



# ҚЫЛМЫСТЫҚ ПРОЦЕСС, КРИМИНАЛИСТИКА, СОТ-САРАПТАМА ҚЫЗМЕТІ / УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА, СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ / CRIMINAL PROCEDURE, CRIMINALISTICS, FORENSIC EXPERTISE

ӨОЖ 343.13  
ХҒТАР 10.79.41

Д.А. Ашимбаев, Г.И. Тогизбаев  
*Қонаев университеті, Алматы қ., Қазақстан Республикасы*

## КИБЕРҚЫЛМЫСТАР: ХАЛЫҚАРАЛЫҚ ҰНТЫМАҚТАСТЫҚ ҚАЖЕТТІЛІГІ МЕН ҚҰҚЫҚТЫҚ РЕТТЕУ ЖОЛДАРЫ

**Аннотация.** Жаңа буындағы жоғары жылдамдықтағы сымсыз байланыс технологиялары киберқылмыстардың өсуіне ықпал етіп, мемлекет пен азаматтардың қауіпсіздігіне қатер төндіруде. Осыған байланысты 2024 жылы Қазақстан Республикасы ІІМ құрылымында Киберқылмысқа қарсы іс-қимыл департаменті құрылды. Дегенмен, елімізде киберқауіптерге қарсы күреске бағытталған кешенді стратегиялық бағдарлама жоқ. Бұл халықаралық тергеу әрекеттерінде процестік шектеулерге алып келіп және ҚПК қағидаттарын толық іске асыруға кедергі келтіреді. Себебі көптеген киберқылмыстар шетелдік юрисдикция шеңберінде жасалады. Осы зерттеу аясында киберқауіпсіздікті қамтамасыз ету мақсатында келесі ұсыныстар әзірленді: 1) «Киберқауіпсіздік туралы» ұлттық заң қабылдау қажеттілігі; 2) киберқылмыстармен күрес жүргізетін халықаралық ұйым құру; 3) киберқылмыстық қауіп төнуі мүкін елдермен киберқауіпсіздік саласындағы халықаралық ынтымақтастық туралы шарт жасау.

Қазақстан Республикасының Қылмыстық-процестік кодексінің 560-бабының 1-тармағына сәйкес «Құқықтық және өзге де көмек көрсету туралы сұрау салу Қазақстан Республикасының тиісті халықаралық шартының талаптарына сәйкес жасайды», - делінген. Яғни, ықтимал жасалуы киберқылмыстар әлемнің кез келген нүктесінен жасалуы мүмкін деп пайымдасақ, онда мақалада ұсынылған барлық шаралардың аса маңызды екендігіне көз жеткіземіз.

**Түйінді сөздер:** киберқылмыс; киберқауіпсіздік; халықаралық шарт; халықаралық ұйым; кибералақтық; қылмыстық топ; қаржы мониторингі; геосаясат; халықаралық ынтымақтастық; кибертерроризм.

Д.А. Ашимбаев, Г.И. Тогизбаев  
*Университет Қунаева, г. Алматы, Республика Казахстан*

## КИБЕРПРЕСТУПЛЕНИЯ: НЕОБХОДИМОСТЬ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА И ПУТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ

**Аннотация.** Развитие высокоскоростных беспроводных технологий нового поколения способствует росту киберпреступности и представляет угрозу для безопасности государства и прав граждан. В связи с этим 5 ноября 2024 года в структуре Министерства внутренних дел Республики Казахстан был создан Департамент по противодействию киберпреступности. Однако в стране отсутствует комплексная стратегическая программа по борьбе с киберугрозами. Это создает процессуальные ограничения при осуществлении международного расследования и затрудняет полную реализацию положений Уголовно-процессуального кодекса. Особенно это актуально в случаях совершения киберпреступлений из под юрисдикции иностранных государств. В рамках настоящего исследования разработаны следующие предложения по обеспечению кибербезопасности: 1) необходимость принятия национального закона «О кибербезопасности»; 2) создание международной организации по борьбе с киберпреступностью; 3) киберугрозы со стороны отдельных государств требуют заключения международных соглашений о сотрудничестве в сфере кибербезопасности.

Согласно пункту 1 статьи 560 Уголовно-процессуального кодекса Республики Казахстан, «запрос о правовой и иной помощи осуществляется в соответствии с требованиями соответствующего



международного договора Республики Казахстан».

Иными словами, если исходить из того, что потенциально киберпреступления могут совершаться из любой точки мира, то становится очевидным, что все предложенные в статье меры имеют чрезвычайно важное значение.

