Мақала туралы мәлімет / Содержание

«ЖАСТАР ЖӘНЕ ҒЫЛЫМ: БҮГІНІ МЕН БОЛАШАҒЫ» жас ғалымдардың халықаралық ғылыми-тәжірибелік конференция материалдар жинағы

Сборник материалов Международной научно-практической конференции молодых ученых «МОЛОДЕЖЬ И НАУКА: НАСТОЯЩЕЕ И БУДУЩЕЕ»

The collection of materials from the International Scientific and Practical Conference of Young Scientists «YOUTH AND SCIENCE: PRESENT AND FUTURE»

Жинақ	IV, Атырау, 8/04/2026, 2026 ж.
ISBN	978-601-262-638-4
Секция	СЕКЦИЯ IV. ЭКОНОМИКА ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ / ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ Секция IV.II. Цифрлық технологиялар жағдайындағы құқықтық жүйені дамыту және құқық қолдану тәжірибесі / Развитие правовой системы и практика правоприменения в условиях цифровых технологий
Жинақтағы рет нөмірі	№ 086
Мазмұндағы беті	428
Жарияланған беттері	428-432
Автор(лар)	Назарбек Думан Назарбекұлы
Мақала атауы	ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫНЫҢ КИБЕРҚЫЛМЫСТАРДЫ АНЫҚТАУ, АШУ ЖӘНЕ ТЕРГЕУ ЖӨНІНДЕГІ ҚЫЗМЕТІН ҚҰҚЫҚТЫҚ РЕТТЕУДІ ЖЕТІЛДІРУ
Мазмұндағы жазылуы	Назарбек Д.Н., Бегалиев Е.Н. ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫНЫҢ КИБЕРҚЫЛМЫСТАРДЫ АНЫҚТАУ, АШУ ЖӘНЕ ТЕРГЕУ ЖӨНІНДЕГІ ҚЫЗМЕТІН ҚҰҚЫҚТЫҚ РЕТТЕУДІ ЖЕТІЛДІРУ

Ескерту: бет нөмірлері жинақтың соңындағы «МАЗМҰНЫ» бөліміндегі жарияланған беттерге сәйкес берілді.

ӘОК 343.98:004.056

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫНЫҢ КИБЕРҚЫЛМЫСТАРДЫ АНЫҚТАУ, АШУ ЖӘНЕ ТЕРГЕУ ЖӨНІНДЕГІ ҚЫЗМЕТІН ҚҰҚЫҚТЫҚ РЕТТЕУДІ ЖЕТІЛДІРУ»

Назарбек Думан Назарбекұлы
duman_01@bk.ru
«Құқықтану» білім бағдарламасының 1 курс магистранты
Х.Досмұхамедов атындағы Атырау университеті, Атырау қ., Қазақстан Республикасы
Ғылыми жетекшісі, з.ғ.д., профессор – Бегалиев Е.Н.

Мақалада Қазақстан Республикасының құқық қорғау органдарының киберқылмыстарды анықтау, ашу және тергеу жөніндегі қызметін құқықтық реттеудің өзекті мәселелері зерттеледі. Киберқылмыстардың ұғымы, жіктелуі, халықаралық стандарттары талданады. Құқық қорғау органдарының құзыреті, киберқылмыстарды анықтау және тергеудің ерекшеліктері, электрондық дәлелдемелермен жұмыс істеу мәселелері қарастырылады. Ерекше назар процестік кепілдіктерге, халықаралық ынтымақтастыққа, жаңа технологияларды қолдануға аударылады. Автор қолданыстағы заңнаманың кемшіліктерін анықтайды және құқықтық реттеуді жетілдірудің кешенді бағдарламасын ұсынады. Мамандандырылған құрылымдарды құру, мамандарды даярлау, жеке сектормен ынтымақтастық, қоғамдық хабардарлықты арттыру маңызды бағыттар ретінде қарастырылады.

Ақпараттық технологиялардың қарқынды дамуы және цифрландыру процестері қоғамдық қатынастардың барлық салаларына енуде. Киберкеңістіктің кеңеюі жаңа мүмкіндіктер ашумен қатар, қылмыстық іс-әрекеттердің жаңа түрлерінің пайда болуына әкеп соқты. Киберқылмыстар қазіргі заманғы қоғамға төнетін ең қауіпті қатерлердің бірі болып табылады және ұлттық қауіпсіздікке нақты қауіп төндіреді. Қазақстан Республикасының құқық қорғау органдары киберқылмыстармен күресте маңызды рөл атқарады, алайда олардың қызметін құқықтық реттеу жедел өзгеріп жатқан киберқауіптерге толық жауап бере алмайды.

