер министрлігінің ұйымдастыруымен киберқылмыстардың, соның ішінде интернет-алаяқтықты ашу және алдын алу бағытында «Hi-tech» жедел алдын алу іс-шарасы өткізіліп, бірнеше күн ішінде аталған құқық бұзушылыққа қатысты 155 факті анықталған. Нақтырақ айтсақ, бұрын жасалған 161 қылмыс ашылған, олардың басым бөлігі интернет-алаяқтық болып табылады. Тексеріс нәтижесінде тауар айналымында тыйым салынған мыңнан астам бірліктер (контрафактілік дискілер, жасырын жазуға арналған техникалық құралдар, лицензияланбаған бағдарламалық жасақтаманың тасымалдаушылары (порнография және басқалар) тәркіленген [8].

2019 жылы 50-ге жуық, 2020 жылы — 134 киберинциденттер жайлы хабарламалар тіркелген. Сәйкесінше, Агенттікпен 2019 жылғы 137-мен салыстырғанда 2020 жылы қаржы нарығының субъектілеріне киберқауіпсіздік қатерлері жайлы 350-ден астам ескертулер мен ақпараттық анықтамалар дайындалып жіберілген екен [9].

Байқап отырғанымыздай, киберқылмыстылықпен күрестің өзектілігі күн санап арта түсуде. Сондықтан да Қазақстан Президентінің 2017 жылғы 31 қаңтардағы Қазақстан халқына Жолдауында Үкімет пен Ұлттық қауіпсіздік комитетіне «Қазақстан киберқалқаны» жүйесін қалыптастыру шараларын қабылдауды тапсыруы тектен-тек емес.

Соңғы кездері «Жаһандық киберқауіпсіздік индексінде (Global Cybersecurity Index) Қазақстан өз позициясын жақсарта алды. Қазақстан 2017 жылғы рейтинг бойынша 82-ші, 2019 жылы 42 пунктке — 40-орынға көтерілсе, ал 2020 жылы 36-орынды иеленді» [10].

Киберқылмыстық әрекеттер компьютерлік жүйеге қарсы бағытталады, ал ол өз кезегінде түрлі процестерді ақпараттардың көмегімен басқарып отырады. Киберқылмыскер қарапайым қылмыскер сияқты пышақ немесе атыс қаруы сияқты дәстүрлі қаруды қолданбайды. Ол желіге кіру, бағдарламаны бұзу және өзгерту, рұқсатсыз ақпарат алу немесе компьютерлік жүйелердің жұмысын бұғаттайтын құралдарды қолданады. Сонымен қатар, компьютерлік вирустар, бағдарламалық бетбелгілерді, компьютерлік жүйеге рұқсатсыз кіруді неғұрлым тиімді ететін шабуыл түрлері қылмыс қаруының қатарына жатады. Мұндай қылмыс құралдарын анықтау іс-тәжірибеде қиындықтар тудырғандықтан кінәлілердің ақпараттық қылмысқа қатыстылығын дәлелдеу оңай бола бермейді [6].

Шынында да компьютерлік қылмыстар өзіндік ерекшелікке ие және оның түбі ақпараттық технологиялар саласындағы мамандардың кәсіби ортасымен байланысты [11]. Себебі техникалық байланыс құралдарын кәсіби меңгерген мамандар ғана ақпараттандыру мен байланыс саласында қылмыстық іс-әрекеттерді жасай алады.

Техниканың дамуымен ақпараттық технология саласында қылмыстық құқық бұзушылықтардың жасалу әдістері көз ілеспей жаңарып отыр. Ал теорияда киберқылмыстар саласын құқықтық реттеуде терминологиялық мәселелерді қоса алғанда, бірыңғай көзқарастардың қалыптаспауы себепті ақпараттандыру және байланыс салаларындағы қылмыстылықпен күресу мәселелері шиеленіскенді. Ал бұл аталған жағдайлар тақырыптың өзектілігін айқындай түспек.

Әдістер мен материалдар

Зерттеу жұмысының әдіснамалық негізін құбылыстар мен процестерді танудың жалпы ғылыми диалектикалық әдісі, сонымен қатар тарихи құқықтық, салыстырмалы құқықтық, лингвистикалық, формальды логикалық зерттеу әдістері құрайды. Сонымен қатар мазмұнын ашу барысында құқықтық талдау, нақтылау, түсіндіру әдістері қолданылды. Ізденудің теориялық негізін отандық және шетелдік ғалымдардың киберқылмысқа қатысты ой пікірлері, ғылыми еңбектері құрады. Зерттеудің эмпирикалық негізі ретінде құқықтық статистикалық деректер танылады. Жұмыста ақпараттандыру және байланыс салаларымен байланысты халықаралық актілер, отандық азаматтық және қылмыстық заңнамалар негізге алынды.

