

АННОТАЦИЯ

Тақырыбы: Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар (қылмыстық-құқықтық және криминологиялық аспектілері)

Зерттеудің мақсаты – ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық құрамын, тарихи аспектілерін, құқық қолдану тәжірибесі мәселелерін кешенді талдау, сондай-ақ заңнаманы жетілдіру және қылмыстық құқық бұзушылықтармен күрестің тиімділігін арттыру бойынша ұсыныстар әзірлеу табылады.

Осы мақсатқа жету үшін жұмыста келесі **міндеттер** айқындалған:

1. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауаптылықтың тарихи аспектілерін зерттеу.

2. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар ұғымының қазіргі қалыптасуын ашып, және оған теориялық талдау жасау.

3. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершілікті реттейтін нормативтік құқықтық базаны талдау және оның кемшіліктерін анықтау.

4. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық сипаттамасын беру.

5. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы күрестің шетелдік тәжірибесіне салыстырмалы талдау жасау.

6. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың алдын алу шаралары мен заңнаманы жетілдіру бойынша ұсыныстар әзірлеу және негіздеу.

Зерттеу объектісі: ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар саласындағы қоғамдық қатынастар.

Зерттеу пәні: ақпараттандыру және байланыс саласындағы құқық бұзушылықтардың қылмыстық-құқықтық және криминологиялық аспектілері.

Зерттеу әдістері. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерттеу әдістемесі талдаудың тарихи-құқықтық, логикалық, статистикалық, салыстырмалы-құқықтық, теориялық және эмпирикалық әдістерін біріктіретін кешенді тәсілге негізделген. Негізгі әдістердің бірі – ақпараттық технологиялар және коммуникациялар саласын реттейтін қолданыстағы заңнаманы зерделеуге мүмкіндік беретін нормативтік құжаттаманы талдау. Бұл әдіс Қылмыстық кодексті, арнайы заңдарды, заңға тәуелді актілерді егжей-тегжейлі зерделеуді, сонымен қатар сот тәжірибесі мен қабылданған шешімдерді талдауды қамтиды. Талдау мақсаты – құқықтық олқылықтарды, қайшылықтарды анықтау және киберқылмыспен күресудегі нормативтік құқықтық актілердің тиімділігін бағалау. Құқық қорғау органдары мен ғылыми-зерттеу институттарының статистикалық мәліметтерін пайдалану мәселенің ауқымын бағалауға, қылмыстық құқық бұзушылықтардың жиі кездесетін түрлерін анықтауға және олардың алдын

алу және ашу бойынша қабылданған шаралардың тиімділігін бағалауға мүмкіндік береді. Сонымен қатар, халықаралық тәжірибені салыстырмалы талдау әртүрлі елдердегі киберқылмысты реттеу мен күресудің тиімді тәжірибесі мен әдістерін зерттеуде маңызды рөл атқарады. Бұл әдіс басқа юрисдикциялар контекстінде бейімделуі және қолданылуы мүмкін табысты стратегияларды анықтауға мүмкіндік береді, осылайша ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресте халықаралық ынтымақтастықты жақсартуға ықпал етеді.

Зерттеудің теориялық және әдіснамалық негіздері. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың теориялық және әдістемелік негіздерін зерттеу олардың тарихи дамуы мен халықаралық ынтымақтастығын ескере отырып, осы қылмыстық құқық бұзушылықтардың түсінігін, жіктелуін және қылмыстық-құқықтық аспектілерін талдауды қамтиды. Криминологиялық аспектіде киберқылмысқа ықпал ететін себептер мен жағдайларды түсінуге және тиімді алдын алу шараларын әзірлеуге мүмкіндік береді. Зерттеу әдістемесі мәселені жан-жақты талдауды қамтамасыз ететін және заңнаманы жетілдіру және ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы күрестің тиімділігін арттыру бойынша ұсыныстар әзірлеуге ықпал ететін теориялық және эмпирикалық әдістерді кешенді пайдалануға негізделген.