Киберқылмыстардың ұғымы мен жіктелуі заңнамада нақты айқындалуын қажет етеді. Киберқылмыстар дегеніміз – ақпараттық-коммуникациялық технологияларды пайдалана отырып немесе ақпараттық жүйелерге, компьютерлік деректерге қарсы жасалатын қылмыстық іс-әрекеттер [1]. Киберқылмыстардың спектрі өте кең: компьютерлік жүйелерге заңсыз қол жеткізу, деректерді бұзу және жою, зиянды бағдарламаларды тарату, фишинг, киберхұқшылық, киберлық қорқыту, балалар порнографиясын тарату, ақпараттық-телекоммуникациялық желілер арқылы террористік және экстремистік идеологияны насихаттау.

Қазақстан Республикасының Қылмыстық кодексі киберқылмыстардың бірқатар құрамдарын қарастырады. Компьютерлік ақпаратқа заңсыз қол жеткізу (227-бап), компьютерлік жүйелердің, телекоммуникациялық желілердің жұмысын бұзу (228-бап), зиянды бағдарламалық қамтамасыз етуді жасау және тарату (229-бап) киберқылмыстардың негізгі құрамдары болып табылады [2]. Алайда қолданыстағы қылмыстық заңнама киберқылмыстардың барлық түрлерін толық қамтымайды және жаңа қауіптерге жедел жауап бере алмайды.Киберқылмыстардың халықаралық сипаты олармен күресте халықаралық ынтымақтастықты қажет етеді. Киберқылмыстылық туралы Будапешт конвенциясы киберқылмыстармен күрестің халықаралық стандарттарын белгілейді және мемлекеттердің өзара іс-қимыл тетіктерін айқындайды [3]. Қазақстан Республикасы Будапешт конвенциясына

қосылмаса да, киберқылмыстылықпен күресте халықаралық ынтымақтастықты белсенді дамытуда. ТМД аясында, ШЫҰ форматында, Интерпол арқылы ынтымақтастық жүзеге асырылады.Құқық қорғау органдарының киберқылмыстармен күрестегі құзыреті бірнеше ведомстволар арасында бөлінген. Ұлттық қауіпсіздік комитеті ұлттық қауіпсіздікке қауіп төндіретін киберқылмыстарды анықтаумен айналысады. Ішкі істер органдары жалпы қылмыстық сипаттағы киберқылмыстарды тергейді. Қаржы полициясы экономикалық және қаржылық киберқылмыстарды қарайды [4]. Құзыреттердің бөлінуі кейде қайталануға, үйлестіру проблемаларына, тиімділіктің төмендеуіне әкеледі.Киберқылмыстарды анықтаудың ерекшеліктері арнайы техникалық құралдар мен әдістерді қолдануды қажет етеді. Киберқылмыстарды анықтау үшін желілік трафикті мониторингтеу, жүйелік журналдарды талдау, зиянды бағдарламаларды анықтау, цифрлық іздерді іздестіру қажет [5]. Құқық қорғау органдары заманауи техникалық құралдармен, бағдарламалық қамтамасыз етумен, дайындалған мамандармен жеткілікті түрде қамтамасыз етілмеген. Техникалық базаның әлсіздігі киберқылмыстарды анықтау мүмкіндіктерін шектейді.

Киберқылмыстарды тергеудің процестік ерекшеліктері қолданыстағы қылмыстық-процестік заңнамада толық ескерілмеген. Электрондық дәлелдемелерді жинау, сақтау, зерттеу арнайы процедураларды қажет етеді. Электрондық деректердің өзгермелі сипаты, оларды оңай жоюға немесе өзгертуге болатындығы дәлелдемелерді бекіту жөніндегі ерекше талаптарды қояды [6]. Қазақстан Республикасының Қылмыстық-процестік кодексі электрондық дәлелдемелермен жұмыс істеудің кейбір ережелерін қарастырады, алайда олар жеткіліксіз және нақтылауды қажет етеді.