Талқылаулар

АҚШ-та киберкеңістікті құқықтық қорғау шарасы 1986 жылы АҚШ Конгресі компьютерлерді және олардағы ақпаратты қорғауды мақсат еткен арнайы заң — 30 жыл бұрын қабылданған компьютерлік алаяқтық және компьютерлік қиянат туралы Заңнан (Computer Fraudand Abuse Actof) басталады екен. Бұл киберкеңістіктегі қатынастарды реттейтін әлемдегі алғашқы ережелер. Яғни бастапқыда теорияларда, заңнамаларда компьютерлік қылмыстар ұғымы қолданысқа ие болды. Мұндағы, к*омпьютерлік қылмыстар — бұл қылмыстық қол сұғушылықтың объектісі компьютерлік ақпарат саналатын қылмыстық заңда қарастырылған әлеуметтік қауіпті әрекеттер. Бұл жағдайда машиналық ақпарат, компьютер, компьютерлік жүйе немесе компьютерлік желі — қылмыстың заты немесе құралы ретінде танылады.*

2001 жылы 23 қарашада Будапеште қол қойылған «Компьютерлік ақпарат саласындағы қылмыс туралы» Еуропа кеңесінің Конвенциясында (ETSN 185) осы саладағы қылмыстарды: компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қолжетімділігіне қарсы; компьютерлік құралдарды пайдаланумен және авторлық құқықты және сабақтас құқықтарды бұзумен байланысты қылмыстар, деп бөлді [12].

Жоғарыда аталған Конвенцияға қатысушы әрбір мемлекеттің киберқылмыстылықпен күрес жөніндегі құзыретті органы істі қарау барысында компьютерлік жүйені, оның тасымалдаушыларын алуға; компьютерлік ақпараттың көшірмесін жасау және тәркілеуге; іске қатысты компьютерлік ақпараттардың тұтастығын, сақталуын қамтамасыз етуге; компьютерлік жүйедегі ақпараттарды жоюға немесе бұғаттауға міндеттенеді.

В.А. Дуленко, Р.Р. Мамлеев және В.А. Пестриков болса, киберқылмысты кең мағынада компьютерлік құрылғылар арқылы немесе онымен байланысты жасалған кез келген заңсыз әрекет деп санайды [13; 22]. Жалпы алғанда, киберқылмыстарды аталған авторлар әртүрлі ақпараттық желілерде жасалған құқық бұзушылықтармен байланыстырады.

Ал киберқылмыстарды желідегі компьютерлік жүйеге қоса, мобильды байланыс құралдарымен жасалынатын қылмыстар қатарында деп қарайды И.Г. Чекунова [14; 15]. Ғылымда ақпараттардың таралу аумағына назар аударған пікірлер де бар. Г.А. Атаманова «кибераумақ кибер жүйеден тұрады, ал кибержүйе — бұл кибер құрылымдардан, оларды байланыстыратын коммуникациялардан, бағдарламалық жасақтамадан және оларда жасалған, өңделетін, берілетін және сақталатын ақпараттық объектілерден тұратын жүйенің бір түрі», – дейді [15]. Мұнан түсінетініміз, киберқылмыстар кибержүйеге қылмыстық қол сұғады, яғни аталған қылмыстық іс-әрекеттерден қол сұғатын объекті назарға алынады.

АҚШ Жоғарғы соты киберкеңістікті «географиялық кеңістікпен» шектемейді, бірақ Интернетке кіру арқылы әлемнің кез келген жерінде барлығына қол жетімді ерекше орта, деп санайды [16].

Ал қоғамдық өмірі жоғары деңгейде компьютерлендірілген елдердің зерттеушілері мен заң шығарушылары жалпы компьютерлік немесе жоғары технологиялық («computer crimes» или «high — tech crimes») деп аталатын қылмыс түрлерін бөліп қарастырды.

Келесі бір еңбекте: «Киберқылмыс» ұғымы (ағылшын тілінде — cybercrime) «компьютерлік қылмыс» (computer crime) ұғымынан кең және де ақпараттық кеңістіктегі қылмыс ретінде жаһандық құбылыстың табиғатын сипаттайды. Егер «киберқылмыс» термині компьютерлермен де, ақпараттық технологиялар мен ғаламдық желілерді қолданумен де байланысты болса, онда «компьютерлік қылмыс» ұғымы негізінен электрондық құрылғыларға және оларда сақталған деректерге қарсы жасалған қылмыстарға жатады», делінген [17; 148–159]. Бұл пайымдауда автор

«ақпараттық технология», «компьютер» және «ғаламдық желі» сынды жалпы, жеке ұғымдарды араласып қолданады.

А.В. Суслопаров өзінің диссертациялық ізденісінде қоғамдағы ақпарат пен ақпараттық процестердің маңыздылығының артуына байланысты ақпараттық қылмыстарды анықтау қажет деп есептейді. Мұнда, ақпарат дегеніміз белгілі бір код түріндегі сигналдар арқылы субъектілер арасында берілетін, мақсатты басқару әсерін білдіретін ақпарат болып табылады [18; 8–10]. Сәйкесінше, ғылыми еңбектерден ҚК-тің тарауын «Ақпараттық қауіпсіздікке қарсы қылмыстар» деп атауды ұстанған пікірді кездестіре аламыз [19; 8,9]. Беларусь ҚК-нің XII-ші тарауы осылай аталған. Ал ондағы қылмыстық нормалар компьютерлік ақпаратқа, компьютерлік жүйе мен байланыс шеңберінде қаралады.

