Alikhan Bokeikhan University

ӘОЖ 343.3/.7
МҒТАР 10.77.51

Қолжазба құқығында

ҚАМБАРОВ АЗАМАТ ҚАМБАРҰЛЫ

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

8D04208 «Қазақстандық құқықтың дамуының заманауи үрдістері»
Философия докторы (PhD) дәрежесін алу үшін дайындалған диссертация

Отандық ғылыми кеңесші
PhD, доцент
Каражанов М.Д.
Шетелдік ғылыми кеңесші
заң ғылымдарының докторы,
профессор Авдеев В.А.,
РФ, Ханты-Мансийск қаласы

Қазақстан Республикасы
Семей, 2024 жыл

МАЗМҰНЫ

НОРМАТИВТІК СІЛТЕМЕЛЕР

Диссертациялық жұмыста қолданылған нормативтік құжаттар:

Қазақстан Республикасының Президенті Қ.Тоқаевтың 2019 жылғы 2 қыркүйектегі «Сындарлы қоғамдық диалог – Қазақстанның тұрақтылығы мен өркендеуінің негізі» тақырыбындағы Қазақстан халқына Жолдауы.

Президенттің 08.01.2013 ж. Жарлығымен бекітілген «Ақпараттық Қазақстан-2020» мемлекеттік бағдарламасы.

Қазақстан Республикасы Президентінің 2017 жылғы 31 қаңтардағы «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Қазақстан халқына жолдауы

«Цифрлық Қазақстан» мемлекеттік бағдарламасы

Президентінің Қазақстан халқына 1997 жылғы 10 қазандағы «Қазақстан - 2030. Өркендеу, қауіпсіздік және барлық қазақстандықтардың әл-ауқатын жақсарту» атты жолдауы

Қазақстан Республикасының Президенті Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауы «Әділетті Қазақстанның экономикалық серпіні». 2 қыркүйек 2024 ж.

Қазақстан Республикасының «Ақпараттандыру туралы» заңы (өзгерістер мен толықтырулар енгізілген нұсқасы). – 2015 жылғы 24 қарашадағы № 418-V ҚРЗ. Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет»

Қазақстан Республикасының «Киберқауіпсіздік тұжырымдамасы – «Қазақстанның киберқалқаны»» бекітілген қаулысы, 2017 жылғы 30 маусымдағы № 407. Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет»

Қазақстан Республикасының «Цифрландыру, инновациялар және аэроғарыш өнеркәсібі министрлігі туралы» Ережесі, 2021 жылғы 26 наурыздағы № 133 қаулысы. Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет»

Қазақстан Республикасының 2025 жылға дейінгі ұлттық киберқауіпсіздік стратегиясы туралы ҚР Үкіметінің қаулысы. Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет»

АНЫҚТАМАЛАР

Осы диссертациялық жұмыста келесі терминдер сәйкес анықтамаларымен қолданылды:

АҚПАРАТ – әртүрлі мақсаттарда берілетін, сақталатын, өңделетін немесе пайдаланылатын деректер, ақпарат немесе фактілердің жиынтығы. Киберқылмыс контекстінде ақпарат жеке деректерді, коммерциялық құпияны, зияткерлік меншікті және заңмен қорғалатын басқа да деректер түрлерін қамтуы мүмкін.

АҚПАРАТТАНДЫРУ – Қоғам өмірінің барлық салаларына, соның ішінде экономика, менеджмент, білім беру және басқа салаларға ақпараттық технологияларды енгізу және пайдалану процесі. Киберқылмыскерлердің нысанасына айналатын компьютерлік жүйелер мен желілерді дамытуды көздейді.

ДАМУ ГЕНЕЗИСІ – Белгілі бір құбылыстардың немесе процестердің пайда болу, қалыптасу және даму процесі. Бұл тұрғыда ол киберқылмыстың тарихи дамуы мен эволюциясына және оған қарсы шараларға сілтеме жасайды.

ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚ – Материалдық пайда немесе жеке ақпаратты алу мақсатында Интернет арқылы пайдаланушыларды алдауды қамтитын киберқылмыстың түрі. Электрондық пошталарды, жалған веб-сайттарды және әлеуметтік медианы пайдаланатын алаяқтықты қамтиды.

ИНТЕРПОЛ – халықаралық қылмыспен, соның ішінде киберқылмыспен күресуде әртүрлі елдердің құқық қорғау органдарының өзара іс-қимылын үйлестіретін халықаралық қылмыстық полиция ұйымы. Ұйым тергеу, ақпарат алмасу және полицияны оқытуға қолдау көрсетеді.

КИБЕРКЕҢІСТІК – пайдаланушылар арасында ақпарат алмасу және өзара әрекеттесу орын алатын желі және компьютерлік жүйелер арқылы жасалған виртуалды орта. Интернетті, ұйымдық интранеттерді және цифрлық өзара әрекеттесудің басқа түрлерін қамтиды.

КИБЕРҚАУІПСІЗДІК – компьютерлік жүйелерді, желілерді және деректерді рұқсатсыз кіруден, шабуылдардан және қауіптерден қорғауға арналған шаралар мен процестер.

КИБЕРҚЫЛМЫСТЫҢ АЛДЫН АЛУ – Ақпараттық технологиялар және киберкеңістік саласындағы қылмыстық құқық бұзушылықтың алдын алуға бағытталған шаралар кешені.

КИБЕРТЕРРОРИЗМ – қорқыныш тудыру, компьютерлік жүйелерді бұзу, инфрақұрылымдарды құлату немесе саяси мақсаттарға жету үшін кибершабуылдарды пайдалану. Үкіметке және маңызды инфрақұрылымға шабуылдарды қамтиды.

КИБЕРШАБУЫЛДАР – компьютерлік жүйелерге, желілерге немесе деректерге зақым келтіру, жою немесе рұқсатсыз қол жеткізу үшін компьютерлік технологияларды пайдаланатын мақсатты әрекеттер. Мысалы, вирустар, трояндық аттар, фишинг және DDoS шабуылдары.

КОМПЬЮТЕРЛІК ТЕХНОЛОГИЯЛАР – Ақпаратты өңдеу, сақтау, беру және

қорғау үшін қолданылатын аппараттық және бағдарламалық құралдар. Аппараттық құралдарды, бағдарламалық құралдарды, желілерді және қауіпсіздік жүйелерін қамтиды.

КРИМИНОЛОГ – Қылмыстың себептерін, сипаты мен динамикасын зерттейтін, сондай-ақ оның алдын алу мен күресу әдістерін, соның ішінде киберқылмыстарды әзірлейтін криминология саласындағы маман.

КРИМИНОЛОГИЯ – қылмысты, оның себептерін, жағдайларын, алдын алу шаралары мен күресу әдістерін зерттейтін ғылыми пән. Киберқылмыстарды талдауды және олардың алдын алу стратегияларын әзірлеуді қамтиды.

ҚЫЛМЫСТЫҚ ЖАУАПТЫЛЫҚ – Қылмыстық жазаларды қолдануға әкеп соғатын қылмыстық заңмен тыйым салынған әрекеттерді жасағаны үшін туындайтын жауапкершілік.

САНДЫҚ КРИМИНАЛИСТИКА – сотта дәлел ретінде пайдалану үшін электронды түрде сақталған ақпаратты зерттеу ғылымы мен тәжірибесі.

ТРАНСҰЛТТЫҚ КИБЕРҚЫЛМЫС – жиі жаһандық желілерді пайдалана отырып, әртүрлі елдердің қылмыскерлері жасайтын киберқылмыстар. Мұндай қылмыстарды тергеу және алдын алу үшін халықаралық ынтымақтастық қажет.

ТРАНСШЕКАРАЛЫҚ – бір елдің шекарасынан шығатын немесе одан тыс жатқан әрекеттерді немесе құбылыстарды сипаттайды. Киберқылмыс контекстінде ол ұлттық шекарадан өтетін қылмыстық әрекетті білдіреді.

ЭКОНОМИКАНЫ ЖАҺАНДАНУ ЖӘНЕ ЦИФРЛАНДЫРУ – халықаралық деңгейде ақпарат пен қаржылық операцияларды жылдам алмасуға мүмкіндік беретін цифрлық технологияларды дамыту арқылы әлемдік экономикаларды интеграциялау процесі. Киберқылмыстардың өсуіне әкеледі және олармен күресу үшін халықаралық ынтымақтастықты талап етеді.

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

РО – Бағдарламалық құралы
G20 – Жиырмалық топ
АҚШ – Америка Құрама Штаттары
IT – Ақпараттық технологиялар
ТМД – Тәуелсіз Мемлекеттер Достастығы
UNIVAC – әмбебап автоматты компьютер
IoT – заттардың интернеті (Internet of Things)
БАҚ – Бұқаралық ақпарат құралдары
ЭЫДҰ – Экономикалық ынтымақтастық және даму ұйымы (Organisation for Economic Co-operation and Development)
БҰҰ – Біріккен Ұлттар Ұйымы
www – World Wide Web
ҚР ҚК – Қазақстан Республикасының Қылмыстық кодексі
АКТ – Ақпараттық-коммуникациялық технологиялар
ЕО – Еуропалық Одақ
BSI – Ақпараттық қауіпсіздік федералды агенттігі (Bundesamt für Sicherheit in der Informationstechnik)
ISO/IEC 15408 – Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлерінің халықаралық стандарты
COBIT – Ақпараттық және байланысты технологияларды басқару мақсаттары
NIS – желілік және ақпараттық жүйелер жөніндегі директивасы

КІРІСПЕ

Жұмыстың жалпы сипаттамасы. Диссертациялық зерттеу жұмысында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың қылмыстық құқықтық және криминологиялық аспектілерінде ашылады. Жұмыста ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың тарихи аспектілері анықталады, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың қалыптасу ұғымының мәселелері, Қазақстан Республикасының және шетелдік ғалымдардың пікірлеріне салыстырмалы талдау жолымен жасалады. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық аспектісі талданып, жетілдіру бағыттары ұсынылды.

Зерттеудің тақырыбының өзектілігі. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерттеудің өзектілігі ақпараттық технологиялардың қарқынды дамуымен және олардың қазіргі қоғамның барлық салаларына жан-жақты енуімен тығыз байланысты. Экономиканы, саясатты, білім мен мәдениетті жаһандану мен цифрландыру жағдайында ақпараттық кеңістік деректер мен білім алмасу құралы ғана емес, сонымен қатар жаңа қылмыстық құқық бұзушылық түрлерінің аренасына айналуда. Бұл қылмыстық құқық бұзушылықтар жеке тұлғаларға ғана емес, жалпы қоғамға қауіп төндіріп, ақпараттық қауіпсіздіктің, экономикалық тұрақтылық пен мемлекеттің егемендігінің негіздеріне нұқсан келтіреді.

Мемлекеттік және жеке ақпараттық жүйелерге кибершабуылдар, интернет-алаяқтық, жеке деректерді заңсыз жинау және тарату, цифрлық кеңістікте зияткерлік меншік құқықтарын бұзу және т.б. сияқты қылмыстық құқық бұзушылықтардың жаңа нысандарының пайда болуына ықпал етеді. Бұл қылмыстық құқық бұзушылықтар анонимділіктің жоғары дәрежесімен, трансшекаралық сипатымен және ашу мен тергеудің қиындығымен сипатталады, бұл құқық қорғау органдарынан жұмыстың жаңа тәсілдері мен әдістерін талап етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың жолын кесу және алдын алу контекстінде қарама-қайшылықтарды анықтау және мәселелерді қою заң ғылымының және құқық қорғау органдарының теориясы мен тәжірибесінің алдында тұрған міндеттердің күрделі және көп қырлы сипатын ашады. Бұл салада егжей-тегжейлі талдауды және тиімді шешімдерді әзірлеуді талап ететін бірнеше күрделі қайшылықтар мен шешімін таппаған мәселелер бар.

Негізгі қарама-қайшылықтардың бірі – ақпараттық технологиялардың қарқынды дамуы және заңнаманың бейімделу мен әрекет ету жылдамдығынан асып түсетін киберқылмыстың жаңа түрлерінің пайда болуы. Бұл құқықтық вакуумды тудырады және киберқылмыспен күресу үшін қолданыстағы қылмыстық заңдарды тиімді қолдануды қиындатады. Сонымен қатар,

қолданыстағы құқықтық анықтамалар мен қылмыстық құқық бұзушылықтардың жіктелуі көбінесе ақпараттық ортада туындайтын қауіптердің ерекшеліктері мен ауқымын көрсетпейді.

Киберқылмыстардың трансұлттық сипатына қатысты, бұл ұлттық алдын алу шаралардың тиімділігіне күмән келтіреді және халықаралық құқықтық тетіктер мен келісімдерді әзірлеуді талап етеді. Бірыңғай халықаралық-құқықтық базаның болмауы және әртүрлі елдердің заңдарындағы айырмашылықтар құқық қорғау органдары арасындағы іс-әрекеттерді үйлестіруді және ақпарат алмасуды қиындатады.

Тағы бір мәселе, құқық қорғау органдары мен сот жүйесі киберқылмыстық істерді тиімді тергеуге және қудалауға дайын емес. Бұған арнайы білім мен техникалық құралдардың жетіспеушілігі ғана емес, сонымен қатар дәлелдемелерді жинау мен жәбірленушілердің құқықтарын қорғаудың жаңа әдістерін әзірлеу қажеттілігі де кіреді. Бұдан басқа, ақпараттық қауіпсіздікті қамтамасыз ету мен адамның құқықтары мен бостандықтарын, оның ішінде жеке өмірге қол сұғылмаушылық пен сөз бостандығын қорғау қажеттілігі арасындағы тепе-теңдікті сақтау мәселесі бар. Киберқылмыстардың алдын алу және жолын кесу жөніндегі іс-шараларды әзірлеу азаматтық құқықтар мен бостандықтарды негізсіз шектеуге әкелмеуі керек. Осылайша, киберқылмыстың алдын алудағы анықталған қайшылықтар мен шешілмеген мәселелер заңнамалық базаны қайта қарауды және бейімдеуді, сондай-ақ халықаралық ынтымақтастықты дамытуды, құқық қорғау тетіктерін және сот жүйесін, сондай-ақ құқық қорғау механизмдерін нығайтуды қамтитын кешенді тәсілді талап етеді.

Қазақстан Республикасының Президенті Қасым-Жомарт Тоқаевтің 2024 жылғы 2 қыркүйектегі «Әділетті Қазақстанның экономикалық серпіні» тақырыбындағы Қазақстан халқына Жолдауы Қазақстанның қазіргі саяси, әлеуметтік-экономикалық дамуының басты бағыттарын көрсетеді және цифрлық трансформация, қауіпсіздік және экономикалық даму мәселелерін қамтиды, бұл зерттеу жұмысының өзектілігін айқындайды. Сонымен қатар, киберқауіптерге қарсы жаңа шараларды қабылдау қажеттілігі осы диссертациялық зерттеудің маңыздылығын арттырады [1]. Жолдаудағы негізгі бағыттарды ескеріп, киберқауіпсіздік мәселелерімен қалайша тиімді күресуге болатынына баса назар аударылды. Жолдауда цифрлық трансформация мен ақпараттық қауіпсіздікті күшейту туралы айтылғаны тікелей диссертациялық зерттеуге қатысты. Ел экономикасын цифрландыру, жаңа технологияларды енгізу және ақпараттық қауіпсіздікті қамтамасыз ету арқылы киберқылмыспен күрестің жаңа қадамдарын әзірлеу қажеттілігі көрсетілген. Жолдаудың мазмұнына сүйене отырып, Қазақстанның цифрлық экономикасын дамыту және осы саладағы қылмыстық құқық бұзушылықтармен күресу маңыздылығы нақты көрініс тапты. Мемлекеттік және жеке секторлар арасындағы ынтымақтастықты нығайту, құқықтық базаны жетілдіру және халықтың киберқауіпсіздік туралы хабардарлығын арттыру – менің жұмысымда көтерілген негізгі мәселелердің бірі. Президенттің

киберқауіптерге қарсы тұру және заңнаманы бейімдеу қажеттілігі туралы айтқаны заңдарды жаңарту және тиімді құқықтық тетіктерді енгізу қажеттігін тағы да дәлелдей түсті.

Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген «Қазақстанның киберқалқаны» киберқауіпсіздік тұжырымдамасы негізгі құжаттардың бірі болып табылады. Бұл құжат саладағы мемлекеттік саясаттың негізгі бағыттарын айқындайды. Электрондық ақпараттық ресурстарды, ақпараттық жүйелерді және телекоммуникация желілерін қорғау, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шаралар кешенін белгілейді. «Қазақстанның киберқалқаны» тұжырымдамасы заманауи сын-қатерлер мен қауіп-қатерлерді ескеретін тұрақты және бейімделген ақпараттық қауіпсіздік жүйесін құру қажеттілігіне баса назар аударады. Ақпараттық қауіпсіздік мониторингі, сондай-ақ ақпараттық қауіпсіздік инциденттерінің алдын алу және жедел әрекет ету тетіктерін әзірлеу маңызды аспект болып табылады. Тұжырымдамада киберқауіпсіздікті қамтамасыз етудің бірыңғай тәсілі қарастырылған, ол мемлекеттік және жеке ақпараттық ресурстарды қорғауды қамтиды. Осы тұжырымдама зерттеудің тақырыбы үшін құқықтық және стратегиялық негіз болып табылады және киберқауіпсіздік саласындағы ұлттық саясатты жетілдіру қажеттілігін көрсетеді [2].

Дегенмен, технологияның қарқынды дамуын және қылмыскерлер қолданатын үнемі өзгеріп отыратын әдістерді ескере отырып, қолданыстағы заңдар мен ережелер үнемі жаңартылып, бейімделуді талап етеді. Бұл жаңа міндеттерге жауап беру үшін бірнеше рет түзетілген Тұжырымдамаға өзгерістер енгізу қажеттілігімен расталады.

«Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасын» бекіту туралы ҚР Президентінің 2021 жылғы 15 қазандағы №674 Жарлығымен де байланысты. Бұл құжат елдің құқықтық жүйесін жаңғыртуға және цифрлық трансформация жағдайында құқықтық реттеуді жетілдіруге бағытталған [3]. Ақпараттық кеңістіктегі қылмыстық құқық бұзушылықтарға қарсы күрес бойынша құқықтық шараларды күшейту және жаңа технологияларға бейімделу қажеттілігі осы диссертациялық жұмыстың негізгі міндеттерімен үйлеседі.

Диссертациялық зерттеудің өзектілігін 2020-2024 жылдар аралығындағы осы саладығы тіркелген қылмыстық құқық бұзушылықтар статистикасы да көрсетіп отыр. Статистикаға мәліметтерге жүгінсек 2020 жылы - 563, 2021 жылы - 579, 2022 жылы - 583, 2023 жылы – 557, 2024 жылдың 1-3 кварталында – 632 қылмыстық құқық бұзушылық тіркелген [4].

Бұл кезеңде киберқылмыстар санының тұрақты өсімі байқалды. Статистикалық деректер құқықтық механизмдерді күшейту және заманауи қауіп-қатерлерге қарсы іс-қимыл жасау қажеттігін айқындайды.

Сонымен қатар, технологияның қарқынды дамуы және әлеуметтік тәжірибенің өзгеруі құқықтық жүйеге үнемі жаңа міндеттер қояды, олар қазіргі

уақытта қылмыстық заңнаманы және оны кеңінен қолдану тәжірибесін бейімдеуді талап етеді. Зерттеудің маңыздылығы ақпараттық саладағы қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық және криминологиялық сипаттамаларына жүйелі талдау жасау, олардың даму тенденцияларын анықтау, сондай-ақ мұндай қылмыстық құқық бұзушылықтардың алдын алу және оларға қарсы күресудің тиімді шараларын әзірлеу қажеттілігінде. Осылайша, бұл зерттеудің өзектілігі ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар мәселесінің жоғары әлеуметтік маңыздылығымен ғана емес, сонымен бірге оларды реттеу мен күресудің ғылыми негізделген әдістерін әзірлеу қажеттілігімен де анықталады.

Жоғарыда айтылған жағдайлардың барлығы диссертациялық зерттеудің өзектілігі мен тақырыпты таңдаудың қажеттілігін анықтаған.

Ғылыми мәселенің зерттеудің қазіргі деңгейі. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың ғылыми мәселесін зерттеу дәрежесі заң қоғамдастығы, криминологтар мен ақпараттық технологиялар саласындағы мамандардың үлкен қызығушылығын көрсетеді. Бірқатар ғылыми жұмыстар мен зерттеулер ақпаратқа рұқсатсыз қол жеткізуге байланысты қылмыстық құқық бұзушылықтарды саралаудан бастап, кибертерроризм мен интернет-алаяқтық мәселелеріне дейін осы мәселенің әртүрлі аспектілерін қарастырады. Зерттеудің маңызды бөлігі цифрлық ортадағы қылмыстық құқық бұзушылықтар үшін жауапкершілікті реттейтін заңнаманы талдау, сондай-ақ халықаралық тәжірибе мен құқық бұзушылықтың осы түріне қарсы күрес тәжірибесін зерделеу болып табылады.

Алайда, тергеу тәжірибесі көрсеткендей, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды саралау барысында айтарлықтай қиындықтар бар, олар әлі күнге дейін шешімін таппаған.

Біріншіден, технологияның қарқынды дамуы тергеушілер дайындағының төмендігі салдарынан және ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды көздейтін нормалардың барлығы бланкеттік сипатта болғанына байланысты бір жағынан қиындық тудырса, екінші жағынан құқықтық актілерде әлі сипатталмаған қылмыстық құқық бұзушылықтардың жаңа түрлері саралауды қиындатады. Екіншіден, киберқылмыспен күресу әдістерін біріздендіруге бағытталған халықаралық стандарттар мен келісімдерді әзірлеу міндеті өзекті болып қала береді.

Ғылыми жұмыста қылмыстық ахуалды талдауға, киберқылмысқа қатысы бар қылмыскерлердің мотивтері мен психологиясын зерттеуге ерекше көңіл бөлінеді, бұл киберқылмыстың алдын алу мен күресудің мақсатты әдістерін жасауға мүмкіндік береді. Сондай-ақ ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға тиімді әрекет ету үшін қажетті білімі мен технологиясы бар мамандандырылған құқық қорғау бөлімшелерін құру қажеттігі талқыланды. Осылайша, жүргізілген зерттеулердің айтарлықтай көлеміне қарамастан, ақпараттандыру және байланыс саласындағы қылмыстық құқық

бұзушылықтар тақырыбы одан әрі терең талдауды және оны зерттеу мен реттеудің кешенді тәсілдерін әзірлеуді талап етеді, бұл одан әрі ғылыми әзірлемелердің өзектілігі мен маңыздылығын көрсетеді.

Тақырыптың зерттелу деңгейі. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар туралы диссертациялық зерттеудің теориялық негіздері шетелдік және қазақстандық ғалымдардың еңбектеріне негізделген. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды қылмыстық құқықтық теориясында: А.Н. Ағыбаев, И.Ш. Борчашвили, Ү.С. Жекебаев, Е.І. Қайыржанов, Bossler, A.M.,Graham R.S., Smith S.K. С.М. Рахметов, К.Ж. Балтабаев сияқты ғалымдардың еңбектеріндегі құнды материалдар толық зерттелді. Ақпараттық заңнаманың тарихи дамуын зерттеген Е.В. Горбачева, Е.В. Середа, Н.А. Чесноков құқық қорғау органдарының цифрлық трансформациясына талдау жасады. Д.М. Беров пен В.В. Бычков., С.В. Харченко киберқылмыспен күресу үшін заңнаманы жетілдіру қажеттігін атап өтті. В.Бабанина Ткаченко И., Матиушенко О., Крутевич М. , Матвеев В., Никитченко О.Е., Стефанова Н., Хрипко С., Ищук А., Паско К. авторлардың эмпирикалық зерттеулері заманауи киберқылмыстарды және олармен күресу әдістерін талдаса, А.Фарсани, М.Думчиков сияқты авторлар бұл қылмыстық құқық бұзушылықтардың криминологиялық аспектілерін зерттейді. Дж.Б. Ақшатаева, А.Ж. Байдалы, А.П. Пернебекова, Сәулен Н., Жамбаев Е.С., Сағадиев А.Н., Рүстемова Г.Р., Ерғалиев С.М., Байжанов Қ.Т. Есенғазиев М.Ә., Қ.Аратұлы, Өтебеков С.Қ.,Темиралиев Т.С., Омаров Е.А. сияқты Қазақстандық ғалымдардың қосқан үлесі – Қазақстандағы киберқылмыстың ерекшеліктерін және ақпараттық қауіпсіздікті қамтамасыз етудің құқықтық шараларын талдау және цифрландыру жағдайында заңнаманы жетілдіру жолдарын ұсыну. Бұл жұмыстар халықаралық және ұлттық тәжірибені біріктіре отырып, киберқылмыспен күресудің тиімді шараларын әзірлеуге теориялық және эмпирикалық негіз береді.

Алайда, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар бағытындағы қылмыстық-құқықтық және криминологиялық аспектілерін ашатын бірде бір докторлық диссертациялық жұмыс жоқтың қасы. Көрсетілген әрбір ғылыми зерттеуде ақпараттық және коммуникация саласындағы қылмыстық құқық бұзушылықтардың белгілі бір түрлері немесе әр тұстары зерттелінген.

Сондықтан, киберқылмысқа қарсы іс қимыл мәселесі өзекті болып тұрған заманда, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың қылмыстық – құқықтық және криминологиялық аспектілерін жан жақты зерттеуге негіз бар және ұсынылыған қарсы іс-қимыл шаралары, тұжырымдар тәжірибелік маңыздылығы жоғары сипат алуда.