Зерттеудің ғылыми жаңалығы. Бұл зерттеудің ғылыми жаңалығы ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды талдау мен саралауға байланысты жаңа ғылыми қағидаларды тұжырымдау мен әзірлеуде жатыр. Жұмыс барысында осындай қылмыстық құқық бұзушылықтарды жасаудың белгілері мен механизмдерін анықтайтын негізгі аспектілер анықталып, жүйеленді, бұл қылмыстық құқық пен криминологиядағы теориялық көзқарастарды жаңартуға мүмкіндік берді. Зерттеу қылмыстық құқық бұзушылықтың сипаты мен құрылымын өзгертуге ақпараттық-техникалық прогрестің әсерін егжей-тегжейлі талдау, сондай-ақ құқықтық жүйені жаңа міндеттерге бейімдеу қажеттілігін негіздеу арқылы заң ғылымының теориялық негіздерін дамытуға ықпал етеді.

Зерттеудің теориялық және тәжірибелік маңызыдылығы.

Зерттеудің теориялық маңыздылығы киберқылмыс туралы бұрыннан бар білімді байыту және кеңейту, сондай-ақ ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерттеу және олармен күресу бойынша әдістемелік тәсілдерді әзірлеуде жатыр. Зерттеу киберқылмыстардың жаңа классификациясын ұсынады, бұл олардың табиғатын дәлірек түсінуге және нәтижесінде құқық қорғау органдарының тиімдірек болуына ықпал етеді. Жұмыс сонымен қатар криминологиялық теорияның шекарасын кеңейтіп, қоғамды цифрландыру мен ақпараттық қауіпсіздікке қатысты аспектілерді енгізеді.

Зерттеудің тәжірибелік маңыздылығы. Диссертацияның тәжірибелік құндылығы заңнаманы және оны ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылыққа қарсы күресте қолдану тәжірибесін жетілдіру бойынша нақты ұсыныстарды әзірлеу және ұсынумен байланысты. Зерттеу

барысында заңнамадағы бар олқылықтарды жоюға және ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың ведомствоаралық және халықаралық ынтымақтастық тетіктерін жетілдіруге бағытталған нормативтік құқықтық базаны нығайту жолдары ұсынылған. Сонымен қатар, жұмыс барысында заманауи технологиялар мен тергеу әдістерін енгізу арқылы ішкі істер органдары қызметінің тиімділігін арттыру, сонымен қатар цифрлық дәуір талабына сай қызметкерлерді оқыту және біліктілігін арттыру бойынша ұсыныстар тұжырымдалды.

Зерттеудің теориялық және тәжірибелік маңызыдылығы.

Зерттеудің теориялық маңыздылығы киберқылмыс туралы бұрыннан бар білімді байыту және кеңейту, сондай-ақ ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерттеу және олармен күресу бойынша әдістемелік тәсілдерді әзірлеуде жатыр. Зерттеу киберқылмыстардың жаңа классификациясын ұсынады, бұл олардың табиғатын дәлірек түсінуге және нәтижесінде құқық қорғау органдарының тиімдірек болуына ықпал етеді. Жұмыс сонымен қатар криминологиялық теорияның шекарасын кеңейтіп, қоғамды цифрландыру мен ақпараттық қауіпсіздікке қатысты аспектілерді енгізеді.

Зерттеудің тәжірибелік маңыздылығы. Диссертацияның тәжірибелік құндылығы заңнаманы және оны ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылыққа қарсы күресте қолдану тәжірибесін жетілдіру бойынша нақты ұсыныстарды әзірлеу және ұсынумен байланысты. Зерттеу барысында заңнамадағы бар олқылықтарды жоюға және ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың ведомствоаралық және халықаралық ынтымақтастық тетіктерін жетілдіруге бағытталған нормативтік құқықтық базаны нығайту жолдары ұсынылған. Сонымен қатар, жұмыс барысында заманауи технологиялар мен тергеу әдістерін енгізу арқылы ішкі істер органдары қызметінің тиімділігін арттыру, сонымен қатар цифрлық дәуір талабына сай қызметкерлерді оқыту және біліктілігін арттыру бойынша ұсыныстар тұжырымдалды.