Расында «киберқылмыс» ұғымы «компьютерлік қылмыс» (compiter crime) ұғымынан кең. Егер ғаламдық желілерді ақпараттық технология құралдарын пайдалану арқылы *ақпараттың алынуы, таралуы, тасымалдануы мүмкін болса, онда киберқылмыстардың жасалу құралы тек компьютермен шектелмейтіні анық.*

БҰҰ сарапшыларының «киберқылмыстар» термині компьютерлік жүйе немесе желі арқылы жасалған қылмыстарды, сондай-ақ компьютерлік жүйе немесе желіге қарсы кез келген қылмыстарды білдіреді, деген пайымдауын ескере отырып, «компьютерлік жүйе немесе желі» ұғымдарын ҒТП нәтижесі ретінде «ақпараттық жүйе, ақпараттық-коммуникациялық желі» ұғымдарымен алмастырсақ, онда «киберқылмыстарда» ақпараттық жүйе, ақпараттық-коммуникациялық желі — қылмыстың жасалу құралы, әрі қол сұғылатын қылмыстар бола да алады.

Халықаралық актілердегі, шетел ғалымдарымен берілген киберқылмыстар туралы түсініктермен таныса отырып, олардың өзге қылмыс түрлерінен ерекшелік белгілерін анықтауға мүмкіндік тудырды. Бұл мәліметтер отандық заңнамамен қарастырылған ақпараттандыру және байланыс саласындағы қылмыстық іс-әрекеттерді талдау барысында ескерілетін болады.

Енді отандық ақпараттандыру мен байланыс салаларындағы заңнамаларды талдауға көшсек.

Қазақстан Республикасының 1997 жылғы Қылмыстық кодексінде бұл мәселе экономикалық қылмыстардың қатарында қаралды. Соңғы кездегі ғылыми техникалық прогрестің нәтижесінде зерттеліп отырған қылмыстық құқық бұзушылықтың объектісінің аясы кеңейді, нәтижесінде ол ақпарат қауіпсіздігімен қатар байланыс жүйесін де қамтитын болды. 1997 жылғы ҚР ҚК-не 2014 жылы енген өзгерістерге сай, бұл қылмыстар жеке тарауға бөлініп шығып (7–1 тарауы ақпараттандыру және байланыс саласындағы қылмыстар), экономикалық қызметке қарсы қылмыстар тарауынан кейінгі орынды иеленді. Ал 2014 жылы қабылданған ҚР ҚК-де олардың орны ауысты. Егер ҚК-нің ерекше бөлігіндегі тараулардың орналасу кезектілігі маңыздылығына қарай құрастырылатынын ескерсек, онда соңғы кодексте екі қылмыстық құқық бұзушылықтардың кезектілігімен толық келісеміз.

2014 жылғы ҚК-нің жобасын талқылау кезінде, «Ақпараттық қауіпсіздікке қол сұғатын қылмыстылыққа қарсы күресте ең алдыменен егжей-тегжейлі түсініктемелік аппаратты құрудың маңызы зор. Бұл терминдер мен ұғымдар ақпаратты өңдеудің жаңа құралдарына техникалық сипаттама беретін және де тасымалдаушы құралдарда сақталып, ақпараттық жүйеде қамтылатын немесе ақпараттық-коммуникациялық желі арқылы беріліп отыратын ақпарат ұғымының мәнін түсіндіретін болады. Құқық қорғау органдары ақпараттық құқықтық қатынастарды реттейтін нормаларды анық түсінбейінше дәлелдеуге жататын мәселелер шеңберін дұрыс анықтай алмайды, одан әрі қылмыстық әрекеттерді дұрыс саралай алмайды» деген пікір айтылған болатын [20].

Бертін келе бұл терминологиялық мәселелер шешімін таба бастады. Мысалы, «ақпараттық қауіпсіздік» ұғымы енгізілген 2012 жылдың 6 қаңтарындағы «Ұлттық қауіпсіздік туралы» ҚР Заңында, ҚР ақпараттық қауіпсіздік тұжырымдамасында қазақстандық заңнамамен рұқсат етілмеген ақпаратты қабылдау, беру және жинақтауды санкцияланбаған қолжетімділіктен техникалық құралдармен қорғау мәселесінің ерекше өзектілігін атап өтті.

Ал Қазақстан Республикасының «Ақпараттандыру туралы» Заңында «автоматтандыру» ұғымына түсінік берілді және ақпараттандыру субъектілері нақтыланды [21]. Келесі «Байланыс туралы» Қазақстан Республикасының Заңында «байланыс» ұғымы ашылды [22].

