

АҚПАРАТТЫҚ ҚОҒАМНЫҢ ЖАҒАНДАНУЫ ЖАҒДАЙЫНДА ҚЫЛМЫСҚА ҚАРСЫ КҮРЕСТІҢ ХАЛЫҚАРАЛЫҚ АСПЕКТІЛЕРІ

Асель Бостановна Шарипова

Заң ғылымдарының кандидаты, әл-Фараби атындағы ҚазҰУ қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедрасының қауымдастырылған профессоры; Алматы қ., Қазақстан Республикасы; e-mail: aselya.sharipova@mail.ru; ORCID iD: <https://orcid.org/0000-0003-0441-858>; Web of Science Researcher ID- FYA-1344-2022; Scopus Author ID: 57193676940

Айжан Арынқызы Арын¹

PhD докторы, әл-Фараби атындағы ҚазҰУ қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедрасының доценті м.а.; Алматы қ., Қазақстан Республикасы; e-mail: Aizhanmoon777@gmail.com; ORCID iD: <https://orcid.org/0000-0003-0605-9727>; Web of Science Researcher ID- A-6210-2015; Scopus Author ID: 57224292156

Гульдана Амангельдиевна Куаналиева

Заң ғылымдарының докторы, әл-Фараби атындағы ҚазҰУ кеден, қаржы және экологиялық құқық кафедрасының профессоры; Алматы қ., Қазақстан Республикасы; e-mail: kuanalieva.guldanakz@mail.ru; ORCID iD: <https://orcid.org/0000-0003-4634-8363>; Web of Science Researcher ID - A-5382-2015; Scopus Author ID: 55945226300

Аннотация. Бұл мақалада авторлар цифрлық кеңістіктегі қауіпсіздіктің халықаралық тәжірибесіне шолу жасады, себебі ақпараттық қауіпсіздік төнетін қатерлердің деңгейі күн сайын өсуде және ол көп көңіл бөлуді және талдауды қажет етеді. Авторлар технологиялардың қарқынды дамуы мен цифрлық қызметтердің кеңеюі әлеуметтік және экономикалық прогреске жаңа мүмкіндіктер ашып қана қоймай, сонымен қатар, халықаралық деңгейде киберқылмыс сияқты елеулі қауіптер туғызғанына назар аударады. Мақалада жаһандандудың әртүрлі аспектілері, мысалы, халықаралық нарықтардың интеграциясы, трансшекаралық өзара әрекеттестік және ақпарат алмасу, қылмысқа қарсы күрес үдерістерін едәуір күрделендіретін факторлар ретінде қарастырылады. Ерекше назар трансұлттық қылмыстық желілерді зерттеуге аударылады, олар өздерінің заңсыз әрекеттерін жаһандық деңгейде жүзеге асыру үшін ақпараттық технологиялардың артықшылықтарын белсенді түрде пайдаланады. Бұл мұндай қауіптермен күресте халықаралық ынтымақтастық пен күш-жігерді үйлестірудің түбегейлі жаңа тәсілдерін талап етеді. Авторлар жаһандану технологияларын қолданумен байланысты қылмыстарға қарсы күрес стратегияларын егжей-тегжейлі ұсынады, оның ішінде киберқауіпсіздік саласындағы заңнаманы жетілдіру, халықтың құқықтық сауаттылығын арттыруға бағытталған білім беру бастамаларын дамыту және инновациялық құқық қолдану әдістерін енгізу арқылы жүзеге асыруды қарастырады. Мақалада сондай-ақ Қазақстан Республикасында осы қауіптерге қарсы күреске бағытталған шаралар талданып, бұл салада халықаралық ынтымақтастық пен озық тәжірибе алмасудың маңыздылығы атап өтіледі. Қорытындысында ұлттық стратегияларды жаһанданған әлемге бейімдеудің қажеттілігі туралы тұжырымдар келтіріледі, бұл цифрлық ортада қылмыстың алдын алуға арналған интеграцияланған механизмдерді құруды, халықаралық құқық тәртібін нығайтуды және киберқылмысқа қарсы тұру үшін жаһандық стандарттарды әзірлеуді көздейді. Бұл мақала жаһандану және ақпараттық қоғам жағдайында қылмысқа қарсы күрестің құқықтық аспектілері жөніндегі пікірталасқа елеулі үлес қосып, осы күрделі міндеттерді шешуге кешенді көзқарасты ұсынады.

Түйінді сөздер: ақпараттық қоғам, қылмыстық құқық бұзушылықтар, киберқылмыс, цифрлық қызметтер, киберқауіп.