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.

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 гипотезасын тұжырымдау деректерді талдау мен түсіндірудің бағытын анықтайтын ғылыми зерттеудің негізгі нүктесі болып табылады. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерделеу кезінде құқықтық тетіктердің тиімділігі мен қылмыс деңгейінің арақатынасына ерекше назар аударылады. Осыған сүйене отырып, біз келесі зерттеу гипотезасын тұжырымдай аламыз:

Егер ақпараттандыру және байланыс саласындағы құқықтық тетіктер жетілдірілсе, *онда* осы саладағы қылмыстық құқық бұзушылық деңгейінің төмендеуіне әкеледі.

Киберкеңістіктің заманауи жағдайларына бейімдеу киберқылмыспен күрестің тиімділігін айтарлықтай арттырады деген болжамға негізделген. Бұл қылмыстық кодексе және басқа да нормативтік құқықтық актілерге өзгертулер енгізумен қатар, тергеу әдістерін жаңарту, құқық қорғау органдары қызметкерлерінің біліктілігін арттыру, трансұлттық киберқылмыспен бірлесіп күресу жөніндегі халықаралық келісімдерді әзірлеуді қамтиды.

Осы гипотезаны тексерудің бөлігі ретінде келесі аспектілер талданады деп күтілуде:

- Ақпараттандыру және байланыс саласындағы заңнамалық және құқық қолдану өзгерістерін киберқылмыс деңгейінің динамикасымен салыстыру.
- Ақпараттандыру және байланыс саласындағы құралдары, сандық

криминалистикалық әдістер енгізудің қылмыстық құқық бұзушылықтарды тергеу тиімділігіне әсерін зерттеу.

- Трансшекаралық киберқылмыс деңгейіне әртүрлі елдердің құқық қорғау органдары арасындағы халықаралық ынтымақтастық пен ақпарат алмасудың әсерін бағалау.

- Оларды жетілдірудің және қазіргі ақпараттық қоғамның сын-қатерлеріне бейімделудің негізгі бағыттарын анықтауға мүмкіндік береді.

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 ақпаратттандыру 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 ақпаратттандыру 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 коммуникация 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 ұсынамыз. 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 айналуда 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 процедулар 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 нәтижелерінің дәлелділігі мен негізділігі: Осы зерттеу нәтижелерінің негізділігі мен сенімділігін қамтамасыз ету үшін ғылыми әдебиеттерге мұқият талдау жүргізілді, зерттеу әдістерінің кешені қолданылды және алынған мәліметтердің статистикалық негіздемесі жүргізілді. Мұның бәрі зерттеу нәтижелерінің зерттеу мақсатына сәйкес келуін қамтамасыз етті, сонымен қатар мүмкін болатын қиғаштықтар мен қателерді азайтуға, олардың ғылыми және тәжірибелік құндылығын растайтын зерттеу қорытындыларының негізділігі мен

сенімділігін қамтамасыз етуге мүмкіндік берді.

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.

Кіріспеде зерттеу тақырыбының өзектілігі дәлелденеді, ғылыми аппарат: нысаны, пәні, мақсаты, болжамы, міндеттері, жетекші идеясы, теориялық негіздері, зерттеу көздері, әдістері, негізгі кезеңдері мен негіздері, қорғауға ұсынылатын негізгі қағидалары,ғылыми жаңалығы көрсетіледі және теориялық және тәжірибелік маңыздылығы, нәтижелерінің дәлелдігі және негізділігі.

Қорытындыда зерттеудің негізгі қағидаларын тұжырымдалып, ғылыми-әдістемелік ұсыныстар беріледі.

Зерттеу нәтижелері Қазақстан Республикасында киберқауіпсіздікті қамтамасыз ету және ақпараттық инфрақұрылымды қорғау бойынша жаңа тетіктерді енгізу қажеттігін көрсетеді.

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

1 ТАРАУ АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ ДАМУ ГЕНЕЗИСІ

1.1 Ақпараттандыру және байланыс саласында жасалатын қылмыстық құқық бұзушылықтар үшін жауаптылықтың тарихи аспектілері

Ақпараттық технологиялардың қарқынды дамуы өткен ғасырдың екінші жартысынан басталғанымен, бұл саламен байланысты қылмыстық құқық бұзушылықтардың қалыптасуының айтарлықтай тарихы жоқ. Дегенмен, технологиялардың қарқынды дамуының әр кезеңінде жаңа құқық бұзушылықтар пайда болып, олар үшін жауапкершілік белгіленетін қылмыстық нормалар қалыптаса бастады. Бұл құқық бұзушылықтар ақпараттық жүйелерді, байланыс құралдарын және ақпаратты қорғау қажеттілігінен туындады.

1. Ең алғашқы құқық бұзушылықтар мен телекоммуникация саласындағы заң бұзушылықтар (1960-1970 жылдар):

1960-1970 жылдары телекоммуникация саласындағы құқық бұзушылықтар технологиялық революцияның алғашқы толқынының нәтижесінде пайда болды. Телефон байланысы осы кезеңдегі негізгі коммуникация құралдарының бірі болды және оның дамуы жаңа қылмыстық мүмкіндіктерді тудырды. Сол кезде құқықтық жүйе телефон жүйелері арқылы жасалатын құқық бұзушылықтарға қарсы тиімді жауап қайтаруға дайын болмады, бұл телефон алаяқтықтары мен заңсыз тыңдау әрекеттерінің таралуына себепші болды.

Телефон алаяқтығының (Phreaking) эволюциясы

Телефон алаяқтығы тек телефон жүйелерін бұзып, тегін қоңыраулар шалумен шектелмеді. Бұл қылмыстық құқық бұзушылықтың түрі күрделеніп, техникалық құралдарды қолдана отырып, телефон жүйелеріне терең қол жеткізуге мүмкіндік беретін әртүрлі әдістерді дамыта бастады. Алаяқтар телефон жүйелерін бұзып, шетелге тегін қоңырау шалып қана қоймай, жүйелердегі қауіпсіздік шараларын айналып өтіп, коммерциялық және мемлекеттік байланыстарға да қол жеткізді [5].

Phreaking-тің маңызды құралдары:

Black Box – телефон жүйелеріндегі сигналдар мен деректерді өзгерту арқылы қоңырауларды бақылауды болдырмайтын қарапайым құрылғы. Бұл құрылғы алаяқтарға қоңырауларды тегін және бақылаусыз жасауға мүмкіндік берді.

Red Box – мұнда қоңырау ақысы төленген сияқты жалған сигналдар жіберіліп, қоңыраулар тегін жүргізілетін еді. Бұл әдіс әсіресе монетамен жұмыс істейтін телефондарда кеңінен қолданылды.

Бұл алаяқтықтар байланыс компанияларына үлкен қаржылық шығын келтіріп, қылмыстық құқық жүйелерін оларды реттеуге мәжбүр етті. Осы кезеңде phreaking қылмыстық субмәдениетке айналды және оның өкілдері өздерін тек алаяқтар емес, сонымен бірге телефон жүйелерін зерттеп, олардың осал тұстарын анықтайтын техникалық сарапшылар ретінде де қарастырды. Олар арнайы

жабдықтар жасап, өзара ақпарат алмасып, телефон жүйелерін бұзудың жаңа әдістерін дамытты.

Құпия тыңдау мен рұқсатсыз кірудің құқықтық салдары

Байланыс арналарын рұқсатсыз тыңдау және оларды заңсыз пайдалану сол кезеңде де елеулі мәселеге айналды. Құпия тыңдау, әсіресе саяси және коммерциялық мақсаттарда, сол кезеңнің қоғамында үлкен алаңдаушылық туғызды. Бұл қылмыстық құқық бұзушылықтар тек жеке тұлғалардың құқықтарын бұзып қана қоймай, сонымен қатар мемлекеттік құпияларға да қауіп төндірді.

Құпия тыңдау әдістері:

Wiretapping (сымға тыңдау құрылғыларын қосу) – байланыс желілеріне тікелей физикалық қол жеткізу арқылы жеке және қызметтік қоңырауларды тыңдау әдісі. Бұл әдіс қылмыскерлерге немесе бәсекелестерге конфиденциалды ақпараттарға қол жеткізуге мүмкіндік берді.

Электрондық тыңдау – сол кездегі жаңадан пайда болған байланыс құралдары арқылы берілетін сигналдарды бұзуға мүмкіндік беретін техникалық құрылғыларды қолдану. Бұл әдіс әсіресе шпиондық және тыңшылық операцияларда кеңінен қолданылды.

1960-1970 жылдардағы заңнамалық реформалар

Телефон алаяқтығы мен байланыс желілеріне рұқсатсыз кіру қылмыстық әрекеттеріне қарсы шаралар қабылдау қажеттілігі арта түсті. Осы құқық бұзушылықтардан кейін құқық қорғау органдары мен заң шығарушы органдар нақты құқықтық негіздерді қалыптастыруға бағытталды.

АҚШ-та қабылданған заңдар:

1968 жылғы «Оның Заңды Сәйкестендіруін Қорғау Актісі» – телефон желілеріне рұқсатсыз қол жеткізу әрекеттеріне қарсы алғашқы заңдардың бірі. Бұл заң бойынша телефон алаяқтары қылмыстық жауапкершілікке тартылды. Сонымен қатар, телефон жүйелерін заңсыз пайдалану жағдайлары арнайы құқық қорғау органдарының назарында болды.

Халықаралық деңгейде: басқа елдерде де телекоммуникация желілерін қорғау қажеттілігі арта бастады. Алайда, сол кезеңде байланыс жүйелері халықаралық деңгейде біріктірілмегендіктен, әр елдің заңдары әртүрлі сипатта болды.

Телефон алаяқтығының салдары мен оны болдырмауға арналған шаралар

Телефон жүйелерін заңсыз пайдалану компаниялар мен үкіметтер үшін үлкен шығындарға әкелді. Байланыс операторлары алаяқтық әрекеттердің қаржылық салдарын азайту үшін түрлі техникалық және құқықтық шараларды қолданды. AT&T сияқты ірі компаниялар жүйелерін қорғау үшін қосымша қауіпсіздік шараларын енгізді, соның ішінде:

Жүйелік сигналдарды шифрлау.

Байланыс арналарына қосылу мүмкіндігін шектеу.

Байланыс операторларына құқық бұзушылықтарды анықтау құралдарын беру [6].

Сонымен қатар, құқық қорғау органдары телекоммуникация жүйелерін қорғау бойынша мамандандырылған бөлімдер құрды. Бұл бөлімдер телефон жүйелерін бұзатын және заңсыз тыңдайтын алаяқтарға қарсы күрес жүргізді.

Құқықтық жауапкершіліктің эволюциясы

1960-1970 жылдардағы құқықтық шаралар телефон алаяқтығы мен рұқсатсыз кіруге қарсы алғашқы қадамдар болды. Телефон желілерін қорғау қажеттілігіне байланысты көптеген елдер өз заңнамаларын жаңартуға мәжбүр болды. Телефон алаяқтығы жаңа қылмыстық құқық бұзушылық түрлерінің бірі ретінде қарастырылып, қылмыстық кодекстерге енгізіле бастады. Бұл кезеңде телекоммуникация жүйелеріне заңсыз қол жеткізгені үшін қылмыстық жауапкершілік енгізіліп, заңнамалық негіздер күшейтілді.

1960-1970 жылдары телекоммуникация саласындағы құқық бұзушылықтар алғашқыда техникалық алаяқтықтар мен телефон жүйелеріне рұқсатсыз қол жеткізу арқылы көрініс тапты. Телефон алаяқтығы сол кезеңнің басты мәселелерінің бірі болды, және бұл құқық бұзушылықтарға қарсы алғашқы заңнамалық шаралар қабылданды. Алайда, бұл тек қылмыстық құқық бұзушылықтардың басы болды, ал кейінгі кезеңдерде компьютерлік және интернет қылмыстарының кеңінен таралуына байланысты телекоммуникация саласындағы құқық бұзушылықтар күрделене түсті.

2. Компьютерлік жүйелердің дамуы және алғашқы компьютерлік қылмыстық құқық бұзушылықтар (1980-1990 жылдар):

1980-1990 жылдары ақпараттық технологиялар қарқынды дамып, компьютерлік жүйелер өмірдің көптеген салаларына ене бастады. Осы кезеңде компьютерлік қылмыстық құқық бұзушылықтар пайда болып, олар телекоммуникация саласындағы құқық бұзушылықтардың жаңа кезеңіне айналды. Компьютерлік жүйелердің дамуы жеке тұлғалар мен ұйымдарға жаңа мүмкіндіктер ғана емес, сондай-ақ ақпараттық қауіпсіздікке жаңа қатерлер де әкелді [7].

Компьютерлік қылмыстық құқық бұзушылықтардың пайда болуы

Компьютерлік жүйелердің кең таралуы жаңа құқық бұзушылықтардың дамуына ықпал етті. Енді қылмыскерлер тек телекоммуникация құралдарын ғана емес, сонымен қатар деректерді өңдеу және сақтау жүйелерін де нысанаға алды. 1980-ші жылдардың басында компьютерлік қылмыстық құқық бұзушылықтардың алғашқы түрлері пайда бола бастады. Олар жүйелерді бұзу, деректерді заңсыз алу, вирустар тарату секілді әртүрлі формаларда көрініс тапты.

Негізгі компьютерлік қылмыстық құқық бұзушылықтар:

Компьютерлік жүйелерді бұзу (Hacking) – компьютерлік жүйелерге рұқсатсыз кіру немесе оларды заңсыз басқару.

Деректерді ұрлау – ұйымдар мен жеке тұлғалардың маңызды ақпараттарын заңсыз алу және оны пайдалану.

Компьютерлік вирустарды тарату – зиянды бағдарламалар арқылы компьютерлік жүйелерге шабуыл жасау.

Моррис құрт бағдарламасы (Morris Worm) – алғашқы ірі компьютерлік қылмыстардың бірі

Компьютерлік қылмыстардың ең алғашқы және ең танымал түрлерінің бірі Моррис құрт бағдарламасы (Morris Worm) болып саналады. 1988 жылы АҚШ-та Корнелл университетінің студенті Роберт Моррис интернет арқылы таралатын зиянды құрт бағдарламасын жасап шығарды. Бұл бағдарлама интернет арқылы көптеген компьютерлерге таралып, мыңдаған компьютерлік жүйелердің жұмысын тоқтатты немесе бұзды.

Моррис құрт бағдарламасының ерекшеліктері:

Құрт бағдарламасы компьютерлік желілерді зақымдап, интернеттің алғашқы кезеңінде кең таралды.

Бағдарламаның зияндылығы оны автоматты түрде басқа компьютерлерге тарату қабілеті болды. Яғни, бір компьютер зақымдалса, ол өз кезегінде басқа компьютерлерге құрт бағдарламасын жіберіп отырды.

Бұл оқиға интернет желісіне және компьютерлік жүйелерге деген сенімділікті әлсіретіп, киберқауіпсіздік мәселесін алдыңғы қатарға шығарды.

Моррис құрт бағдарламасының салдары:

Роберт Моррисқа қатысты қылмыстық іс қозғалып, ол АҚШ-та алғашқы Компьютерлік алаяқтық және құқық бұзушылықтар туралы Заң (Computer Fraud and Abuse Act, CFAA) бойынша жауапкершілікке тартылды.

Бұл оқиға компьютерлік қылмыстарға қарсы заңнаманың күшеюіне себепші болды және АҚШ-та ақпараттық қауіпсіздікке қатысты алғашқы елеулі заңнамалық өзгерістерге әкелді.

АҚШ-та 1986 жылы қабылданған Computer Fraud and Abuse Act (CFAA) заңы ақпараттық жүйелерге рұқсатсыз қол жеткізуге қарсы ең маңызды заңдардың бірі болды. Бұл заң рұқсатсыз кіру және деректерді заңсыз пайдалану сияқты әрекеттерді қылмыстық құқық бұзушылық ретінде тануды енгізді [8].

1980-1990 жылдардағы компьютерлік қылмыстардың басқа да маңызды оқиғалары

1. Компьютерлік жүйелерді бұзу және деректерді ұрлау: Компьютерлік жүйелердің дамуы қылмыскерлерге коммерциялық және мемлекеттік деректерді ұрлауға мүмкіндік берді. Жеке тұлғалар мен ұйымдардың компьютерлік жүйелерін бұзып, олардан құпия ақпараттарды, қаржылық деректерді, зияткерлік меншік құжаттарын алу жиі кездесетін қылмыстық әрекеттердің біріне айналды.

Мысал:

Кевин Митник (Kevin Mitnick) – әлемдегі ең танымал хакерлердің бірі. 1980-ші жылдардың соңында Митник бірнеше корпорацияның компьютерлік жүйелеріне рұқсатсыз кіріп, олардың маңызды құпияларын ұрлаған. Ол техникалық жүйелерді бұзып қана қоймай, әлеуметтік инженерия әдістерін де қолданып, компаниялардың құпия деректеріне қол жеткізді. Митник 1995 жылы тұтқындалғаннан кейін компьютерлік қауіпсіздікке қатысты шаралар айтарлықтай күшейтілді.

2. Компьютерлік вирустардың таралуы: Компьютерлік вирустардың таралуы да осы кезеңде кең етек жайды. Вирустар компьютерлердің жұмысын бұзатын, деректерді бүлдіретін және ақпараттарды заңсыз алуға бағытталған бағдарламалар болды. Вирустардың таралуы компьютерлерді пайдаланушыларға ғана емес, сонымен қатар бүкіл компаниялар мен ұйымдарға үлкен шығындар келтірді.

Мысал:

«Brain» вирусы – бұл әлемдегі ең алғашқы компьютерлік вирустардың бірі болып саналады. 1986 жылы екі пакистандық программист жасаған бұл вирус компьютерлік дискілерге таралып, деректерді зақымдады. Вирус дискілерді көшірмелеу кезінде іске қосылып, басқа компьютерлерге тарала бастады. Бұл оқиға вирусқа қарсы бағдарламаларды дамыту қажеттілігін көрсетті.

Халықаралық заңнамалық шаралар

Компьютерлік қылмыстардың халықаралық деңгейде таралуы көптеген елдерді ақпараттық жүйелерге қарсы құқық бұзушылықтарға қатысты қатаң заңнамалар қабылдауға мәжбүр етті. Сол кезеңде әлемнің көптеген елдерінде компьютерлік қылмыстарды анықтайтын және олармен күресетін заңдар қабылданды [9].

Мысалдар:

1986 жылы АҚШ-та қабылданған Computer Fraud and Abuse Act (CFAA) заңы компьютерлік жүйелерге рұқсатсыз қол жеткізуге қарсы ең маңызды заңдардың бірі болды.

1990 жылы Ұлыбританияда Computer Misuse Act қабылданды, бұл заң бойынша компьютерлік жүйелерге рұқсатсыз кіру, деректерді ұрлау және зиян келтіру құқық бұзушылықтары қылмыстық жауапкершілікке тартылатын болды.

Қазақстандағы компьютерлік қылмыстық құқық бұзушылықтар және заңнамалық шаралар

Қазақстанда да 1990-шы жылдардың соңында компьютерлік қылмыстарға қарсы заңнамалық шаралар қабылдана бастады. Қазақстан Республикасының Қылмыстық кодексіне ақпараттық жүйелерге рұқсатсыз қол жеткізу, компьютерлік жүйелерді бұзу, ақпараттарды заңсыз алу және зиянды бағдарламалық жасақтаманы тарату сияқты қылмыстық құқық бұзушылықтарды қылмыстық жауапкершілікке тарту үшін арнайы баптар енгізілді. Сонымен қатар, компьютерлік қылмыстардың алдын алу мақсатында ұлттық заңнаманы халықаралық нормалармен сәйкестендіру қолға алынды.

1980-1990 жылдары компьютерлік жүйелердің дамуы мен таралуы қылмыстық құқық бұзушылықтардың жаңа түрлерінің пайда болуына ықпал етті. Компьютерлік қылмыстар осы кезеңде кең таралып, қоғам мен бизнеске үлкен қауіп төндірді. Алғашқы ірі компьютерлік қылмыстардың бірі – Моррис құрт бағдарламасы – ақпараттық қауіпсіздікке деген көзқарасты түбегейлі өзгертті. Бұл кезеңде көптеген елдер компьютерлік қылмыстарға қарсы күресуге арналған арнайы заңдарды қабылдап, ақпараттық жүйелерді қорғауға бағытталған жаңа технологияларды дамыта бастады [10].

3. Интернеттің таралуы және жаңа қылмыс түрлері (1990-2000 жылдар):

1990-2000 жылдар аралығында интернеттің жаһандық таралуы ақпараттық технологиялар саласындағы қылмыстардың жаңа кезеңін ашты. Бұл кезеңде интернет қылмыстары кеңінен таралып, құқық қорғау органдары мен заңнамалық жүйелерге жаңа қиындықтар туғызды. Интернеттің кеңінен таралуы қылмыстық әрекеттердің түрлері мен ауқымын едәуір арттырды, соның нәтижесінде киберқылмыс ұғымы пайда болды.

Интернеттің таралуы және оның қылмыстық құқық бұзушылықтарға әсері

Интернеттің таралуы әлемдік деңгейде жаңа байланыс, ақпарат алмасу және сауда құралдарын ұсынды. Алайда, оның ашық және жаһандық табиғаты жаңа қылмыс түрлерінің пайда болуына да ықпал етті. 1990-шы жылдары интернет қылмыстарының кеңінен таралуына интернет арқылы жасалатын заңсыз әрекеттер, алаяқтық, құпия ақпараттарды ұрлау және зияткерлік меншік құқықтарын бұзу секілді қылмыстар жатады.

Интернет қылмыстарының таралуы заңсыз әрекеттердің трансұлттық сипат алуына мүмкіндік берді, себебі интернет арқылы жасалатын қылмыстар белгілі бір шекаралармен шектелмеді. Қылмыскерлер басқа елдердегі адамдарды алдап, жеке деректерді ұрлап немесе заңсыз ақпарат тарата алатын болды.

Интернет қылмыстарының негізгі түрлері

Интернет-алаяқтық

Интернет арқылы жасалатын алаяқтықтар 1990 жылдары кеңінен тарала бастады. Алаяқтар интернет арқылы жалған сайттар құрып, заңсыз тауарлар мен қызметтерді сату, несие карталарын ұрлау, жалған ұсыныстар жасау секілді қылмыстық құқық бұзушылықтарды жүзеге асырды.

Мысалдар:

Аукцион алаяқтығы – алаяқтар интернет-аукциондарда жалған тауарларды сату арқылы адамдарды алдап, олардан ақша жинайтын. Тауарлар ешқашан жеткізілмейтін немесе сапасыз болатын.

Нигериялық хаттар алаяқтығы (Nigerian Scam) – бұл алаяқтықтың түрі электрондық пошта арқылы таралатын және қаражат немесе жеке ақпаратты ұрлауға бағытталған әрекеттер болып табылатын. Алаяқтар өздерін банк қызметкерлері немесе бай мұрагерлер ретінде таныстырып, қаражат сұрайтын.

Фишинг (Phishing)

Фишинг – бұл интернет арқылы құпия деректерді, атап айтқанда, банк шоттары, кредит карталарының деректері және жеке құпия сөздерді ұрлау мақсатында жасалатын қылмыстық әрекет. Фишингтік шабуылдар арнайы жалған сайттар немесе электрондық хаттар арқылы жүзеге асырылады. Бұл әдіс қылмыскерлерге заңсыз пайда табу үшін пайдаланушылардың жеке ақпаратын алуға мүмкіндік береді [11].

Фишинг әдістері:

Алаяқтар заңды банктердің немесе ұйымдардың атынан жалған хаттар немесе сайттар жіберіп, пайдаланушылардан құпия ақпараттарын беруін талап етеді.

Электрондық пошталар арқылы жіберілген жалған сілтемелер пайдаланушыларды зиянды сайттарға апарып, құпия деректерін ұрлайды.

Кибершабуылдар

1990-шы жылдары интернеттің кеңінен таралуымен бірге кибершабуылдар саны да артты. Кибершабуылдар компьютерлік жүйелерді, желілерді және серверлерді бұзу немесе зақымдау арқылы жүзеге асырылды. Бұл шабуылдар деректерді ұрлау, жүйелерді істен шығару немесе оларды заңсыз бақылауға алу мақсатында жасалды.

Танымал кибершабуылдардың түрлері:

DDoS (Distributed Denial of Service) шабуылдары – бұл шабуылдар интернет-серверлерге көп мөлшерде сұраныстар жіберу арқылы олардың жұмысын тоқтатуға бағытталған. Аталмыш шабуылдар компаниялардың серверлерін уақытша істен шығарып, қаржылық шығындарға ұшыратты [12].

Зиянды бағдарламаларды тарату – интернет арқылы таралатын вирустар, трояндық бағдарламалар және басқа да зиянды бағдарламалар компьютерлік жүйелерге зақым келтіріп, деректерді ұрлау немесе оларды жоюға бағытталған.

Зияткерлік меншік құқықтарын бұзу

Интернет арқылы зияткерлік меншік объектілеріне (фильмдер, музыка, бағдарламалық жасақтама, т.б.) қатысты құқық бұзушылықтар кең таралды. Пираттық контентті тарату, заңсыз көшірмелер жасау және таратуды жеңілдететін технологиялардың дамуы зияткерлік меншік құқықтарының бұзылуына алып келді.

Мысал:

Napster – бұл интернет арқылы музыкалық файлдармен заңсыз алмасуға арналған алғашқы платформалардың бірі. Napster платформасы арқылы пайдаланушылар авторлық құқықпен қорғалған музыкалық файлдарды тегін көшіріп алатын болды. 2000 жылы сот шешімі бойынша Napster қызметі заңсыз деп танылды, бірақ бұл жағдай басқа осындай платформалардың дамуына кедергі бола алмады.