Жоғарыда айтып кеткеніміздей, ақпараттандыру мен байланыс салаларындағы қылмыстық іс-әрекеттер ҚК-нің 7-тарауында бірге қаралатын болды, оның себебін соңғы заңда «байланыс» ұғымына берілген түсініктемеден іздей аламыз. Онда ақпаратты жинау, өңдеу, тарату шаралары «байланыс» ұғымымен қамтылады. Десе де мұндағы «байланыс» ұғымы тек «ақпаратпен»

шектелінбейді, оған «пошта және арнаулы жөнелтілім, пошталық ақша аударым» да кіреді. Бірақ та соңғыларға қатысты қылмыстық іс-әрекеттер ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар ұғымымен қарастырылмайды.

«Ақпараттық технология — есептеу техникасы құралдарын қолдану негізінде ақпаратты жинау, сақтау, жинақтау, іздеу, өңдеу сынды өзара байланысты әдістері мен тәсілдерінің жүйесі. Ақпараттық технологияның негізгі мақсаты адамның талдауы үшін ақпарат шығару және оның негізінде кез келген әрекетті (басқару шешімін) орындау туралы шешім қабылдау болып табылады.

It–дың ерекшелігі сол, оның еңбек заты мен еңбек өнімі — ақпарат, ал еңбек құралдары — есептеу техникасы мен байланыс құралдары деп танылады» [23].

Ақпараттық технология құралдары деп, әдетте компьютерлік техника түрін айтамыз, онымен ақпараттарды іздеуге, өңдеуге, таратуға болады. Ол тапсырмаларды тез және жеңіл орындау мүмкіндігіне ие. Олардың есептеуіш-ақпараттарды жинап, өңдейтін автоматтандырылған құрылғы, тапсырмаларды техникалық тұрғыдан орындайтын жабдық, байланыс техникасы (ноутбуктер, компьютерлер және т.б.) сынды түрлері бар [24].

Егер ақпараттандыру қызметі ақпараттық технологияның көмегімен жүзеге асырылатындығын, ал соңғысына байланыс техникасының кіретіндігін ескерсек, онда ҚР ҚК-нің 7-тарауындағы «ақпараттандыру мен байланыс саласындағы қылмыстық құқық бұзушылықтар» ұғымының орнына «ақпараттық технология саласындағы қылмыстық құқық бұзушылықтар» ұғымын қолданған дұрыс деп есептейміз.

Нәтижелер

Бұл ұғымның заңнамамен нақтыланбауы әдетте, іс-тәжірибеде қылмыстық іс-әрекеттерді саралауда жиі қиындықтар тудырып жатады. Сондықтан да ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар ұғымын нақтылау ұқсас қылмыстық іс-әрекеттерден ажыратуға зор мүмкіндік берер еді, деп есептейміз.

Мемлекет теориясында құқық бұзушылық, қылмыс ұғымдарына түсінік бергенде әдетте, құқыққа қайшылық, қоғамға қауіптілік (дәрежесі), кінәлілік және қылмыстық іс-әрекеттің қылмыстық заңдағы жазалау қатерімен тыйым салынуы сынды белгілер ескерілу керектігі айтылады.

ҚР ҚК-де қылмыстық құқық бұзушылық ұғымына түсінік берілмейді, бірақ қылмыстық теріс қылық, қылмыс ұғымдары ашылған. Ондағы анықтамаларда соңғы екі ұғым жаза түрімен ерекшеленеді. Егер жаза үкім шығару кезінде белгіленетін мәжбүрлеу шарасы болса, онда қылмыстық істі сотқа дейін тергеп-тексеруде оның көмегімен қылмыс пен қылмыстық теріс қылықты қалай ажыратуға болады екен, деген сауал туындары анық. Сондықтан зерттеліп отырған қылмыстық құқық бұзушылығымыз ең алдыменен нақты қол сұғылатын объектісімен және қылмыстық құралымен, тәсілімен ерекшеленгені дұрыс.

Жоғарыда айтылған ғалымдардың пікірлерін және қылмыстық құқық бұзушылықтарға тән белгілерді ескеріп, мынадай анықтама береміз:

Ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар деп ақпараттық қауіпсіздікке қол сұғатын, ақпараттық ықпал ету тәсілімен жасалынатын немесе (және) қылмыстық құқық бұзушылық затты тасымалдаушы құралдарда сақталатын, ақпараттық жүйеде қамтылған немесе ақпараттық-коммуникациялық желі арқылы берілетін материалдық емес нысандағы ақпарат саналатын, қылмыстық жазалану қатерімен тыйым салынған, қоғамға қауіпті не (немесе) қоғамға зор қауіп төндірмейтін, жеке адамға, ұйымға, қоғамға немесе мемлекетке болмашы зиян келтірген не зиян келтіру қатерін туғызған айыпты жасалған іс-әрекет (әрекет не әрекетсіздік) танылады.

