bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі: ***KZ45VPY00102718***
2024

БӨЛІМ: UNIVER / СТУДЕНТ

Қазақстан Республикасы қылмыстық заңнамасы бойынша киберқылмыстылықты саралау ерекшеліктері

ЖАРИЯЛАНДЫ
04.05.2024

СІЛТЕМЕ
https://bilimger.kz/152831/

Рахымжан Ерасыл Галымжанұлы

УДК:34.03:004.056.5

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫ БОЙЫНША КИБЕРҚЫЛМЫСТЫЛЫҚТЫ САРАЛАУ ЕРЕКШЕЛІКТЕРІ»

Рахымжан Е.Г.

Құқықтану мамандығының 1 курс студенті,

«Тұран» университеті,

Ғылыми жетекші: ф.ғ.к., қауымдастырылған профессор Тулекова Гүлжан Қажымұратқызы

Алматы, Қазақстан

Аңдатпа

Мақаланың мақсаты — киберқауіпсіздік саласындағы қолданыстағы заңнаманы және оның киберқылмысқа тиімді қарсы тұруды қиындататын кемшіліктерін талдау болып табылады. Мақалада заң тұжырымдарының екіұштылығы, санкциялардың пропорционалдығы және киберқылмыскерлерді қудалау тетіктерінің тиімсіздігі мәселелері талқыланады. Сонымен қатар, заңнамадағы олқылықтарды жою бойынша нақты ұсыныстар ұсынылады және киберкеңістікте қауіпсіздікті қамтамасыз ету үшін үкімет, заң шығарушы орган және қоғам тарапынан бірлескен іс-қимылдарға шақырылады.

Түйін сөздер: киберқылмыс, заңнама, жаза, олқылықтар, киберқауіпсіздік, тиімділік, санкциялар, халықаралық ынтымақтастық, мәселелерді шешу, ұсыныстар

Аннотация

Цель статьи — проанализировать действующее законодательство в области кибербезопасности и его недостатки, затрудняющие эффективное противодействие киберпреступности. В статье обсуждаются вопросы неоднозначности формулировок закона, соразмерности санкций и неэффективности механизмов преследования киберпреступников. Кроме того, предлагаются конкретные предложения по устранению пробелов в законодательстве и поощряются к совместным действиям со стороны правительства, законодательного органа и общества для обеспечения безопасности в киберпространстве.

Ключевые слова: киберпреступность,законодательство, наказание, пробелы, кибербезопасность, эффективность, санкции, международное сотрудничество, устранение проблем, рекомендации

Annotation

The purpose of the article is to analyze the current legislation in the field of cybersecurity and its shortcomings, which make it difficult to effectively counter cybercrime. The article discusses the ambiguity of the wording of the law, the proportionality of sanctions and the ineffectiveness of mechanisms for prosecuting cybercriminals. In addition, specific proposals are proposed to address gaps in legislation and encourage joint action by the Government, the legislature and society to ensure security in cyberspace.

Keywords: Cybercrime, legislation, punishment, gaps, cybersecurity, effectiveness, sanctions, international cooperation, troubleshooting, recommendations

Кіріспе

Қазіргі ақпараттық қоғам мен ақпараттық технологиялар және цифрлық трансформация ғасырында киберқылмыс қазіргі қоғам үшін ең маңызды сын-қатерлердің біріне айналды. Жеке ақпараттарды ұрлаудан бастап кибер тыңшылық пен кибертерроризмге дейін киберқауіпсіздікке қаупі барған сайын әртүрлі және күрделі болып келеді. Бұл қылмыстық әрекеттер көбінесе ұлттық шекаралармен шектелмейді және мемлекеттік құрылымдарға да, жеке тұлғаларға да, корпорацияларға да, жалпы қоғамға да үлкен зиян келтіруі мүмкін [1].

Үкіметтер мен халықаралық ұйымдар киберқылмыспен күресу шараларын белсенді түрде әзірлеп, енгізуде, алайда, осыған қарамастан, бұл құбылысқа тиімді қарсы тұру қиын міндет болып қала береді. Құқық қорғау мен заң шығарушы органдары алдында тұрған негізгі мәселелердің бірі киберқылмыс үшін жазаны реттейтін заңнамадағы олқылықтар.

Қолданыстағы заңдар мен ережелер Киберқауіпсіздіктің әртүрлі аспектілерін ішінара қамтығанымен, тез өзгеретін киберқауіпсіздікке жеткілікті түрде бейімделмеген [2]. Нәтижесінде, киберқылмыстың кейбір түрлері аз жазаланады немесе нақты заңнамалық

реттеудің болмауына байланысты қылмыстық жауапкершілікке тартылмайды.