Киберқылмыс пен кибершабуылдардың трансұлттық сипаты

Интернеттің жаһандық сипаты қылмыстық әрекеттердің бір елден екінші елге жылдам таралуына мүмкіндік берді. Киберқылмыстардың трансұлттық сипаты құқық қорғау органдары үшін жаңа қиындықтар туғызды, себебі қылмыскерлер басқа елдерде отырып, халықаралық заңдарды бұзатын әрекеттер жасайтын болды.

Халықаралық құқықтық шаралар

Интернет қылмыстарының жаһандық сипат алуы құқықтық жүйелерді халықаралық деңгейде ақпараттық қауіпсіздікке қатысты жаңа заңнамалар қабылдауға мәжбүр етті. 1990 жылдары бірнеше мемлекет киберқылмыстарға қарсы халықаралық ынтымақтастықты арттыратын келісімдер мен конвенциялар қабылдады [13].

Мысалдар:

2001 жылы қабылданған Будапешт конвенциясы – бұл киберқылмыстарға қарсы халықаралық деңгейде қабылданған алғашқы конвенция. Конвенцияның мақсаты – киберқылмыстарға қарсы құқықтық шараларды халықаралық деңгейде үйлестіру және оларға қарсы күресті күшейту.

Еуропа Кеңесі осы конвенция шеңберінде ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған ынтымақтастықты күшейтті. Будапешт конвенциясы көптеген мемлекеттерде киберқылмыстарға қатысты заңнаманы дамытудың негізі болды.

Киберқылмыспен күрес саласындағы халықаралық ынтымақтастықты күшейту Қазақстанның ақпараттық қауіпсіздігін қамтамасыз етудегі стратегиялық басымдықтарының бірі болып табылады. Жаһандық киберқауіптерге тиімді қарсы тұру үшін Қазақстанның халықаралық құқықтық жүйемен үйлесімді әрекет етуі және басқа елдердің құқық қорғау органдарымен тығыз ынтымақтастық орнатуы өте маңызды. Бұл бағытта бірнеше негізгі шаралар іске асырылуы қажет.

Қазақстанның Будапешт конвенциясына қосылуы халықаралық ынтымақтастықты дамытудағы маңызды қадамдардың бірі болып табылады. Будапешт конвенциясы – киберқылмыстарға қарсы күрестегі алғашқы және негізгі халықаралық келісім. Оған қосылу Қазақстанға киберқылмыстарды тергеу және алдын алу барысында халықаралық стандарттарды қолдануға, басқа елдермен өзара құқықтық көмек алмасуға мүмкіндік береді. Бұл келісімнің шарттарын орындау Қазақстанның құқық қорғау органдарына киберқылмыскерлерді трансшекаралық деңгейде қудалау және олардың әрекеттерін бақылау үшін құқықтық негіз қалыптастырады.

Трансшекаралық кибершабуылдарға қарсы жедел әрекет ету үшін шетелдік серіктестермен бірлескен операциялар ұйымдастыру қажет. Бұл Қазақстанға басқа мемлекеттердің құқық қорғау органдарымен бірлесіп күрделі киберқылмыстарды ашуға және дер кезінде жауап қатуға мүмкіндік береді. Бірлескен операциялар ұйымдастыру трансшекаралық қылмыстық құқық бұзушылықтар иімді тергеуге жол ашып, кибершабуылдарды ерте кезеңде анықтауға мүмкіндік береді. Бұл бағытта INTERPOL және Europol сияқты халықаралық ұйымдармен серіктестік орнату және бірлескен операцияларды үйлестірудің маңызы зор. Сонымен қатар, кибершабуылдарға жедел әрекет ету үшін Қазақстанда халықаралық талаптарға сай жабдықталған арнайы киберқауіпсіздік бөлімшелерін құру қажет.

Киберқауіптер туралы ақпарат алмасу – халықаралық ынтымақтастықтың маңызды элементтерінің бірі. Бұл Қазақстанға жаңа киберқауіптер туралы деректерді тез қабылдап, алдын алу шараларын уақытылы жүзеге асыруға мүмкіндік береді. Мемлекеттік сектор мен жеке компаниялар арасындағы тығыз байланыс арқылы деректердің қауіпсіздігі қамтамасыз етіледі. Сонымен қатар, кибершабуылдарға қарсы күрес саласында тәжірибе алмасу және озық технологияларды қолдану Қазақстанның киберқауіпсіздік деңгейін арттырады. Ірі IT компаниялар және халықаралық ұйымдармен ынтымақтастық орнату арқылы

Қазақстан кибершабуылдарға қарсы күресте тиімді шешімдер мен технологияларға қол жеткізе алады.

Жалпы, халықаралық ынтымақтастықты дамыту киберқауіпсіздік мәселелерінде тұрақты дамуды қамтамасыз етіп, қылмыстық әрекеттерге қарсы жаһандық күресте Қазақстанның рөлін күшейтеді. Киберқылмыстарға қарсы күресте тек ұлттық шаралармен шектелу жеткіліксіз, себебі қазіргі кибершабуылдар шекараларды білмейді және бір елдің шеңберінде тоқтатуға келмейді. Сондықтан Қазақстан халықаралық ынтымақтастықты нығайту арқылы киберқылмыстарға қарсы тиімді стратегиялар мен тетіктерді қалыптастыруға тиіс.

Қазақстандағы интернет қылмыстық құқық бұзушылықтары

Қазақстанда интернет қылмыстарының таралуы 1990-шы жылдардың соңында және 2000-шы жылдардың басында байқалды. Осы кезеңде Қазақстанның Қылмыстық кодексіне ақпараттық жүйелерге рұқсатсыз қол жеткізу, интернет арқылы алаяқтық жасау, құпия деректерді ұрлау және зиянды бағдарламаларды тарату секілді қылмыстарды қылмыстық жауапкершілікке тартуға арналған баптар енгізілді [14].

Қабылданған заңнамалар:

1997 жылы Қазақстанның Қылмыстық кодексіне ақпараттық қауіпсіздікке қатысты арнайы баптар енгізілді. Бұл баптар интернет қылмыстарының алдын алуға және кибершабуылдарға қарсы күрес жүргізуге бағытталған.

1990-2000 жылдары интернеттің жаһандық таралуы ақпараттық технологияларға негізделген жаңа қылмыс түрлерінің пайда болуына ықпал етті. Интернет-алаяқтық, фишинг, кибершабуылдар және зияткерлік меншік құқықтарының бұзылуы кең таралған интернет қылмыстарының негізгі түрлеріне айналды. Бұл кезеңде киберқылмыстардың трансұлттық сипаты артып, халықаралық құқықтық шаралар қабылдана бастады. Қазақстан да бұл үрдістен тыс қалмай, ақпараттық қауіпсіздікке қатысты заңнамаларын дамыта бастады.

4. Қазіргі кезең (2000 жылдан бастап қазіргі уақытқа дейін):

2000 жылдан бастап қазіргі уақытқа дейінгі кезең интернет пен ақпараттық технологиялардың жаппай таралуымен және дамуының күрделі кезеңі болып саналады. Бұл кезеңде цифрлық технологиялар күнделікті өмірдің ажырамас бөлігіне айналып, адамдардың жеке өмірі мен бизнесі көп жағдайда интернетке тәуелді болды. Соның нәтижесінде, киберқылмыстар да жаңа сипат алып, олардың күрделілігі арта түсті. Қазіргі кезде киберқылмыстардың жаңа түрлері пайда болып, олар трансұлттық және ұйымдасқан қылмыстық топтардың негізгі саласына айналды.

Кибершабуылдардың жаңа түрлері

2000 жылдан бастап интернет қылмыстары айтарлықтай дамыды, бұл кезеңде кібершабуылдардың жаңа, күрделі түрлері пайда болды. Атап айтқанда, киберқылмыскерлер зиянды бағдарламалар, кибершабуылдар, деректерді шифрлау арқылы құнды ақпараттарды заңсыз иемденуге немесе оларды сатуға бағытталған әрекеттер жасай бастады [15].

1. Кибершабуылдардың жаңа түрлері

Кибершабуылдар және кибершпиондық

Қазіргі кезеңде кибершабуылдар кең ауқымды және ұйымдасқан сипат алды. Кибершабуылдар жеке тұлғаларға ғана емес, сонымен қатар үлкен компанияларға, үкіметтік ұйымдарға, банктерге және маңызды инфрақұрылымдарға бағытталуда. Осы шабуылдардың мақсаты ақпаратты ұрлау, оны бұзу немесе заңсыз пайдалану болды.

Мысал:

Stuxnet вирусы (2010) – бұл вирус Иранның ядролық объектілерін зақымдауға арналған зиянды бағдарлама ретінде белгілі. Stuxnet вирусы нақты мақсатқа бағытталып, өнеркәсіптік жүйелерге зақым келтіру арқылы оның жұмысын тоқтатуға бағытталған алғашқы күрделі кибершабуыл болды. Бұл шабуыл халықаралық деңгейдегі киберқылмыстардың жаңа толқынына жол ашты.

WannaCry (2017) – бұл интернет арқылы таралған вирус компьютерлік жүйелерді шифрлап, оларды құлыптап тастайтын және оларды ашу үшін төлем талап ететін бағдарлама болды. WannaCry вирусы әлемнің жүзден астам еліндегі мыңдаған ұйымдарға зиян келтірді, соның ішінде ауруханалар, банктер және мемлекеттік мекемелер бар.

Ботнеттер және DDoS-шабуылдар

DDoS-шабуылдар (Distributed Denial of Service) – бұл көптеген компьютерлерді (әдетте ботнет деп аталатын желілерді) қолдану арқылы серверлерді немесе веб-сайттарды артық жүктеп, олардың жұмысын тоқтататын шабуыл түрі. Бұл шабуылдар ірі компаниялар мен қызмет көрсетушілерге қаржылық шығын әкеліп, олардың жүйелерін уақытша істен шығарады [16].

Мысал:

Mirai ботнеті (2016) – бұл ботнет арқылы әлемнің көптеген веб-сайттары мен серверлері DDoS шабуылына ұшырады. Mirai ботнеті интернетке қосылған құрылғыларды (интернет заттары, IoT) пайдаланып, олардың осал тұстарын қолдана отырып шабуылдар ұйымдастырды. Нәтижесінде, ірі интернет қызмет көрсетушілер мен серверлер жұмысын тоқтатуға мәжбүр болды.

Кибертерроризм және киберқауіпсіздік

Кибертерроризм интернет арқылы мемлекеттік ұйымдарға, инфрақұрылымдарға немесе қоғамдық қауіпсіздікке зиян келтіруге бағытталған қылмыстық әрекеттер болып табылады. Кибертеррористік шабуылдар мемлекеттік органдардың маңызды деректерін ұрлау, бұзу немесе желілерді басқаруға бағытталған.

Мысал:

2007 жылы Эстония үкіметтік және қаржылық жүйелерге жаппай кибершабуылдар жасалды. Бұл оқиға «киберсоғыс» терминінің кеңінен таралуына себеп болды және мемлекеттерді киберқауіпсіздікке ерекше назар аударуға мәжбүр етті.

2. Зиянды бағдарламалар мен кибералаяқтық

1. Рансомвар (Ransomware)

Рансомвар деп аталатын зиянды бағдарламалар 2000 жылдардың ортасында кең тарала бастады. Рансомвар бағдарламалары компьютерлер мен жүйелерді шифрлап, пайдаланушылардан төлем талап етеді. Рансомвар шабуылдарының кең таралуы кибералаяқтықтың жаңа тәсілі болып табылады.

Мысалдар:

WannaCry және Petya вирустары рансомвар түрлеріне жатады. Бұл вирустар жүйелерді шифрлап, оларды ашу үшін биткоин немесе басқа криптовалюталар арқылы төлем талап етті.

2. Банктық алаяқтық және төлем жүйелеріне шабуылдар

Қазіргі кезде кибералаяқтар банктік жүйелер мен төлем платформаларына бағытталған шабуылдарды жиі жасайды. Бұл шабуылдар арқылы олар клиенттердің қаржылық деректерін ұрлап, заңсыз төлемдер жасайды.

Мысал:

SWIFT жүйесіне шабуылдар – бұл халықаралық банк аударымдары жүйесіне бағытталған шабуылдар. 2016 жылы SWIFT жүйесі арқылы Бангладештің орталық банкінен заңсыз аударымдар жасалып, үлкен сомада қаражат ұрланды.

3. Әлеуметтік желілер мен құпиялылыққа қатысты қылмыстық құқық бұзушылықтар [17].

Әлеуметтік желілердің дамуы интернет қылмыскерлеріне жеке деректерді ұрлау, адамдарды алдау және жалған ақпарат тарату үшін жаңа мүмкіндіктер берді. Әлеуметтік инженерия әдістерін қолданатын қылмыскерлер адамдардың сенімін пайдаланып, олардың жеке мәліметтерін немесе қаржылық ақпаратын алуға тырысады.

1. Фишинг және алдау

Қазіргі кезде әлеуметтік желілерде жасалатын фишинг шабуылдары арқылы адамдардың жеке деректері мен құпия сөздері ұрланады. Алаяқтар жалған хабарламалар мен сайттар арқылы пайдаланушылардың сеніміне кіріп, құпия ақпаратын алады.

2. Дезинформация және жалған ақпарат тарату

Әлеуметтік желілер жалған ақпарат таратудың құралына айналып отыр. Киберқылмыскерлер немесе ұйымдасқан топтар жалған ақпарат таратып, қоғамдық пікірді өзгертуге немесе дау-жанжал туғызуға тырысады. Бұл әрекеттердің салдарынан саяси немесе қаржылық тұрақсыздық пайда болуы мүмкін.

4. Криптовалюталар және блокчейн технологиясына байланысты қылмыстық құқық бұзушылықтар

Криптовалюталардың дамуы киберқылмыстардың жаңа түрлерін тудырды. Биткоин және басқа криптовалюталар анонимді және қауіпсіз болғандықтан, оларды заңсыз әрекеттер жасау үшін қолдану кеңінен таралды. Криптовалюталарды ұрлау, жалған ICO (Initial Coin Offering) жобалары арқылы

алдау, сондай-ақ биткоин төлемдерін талап ететін рансомвар шабуылдары кең етек жайды.

Халықаралық құқықтық және заңнамалық шаралар

2000 жылдан бастап киберқылмыстардың өсуіне байланысты көптеген елдер ақпараттық қауіпсіздікке қатысты заңнамаларын жаңартты және күшейтті. Сонымен қатар, халықаралық ынтымақтастық күшейіп, киберқылмыстарға қарсы күреске бағытталған келісімдер қабылданды [18].

Мысалдар:

Еуропалық Одақтың Киберқауіпсіздік директивасы (NIS Directive) – бұл директива 2016 жылы қабылданып, мүше мемлекеттерді ұлттық киберқауіпсіздік стратегияларын құруға және оларды халықаралық деңгейде үйлестіруге міндеттеді.

Жаңа технологияларға қатысты заңдар – АҚШ, Ұлыбритания және басқа да елдер киберқылмыстарға қарсы жаңа заңдар қабылдап, криптовалюталарды реттеу, деректерді қорғау және киберқауіпсіздікке қатысты талаптарды күшейтті.

Қазақстандағы киберқауіпсіздік және заңнамалық шаралар

Қазақстанда да киберқылмыстарға қарсы күрес жүргізу мақсатында заңнамалық шаралар күшейтілді. Қазақстанның Қылмыстық кодексіне ақпараттық қауіпсіздікке, деректерді қорғауға және кибершабуылдарға қатысты арнайы баптар енгізілді. Сонымен қатар, мемлекет киберқауіпсіздікті күшейту мақсатында ақпараттық жүйелерді қорғауға бағытталған іс-шаралар кешенін қабылдады.

Мысал:

2015 жылы Қазақстанда «Ақпараттандыру туралы» заң қабылданды, ол цифрлық кеңістіктегі құқықтық тәртіпті қамтамасыз етуге және ақпараттық қауіпсіздікті күшейтуге бағытталды.

Кибершабуылдарға қарсы ұлттық стратегиялар қабылданып, мемлекеттік органдардың киберқауіпсіздігін қамтамасыз ету үшін арнайы жүйелер енгізілді.

2000 жылдан бастап қазіргі уақытқа дейінгі кезеңде интернет пен ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар айтарлықтай дамыды. Кибершабуылдар, рансомвар, криптовалюталарға байланысты қылмыстық құқық бұзушылықтар және әлеуметтік желілердегі алдаулар киберқылмыстардың ең кең таралған түрлеріне айналды. Қазіргі кезде мемлекеттер киберқауіпсіздікті күшейту мақсатында жаңа заңдар қабылдап, халықаралық ынтымақтастықты арттырып жатыр. Қазақстан да бұл үдерістен тыс қалмай, киберқылмыстарға қарсы заңнамалық шараларды дамытып, ақпараттық қауіпсіздік саласындағы өз саясатын күшейтуде.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи дамуы бірнеше кезеңнен өтті. Әр кезеңде жаңа технологиялардың таралуы мен дамуымен бірге қылмыстардың жаңа түрлері пайда болып, оларға қарсы заңнамалық шаралар қабылданды. Қазіргі кезде бұл құқық бұзушылықтардың трансұлттық сипаты мен күрделілігі құқық

қорғау органдары мен заңнамалық жүйелерден жаңа тәсілдер мен әдістерді талап етеді.

Ақпараттандыру және байланыс саласында жасалған қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи аспектілері қазіргі және қарқынды дамып келе жатқан осы саланың құқықтық реттеуіндегі күрделі өзгерістерді көрсетеді. Д.М. Берованың мақаласында ақпараттық технологиялар саласындағы революциялық прогрестің нәтижесінде туындаған жаңа міндеттерге заңнаманы бейімдеу процесін көрсетеді. Автор компьютерлік ақпаратқа сұраныстың жылдам өсуіне және осы саладағы қылмыстық құқық бұзушылықтардың қатар өсуіне қарамастан, ресейлік заңнамалық база мұндай әрекеттер үшін қылмыстық жауапкершілікті реттеуде әлі де күрделі мәселелерге тап болып отырғанын атап көрсетеді. Қазіргі жағдайды талдау қолданыстағы нормативтік-құқықтық актілердің уақыт талабына толық жауап бермей, компьютерлік ақпарат саласындағы қылмыстық құқық бұзушылықтармен тиімді күресу мәселелерін ашық қалдырып отырғанын көрсетеді. Д.М. Берова цифрлық дәуірдің сын-қатерлеріне, оның ішінде жасанды интеллект жүйелерін пайдалануға қатысты заңсыз әрекеттерге барабар жауап бере алатын қылмыстық-құқықтық тетіктерді құру және дамыту қажеттілігін атап көрсетеді.

Цифрлық ақпараттың қарқынды өсуі мен заңнаманың салыстырмалы инерциясы арасындағы теңгерімсіздік қылмыстық заңнамаға уақтылы өзгерістер енгізу бойынша белсенді әрекетті талап етеді. Бұл жаңа нормаларды енгізуді ғана емес, сонымен қатар ақпараттық технологиялар мен қылмыстық құқық бұзушылықтың дамуының соңғы тенденцияларын ескере отырып, қолданыстағыларын түзетуді де қамтиды. Тарихи тұрғыдан алғанда, мақалада атап көрсетілгендей, анықталған мәселелерді шешу қылмыстық заңнаманы динамикалық өзгеретін ақпараттық ландшафтқа тұрақты талдау және бейімдеу болып табылады. Бұл тәсіл цифрлық әлемнің жаһандануы жағдайында құқықтық тәртіпті нығайтуға көмектесе отырып, ақпараттандыру және байланыс саласындағы тиімді құқықтық реттеуді қамтамасыз етеді [19].

Ақпараттандыру және байланыс саласында жасалған қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи аспектілері В.В.Бычковтың және С.В.Харченконың компьютерлік қылмыс тұжырымдамасының эволюциясы призмасы арқылы және осы саладағы құқықтық реттеуді дамыту мақаласында ашылған. Авторлар ақпараттық технологиялардың пайда болуымен және қарқынды дамуымен қоғамды реттеу мен алдын алуға ерекше көзқарасты талап ететін жаңа қылмыс түрімен бетпе-бет келгенін атап көрсетеді. Мақалада мемлекеттің ақпараттық қауіпсіздікті қамтамасыз етуге қатысты сын-қатерлерге қалай әрекет ететіні, компьютерлік қылмыспен күресу үшін қандай шаралар қабылданып жатқаны талданады. Зерттеу контекстінде заңсыз баю мақсатында компьютерлік жүйелерді пайдалана отырып жасалған экономикалық қылмыстардың айтарлықтай саны анықталған АҚШ-та 70-ші жылдардан бастап компьютерлік қылмыс туралы түсінік қалай қалыптасқанына ерекше назар

аударылады. Интерпол компьютерлік қылмыстарды, оның ішінде ақпаратқа рұқсатсыз қол жеткізуді және ұстап алуды, деректерді өзгертуді, компьютерлік алаяқтықты, заңсыз көшіруді, компьютерлік диверсияны және коммерциялық құпияны құрайтын ақпаратты ұрлаумен байланысты қылмыстардың басқа түрлерін жіктейтін арнайы кодификатор әзірледі [20].

Н.К.Қабылов ақпараттық қауіпсіздік деңгейін арттыру қажеттілігі туралы мәселені көтереді және ақпараттық-технологиялық дамудың үнемі өсіп келе жатқан көлемі жағдайында вирустар мен хакерлік шабуылдардан абсолютті қорғауды құрудың қиындығына назар аударады. Ресми статистикалық деректерді және компьютерлік қылмыстық құқық бұзушылықтардан келтірілген залалды бағалауды ескере отырып, ұйымдар мен жалпы мемлекет деңгейінде АТ (ақпараттық технологиялар) қауіпсіздігі саласындағы инновацияларды әзірлеу мен енгізудің маңыздылығы атап өтіледі. Осылайша, ақпараттық саладағы қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи аспектілері заңнаманы цифрлық революция тудырған жаңа сын-қатерлерге бейімдеудің күрделі жолын көрсетеді және барлық деңгейде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шараларды үнемі әзірлеудің өзектілігі мен қажеттілігін атап көрсетеді [21].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың дамуының генезисі туралы бөлімнің қорытындысы компьютерлік қылмыстық құқық бұзушылықпен күресу заңнамасы мен тәжірибесінің тарихи дамуына арналған зерттеулерді талдау нәтижелерін қорытындылайды.

Талдау көрсеткендей, ақпараттық қоғам мен технологияның дамуы компьютерлік қылмыстық құқық бұзушылықтан қорғауды қамтамасыз ету үшін жаңа нормалар мен қолданыстағы заңдарға түзетулер жасау қажеттілігін тудырды. Середа Е.В. мен Чесноков Н.А. зерттеген Ресей Федерациясы мен ТМД елдеріндегі прокуратура органдарының цифрлық трансформация процесі мемлекеттік органдардың киберқауіпсіздікке қатысты жаңа сын-қатерлерге бейімделуге ұмтылысын көрсетеді.

Д.М. Берова қазіргі заманғы технологиялық және ақпараттық сын-қатерлер жағдайында құқықтық реттеу мәселелерінің өзектілігін атап өтіп, компьютерлік қылмыстардың алдын алу және жазалау шараларының жеткіліксіздігін көрсетеді. Бычков В.В. пен Харченко С.В. ұсынған компьютерлік қылмыс концепциясын талдау қазіргі қоғам алдында тұрған қауіптердің ауқымы мен ерекшелігін жақсырақ түсінуге мүмкіндік береді [19, б.123].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи аспектілері өз тарихын компьютерлік технологиялар мен смартфондардың пайда болуы және кейінгі қарқынды дамуымен тұспа-тұс келген өткен ғасырдың ортасынан бастайды. Бабанина В., Ткаченко И., Матиушенко О. және Крутевич М. атап өткендей, компьютерді қолданумен байланысты алғашқы қылмыстық құқық бұзушылықтың

осы түрінің динамикасы мен эволюциясына ерекше мән беретін қазіргі киберқылмыстан айтарлықтай ерекшеленеді. Уақыт өте келе құрылғылар мен Интернет-қызметтердің көбеюі пайдаланушылар санының артуына және сәйкесінше киберқылмыстардың саны мен оларды ұйымдастыру деңгейінің артуына әкелді [22].

Авторлар киберқылмыстарды тергеп-тексеру және күресу кезінде құқық қорғау органдарының алдында тұрған мәселелерге ерекше назар аударады. «Киберқылмыс» пен «компьютерлік қылмыстар» ұғымдарының арасындағы айырмашылықтарды талдау, сондай-ақ киберқылмыстардың негізгі белгілерін анықтау осы мәселені жақсы түсінуге және осындай қылмыстық құқық бұзушылықтармен күресудің негізгі бағыттарын анықтауға, оның ішінде тиімді шараларды әзірлеуге мүмкіндік береді.

Компьютерлік қылмыстың даму тарихы 1960 жылдардан, компьютерлер қызметтің әртүрлі салаларына белсенді түрде енгізіле бастаған кезден басталады. Екінші дүниежүзілік соғыстан кейін UNIVAC сияқты коммерциялық компьютерлер шығарыла бастады, бұл киберқылмыстардың дамуының триггерлерінің бірі болды. Транзисторлық технологияның және компьютер жадысын ұйымдастырудың жаңа тәсілдерінің дамуы компьютерлердің көлемін кішірейтуге, олардың жылдамдығы мен сенімділігін арттыруға әкелді, бұл да осы құрылғыларды қылмыстық мақсатта пайдалану мүмкіндіктерін кеңейтуде маңызды рөл атқарды. Бұл өзгерістер құқықтық негіздерді үнемі өзгеретін технологиялық шындыққа және киберқылмыстың дамып келе жатқан нысандарына бейімдеу қажеттілігін көрсетеді [23].