Қорытынды

Авторлар мынадай қорытынды жасайды:

1. Қазақстанда соңғы уақытта ақпараттық технология саласындағы қылмыстық құқық бұзушылықтар саны өсіп, оның қоғамға қауіптілігі артып отыр.

2. Қоғамда ақпараттандыру және байланыс шаралары ақпараттық технологиялар арқылы қамтамасыз етіледі. Ақпараттық технология — бұл ақпараттар ізделетін, өңделетін және берілетін, компьютерлік техниканың түрлері. Ақпараттық технология тек ақпараттандыруды ғана емес, байланысты қамтамасыз ететін құрал.

3. ҚР ҚК-нің 7-тарауымен қарастырылған қылмыстық құқық бұзушылықтар тұтастай ақпараттық технологиялар саласына қолсұғатындықтан аталған тарауды («ақпараттандыру мен

байланыс саласындағы қылмыстық құқық бұзушылықтар» деп аталатын) «Ақпараттық технология саласындағы қылмыстық құқық бұзушылықтар» деп атаған жөн.

4. «Ақпараттық технология саласындағы қылмыстық құқық бұзушылықтар» ұғымына берілген түсінік қылмыстық іс-әрекеттерді дұрыс саралауға мүмкіндік береді.

Әдебиеттер тізімі

1 Смагулов А.А. «Киберщит» и «кибермеч» / А.А. Смагулов // Федерации. [Электронный ресурс]. — Режим доступа: https://www.parlam. kz/ru/blogs/smagylov/Details/4/41406.

2 «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік». Мемлекет басшысы Н. Назарбаевтың Қазақстан халқына жолдауы. 2017 жылғы 31 қаңтар [Электрондық ресурс]. — Қолжетімділік тәртібі: https://www.akorda.kz/kz/addresses/addresses_of_president/memleket-basshysy-nnazarbaevtyn-kazakstan-halkyna-zholdauy-2017-zhylgy-31-kantar.

3 2022 жылға дейінгі киберқауіпсіздік тұжырымдамасын («Қазақстан киберқалқаны») іске асыру жөніндегі іс-шаралар жоспары (Қазақстан Республикасы Үкіметінің 2017 жылғы 28 қазандағы № 676 қаулысы) [Электрондық ресурс]. — Қолжетімділік тәртібі: http://adilet.zan.kz/kaz/docs/P1700000676

4 Мемлекет басшысы Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауы. «Жаңа жағдайдағы Қазақстан: іс-қимыл кезеңі». 2020 жылғы 1 қыркүйек [Электрондық ресурс]. — Қолжетімділік тәртібі: https://www.akorda.kz/kz/addresses/addresses_of_president /memleket-basshysy-kasym-zhomart-tokaevtyn-kazakstan-halkyna-zholdauy-2020-zhylgy-1-kyrkuiek.

5 В Казахстане выявили более 21 тысячи инцидентов по нарушению информационной безопасности. К 2021 году глобальный ущерб от киберпреступности достигнет шести триллионов долларов США / Редакция «Литер» – Федерации [Электронный ресурс]. — Режим доступа: https://liter.kz/v-kazahstane-za-2019-god-bylo-vyyavleno-bolee-21-tysyachi-inczidentov-po-narusheniyu-informaczionnoj-bezopasnosti/ (Дата пупликации: 31 января 2020).

6 Аратулы К. Современные взгляды на некоторые аспекты киберпреступлений / К.Аратулы // Федерации [Электронный ресурс]. — Режим доступа: https://articlekz.com/article/9662

7 Случаи совершения киберпреступлений участились в Казахстане. 15 февраля 2021 12:29 // Федерации [Электронный ресурс]. — Режим доступа: inform.kz https://www.inform.kz/ru/sluchai-soversheniya-kiberprestupleniy-uchastilis-v-kazahstane_a3753267.

8 155 правонарушений в сфере кибербезопасности. 9 ноября 2020 11:28 // Федерации [Электронный ресурс]. — Режим доступа: inform.kz https://www.inform.kz/ru/155-kiberprestupleniy-vyyavili-v-kazahstane_a3716257.

9 Кутубаева А. Банки Казахстана будут сами раскрывать киберпреступления. Такой подход будет эффективнее защищать финансовые данные казахстанцев / А. Кутубаева // Федерации [Электронный ресурс]. — Режим доступа: https://liter.kz/ 7 октября, 2020.

10 Жандыбаев К. Как развивается кибербезопасность Казахстана // strategy2050.kz // Федерации [Электронный ресурс]. — Режим доступа: https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/

11 Николаев Д. К вопросу о понятии компьютерных преступлений / Д.Николаев // Федерации [Электронный ресурс]. — Режим доступа: https://articlekz.com/article/20758.

12 Конвенция о компьютерных преступлениях (Конвенция совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 г. Вступила в силу 1 июля 2004 г. Дополнительный протокол к ней, касающийся криминализации актов расистского и ксенофобского характера, совершенных через компьютерные системы (ETS № 189). Вступил в силу 1 марта 2006 г. // Федерации [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/? doc_id=30170556 #pos=6;-60.