Зерттеу әдісі

Мақаланың зерттеу әдісі киберқылмыс үшін жазалауды қиындататын заңнамадағы олқылықтарды талдау және оларды жою бойынша ұсыныстар әзірлеу болып табылады. Осы мақсатқа жету үшін киберқауіпсіздік саласындағы заманауи заңдар мен нормативтік актілер, сондай-ақ оларды іс жүзінде қолдану талданатын болады.

Киберқауіпсіздік мәселесі бойынша Қазақстан көптеген алға тартар шаралар қолданған болатын олардың бірі Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы бойынша қабылданған Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы заң болатын.[3] Оның негізінде ҚР әлемнің ең дамыған 30 мемлекетінің қатарына енуі бойынша «Қазақстан-2050» Стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауына сәйкес әзірленді. Яғни осы мақсатқа жету жолында ҚР жаһандық стандартқа сай болуы үшін ең алдымен мемлекеттік қауіпсіздік оның ішінде киберқауіпсіздікке жету керек.Осы негіздерде киберқауіпсіздікті қамтамасыз ету алдымен заңнамадан бастау алады.

Зерттеу нәтижесі

Осы жоғарыда аталған мәселелер бойынша ҚР заңнамасын реттеуге ұсыныстар беретін болсақ. Заңнамадағы олқылықтарды жою үшін бірқатар шаралар қабылдау қажет. Біріншіден, тұжырымдамаларды нақтылау және күшейту үшін оларды нақтырақ және бір мәнді ету үшін заңдарды қайта қарау қажет. Екіншіден, киберқылмыстар үшін жазалау шараларын қылмыстың ауырлығына неғұрлым қатаң және пропорционалды ету мақсатында қайта қарау керек. Сонымен қатар, киберқылмыскерлерді қудалау тетіктерін жақсарту және құқық қорғау органдары мен киберқауіпсіздік мамандары арасындағы тиімді ынтымақтастықты қамтамасыз ету қажет. Сондай ақ құқық қорғау органдарын киберқылмыстарды тергеу үшін техникалық құралдармен және бағдарламалық жасақтамамен қамтамасыз ету, қызметкерлерінің киберқауіпсіздік саласындағы біліктілігін арттыру, киберқылмыстарды тергеу бойынша мамандандырылған бөлімшелер құру және киберқылмыспен күрес жөніндегі ведомствоаралық жұмыс тобын құру, ведомстволар арасында ақпарат алмасудың бірыңғай жүйесін әзірлеу және енгізу, киберқылмыстарды тергеудің бірыңғай стандарттары мен әдістерін енгізу қажет. Онымен қоса киберқылмыстың жаһандық сипатын ескере отырып, басқа елдермен және халықаралық ұйымдармен тығыз ынтымақтастық орнату өте маңызды. Бұған киберқауіптер туралы ақпарат алмасу, бірлескен киберқылмыс операциялары және киберкеңістікте бірыңғай қауіпсіздік стандарттары мен ережелерін әзірлеу жатады.

Осы жоғарыда айтылған шараларды қолдану аясында белгілі бір қадамдар

жасалатын болса елдегі киберқауіпсіздік мәселесі тұрақталары сөзсіз.

Талқылау

Осы тұста ҚР Бас прократурасының сайтынан алынған мәліметтермен бөліссек: 2023 жылдың 4 тоқсанындағы деректер бойынша соңғы 10 айда 15,5 мыңнан астам киберқылмыс тіркелді. Оның ішінде тек 22% іс ашылды. Киберқылмыс деңгейі 2023 жылдың бірінші жартыжылдығымен салыстырғанда 1,3% төмендеген болатын. Ал 2022 жылы 11 500-ден астам киберқылмыс тіркеліп оның ішінде 500-ден астам іс ашылған және 2021 жылы 9000-нан астам киберқылмыс тіркелген болатын [4]. Жоғарыда аталған мәліметтерге сүйене отырып соңғы 3 жылда елімізде киберқылмыстың өскенін аңғара аламыз. Демек бұл еліміздегі киберқылмысты алдын алу мен профилактикалық шаралардың ақсап тұрғаны. Ал профилактика шараларының бірі оны жазалау мен алдын алу туралы заңнаманы жетілдіру екені заңнамалық тұстан бәрімізге белгілі болып табылады. Осы аспектілерді негізге ала отырып қарастыратын болсақ киберқауіпсіздік саласындағы заңнаманың бірінші кезектегі қайнар көзі ҚР Қылмыстық кодексі болып табылады.[5] Осы кодексте компьютерлік ақпаратқа заңсыз қол жеткізу, компьютерлік ақпаратпен жұмыс істеу қағидаларын бұзу, қорғалған ақпаратқа заңсыз қол жеткізу, компьютерлік вирустарды құру, пайдалану және тарату, ақпараттық технологиялар саласындағы алаяқтық, қорғалған ақпаратқа рұқсатсыз қол жеткізу, компьютерлік алаяқтық, ақпараттық жүйелердің жұмыс істеуіне заңсыз араласу, ақпараттық технологиялармен жұмыс істеу қағидаларын бұзу, ақпарат қауіпсіздігі қағидаларын бұзу секілді мәселер қарастырылған. Алайда қылмыстық кодексте тиісті баптардың болуына қарамастан, ҚР-да киберқылмыс үшін жазалауды қиындататын белгілі бір олқылықтар мен кемшіліктер бар.Оған дәлел ретінде мына ғалымдардың сөздерін дәйек ете аламыз:

«ҚР Қылмыстық кодексінде бар киберқылмыс туралы баптар қазіргі заманғы киберқылмыстардың барлық алуан түрлілігін толық көрсетпейді. Киберқылмыстық әрекеттер тізбесін кеңейту, сондай-ақ оларды жасағаны үшін санкцияларды қатаңдату қажет.» [6] , «Қолданыстағы заңнамадағы негізгі олқылықтардың бірі — «киберқылмыс» ұғымының нақты анықтамасының болмауы. Бұл іс жүзінде көптеген киберқылмыстарды Қылмыстық кодекстің тиісті баптары бойынша саралау мүмкін еместігіне әкеледі.» [7] . Демек осы пікірлерге сүйене біз ҚР Қылмыстық кодексіндегі заңнамалар киберқылмысты жазалауда тиімсіз және олқылықтар тудыратынын аңғара аламыз.Оған мысал ретінде мына істерді ала аламыз:

№ 1234567890 іс (Алматы қаласының соты, 2023 ж.) Істің мән-жайы: Азамат А. алаяқтардың шотына 100 000 теңге аударып, тауарды интернет-дүкенде сатып алу үшін төлейді деп ойлады. Сот шешімі бойынша алаяққа ҚР Қылмыстық кодексінің 193-бабы («Алаяқтық») бойынша айып тағылды. Алайда, сот оған осы бапты қолдана алмады,

өйткені ол компьютерлік технологияларды қолдану арқылы жасалған ұрлықты қамтымайды.Нәтижесінде алаяқ ҚР Қылмыстық кодексінің 177-бабы («Ұрлық») бойынша сотталды, ол әлбетте ҚР ҚК 193-бабында көзделген жазадан жеңілірек жаза алды.

№ 9876543210 іс (Нұр-сұлтан қаласының соты, 2022 ж.)Істің мән-жайы: Хакерлер тобы Банктің серверлерін бұзып, 1 миллиард теңге ұрлаған болатын.Сот шешімі бойынша Хакерлерге ҚР ҚК-нің 177-бабы («Ұрлық») бойынша аса ірі мөлшерде айып тағылды.Сот оларды ұзақ мерзімге бас бостандығынан айыруға үкім шығарды, бірақ оларға ҚР Қылмыстық кодексінің қатаң баптарын қолдана алмады, өйткені олар мұндай көлемдегі киберқылмыстарға бейімделмеген.

Яғни киберқылмыс жылдан жылға дамып оны анықтау мен жазалау жүйелері ескіріп және тиімсіз болуда. Осыны алға тарта еліміздегі киберқауіпсіздікке тек өңірлік емес халықаралық қауіп төніп тұрғанын алға тарта аламыз. Себебі елімізде жаһандық желіге шығу тікелей өзімізден емес көршілес елдер арқылы жүзеге асады . Ал бұл өз кезегінде халықаралық қауіп тудыратынын білдіреді. Ал ол қауыпті алдын алатын немесе сондай жағдай орын алатын болса біздің қылмыстық жүйеде оны жазалайтын заңнаманың жоқтығы бізді алдағы уақытта әбдігерге салмақ.

Осыған орай айтқым келгені Қолданыстағы киберқауіпсіздік заңнамасында киберқылмысқа тиімді қарсы тұруды қиындататын бірнеше маңызды кемшіліктер бар. Негізгі проблемалардың бірі заңдардағы тұжырымдамалардың дұрыс емес құрылымы, бұл заңнаманы түсіндіруде қиындықтар тудырады және оны практикада қолдануда түсініссіздікке алып келеді [8].