В.Матвеев пен оның әріптестерінің мақаласында киберқылмыс терең доктриналық талдауды және тиімді қарсы әрекет құралдарын әзірлеу үшін халықаралық ынтымақтастықты қажет ететін күрделі құбылыс ретінде қарастырылады. Авторлар «киберқылмыс» терминінің танымалдығына қарамастан, оның ресми нормативтік құжаттарда нақты анықтамасы жоқ екенін, бұл ұлттық және халықаралық заңнама деңгейінде құқықтық белгісіздік тудыратынын атап көрсетеді. Қылмыстық жауапкершілікке тартылатын заңсыз әрекеттердің тізбесін үнемі жаңартып отыруды талап ететін ақпараттық технологиялардағы өзгерістердің заңнамалық реттеуден қалай озып тұрғаны талданады [24].

Авторлар киберқылмыстың жағымсыз салдарын барынша азайту үшін ұлттық заңнаманы жетілдіру және халықаралық ынтымақтастық орнату қажеттігін атап көрсетеді. Киберқылмыс шекараны білмейтіні, ал интернет желісінің жасырындығы мен шексіз мүмкіндіктерін заңсыз әрекеттерді жасау үшін пайдаланатын қылмыскерлер үшін ең танымал және сенімді баспана екені атап өтілген. Бұл халықаралық үйлестірудің және киберқылмыспен күресудің бірлескен тәсілдерін дамытудың маңыздылығын көрсетеді.

Сонымен қатар, зерттеу ақпараттық қылмыстық құқық бұзушылық жасауға мотивациялық ынталандыру бола алатын интернетте бүркеншік аттарды қолдану

құбылысына қатысты. Бүркеншік атаулар құндылықтар жүйесін, әлеуметтік жағдайды, тіпті этномәдени стереотиптерді көрсететін белгілі бір идеологиялық жүкті арқалайды. Бұл аспектілер виртуалды кеңістікте өзін-өзі тану мен мінез-құлықтың жаңа нысандарын түсінуді қоса алғанда, киберқылмыспен күресу бойынша шараларды әзірлеу контекстінде одан әрі зерттеуді талап етеді.

Амин Амириан Фарсанидің жұмысы киберқылмыстардың эволюциясын атап көрсетеді, олардың көпшілігі дәстүрлі қылмыстық құқық бұзушылықтардың цифрлық ортаға бейімделген жаңа нысандары екенін, ал басқалары тек виртуалды кеңістікте пайда болатынын атап көрсетеді. Киберқылмыстарды зерттеу анонимдік менталитетпен виртуалды тұлғаны құру киберкеңістікте қылмыс жасау мүмкіндіктерін жеңілдететінін және кеңейтетінін көрсетеді. Бұл жағдай құқық қорғау жүйелерінен жаңа жағдайлар мен мәселелерге бейімделуді талап етеді. Фарсани бұл құбылысты криминологиялық талдау және киберқылмыстардың алдын алу шараларын әзірлеу қажеттілігіне назар аударады. Автор ақпараттық технологиялардағы өзгерістер қылмыстық құқық бұзушылықтардың жаңа түрлерінің пайда болуына себеп болатынын, бұл өз кезегінде құқықтық жүйелерді осы өзгерістерге бейімделуге мәжбүр ететінін атап көрсетеді [25]. Мұндай өзгерістер компьютерлік желілердің осалдығын және оларды бұзудың ықтимал ауыр салдарын, соның ішінде мемлекеттік құрылымдардың тұрақсыздануын көрсетеді.

Халықаралық деңгейде компьютерлік қылмыспен күресу шаралары қабылдануда, оның ішінде Будапешт конвенциясы мен басқа да халықаралық құжаттар қабылдануда. Мәселен, Иранда компьютерлік қылмысқа қарсы заң жобасы 2005 жылы ұсынылып, 2009 жылы қабылданған. Бұл әрекеттер киберкеңістіктегі қауіптермен күресу үшін барабар заңнаманы құру бойынша жаһандық күш-жігерді көрсетеді, бірақ Фарсани атап өткендей, олар әлі жеткіліксіз болып табылады [25, б.82-84].

Думчиков М., Юнин О., Несторова Н., Борко А. және Ерменчук О. зерттеулері ақпараттық технологияларды пайдалана отырып қолма-қол ақша ұрлаудың криминалистикалық аспектілерін егжей-тегжейлі қамтиды, бұл қазіргі әлемдегі киберқылмыстардың ауырлығы мен ауқымын атап көрсетеді. Авторлар қазір жекелеген мемлекеттерге ғана емес, жалпы әлемдік қауымдастыққа қауіп төндіретін киберқылмыстың қарқынды таралуына тоқталды. Бұл динамика ақпараттық технологиялардың белсенді дамуымен түсіндіріледі, бұл компьютерлік ақпаратпен байланысты қылмыстық құқық бұзушылықтардың құрылымының сапалық өзгеруіне әкелді [26].

Төлем карталарын пайдалану, скиминг, зиянды бағдарлама, әлеуметтік инженерия, фишинг және электрондық коммерциядағы алаяқтық сияқты киберқылмыстың әртүрлі нысандарын талдау қылмыскерлердің жаңа технологияларға бейімделуін көрсетеді. Бұл қылмыстық құқық бұзушылықтар алдыңғы қатарлы технологияларды әзірлеу мен қолданудың арқасында мүмкін

болды, бұл құқық қорғау органдарынан мұндай әрекеттерді тергеу мен алдын алудың жаңа тәсілдерін қолдануды талап етеді.

Сондай-ақ авторлар құпия ақпаратқа заңсыз қол жеткізу үшін бірегей технологияларды пайдаланатын карташылар, фишерлер және фракерлер сияқты қылмыскерлердің киберкеңістіктегі мамандануына назар аударады. Бұл ұлттық және халықаралық заңнаманы заманауи шындықты көрсету және киберқылмыспен тиімді күресуді қамтамасыз ету үшін бейімдеу қажеттілігін көрсетеді.

М.Мұстафидың мақаласында ақпараттық технологиялардың дамуының тарихи аспектілері және олардың құқықтық әділдік пен қылмыстық жауапкершілікке әсері қарастырылған. Автор қазіргі заманда ақпараттық технологияның қарқынды дамуы экономикалық және әлеуметтік өмірдің барлық салаларында елеулі өзгерістерге әкелгенін атап көрсетеді. Бұл өзгерістер, бір жағынан, көптеген процестерді жеңілдетті, бірақ екінші жағынан, заңсыз әрекеттерге мүмкіндіктер туғызды, нәтижесінде жеке адамдар немесе топтар заңсыз пайда алып, жеке азаматтарға да, жалпы қоғамға да зиян келтіреді [27].

М.Мұстафи сонымен қатар қоғамға қауіп төндіретін технологиялық жетістіктерді қасақана теріс пайдаланумен байланысты мәселелерді атап көрсетеді. Ақпараттық технологиялардың дамуы мен жұмыс процестерін автоматтандыру жеделдеді және бұл бұрын белгісіз болып келген қылмыстық құқық бұзушылықтардың жаңа түрлерінің пайда болуына әкелді. Бұл заңнаманың икемді болуын және жаңа сын-қатерлермен тиімді күресу және ықтимал залалды барынша азайту үшін үнемі өзгеретін технологиялық ландшафтқа бейімделуді талап етеді.

Қорытындылай келе, М.Мұстафи ақпараттық төңкеріс әкелген орасан зор пайдаға қарамастан, оның бірқатар келеңсіз салдары да бар екенін атап көрсетеді. Ақпараттық технологиялардың жаһандануы жағдайында сот төрелігін және азаматтардың құқықтары мен мүдделерін қорғауды қамтамасыз ету мақсатында қылмыстық жауаптылық пен құқықтық шараларды қолдану тәсілдері осы өзгерістерді ескеруі тиіс.

Харитонов Е., Харитонова О., Толмачевская Ю., Фасий Б., М.Ткалич өз мақалаларында ақпараттық қауіпсіздікті әлемдік деңгейде құқықтық реттеу мәселелерін жан-жақты талдайды. Олар ақпараттық технологиялардың қарқынды дамуы мен экономикалық және әлеуметтік өмірдің барлық салаларындағы жұмыс процестерінің автоматтандырылуы ұлттық қауіпсіздікке тың қатерлердің пайда болуына әкелгенін атап көрсетеді. Бұл қауіптер шетелдік барлау қызметтерінің нұсқауымен әрекет ететін, конституциялық құрылысты құлатуға шақыруларды тарататын және террористік ұйымдарды қолдайтын тұлғалардан болуы мүмкін [28].

Сондай-ақ авторлар ақпараттық технологиялардағы өзгерістер қылмыстық құқық бұзушылықтың жаңа түрлеріне, соның ішінде ақпараттық технологиядағы алаяқтыққа қалай әкелгенін талқылай отырып, осы қауіптермен күресу үшін

заңнаманы жетілдіру және халықаралық ынтымақтастық қажеттігін атап өтеді. Атап айтқанда, мәліметтерді ұрлау және жүйеге кіру сияқты қылмыстық құқық бұзушылықтар жиірек және техникалық жағынан күрделі бола бастады, бұл құқық қорғау органдарынан жаңа тәсілдер мен тергеу әдістерін қабылдауды талап етеді.

Сонымен қатар, Е.Харитонов және оның әріптестері ақпараттық салада теріс пайдаланудың алдын алуға бағытталған шаралар кешені болып табылатын «ақпараттық гигиена» түсінігін енгізеді. Бұл тұжырымдама жеке адамдар деңгейінде де, жалпы қоғамда да қауіпсіздік пен тұрақтылықты қамтамасыз ететін салауатты ақпараттық ортаны құрудың маңыздылығын атап көрсетеді. Зерттеу ұлттық деңгейде де, халықаралық деңгейде де ақпараттық қатынастарды тиімдірек реттеу үшін заңнамалық өзгерістерді енгізу қажет деген қорытындыға келеді.

Ақпараттандыру және байланыс саласында жасалған қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи аспектілері туралы бөлімді қорытындылай келе, киберқылмысты талдауға кешенді көзқарастың маңыздылығын атап өткен жөн. Бабанина В., Ткаченко И., Матиушенко О. және Крутевич М., Матвеев В. және әріптестері, Амириан Фарсани, Думчиков және оның командасы Мустафи М. және Харитонов Е. және оның командасы сияқты зерттеушілер ұсынған зерттеулер киберқылмыс эволюциясын түсіну және тиімді реттеу стратегияларын әзірлеу үшін кілт болып табылады.

Бұл зерттеулер ақпараттық технологиялардың дамуы заңнаманы үнемі бейімдеуді және жаңартуды талап ететін қылмыстық құқық бұзушылықтың жаңа түрлерінің пайда болуына ықпал ететінін анықтады. Мұстафи М. атап өткендей, құқық қорғау органдарындағы тарихи өзгерістер қазіргі сот төрелігі тек қылмыстық әрекеттің дәстүрлі нысандарын ғана емес, сонымен қатар жаһандық ақпараттандыру нәтижесінде туындайтын жаңа сын-қатерлерді де ескеруі қажет екенін көрсетеді.

Е.Харитонов және оның әріптестері киберқылмысқа қарсы күресте халықаралық үйлестіру қажеттігін атап көрсеткен халықаралық ынтымақтастық және заңнамалық шараларды біріздендіру аспектісі ерекше маңызды. Бұл ынтымақтастық жаһандық деңгейде ақпараттық қауіпсіздікті қамтамасыз ету үшін өте маңызды, ол сонымен бірге «ақпараттық гигиенаны» құру және ақпараттық соғыстан қорғау қажеттілігін көрсетеді.

Ұсынылған зерттеулер аясында киберқылмыспен тиімді күресу тек технологиялық, әлеуметтік және халықаралық-құқықтық өлшемдерге назар аудара отырып, осы қылмыстық құқық бұзушылықтардың криминологиялық және криминалистикалық аспектілерін терең түсінгенде ғана мүмкін болады. Осы көп қырлы және күрделі мәселені білу киберқылмыспен күресу мен оның алдын алудың кешенді стратегияларын әзірлеудің , сондай-ақ тұрақты және бейімделген құқықтық өрісті қалыптастырудың шешуші факторына айналады.

1-кестеде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершіліктің дамуының негізгі тарихи аспектілеріне шолу берілген. Бұл шолу заңнамадағы өзгерістерді, технологиялық прогресті және

әртүрлі кезеңдердегі академиялық зерттеулердің негізгі нәтижелерін қамтиды. Бұл құрылым технологиялық инновациялар мен әлеуметтік трансформациялар киберқылмысты реттеудің құқықтық тәсілдеріне қалай әсер еткенін жүйелі түрде қарастыруға, сондай-ақ халықаралық ынтымақтастық эволюциясын қадағалауға және құқықтық контексте киберқауіпсіздікті түсінуді тереңдетуге мүмкіндік береді.

1-кесте

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершіліктің тарихи дамуы

Кезең	**Заңнамадағы және тәжірибедегі негізгі өзгерістер**	**Технологиялық өзгерістер**	**Зерттеудің негізгі қорытындылары**
1960 жылдар	Алғашқы компьютерлердің пайда болуымен киберқылмыс түсінігінің пайда болуы.	Компьютерлік технологияларды өмірдің әртүрлі салаларына енгізу.	Ақпараттық технологияларды қылмыстық мақсатта қолданудың басталуы.
1980-1990 жылдар	Киберқауіпсіздік туралы алғашқы заңдардың қалыптасуы. Интернет пен цифрлық технологиялардың таралуы заңнамалық қорғау қажеттілігін арттырды.	Интернет пен дербес компьютерлердің жаппай таралуы.	Киберқылмыстың жаңа түрлерімен күресуге бағытталған құқықтық нормаларды әзірлеу.
2000 жж.	Күресте халықаралық ынтымақтастықты нығайту . Будапешт конвенциясының қабылдануы.	Шифрлау және бұлтты есептеу технологияларын дамыту	Киберқылмыстардың артуы халықаралық реакцияға түрткі болуда.
2010 жылдардан бастап	Әртүрлі елдерде жеке деректерді қорғау және киберқауіптерге қарсы тұру туралы заңдарды қоса алғанда, нақты заңдарды қабылдау.	Мобильді құрылғылар мен IoT тарату.	Жаһандану және жаңа технологияларды дамыту аясында киберқауіпсіздік мәселелерін тереңдету.

Келесі кезекте ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершіліктің құқықтық негіздерін қалыптастыруға және дамытуға елеулі әсер еткен қазақстандық ғалымдардың еңбектерін және Қазақстан Республикасының заңнамасын зерделеуге тоқталамыз. Атап айтқанда, біз ақпараттық технологиялар мен жаһанданудағы өзгерістер ұлттық заңнамаға қалай әсер етіп жатқанын және бұл Қазақстанның құқық қорғау жүйесіне қойылатын бірегей міндеттер мен мүмкіндіктерді қарастырамыз. Сондай-ақ ақпараттық ресурстарды заңсыз пайдаланумен байланысты қауіптермен күресу үшін құқықтық нормалардың қалай бейімделіп жатқаны, соның ішінде осы саладағы халықаралық ынтымақтастық мәселелері талданады. Зерттеу қазақстандық ғалымдар мен заң шығарушылардың киберқауіпсіздік мәселелеріне қалай әрекет ететінін және киберқылмыспен байланысты тәуекелдерді азайту үшін ұлттық деңгейде қандай қадамдар жасалып жатқанын тереңірек түсінуге мүмкіндік береді, осылайша азаматтардың құқықтық қорғалуын және елдің ақпараттық кеңістігіндегі тұрақтылықты қамтамасыз етеді.

Ж.Б.Ақшатаева және А.Ж.Байдалы зерттеуінде Қазақстанның ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың ерекшеліктерін көрсетеді, еліміздің әлеуметтік-құқықтық салаларында ақпараттық технологиялардың өсіп келе жатқан рөлін атап көрсетеді. Авторлар технологияның дамуы заңнаманың үнемі өзгеріп отыратын технологиялық ортаға бейімделу мен әрекет етуді талап ететін жаңа қылмыстық құқық бұзушылық түрлеріне қалай әкелетінін талдайды. Олар Қазақстанның кейбір батыс елдерімен салыстырғанда киберқылмыс деңгейі төмен болғанымен, ел әлі де киберқауіпсіздікке қатысты күрделі мәселелерге тап болып отырғанын атап өтті. Қазақстанда 2012 жылы қабылданған және ұлттық қауіпсіздіктің маңызды құрамдас бөлігі ретінде ақпараттық қауіпсіздікті қорғауға бағытталған ережелерді қамтитын «Ұлттық қауіпсіздік туралы» Заңға ерекше назар аударылады.

Сонымен қатар, зерттеу қазіргі заманғы технологиялық өзгерістер мен жаһанданудың елдегі заңның үстемдігіне қалай әсер ететініне назар аударады, ақпараттық дәуірде азаматтардың құқықтары мен бостандықтарын реттеу мен қорғауда құқықтық жүйенің икемді және жаңашыл болуын талап етеді. Авторлар тиімді халықаралық ынтымақтастықты дамыту жергілікті деңгейден жаһандық деңгейге дейінгі барлық деңгейде ақпараттық қауіпсіздікті қамтамасыз етудің кілті болып табылатынын атап көрсетеді.

Ж.Б.Ақшатаева мен А.Ж.Байдалы атап өткендей, Қазақстан заңнамасы елдің ақпараттық қауіпсіздігін қамтамасыз ету үшін маңызды болып табылатын электронды ақпаратқа қол жеткізуге қатысты егжей-тегжейлі жіктеу мен шектеулерді қарастырады. Зерттеуде электрондық ақпараттық ресурстардың қолжетімділігі тек ұлттық деңгейде бекітілген заңнамамен шектелуі мүмкін екендігі атап көрсетілген. Мемлекеттік құпияға жататын мәліметтерді қорғауға байланысты қылмыстық жауапкершіліктің құқықтық аспектілеріне ерекше назар

аударылады. Авторлар мұндай ақпараттық ресурстарға қолжетімділікті нақты саралау және оларды заңға сәйкес қорғауды қамтамасыз ету қажеттілігін атап көрсетеді, бұл қоғамдық және мемлекеттік қауіпсіздікті нығайтуға ықпал етеді. Осылайша, зерттеудің қорытындысы Қазақстанның ақпараттық қауіпсіздік және киберқылмыс саласындағы заңнамалық базасын одан әрі дамыту және жетілдіру, оны тез өзгеретін технологиялар мен халықаралық стандарттарға бейімделу талабымен күшейту қажеттілігін көрсетеді [29].

А.П.Пернебековаңың зерттеуінде ақпараттандыру және байланыс саласындағы құқық бұзушылықтар үшін қылмыстық жауапкершілікке қатысты Қазақстанның заңнамалық базасының негізгі аспектілерін көрсетеді. Автор қоғамды цифрландыру дәуіріндегі құқықтық реттеудің маңыздылығын айта отырып, заңнаманың дамуы ақпараттық қауіпсіздікке қалай әсер ететінін егжей-тегжейлі қарастырады. «Бұқаралық ақпарат құралдары туралы» және «Ұлттық қауіпсіздік туралы» сияқты заңдарды талдау Пернебековаға өсіп келе жатқан технологиялық ену мен киберқауіптерге байланысты жаңа сын-қатерлерге бейімделу контекстінде заң саласының эволюциясын бағалауға мүмкіндік береді. Ақпаратты қорғауға, шетелдік БАҚ-қа қолжетімділікті реттеуге және ақпараттық кеңістікті бақылау арқылы ұлттық қауіпсіздікті қамтамасыз етуге ерекше көңіл бөлінеді. Осылайша, А.П. Пернебековаңың жұмысы қазіргі ақпараттық қоғам құқықтық қорғауға кешенді көзқарасты талап ететінін мойындай отырып, ақпараттық қауіпсіздік саласындағы заңнамалық шараларды күшейту қажеттілігін көрсетеді. Бұл зерттеу үнемі өзгеріп отыратын цифрлық экономикаға тиімді әрекет ету және мемлекет пен қоғамның қауіпсіздігін қамтамасыз ету үшін заңнаманың технологиялармен бірге дамуы керек екенін атап көрсетеді [30].

Қазіргі Қазақстанда Сәулен Н., Жамбаев Е.С., Сағадиев А.Н. атап өткендей цифрландыру және ақпараттандыру конституциялық құндылықтардың өзгеруіне ықпал етеді, бұл ақпараттық қауіпсіздік саласындағы заңнамалық базаға айтарлықтай әсер етеді. Авторлар жылдам дамып жатқан технологиялар жағдайында жеке деректер мен құпиялылықты қорғау үшін жаңа заңнаманың қажеттілігін атап көрсетеді. Олар цифрландырудың құпиялылық пен демократияға қалай әсер ететінін талдап, технологиялық жетістіктердің көптеген артықшылықтары бар екеніне, мониторинг пен деректерді жинаудың артуына байланысты құпиялылықты жоғалтудың айтарлықтай қаупі бар екенін атап көрсетеді. Зерттеуде бұл жағдай ақпараттық қауіпсіздікке деген көзқарастарды қайта қарауды және цифрландыру дәуірінде азаматтарды қорғауға қабілетті жаңа құқықтық базаны қалыптастыруды талап ететіні [31].

Негізгі құқықтар мен бостандықтарға қауіп төндіретін басқару және бақылау мүмкіндіктерін кеңейтудегі интернет-технологиялардың рөлі де маңызды. Авторлар осы саланы реттеудің құқықтық құралы ретінде «ақпараттық диетаны» енгізуді ұсынады, бұл құпиялылықты бұзу қаупін азайтуға көмектеседі. Олардың пайымдауынша, бұл тәсіл қоғамның ақпараттың ашықтығы мен қолжетімділігіне деген қажеттіліктерін де, азаматтардың жеке өмірі мен

деректерін қорғау қажеттілігін де ескере отырып, теңгерімді және қауіпсіз ақпараттық ортаны қалыптастырады.

Бижанова А.Р., Мейірбекова Г.Б., және Жүнісова Г.Ә. жаһандану мен ақпараттық технологиялар әсерінен қоғамның өзгеруін сипаттай отырып, 21 ғасыр адам өмірінің барлық салаларын түбегейлі өзгерткен ақпарат ғасырына айналғанын атап көрсетеді. Олар Интернет пен цифрлық технологиялардың қарқынды дамуы білім, медицина және бизнес үшін жаңа мүмкіндіктер туғызып қана қоймай, сонымен қатар ақпараттық қауіпсіздік саласындағы жаңа міндеттерді алға шығарғанын атап өтті. Авторлардың пікірінше, жан-жақты киберқауіпсіздікті енгізу қажеттілігі көптеген елдер үшін, соның ішінде Қазақстан үшін де басымдыққа айналды [32].

Сондай-ақ авторлар ақпараттық технологиялардың жеке өмірге және жеке өмірге тигізетін әсеріне тоқталып, Интернет пен әлеуметтік желілердің ақпарат алмасу және сауда алаңына айналғанын атап көрсетеді. Олар бұл цифрлық технологияларға тәуелділіктің артуы жағдайында жеке және заңды тұлғалардың құқықтарын қорғау қажеттігіне баса назар аудара отырып, кибербуллинг және фишинг сияқты жаңа қауіптердің пайда болуына әкелгенін атап өтті.

А.Р.Бижанованың, Г.Б.Мейірбекова және Г.Ә.Жүнісованың жүргізген зерттеуінде Қазақстандағы киберқауіпсіздік мәселесінің ауқымын көрсететін статистикалық мәліметтерді ұсынады. Авторлар атап өткендей, 2019 жылы елімізде ақпараттық қауіпсіздікті бұзуға байланысты 21 мыңнан астам оқиға тіркелген. Оның 17,7 мыңы ботнеттерді пайдаланатын шабуылдарға қатысты , бұл ұйымдасқан киберқылмыстың жоғары деңгейін көрсетеді. Сонымен қатар, пайдаланушылардың жеке деректерін қорғау мәселесінің өзектілігін көрсете отырып, фишингтік шабуылдардың 883 жағдайы анықталды. Бұл тұжырымдар Қазақстанда киберқауіпсіздікті жақсарту және киберқауіптерге қарсы тұрудың тиімді әдістерін әзірлеу бойынша күш-жігерді арттыру қажеттілігін көрсетеді [32,б.111-112].

Ақпараттық технологиялардың дамуы бүкіл әлемдегі құқықтық жүйелерге айтарлықтай әсер етті, заңнаманың киберкеңістік тудыратын жаңа сын-қатерлерге бейімделуін талап етеді. Жетекші елдер, соның ішінде Қазақстан азаматтардың киберқауіптерден қорғалуын қамтамасыз ету үшін заңнамалық және нормативтік-құқықтық базаларын жетілдіру бойынша белсенді жұмыс жүргізуде.

Тарихи талдау көрсеткендей, қоғамның цифрлық технологияларға тәуелділігі артқан сайын киберқылмыс қаупі де артып, қатаң реттеулер мен бақылауды қажет етеді. Талданған мақалалар мен зерттеулер осы құбылыспен күресудегі құқықтық шаралардың маңыздылығын, сондай-ақ киберқылмысты тиімді реттеу және алдын алу үшін халықаралық ынтымақтастықтың қажеттілігін көрсетеді.