Киберкеңістікте тінту жүргізу дәстүрлі тінтуден елеулі ерекшеленеді. Электрондық ақпарат көздерінен тінту желілік жүйелерге қашықтан қол жеткізуді, үлкен көлемдегі деректерді алуды, бұлттық қоймаларға кіруді қамтуы мүмкін [7]. Қолданыстағы заңнама киберкеңістікте тінту жүргізудің нақты тәртібін белгілемейді, бұл құқық қорғау органдарының өкілеттіктерінің шекараларын анықтауды қиындатады. Жеке өмірге құрметтеу құқығы мен тергеу мүдделерінің арасындағы теңгерім қамтамасыз етілуі тиіс.Телекоммуникация операторларының киберқылмыстармен күресте рөлі маңызды болып табылады. Операторлар трафик деректерін сақтау, құқық қорғау органдарына ақпарат беру, зиянды контентке қол жеткізуді шектеу жөніндегі міндеттерді атқарады [8]. «Байланыс туралы» Қазақстан Республикасының Заңы операторлардың міндеттерін белгілейді, алайда іс жүзінде орындау тетіктері әрдайым тиімді жұмыс істемейді. Операторлардың техникалық мүмкіндіктері шектеулі, деректерді сақтау қымбат, құқық қорғау органдарымен өзара іс-қимыл стандартталмаған.

Шифрлау технологиялары киберқылмыстарды тергеуде маңызды мәселе болып табылады. Қылмыскерлер байланысты және деректерді қорғау үшін шифрлауды белсенді пайдаланады. Шифрланған ақпаратқа қол жеткізу техникалық және құқықтық қиындықтар туғызады [9]. Кейбір мемлекеттер операторларды шифрлауға арналған кілттерді беруге міндеттейді, бұл жеке өмірдің құпиясы мен ақпараттық қауіпсіздік туралы пікірталастар тудырады. Қазақстан заңнамасы шифрлау мәселесін толық реттемейді.Киберқылмыстарды тергеуде халықаралық құқықтық көмек маңызды рөл атқарады. Киберқылмыстардың трансшекаралық сипаты шетелдік серверлерден деректерді алуды, басқа мемлекеттердің аумағында тергеу әрекеттерін жүргізуді, қылмыскерлерді экстрадициялауды қажет етеді [10]. Халықаралық құқықтық көмек рәсімдері көбінесе ұзақ уақытты қажет етеді, бұл киберқылмыстарды тергеу тиімділігін төмендетеді. Деректерді жедел алмасу тетіктерін жетілдіру, тікелей ынтымақтастық арналарын құру қажет.

Киберқылмыстармен күресте жасанды интеллект пен үлкен деректерді талдау технологияларын қолдану жаңа мүмкіндіктер ашады. Машиналық оқыту алгоритмдері аномалияларды анықтауға, қылмыстық схемаларды табуға, кибершабуылдарды болжауға мүмкіндік береді [11]. Алайда осы технологияларды қолдану құқықтық реттеуді қажет етеді. Автоматтандырылған жүйелердің шешімдерінің заңдылығы, дәлелдемелік маңызы, жеке деректерді қорғау мәселелері шешілуі тиіс.Киберқылмыстармен күресте мамандандырылған

құрылымдар құру тиімділікті арттырады. Кейбір мемлекеттерде киберполиция бөлімшелері, цифрлық криминалистика зертханалары, киберқауіпсіздік орталықтары жұмыс істейді [12]. Қазақстанда киберқауіпсіздік орталығы құрылды, алайда оның құзыреті негізінен ақпараттық инфрақұрылымды қорғауға бағытталған. Киберкылмыстарды тергеуге мамандандырылған құрылымдарды құру, оларды заманауи техникалық құралдармен жабдықтау, білікті мамандарды даярлау қажет.

Киберкылмыстармен күресте мамандарды даярлау өзекті міндет болып табылады. Тергеушілер, сот сарапшылары, прокурорлар, судьялар ақпараттық технологиялар, цифрлық криминалистика, киберқауіпсіздік саласында білімге ие болуы тиіс [13]. Қазіргі кезде мамандарды даярлау жүйесі жеткіліксіз дамыған. Арнайы оқу бағдарламалары, сертификаттау жүйесі, үздіксіз біліктілікті арттыру тетіктері қажет. Халықаралық тәжірибемен алмасу, шетелдік мамандармен ынтымақтастық маңызды.