¹ Хат-хабарларға арналған автор

МЕЖДУНАРОДНЫЕ АСПЕКТЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Шарипова Асель Бостановна

Кандидат юридических наук, ассоциированный профессор кафедры уголовного права, уголовного процесса и криминалистики КазНУ имени аль-Фараби; г. Алматы, Республика Казахстан, e-mail: aselya.sharipova@mail.ru; ORCID iD: <https://orcid.org/0000-0003-0441-858>; Web of Science Researcher ID- FYA-1344-2022; Scopus Author ID: 57193676940

Арын Айжан Арынкызы

Доктор PhD, и.о. доцента кафедры уголовного права, уголовного процесса и криминалистики КазНУ имени аль-Фараби; г. Алматы, Республика Казахстан; e-mail: Aizhanmoon777@gmail.com; ORCID iD: <https://orcid.org/0000-0003-0605-9727>; Web of Science Researcher ID- A-6210-2015; Scopus Author ID: 57224292156

Куаналиева Гульдана Амангельдиевна

Доктор юридических наук, профессор кафедры таможенного, финансового и экологического права КазНУ им. аль-Фараби; г. Алматы, Республика Казахстан; e-mail: kuanalieva.guldanakz@mail.ru; ORCID iD: <https://orcid.org/-0000-0003-4634-8363>; Web of Science Researcher ID - A-5382-2015; Scopus Author ID: 55945226300

Аннотация. В данной статье авторы рассмотрели международный опыт безопасности в цифровом пространстве, которая требует большого внимания и анализа, поскольку возрастает уровень угроз информационной безопасности. Авторы акцентируют внимание на том, что стремительное развитие технологий и распространение цифровых услуг создали как новые возможности для социального и экономического прогресса, так и серьезные угрозы, включая киберпреступность на международном уровне. В статье рассматриваются различные аспекты глобализации, такие как интеграция международных рынков, трансграничное взаимодействие и обмен информацией, которые значительно усложняют процессы борьбы с преступностью. Особое внимание уделяется изучению транснациональных преступных сетей, которые активно используют преимущества информационных технологий для осуществления своей противоправной деятельности на глобальном уровне, что требует кардинально новых подходов к международному сотрудничеству и координации усилий в борьбе с такими угрозами. Авторы предлагают детализированные стратегии противодействия преступлениям, связанным с использованием технологий глобализации, в том числе через улучшение законодательства в сфере кибербезопасности, развитие образовательных инициатив, направленных на повышение правовой грамотности населения, и внедрение инновационных правоприменительных методов. В статье также анализируются меры, принимаемые в Республике Казахстан для борьбы с этими угрозами, подчеркивая важность международного сотрудничества и обмена передовым опытом в данной области. В заключение приводятся выводы о необходимости адаптации национальных стратегий к новым реалиям глобализованного мира, что предполагает создание интегрированных механизмов предотвращения преступлений в цифровой среде, укрепление международного правопорядка и разработку глобальных стандартов для противодействия киберпреступности. Данная статья представляет собой значимый вклад в дискуссию о правовых аспектах борьбы с преступностью в условиях глобализации и информационного общества, предлагая комплексный подход к решению этих сложных задач.

Ключевые слова: информационное общество, уголовные правонарушения, киберпреступность, цифровые услуги, киберугроза.

INTERNATIONAL ASPECTS OF FIGHTING CRIME IN THE CONTEXT OF GLOBALIZATION OF THE INFORMATION SOCIETY

Sharipova Assel Bostanovna

Candidate of Legal Sciences, Associate Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics of Al-Farabi Kazakh National University; Almaty c., Republic of Kazakhstan, e-mail: aselya.sharipova@mail.ru; ORCID iD: <https://orcid.org/0000-0003-0441-858>; Web of Science Researcher ID- FYA-1344-2022; Scopus Author ID: 57193676940

Aryn Aizhan Arynkyzy

PhD doctor, Acting Associate Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics of Al-Farabi Kazakh National University; Almaty c., Republic of Kazakhstan; e-mail: Aizhanmoon777@gmail.com; ORCID iD: <https://orcid.org/0000-0003-0605-9727>; Web of Science Researcher ID- A-6210-2015; Scopus Author ID: 57224292156

Kuanaliyeva Guldana Amangeldievna

Doctor of Legal Sciences, Professor of the Department of Customs, Fiscal and Environmental Law at Al-Farabi Kazakh National University; Almaty c., Republic of Kazakhstan; e-mail: kuanaliyeva.guldanakz@mail.ru; ORCID iD: <https://orcid.org/0000-0003-4634-8363>; Web of Science Researcher ID - A-5382-2015; Scopus Author ID: 55945226300

Abstract. *In this article, the authors reviewed international experience in security in the digital space, which requires great attention and analysis, as the level of information security threats increases. The authors emphasize that the rapid development of technology and the spread of digital services have created both new opportunities for social and economic progress and serious threats, including cybercrime at the international level. The article examines various aspects of globalization, such as the integration of international markets, cross-border interaction, and information exchange, which significantly complicate the processes of combating crime. Special attention is given to the study of transnational criminal networks that actively exploit the advantages of information technologies to carry out their illegal activities on a global scale, necessitating radically new approaches to international cooperation and coordination of efforts in addressing such threats. The authors propose detailed strategies for countering crimes associated with the use of globalization technologies, including improving cybersecurity legislation, developing educational initiatives aimed at increasing the legal literacy of the population, and implementing innovative law enforcement methods. The article also analyzes the measures being taken in the Republic of Kazakhstan to combat these threats, emphasizing the importance of international cooperation and the exchange of best practices in this field. In conclusion, the authors draw conclusions about the need to adapt national strategies to the new realities of a globalized world, which involves creating integrated mechanisms for preventing crimes in the digital environment, strengthening international law and order, and developing global standards to counter cybercrime. This article makes a significant contribution to the discussion on the legal aspects of combating crime in the context of globalization and the information society, offering a comprehensive approach to addressing these complex challenges.*

Keywords: *information society, criminal offenses, cybercrime, digital services, cyber threat.*

DOI: 10.52026/2788-5291_2025_80_1_147

Кіріспе

Жаһандану тақырыбы қазіргі әлеуметтік ғылымдарда белсенді түрде талқыланды және талқылау осы құбылыстың жағымды және жағымсыз жақтарын қамтиды.