Жалпылама түрде тарихи кезеңдерді келесідей жіктеуге болады деп есептейміз:

1 – кезең. Ең алғашқы құқық бұзушылықтар мен телекоммуникация саласындағы

заң бұзушылықтар 1960-1970 жылдары телекоммуникация саласындағы құқық бұзушылықтар технологиялық революцияның алғашқы толқынының нәтижесінде пайда болды.
2 – кезең. Компьютерлік жүйелердің дамуы және алғашқы компьютерлік қылмыстық құқық бұзушылықтар 1980-1990 жылдары ақпараттық технологиялар қарқынды дамып, компьютерлік жүйелер өмірдің көптеген салаларына ене бастады.
3 – кезең. Интернеттің таралуы және жаңа қылмыс түрлері 1990-2000 жылдар аралығында интернеттің жаһандық таралуы ақпараттық технологиялар саласындағы қылмыстардың жаңа кезеңін ашты.
4 – кезең. Қазіргі кезең 2000 жылдан бастап қазіргі уақытқа дейінгі кезең интернет пен ақпараттық технологиялардың жаппай таралуымен және дамуының күрделі кезеңі болып саналады.

Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершілік бірнеше кезеңге бөлініп қарастырылады. Әрбір кезеңде технологияның таралуы мен дамуының нәтижесінде қылмыстардың жаңа түрлері пайда болып, оларға қарсы тиісті заңнамалық шаралар енгізілді. Қазіргі уақытта бұл құқық бұзушылықтар халықаралық сипатқа ие болып, олардың күрделілігі құқық қорғау органдары мен заң жүйелерінен жаңа тәсілдер мен әдістерді талап етеді.

Дегенмен, жетістіктер мен заңнамалық әзірлемелерге қарамастан, киберқауіптердің үнемі өзгеретін сипаты заңдар мен қауіпсіздік шараларын үздіксіз қайта қарауды және бейімдеуді талап етеді. Сондықтан үнемі өзгеретін цифрлық әлемде ақпараттың қауіпсіздігі мен қауіпсіздігін қамтамасыз ету үшін заңнамалық базаны жаңартып отыру және қауіпсіздік технологияларын дамыту маңызды.

Ақырында, Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың эволюциясы, сондай-ақ құқықтық жауаптар бүкіл әлемде болып жатқан терең әлеуметтік, технологиялық және мәдени өзгерістерді көрсететінін атап өтеміз. Құқықтық реттеу саласындағы елеулі прогреске қарамастан, тұрақты назар аударуды, зерттеуді және заңнаманы жылдам өзгеретін цифрлық ландшафтқа бейімдеуді талап ететін бірқатар мәселелер мен міндеттер сақталуда. Бұл бағыттағы жұмыстарды жалғастыру ақпараттық қауіпсіздік пен қорғауды қамтамасыз етудің кепілі болып табылады.

1.2 Ақпараттандыру және байланыс саласында жасалатын қылмыстық құқық бұзушылықтардың ұғымы мен жіктеу мәселелері

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен жіктелуіне арналған диссертацияның 1.2 бөлімінде киберқылмыстың қазіргі жағдайы мен белгілеріне терең талдау жасалып, сонымен

қатар оларды саралаудың жүйелік тәсілі әзірленген. Бұл бөлім заң ғылымы мен тәжірибесінің дәлдігі мен бірлігін қамтамасыз ету үшін қажетті қадам болып табылатын ақпараттық кеңістіктегі қызметті қылмыстық-құқықтық реттеудің негізінде жатқан негізгі терминдер мен түсініктерді анықтаудан басталады. Әрі қарай, қолданыстағы заңнама мен сот тәжірибесін талдау негізінде ақпаратқа рұқсатсыз қол жеткізу сияқты әрекеттердің дәстүрлі түрлерін де, технологиялық прогресс нәтижесінде пайда болған жаңа нысандарды да ескеретін киберқылмыстардың егжей-тегжейлі жіктелуі ұсынылады. Ақпараттық-коммуникациялық технологияларды қолдану арқылы жасалған қылмыстық құқық бұзушылықтарды саралау критерийлеріне ерекше назар аударылады, бұл осы саладағы қылмыскерлердің нақты белгілері мен мотивтерін көрсетуге мүмкіндік береді. Бұл бөлім киберқылмыспен күресу тетіктерін одан әрі зерделеу және цифрлық дәуірде ақпараттық қауіпсіздік пен деректерді қорғауды күшейтуге бағытталған тиімді құқықтық реттеу шараларын әзірлеу үшін негіз болады.

Ақпараттық технологиялардың қарқынды дамуы мен заңнаманы жаңа сын-қатерлерге бейімдеу қажеттілігінің тоғысқан тұсында «ақпараттандыру және байланыс» саласында жасалған қылмыстық құқық бұзушылықтардың түсінігі мен жіктелуінің мәселелері айқындалды. Г.Р.Рүстемованың мақаласында деректер базасына заңсыз енуден және киберқылмыстың басқа да нысандарынан қорғаудың кешенді тәсілінің маңыздылығын айта отырып, Қазақстан Республикасындағы ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың алдын алуды қамтиды. Қазақстан Республикасы Қылмыстық кодексінің жаңа VII тарауы осы саладағы қылмыстық-құқықтық қорғау қажеттілігіне жауап болды, дегенмен ақпараттық салада қылмыстық құқық бұзушылықтардың тұжырымдамалық аппараты мен саралау жүйесін дамыту өзекті мәселе болып қалуда [33].

Ақпараттандыру және байланыс саласында жасалатын қылмыстық құқық бұзушылықтарды жіктеу мәселесі халықаралық ынтымақтастық және әртүрлі елдердің заңдарын салыстыру жағдайында ерекше байқалады. Ақпараттандыру және байланыс саласында алдын алу мен жауапкершілікке бағытталған бірқатар заңдардың қабылданғанына қарамастан, киберқылмыстың нысандары мен әдістерінің алуан түрлілігі құқықтық және ұйымдастырушылық және техникалық шараларды неғұрлым егжей-тегжейлі әзірлеуді талап етеді. Қылмыстық құқық бұзушылықтардың алдын алуда оларды жасауға ықпал ететін себептер мен жағдайларды анықтауға және жоюға ерекше көңіл бөлінеді. Бұл тек заңнамалық реттеуді ғана емес, сонымен қатар қорғаныстың техникалық құралдарын, білім беру бағдарламаларын және киберқылмысқа қарсы күресте халықаралық тәжірибе алмасудың да маңыздылығын білдіреді [34].

Интерпол ұсынған компьютерлік қылмыстардың жіктелуіне рұқсатсыз кіру, вирустар, компьютерлік алаяқтық және халықаралық деңгейде қарсы күрестің біртұтас жүйесін қалыптастыруға негіз болатын басқа да түрлері бар. Қазақстан Республикасында, көптеген басқа елдердегі сияқты, ақпараттандыру және

байланыс саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен жіктелуінің мәселелері киберқауіптердің үнемі өзгеріп отыратын сипатын ескере отырып, одан әрі зерттеулер мен әзірлемелерді талап етеді. Осылайша, «ақпараттандыру және байланыс» саласындағы қылмыстық құқық бұзушылықтардың тұжырымдамасы мен жіктелуінің мәселелері заңнаманы үздіксіз талдау және бейімдеу, киберқылмыспен тиімді күресу үшін алдын алу шараларын және халықаралық ынтымақтастықты дамыту қажеттілігін көрсетеді.

Келесі кезекте ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың ұғымдары мен классификациялары талданып, осы екі саланың аражігін ажырату қажеттігін атап өтеді. Ақпараттық технология қылмыстық құқық бұзушылықтары әдетте рұқсат етілмеген қол жеткізуді, зиянды бағдарламаларды таратуды, кибералаяқтықты және деректердің бұзылуын қамтиды. Бұл әрекеттер ақпараттық жүйеге зиян келтіреді немесе берілген деректерді теріс пайдаланады.

Киберқылмыс қазіргі уақытта кең ауқымды құқық бұзушылықтарды қамтитын ұғым ретінде танылады. Бұл құқық бұзушылықтардың қатарына деректерді ұрлау, жеке ақпаратқа рұқсатсыз қол жеткізу, зиянды бағдарламаларды тарату, интернет арқылы алаяқтық, кибершабуылдар, сондай-ақ зияткерлік меншік құқықтарын бұзу жатады. Қазіргі заманғы киберқылмыстардың басты ерекшелігі – олардың трансұлттық сипаты, яғни шекаралардың болмауы, және интернет пен ақпараттық технологиялардың қарқынды дамуы нәтижесінде қылмыстық құқық бұзушылықтардың түрлері мен әдістерінің күрделене түсуі.

Киберқылмыстарды бірнеше негізгі категорияға бөлуге болады. Біріншіден, деректерді рұқсатсыз пайдалану және ұрлау қылмыстық құқық бұзушылықтары жатады. Бұл әрекеттер деректерді заңсыз алу және оларды өз мақсаттарында қолдануды қамтиды. Оған мысалы, банк деректерін ұрлау, жеке мәліметтерді ұрлау немесе корпоративтік құпия ақпаратты рұқсатсыз пайдалану жатады.

Екіншіден, интернет алаяқтық және фишинг секілді қылмыстық құқық бұзушылықтар таралған. Мұнда алаяқтар жалған веб-сайттар немесе электрондық пошта арқылы пайдаланушылардың құпия ақпараттарын алуға тырысады. Фишинг – қолданушылардың сенімін пайдаланып, өздерінің деректерін білместен беруіне итермелейтін алаяқтық түрі.

Үшіншіден, зиянды бағдарламаларды тарату кең таралған киберқылмыс болып табылады. Зиянды бағдарламалардың қатарына компьютерлік вирустар, трояндық бағдарламалар, рансомвар сияқты түрлер кіреді. Бұл бағдарламалар компьютерлерді зақымдап, пайдаланушылардың деректеріне қол жеткізуді немесе олардың жүйелерін істен шығаруды көздейді.

Келесі маңызды қылмыстық құқық бұзушылық түрі – кибершабуылдар. Олардың арасында DDoS-шабуылдар (сервистен бас тарту шабуылдары), компьютерлік желілерге рұқсатсыз қол жеткізу, жүйелерді зақымдау және оларды бақылауға алу секілді әрекеттер бар. Бұл шабуылдар компаниялардың, мемлекеттік мекемелердің жұмысын тоқтатуға, ақпараттық жүйелердің

сенімділігін бұзуға бағытталған.

Сонымен қатар, зияткерлік меншік құқықтарын бұзу да қазіргі киберқылмыстардың кең таралған түрлеріне жатады. Интернет арқылы авторлық құқықпен қорғалған контентті заңсыз тарату, бағдарламалық жасақтаманы рұқсатсыз көшіріп сату немесе пайдалану қылмыстық құқық бұзушылықтың осы түріне жатады.

Киберқылмыстарды жіктеу олардың күрделілігін және қоғамға зиянының артуын ескере отырып жасалды. Киберқылмыстарды тиімді саралау құқық қорғау органдары үшін өте маңызды, себебі бұл шара құқық бұзушылықтарды анықтап, олар үшін тиісті жазалау механизмдерін енгізуді жеңілдетеді.

Киберқылмыстар бірнеше топқа бөлінеді. Біріншісі – техникаға қол жеткізу арқылы жасалатын қылмыстық құқық бұзушылықтар. Бұл топқа компьютерлік жүйелер мен желілерге рұқсатсыз кіру, ақпараттық жүйелерден деректерді ұрлау, сондай-ақ компьютерлік жүйелерді бұзу және зақымдау кіреді. Екінші топ – деректерге қатысты қылмыстық құқық бұзушылықтар, оның ішінде жеке және корпоративтік деректерді ұрлау, құпия ақпаратты рұқсатсыз алу және оны заңсыз пайдалану, деректерді жою немесе өзгерту жатады.

Зиянды бағдарламаларды тарату – киберқылмыстардың тағы бір кең таралған түрі. Бұл компьютерлік вирустарды, трояндық бағдарламалар мен ренсомварды тарату, сондай-ақ бағдарламалық жасақтаманы өзгерту немесе оны зақымдау арқылы жүйелерге зиян келтіру секілді әрекеттерді қамтиды.

Интернет арқылы алаяқтық жасау да кең таралған қылмыстық әрекет болып саналады. Мұнда фишинг және интернет арқылы құпия ақпаратты алдау арқылы ұрлау әрекеттері орын алады. Сондай-ақ, қаржылық алаяқтық, яғни интернет-банкинг жүйелеріне шабуыл жасау немесе төлем жүйелерін заңсыз пайдалану сияқты әрекеттер де осы топқа жатады.

Зияткерлік меншікке қатысты құқық бұзушылықтар да маңызды санатқа жатады. Бұл топқа авторлық құқықпен қорғалған контентті, мысалы, бағдарламалық жасақтама, фильмдер немесе музыка сияқты өнімдерді рұқсатсыз тарату жатады.

Қазақстанда киберқылмыстарға қарсы заңнамалық шаралар айтарлықтай күшейтілді. Қазақстан Республикасының Қылмыстық кодексінің VII тарауы киберқылмыстарды реттейтін баптармен толықтырылды. 205-213 баптарда компьютерлік жүйелерге және ақпараттық инфрақұрылымға қатысты құқық бұзушылықтар үшін жазалар белгіленген. Мысалы, компьютерлік жүйелерге рұқсатсыз кіру, зиянды бағдарламаларды тарату, ақпараттық жүйелердегі деректерді заңсыз алу немесе жою бойынша қылмыстық құқық бұзушылықтар үшін қатаң жауапкершілік көзделген [35].

Қазақстанда «Ақпараттандыру туралы» заң қабылданып, ақпараттық қауіпсіздік пен деректерді қорғауға қатысты жаңа талаптар енгізілді. Бұл заң киберқылмыстарға қарсы күрестің құқықтық негізін күшейтіп, ақпараттық жүйелерді қорғауға бағытталған шараларды қамтиды.

Киберқылмыстарды болдырмау және олармен күресу үшін бірнеше маңызды бағыт бойынша іс-шаралар жүргізілуі тиіс. Біріншіден, заңнаманы жетілдіру қажет, себебі киберқылмыстарды құқықтық тұрғыдан тиімді реттеу үшін заңдар үнемі жаңартылып отыруы тиіс. Екіншіден, халықаралық ынтымақтастықты күшейту керек, себебі трансұлттық қылмыстық құқық бұзушылықтарға қарсы күресу үшін басқа мемлекеттермен ақпарат алмасу және тәжірибе бөлісу маңызды.

Үшіншіден, техникалық қорғау құралдарын күшейту қажет. Компьютерлік жүйелер мен желілерді қорғау үшін жаңа қауіпсіздік технологияларын енгізу маңызды. Төртіншіден, қоғамның киберқауіпсіздік бойынша білімін арттыру мақсатында арнайы білім беру бағдарламаларын дамыту қажет.

Киберқылмыстарға қарсы халықаралық ынтымақтастық аясында Еуропа Кеңесінің 2001 жылғы Будапешт конвенциясы ерекше орын алады. Бұл конвенция киберқылмыстармен күресте біртұтас құқықтық және ұйымдастырушылық негіздерді қалыптастыруға бағытталған. Конвенция аясында киберқылмыстарды анықтау, олардың алдын алу және олармен халықаралық деңгейде күресу бойынша маңызды шаралар қабылданды [36].

Киберқылмыстардың қазіргі жағдайы олардың күрделілігі мен трансұлттық сипатының артуына байланысты қоғамның қауіпсіздігіне үлкен қатер төндіреді. Қазақстанда қабылданған заңнамалық шаралар киберқауіпсіздікті қамтамасыз етуге бағытталған, дегенмен киберқылмыстарды жіктеу мен оларды саралау жүйесін одан әрі дамыту қажет. Халықаралық тәжірибені ескере отырып, жаңа технологияларды енгізу және құқықтық нормаларды жетілдіру осы салада маңызды қадамдар болып табылады.

Ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар ақпараттық жүйелерге рұқсатсыз кіруді, зиянды бағдарламаларды таратуды, кибералаяқтықты және жеке деректерді өңдеуді бұзуды қоса алғанда, заңсыз әрекеттердің кең ауқымын білдіреді. Бұл қылмыстық құқық бұзушылықтар дерекқорларды бұзудан жеке ақпаратты ұрлауға немесе компьютерлік желілерді бұзуға арналған бағдарламаларды таратуға дейін болуы мүмкін. Рұқсат етілмеген қол жеткізу көбінесе басқа біреудің ақпараттық жүйесіне иесінің рұқсатынсыз кіруді білдіреді. Бұл деректерді ұрлау, саботаж жасау немесе тіпті қоңырау шалу мақсатында жасалуы мүмкін. Зиянды бағдарламаларды тарату компьютерлерге, желілерге немесе тіпті бүкіл ақпараттық жүйелерге зақым келтіруі мүмкін бағдарламаларды жасауды және таратуды қамтиды. Мұндай бағдарламалар маңызды ақпаратты ұрлауы, зақымдауы немесе жоюы, жүйелерді баяулатуы немесе толығымен тоқтатуы мүмкін [37].

Сонымен, авторлық теориялық анықтама ретінде Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар деп- «ақпараттық жүйелерді, мәліметтер базасын және телекоммуникация, компьютерлік коммуникация желілерін заңсыз пайдалану арқылы жүзеге асырылатын, жеке және мемлекеттік деректерге қол жеткізу, оларды өзгерту немесе жою мақсатындағы қылмыстық құқық бұзушылық».

Кибералаяқтық – компьютерлік технологияны заңсыз ақша немесе басқа пайда алу үшін пайдалану. Бұл фишингті, қаржылық шоттарға кіру үшін жалған немесе ұрланған онлайн сәйкестіктерді пайдалануды немесе ақшаны заңсыз аудару үшін компьютерлік жүйелерді басқаруды қамтуы мүмкін. Жеке ақпаратты иесінің келісімінсіз рұқсатсыз жинау, сақтау немесе беру сияқты деректердің бұзылуы да деректерді қорғау заңнамасын қатайту аясында басты алаңдаушылық туғызуда. Бұл әрекеттер жеке тұлғаларға да, ұйымдарға да елеулі зиян келтіріп, цифрлық технологияларға деген сенімді әлсіретіп, айтарлықтай қаржылық және операциялық шығындарға әкеледі. Осындай қылмыстық құқық бұзушылықтармен күресудің тиімді әдістерін әзірлеудің және осы саладағы заңнамалық базаны нығайтудың маңыздылығын олардың ауқымы мен күрделілігін ескере отырып, атап өтуге болмайды [38].

Жеке мәселе телекоммуникациялық жабдықты заңсыз пайдалану немесе зақымдау, байланыстарды ұстап алу және байланыс желілерінің қалыпты жұмысына кедергі жасаудың басқа да нысандарын қамтитын байланыс саласындағы қылмыстық құқық бұзушылыққа қатысты. Бұл әрекеттер маңызды инфрақұрылымның интеграциясы мен функционалдығына және азаматтардың жеке қауіпсіздігіне тікелей қатер төндіреді. Байланыс саласындағы қылмыстық құқық бұзушылықтар мысалы, телекоммуникация құралдарын заңсыз пайдалану немесе зақымдау, байланыстарды ұстап алу және желілердің қалыпты жұмысына кедергі жасаудың басқа да түрлері қоғамның тұрақтылығы мен қауіпсіздігіне үлкен қауіп төндіреді. Бұл әрекеттер деректердің құпиялылығы мен тұтастығын бұзып қана қоймайды, сонымен қатар маңызды әлеуметтік және экономикалық процестер тәуелді болатын маңызды инфрақұрылымның жұмысына елеулі әсер етуі мүмкін.

Телекоммуникациялық жабдықты заңсыз пайдалану телекоммуникация желілерінің сенімділігіне нұқсан келтіретін деректерді ұстап алу немесе беру үшін заңсыз құрылғыларды орнатуды қамтуы мүмкін. Сондай-ақ мұндай жабдықтың зақымдануы осы желілердің айтарлықтай бұзылуына әкелуі мүмкін, бұл төтенше жағдайлар қызметтері, банк және көлік жүйелері сияқты өмірлік маңызды қызметтерді бұзуы мүмкін. Жеке және корпоративтік шығындарға әкеп соқтыратын құпия ақпараттың ағып кетуіне әкелетін тағы бір күрделі мәселе байланыстарды тоқтату болып табылады. Сондай-ақ, егер мұндай ақпарат зиянкестердің немесе шет елдердің қолына түссе, ол ұлттық қауіпсіздікке әлеуетті қауіп төндіреді. Желілік кедергілердің басқа түрлері желілік инфрақұрылымды салдандырып, апаттарға немесе маңызды жүйелердің толық өшірілуіне әкелетін телекоммуникациялық жүйелер арқылы зиянды бағдарламалардың таралуын қамтуы мүмкін. Мұндай әрекеттер мемлекеттік мекемелердің, бизнестің қалыпты жұмысын және азаматтардың күнделікті өмірін бұза отырып, маңызды инфрақұрылымның интеграциясы мен функционалдылығына тікелей қауіп төндіреді. Сондықтан ұлттық және жеке қауіпсіздікті қамтамасыз ету үшін телекоммуникациялық инфрақұрылымды қорғау шараларын күшейту және

мұндай қылмыстық құқық бұзушылықтар үшін жауапкершілікті арттыру қажет [39].

Цифрландыру мен жаһандық қосылудың қазіргі әлемінде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар арасындағы айырмашылық барған сайын маңызды бола түсуде. Қоғамның ақпараттық технологиялар мен телекоммуникациялық желілерге тәуелділігінің күшеюі тәуекелдерді арттырады және ерекше назар аударуды және нақты реттеуді қажет ететін жаңа қауіптерді тудырады. Бұл екі саладағы құқық бұзушылықтарды нақты ажырата білу маңызды, өйткені олар қоғамның әртүрлі аспектілеріне әсер етеді және олардың алдын алу мен жолын кесуге әртүрлі көзқарастарды талап етеді. Бұл 1-суретте ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды жүйелеуге, олардың негізгі сипаттамаларын анықтауға және оларды саралау мен орындауға байланысты мәселелерді анықтауға бағытталған. Бұл осы салалардағы қылмыстық құқық бұзушылықтардың құрылымы мен даму динамикасын жақсы түсінуге, сондай-ақ заңнамалық және құқық қорғау органдарының араласуының негізгі сәттерін анықтауға мүмкіндік береді [40].

Сурет 1 – Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен жіктелуі

Осылайша, құрылым ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды нақты бөлудің маңызды маңыздылығын көрсетеді. Осы салалардың әрқайсысындағы құқық бұзушылықтардың бірегей

сипаттамалары мен салдарын түсіну тиімді заңнамалық және алдын алу шараларын әзірлеудің кілті болып табылады. Бұл ерекшелік киберқылмыспен күресудің нақты құқықтық базасын жасауға көмектесіп қана қоймайды, сонымен қатар ақпараттық қауіпсіздік пен коммуникациялық инфрақұрылымды қорғау тетіктерін тереңірек түсінуге ықпал етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың жекелеген тәсілдерін әзірлеу технологиялық процестердің ерекшеліктерін және ықтимал қауіптерді ескеруге мүмкіндік береді, бұл құқық қолдану тәжірибесінің тиімділігін арттыруға көмектеседі. Ол сондай-ақ ақпараттық ағындар мен коммуникациялардың жаһандық сипатын ескере отырып, киберқауіпсіздік саласындағы халықаралық ынтымақтастыққа мүмкіндік береді.

Осылайша, мұндай қылмыстық құқық бұзушылықтарды саралау мен реттеуге байланысты мәселелер заңнамалық бейімделу мүмкіндіктерінен жиі асып түсетін жылдам технологиялық дамумен шиеленісе түседі. Осы қылмыстық құқық бұзушылықтардың көпшілігінің халықаралық сипаты бірлескен операциялар мен ақпарат алмасуды қамтитын киберқылмыспен күресте жаһандық ынтымақтастық пен үйлестіруді талап етеді. Сонымен қатар, киберқылмыс істері бойынша юрисдикцияны анықтау қиын болып қала береді, бұл көбінесе кінәлілерді жауапқа тартуды қиындатады. Сондай-ақ жеке ақпаратты қорғауды қылмыстық құқық бұзушылықтарды тергеу үшін деректерге қол жеткізу қажеттілігімен теңестіру қажет. Осылайша, заңнаманы жаңарту және халықаралық ынтымақтастықты нығайту ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға тиімді әрекет ету үшін маңызды болып табылады, бұл жаһандану мен цифрландыру жағдайында қоғамдық және ұлттық қауіпсіздікті қорғауды қамтамасыз етуге көмектеседі [41].

Р.Р.Феткулиннің және А.К.Арюков еңбегінде 2019 жылы Baikal Research Journal журналында жарияланған «Цифрлық ақпараттық қылмыстар: тұжырымдамасы мен түрлері» ақпараттық технология қылмыстық құқық бұзушылықтарының негізгі ұғымдары мен жіктелуін қарастырады. Авторлар бұл қылмыстық құқық бұзушылықтарды ақпараттың құпиялылығына, тұтастығына және қолжетімділігіне әсер етуіне байланысты дұрыс түсіну мен жүйелеудің маңыздылығын атап көрсетеді [42]. И.Р.Бегишев ұсынған классификация ақпаратқа рұқсатсыз қол жеткізу, зиянды бағдарламаларды жасау және тарату, деректерді сақтау және беру жүйелерін пайдалану ережелерін бұзу, сондай-ақ алаяқтық және ақпарат алуға арналған арнайы техникалық құралдардың заңсыз айналымы сияқты санаттарды қамтиды. Мақалада бұл әрекеттердің ақпараттық қауіпсіздікке елеулі зиян келтіруі және тиісті қылмыстық-құқықтық реттеу қажет екендігі атап өтілген [43].