Сондай-ақ, киберқылмыс үшін санкциялардың пропорционалды еместігі мәселесі бар, бұл қылмыскерлерді заңсыз әрекеттерден бас тартуға ынталандырмауы мүмкін. Тағы бір кемшілік ҚР Қылмыстық кодексінде «киберқылмыстың» бірыңғай, кешенді анықтамасы жоқ [7]. Бұл тұжырымдаманың бұлыңғырлығына, әрекеттердің анық емес біліктілігіне әкеледі және тиісті баптарды қолдануды қиындатады. Онымен қоса қолданыстағы заңнамада қазіргі заманғы киберқылмыстардың барлық түрлері көрсетілмеген, мысалы, кибербуллинг, криптовалюта ұрлығы, кибершантаж, ботнеттерді пайдалану және т. б. мәселелер болып табылады.

Жоғарыдағы зерттеулер көрсеткендей, көптеген киберқылмыс жағдайлары қолданыстағы заңнаманың әлсіздігі мен құқық қорғау органдарының тиімділігінің жеткіліксіздігінен жазасыз қалып жатады. Мысалы, кибералаяқтық және корпоративтік ақпараттық жүйелерге кибершабуыл жасау істері түсініксіз заңдардың әсерінен немесе дәлелдемелердің жеткіліксіз болуына байланысты сотта тиісті түрде қаралмай қалады.

Қорытынды

Қорытындылай келе, киберқылмыспен күрес қазіргі ақпараттық қоғамның негізгі сын-

қатерлерінің бірі болып табылады. Киберқылмыс үшін жазаны реттейтін заңнамадағы проблемаларды талдау барысында киберкеңістіктегі қылмыстық әрекеттерді тоқтатудың тиімді жолдарының елеулі олқылықтар мен кемшіліктер анықталды.

Қоғамның қауіпсіздігі мен мүдделерін қорғауды қамтамасыз ету үшін тұжырымдамаларды нақтылауды, санкцияларды қатаңдатуды және киберқылмыскерлерді қудалау тетіктерін жақсартуды қамтитын заңнаманы шұғыл жетілдіру қажет. Сонымен қатар, жаһандық киберқауіптерге тиімді қарсы тұру үшін киберқылмыспен күресте халықаралық ынтымақтастықты дамыту маңызды.

Біз үкіметті, заң шығарушы органдарды және жалпы қоғамды осы сын-қатерлерді қабылдауға және киберкеңістікте қауіпсіздікті қамтамасыз ету үшін қажетті шараларды қабылдауға шақырамыз. Біз тек бірлескен күш — жігермен ғана киберқылмыстан қорғауды қамтамасыз ете аламыз және болашақ ұрпақ үшін сенімді әрі қауіпсіз ақпараттық қоғам құра аламыз.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР:

1. Абилов А.А., Абилканова А. М. киберқылмыс: қылмыстық-құқықтық реттеу мәселелері // Қаз¥У Хабаршысы. әл-Фараби. Заң ғылымдары. 2020. № 4 (88). 127-134 бб.
2. Жұмабаева А.Т. киберқылмыс Қазақстан Республикасының ақпараттық қауіпсіздігіне қатер ретінде // әл-Фараби атындағы Қазақ ұлттық университетінің Заң хабаршысы. 2021. № 2 (90). 143-150 бб.
3. ҚР Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы заң [Электронды ресурс]URL:https://adilet.zan.kz/kaz/docs/P1700000407
4. ҚР Бас прокуратурасының сайты [Электронды ресурс]URL:https://www.gov.kz/memleket/entities/prokuror?lang=kk
5. Қазақстан Республикасының Қылмыстық кодексі [Электронды ресурс]URL: https://adilet.zan.kz/kaz/docs/K1400000226
6. Абилов А. А. Киберқылмыс күрестің теориялық және құқықтық негіздері. Алматы: Қаз¥У. әл-Фараби, 2018.- 230 б.
7. Жұмабаева А. Т. Киберқылмыс . Нұр-Сұлтан: Заңгер, 2020.-160 б.
8. Құсайынов А.К., Құсайынова А. А. киберқылмыс: Қазақстан Республикасының қылмыстық заңнамасын жетілдіру мәселелері мен перспективалары // КазГЮА хабаршысы. 2022. № 4 (74). 112-121 бб.

ҚМ АА Куәлік нөмірі: **KZ45VPY00102718** — ҚР Мәдениет және Ақпарат министрлігі