Қорғаудың ұсынылатын негізгі тұжырымдар:

1. Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасы мен Киберқауіпсіздік тұжырымдамасының жүзеге асуын ескере отырып, автормен ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың теориялық сипатта авторлық анықтамасы берілді.

Инновациялық цифрлық технологиялардың қарқынды дамуы жағдайында құқық бұзушылар қылмыстық құқық бұзушылықтар жасаудың жаңа тәсілдерін қолданады, сондай-ақ қоғамдық өмірдің көптеген салалары үшін, оның ішінде кәсіпкерлік қызметтің еркіндігі үшін қосымша қылмыстық қауіптер туындайды, осындай жағдайда толыққанды ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық анықтамасы қажет.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар дегеніміз - «ақпараттық жүйелерді, мәліметтер базасын және телекоммуникация, компьютерлік коммуникациялар желілерін заңсыз

пайдалану арқылы жүзеге асырылатын, жеке және мемлекеттік деректерге қол жеткізу, оларды өзгерту немесе жою мақсатындағы қылмыстық құқық бұзушылық».

2. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды саралау барысында ұғымдық аппаратта кемшіліктер анықталды. Осы бағытта кемшіліктерді жою мақсатында келесі ұғымдарды енгізуді ұсынымыз. Қазақстан Республикасы Қылмыстық кодекстің 3-бабының 41-1 тармағын енгізу және мынадай ұғымдармен толықтыру қажет: «киберқылмыс», «компьютерлік коммуникация», «киберқауіпсіздік». «Киберқылмыс – киберкеңістікте ақпараттық технологияларды, компьютерлік жүйелерді, құпия ақпаратты, жеке деректерді заңсыз иемдену және қолдану әрекеттері», «Компьютерлік коммуникация - бұл компьютерлер арасында деректерді жіберу және қабылдау үшін Интернет, локальды (LAN) және сымсыз желілер сияқты түрлі желілік технологияларды пайдалану процесі», «Киберқауіпсіздік - компьютерлік жүйелерді, желілерді және деректерді рұқсатсыз кіруден, шабуылдардан және қауіптерден қорғауға арналған шаралар мен процестер». Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерттеу барысында қоғамдық қауіпті әрекеттер мен әрекетсіздіктердің, сондай-ақ ықтимал немесе нақты туындайтын ауыр және аса ауыр зардаптардың негізгі белгілерін дефинициялар арқылы нақты және уақтылы анықтау қажеттілігі туындайды. Мұндай дефинициялар қылмыстық құқық бұзушылықтарды жіктеуге, құқық қолдану тәжірибесін жетілдіруге және осындай әрекеттерге қарсы тиімді құқық қорғау шараларын қолдануға мүмкіндік береді. Бұл тұрғыда, қылмыстық құқық бұзушылықтардың дер кезінде анықталуы мен нақты сипатталуы маңызды рөл атқарады, себебі ол құқық қорғау органдарының дұрыс әрекет етуіне және ақпараттық қауіпсіздікті қамтамасыз етуге ықпал етеді.

Сонымен қатар ҚР ҚК 3 бабының 38 тармағына ҚР ҚК 205, 206, 208 баптарымен толықтыру, яғни *ірі залал және ірі мөлшер ретінде айлық есептік көрсеткіштен бір мың есе асатын мүлік құны немесе залал мөлшері ретінде өзгерістер енгізу* ұсынылады. Себебі, Ірі залал және ірі мөлшер ұғымдары қылмыстық құқық бұзушылықтың қоғамға тигізетін зиянының дәрежесін объективті бағалауға мүмкіндік береді. Осылайша, қылмыстық құқық бұзушылықтың ауырлығын нақты анықтап, құқық қорғау органдарының дұрыс әрекет етуін қамтамасыз етеді. Анықталған шектердің болуы құқық қорғау органдары мен соттар үшін қылмыстық құқық бұзушылықтарды анықтау және оларға баға беру үдерістерін жеңілдетеді. Халықаралық тәжірибеде мүліктік залал және шығындар мөлшерін нақтылау кең таралған тәжірибе. Бұл өзгерістер халықаралық стандарттарға сәйкестікті қамтамасыз етіп, құқықтық жүйені жаһандық деңгейде жақсартады.