13 Дуленко В.А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учеб. пос. / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. — Уфа: УЮИ МВД России, 2007. — 256 с.

14 Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. — М.: Юрист, 2012. — С. 9–22.

15 Атаманов Г.А. Комментарий к проекту Концепции Стратегии кибербезопасности Российской Федерации, размещённому на сайте Совета Федерации [Электронный ресурс]. — Режим доступа: http://council.gov.ru/press-center/discussions/38324/ (Дата обращения: 28.09.2014).

16 Савельев Д. Некоторые проблемы международного права телекоммуникаций / Д. Савельев // Международное право. 2006 [Электронный ресурс]. — Режим доступа: http://russianlaw.net/ (Дата обращения 21.09.2014).

17 Номоконов В.А. Киберпреступность: проблемы борьбы и прогнозы / В.А. Номоконов, Т.Л. Тропина // Библиотека криминалиста. — 2013. — С. 148–159.

18 Суслопаров А.В. Информационные преступления: автореф. ... канд. юрид. наук / А.В. Суслопаров. — Красноярск, 2008. — 24 с.

19 Маляров А.И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. ... канд. юрид. наук / А.И. Маляров. — Краснодар, 2008. — 27 с.

20 Лоскутов И.Ю. Преступления в сфере информационных технологий в проекте новой редакции Уголовного кодекса Республики Казахстан / И.Ю. Лоскутов. — Федерации [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/? doc_id=31254918&resp= 31254918&status = 0&excludeArcBuh=0#pos=4;-98&doclist_pos=0.

21 *«Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы* (2021.02.01. берілген өзгерістер мен толықтырулармен) [Электрондық ресурс]. — Қолжетімділік тәртібі: http://adilet.zan.kz/kaz/docs/Z1500000418/z150418.htm.

22 Байланыс туралы Қазақстан Республикасының 2004 жылғы 5 шілдедегі № 567-II Заңы (2020.02.07. берілген өзгерістер мен толықтырулармен) [Электрондық ресурс]. — Қолжетімділік тәртібі: http://adilet.zan.kz/kaz/docs/Z040000567_

23 Понятие информационной технологии (ИТ): определение, основные принципы и инструментарий // Федерации [Электронный ресурс]. — Режим доступа: https://cde.osu.ru/courses2/course157/ text/1.2.html.

24 Что такое информационные технологии — понятие, классификация и этапы развития // Федерации [Электронный ресурс]. — Режим доступа: https://ktonanovenkogo.ru/voprosy-i-otvety/informacionnye-tekhnologii-chto-ehto-takoe.html. (Дата публикации: 1 января 2021).

А.Р. Бижанова, Г.Б. Мейрбекова, Г.А. Жунисова

О понятии уголовных правонарушений в сфере информатизации и связи

Проблема обеспечения безопасности компьютерной информации и технологий, в том числе уголовно-правовых средств сегодня является одной из наиболее острых во многих развитых странах мира. Особенно часто компьютеры, их системы и сети используются в промышленности и бизнесе. Предприятия несут большие потери из-за различных компьютерных атак и сбоев. Глобальная компьютерная сеть Интернет превратилась из академического ресурса в коммерческую среду, где важно обеспечить безопасность и предотвратить возможные атаки на развивающиеся отношения. Целью исследования является рассмотрение вопроса правового регулирования киберпреступлений отечественным и зарубежным законодательством и решение терминологических проблем. В результате исследования уточняется понятие уголовных правонарушений в сфере информационных технологий. Авторами рассмотрены состояние, опасность киберпреступности в Казахстане. Учитывая, что уголовные правонарушения в гл. 7 УК РК охватывают сферы информационных технологий, предложено переименовать название главы.

Ключевые слова: информационные технологии, компьютерная информация, компьютерные преступления, уголовные правонарушения в сфере информатизации и связи, уголовные правонарушения в сфере информационной технологии.

A.R. Bizhanova, G.B. Meyrbekova, G.A. Zhunisova

On the concept of criminal offenses in the field of informatization and communication

The problem of ensuring the security of computer information and technologies, including criminal legal means, is today one of the most acute in many developed countries of the world. Computers, their systems, and networks are especially often used in industry and business. Enterprises suffer heavy losses due to various computer attacks and failures. The global computer network Internet has evolved from an academic resource to a commercial environment where it is important to ensure security and prevent possible attacks on developing relationships. The purpose of the study is to consider the issue of legal regulation of cybercrime by domestic and foreign legislation and to solve terminological problems. As a result of the study, the concept of criminal offenses in the field of information technology is clarified. The authors of the article consider the state and danger of cybercrime in Kazakhstan. Given that the criminal offenses in Chapter 7 of the Criminal Code of the Republic of Kazakhstan cover the areas of information technology, it is proposed to rename the title of the chapter.