**Ключевые слова:** киберпреступление; кибербезопасность; международный договор; международная организация; кибермошенничество; преступная группа; финансовый мониторинг; геополитика; международное сотрудничество; кибертерроризм.

**D.A. Ashimbayev, G.I. Togizbayev**  
*Kunayev University, Almaty, the Republic of Kazakhstan*

## **CYBERCRIMES: THE NEED FOR INTERNATIONAL COOPERATION AND LEGAL REGULATORY APPROACHES**

**Abstract.** The development of next-generation high-speed wireless technologies contributes to the rise of cybercrime and poses a threat to state security and citizens' rights. In response, on November 5, 2024, the Department for Combating Cybercrime was established within the structure of the Ministry of Internal Affairs of the Republic of Kazakhstan. However, there is still no comprehensive strategic program in the country aimed at countering cyber threats. This results in procedural limitations during international investigations and hinders the full implementation of the provisions of the Criminal Procedure Code. This issue becomes particularly relevant when cybercrimes originate from the jurisdiction of foreign states. Based on the findings of this research, the following proposals have been developed to strengthen cybersecurity: 1) adoption of a national law "On Cybersecurity"; 2) establishment of an international organization to combat cybercrime; 3) Cyber threats posed by certain states necessitate the conclusion of international agreements on cooperation in the field of cybersecurity.

According to paragraph 1 of Article 560 of the Criminal Procedure Code of the Republic of Kazakhstan, "a request for legal and other assistance shall be made in accordance with the requirements of the relevant international treaty of the Republic of Kazakhstan".

In other words, considering that potential cybercrimes can be committed from any point in the world, it becomes evident that all the measures proposed in the article are of paramount importance.

**Keywords:** cybercrime; cybersecurity; international treaty; international organization; cyber fraud; criminal group; financial monitoring; geopolitics; international cooperation; cyberterrorism.

DOI: 10.52425/25187252\_2026\_39\_123

*Кіріспе.* Киберқылмыстарды тергеу барысында туындайтын негізгі қиындықтардың бірі – қылмыстардың нақты басталу нүктесінің белгісіз болуы, сондай-ақ қылмыскерлердің заманауи нанотехнологиялар мен жасанды интеллект мүмкіндіктерін өз мақсаттарына теріс пайдалануымен байланысты.

Зерттеу жұмысымызда төмендегі терминдерге ғылыми анықтама алынды, берілген анықтама ғылыми жұмыстың жаңалығы ретінде ұсынылады. Себебі елімізде киберқауіпсіздік туралы заң қыбалданған жоқ. Алайда елімізге күн сайын төніп тұрған киберқауіптер заңның шұғыл қабылданғанын талап етеді.

*Киберкеңістік дегеніміз* – кабельді немесе ғарыштық технологиялармен қуатталған

толқынды интернет желілерімен немесе жасанды интеллектпен қамтамасыз етілген сандық коммуникациялық және компьютерлік технологиялырадың артықшылықтарын пайдалану арқылы жүзеге асырылатын виртуалды кеңістік.

*Киберқылмыс дегеніміз* – кабельді немесе ғарыштық технологиялармен қуатталған толқынды интернет желілерімен немесе жасанды интеллектпен қамтамасыз етілген сандық коммуникациялық және компьютерлік технологиялардың киберкеңістік жүйесінде қылмыстық қатер төндірумен немесе сондай қатер төндіруі мүмкін қоғамға қауіпті қылмыстық заңға қайшы іс-әрекетті (әрекет немесе әрекетсіздікті) айтамыз.

*Киберқауіпсіздік дегеніміз* – адамың



өмірі мен денсаулығы, ар-намыс, қадыр – қасиеті, жеке мүлкі мен дербес деректері, сондай-ақ заңды тұлғалардың мүлкі мен заңды мүдделері, сандық технологиялар мен киберкеңістіктің қорғалуы, ұлттық қауіпсіздік пен елдің біртұтастығы және де демократиялық құндылықтардың сақталуының қауіпсіздігін қамтамасыз етуді айтамыз.

Аталған ғылыми териминалогияларға Қазақстан Республикасының Әділет министрлігінің Ұлттық зияткерлік меншік институтынан 23 желтоқсан 2025 жылы «Киберқауіпсіздік саласындағы ғылыми анықтама» атауымен авторлық қорғауға алынып № 65694 куәлік берілді.