3. Тергеу және сот практикасы көрсеткендей, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объективтік немесе субъективтік белгілерінде заңнамалық кемшіліктер байқалады. Зерттеулерге сәйкес, мұндай құқық бұзушылықтардың санының өсуі

ақпараттық технологияларды қолдану аясының кеңеюіне байланысты болып отыр. Қаржы институттары, энергетикалық жүйелер және мемлекеттік басқару секілді негізгі инфрақұрылымдар киберқылмыскерлердің басты нысаналарына айналуға және олар тиімді киберқорғаныс пен қылмыстық-құқықтық шараларды талап етеді. Технологиялық прогресс пен қоғамның цифрлану үдерісінде қылмыстық заңнаманы жаңарту қажеттілігі туындайды. Бұл өз кезегінде, ақпараттық қауіпсіздік пен инновациялар арасындағы тепе-теңдікті сақтауға мүмкіндік береді. Осылайша, ақпараттық қылмыстық құқық бұзушылықтарға қарсы күрес шараларын күшейту қажеттілігі арта түседі. Заңнамалық актілердің нақтылығын арттыру мен құқық қолдану тәжірибесін жетілдіру қылмыстық құқық бұзушылықтардың уақтылы анықталуына, олардың жіктелуіне және құқық қорғау органдарының тиімді әрекет етуіне ықпал етеді. Осы тұрғыда, ақпараттық құқық бұзушылықтармен күресу үшін заманауи саясат пен әдістемелерді енгізу, сондай-ақ құқықтық реттеуді жетілдіру қажет. Осы әрекеттер құқықтық қауіпсіздікті қамтамасыз ету және киберқауіптерден қорғауды күшейтуге бағытталған маңызды қадамдарды құрайды.

Сондықтан, келесі өзгерістер мен толықтырулар ұсынылады:

- ҚР ҚК-нің 205-бабының 4-бөлігін келесі редакцияда беру ұсынылады: «Электрондық жеткізгіштегі заңмен қорғалатын ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделерін елеулі түрде бұзуға әкеп соққан қасақана құқыққа сыйымсыз қол жеткізу, *абайсызда ауыр зардаптарға әкеп соққан дәл сол іс-әрекет, адамдар тобының алдын ала сөз байласуымен, бірнеше рет жасалған іс әрекеттер*» - «белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан төрт жылға дейінгі мерзімге айыра отырып немесе онсыз, екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не *алты жылға дейінгі* мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады»

- ҚР Қылмыстық кодексінің 206 бабы 1-бөлігін диспозициясын «компьютерлік коммуникация» ұғымымен толықтыру ұсынылады. Себебі, ақпаратты құқыққа сыйымсыз жою немесе түрлендіру әрекеттері *компьютерлік коммуникация* желісі арқылы беріледі. ҚР ҚК 206 бабының 1-бөлігі келесі редакцияда ұсынылады: «Электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникациялар, *компьютерлік коммуникация* желісі бойынша берілетін, заңмен қорғалатын ақпаратты қасақана құқыққа сыйымсыз жою немесе түрлендіру, сол сияқты ақпараттық жүйеге көрінеу жалған ақпарат енгізу, егер бұл азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделерін елеулі түрде бұзуға әкеп соқса»

- ҚР Қылмыстық кодексінің 208 бабы 1-бөлігін диспозициясын «компьютерлік коммуникация» ұғымымен толықтыру ұсынылады. Себебі,

ақпаратты құқыққа сыйымсыз иеленіп алу әрекеттері компьютерлік коммуникация желісі жүзеге асырылады. ҚР ҚК 208 бабының 1-бөлігі келесі редакцияда ұсынылады: «Электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникациялар, *компьютерлік коммуникация* желісімен берілетін заңмен қорғалатын ақпаратты қасақана құқыққа сыйымсыз көшіру немесе өзгедей құқыққа сыйымсыз иеленіп алу, егер бұл азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделерін елеулі түрде бұзуға әкеп соқса»