Keywords: information technologies, computer information, computer crimes, criminal offenses in the field of informatization and communication, criminal offenses in the field of information technology.

References

1 Smagulov, A.A. «Kibershchit» i «kibermech» [«Cyberschit» and «cybermech»]. *parlam. kz.* Retrieved from https://www.parlam. kz/ru/blogs/smagylov/Details/4/41406 [in Russian].

2 Qazaqstannyn ushinshi zhangyruy: zhakhandyq basekede qabilettilik. Memleket basshysy N. Nazarbayevtyn Qazaqstan khalqyna zholdauy. 2017 zhylgy 31 qantar [Address of the head of State N. Nazarbayev to the people of Kazakhstan «third

modernization of Kazakhstan: Global Competitiveness». January 31, 2017]. *akorda.kz.* Retrieved from https://www.akorda.kz/kz/addresses/addresses_of_presıdent/memleket-basshysy-nnazarbaevtyn-kazakstan-halkyna-zholdauy-2017-zhylgy-31-kantar. [in Kazakh].

3 2022 zhylga deiingi kiberqauipsizdik tuzhurymdamasyn ("Qazaqstan kiberqalqany") iske asyru zhonindegi is-sharalar zhospary (Qazaqstan Respubliksy Ukimetinin 2017 zhylgy 28 qasandagy No. 676 qaulysy) [Action plan for the implementation of the concept of cybersecurity until 2022 («Cyber Shield of Kazakhstan») (resolution o the Government of the Republic of Kazakhstan dated October 28, 2017 No. 676)]. *akorda.kz.* Retrieved from http://adilet.zan.kz/kaz/docs/P1700000676 [in Kazakh].

4 Memleket basshyshy Qasym-Zhomart Toqaevtyn Qazaqstan khalqyna Zholdauy. "Zhana zhagdaidagy Qazaqstan: is-qimyl kezeni". 2020 zhylgy 1-qyrkuiek [The message of the Head of State Kassym-Jomart Tokayev to the people of Kazakhstan. «Kazakhstan in new conditions: the period of action». September 1, 2020]. *akorda.kz.* Retrieved from https://www.akorda.kz/kz/addresses/addresses_of_presıdent /memleket-basshysy-kasym-zhomart-tokaevtyn-kazakstan-halkyna-zholdauy-2020-zhylgy-1-kyrkuıek [in Kazakh].

5 V Kazahstane vyiavili bolee 21 tysiachi intsidentov po narusheniiu informatsionnoi bezopasnosti. K 2021 godu globalnyi ushcherb ot kiberprestupnosti dostignet shesti trillionov dollarov SShA / Redaktsiia2 «Liter2» [More than 21 thousand incidents of information security violations were identified in Kazakhstan. By 2021, the global damage from cybercrime will reach six trillion US dollars/ Editorial Board of «Liter»]. *liter.kz*. Retrieved from https://liter.kz/v-kazahstane-za-2019-god-bylo-vyyavleno-bolee-21-tysyachi-inczidentov-po-narusheniyu-informaczionnoj-bezopasnosti [in Russian].

6 Aratuly, K. Sovremennye vzgliady na nekotorye aspekty kiberprestupleniia [Modern views on some aspects of cybercrime. Federations]. *articlekz.com.* Retrieved from https://articlekz.com/article/9662 [in Russian].

7 Sluchai soversheniia kiberprestupleniia uchastilis v Kazakhstane. 15 fevralia 2021. 12:29 [Cases of cybercrime have become more frequent in Kazakhstan. February 15, 2021 12: 29]. *inform.kz.* Retrieved from inform.kz https://www.inform.kz/ru/sluchai-soversheniya-kiberprestupleniy-uchastilis-v-kazahstane_a3753267 [in Russian].

8 155 pravonarushenii v sfere kiberbezopasnosti. 9 noiabria 2020. 11:28 [155 cybersecurity offenses. November 9, 2020 11: 28]. *inform.kz.* Retrieved from inform.kz https://www.inform.kz/ru/155-kiberprestupleniy-vyyavili-v-kazahstane_a3716257 [in Russian].

9 Kutubaeva, A. Banki Kazakhstana budut sami raskryvat kiberprestupleniia. Takoi podkhod budet effektivnee zashchishchat finansovye dannye kazakhstantsev [Kazakhstan's banks will disclose cybercrimes themselves. This approach will more effectively protect the financial data of Kazakhstanis]. *liter.kz*. Retrieved from https://liter.kz [in Russian].

10 Zhandybaev, K. Kak razvivaetsia kiberbezopasnost Kazakhstana [How is Kazakhstan's cybersecurity developing]. *strategy2050.kz.* Retrieved from https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana [in Russian].

11 Nikolaev, D.K. Voprosu o poniatii kompiuternykh prestuplenii [On the question of the concept of computer crimes]. *articlekz.com.* Retrieved from https://articlekz.com/article/20758 [in Russian].