*Материалдар мен әдістер.* Мақалада салыстырмалы құқықтық талдау және теориялық жалпылау, индуктивті және дедуктивті, нормативтік құқықтық талдау және болжау әдістері қолданылды. Ғылыми зерттеу жұмысы барысында қойылған ғылыми міндеттерді шешу және зерттеу мақсатына қол жеткізу үшін жалпығылыми және арнайы ғылыми таным әдістерінің кешені қолданылды. Атап айтқанда, салыстырмалы құқықтық талдау әдісі арқылы ұлттық және шетелдік құқықтық нормалар, ғылыми тұжырымдамалар мен тәжірибелер өзара салыстырылып, олардың ұқсастықтары мен айырмашылықтары айқындалды, құқықтық реттеудің тиімді үлгілері анықталды. Теориялық жалпылау әдісі зерттеліп отырған құбылыстың мәнін ашуға, ғылыми көзқарастарды жүйелеуге және тұжырымдамалық қорытындылар қалыптастыруға мүмкіндік берді. Соның ішінде Қазақстан Республикасының Қылмыстық процестік кодексінің Қылмыстық сот ісін жүргізу саласындағы халықаралық ынтымақтастық бөлімі аталған мақаланың тірегі болып саналады. Шетелдік ғалымдардың зерттеу нәтижелері ғылыми зерттеудің эмпирикалық негізін құрады.

Зерттеу барысында индуктивті әдіс жекелеген деректер мен нақты құқық қолдану тәжірибелерін талдау негізінде жалпы ғылыми тұжырымдар жасауға бағытталған

болса, ал дедуктивті әдіс жалпы теориялық қағидалар мен құқықтық ережелерден жекелеген қорытындылар мен ұсыныстар шығаруға мүмкіндік берді. Зерттеу шеңберінде нормативтік құқықтық талдау әдісі ұлттық заңнама актілерінің мазмұнын, құрылымын және құқықтық реттеу тетіктерін зерделеуге, олардың өзара байланысы мен қолданылу ерекшеліктерін анықтауға және киберқылмыстарға қарсы күреске бағытталған халықаралық конвенцияларға шолу жасалды.

Бұдан басқа болжау (прогностикалық) әдісі зерттеу нысанына қатысты құқықтық реттеуді жетілдірудің ықтимал бағыттарын айқындауға, құқықтық дамудың болашақ тенденцияларын негіздеу және практикалық ұсыныстар әзірлеу мақсатында пайдаланылды.

*Нәтижелер, талқылау.* 2025 жылғы 23 қыркүйекте Қазақстан Республикасы Ішкі істер министрлігінің Киберқылмыстарға қарсы іс-қимыл департаменті, ҚР Бас прокуратурасы, Украина Ұлттық полициясы және Украина Бас прокуратурасымен бірлесіп, трансұлттық кибералаяқтық қылмыстық тобының әрекетіне тосқауыл қойды<sup>1</sup>. Ұзақ мерзімді бірлескен жедел-іздістіру іс-шараларының нәтижесінде Черновцы және Одесса қалаларында қазақстандық азаматтарға қарсы алаяқтық әрекеттер жасаған call-орталықтың қызметі тоқтатылды. Трансұлттық ұйымдасқан қылмыстық топ мүшелері алдын ала құрылған схема бойынша әрекет еткен. Олар өзін Қазақстанның Ұлттық банкі, құқық қорғау органдары мен арнайы қызмет өкілдері ретінде таныстырып, жәбірленушілерге «күдікті операциялар» және «террористік ұйымдарды қаржыландыру» бойынша қылмыстық жауаптылыққа тарту қаупімен психологиялық қысым жасаған. Соның нәтижесінде азаматтар несие рәсімдеуге, мүліктерін сатуға және ақшалай қаражаттарын бөгде тұлғалардың есепшоттарына аударуға мәжбүр болған. Сондай-ақ ұсталған қылмыстық топтың қатаң иерархиялық құрылымы болған: қатысушылар арасында нақты рөлдер – әкімшілік қызметкерлер, HR-менеджерлер, «клоузерлер», «холдингер»,

<sup>1</sup> Казахстан и Украина провели совместную спецоперацию в Киеве [Электрондық ресурс] – Айналыс режимі: <https://tengrinews.kz/crime/kazakhstan-ukraina-proveli-sovmestnuyu-spetsoperatsiyu-kieve-581141/> (жүгінген күні: 19.10.2025).



техникалық персонал және т.н. «күштік блок» бөлінген.

Кибералаяқтық жолымен алынған қаражат call-орталықты ұстауға, автокөлік сатып алуға және өзге де шығындарға жұмсалған. Офисті ай сайын ұстау шығындары ұйымдастырушыларға шамамен 60 мың АҚШ долларын құраған. Күдіктілердің бірі соңғы алты айда қылмыстық жолмен алынған қаражатқа бес автокөлік сатып алған.