- Қазақстан Республикасының «Ақпараттандыру туралы» заңы 2015 жылғы 24 қарашадағы № 418-V қабылданған заңының 1- бабының 7-1 тармақшасына, Осы Заңда пайдаланылатын негізгі ұғымдарға өзгерту мен толықтырулар енгізу ұсынамыз: *«Киберқауіпсіздік - бұл компьютерлік жүйелерді, желілерді және деректерді рұқсатсыз қол жеткізуден, шабуылдардан және қауіптерден қорғауға бағытталған шаралар мен процестер жиынтығы»* анықтама ұғымымен толықтыруды ұсынамыз. Себебі, Киберқауіпсіздік ұғымының заңнамаға енгізілуі құқықтық жауапкершілікті нақтылау, ақпараттық қауіпсіздік деңгейін арттыру, халықаралық стандарттарға сәйкестікті қамтамасыз ету, экономикалық және ұлттық қауіпсіздікті нығайту мақсаттарына бағытталған маңызды қадам болып табылады.

4. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресудің отандық және шетелдік тәжірибесін салыстырмалы талдау көрсеткендей, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресу бойынша келесі іс-шараларды ұсынамыз:

- *Халықаралық ынтымақтастықты нығайту.* Киберқылмыспен күресудегі белсенді халықаралық ынтымақтастыққа, оның ішінде міндетті ақпарат алмасуды және шетелдік серіктестермен бірлескен операцияларды жүргізуге міндеттемені өзара халықаралық келісіммен бекіту. Трансшекаралық киберқылмысқа қарсы күреске бағытталған халықаралық келісімдер мен конвенцияларды ратификациялауды ұсынамыз. Осыған, Будапешт конвенциясы сияқты халықаралық келісімдерге қосылу ұсынылады, бұл конвенция компьютерлік желілер арқылы және интернет арқылы жасалатын қылмыстық құқық бұзушылық туралы ең алғашқы халықаралық шарт болып табылады. Мұнда компьютерлік желілерді іздеу, ұстап алу сияқты бірқатар процедуралар мен өкілеттіктер бар, сондықтан біздің ойымызша осы ұсыныс өте маңызды деп есептейміз. Киберқылмыс туралы Будапешт конвенциясын ратификациялау Қазақстан Республикасына киберқылмыспен күресудегі халықаралық ынтымақтастық жүйесіне қосылуға мүмкіндік береді. Бұл киберқылмыспен күресу үшін құқықтық базаны нығайтуға, басқа елдермен тиімді ынтымақтастықты қамтамасыз етуге және азаматтар мен ұйымдарды киберқауіптерден қорғауды жақсартуға мүмкіндік береді. Сонымен қатар, конвенцияны ратификациялау киберқауіптер мен инциденттер туралы ақпарат алмасуға арналған халықаралық желіге қол

жеткізеді, бұл жаңа қауіптерге тезірек ден қоюға мүмкіндік береді.

- *Профилактикалық мониторинг жүйесін енгізу.* Технологияның қарқынды дамуы және киберқылмыстардың өсуі жағдайында бұл қағида құқық қорғау органдарына ақпаратты талдаудың және ақпараттық ортаны бақылаудың заманауи құралдарымен жабдықталған мамандандырылған орталықтарды құруды көздейді, бұл құқық қорғау органдарына жедел әрекет етуге мүмкіндік береді. Ақпараттық қауіпсіздікті қамтамасыз ету үшін «Мемлекеттік техникалық қызмет» негізінде киберқауіптерді ерте анықтайтын мониторинг орталығын құру ұсынылады. Бұл орталық ақпаратты талдау және қауіптерді ертерек анықтау үшін заманауи технологиялармен жабдықталады. Мұндай орталықтар трансшекаралық киберқауіптерге шұғыл әрекет етіп, қылмыстық құқық бұзушылықтарды алдын алу шараларын жоспарлау сатысында іске асыруға мүмкіндік береді.

- *Оқу жоспар бағдарламасын әзірлеу.* Құқық қолдану тәжірибесі көрсеткендей қазір осы саладағы қылмыстық құқық бұзушылықтарды тергейтін кәсіби мамандардың жоқшылығы қатысты оларды даярлау талабы туып отыр. Сондықтан, Құқық қорғау қызметкерлерін киберқылмыстарды тергеу және цифрлық сараптама бойынша оқыту үшін «Кибертергеуші» бағытындағы міндетті оқу бағдарламаларын әзірлеу. Бұл оқу бағдарламасы заманауи кибершабуылдарды анықтау және тергеудің соңғы әдістерін, сондай-ақ халықаралық құқық нормаларын қамтуы қажет.