Жаһандану экономикалық, саяси, әлеуметтік, мәдени, демографиялық, ақпараттық және басқа салаларда көрініс табады.

Жаһанданудың негізгі идеясын жаһандық деңгейде әмбебап алмасу және өзара әрекет-

тесу деп санауға болады. Экономиканың, мәдениеттің және этникалық топтардың өзара әрекеттесуі мен ықпалы әрқашан тән болғанымен, бұл процестердің жаһандық және динамикалық сипаты авиация және интернет сияқты заманауи байланыс, көлік және коммуникация технологияларының дамуымен ғана мүмкін болғандығын айта кету керек.

Осылайша, өмірдің барлық салаларында айтарлықтай дамуға ие болған жаһандық процесс ХХІ ғасырдағы әлемдік прогрестің негізгі элементіне айналды. Ол қазіргі заман тәртібін түбегейлі өзгертетін ақпараттық технологиялар төңірегінде шоғырланған ғылыми-техникалық эволюцияның жаңа кезеңіне байланысты.

Бұл ғылыми-техникалық революцияның бірегейлігі оның ақпараттық салаға әсер етуімен сипатталады, негізгі процестерге, мысалы, ақпаратты генерациялау және өңдеу, сақтау және жеткізу сияқты фундаменталды процестерді қамтумен, бұл экономика, саясат, мәдениет сияқты қоғамдық салаларда, сондай-ақ адамның ойлау қабілетінде елеулі өзгерістерге әкеледі, нәтижесінде жаңа қоғам түрінің – постиндустриалдық қоғамның қалыптасуына ықпал етеді [1, с. 121].

Бұрын атап өтілгендей, бұл тенденцияның оң жақтарымен қатар, теріс жақтары да бар. Атап айтқанда, инновациялық технологиялардың жаңа мүмкіндіктерін қолдану, батыс құндылықтары мен өмір салтын насихаттау қоғамда ақпараттық қақтығыстардың пайда болуына ықпал етеді. Сол сияқты, қазіргі заманғы интернет технологияларының мүмкіндіктері қылмыстың жаңа көріністерінің көзіне айналуда.

Цифрлық қызметтер мемлекеттік, білім беру және медициналық қызметтер туралы пікірді өзгертті. Инфрақұрылымы дамыған елдерде цифрлық технологияларды, мобильді байланысты және электрондық сервистерді белсенді енгізу жүзеге асырылып, олардың құнын төмендетуде. Алайда, цифрландырудың және технологиялық инновациялардың жылдам өсуі қосымша қауіптерді, соның ішінде қылмыстық әрекеттерді де тудырады. Қылмыскерлер өзгеріп жатқан жағдайларға тез бейімделіп, жаңа технологияларды игеріп, оларды заңсыз мақсаттарда пайдаланады. Қылмыстық әлем құқық қорғау органдарынан алда жүр, ал ғаламдық үдерістер қылмыспен күрес мәселелерін күрделендіреді.

Материалдар мен әдістер

Зерттеу барысында Біріккен Ұлттар Ұйымының есептері, Есірткіні бақылау

жөніндегі ұлттық комитетінің мәліметтері, сондай-ақ Интерпол және Халықаралық киберқауіпсіздік одағы (ICSPA) сияқты үкіметтік және халықаралық ұйымдардың материалдары сияқты ашық дереккөздерден алынған мәліметтер пайдаланылды. Қазақстан Республикасындағы киберқылмыстың динамикасын талдау үшін ішкі істер органдары ұсынған статистикалық ақпарат, сондай-ақ ақпараттандыру және байланыс саласындағы тіркелген қылмыстық құқық бұзушылықтар туралы деректер пайдаланылды. Зерттеудің әдістемелік негізі Қазақстан Республикасының нормативтік-құқықтық базасын талдауды, қылмысқа қарсы күрес жөніндегі халықаралық стратегияларды салыстырмалы талдауды, сондай-ақ киберқылмыс мәселелері бойынша ғылыми жарияланымдар мен есептердің мазмұндық талдауын қамтитын кешенді тәсіл болды. Зерттеу барысында трансұлттық қылмыстар мен киберқатерлердің өсу тенденцияларын зерттеуге, сондай-ақ осы құбылыстармен күресте қолданыстағы халықаралық шаралардың тиімділігін бағалауға ерекше назар аударылды. Қылмысқа қарсы күрес стратегияларының тиімділігін бағалау үшін ақпараттық технологиялардың дамуы мен қоғамдағы криминогендік факторлардың күшеюі арасындағы өзара байланысты анықтауға мүмкіндік беретін жүйелік талдау әдістері қолданылды. Сонымен қатар, киберқылмыстың жаһандық контексте даму перспективаларын бағалау үшін болжау әдістері қолданылды.