Бір мезгілде жүргізілген тінту барысында күдіктілердің тұрғылықты мекенжайларынан жәнес call-орталықтан 30-дана стам компьютер, 79 ұялы телефон, көп санды Sim-карталар, құқық қорғау және арнайы органдардың, сондай-ақ Ұлттық Банктің атынан жалған куәліктер мен формалық киімдер, алдын ала дайындалған жауап сценарийлері және өзге де заттай дәлелдемелер тәркіленді. Сонымен қатар, deepfake технологиясын пайдалана отырып бейне және дауыс жасауға арналған арнайы бағдарламалық қамтамасыз ету анықталды.

Аталған қылмыстық топтың әрекетінен Қазақстан азаматтарына 900 миллион теңгеден астам материалдық зиян келтірілген. Тергеу шараларының нәтижесінде Украина аумағында тоғыз азамат ұсталып, олардың бесеуі қамауға алынды. ҚР Ішкі істер министрлігі бұл операцияны екі елдің құқық қорғау органдарының үйлесімді өзара іс-қимылының нәтижесі және трансұлттық қылмыстық топтардың қызметін тоқтатуға бағытталған бірлескен табанды әрекет деп бағалады<sup>2</sup>.

Қазіргі уақытта ҚР-ның киберкеңістігінде заңсыз криптовалюта айырбастау бөлімшелері анықталуда. Солардың ішіндегі ең ірісі RAKS Exchange сервисі, оны Қаржы мониторингі агенттігі жедел-іздістіру іс-шаралары барысында әшкерелеп, қылмыстық әрекетке қатысы бар тұлғаларды жауаптылыққа тартты. Анықталған мәліметтерге сәйкес бұл платформа арқылы интернет-алаяқтар мен есірткі

сатумен айналысатын тұлғалар заңсыз табыстарын заңдастырып отырған. RAKS Exchange қызметін трансұлттық ұйымдасқан қылмыстық топтар ұйымдастырып, ол 20 ірі Darknet-маркетпен серіктестік орнатқан және 5 миллионға жуық пайдаланушыны қамтыған.

Аталған деректер ұйымдасқан қылмыстық топтың халықаралық деңгейде әрекет еткенін көрсетеді. Оның қызметі бірқатар елдердің азаматтарына айтарлықтай материалдық және денсаулыққа зиян келтіріп, ұлттық қауіпсіздікке қауіп төндірген. RAKS

Exchange платформасы арқылы көптеген адамдар, оның ішінде жасөспірімдер, есірткі заттарына қол жеткізіп, есірткіге тәуелділікке ұшыраған. Тек ТМД елдерінде осы сервис арқылы 200 мыңнан астам есірткі сатып алу әрекеті (наркошопинг) тіркелген. Аталған платформаның заңсыз жолмен тапқан табысы 224 миллион АҚШ долларынан асқан.

Қазіргі уақытта 67 крипто-әмиян жойылып, жалпы сомасы 9,7 миллион АҚШ доллары (шамамен 5,2 млрд теңге) бұғатталды<sup>3</sup>.

Қылмыстық сот ісін жүргізу саласындағы халықаралық ынтымақтастық мәселесі ҚР ҚПК-нің 12-бөлімімен реттеледі<sup>4</sup>.

Одан бөлек Қазақстан Республикасының халықаралық шарттары туралы 2005 жылғы 30 мамырдағы заңының нормасына сәйкес халықаралық шарттар келесідей түрлерге бөлінеді:

1) ҚР-нің атынан;

2) ҚР-нің Үкіметінің атынан;

3) ҚР Президентіне тікелей бағынатын және есеп беретін ҚР мемлекеттік органдарының, сондай-ақ ҚР орталық атқарушы органдарының атынан ҚР заңнамасында айқындалған өз құзыреті шегінде шет мемлекеттермен және (немесе) халықаралық ұйымдармен жасалған шарттар<sup>5</sup>.

Қазіргі таңда ҚР азаматтық және қылмыстық істер бойынша өзара құқықтық көмек көрсету саласында алыс және жақын шетел мемлекеттерімен 17 халықаралық шартты ратификациялаған. Аталған халықаралық-

<sup>2</sup> Казахстан и Украина провели совместную спецоперацию в Киеве [Электрондық ресурс] – Айналыс режимі: <https://tengrinews.kz/crime/kazakhstan-ukraina-proveli-sovmestnuyu-spetsoperatsiyu-kieve-581141/> (жүгінген күні: 19.10.2025).

<sup>3</sup> Сол жерде.