- *Халықтың цифрлық сауаттылығын арттыру.* Халықтың интернеттегі қауіпсіздікке қатысты хабардарлығын арттыру мақсатында үкімет пен азаматтық қоғам арасында тығыз қарым-қатынас орнату маңызды. Жаппай ақпараттық науқандар, цифрлық қауіпсіздік бойынша тренингтер мен білім беру бағдарламалары азаматтардың өздерін және деректерін киберқауіптерден қорғауға мүмкіндік береді. Азаматтардың интернеттегі қауіпсіздік туралы хабардарлығының артуы құқықтық тәртіпті сақтау үшін маңызды, себебі бұл құқық бұзушылықтардың алдын алу және оларға қарсы шаралар қолдану мүмкіндігін арттырады. Цифрлық қауіпсіздік бойынша тренингтер мен білім беру бағдарламалары арқылы азаматтардың құқықтары мен міндеттері туралы түсініктерін кеңейту олардың құқықтық жауапкершілігін арттырады. Бұл шаралар құқық қорғау органдарына келіп түсетін киберқылмысқа қатысты шағымдардың санын азайтуға да ықпал етеді.

Зерттеу нәтижелерін талқылау және енгізу:

Диссертациялық зерттеу жұмысы «Alikhan Bokeikhan University» заң факультеті, қылмыстық-құқықтық пәндер кафедрасында дайындалды, рецензияланды және талқыланды. Диссертациялық зерттеу бойынша 5 ғылыми мақала жарияланды:

2 мақала Scopus (Elsevier) халықаралық ақпараттық ресурсына кіретін ғылыми басылымдарда: «Revista de Direito, Estado e Telecomunicacoes» (Brazil), ISSN 1984-9729, Topical Issues in the Fight Against Criminal Offences in the Field of Informatisation and Communications // Revista de Direito, Estado e Telecomunicacoes. – 2023. – Vol. 15, Iss. 1. – P. 177-190.

Revista de Direito, Estado e Telecomunicacoes» (Brazil), ISSN 1984-9729,

Measures to Prevent Criminal Offences in the field of Informatisation and Communications in the Republic of Kazakhstan // Revista de Direito, Estado e Telecomunicacoes. – 2024. – Vol. 16, No 2. – P. 276-294.

3 мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету комитеті журналында:

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресудің кейбір теориялық аспектілер, «Құқық қорғау органдары Академиясының жаршысы» Ғылыми журналы №2 (24) 2022 ж. 58б.

International cooperation in combating criminal offences in the field of informatization and communications, «Құқық қорғау органдары Академиясының жаршысы» Ғылыми журналы № 2 (28) 2023 ж. 74 б.

Киберқылмыскер тұлғасының криминологиялық сипаттамасы// Қазақстан Республикасы ІІМ Бәрімбек Бейсенов атындағы Қарағанды академиясының 2022 жылғы 30 қыркүйек № 3 (77) «ХАБАРШЫ — ВЕСТНИК» журналы б.139-144

Зерттеу жұмысының құрылымы: диссертация 171 беттен, кіріспеден, 3 тараудан, қорытындыдан және дереккөзден тұратын әдебиеттер тізімінен тұрады.

Зерттеу нәтижелері Қазақстан Республикасында киберқауіпсіздікті қамтамасыз ету және ақпараттық инфрақұрылымды қорғау бойынша жаңа тетіктерді енгізу қажеттігін көрсетеді. Сонымен қатар, жұмыста құқықтық нормаларды жетілдіру және құқық қорғау органдарының тиімділігін арттыру бойынша нақты ұсыныстар беріледі.

Жалпы алғанда, бұл диссертация заманауи ақпараттық қоғамда кездесетін құқықтық және ұйымдастырушылық мәселелерді шешуге бағытталған кешенді зерттеу болып табылады.