Талқылау. Нәтижелер

Цифрлық кеңістікте шекаралардың болмауына байланысты киберқылмыс халықаралық сипатқа ие болып, трансұлттық қылмыстарға айналуда. Халықаралық деңгейде қылмыстарды анықтаудағы келісілмеген тәсілдер мен байланыс желілерінің қолжетімділігі қылмыскерлерге ең қолайлы заңнамасы бар елдерді таңдауға және жазалаудың тәуекелдерін барынша азайтуға мүмкіндік береді. Бұл мәселені шешу мемлекеттік-жекеменшік әріптестікті, соның ішінде әртүрлі елдердің үкіметтері мен құқық қорғау органдарының ынтымақтастығын талап етеді. Электрондық дәлелдерді бағалау және олардың жасандылығымен күресу үшін әлемдік стандарттарды әзірлеу қажет, сонда соттар бүкіл әлемде тиімді жұмыс істей алады [2, 6- с. 7].

Цифрлық дәлелдемелер қазіргі заманғы киберқылмыстарды тергеуде негізгі рөл атқарады, бұл құқық қорғау органдарынан

деректерді жинау мен талдауға арналған арнайы әдістерді қолдануды талап етеді. Кей-си атап өткендей, цифрлық дәлелдерді өңдеу олардың түпнұсқалығын және тұтастығын қамтамасыз етуге бағытталған бірегей процестерді қамтиды, бұл сот ісін жүргізу үшін өте маңызды [3, p. 17].

Қазіргі заманғы коммуникациялық жүйелер ақпараттың киберкеңістікте қауіпсіз берілуін қамтамасыз етіп, оны барынша құпия және бірнеше минут ішінде әлемнің кез келген нүктесінен қолжетімді етеді, сонымен бірге ең аз із қалдырады. Осыған байланысты қазіргі заманғы технологиялар мен жаһандық ақпараттық жүйелер трансұлттық қылмыстық қызмет үшін бірегей мүмкіндіктер ұсынады және қылмыстық топтарға заңсыз операцияларды неғұрлым тиімді және табысты жүзеге асырудың жаңа тәсілдерін береді. Қылмыстық топтар өздерінің өнімдері мен қызметтерін бүкіл әлем бойынша таратады. Әлемдік заңсыз сауданың ең айқын мысалдарының бірі – есірткі заттарының заңсыз саудасы, ол жаһандық маңызға ие болып, негізгі халықаралық тауарға айналды. Біріккен Ұлттар Ұйымының Есірткіні бақылау жөніндегі ұлттық комитеті 2021 жылы жариялаған бағалау деректері бойынша, криптоарықтардағы есірткі саудасының жылдық жиынтық көлемі шамамен 315 миллион долларды құрайды, ал есірткі саудасының жалпы жылдық көлемі 600 миллиард долларға жетеді, бұл әлемдік сауданың 8%-на тең².

Тағы бір маңызды жайтқа назар аудару қажет. Адамзат тарихында тұңғыш рет ештеңе өндірмейтін және тек өзін ғана қайта құратын виртуалды экономика пайда болды. Экономика әрқашан өндірістік сипатта болған, ал соңғы 25-30 жылда пайда болған виртуалды экономика ештеңе өндірмек түгілі, оны жасай алмайды да. Мысалы, ақшаның әмбебап эквивалент ретіндегі функциясы тез арада өзінің маңызын жоғалта бастады, бұл адам қызметінің басқа түрлерін ынталандырмайды. Ақша өздері сауда объектісіне айналды. 2022 жылғы сәуірде жарияланған есепке сәйкес, осы жылдың сәуір айында әлемдегі валюта саудасының көлемі жаңа рекордқа жетіп, тәулігіне 7,5 триллион долларды құрады, бұл 2019 жылмен салыстырғанда 14%-ға артқан. Сондықтан банктерге жасалатын хакерлік шабуылдардың ақша қаражатын алып кету мақсатын-

да банктік операцияларға қол жеткізу үшін жиілеуі таңқаларлық емес³.

Осылайша, әлемдік деңгейде компьютерлік технологиялардың дамуы және қаржы операцияларының күрделілігінің артуы ең алдымен халықаралық қаржы транзакцияларының көлемін, жылдамдығын және құпиялылығын арттыру үшін жағдай жасауға әсер етті. Бұл өз кезегінде трансұлттық ұйымдасқан қылмыстың мүмкіндіктерін кеңейтіп, оны анықтау мен алдын алу ықтималдығын төмендетті. Енді қылмыстық топтар заңсыз қызметтен түскен кірістерді еш қиындықсыз заңдастыра алады.

Сарапшылардың пікірінше, бұл процесс қара нарықта есірткі саудасынан басқа, қару-жарақ және адам ағзаларын сатумен қатар, ақшаны жылыстату операциялары және трансұлттық қылмыстық топтардың басқа да қылмыстық қызмет түрлерін жандандыруға ықпал етті. Бұл қылмыстық топтар арасындағы байланыстарды жеңілдетіп, әлемдік деңгейде ұйымдасқан қылмыстың өсуіне ықпал етіп, қылмысты мемлекеттік деңгейде бақылауды әлдеқайда қиындатып жіберді дегенді білдіреді.