<sup>4</sup> Қазақстан Республикасының Қылмыстық-процестік кодексі: 2014 ж. 4 шілдедегі № 231-V ҚРЗ [Электрондық ресурс] – Айналыс режимі: [https://adilet.zan.kz/kaz/docs/K1400000231/k14231\\_.htm](https://adilet.zan.kz/kaz/docs/K1400000231/k14231_.htm) (жүгінген күні: 16.10.2025).

<sup>5</sup> Қазақстан Республикасының халықаралық шарттары туралы: Қазақстан Республикасының 2005 ж. 30 мамырдағы № 54 Заңы [Электрондық ресурс] – Айналыс режимі: [https://adilet.zan.kz/kaz/docs/Z050000054\\_](https://adilet.zan.kz/kaz/docs/Z050000054_) (жүгінген күні: 16.10.2025).



құқықтық құжаттардың 15-і екіжақты сипатта болса, қалған 2-уі көпжақты халықаралық шарттар болып табылады.

11 желтоқсан 2025 жылы Иран Президенті Масуд Пезешкианның Қазақстанға жасаған ресми сапарының қорытындысы бойынша елдер сегіз үкіметаралық және ведомствоаралық құжатқа қол қойды, деп хабарлайды Ақорданың баспасөз қызметі<sup>6</sup>. Екі жақты құжаттардың ішінде құқық қорғау органдары үшін маңызды болып саналатын «Қазақстан Республикасы мен Иран Ислам Республикасы арасындағы қылмыстық істер бойынша өзара құқықтық көмек көрсету туралы шарт», - деп білеміз. Бұндай құқықтық көмек көрсету туралы халықаралық шарттар біздің зерттеу мақаламыздың өзектілігін арттыра түседі.

ҚР қылмыстық істер бойынша халықаралық құқықтық ынтымақтастықты нығайту мақсатында шет мемлекеттермен екіжақты шарттар жасасу жұмыстарын жандандыруы маңызды. Қазіргі шарттық-құқықтық база халықаралық өзара іс-қимылдың барлық бағытын толық қамти алмай отыр. Әсіресе, киберқылмыстардың қарқынды дамуы және трансұлттық қылмыс қатерінің артуы жағдайында шет мемлекеттермен тиімді құқықтық өзара көмек көрсету механизмдерін қалыптастыру еліміздің құқықтық қауіпсіздігін қамтамасыз етудің маңызды тетігі болып табылады.

ҚХР ішкі киберқылмыстарға қарсы күрес жүргізу мақсатында «киберегемдік» ұғымына негізделген ұлттық стратегия әзірлеген. Сол сияқты Еуропа мемлекеттері де әлеуметтік желілердің қызметін құқықтық тұрғыдан реттейтін заңдар қабылдап, киберқылмыстардың алдын алу шараларын өз деңгейінде жүзеге асыруда. Бұл үрдістер мемлекеттердің цифрлық даму саласында өз егемендігін айқындауға ұмтылып отырғанын көрсетеді [1].

Аталған елдердің тәжірибесіне сүйене отырып, Қазақстан Республикасы да цифрлық қауіпсіздікті қамтамасыз етуге ерекше назар аударып отыр. Осы мақсатта «Киберқалқан» тұжырымдамасы қабылданып, іске

асырылуда. Бүгінгі таңда Мемлекет басшысының тапсырмасы бойынша «Ұлттық суперкомпьютер орталығы» құрылып, тестілік режимде өз жұмысын бастады. Бұл орталық елімізге төнуі мүмкін киберқатерлердің алдын алу және киберқылмыстармен күрес бағытында маңызды рөл атқарады деп күтілуде.

Жалпы киберкеңістік ұғымына арнайы тоқталу маңызды. Қазіргі уақытта киберкеңістікте орын алатын процестерге дәстүрлі құқықтық нормалармен тиімді қарсы тұру мүмкін емес. Бұл жағдай киберкеңістіктің тек физикалық және виртуалды әлем арасындағы байланысты қамтамасыз етіп қана қоймай, сондай-ақ мемлекет егемендігіне, ішкі істеріне араласпау қағидасына және құқықтық нормалардың сақталуына қауіп төндіруімен байланысты [2].

Қазіргі уақытта халықаралық құқық аясында «кибершабуыл» немесе «киберсоғыс» ұғымдарына нақты және бірізді анықтама берілмеген. Осы мақалада жүргізілген зерттеу нәтижелеріне сүйене отырып, аталған ұғымдарға құқықтық тұрғыдан айқын анықтама беру, сондай-ақ қылмыстық және қылмыстық процестік заңнамаларына тиісті өзгерістер мен толықтырулар енгізу қажет деп санаймыз.