И.Р. Бегишевтің заң ғылымдарының кандидаты ғылыми дәрежесін алу үшін жазған диссертациясының авторефератында ұсынылған жұмысында цифрлық ақпарат саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен түрлеріне қатысты мәселелер жан-жақты қамтылған. И.Р.Бегишев осындай қылмыстық

құқық бұзушылықты саралау мәселелеріне тоқталып, негізгі санаттарды, соның ішінде цифрлық технологияларды пайдалана отырып, алаяқтық, компьютерлік ақпаратқа рұқсатсыз қол жеткізу және ақпараттық жүйелердің жұмыс істеу тәртібін бұзуды анықтайды. Диссертацияда осы саладағы қылмыстық-құқықтық реттеуді жетілдіру тетіктеріне ерекше назар аударылып, жауапкершілікті саралау және қолданыстағы нормаларды нақтылау қажеттігін атап өтеді. Автор Ресей Федерациясының Қылмыстық кодексінің баптарына өзгертулер енгізуді ұсынады, бұл цифрлық технологияларды қолдануға байланысты қылмыстық құқық бұзушылықтармен тиімді күресуге ықпал етуі тиіс. И.Р.Бегишев, сондай-ақ, ақпараттарды жасырын алу үшін арнайы техникалық құралдарды пайдаланғаны үшін жауапкершілікті күшейту жөнінде ұсыныстар енгізіп, мұндай әрекеттердің әлеуметтік қауіптілігі қолданыстағы заңнамада жеткіліксіз ескерілуде. Бұл өзгерістер жеке деректердің құпиялылығын қорғауға және мемлекеттік және жеке мүдделер деңгейінде ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған.

Е.Н.Рахманова және Т.В.Пинкевич Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды саралау мәселелері жан-жақты талқыланады, бұл цифрлық технологиялардың қарқынды дамуы жағдайында өте маңызды. MTDE 2020 конференциясында ұсынылған зерттеулерінде олар «компьютерлік қылмыс» түсінігі Стэнфорд зерттеу институтының есеп берулерінде 40 жылдан астам уақыт бұрын пайда болғанын және содан бері айтарлықтай өзгерістерге ұшырағанын атап өтеді. Авторлар ақпараттық жүйелерді қорғау бойынша 1992 жылы ЭЫДҰ ұсынымдарынан бастап, ақпараттық жүйелер мен желілердің қауіпсіздік мәдениетін құруға бағытталған 2002 жылғы соңғы ұсынымдардан бастап нормативтік базаны әзірлеуге назар аударады. Е.Н.Рахманова мен Т.В.Пинкевич 2000 жылы БҰҰ Қылмыстың алдын алу және қылмыстық сот төрелігі жөніндегі оныншы конгресінде қабылданған киберқылмыстың анықтамасын талдайды, ол киберқылмысты компьютерлік жүйелерді немесе желілерді пайдалану арқылы жасалуы мүмкін кез келген қылмыстық әрекет ретінде анықтайды [44].

Зерттеу БҰҰ-ның Қылмыстың алдын алу және қылмыстық сот төрелігі жөніндегі он бесінші конгресіндегі талқылауларға ерекше назар аударады, онда компьютерлік қылмыстық құқық бұзушылықты цифрлық технологияларды қолдануға байланысты заңмен немесе сот тәжірибесімен тыйым салынған әрекеттер ретінде қарастыру ұсынылды. Қорытындылай келе, зерттеу цифрлық ақпараттандыру және байланыс қылмыстық құқық бұзушылықтарды анықтау және жіктеумен байланысты қиындықтарды көрсете отырып, қылмыстық заңнаманы қазіргі цифрлық дәуірдің шындықтарына бейімдеу қажеттілігін көрсетеді.

2021 жылы «International Journal of Computer Science and Network Security» журналында жарияланған «Экономикалық кеңістіктегі киберқылмыс: психологиялық мотивация және семантикалық және терминологиялық ерекшелігі» мақаласында Матвеев В., Никитченко О.Е. және олардың әріптестері қазіргі

цифрлық дәуірдегі киберқылмысты жіктеуге және түсінуге қатысты маңызды сұрақтарды көтереді. Авторлар киберқауіпсіздік пен киберқылмыспен күрес 21 ғасырдың негізгі сын-қатерлері болып табылады, ол терең талдауды және киберқауіптердің алдын алу және анықтау үшін озық технологияларды енгізуді талап етеді. Гибридтік соғыс жағдайында жеке шаруашылық жүргізуші субъектілер деңгейінде де, жалпы ел деңгейінде де деректерді қорғау және құпиялылық міндетін қоятын бұқаралық ақпарат құралдары мен коммуникациялық компоненттерді пайдалануға ерекше көңіл бөлінеді. Авторлар «деректер мен құпиялылықты қорғау – бұл кез келген саладағы әрбір лауазымды тұлғаның жауапкершілігі тек ұйымдарға ғана емес, сонымен қатар жеке тұлғаларға да қатысты» деп атап көрсетеді. Дегенмен, киберкеңістіктегі кез келген киберқылмыс тек жалғыздықтың көрінісі немесе қатыгез әзіл ойнауға құштарлық емес екенін түсіну керек. Бұл, ең алдымен, материалдық пайда алу ниетінің жүзеге асуы. Кибералаяқтықтың дәл осы ерекшелігі авторлардың зерттеулерінің мақсаттары мен мазмұнын анықтады [45].

Сондай-ақ авторлар технологияның тұрақты дамуына және Интернетте қылмыстық әрекеттің жаңа түрлерінің пайда болуына байланысты киберқылмыстарды жіктеу күрделі мәселе болып қала беретінін атап өтеді. Олар мұндай қылмыстық құқық бұзушылықтармен күресу үшін заңнамада нақты анықтамалар мен стандарттарды әзірлеу қажеттігін алға тартады. Зерттеушілердің пікірінше, киберқылмыстың не екенін анықтап қана қоймай, оның жасалу механизмдерін және зардап шеккендер үшін салдарын түсіну маңызды. Зерттеуде киберқылмыс көбіне тек техникалық аспектілермен ғана емес, сонымен қатар жеке пайдаға немесе басқаларға зиян келтіруге ұмтылу сияқты психологиялық мотивтермен де байланысты екенін атап көрсетеді. Бұл киберқылмысты талдау мен бақылауды бірегей және қиын құбылысқа айналдырады. Қорытындылай келе, Матвеев пен оның әріптестерінің жұмысы халықаралық ынтымақтастық пен киберқылмыспен тиімді күресу үшін құқықтық базаны күшейтуге шақырады, бұл барлық деңгейде үйлестірілген күш-жігерді қажет ететін жаһандық мәселе екенін атап өтті [45, б.135].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен жіктелуінің мәселелері осы саладағы халықаралық өзара іс-қимылмен тығыз байланысты. «Ұжымдық қауіпсіздік туралы шарт ұйымына мүше мемлекеттердің ақпарат саласындағы қылмыстық құқық бұзушылыққа қарсы іс-қимыл саласындағы өзара іс-қимылы туралы хаттаманы ратификациялау туралы» Қазақстан Республикасының 2016 жылғы 28 наурыздағы № 476-V Заңына сәйкес қатысушылардың ақпараттық кеңістігін бірлесіп қорғау бойынша шаралар қабылдануда. Бұл заң ақпараттық қауіптерге қарсы тұру және осы саладағы ынтымақтастықтың құқықтық негіздерін нығайту бойынша келісілген іс-шараларды әзірлеу және жүзеге асыру қажеттілігіне баса назар аударады [46].

Осы заңға сәйкес, осы саладағы қылмыстық құқық бұзушылықтарды дұрыс түсіну және саралау үшін маңызды болып табылатын «ақпараттық сала», «ақпараттық кеңістік», «ақпараттық технологиялар» сияқты негізгі терминдер мен ұғымдарды анықтауға ерекше назар аударылады. Сондай-ақ, заң ақпарат саласындағы қылмыстық құқық бұзушылықтарды алдын алу үшін негіз болатын ақпараттық ресурстар мен инфрақұрылымды қорғауға бағытталған шараларды әзірлеу мен бекітуді көздейді. Бұл нормативтік-құқықтық база Ұжымдық қауіпсіздік туралы шарт ұйымының мүшелеріне қылмыстық мақсатта ақпараттық технологияларды пайдаланумен байланысты сын-қатерлерге тиімді әрекет етуге мүмкіндік береді және тұрақты және қауіпсіз ақпараттық ортаны құру үшін маңызды болып табылатын киберқылмысқа қарсы күресте халықаралық ынтымақтастық тетіктерін қалыптастырады.

Мысалы, осы Хаттаманың 1-бабында ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды дұрыс түсіну және саралау үшін маңызды негізгі терминдердің анықтамалары берілген. Сонымен, «ақпараттық өріс» ұғымы тек ақпаратты ғана емес, ақпараттық инфрақұрылымды, сондай-ақ ақпараттық қызметпен айналысатын субъектілерді де қамтиды. Тұжырымдамалық базаның осылайша кеңеюі ақпараттық саладағы құқықтық қорғау объектілерін толық сипаттауға мүмкіндік береді. Ақпаратты өңдеуге байланысты қызмет саласы ретінде айқындалатын «ақпараттық кеңістік» ақпараттық процестердің қоғам мен жеке адамға көп өлшемді әсерін атап көрсетеді. Бұл тұжырымдама киберқауіпсіздік қауіптерінің ауқымы мен әлеуетін түсіну үшін маңызды. Ақпаратпен жұмыс істеу үшін қажетті техникалық құралдардың жиынтығы ретінде «ақпараттық инфрақұрылым» анықтамасы деректерді қорғаудың техникалық жағын түсінуді күшейтеді. Қылмыстық құқық тұрғысында бұл қылмыстық құқық бұзушылықтарды объектілерін және оларды қорғау әдістерін анықтау үшін маңызды. Ақпараттық саладағы қылмыстық жауаптылықтың негізі ретінде «ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар» санаты көрсетілген, бұл әрекеттерді заңнамалық реттеу және қылмыстық қорғау қажеттігін атап көрсетеді. Жалпы алғанда, 1-бапта белгіленген тұжырымдамалық аппарат жаһандану және технологиялық даму жағдайында қылмыстық құқық бұзушылықпен тиімді күресу үшін аса маңызды ақпарат саласындағы әрекеттерді құқықтық бағалау үшін негіз жасайды.

«Ақпараттандыру және байланыс» саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен жіктелуінің мәселелері технологияның қарқынды дамуымен және қылмыстық құқық бұзушылық жасау әдістерінің үнемі өзгеруімен байланысты екенін атап өткен жөн. Бұл қылмыстық заңнаманы жаңа сын-қатерлер мен қауіптерге барабар жауап бере алатындай үздіксіз бейімдеуді талап етеді. Киберқылмыстарды жіктеудің бірыңғай терминологиясы мен бірыңғай тәсілдерін әзірлеу құқық қолдану тәжірибесі мен халықаралық ынтымақтастықты жақсартуға көмектесетін негізгі аспект болып табылады. Қылмыстық заңнаманы жетілдіру ақпараттық технологиялардың техникалық аспектілерін ғана емес,

қылмыскерлердің психологиялық мотивациясын, сондай-ақ ақпараттық кеңістіктердің жеке тұлғалардың мінез-құлқына әсер етуінің әлеуметтік-мәдени ерекшеліктерін де ескеруі қажет. Сондай-ақ, жаһандық деңгейде киберқауіптерге қарсы тұрудың және алдын алудың тиімді тетіктерін құруға мүмкіндік беретін киберқылмыспен күресудің халықаралық стандарттары мен хаттамаларын әзірлеуге назар аудару маңызды. Осылайша, «ақпараттандыру және байланыс» саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен саралау мәселелерін шешу заңнамалық, технологиялық, психологиялық және халықаралық аспектілерді қамтитын кешенді көзқарасты талап ететін көп өлшемді міндет болып табылады.

Бұл бөлімде сондай-ақ Қазақстан Республикасы Қылмыстық кодексінің 205–213-баптарында көзделген статистикалық деректер негізінде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар да көрсетілген. Бұл деректерді талдау киберқылмыс контекстінде құқық қорғау органдарының алдында тұрған міндеттердің сипаты мен көлемін түсінуге мүмкіндік береді. Ақпарат саласында ең көп таралған қылмыстық құқық бұзушылықтар Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу (ҚР ҚК-нің 205-бабы), Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру (ҚК 206-бап), сондай-ақ Ақпараттық жүйенің немесе телекоммуникациялар желісінің жұмысын бұзу (ҚР ҚК 207-бап). Статистика көрсеткендей, бұл қылмыстық құқық бұзушылықтың көбін 18 бен 35 жас аралығындағы жастар жасайды, бұл жастардың компьютерлік сауаттылығының жоғары деңгейін көрсетеді, сонымен қатар бұл ортада айтарлықтай тәуекелдер бар.

Қазіргі цифрлық дәуір жағдайында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар өзекті бола түсуде. Бұл аспектіде ақпаратқа, ақпараттық жүйелерге немесе телекоммуникация желілеріне заңсыз қол жеткізуге байланысты әрекеттерді қамтитын Қазақстан Республикасы Қылмыстық кодексінің 205-бабына ерекше назар аудару қажет. Осы бапқа сәйкес, азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін, сондай-ақ қоғамның немесе мемлекеттің мүдделерін елеулі түрде бұзуға әкеп соққан заңмен қорғалатын ақпаратқа қасақана заңсыз қол жеткізу – айыппұл салуға, түзеу жұмыстарына, қоғамдық жұмысқа тартуға, қамауға алу жазаланады. Жаза нұсқалары қылмыс зардаптарының ауырлығына және оның ерекшеліктеріне, оның ішінде белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан айыруға байланысты. Ақпараттық-коммуникациялық инфрақұрылымның маңызды объектілеріне қатысты жасалған әрекеттер үшін жауапкершілікті күшейту көзделген. Мұндай әрекеттер айыппұлдар мен қамауға алу мерзімін ұлғайтуды қоса алғанда, одан да ауыр жазаларға әкеп соғады. Іс-әрекеттер абайсыздықтан ауыр зардаптарға әкеп соқтырса, жағдай одан әрі қиындайды. Мұндай жағдайларда заңда бас бостандығынан айыруға дейін жазаны бұдан да айтарлықтай қатайту көзделген. Соңғы жылдары 205-бапқа енгізілген

өзгерістер заң шығарушының қылмыстық заңнаманы цифрлық дәуірдің сын-қатерлеріне бейімдеуге және елдің ақпараттық кеңістігін қорғауды күшейтуге деген ұмтылысын көрсетеді. Бұл өзгерістер технологиялық өзгерістерге және ақпараттық қауіптердің артуына жауап ретінде құқықтық нормаларды үнемі жаңарту қажеттілігін көрсетеді [47].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объективтік немесе субъективтік белгілерін талдау көрсеткендей, ҚР қылмыстық кодексінің 205 бабына қосымша 4 бөлігін енгізу яғни диспозициясына абайсызда ауыр зардаптарға әкеп соққан іс-әрекеттер, адамдар тобының алдын ала сөз байласуымен,бірнеше рет жасалған іс әрекеттермен толықтыру. Санкциясына келетін болсақ алты жылға дейінгі бас бостандығынан айыруға жазасын көтеру мәселесі ұсынылады.

Қазақстан Республикасы Қылмыстық кодексінің 206-бабы цифрландыру дәуірінде ерекше маңызды болып табылатын ақпаратты заңсыз жою немесе өзгерту бойынша әрекеттерді сараптайды. Бірақ, осыған қоса ақпаратты құқыққа сыйымсыз жою компьютерлік коммуникациялар желісімен де беріледі, сондықтан осы баптың диспозиясына «*компьютерлік коммуникациялар*» ұғымын толықтыру қажеттігі туындайды.Заңға сәйкес, ақпараттық жүйелерге қасақана және заңсыз араласуға байланысты бұзушылықтар ауыр зардаптарға әкеп соғады және қатаң жазаға тартылады. Мысалы, ақпаратты қарапайым жою немесе өзгерту екі жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға немесе елу тәулікке дейін қамауға алуға әкеп соғады. Егер іс-әрекет аса маңызды объектілерге қатысты немесе адамдар тобымен жасалса, санкциялар жеті жылға дейінгі мерзімге бас бостандығынан айыруға дейін көбейтіледі, бұл мұндай қылмыстық құқық бұзушылықтардың қоғамдық қауіптілігінің жоғары дәрежесін көрсетеді. Статистика мұндай қылмыстық құқық бұзушылықтардың санының өсуін көрсетеді, бұл өмірдің әртүрлі салаларында ақпараттық технологияларды қолдану аясының кеңеюімен байланысты. Маңызды инфрақұрылымдар, соның ішінде қаржы институттары, энергетикалық жүйелер және мемлекеттік басқару, киберқорғаныс шараларын және қылмыстық құқық қорғау шараларын күшейтуді талап ететін шабуылдаушылар үшін нысанаға айналуда. Осылайша, технологияның дамуы мен қоғамды цифрландыру қылмыстық заңнаманы бейімдеу және инновациялар мен қауіпсіздік арасындағы тепе-теңдікті сақтай отырып, ақпараттық қылмыстық құқық бұзушылықтармен күресу шараларын күшейту қажеттілігін жүктейді [48].

ҚР Қылмыстық кодексінің 206 бабы 1 бөлігінің диспозициясын «*компьютерлік коммуникациялар*» ұғымымен толықтыру ұсынылады. Себебі Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру әрекеттері компьютерлік коммуникациялар желісі арқылы беріледі. Сондықтан біздің ойымызша, ҚР ҚК 206 бабының диспозициясы мынадай түрде тұжырымдалады: «Электрондық жеткізгіште сақталатын, ақпараттық жүйеде қамтылатын немесе телекоммуникациялар, *компьютерлік коммуникациялар* 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». Сонымен қатар осы келтірілген әрекеттер ірі залал және ірі мөлшер ретінде ауырлығын нақты анықтау керек, сондықтан ҚР ҚК 3 бабының 38 тармағында көрсетілген *ірі залал және ірі мөлшер ретінде айлық есептік көрсеткіштен бір мың есе асатын мүлік құны немесе залал мөлшері ретіндегі,* ҚР Қылмыстық кодексінің 205, 206, 208 баптарын енгізуді ұсыну қажеттілігі туындайды.

Қазақстан Республикасы Қылмыстық кодексінің 207-бабында осы жүйелер мен желілердің жұмысын бұзуға бағытталған қасақана әрекеттер немесе әрекетсіздік үшін жауапкершілік көзделген. Мысалы, қарапайым тәртіп бұзушылық екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға немесе түзеу жұмыстары, бас бостандығын шектеу, тіпті белгілі бір мерзімге бас бостандығынан айыру сияқты жазаның басқа түрлеріне әкеп соғады. Ақпараттық-коммуникациялық инфрақұрылымның маңызды объектілеріне әсер ететін немесе алдын ала сөз байласу бойынша бір топ адамдар жасаған әрекеттер ерекше қатаң жазаланады. Мұндай жағдайларда айыппұлдар мен бас бостандығынан айыру мерзімдері айтарлықтай өседі, бұл ұлттық қауіпсіздік пен мемлекеттік жүйелердің жұмысына елеулі әсер ететінін көрсетеді. Бұл қылмыстық құқық бұзушылықтардың аса ауыр зардаптары, мысалы, қылмыстық топтар жасаған немесе ауыр шығынға немесе тіпті адам өліміне әкеп соққан қылмыстар он жылға дейін бас бостандығынан айыруға әкеп соғады. Бұл ұлттық инфрақұрылымның маңызды элементі ретінде ақпараттық жүйелер мен желілерді қорғаудың маңыздылығын көрсетеді. Бұл сақтық шаралары мен заңнамалық базалар қазіргі цифрлық дәуірде тұрақтылық пен қауіпсіздікті сақтаудың басымдығы болып табылатын елдің технологиялық және ақпараттық қауіпсіздігіне елеулі нұқсан келтіруі мүмкін қылмыстық құқық бұзушылықтардың алдын алу және жазалау үшін қызмет етеді [49].

Ақпаратты заңсыз иемденуге арналған Қазақстан Республикасы Қылмыстық кодексінің 208-бабында құқық бұзушылықтардың әртүрлі түрлері мен оларға сәйкес жазалар белгіленген, бұл ақпараттық қауіпсіздікті қорғауға заңнамалық көзқарастың маңыздылығын көрсетеді. Статистикалық деректерге сүйене отырып, баптың нұсқауларын талдап көрейік. Баптың бірінші абзацы ақпаратты қасақана заңсыз көшіруге немесе өзге де жолмен алуға қатысты. Мұндай әрекеттер құқық бұзушылықтың көлеміне және оның салдарына байланысты айыппұлдарға немесе жазаның басқа түрлеріне әкеледі. Қазақстан Республикасы Ішкі істер министрлігінің мәліметінше, мұндай құқық бұзушылықтардың тіркелген жағдайлары цифрлық технологиялардың дамуы мен интернетті пайдаланушылар санының артуына байланысты өсу үрдісін көрсетеді. Жазаны елеулі түрде күшейту ақпараттық-коммуникациялық инфрақұрылымның маңызды

объектілеріне қатысты жасалған немесе адамдар тобы жасаған әрекеттер үшін қарастырылады. Бұл жағдайлар мемлекеттік және коммерциялық ақпараттық жүйелерге соңғы жылдары тіркелген кибершабуыл жағдайларымен расталған ұлттық қауіпсіздік пен үкіметтің тұрақтылығына жоғары тәуекелмен байланысты. Ауыр зардаптарға, оның ішінде елеулі қаржылық шығындарға немесе азаматтардың өмірі мен денсаулығына қауіп төндіретін әрекеттерге аса маңызды көңіл бөлінеді . Мұндай бұзушылықтар елеулі түрмеге қамаумен жазаланады. Қоғамның ақпараттық технологияларға тәуелділігінің артуына байланысты осы саладағы қылмыстық құқық бұзушылықтар саны да артып отырғанын статистика растайды, бұл заңнамалық базаны ұдайы нығайтуды және мұндай қылмыстық құқық бұзушылықтардың алдын алу мен ашу әдістерін әзірлеуді талап етеді [50].

Сонымен қатар, ҚР Қылмыстық кодексінің 208 бабы 1-бөлігін диспозициясын «*компьютерлік коммуникация*» ұғымымен толықтыру керек. Себебі, ақпаратты құқыққа сыйымсыз иеленіп алу әрекеттері компьютерлік коммуникация желісі арқылы беріледі. Ақпаратты құқыққа сыйымсыз иеленіп алу әрекеттерін нақты саралауға үлесін қосады.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар тұрғысында Қазақстан Республикасы Қылмыстық кодексінің 209-бабында ақпаратты беруге мәжбүрлеуге ерекше назар аударылған. Түрлі қоқан-лоққылармен, соның ішінде зорлық-зомбылықпен немесе мүлікті жоюмен жүзеге асырылатын бұл әрекет жеке өмірге және ақпараттық қауіпсіздікке жеке және корпоративтік құқықтарды елеулі түрде бұзу болып табылады. Осы бапқа сәйкес, кінәлі адамдарға екі мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салу немесе жеті жылға дейінгі мерзімге бас бостандығынан айыруды қоса алғанда, әсіресе қылмыс аса маңызды объектілерге қарсы немесе физикалық күш қолдану арқылы жасалған өзге де шаралармен жазалануы мүмкін. Статистика көрсеткендей, бизнес пен мемлекеттік органдардың цифрлық технологияларға тәуелділігі артқан сайын, мұндай істер тергеу және жолын кесу тұрғысынан жиі және күрделі болып келеді. Нақты цифрлардың жоқтығына қарамастан, мұндай қылмыстық құқық бұзушылықтар саны жыл сайын артып келеді, бұл құқық қорғау органдарынан ақпараттық жүйелерді қорғауға көбірек көңіл бөлуді талап етеді деп айтуға болады [51].

Қазақстан Республикасы Қылмыстық кодексінің 210-бабында зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасағаны, пайдаланғаны және таратқаны үшін қылмыстық жауаптылық белгіленген. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар санатына жатқызылған бұл әрекеттер қазіргі цифрлық әлемдегі елеулі қатерлерді көрсетеді. Заңға сәйкес, ақпараттық жүйелердің немесе желілердің жұмысына заңсыз кедергі жасау, сондай-ақ оларды пайдалану немесе тарату мақсатында компьютерлік бағдарламаларды жасау немесе өзгерту өте қатаң жазаланады. Мұндай әрекеттер үшін үш мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салу, түзеу жұмыстарына немесе елеулі мерзімге қоғамдық жұмыстарға

тартуға, бас бостандығын шектеуге, тіпті үш жылға дейінгі мерзімге бас бостандығынан айыруға санкциялар қарастырылған. Алдын ала сөз байласу арқылы немесе қызметтік бабын пайдалана отырып, адамдар тобы жасаған әрекеттерге, сондай-ақ аса маңызды инфрақұрылым объектілеріне қатысты неғұрлым қатаң шаралар қарастырылған. Мұндай жағдайларда жазалау шаралары үш жылдан жеті жылға дейінгі мерзімге бас бостандығынан айыру жазасына дейін күшейтіліп, мұндай қылмыстық құқық бұзушылықтардың қоғамдық қауіптілігі жоғары болады. Мұндай қылмыстық құқық бұзушылықтардың әсіресе ауыр зардаптары, мысалы, қылмыстық топтардың әрекеттерінен туындаған немесе ауыр шығындарға немесе тіпті құрбандарға әкеп соққан қылмыстық құқық бұзушылықтар одан да ауыр жазаға әкеп соғады – он жылға дейін бас бостандығынан айыру. Бұл ұлттық деңгейде ақпараттық қауіпсіздікті қорғау үшін заңнамалық және техникалық шараларды ұдайы күшейту қажеттілігін көрсетеді [52].