Жекелеген мемлекеттер деңгейінде жағдай аса қолайлы емес, мысалы, 2018 жылдан 2021 жылға дейінгі кезеңде Қазақстан Республикасында ақпараттандыру және байланыс саласында 364 қылмыстық құқық бұзушылық және 43911 интернет-алаяқтық жасалған. Келтірілген статистика жағдайды толық сипаттай алмайды, өйткені азаматтар ұсақ алаяқтық әрекеттердің құрбаны болған жағдайда, бұл туралы құқық қорғау органдарына жүгінуді жүйке мен уақытты босқа кетіру деп санап, бас тартуы мүмкін. Қылмыскерлер азаматтардың қылмысқа немқұрайлы қарауын пайдаланып, ұсақ сомаларға көбірек алаяқтық жасауда [4].

Жоғарыда келтірілген мәліметтерге сәйкес, ең көп тіркелген қылмыстық құқық бұзушылықтар интернет-алаяқтықпен байланысты істерде байқалады. Жалпы алғанда, Қазақстан Республикасы Қылмыстық кодексінің 7-тарауында көзделген қылмыстық құқық бұзушылықтар бойынша жыл сайын интернет-алаяқтық істеріне қарағанда әлдеқайда аз фактілер тіркеледі. Тіркелген қылмыстық істердің сандық қатынасының айтарлықтай айырмашылығын ескере отырып, тереңірек зерттеу үшін және талдауды

² Международнoй комитет по контролю над наркотиками (МККН). - Доклад за 2023 г. [Электронный ресурс]: // https://unis.unvienna.org/unis/uploads/documents/2024-INCB/2325540R_INCB_Annual_Report.pdf (дата обращения: 10.07.2024).

³ Triennial Central Bank Survey of foreign exchange and Over-the-counter (OTC) derivatives markets in 2022 // <https://www.bis.org/statistics/rpfx22.htm> (date of reference: 11.07.2024).

жеңілдету мақсатында, Қазақстан Республикасы Қылмыстық кодексінің 7-тарауында көзделген қылмыстық құқық бұзушылықтарды интернет-алаяқтықтан бөлек талдау орынды болады. Сонымен, киберқылмыстың динамикасын зерттей отырып, Қазақстан Республикасы Қылмыстық кодексінің 7-тарауында көзделген ең кең таралған қылмыстық құқық бұзушылықтардың үштігіне мыналар кіретінін атап өткен жөн:

1. Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу (ҚР ҚК 205-бабы), бұл қылмыстық құқық бұзушылықтардың жалпы санының 56%-ын құрайды;

2. Ақпаратты құқыққа сыйымсыз иеленіп алу (ҚР ҚК 208-бабы), оның тіркелу пайызы 12%-ды құрайды;

3. Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру (ҚР ҚК 206-бабы), тіркелу пайызы 10%-ды құрайды.

Интернет-алаяқтықтардың тіркелуінің өсуін бақылап, бір жағынан, осы әрекеттердің алдын алу және профилактика шараларының жеткіліксіздігі мен тиімсіздігі туралы қорытынды жасауға болады; екінші жағынан, азаматтардың сенгіштігі мен құқықтық сауатсыздығы, алаяқтық мобильді қосымшалардың бақылаусыз таралуы, қаржылық интернет-пирамидалардың ашық жарнамасы, төлем интернет-платформаларының қолданыстағы киберқорғау шараларының тиімсіздігі, киберқауіпсіздік саласындағы мамандардың тапшылығы және басқа да мәселелер туралы айтуға болады.

Халықаралық технологиялық компаниялардың көшбасшылары мемлекеттер мен халықаралық ұйымдарды жаһандық киберкеңістікті басқаруға белсенді қатысуға шақырады. Соңғы жылдары қаскөйлер тек компаниялар мен жеке тұлғаларға ғана емес, сонымен қатар қоғамдық маңызы бар нысандарға да кибершабуылдар жасауды жиілетті. «Интернет-офшорлармен» күресте бірлескен күш-жігерді қажет етеді: қылмыскерлер басқа домендерге ауысқан кезде де жауапкершіліктен құтыла алмайтынын түсінуі керек, өйткені олар халықаралық нормаларды бұзады. Сондықтан киберқылмыспен күресуге арналған халықаралық ережелер мен стандарттарды мүмкіндігінше тезірек әзірлеу және осы қызметті реттеуге жауапты халықаралық орган құру қажет. Қолданыстағы тәжірибе негізінде ақпараттық кеңістіктегі үрдістердің дамуын болжау

және жаңа қауіптерді анықтау, сондай-ақ киберқауіпсіздікті қамтамасыз етудің бірыңғай жүйесін әзірлеп, енгізу қажет.

Броджерст пен Чанг Азиядағы киберқылмыстың өсуі тығыз халықаралық ынтымақтастықты қажет ететінін атап көрсетеді. Олар аймаққа тән мәліметтерді құқықтық қорғаудың әлсіздігі және киберинфрақұрылымның жоғары осалдығы сияқты ерекше проблемаларды бөліп көрсетеді, бұл қылмыскерлерді қудалауды қиындатып, алдын алу шараларының тиімділігін төмендетеді [5, р. 78].