Қазақстан 2025 жылы «Еуропа Кеңесінің компьютерлік қылмыстар туралы конвенциясын» (Будапешт конвенциясы) ратификациялау үдерісіне кірісті. Бұл үдеріс 2023 жылдың сәуір айында Еуропа Кеңесінен ресми шақыру алынғаннан кейін басталды. Конвенцияны ратификациялау киберқылмыстарға қарсы күресте халықаралық ынтымақтастықтың құқықтық негізін қалыптастырып, компьютерлік жүйелерге рұқсатсыз қол жеткізу, деректерді ұстап қалу және компьютерлік жүйелердің құпиялылығы мен тұтастығына қарсы бағытталған өзге де әрекеттерге қарсы іс-қимылдың тиімділігін арттыруға мүмкіндік береді.

Геосаяси ахуалдың тұрақсыздығы және киберқауіпсіздік саласындағы халықаралық

<sup>6</sup> Казахстан и Иран подписали восемь документов по итогам переговоров лидеров [Электрондық ресурс] – Айналыс режимі: [https://ratel.kz/raw/kazakhstan\\_i\\_iran\\_podpisali\\_vosem\\_dokumentov\\_po\\_itogam\\_peregovorov\\_liderov](https://ratel.kz/raw/kazakhstan_i_iran_podpisali_vosem_dokumentov_po_itogam_peregovorov_liderov) (жүргізілген күні: 16.10.2025).



құқықтық нормалардың бірізді еместігі бұл мәселеге қатысты сыни тұрғыдан талдау жүргізудің өзектілігін айқындайды [3].

Фелисити Герри мен Кэтрин Мур өз зерттеуінде Экономикалық ынтымақтастық және даму ұйымы ұсынған тәсілге сүйене отырып, киберқұқық саласында бірыңғай жаһандық құрылымды қалыптастыруға бағытталған халықаралық конвенцияны әзірлеу қажеттігін атап өткен. Ғалымдардың пікірінше, киберқылмыстың трансұлттық сипаты оны халықаралық сот ынтымақтастығынсыз тиімді бақылауға мүмкіндік бермейді. Сондай-ақ, киберқылмысқа қарсы заңнаманы әзірлеу қымбатқа түсетіндігімен қатар, заманауи техникалық ресурстарды талап етеді деген қорытынды жасалған [4].

Аталған ғалымдардың тұжырымдармен ішінара келісе отырып, біздің ойымызша киберқылмыспен күрес саласында халықаралық соттан гөрі, қылмыстық қудалау жүргізу юрисдикциясына ие, құқықтық ықпалы бар әмбебап халықаралық ұйым құру орынды болар еді. Мұндай ұйымның БҰҰ-мен тікелей құқықтық байланыста әрекет етуі маңызды. Сонымен қатар киберкеңістіктегі қылмыстарға қарсы іс-қимыл халықаралық деңгейде біріздендіріліп, бірыңғай құқықтық мәртебесі бар халықаралық акт негізінде жүзеге асырылуы тиіс.

Будапешт конвенциясы (Киберқылмыс туралы конвенция) 2001 жылы 23 қарашада қабылданған (күшіне 2004 жылы 1 шілде де енді) ең алғашқы халықаралық құжат, алайда оның қатысушылары тек қана еуропа елдері. Сол үшін бұл конвенция өз тиімділігін толық бере алмайды. Қазақстан Республикасы аталған конвенцияның қатысушысы емес. Еліміздегі киберқылмыстардың артуы және кибершабуылдардың көпшілігі еуропа елдерінен басталатынын ескерсек біз осы конвенцияның қатысушысы атанып өзімізде ратификацилауымыз қажет. Сонда ғана бізге қарсы жасалған киберқауіптердің алдын алып және оларды жасаған адамдарды құрықтай аламыз.

Аталған конвенцияны талдасақ, онда киберқылмыскерлердің жауапқа тартылмай қалмайтындығы және бір-біріне жылдам

халықаралық құқықтық көмек көрсету туралы негізгі қағидалардың әрекет етуін аңғарамыз. Бірақ конвенцияда нақты «ұйымдасқан топ» ұғымы берілмеген. Онда тек қылмыстық әрекеттердің күрделілігі, алдын ала келісілген рөлдер, құралдарды заңсыз әзірлеу мен тарату (malware, botnet, exploits) сияқты сипаттар ұйымдасқан қылмыстық құрылымдарды айқындауға мүмкіндік беретін түсініктер ғана анықталған.