Қазақстан Республикасының Қылмыстық кодексі, оның ішінде 211-бап қолжетімділігі шектеулі электрондық ақпараттық ресурстарды таратуға қатысты құқықтық аспектілерді реттейді. Бұл бап азаматтардың жеке деректерін және тиісті рұқсатсыз таратылуы жеке тұлғаларға да, қоғамдық мүдделерге де елеулі зиян келтіруі мүмкін басқа да құпия ақпаратты қорғауға бағытталған. Қазақстан заңнамасына сәйкес мұндай ақпаратты заңсыз тарату ауыр құқықтық зардаптарға әкеп соғады. Мұндай әрекеттер үшін жазалар құқық бұзушылықтың ауырлығына және адамдар тобының жеке пайда үшін немесе лауазымдық өкілеттіктерін пайдалану арқылы қылмыс жасауы сияқты ауырлататын мән-жайлардың болуына байланысты айыппұлдар мен қоғамдық жұмыстарға тартудан бас бостандығынан айыруға дейін болуы мүмкін. позиция. Егер іс-әрекеттер ауыр зардаптарға әкеп соқтырса немесе қылмыстық топ жасаса, ерекше қатаң шаралар қолданылады. Шектеулі ақпаратты теріс пайдалануды тиімді шектеу және жазалау ақпараттық қауіпсіздікті қамтамасыз етуде, жеке деректерді қорғауда және цифрлық кеңістікке сенімді сақтауда маңызды рөл атқарады. Статистика көрсеткендей, мұндай қылмыстық құқық бұзушылыққа қарсы шараларды күшейту құқық бұзушылықтардың санын азайтуға және ұлттық деңгейде ақпараттық қауіпсіздік жүйесінің тиімділігін арттыруға көмектеседі [53].

Қазақстан Республикасы Қылмыстық кодексінің 212-бабы заңсыз мақсаттарды көздейтін интернет-ресурстарды орналастыру қызметтерін көрсеткені үшін қылмыстық жауаптылықты реттейді. Бұл заңнама ақпараттық-коммуникациялық технологияларды заңсыз әрекеттер үшін пайдалануды көздейтін цифрлық қылмыспен күресудің кілті болып табылады. Осы бапты қолдану цифрлық кеңістікте теріс пайдалануды, соның ішінде зиянды бағдарламаларды таратуды, деректерге заңсыз қол жеткізуді және ақпараттық қылмыстық құқық бұзушылықтардың басқа түрлерін болдырмау үшін маңызды. Бапта қарастырылған айыппұлдар мен басқа да жазалар әлеуетті бұзушылардың жолын кесуге және қоғамдық қауіпсіздікке төнетін қауіпті азайтуға бағытталған.

Дегенмен, заңнаманың тиімділігін қамтамасыз ету үшін Интернеттегі қылмыстық әрекетті дер кезінде анықтауға және жолын кесуге мүмкіндік беретін тиісті технологиялық және құқық қорғау ресурстарының болуы өте маңызды. Құқықтық, техникалық және білім беру аспектілерін қамтитын кешенді тәсіл ақпараттық қауіпсіздік саласындағы жағдайды айтарлықтай жақсарта алады [54].

Қазақстан Республикасы Қылмыстық кодексінің 213 бабымен реттеледі Ұялы абоненттік құрылғының сәйкестендіру кодын заңсыз өзгертуге, сондай-ақ осындай мақсаттарға арналған бағдарламаларды жасауға, пайдалануға және таратуға байланысты қылмыстық құқық бұзушылықтар байланыс желілерінің қауіпсіздігі мен сенімділігіне айтарлықтай әсер етеді. Ұялы байланыс абоненттік құрылғысының сәйкестендіру кодын заңсыз өзгерту, сондай-ақ өндірушінің немесе заңды иесінің келісімінсіз ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасау әртүрлі айыппұлдарға, соның ішінде айыппұл салуға, түзеу жұмыстарына, қоғамдық жұмыстарға тартуға немесе белгілі бір мерзімге қамауға алу. Ұялы байланыс абоненттік құрылғысының сәйкестендіру кодын өзгертуге немесе ұялы байланыс абонентінің сәйкестендіру картасының телнұсқасын жасауға мүмкіндік беретін бағдарламаларды заңсыз жасау, пайдалану және тарату да айыппұл, түзеу жұмыстары, қоғамдық жұмыстарға тарту немесе бас бостандығын шектеу түріндегі жазаға әкеп соғады. Бұл қылмыстық құқық бұзушылықты қылмыстық топ жасаған жағдайда, ұзақ мерзімге бас бостандығынан айыруды қоса алғанда, неғұрлым қатаң жаза тағайындалуы мүмкін. Ақпарат және коммуникациялар саласындағы қауіпсіздікті қамтамасыз етудің маңыздылығын ескере отырып, мұндай қылмыстық құқық бұзушылықтардың жолын кесу азаматтардың құқықтары мен мүдделерін, жалпы қоғамдық қауіпсіздікті қорғауға бағытталған мемлекет пен құқық қорғау органдарының кезек күттірмейтін міндетіне айналады [55].

Киберқылмыс саласындағы өзекті мәселелердің бірі – заңнаманы бейімдеу мүмкіндігінен асып түсетін технологияның қарқынды дамуы. Бұл жаңа технологиялық сын-қатерлер жағдайында қолданыстағы заңдарды тиімсіз етіп, құқықтық реттеуде олқылықтарды тудырады. Айта кетуге болатын мәселе – технологиялық прогресті есепке алу үшін құқықтық базаны үнемі жаңартып отыру, сонымен қатар шекараны білмейтін киберқылмыспен күресу үшін халықаралық ынтымақтастықты нығайту қажет.

Осылайша, ақпараттық технологиялардың қарқынды дамуы және олардың қазіргі қоғам өмірінің барлық аспектілеріне ықпалының күшеюі жағдайында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды зерттеу аса маңызды болып табылады. Соңғы жылдары Қазақстанда киберқылмыс қаупі артып отыр, бұл жағдайды терең талдау мен бақылау қажеттілігін көрсетеді. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар туралы статистиканы енгізу мәселенің ауқымын бағалауға ғана емес, сонымен қатар киберқылмыстардың алдын алу және оған қарсы күрес бойынша неғұрлым тиімді шараларды әзірлеу үшін пайдалануға болатын үрдістерді анықтауға

мүмкіндік береді.

Ақпараттандыру және байланыс саласында тіркелген қылмыстық құқық бұзушылықтар санының артуы, сондай-ақ аяқталған тергеу және сотқа жіберілген істер санының артуы Қазақстандағы киберқылмыс мәселесінің ауқымдылығын көрсетеді. Сотқа дейінгі тергеп-тексеру кезінде шеттетілген адамдар санының артуы мұндай қылмыстық құқық бұзушылықтарды тергеуде бейтараптық пен тиянақтылықты қамтамасыз етудің маңыздылығын көрсетеді. Бұл тұжырымдар киберқылмыспен күресу бойынша құқықтық және ұйымдастырушылық шараларды үздіксіз жетілдіру қажеттілігін, сондай-ақ халықаралық ынтымақтастық пен ақпарат алмасудың маңыздылығын көрсетеді. Осылайша, бұл зерттеу Қазақстанда ақпаратты қорғаудың және ақпараттық қауіпсіздікті қамтамасыз етудің тиімді жүйесін құру жолындағы маңызды қадам болып табылады.

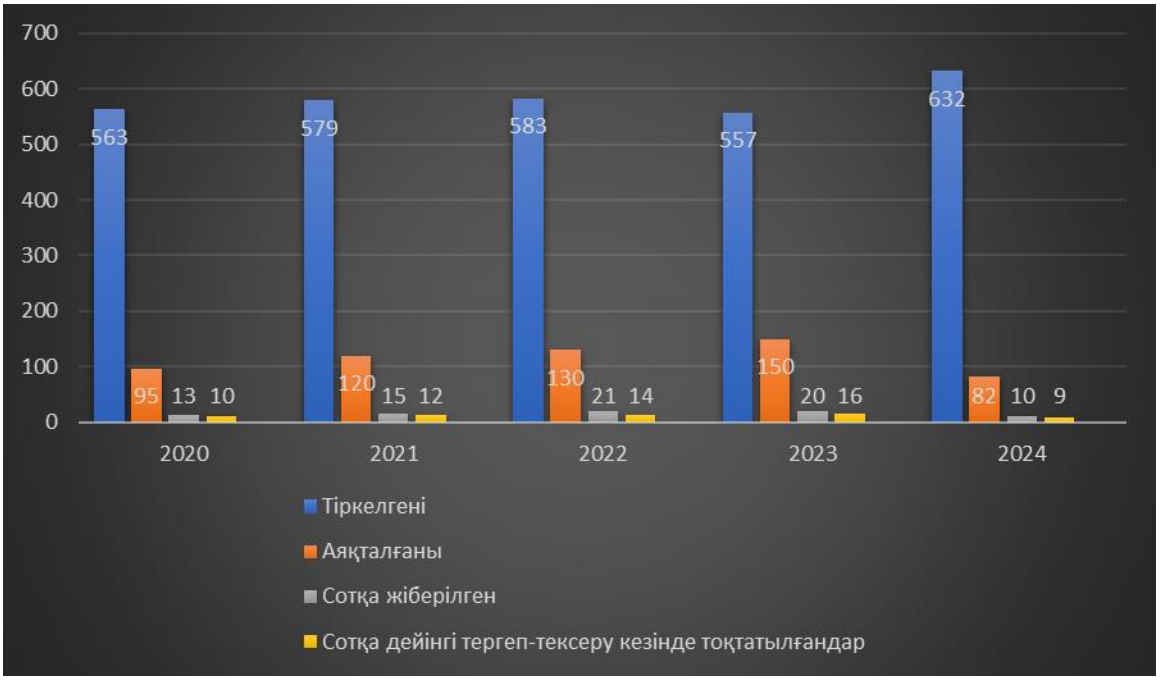
Қазақстан Республикасы Қылмыстық кодексінің 205-213-баптары бойынша тіркелген қылмыстық құқық бұзушылықтардың саны талданып отырған кезеңде айтарлықтай өскенін көрсетеді. 2020 жылы 563 оқиға тіркелді, бұл киберқылмыс белсенділігінің жоғары деңгейін көрсетеді. Одан кейінгі жылдары тіркелген жағдайлар санының тұрақты өсуі байқалады: 2021 жылы 579, 2022 жылы 583 және 2023 жылы 557, 2024 жылдың бірінші жартыжылдығында қазірдің өзінде 632 оқиға тіркелді, бұл құқық бұзушылықтар санының жалғасуын көрсетеді.

Әр жыл ішінде аяқталған қылмыстық істердің саны да оң динамикаға ие. 2020 жылы 95 іс аяқталды, бұл құқық қорғау қызметінің маңыздылығын көрсетеді. Бұл сан 2021 жылы 120, 2022 жылы 130, 2023 жылы 150 жағдайға өсті. 2024 жылдың бірінші жартыжылдығында 82 іс аяқталды, бұл аяқталған тергеулердің өсу үрдісін растайды.

Тергеу аяқталғаннан кейін сотқа жолданған істердің саны өскенін көрсетеді, бірақ тіркелген істердің жалпы санымен салыстырғанда айтарлықтай азырақ. 2020 жылы сотқа 13 іс жолданды, 2021 жылы 15 іске, 2022 жылы 21 іске, 2023 жылы 20 іске өсті. 2024 жылдың бірінші жартыжылдығында сотқа 10 іс жолданды, бұл да өскенін көрсетеді, бірақ біршама тұрақталған [56].

Сотқа дейінгі тергеп-тексеру барысында қызметінен уақытша шеттетілгендер саны біртіндеп артып отырғанын көрсетеді. 2020 жылы мұндай 10 адам болса, 2021 жылы 12, 2022 жылы 14 және 2023 жылы 16-ға өсті. 2024 жылдың бірінші жартыжылдығында 9 уақытша тоқтату болды, бұл аздап төмендегенін көрсетеді, бірақ жалпы өсу үрдісін сақтайды (сурет -2).

Сурет 2 – ҚР 2020-2024 жылдар аралығындағы ҚР ҚҚ 205-213 бабы бойынша статистикасы



Жалпы, 2020-2024 жылдар аралығында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар санының тұрақты өсуі байқалады. Құқық бұзушылықтардың ең көп саны ақпаратқа заңсыз қол жеткізу және ақпаратты заңсыз алумен байланысты. Сондай-ақ статистика ақпаратты жою немесе өзгерту және ақпараттық жүйе жұмысын бұзу жағдайларының артқанын көрсетеді. Бұл киберқылмыспен күресу шараларын одан әрі күшейту және құқық қорғау органдары қызметінің тиімділігін арттыру қажеттілігін көрсетеді.

Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың түсінігі мен саралау мәселелеріне арналған бұл бөлім осы саланы заңнамалық реттеудегі қиындықтар мен кемшіліктерді анықтауға мүмкіндік береді. Негізгі мәселелердің бірі – ақпараттық технологиялардың қарқынды дамуы, ол құқықтық реттеу деңгейіне сәйкес келе бермейді. Бұл саладағы қылмыстық құқық бұзушылықтарды саралау да қиындық туғызады, өйткені технологиялық жаңалықтар ақпараттық қылмыстық құқық бұзушылықтың бет-бейнесін үнемі өзгертіп отырады және заңнама осы өзгерістерге үнемі бейімделуі керек. Оның үстіне, әртүрлі тараптардың – құқық қорғау органдарының, ақпараттық технологиялар саласындағы мамандардың және қоғамның мүдделерін кешенді талдауды және үйлестіруді талап ететін мұндай қылмыстық құқық бұзушылықтарды анықтау мен саралауда бірыңғай көзқарасты қамтамасыз ету қажеттілігі туындайды. Бұл мәселелерді шешу технологияның қарқынды даму қарқынын және олардың қазіргі қоғамға әсерін ескере отырып, жүйелі көзқарас пен заңнамалық актілерді мұқият қарастыруды талап етеді.

2 ТАРАУ АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТЫҢ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ СИПАТТАМАСЫ

2.1 Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объектісінің ерекшеліктері

Бұл тарау ақпараттандыру және байланыс саласындағы құқық бұзушылықтардың қылмыстық-құқықтық сипаттамаларына арналған, мұндай қылмыстық құқық бұзушылықтар контекстіндегі объектімен, субъектісімен, және жазамен байланысты бірегей аспектілерін ашады. Зерттеу осы саладағы қылмыстық құқық бұзушылық объектісінің белгілерін талдаудан басталады, өйткені қазіргі қоғамда ақпарат пен коммуникация негізгі рөл атқарады, бұл ақпараттық қауіпсіздікті және оны қорғауды ерекше өзекті етеді. Келесі кезекте, қылмыстық құқық бұзушылықты құрайтын әрекеттерді анықтаудағы қиындықтарды қамтитын, әсіресе үздіксіз дамып келе жатқан технологиялар жағдайында мұндай құқық бұзушылықтардың объективтік жағының мәселелері қарастырылады. Субъективті сұрақтар киберқылмыстың негізінде жатқан мотивтер мен ниеттерді зерттейді, мұндай әрекеттердің алдын алу және онымен күресудің тиімді шараларын әзірлеу үшін қылмыскерлердің психологиясын түсінудің маңыздылығын атап көрсетеді. Бұл саладағы қылмыстық құқық бұзушылықтың нысанасы заңсыз әрекеттерден қорғалуы тиіс нақты деректер немесе ақпараттық активтерді сипаттайды. Тарау киберқылмысты болдырмау және алдын алу контекстінде қолданыстағы санкциялар мен олардың барабарлығын зерттейтін жаза тағайындау мәселелерін талқылаумен аяқталады. Тұтастай алғанда, бұл тарауда қылмыстық ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды реттейтін күрделі заңнамалық базаны жүйелі түрде зерттеуге және бағалауға, сот орындау тәжірибесін жетілдіру жолдарын ұсынуға ұмтылады.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық объектісінің белгілері осы саланың ерекше белгілерімен анықталады. Ақпарат заңмен қорғалатын негізгі ресурс болып табылады және оны теріс пайдалану жеке адамға да, жалпы қоғамға да елеулі зиян келтіруі мүмкін. Осы саладағы қылмыстық құқық бұзушылық объектілері компьютерлік жүйелер, деректер базалары, ақпараттық желілер, электрондық құжаттар және цифрлық инфрақұрылымның басқа элементтері болуы мүмкін. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық объектісінің ерекшелігі оның қылмыстық құқық бұзушылықтарды ашу мен жолын кесуді қиындатуы мүмкін виртуалды сипаты болып табылатынын атап өткен жөн. Сонымен қатар, технологияның дамуы мен ақпараттық желілердің кеңеюіне байланысты осы саладағы қауіп-қатер объектілері үнемі дамып, жаңа нысандарға ие болып, заңнама мен киберқылмыспен күресу әдістерін үнемі жетілдіруді талап етеді.

Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық объектісінің белгілерін түсіну қылмыстық әрекеттерді тиімді жолын кесу және ақпараттық кеңістіктің қауіпсіздігін қамтамасыз ету үшін қажет.

Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объектісі ақпараттық жүйелер мен байланыс желілерінің қалыпты жұмыс істеуін, сондай-ақ ақпараттың қауіпсіздігін қамтамасыз ететін қоғамдық қатынастар болып табылады. Бұл тұрғыда объектіні үш категорияға бөлуге болады: тікелей, жалпы және топтық. Тікелей объект теріс пайдаланатын нақты ақпараттық жүйелер, деректер базалары және желілер жатады. Жалпы объект – рұқсат етілмеген қол жеткізуден және кедергілерден қорғауды қоса алғанда, бүкіл цифрлық инфрақұрылымды қамтитын кеңірек санат. Топтық объект әртүрлі субъектілерге тиесілі және жалпы қоғамның ақпараттық қауіпсіздігін қамтамасыз ету үшін пайдаланылатын ақпараттық активтердің жиынтығын біріктіреді. Бұл аймақтағы объектінің ерекшелігі оның виртуалды табиғатымен анықталады, бұл сәйкестендіру мен қорғауды қиындатады. Заманауи технологиялар үнемі дамып келеді және осы саладағы қауіп-қатер нысандары да дамып келеді, олар барабар құқықтық реттеуді және киберқылмыспен күресудің жетілдірілген әдістерін талап етеді.

Ақпараттандыру және байланыс саласындағы құқық бұзушылықтар объектісі ақпараттық-коммуникациялық жүйелерді пайдалану мен қорғауға қатысты барлық аспектілерді қамтитындықтан, қазіргі қоғамда ерекше маңызға ие. Ақпараттық ресурстар мен коммуникациялық желілер адам қызметінің әртүрлі салаларының, соның ішінде экономика, менеджмент, ғылым, білім және жеке өмірдің қызмет етуінің негізі болды.

Цифрлық дәуірдегі ақпарат сауданың объектісі де, қылмыстық шабуылдардың нысанасы да бола алатын негізгі ресурс болып табылады. Ақпаратқа қол жеткізуді қамтамасыз ететін компьютерлік жүйелер, мәліметтер базасы және желілер өмірдің әртүрлі салаларының тұрақтылығы мен тиімділігін сақтауда маңызды рөл атқарады. Бұл жүйелерді бұзу немесе заңсыз араласу ауыр зардаптарға әкелуі мүмкін.

Біріншіден, мұндай құқық бұзушылықтардың экономикалық салдары айтарлықтай болуы мүмкін. Жүйелері шабуылға ұшыраған компаниялар мен ұйымдар деректерді ұрлау, жүйенің бұзылуы немесе қалпына келтіру әрекеттерінің қажеттілігі салдарынан айтарлықтай қаржылық шығындарға ұшырауы мүмкін . Құпия ақпаратты жоғалту сонымен қатар клиенттер мен серіктестердің сеніміне нұқсан келтіруі мүмкін, бұл бизнестің беделі мен одан әрі дамуына теріс әсер етеді.

Екіншіден, мұндай құқық бұзушылықтар ұлттық қауіпсіздікке қатер төндіруі мүмкін. Мемлекеттік ақпараттық жүйелерге жасалған шабуылдар құпия ақпараттың ағып кетуіне және энергетика, көлік және байланыс сияқты маңызды инфрақұрылымдардың бұзылуына әкелуі мүмкін. Бұл өз кезегінде қоғамдық тәртіп пен азаматтардың қауіпсіздігіне қауіп төндіруі мүмкін.

Үшіншіден, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар азаматтардың жеке өміріне орны толмас зиян келтіруі мүмкін. Медициналық жазбалар, қаржылық ақпарат және басқа да құпия ақпарат сияқты жеке ақпаратты ұрлау алаяқтықтың, бопсалаудың және жеке өмірді бұзудың әртүрлі түрлеріне әкелуі мүмкін. Сонымен, ақпараттандыру және байланыс саласындағы құқық бұзушылық нысанасының маңыздылығы оның қазіргі қоғамның барлық аспектілерінің тұрақтылығы мен қауіпсіздігін қамтамасыз етудегі шешуші рөлінде. Ақпараттық ресурстар мен коммуникация жүйелерін қорғау кешенді көзқарасты және осы саладағы қылмыстық құқық бұзушылықтардың алдын алуға және жолын кесуге бағытталған құқықтық және техникалық шараларды ұдайы жетілдіруді талап етеді.

1997 жылы Ресей Федерациясының Қылмыстық кодексінің күшіне енуімен Ресей Федерациясының Қылмыстық кодексіне (ҚК) 28-тарауды енгізудің орындылығы мен қажеттілігі туралы ғылыми пікірталастар жалғасуда - «Компьютерлік ақпарат саласындағы қылмыстар. Ғылыми әдебиеттерді талдау Ресейде, сондай-ақ халықаралық қылмыстық саясатта бұл мәселені шешудің бірнеше тәсілдері бар екенін көрсетеді. Осылайша, кейбір батыс зерттеушілері бұл қылмыстардың барлығын қазіргі «дәстүрлі» қылмыстық құқық бұзушылықтардың ерекше түрі деп санайды. Мұндағы ерекшелік, олардың пікірінше, заңсыз мақсаттарға жету үшін тек компьютерді немесе компьютерлік технологияны пайдалану болып табылады.

Бүгінгі таңда ақпараттық қоғамдағы қызмет ақпаратпен, ақпараттық ресурстармен және ақпараттық өнімдермен жұмыс істеуге негізделген. Осыған байланысты қазіргі қоғамның құқықтық негізі болып табылатын ақпараттық құқықтың негізгі мақсаты ақпаратпен жұмыс істеу кезінде туындайтын қатынастарды реттеу болып табылады. Дәл ақпарат қоғамның қозғаушы күші болып табылатын озық технология кезеңінде ол жеке адамға және жалпы қоғамға да үлкен қауіп төндіруі мүмкін. Сондықтан ақпаратты заңсыз бұзудан, заңсыз жинаудан, сақтаудан және өңдеуден қорғау қажет [57,б.9].

Ақпараттық қатынастарды реттейтін заңнаманы бұзғаны үшін құқықтық жауапкершіліктің бірқатар ерекше белгілері бар. Бұл саладағы қылмыстық құқық бұзушылық әрқашан ақпаратпен байланысты, сондай-ақ егер олар ақпаратқа тікелей қатысты болса ғана емес, сонымен бірге оның материалдық тасымалдаушысының болуы арқылы делдалдық болса, ақпараттық және құқықтық деп санауға болады. Ақпараттық саладағы құқық бұзушылықтың объектісі ақпараттық жүйелер мен байланыс желілерінің қалыпты жұмыс істеуін, сондай-ақ ақпараттың қауіпсіздігін қамтамасыз ететін қоғамдық қатынастардың жиынтығы болып табылатынын атап өткен жөн. Қосымша объект бағдарлама жасаушылар мен бағдарламалық өнімдердің авторлық құқығы болуы мүмкін. [58, б.673].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объектісі ақпараттық жүйелер мен байланыс желілерінің қалыпты жұмыс істеуін, сондай-ақ ақпараттың қауіпсіздігін қамтамасыз ететін қоғамдық

қатынастар болып табылады. Бұл қатынастарға ақпаратты пайдалану мен қорғауға байланысты жеке және заңды тұлғалардың құқықтары мен мүдделері, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз етудегі мемлекеттің мүдделері жатады.

Бұл тұрғыда объектіні үш категорияға бөлуге болады: тікелей, жалпы және топтық.

Тікелей объектіге теріс пайдаланатын нақты ақпараттық жүйелер, деректер базалары және желілер жатады. Бұл кәсіпорындардың компьютерлік желілері, мемлекеттік органдардың деректер базалары, қаржылық ұйымдардың ақпараттық жүйелері және қылмыстық шабуылдардың тікелей нысанасына айналатын цифрлық инфрақұрылымның басқа элементтері болуы мүмкін.

Жалпы объект – рұқсат етілмеген қол жеткізуден және кедергілерден қорғауды қоса алғанда, бүкіл цифрлық инфрақұрылымды қамтитын кеңірек санат. Бұған қоғамның әртүрлі салаларының қызметін қамтамасыз ететін, киберқауіптерден және қылмыстық әрекеттің басқа да нысандарынан қорғалуы тиіс барлық ақпараттық-коммуникациялық жүйелер жатады [59].

Топтық объект әртүрлі субъектілерге тиесілі және жалпы қоғамның ақпараттық қауіпсіздігін қамтамасыз ету үшін пайдаланылатын ақпараттық активтердің жиынтығын біріктіреді. Бұл біріктірілген мәліметтер базасы, әртүрлі ұйымдар мен мекемелер арасындағы ақпарат алмасу жүйелері, сондай-ақ ақпараттық кеңістікті қорғау мен тұрақтылығын қамтамасыз ету үшін бірлесіп пайдаланылатын кез келген басқа ақпараттық ресурстар болуы мүмкін (3-сурет).