Киберқылмысқа қатысты құқықтық аспектілер бірыңғай халықаралық стандарттар мен тетіктерді әзірлеуді талап етеді. Клоуф құқықтық жүйелердің әртүрлілігіне қарамастан, қылмыскерлерді қудалау тиімділігін арттыру үшін елдерге киберқылмысқа қарсы күрестің бірыңғай қағидаларын қалыптастыру қажет екенін атап көрсетеді [6, р. 57].

Ақпараттық қоғамдағы қылмыспен халықаралық күрес ғаламдық келісімдер мен конвенцияларсыз мүмкін емес, олар құқықтық шектерді белгілеп, елдер арасындағы ынтымақтастықты қамтамасыз етеді. Осы саладағы негізгі халықаралық конвенциялардың бірі – 2001 жылы Еуропа Кеңесіне мүше елдер қабылдаған Будапешт киберқылмыс туралы Конвенциясы. Бұл конвенция киберкеңістіктегі қылмыстармен күресуге бағытталған алғашқы құжат болып табылады және елдерге трансұлттық қылмыстарға жедел әрекет етуге мүмкіндік беретін ақпарат алмасу қағидаларын белгілейді. Ол сонымен қатар қатысушы мемлекеттерді киберқауіпсіздік саласындағы халықаралық стандарттарға сәйкес өз заңнамаларын үйлестіруге шақырады және киберқылмыскерлерді тиімді қудалауға ықпал етеді. Осы конвенцияның арқасында елдердің құқық қорғау органдары тергеу жүргізу үшін бір-біріне көмек сұрап жүгіне алады, бұл цифрлық ортадағы қылмыспен күрестің тиімділігін айтарлықтай арттырады.

Киберқылмыстардың қаупі Біріккен Ұлттар Ұйымын да айналып өтпеді, 2021 жылғы 29 маусымда қылмыстық мақсатта ақпараттық-коммуникациялық технологияларды пайдалануға қарсы күрес туралы Конвенция қабылданды⁴.

Конвенцияда оның мақсаттары мен міндеттері көрсетілген, әрбір бабы ақпараттық-құқықтық салада жасалатын қылмыстардың жекелеген түрлерін сипаттап, қылмыскерлерді жауапкершілікке тартуға

⁴ *Всестороннее исследование проблемы киберпреступности. - Организация Объединенных Наций. - Нью-Йорк, 2013. - [Электронный ресурс] – Access Mode: https://www.unodc.org/documents/orga-nized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 11.07.2024).*

шақырады және олардың әрекеттері үшін жазаның бұлтартпастығын қамтамасыз етеді⁵.

Киберқылмыспен күрес жөніндегі халықаралық ұйымдардың міндеттері: интернет салаларындағы қылмысқа жатқызылатын іс-әрекеттерге қатысты бірыңғай халықаралық стандарттарды әзірлеу; бірыңғай терминология мен ұғымдық аппаратты қалыптастыру; ұлттық деңгейде тиісті қылмыстық-құқықтық нормаларды қабылдауда кеңес беру көмегін көрсету.

Сонымен қатар, киберқауіптерге қарсы халықаралық көпжақты серіктестік (IMPACT) бар, ол ақпараттық-телекоммуникациялық технологиялар мәселелері бойынша БҰҰ-ның мамандандырылған мекемесі – Халықаралық электрбайланыс одағының (ХЭО) киберқауіпсіздік саласындағы атқарушы органы болып табылады.

IMPACT – бұл ақпараттық қауіпсіздікті қорғау тиімділігін арттыру мақсатында үкіметтерді, академиялық институттарды және саланың жетекші сарапшыларын біріктіретін киберқауіптерге қарсы күрестегі бірегей халықаралық одақ. IMPACT мүшелері киберқауіптерге қарсы тиімді күресу үшін мамандандырылған білімге, ресурстарға және құралдарға қол жеткізіп, БҰҰ ұйымдарына олардың ақпараттық-телекоммуникациялық инфрақұрылымын қорғауда қолдау көрсетеді.

Халықаралық киберқауіпсіздік одағы (ICSPA) киберқылмыспен халықаралық деңгейде күресу және осы салада тәжірибе алмасу мақсатында үкіметтер, халықаралық бизнес және құқық қорғау органдары, соның ішінде Еурополдың күш-жігерін біріктіреді.

Интерпол, ең ірі халықаралық полиция ұйымы ретінде, ақпараттық-телекоммуникациялық технологияларды пайдалану арқылы жасалатын трансшекаралық қылмыстарды анықтау және әшкерелеу үшін мүше мемлекеттердің құқық қорғау органдарымен белсенді түрде ынтымақтасады. Сингапурдағы Интерполдың Халықаралық инновациялар орталығы киберқылмыспен күресу үшін жаңа қызметтер мен стратегияларды әзірлеп, іске асырады [7, с. 147].

Интерпол, IMPACT және ICSPA сияқты халықаралық ұйымдар киберкеңістікте бірыңғай стандарттар мен ережелерді әзірлеуге бағытталған ынтымақтастық механизмдерін белсенді түрде әзірлеуде. Олардың қызметінің маңызды аспектілерінің бірі халықаралық құқықтық алаңды қалып-

тастыру болып табылады, мұнда:

Интернет саласындағы қылмысқа жатқызылатын әрекеттердің критерийлері анықталады.