Бірақ біздің еліміз БҰҰ киберқылмыстылыққа қарсы конвенциясына 27 қазан 2025 жылы қол қойып қатысушысы атанды. Аталған маңызды іс – шара Ханой қаласында өтті, оған Қазақстан Республикасының Ішкі істер министрінің орынбасары, генерал-майор Бауыржан Аленов қатысты. Бұл конвенция шамамен 2027 жылы күшіне енеді деп күтілуде, себебі 40 мемлекет аталған конвенцияны өздерінде ратификациялау қажет.

Аталған конвенцияларға киберқылмыстардың қылмыстардың сыбайласып жасалатынын ескерсек киберқылмыстық ұйым, киберқылмыс саласындағы ұйымдасқан қылмыстық топ нысандарымен белгіленген өзгерістер мен толықтырулар енгізуді ұсынамын.

Соңғы уақытта «кибертерроризм» ұғымы кеңінен қолданыла бастады. Бұл ұғымның қалыптасуына террористік ұйымдарды қолдайтын интернет-платформалардың киберкеңістікте белсенді әрекет етуі себеп болды. Соңғы жылдары кейбір террористік құрылымдар жасанды интеллект технологияларын, оның ішінде дрондарды пайдалану арқылы террористік актілерді жүзеге асыруды жүйелі түрде қолдана бастағаны байқалады.

Шетелдік ғалымдар тобы өз зерттеулерінде терроризмге қарсы күресте киберқауіпсіздіктің өзектілігі технологиялар мен қоғам, саясат пен экономиканың қарқынды дамуының күнделікті өмірге әсер етуімен байланысты екені атап өтілген. Мақаланы талдау барысында аталған ғалымдар террористік ұйымдарға тиесілі веб-сайттардың саны айтарлықтай өскенін, олардың жүздеген сайт арқылы



өз жақтаушыларымен байланыс орнатып, кейбіреуін өз қатарына қосқанын атап өткен. Бұл сайттар киберкеңістікке анонимді шығу мүмкіндігін беріп, киберқылмыс жасауға жол ашады [3].

Тағы бір шетелдік авторлардың еңбегінде киберкеңістік ұғымына тоқталады. Олар киберкеңістікті мәдениеттің барлық салаларын біріктіретін орта ретінде сипаттаған [5]. Бұл ретте ғалымдардың пікірін қолдай келе, олардың БҰҰ-ның «Трансұлттық ұйымдасқан қылмысқа қарсы конвенциясы» халықаралық терроризмге қатысты баптарды да қамтитыны туралы тұжырымымен келісеміз. Бұл ретте ғалымдар кибертерроризммен күресуде міндетті халықаралық келісімді әзірлеу қажеттігін көрсетіп, киберқылмыстардың алдын алу мен кінәлілерді жауапқа тартуды маңызды фактор ретінде атайды [5].

**Қорытынды.** Қазіргі таңда киберкеңістікте жасалатын киберқылмыстардың түрі артып отыр. Ең кең таралғандары ретінде интернет-алаяқтық, кибербуллинг, кибертерроризм, хакерлік шабуылдар, интернет-шопинг арқылы есірткі саудасы және дербес деректерді ұрлау сияқты ашуы қиын қылмыстарды айтуға болады. Киберқылмыстарды тергеуде басты қиындық – киберқауіп төндірген ошақтарды дәл анықтау мен әшкерелеу болып табылады. Бұл мәселе, әсіресе киберқауіптер көбінесе шетелдік юрисдикциядан жүзеге асырылатындықтан, олардың уақытылы қолға түсуін қиындатады. Бұл мәселенің негізгі себебі – Қазақстанның көптеген мемлекеттермен құқықтық көмек көрсету туралы екіжақты халықаралық шарттың болмауымен сипатталады. Дегенмен ҚР ҚПК

558-бабының талаптарына сәйкес құқықтық немесе өзге де көмек өзара түсіністік қағидатында шет мемлекеттің сұрау салуы негізінде көрсетілуі немесе оны Қазақстан Республикасының орталық органы сұратуы мүмкін.

Алайда бұл норма халықаралық шарт мәртебесіне ие болмағандықтан, оның қолданылу ауқымы Қазақстан Республикасының шегінен аспайды. Сондықтан осындай құқықтық нормалар көпжақты халықаралық шартпен бекітіліп, оған қатысушы мемлекеттерді міндеттейтін деңгейде жүзеге асырылуы тиіс.

Мақалада қарастырғандай киберқылмыстармен бірлесіп күресетін халықаралық ұйым құрылуы қажет. Ол ұйым Біріккен Ұлттар Ұйымының юрисдикциясында немесе Орталық Азия елдерінің өңірлік киберқылмысқа қарсы күрес орталығы болса деген ұсыныс беріледі. Бұл орталықты осы идеяның бастамашысы ретінде біздің елде, Астана қаласында ашуға ұсыныс береміз.