Киберкылмыстармен күресте жеке сектормен ынтымақтастық тиімділікті арттырады. Ақпараттық технологиялар компаниялары, телекоммуникация операторлары, банктер, киберқауіпсіздік компаниялары маңызды ақпаратқа, техникалық мүмкіндіктерге, сараптамаға ие [14]. Мемлекеттік-жекешелік әріптестік киберқылмыстарды анықтауды, тергеуді, алдын алуды жеделдетуге мүмкіндік береді. Ақпарат алмасу, бірлескен жобалар, оқыту бағдарламал ары ынтымақтастықтың негізгі нысандары болып табылады.

Киберкылмыстармен күресте қоғамдық хабардарлықты арттыру алдын алу жұмысының маңызды бағыты болып табылады. Азаматтар киберқауіптер туралы, қауіпсіздік шаралары туралы, құқық бұзушылықтар туралы хабарлау тәртібі туралы ақпаратқа ие болуы тиіс [15]. Ақпараттық науқандар, білім беру бағдарламалары, БАҚ-пен жұмыс қоғамдық хабардарлықты арттырудың тиімді құралдары болып табылады. Киберқауіпсіздік мәдениетін қалыптастыру киберкылмыстардың санын азайтуға ықпал етеді.Киберкылмыстармен күресте заңнаманы жетілдірудің негізгі бағыттары анықталуы тиіс. Қылмыстық заңнаманы жаңа киберқауіптерді ескере отырып жаңарту қажет. Киберкылмыстардың жаңа құрамдарын енгізу, қолданыстағы нормаларды нақтылау, жауапкершілікті күшейту қарастырылуы тиіс. Криптовалюталармен байланысты қылмыстар, жасанды интеллектті қылмыстық мақсатта пайдалану, Интернет заттары құрылғыларына шабуылдар заңнамалық реттеуді қажет етеді.Қылмыстық-процестік заңнаманы жетілдіру электрондық дәлелдемелермен жұмыс істеудің нақты процедураларын белгілеуі тиіс. Киберкеңістікте тінту жүргізу тәртібі, электрондық деректерді алу және сақтау ережелері, цифрлық сараптаманың мәртебесі, шифрланған ақпаратқа қол жеткізу тетіктері заңнамалық деңгейде реттелуі қажет. Процестік кепілдіктерді сақтай отырып, тергеу органдарының тиімді жұмыс істеу мүмкіндіктерін қамтамасыз ету қажет.

Ведомствоаралық өзара іс-қимылды реттеу құзыреттердің нақты бөлінуін, ақпарат алмасу тетіктерін, бірлескен операцияларды жүргізу тәртібін қарастыруы тиіс. Киберкылмыстармен күресте үйлестіруші органды айқындау, бірыңғай ақпараттық жүйені құру, бірлескен жұмыс топтарын құру тиімділікті арттырады. Құзыреттердің қайталануын жою, ресурстарды ұтымды пайдалану маңызды міндет болып табылады.Телекоммуникация операторларының міндеттерін нақтылау деректерді сақтау мерзімдерін, беру тәртібін, техникалық талаптарды белгілеуі тиіс. Операторлардың шығындарын өтеу тетіктері, техникалық жабдықтауға мемлекеттік қолдау, стандарттарды әзірлеу қарастырылуы қажет. Операторлардың құқықтары мен міндеттерінің теңгерімі қамтамасыз етілуі тиіс.Жеке деректерді қорғау мен киберкылмыстармен күрестің арақатынасы заңнамалық деңгейде реттелуі қажет. Құқық қорғау органдарының жеке деректерге қол жеткізу өкілеттіктері нақты белгіленуі, қол жеткізу негіздері мен тәртібі айқындалуы, бақылау тетіктері қарастырылуы тиіс. Жеке өмірдің құпиясын қорғау конституциялық құқығын сақтай отырып, қоғамдық қауіпсіздікті қамтамасыз ету қажет.

Халықаралық ынтымақтастықты дамыту халықаралық шарттарды жасасуды, ақпарат алмасу тетіктерін жетілдіруді, бірлескен тергеу топтарын құруды қарастырады. Киберқылмыстылық туралы Будапешт конвенциясына қосылу мәселесін қарастыру, өңірлік

ынтымақтастықты нығайту, екіжақты келісімдерді жасасу халықаралық өзара іс-қимылды күшейтеді. Экстрадиция рәсімдерін жеделдету, деректерді тікелей алмасу мүмкіндіктерін кеңейту тиімділікті арттырады.