Елдер арасындағы үйлесімділікті қамтамасыз ететін бірыңғай терминология мен ұғымдар әзірленеді.

Ұлттық қылмыстық-құқықтық нормаларды енгізу барысында кеңес беру көмегі көрсетіледі.

Қорытынды

Мемлекет ұлттық құқықтық жүйеде қолданатын халықаралық нормалар мен стандарттар Қазақстан Республикасында киберқылмысқа қарсы күресті құқықтық реттеу шарттарының бірі болып табылатындығын атап өткен жөн. Әлемдік қоғамдастық деңгейінде киберқылмыспен күрестің тиімді тетіктері апробациядан өтті. Мысалы, 2001 жылғы 23 қарашада Будапешт қаласында қол қойылған Еуропалық Одаққа мүше елдер арасында жасалған Компьютерлік қылмыстар туралы (киберқылмыс) Еуропалық конвенцияға сәйкес, олардың аумақтарында мәліметтер алу үшін жеңілдетілген механизм қолданылады. Ал Орталық Азия елдерінің аумақтарында халықаралық тапсырмалар Минск және Кишинев конвенциялары арқылы орындалады.

Ақпараттық қоғам жағдайында қылмыспен тиімді күресу үшін дүниежүзі елдері тәжірибе алмасып, өздерінің киберқауіпсіздігін нығайту мақсатында үздік тәжірибелерді қолданады. Осы тұрғыда киберқылмыспен күресу стратегиялары назар аударуға лайық бірқатар елдердің тәжірибесі ерекше қызығушылық тудырады. Мысалы, Ұлыбритания киберқауіпсіздікке кешенді тәсіл енгізіп, киберқылмыспен күресуде күш-жігерді үйлестіру және ұлттық инфрақұрылымды қорғау үшін Ұлттық киберқауіпсіздік орталығын (NCSC) құрды. Германия өз кезегінде нормативтік-құқықтық актілерін нығайтып, құқық қорғау органдарының киберқауіптерге қарсы тұру мүмкіндіктерін едәуір кеңейтті.

Осы елдердің халықаралық тәжірибесі киберқылмыспен күресудің тиімділігін арттыруға бағытталған «Қазақстанның киберқалқаны» («Кибершит Казахстана») тұжырымдамасын әзірлеу кезінде ескерілді. Бұл тәжірибені қолдану Қазақстан Республикасына киберқорғаудың озық әдістерін белсенді енгізуге және киберкеңістіктегі қылмыстардың алдын алудың жаңа тәсіл-

⁵ Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях от 29.06.2021г. - [Электронный ресурс] – Режим доступа: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 20.07.2024).

дерін әзірлеуге мүмкіндік береді. Халықаралық ауқымдағы маңыздылығын қарастыратын болсақ, киберқылмыспен күресудің негізгі қағидаттары мен бағыттары, алдын алу және тергеу мақсаттары мен міндеттері бүкіл әлемде бірдей, бірақ әр мемлекетте заңнама мен құқықтық жүйеге сәйкес өзіне тән ерекшеліктер бар.

Қазақстан Республикасындағы ақпараттық кеңістікте құқықтар мен заңды мүдделерді қорғау саласындағы заңнама Қазақстан Республикасының Қылмыстық кодексінің 7-тарауын, сондай-ақ 2017 жылғы 30 маусымдағы № 407 Қазақстан Республикасы Үкіметінің «Киберқауіпсіздік тұжырымдамасын бекіту туралы» қаулысын қамтиды.

Дегенмен, киберқылмыскерлер қаншалықты жағымсыз естілсе де, бір қадам алда, сондықтан халықаралық ұйымдар мен барлық мемлекеттер үйлесімді жұмыс істеп, келесі мәселелерді шешіп, назарға алуы қажет:

1. Құқықтық реттеуге виртуалды кеңістіктегі қоғамдық қатынастарды енгізу ұсынылады.

2. Интернет-пирамидалар және экстремистік немесе заңнамаға қайшы келетін басқа да қауіпті контенті бар сайттарды жабу үшін интернетті бақылау қажет.

3. Ішкі істер органдарының басқа құқық қорғау және мемлекеттік органдармен, сондай-ақ коммерциялық ұйымдармен алаяқтық сайттар мен колл-орталықтарды жедел жабу мақсатында ынтымақтастық механизмдерін әзірлеу.

4. Шетелдік IP-мекен-жайлармен тіркелуден бас тартуды және пайдаланушыларды сәйкестендіру үшін дауыс биометриясын енгізуді қоса алғанда, IP-телефония қызметтерін ұсыну туралы заңнаманы қатаңдатуды қарастыру.

5. Сот және тергеу практикасын талдау негізінде компьютерлік ақпарат және ақпараттық-телекоммуникациялық технологиялар саласындағы қылмыстарды анықтау және тергеу бойынша әдістемелік ұсынымдар әзірлеу.

6. Компьютерлік ақпарат саласындағы қылмыстарды жасау әдістері және олардан қорғану тәсілдері туралы қоғамды бұқара-

лық ақпарат құралдары және білім беру компаниялары арқылы хабардар ету.

7. Киберқылмыспен тиімді күресу үшін ішкі істер органдарына профильді білімі бар адамдарды қызметке тартып, олардың қайта даярлануын қамтамасыз ету.