12 Konventsiia o kompiuternykh prestupleniiakh (Konventsiia Soveta Evropy o kiberprestupnosti, Convention on Cybercrime CETS № 185) (Budapesht, 23 noiabria 2001g., vstupila v silu 1 iiulia 2004 goda. Dopolnitelnyi protokol k nei, kasaiushchiisia kriminalizatsii aktov rasistskogo i ksenofobskogo kharaktera, sovershennykh cherez kompiuternye sistemy (ETS № 189), vstupil v silu 1 marta 2006 goda [Convention on Computer Crimes (Council of Europe Convention on Cybercrime, Convention on Cybercrime CETS No. 185) (Budapest, November 23, 2001 Entered into force on 1 July 2004. Its Additional Protocol on the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS No. 189) entered into force on 1 March 2006]. *online.zakon.kz.* Retrieved from https://online.zakon.kz/Document/? doc_id=30170556 #pos=6;-60 [in Russian].

13 Dulenko, V.A., Mamleev, R.R., & Pestrikov, V.A. (2007). *Ispolzovanie vysokikh tekhnologii kriminalnoi sredoi. Borba s prestupleniiami v sfere kompiuternoi informatsii [The use of high technologies by the criminal environment. Combating crimes in the field of computer information]*. Ufa: UYUI MVD Rossii, 256 [in Russian].

14 Chekunov, I.G. (2012). Sovremennye kiberugrozy. Ugolovno-pravovaia i kriminologicheskaia klassifikatsiia i kvalifikatsiia kiberprestuplenii [Modern cyber threats. Criminal-legal and criminological classification and qualification of cybercrimes. Law and cybersecurity]. — Pravo i kiberbezopasnost, 1, 9–22 [in Russian].

15 Atamanov, G.A. Kommentarii k proektu Kontseptsii Strategii kiberbezopasnosti Rossiiskoi Federatsii, razmeshchaennomu na saite Soveta Federatsii [Comment on the draft Concept of the Cybersecurity Strategy of the Russian Federation, posted on the website of the Federation Council]. *council.gov.ru.* Retrieved from http://council.gov.ru/press-center/discussions/38324 [in Russian].

16 Savel'ev, D. (2006). Nekotorye problemy mezhdunarodnogo prava telekommunikatsii [Some problems of international telecommunications law]. *russianlaw.net.* Retrieved from http://russianlaw.net [in Russian].

17 Nomokonov, V.A. & Tropina, T.L. (2013). Kiberprestupnost: problemy borby i prognozy [Cybercrime: problems of struggle and forecasts. Library of Criminalist]. *Biblioteka kriminalista, 1(3),* 148–159 [in Russian].

18 Susloparov, A.V. (2008). Informatsionnye prestupleniia [Information crimes]. *Extended abstract of the candidate's dissertation.* Krasnoyarsk, 24 [in Russia].

19 Malyarov, A.I. (2008). Ugolovno-pravovye i kriminologicheskie aspekty mezhdunarodnogo sotrudnichestva v sfere zashchity elektronno-tsifrovoi informatsii [Criminal and criminological aspects of international cooperation in the field of protection of electronic digital information]. *Extended abstract of the candidate's dissertation*. Krasnodar [in Russia].

20 Loskutov, I.Yu. Prestupleniia v sfere informatsionnykh tekhnologii v proekte novoi redaktsii Ugolovnogo kodeksa Respubliki Kazakhstan [Crimes in the field of information technologies in the draft of the new edition of the Criminal Code of the Republic of Kazakhstan]. *online.zakon.kz*. Retrieved from https://online.zakon.kz/Document/? doc_id=31254918 [in Russian].

21 «Aqparattandyru turaly» Qazaqstan Respublikasynyn 2015 zhylgy 24 qarashadagy No. 418-V Zany (2021.02.01. berilgen ozgerister men tolyqtyrularmen) [Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V "On informatization" (As amended and supplemented on February 1, 2021)] [in Kazakh].

22 Bailanys turaly Qazaqstan Respublikasynyn 2004 zhylgy 5 shildedegi No. 567-II Zany (2021.02.07. berilgen ozgerister men tolyqtyrularmen) [Law of the Republic of Kazakhstan on Communications dated July 5, 2004 No. 567-II (as amended and supplemented on February 7, 2020)] [in Kazakh].

23 Poniatie informatsionnoi tekhnologii (IT): opredelenie, osnovnye printsipy i instrumentarii [The concept of information technology (IT): definition, basic principles and tools]. *cde.osu.ru.* Retrieved from https:// https://cde.osu.ru/demoversion/course157/text/1.2.html. [in Russian].

24 Chto takoe informatsionnye tekhnologii — poniatie, klassifikatsiia i etapy razvitiia [What is information technology-the concept, classification and stages of development]. *ktonanovenkogo.ru.* Retrieved from https://ktonanovenkogo.ru/voprosy-i-otvety/informacionnye-tekhnologii-chto-ehto-takoe.html [in Russian].