Мамандандырылған құрылымдарды құру киберполиция бөлімшелерін, цифрлық криминалистика зертханаларын, киберқауіпсіздік орталықтарын ұйымдастыруды қамтиды. Құрылымдарды заманауи техникалық құралдармен жабдықтау, бағдарламалық қамтамасыз етумен қамтамасыз ету, жоғары технологиялық инфрақұрылым құру қажет. Мамандандырылған құрылымдардың құқықтық мәртебесін белгілеу, құзыреттерін айқындау заңнамалық деңгейде жүзеге асырылуы тиіс.

Мамандарды даярлау жүйесін құру арнайы білім беру бағдарламаларын әзірлеуді, сертификаттау жүйесін енгізуді, үздіксіз біліктілікті арттыру тетіктерін қарастырады. Жоғары оқу орындарында киберкриминалистика мамандықтарын ашу, қысқа мерзімді оқыту курстарын ұйымдастыру, халықаралық сертификаттар алу мүмкіндіктерін қамтамасыз ету қажет. Тәжірибелік дағдыларды қалыптастыру, заманауи технологияларды меңгеру маңызды.Жеке сектормен ынтымақтастықты институционалдандыру мемлекеттік-жекешелік әріптестік келісімдерін жасасуды, бірлескен жобаларды іске асыруды, ақпарат алмасу платформаларын құруды қамтиды. Киберқауіпсіздік саласындағы компаниялармен ынтымақтастық, технологиялық компаниялардың сараптамасын пайдалану, банктік секторды тарту тиімділікті арттырады. Ақпарат құпиялылығын қамтамасыз ету, коммерциялық құпияны қорғау тетіктері қарастырылуы тиіс.

Қоғамдық хабардарлықты арттыру бағдарламасын әзірлеу ақпараттық науқандарды жоспарлауды, білім беру материалдарын дайындауды, БАҚ-пен өзара іс-қимылды ұйымдастыруды қамтиды. Мектептерде, жоғары оқу орындарында киберқауіпсіздік сабақтарын енгізу, халық арасында түсіндіру жұмысын жүргізу, әлеуметтік желілерді пайдалану тиімді әдістер болып табылады. Киберқауіпсіздік апталығын, конференцияларды, семинарларды өткізу қоғамдық назарды аударады.Киберкылмыстармен күресте жаңа технологияларды енгізу жасанды интеллектті, үлкен деректерді талдауды, блокчейн технологияларын пайдалануды қарастырады. Автоматтандырылған мониторинг жүйелері, болжамды аналитика, цифрлық іздерді іздестіру құралдары тиімділікті арттырады. Технологияларды енгізудің құқықтық негіздерін айқындау, стандарттарды әзірлеу, қауіпсіздікті қамтамасыз ету қажет.

Киберкылмыстармен күресте халықаралық тәжірибені зерделеу озық практиканы анықтауға, оны ұлттық жағдайларға бейімдеуге мүмкіндік береді. Еуропалық мемлекеттердің, АҚШ-тың, Азия елдерінің тәжірибесі қызығушылық тудырады. Заңнамалық шешімдер, ұйымдастырушылық модельдер, технологиялық тәсілдер салыстырмалы талдауды қажет етеді. Тәжірибені механикалық көшіру емес, ұлттық ерекшеліктерді ескере отырып бейімдеу маңызды.Киберкылмыстармен күресте стратегиялық жоспарлау ұзақ мерзімді бағдарламаларды әзірлеуді, басымдықтарды айқындауды, ресурстарды бөлуді қамтиды. Ұлттық киберқауіпсіздік стратегиясы, киберкылмыстылықпен күрес бағдарламасы, іс-қимыл жоспары стратегиялық құжаттар болып табылады. Мақсаттарды белгілеу, индикаторларды әзірлеу, мониторинг жүргізу стратегияны іске асыруды қамтамасыз етеді.Қорытындылай келе, Қазақстан Республикасының құқық қорғау органдарының киберкылмыстарды анықтау, ашу және тергеу жөніндегі қызметін құқықтық реттеу кешенді жетілдіруді қажет етеді. Қолданыстағы заңнама жедел өзгеріп жатқан киберқауіптерге толық жауап бере алмайды және бірқатар олқылықтарға ие. Қылмыстық және қылмыстық-процестік заңнаманы жаңарту, ведомствоаралық өзара іс-қимылды реттеу, халықаралық ынтымақтастықты дамыту маңызды міндеттер болып табылады.