8. Киберқылмыспен күресу үшін халықаралық ынтымақтастық механизмдерін әзірлеп, оларды тиісті құжаттарда бекіту.

9. Коммерциялық ұйымдар мен IT-компаниялардың көмегімен ақпарат беру арналары мен деректер базаларын рұқсатсыз қол жеткізуден қорғау жүйесін жетілдіру.

10. Жеке деректерді заңсыз жариялау немесе иесінің келісімінсіз пайдалану үшін, әсіресе ақпарат қызметтік міндеттерін атқару барысында берілген немесе алынған жағдайда, қатаң жаза тағайындау туралы ұсыныстарды қарастыру.

11. Ұйымдасқан қылмыс, экстремизм, есірткі, порнография және жыныстық қанау сияқты компьютерлік ақпарат пен ақпараттық технологияларға қатысты қылмыстарға қарсы күресті күшейту.

12. Ата-аналарды балаларға қолжетімді контентке қырағылық танытуға және оларды зиянды ақпараттан қорғауға ынталандыру.

13. Киберқауіпсіздікті қамтамасыз етудің тиімділігін арттыру мақсатында киберқылмысты зерттеуді жандандыру.

Осылайша, бұл мәселені шешу көптеген факторларға, соның ішінде әрбір жекелеген мемлекеттің қатысуына байланысты. Себебі, бұл мемлекеттердің технологиялық дамуы мен осы саладағы заңнамалық базасының деңгейі әртүрлі, және олардың арасындағы ақпарат алмасу, сөзсіз, қажетті әсер береді, дегенмен, киберқылмыс сияқты құқыққа қайшы құбылыстың түп-тамырын жоя алмайды.

Сондай-ақ, киберқауіптерге тиімді қарсы тұру үшін мемлекеттердің құқық қорғау органдарының жұмысын жетілдіру және ұлттық деңгейде барлық мүдделі тараптардың, соның ішінде кәсіпкерлік қауымдастық, қоғамдық ұйымдар, зерттеу мекемелері және азаматтардың күш-жігерін біріктіру қажет.

Авторлардың мақаладағы үлесі

Шарипова А.Б. - кіріспе, талқылау және нәтижелер, библиографиялық қайнар көздерді талдау.

Арын А.А. - материалдар мен әдістер, қорытынды, әдебиеттерді рәсімдеу, транслитерация.

Куаналиева Г.А. - талқылау, қорытынды.

ӘДЕБИЕТТЕР

1. Чешков М. Глобализация: сущность, нынешняя фаза, перспективы // Проблемы глобализации. - М., 1999. - Т.4. - №4. - С. 121-127.
2. Долгова А. И. Преступность, ее организованность и криминальное общество. - М.: Российская криминологическая ассоциация, 2003. - 572 с.
3. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd ed.- UK: Elsevier Academic Press, 2011. - 807 p.
4. Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения // Российско-азиатский правовой журнал. - М., 2022. - [Электронный ресурс] // <https://cyberleninka.ru/article/n/osobennosti-dinamiki-kiberprestupnosti-v-respublike-kazahstan-i-ee-vliyanie-na-voprosy-eyo-preduprezhdeniya> (дата обращения: 15.07.2024).
5. Broadhurst, R., & Chang, L. *Cybercrime in Asia: Trends and Challenges*. - London: Palgrave Macmillan, 2013. - 458 p.
6. Clough, J. *Principles of Cybercrime*. - Cambridge: Cambridge University Press, 2015. - 430 p.
7. Мороз Н.О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. - 2011. - № 14. - С. 147.

REFERENCES

1. Cheshkov M. *Globalizacija: sushhnost', nyneshnjaja faza, perspektivy* // *Problemy globalizacii*. - M., 1999. - T.4. - №4. - S. 121-127.
2. Dolgova A. I. *Prestupnost', ee organizovannost' i kriminal'noe obshhestvo*. - M.: Rossijskaja kriminologicheskaja associacija, 2003. - 572 s.
3. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd ed.- UK: Elsevier Academic Press, 2011. - 807 r.
4. Muhamedzhanova A.D. *Osobennosti dinamiki kiberprestupnosti v Respublike Kazahstan i ee vlijanie na voprosy ejo preduprezhdenija* // *Rossijsko-aziatskij pravovoj zhurnal*. - M., 2022. - [Elektronnyj resurs] // <https://cyberleninka.ru/article/n/osobennosti-dinamiki-kiberprestupnosti-v-respublike-kazahstan-i-ee-vliyanie-na-voprosy-eyo-preduprezhdeniya> (data obrashhenija: 15.07.2024).
5. Broadhurst, R., & Chang, L. *Cybercrime in Asia: Trends and Challenges*. - London: Palgrave Macmillan, 2013. - 458 r.
6. Clough, J. *Principles of Cybercrime*. - Cambridge: Cambridge University Press, 2015. - 430 p.
7. Moroz N.O. *Dejatel'nost' Interpola po koordinacii sotrudnichestva v bor'be s prestupnost'ju v sfere vysokih tehnologij* // *Vestnik Polockogo gosudarstvennogo universiteta. Serija D: Jekonomicheskie i juridicheskie nauki*. - 2011. - № 14. - S. 147.