Сонымен қоса киберқауіпсіздік туралы заң қабылдап, сол заңның шеңберінде киберқауіпсіздік гигиенасы ұғымын енгізіп, киберқауіптерге қарсы тұруда ең бастысы болып табылатын алдын алу шараларын негізгі қағидасы ретінде енгізуді дұрыс деп білеміз.

Елімізде қылмыстық сот ісін жүргізу саласында халықаралық ынтымақтастық аясын кеңетуді ұсынмыз. Әсіресе киберқылмыстармен күрсете халықаралық немесе мелекет аралық екіжақты құқықтық көмек көрсету туралы шарттарсыз трансұлттық киберқылмыстармен күресу құқықтық дәрменсіздікке алып келеді деп қорытындылаймыз.

#### **Пайдаланылған әдебиеттер тізімі:**

1. Balarabe, K. Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law / K. Balarabe // Computer Law & Security Review. – 2025. – Vol. 58. – 106180.
2. Gerry, F. A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human rights standards / F. Gerry, C. Moore // Computer Law & Security Review. – 2015. – Vol. 31. Issue 5. – Pp. 628-650.
3. Omelchuk, O.M. Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences / O.M. Omelchuk, et al. // Journal of Money Laundering Control. – 2022. – Vol. 25. Issue 3. – Pp. 700-716.



4. Khater, M.-H. International Perspective on Securing Cyberspace Against Terrorist Acts [Электрондық ресурс] / M.-H. Khater // International Journal of Sociotechnology and Knowledge Development. – 2023. – Vol. 15. Issue 1. – Айналыс режимі: <https://doi.org/10.4018/IJSKD.318706> (жүгінген күні: 19.10.2025).

5. Burrell, D.-N. Religious conflict, workplace inclusion, diversity in technical and cyber-driven organizations / D.-N. Burrell // International Journal of Sociotechnology and Knowledge Development (IJSKD). – 2021. – Vol. 13. Issue 3. – Pp. 17-32.

#### References:

1. Balarabe, K. Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law / K. Balarabe // Computer Law & Security Review. – 2025. – Vol. 58. – 106180.

2. Gerry, F. A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human rights standards / F. Gerry, C. Moore // Computer Law & Security Review. – 2015. – Vol. 31. Issue 5. – Pp. 628-650.

3. Omelchuk, O.M. Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences / O.M. Omelchuk, et al. // Journal of Money Laundering Control. – 2022. – Vol. 25. Issue 3. – Pp. 700-716.

4. Khater, M.-H. International Perspective on Securing Cyberspace Against Terrorist Acts [Электрондық ресурс] / M.-H. Khater // International Journal of Sociotechnology and Knowledge Development. – 2023. – Vol. 15. Issue 1. – Айналыс режимі: <https://doi.org/10.4018/IJSKD.318706> (жүгінген күні: 19.10.2025).

5. Burrell, D.-N. Religious conflict, workplace inclusion, diversity in technical and cyber-driven organizations / D.-N. Burrell // International Journal of Sociotechnology and Knowledge Development (IJSKD). – 2021. – Vol. 13. Issue 3. – Pp. 17-32.

#### **АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS**

**Дарын Азатович Ашимбаев** – Қонаев университетінің докторанты, заң ғылымдарының магистрі, e-mail: [ralym-algosh@mail.ru](mailto:ralym-algosh@mail.ru).

**Ашимбаев Дарын Азатович** – докторант университета Конаева, магистр юридических наук, e-mail: [ralym-algosh@mail.ru](mailto:ralym-algosh@mail.ru).

**Ashimbayev Daryn Azatovich** – Doctoral Student at Kunanayev University, Master of Laws, e-mail: [ralym-algosh@mail.ru](mailto:ralym-algosh@mail.ru).

**Галымжан Исатаевич Тогизбаев** – Қонаев университетінің «Қоғамдық қауіпсіздік» дайындық бағытының аға оқытушысы, заң ғылымдарының кандидаты, e-mail: [zhanikissatayev@gmail.com](mailto:zhanikissatayev@gmail.com).

**Тогизбаев Галымжан Исатаевич** – старший преподаватель направления подготовки «Общественная безопасность» университета Конаева, кандидат юридических наук, e-mail: [zhanikissatayev@gmail.com](mailto:zhanikissatayev@gmail.com).

**Togizbayev Galymzhan Isatayevich** – Senior Lecturer in the Department of Public Safety at Konaeva University, Candidate of Law, e-mail: [zhanikissatayev@gmail.com](mailto:zhanikissatayev@gmail.com).