Киберкылмыстармен күресте тиімділікті арттыру үшін мамандандырылған құрылымдарды құру, мамандарды даярлау жүйесін дамыту, заманауи технологияларды енгізу, жеке сектормен ынтымақтастықты нығайту қажет. Құқықтық реттеу технологиялық дамумен қатар жүруі, жаңа қауіптерге жедел жауап беруі, халықаралық стандарттарға сәйкес келуі тиіс.

Киберқылмыстармен күрес жеке құқықтар мен қоғамдық қауіпсіздіктің арақатынасын қамтамасыз етуді талап етеді. Жеке өмірдің құпиясын, жеке деректерді қорғау конституциялық құқықтарын сақтай отырып, құқық қорғау органдарының тиімді жұмыс істеу мүмкіндіктерін қамтамасыз ету қажет. Тек кешенді тәсіл, заңнамалық, ұйымдастырушылық, технологиялық, халықаралық шараларды біріктіру арқылы ғана киберқылмыстармен күресте айтарлықтай нәтижелерге қол жеткізуге болады.

Қолданылған әдебиеттер тізімі

1. Карпов В.С. Киберқылмыстылық: ұғымы, түрлері және қауіптілігі. – Мәскеу: Юрайт, 2020. – 342 б.
2. Қазақстан Республикасының Қылмыстық кодексі (2014 жылғы 3 шілдедегі № 226-V, өзгерістермен және толықтырулармен). – Астана, 2014.
3. Киберқылмыстылық туралы Конвенция (Будапешт, 2001 жылғы 23 қараша). – Будапешт, 2001.
4. «Қазақстан Республикасындағы ішкі істер органд ары туралы» Қазақстан Республикасының Заңы (2014 жылғы 23 сәуірдегі № 199-V, өзгерістермен). – Астана, 2014.
5. Нұрғалиев Е.С. Киберқылмыстарды анықтаудың техникалық және тактикалық ерекшеліктері // Заң және технология. – 2021. – № 3. – 78-86 б.
6. Әбдіғалиева Г.К. Электрондық дәлелдемелер қылмыстық процесте: теориялық және практикалық аспектілер. – Алматы: Қазақ университеті, 2020. – 287 б.
7. Қазақстан Республикасының Қылмыстық-процестік кодексі (2014 жылғы 4 шілдедегі № 231-V, өзгерістермен). – Астана, 2014.
8. «Байланыс туралы» Қазақстан Республикасының Заңы (2004 жылғы 5 шілдедегі № 567-II, өзгерістермен). – Астана, 2004.
9. Сейдахметов М.А. Шифрлау технологиялары және киберқылмыстарды тергеу проблемалары // Қазақстан Республикасының Жоғарғы Сотының Бюллетені. – 2020. – № 4. – 67-74 б.
10. Жұмабаев К.Т. Киберқылмыстармен күресте халықаралық құқықтық көмек. – Астана: Фолиант, 2019. – 234 б.
11. Бекболатов С.Р. Жасанды интеллект киберқауіпсіздікте: мүмкіндіктер және қауіптер // Ақпараттық қауіпсіздік. – 2021. – № 2. – 45-53 б.
12. Оразбаева А.Н. Киберполиция: шетелдік тәжірибе және Қазақстан үшін ұсыныстар // Құқық және мемлекет. – 2020. – № 3. – 89-97 б.
13. Қалиева Д.М. Киберқылмыстармен күресте мамандарды даярлау мәселелері // Заңгер. – 2021. – № 1. – 56-62 б.
14. Мұхамеджанов Р.Б. Киберқауіпсіздікте мемлекеттік-жекешелік әріптестік. – Алматы: LEM, 2020. – 198 б.
15. Сапарова Л.К. Киберқауіпсіздік мәдениетін қалыптастыру: қоғамдық хабардарлық пен білім беру // Қазақстандық әлеуметтанулық зерттеулер. – 2020. – № 4. – 112-119 б.