Сурет 3 – Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объектілері

Бұл аймақтағы объектінің ерекшелігі оның виртуалды табиғатымен анықталады, бұл сәйкестендіру мен қорғауды қиындатады. Ақпараттық ресурстардың физикалық нысаны жоқ, бұл оларды қорғауды қиындатады және олардың қауіпсіздігін қамтамасыз ету үшін арнайы білім мен технологияларды қажет етеді. Заманауи технологиялар үнемі дамып келеді және осы саладағы қауіп-қатер нысандары да дамып келеді, олар барабар құқықтық реттеуді және киберқылмыспен күресудің жетілдірілген әдістерін талап етеді.

Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объектісі ақпараттық жүйелер мен байланыс желілерін пайдаланумен, қорғаумен және жұмыс істеуімен байланысты қоғамдық қатынастардың бүкіл кешенін қамтиды, бұл оны қорғауды қазіргі заманның маңызды міндеттерінің біріне айналдырады. құқықтық жүйе. Келесі кезекте құқық бұзушылықтың жалпы объектісін, оның ішінде жалпы объект ұғымын және ақпараттық жүйелер мен желілердің қоғамдағы рөлін толығырақ қарастырамыз. Содан кейін біз топтық және тікелей объектілерді қарастыруға көшеміз, қауіп төндіретін объектілерді талдаймыз және заңнаманы жетілдіру бойынша ұсыныстармен қорытындылаймыз.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың *жалпы объектісі бүкіл цифрлық инфрақұрылымның қалыпты жұмыс істеуін қамтамасыз ететін қоғамдық қатынастардың жиынтығы болып табылады.* Бұған қазіргі ақпараттық қоғамның негізі болып табылатын ақпараттық жүйелер, коммуникациялық желілер, мәліметтер базасы және басқа да компоненттер жатады. «Ақпараттандыру туралы» Қазақстан Республикасының Заңына сәйкес ақпараттандыру объектілері болып электрондық ақпараттық ресурстар, ақпараттық-коммуникациялық инфрақұрылым объектілері және рұқсат етілмеген қол жеткізу мен араласудан қорғалуы тиіс жүйелер табылады. Жалпы объект ақпаратты құру, сақтау, өңдеу және берумен байланысты барлық элементтерді қамтиды және тұтастай алғанда ақпараттық инфрақұрылымның қауіпсіздігі мен тұтастығын қамтамасыз етуге бағытталған [60].

Ақпараттық жүйелер мен желілер өмірдің барлық дерлік саласының құрамдас бөлігі бола отырып, қазіргі қоғамда шешуші рөл атқарады. Олар мемлекеттік және жеке мекемелердің, қаржы ұйымдарының, білім беру және медициналық мекемелердің жұмыс істеуін, сондай-ақ азаматтардың күнделікті өмірін қамтамасыз етеді. «Ақпараттандыру туралы» Қазақстан Республикасының Заңына сәйкес ақпарат объектілерінің иелері ақпараттың қорғалуын, үшінші тұлғалардың құқықтары мен заңды мүдделерінің сақталуын қамтамасыз етуге, сондай-ақ ақпараттық қауіпсіздік инциденттерінің алдын алу бойынша шаралар қабылдауға міндетті.

Ақпараттық жүйелер мен желілер басқару тиімділігін арттыруға, көрсетілетін қызметтердің сапасын жақсартуға, ақпарат алмасуды жеделдетуге және әртүрлі

процестерде ашықтық пен есептілікті қамтамасыз етуге көмектеседі. Олар сонымен қатар бизнестің цифрлық трансформациясын жеңілдету және жаңа кәсіпкерлік мүмкіндіктер жасау арқылы экономикалық дамуда маңызды рөл атқарады. Дегенмен, ақпараттық технологияларға тәуелділіктің артуымен киберқауіптердің қаупі де артады, бұл барабар құқықтық реттеуді және қорғау әдістерін үнемі жетілдіруді талап етеді [61].

Ақпараттандыру және байланыс саласындағы құқық бұзушылықтың *топтық объектісі – әртүрлі субъектілерге тиесілі және жалпы қоғамның ақпараттық қауіпсіздігін қамтамасыз ету үшін пайдаланылатын ақпараттық құндылықтардың жиынтығы.* Бұл тұжырымдама деректерді қорғау, құпиялылықты қамтамасыз ету және ақпараттық жүйелердің тұтастығын сақтау сияқты ортақ мақсаттарға жету үшін біріктірілуі мүмкін ақпараттық ресурстар мен жүйелердің әртүрлі түрлерін қамтиды. «Ақпараттандыру туралы» Қазақстан Республикасының Заңына сәйкес ақпарат объектілерінің меншік иелері объектілердің меншік иелерінің және үшінші тұлғалардың құқықтары мен заңды мүдделерін сақтауға, сондай-ақ ақпарат объектілерін қорғау жөніндегі шараларды қолдануға міндетті [62].

Ақпараттық қылмыстық құқық бұзушылықтардың топтық объектілерін жіктеу ақпараттық жүйедегі атқаратын қызметтері мен рөліне қарай бірнеше категорияларды қамтиды. Ең алдымен, бұл мемлекеттік және қоғамдық институттардың жұмыс істеуін қамтамасыз етуде шешуші рөл атқаратын аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектілері. Бұл нысандарға мемлекеттік органдардың, қаржы институттарының, медициналық мекемелердің бақылау жүйелері және басқа да негізгі инфрақұрылым элементтері кіреді. «Ақпараттандыру туралы» Қазақстан Республикасының Заңына сәйкес мұндай объектілердің иелері жедел ақпараттық қауіпсіздік орталықтарын құруға немесе үшінші тұлғалардан тиісті қызметтерді сатып алуға міндетті.

Тағы бір маңызды категория – электрондық мемлекеттік жүйелердің жұмыс істеуін қамтамасыз ететін объектілер. Бұл жүйелерге азаматтардың интернет арқылы мемлекеттік қызметтерге қол жеткізуін қамтамасыз ететін мәліметтер базасы мен ақпараттық жүйелер кіреді (Мысалы: egov.kz). Осы объектілердің иелері «электрондық үкіметтің» ақпараттандыру объектілері туралы мәліметтерді есепке алуды және жаңартуды және электрондық ақпараттық ресурстардың резервтік көшірмелерін бірыңғай ұлттық резервтік сақтау платформасына көшіруге міндетті.

Қорғалатын ақпараттық активтер – қоғам мен мемлекеттің жұмыс істеуі үшін маңыздылығына байланысты ерекше қорғалатын және қорғалатын ақпараттық ресурстар, деректер мен жүйелер. Бұл активтерге азаматтардың жеке деректері, мемлекеттік және жеке ұйымдардың құпия ақпараты, сондай-ақ рұқсатсыз кіруден, жоғалтудан немесе өзгертуден қорғауды талап ететін басқа да деректер кіреді. Қазақстан Республикасының заңнамасына сәйкес ақпараттық технологиялар объектілерінің меншік иелері осы активтердің қорғалуын

қамтамасыз етуге және ақпараттық қауіпсіздік инциденттерін болғызбау жөнінде шаралар қабылдауға міндетті.

Қорғалатын ақпараттық активтердің маңыздылығы олардың ақпараттық қауіпсіздікті және ақпараттық жүйелердің тұрақтылығын қамтамасыз етудегі маңызды рөлінде. Бұл активтерді тиісті түрде қорғамау маңызды салдарға, соның ішінде құпия деректердің жоғалуына, негізгі инфрақұрылымның бұзылуына және ұлттық қауіпсіздікке нұқсан келтіруге әкелуі мүмкін. Сондықтан заңнама мұндай активтерді қорғауға қатаң талаптар қояды және ақпараттық технологиялар объектілерінің иелеріне олардың қауіпсіздігін қамтамасыз ету жөніндегі міндеттемелерді белгілейді [63].

Цифрлық трансформация web3 және MetaVerse сияқты жаңа технологияларды белсенді пайдалану ақпараттық активтерді қорғау тәсілдерін қайта қарауды талап етеді. Сетураман бизнес деректер қауіпсіздігі мен құпиялылық міндеттемелерін сақтай отырып, бәсекеге қабілетті болып қалу үшін цифрлық түрлендіру бойынша күш-жігерін еселеуі керек екенін атап көрсетеді. Қауіпсіз деректерді ортақ пайдалану үшін бұлтты нарықтарды пайдалану ұйымдарға ортақ мәселелерді шешу және зияткерлік меншікті бұзбай маңызды зерттеулер жүргізу үшін бірлесіп жұмыс істеуге жаңа мүмкіндіктер ашады.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың *тікелей объектісіне құқыққа қайшы әрекеттерге жататын нақты ақпараттық жүйелер, мәліметтер базасы және желілер жатады.* Бұл элементтер заманауи цифрлық инфрақұрылымның негізі және көптеген ұйымдар үшін маңызды ресурстар болып табылады. Ақпараттық жүйелер процестерді автоматтандыруды және басқаруды қамтамасыз етеді, деректер базасы деректердің маңызды көлемін сақтайды және өңдейді, ал желілер ақпарат алмасуға мүмкіндік беретін цифрлық экожүйенің әртүрлі құрамдастарын байланыстырады.

Бұл құрамдастарды қорғау басымдылық болып табылады, өйткені олардың ымыраға келуі елеулі зақымға, деректердің жоғалуына және ұйымдардың қалыпты жұмысының бұзылуына әкелуі мүмкін. Лазарева Т. атап өткендей, осы саладағы құқықтық реттеу виртуалды объектілердің сипаттамаларын ескеруі керек, бұл жаңа заңнамалық тәсілдерді әзірлеуді талап етеді [64].

Қазіргі ақпараттық жүйелер мен желілер виртуалды сипатқа ие, бұл оларды қорғауды және құқықтық реттеуді айтарлықтай қиындатады. Цифрлық деректер, бағдарламалар және онлайн қызметтер сияқты виртуалды объектілердің физикалық көрінісі жоқ, бірақ нақты құндылығы бар және құқық бұзушылықтың нысанасы болуы мүмкін. Виртуалды объектілер пара алу және алаяқтық сияқты қылмыстық әрекеттердің объектісіне айналады, бұл қылмыстық заңнаманы цифрлық дәуірдің жаңа сын-қатерлеріне бейімдеуді талап етеді.

Кейбір елдерде, мысалы, Қытай мен Тайваньда виртуалды объектілерді меншік құқығының объектілері ретінде тану олардың маңыздылығын және оларды құқықтық қорғау қажеттілігін растайды. Виртуалды объектілерге қатысты істер

бойынша соттар осы мүліктің экономикалық құндылығын ескереді және оларды меншік объектілері деп таниды. Бұл пайдаланушыларға виртуалды активтерге құқықтарын қорғауға және жоғалған жағдайда өтемақы талап етуге мүмкіндік береді. Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың тікелей объектісіне өзінің маңыздылығына байланысты ерекше қорғауды қажет ететін нақты ақпараттық жүйелер, мәліметтер базасы және желілер жатады. Бұл объектілердің виртуалды сипаты оларды құқықтық қорғауды қиындатады және жаңа заңнамалық тәсілдерді әзірлеуді талап етеді. Пайдаланушылардың құқықтарын тиімді қорғау және цифрлық саладағы құқық бұзушылықтардың алдын алу үшін виртуалды объектілердің экономикалық құндылығын ескеру және оларды меншік құқығының объектілері ретінде тану маңызды.

Бұл аймақтағы объектілердің ерекшелігі олардың виртуалды табиғатымен анықталады, бұл оларды анықтау мен қорғауды қиындатады. Заманауи технологиялар үнемі дамып келеді және осы саладағы қауіп-қатер нысандары да дамып келеді, олар барабар құқықтық реттеуді және киберқылмыспен күресудің жетілдірілген әдістерін талап етеді.

Төменде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық объектілерінің санаттары, олардың негізгі элементтері мен мағынасы жүйеленген 2-кестеде берілген.

Кесте 2 – Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объектілері

Объекті категориясы	**Сипаттама**	**Маңызды элементтер**	**Мағынасы**
Тікелей объект	Арнайы ақпараттық жүйелерді, дерекқорларды және теріс пайдаланылуы мүмкін желілерді қамтиды	- Ақпараттық жүйелер - Дерекқор - Желілер	Автоматтандыруды және процестерді басқаруды, деректерді сақтау мен өңдеуді, ақпарат алмасуды қамтамасыз етеді

Жалпы объект	Бүкіл цифрлық инфрақұрылымның қалыпты жұмыс істеуін қамтамасыз ететін әлеуметтік қатынастардың жиынтығы	- Ақпараттық жүйелер - Коммуникациялық желілер - Дерекқор	Бүкіл ақпараттық инфрақұрылымның қауіпсіздігі мен тұтастығын қамтамасыз етеді, басқару тиімділігі мен көрсетілетін қызметтердің сапасын арттырады
Топтық объект	Қоғамның ақпараттық қауіпсіздігін қамтамасыз ету үшін пайдаланылатын әртүрлі субъектілерге тиесілі ақпараттық активтердің жиынтығы	- маңызды ақпараттық-коммуникациялық инфрақұрылым объектілері - электронды үкімет жүйелері	Мәліметтердің қорғалуын, ақпараттық жүйелердің құпиялылығы мен тұтастығын қамтамасыз етеді, ұлттық қауіпсіздікті қолдайды

Сонымен, технологияның дамуы мен цифрландырудың өсуімен ақпарат пен желілер киберқылмыскерлердің басты нысанасына айналуда. Технологияларды үнемі жаңарту шабуылдаушылар пайдалана алатын жаңа осалдықтардың пайда болуына әкеледі. Павлов А. атап өткендей, технологияның қарқынды дамуы киберқауіпсіздікті қамтамасыз ету тәсілдерін үнемі жаңартып отыруды талап етеді, өйткені кибершабуылдар күрделене түседі және оны анықтау қиынға түседі [65].

Жыл сайын жасанды интеллект (AI) және заттар интернеті (IoT) сияқты жаңа технологиялар пайда болады, олар бір жағынан бизнес пен қоғамға айтарлықтай пайда әкелсе, екінші жағынан шабуылдың жаңа векторларын жасайды. Пандей мен Сайяд бұл технологиялар операциялық тиімділікті арттырып қана қоймай, киберқылмыскерлерге жаңа мүмкіндіктер ашатынын, бұл қорғаныс шараларын бейімдеуді талап ететінін атап көрсетеді. Шабуыл жасаушылар шабуылдың жаңа әдістерін жасап, жаңа осалдықтарды тапқан кезде киберқауіптердің жаңа түрлері пайда болуда. Заманауи кибершабуылдарға фишинг, зиянды бағдарлама (соның ішінде төлем бағдарламалық құралы), кеңейтілген тұрақты қауіптер (APT) және жеткізу тізбегі шабуылдары жатады. Ransomware сияқты зиянды бағдарламалар деректерге қол жеткізуді блоктайды және оның құлпын ашу үшін төлемді талап етеді, бұл айтарлықтай қаржылық және беделді жоғалтуға әкелуі мүмкін [90].

Фишинг пен әлеуметтік инженерия ең көп таралған шабуыл әдістерінің бірі

болып қала береді, өйткені олар адамның әлсіздігі мен сенімін пайдаланады. Бұл шабуылдар көбінесе тіркелгі деректері, қаржылық ақпарат немесе корпоративтік желілерге кіру сияқты құпия ақпаратты алуға бағытталған. Заманауи технологиялар шабуылдаушыларға бұл шабуылдарды автоматтандыруға және оларды үлкен көлемде жүзеге асыруға мүмкіндік береді, бұл оларды аса қауіпті етеді. Жеткізу тізбегіне шабуылдар жиілеп барады, өйткені компаниялар өздерінің ақпараттық технологиялары мен қызметтері үшін сыртқы жеткізушілерге көбірек сенім артады. Шабуылшылар соңғы пайдаланушы деректері мен жүйелеріне қол жеткізу үшін жеткізушілердің жүйелеріндегі осалдықтарды пайдалана алады, бұл серіктестерді мұқият таңдау және жеткізу тізбегінің барлық деңгейлерінде қатаң қауіпсіздік шараларын енгізу қажеттілігін көрсетеді [66].

Осылайша, қауіп-қатер объектілерін талдау технологиялардың үнемі дамуы және қауіптердің жаңа нысандарының пайда болуы киберқорғаныс әдістерін үнемі жаңартуды және жетілдіруді талап ететінін көрсетеді. Қауіпсіздікті қамтамасыз ету үшін жаңа технологияларды әзірлеу ғана емес, сонымен қатар қызметкерлерді оқыту, тұрақты аудит пен тестілеу жүргізу, сенімді жеткізушілермен ынтымақтастық орнату маңызды. Киберқауіпсіздікке кешенді көзқарас қана үнемі өзгеріп отыратын киберқауіптердің ландшафты жағдайында деректер мен жүйелердің сенімді қорғалуын қамтамасыз ете алады.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың мақсаттарын түсіну киберқылмыспен тиімді күресу үшін өте маңызды. Бұл саладағы құқық бұзушылықтың объектілері ақпараттық жүйелер мен байланыс желілерінің қалыпты жұмыс істеуін, сондай-ақ ақпараттың қауіпсіздігін қамтамасыз ететін қоғамдық қатынастар болып табылады. Қауіп дәрежесін барабар бағалау және тиімді қорғаныс шараларын әзірлеу үшін осы объектілерді нақты анықтау және жіктеу маңызды. Қылмыстың объектісі – бұл қылмыстық әрекетті жасаушы адамның қол сұғатын нәрсесі, қылмыстың нәтижесінде не келтірілген немесе зиян келтіруі мүмкін. Осылайша, осы субъектілерді егжей-тегжейлі түсіну құқық қорғау органдары мен заң шығарушыларға киберқылмыстардың алдын алуға және оған қарсы күресуге бағытталған неғұрлым дәл және тиімді құқықтық реттеулерді жасауға көмектеседі.

Ақпараттандыру және байланыс саласындағы объектілерді тиісінше қорғауды қамтамасыз ету үшін қолданыстағы заңнаманы жетілдіру қажет. Ең алдымен технологияның серпінді дамуын ескеріп, құқықтық нормаларды цифрлық әлемнің жаңа шындықтарына бейімдеу керек. Заң шығарушылар жаңа қауіп-қатерлердің пайда болуын белсенді түрде бақылап, нормативтік актілерге ағымдағы сын-қатерлер мен қауіптерді көрсететіндей өзгерістер енгізуі қажет.

Заңнамаларды жетілдірудің негізгі бағыттарының бірі тұжырымдамалық аппаратты кеңейту және нақтылау болып табылады. Құқықтық белгісіздікке жол бермеу және құқық қолдану тәжірибесінің бірлігін қамтамасыз ету үшін «виртуалды объектілер», «киберкеңістік», «цифрлық инфрақұрылым» және басқалар сияқты терминдерді нақты анықтау қажет. Сондай-ақ виртуалды

объектілер мен қорғалатын ақпараттық активтер айналымы саласындағы құқықтық қатынастарды реттейтін арнайы ережелерді әзірлеу маңызды, бұл киберқауіптердің өсуі жағдайында ерекше маңызды.

Сонымен қатар, киберқауіпсіздік саласындағы халықаралық ынтымақтастықты дамытуға назар аудару қажет. Киберқылмыстар көбінесе трансшекаралық сипатқа ие және олармен тиімді күресу әртүрлі мемлекеттердің күш-жігерін үйлестірусіз мүмкін емес. Осы тұрғыда елдер арасындағы тәжірибе мен озық тәжірибе алмасу, сондай-ақ киберқылмыспен бірлесіп күресуге бағытталған халықаралық келісімдерді әзірлеу пайдалы болуы мүмкін.

Сондай-ақ киберқауіпсіздік саласындағы мамандардың хабардар болу және оқыту деңгейін арттыру маңызды аспект болып табылады. Құқық қорғау органдары қызметкерлеріне, заңгерлерге және IT мамандарына арналған тұрақты тренингтер мен білім беру бағдарламалары киберқылмыстың ерекшеліктерін жақсы түсінуге және жаңа сын-қатерлерге тиімді әрекет етуге көмектеседі. Осылайша, ақпараттандыру және байланыс саласындағы заңнаманы жетілдіру киберқауіпсіздіктің техникалық және құқықтық аспектілерін де ескеретін құқықтық қорғаудың кешенді жүйесін құруға бағытталуы тиіс. Тек осы тәсіл заманауи қауіптерге тиімді қарсы тұрады және ақпараттық жүйелер мен желілердің сенімді қорғалуын қамтамасыз етеді.

2.2 Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағының мәселелері

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағының мәселелеріне қылмыстық құқық бұзушылықтарды анықтау, құжаттау және дәлелдеумен байланысты бірқатар қиындықтар жатады. Осы саладағы көптеген қылмыстық құқық бұзушылықтардың виртуалды сипаты оларды ашуды қиындатады, өйткені олар көбінесе ашылмай қалады немесе арнайы тергеу әдістерін қажет етеді. Сонымен қатар, көптеген киберқылмыскерлер анонимді немесе қауіпсіз байланыс құралдарын пайдаланады, бұл оларды анықтау мен қудалауды қиындатады. Тағы бір қиындық аумақтық белгісіздік болып табылады, өйткені киберқылмыстар әлемнің кез келген жерінен жасалуы және юрисдикция шекараларын кесіп өтуі мүмкін. Бұл әртүрлі елдердің құқық қорғау органдарының ынтымақтастығында қиындықтар туғызып, мұндай қылмыстық құқық бұзушылықтардың жолын кесуді қиындатады. Сонымен қатар, технологиялық дамудың жылдам қарқыны ақпараттық саладағы жаңа қауіптер мен сын-қатерлерге сәйкес келетіндей заңнаманы және киберқылмыспен күресу әдістерін үнемі жаңартып отыруды талап етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағына ақпараттық жүйелер мен желілерді

пайдаланудың белгіленген тәртібін бұзатын әрекеттер немесе әрекетсіздік жатады. Мұндағы негізгі мәселелер қылмыстық құқық бұзушылықтың субъектісін, қылмыстық құқық бұзушылық жасау құралдарын және қылмыстың факультативті белгілерін анықтаумен байланысты. Қылмыс құралдарына компьютерлер, желілер және мамандандырылған хакерлік бағдарламалық қамтамасыз ету сияқты әртүрлі техникалық құралдар жатады. Қылмыстық құқық бұзушылықтың факультативті белгілеріне қылмыстың жасалу тәсілі, орны және уақыты кіруі мүмкін. Киберқылмыстардың аумақтық белгісіздігі және анонимділігі оларды сәйкестендіру мен құжаттандыруда қосымша қиындықтар туғызады. Технологияның қарқынды дамуы ақпараттық саладағы жаңа қауіптерге тиімді қарсы тұру үшін заңнамалық база мен тергеу әдістерін үнемі жаңартып отыруды талап етеді.

Қылмыстық құқық бұзушылықтың объективтік жағы қылмыстық әрекеттің мәнін және оның құқықтық квалификациясын түсінуде шешуші рөл атқарады. Қылмыстық құқық бұзушылықтар көбінесе виртуалды сипатта болатын ақпараттандыру және байланыс саласында объективтік жағын егжей-тегжейлі талдау ерекше маңызға ие. Ол әрекетті қылмыс ретінде квалификациялайтын нақты әрекеттерді (немесе әрекетсіздікті), салдарды және себеп-салдарлық байланыстарды қамтиды .

Құқық бұзушылықтың объективтік жағы құқыққа қарсы әрекеттің сыртқы көріністерін, оның физикалық құрамын қамтитынын атап өткен жөн . И.В.Маштаковтың еңбектерінде объективтік жағына іс-әрекет немесе әрекетсіздік, қоғамдық қауіпті салдарлар және олардың арасындағы себептік байланыс жатады. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар контекстінде бұл ақпараттық жүйелерге рұқсатсыз кіруді, зиянды бағдарламаларды таратуды, деректерді ұрлауды және цифрлық инфрақұрылымның қалыпты жұмысын бұзатын басқа да заңсыз әрекеттерді білдіруі мүмкін.

Қылмыстық құқық бұзушылықтың объективтік жағын талдау қылмыстық құқық бұзушылықты дұрыс саралау және оларды тергеу үшін өте маңызды. Бұл әрекеттің қылмыстық болғанын және қандай нақты құқық нормалары бұзылғанын анықтауға мүмкіндік беретін объективті жағы екенін атап өтеді. Бұл әсіресе қылмыстық әрекеттер жасырын және техникалық жағынан күрделі болуы мүмкін ақпараттандыру және байланыс саласында маңызды. Объективті жағын егжей-тегжейлі талдау қылмыс жасаудың нақты әдістері мен құралдарын анықтауға, сондай-ақ олардың жәбірленушілер мен жалпы қоғам үшін салдарын анықтауға көмектеседі [67].

Объективті жағын дұрыс түсіну құқық қорғау органдарына ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды тиімді тергеуге және жолын кесуге, сондай-ақ алдын алу шараларын әзірлеуге мүмкіндік береді. А.Н.Федорова атап өткендей, қылмыстық құқық бұзушылықтың объективтік жағын анықтау құқық қолдану және құқықтық жауапкершілік шараларын жүзеге

асыру үшін негіз болып табылады. Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективті жағын түсіну және талдау тиімді құқық қорғау және киберқылмыспен күресудің негізгі аспектілері болып табылады. Бұл технологияның динамикалық дамуы мен қауіп-қатерлердің жаңа нысандарының пайда болуына ілесу үшін құқықтық базаны және тергеу әдістерін үнемі жаңартып отыруды талап етеді.

Бұл бөлімде біз ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағын дәйекті түрде талқылаймыз. Ең алдымен, қылмыстың объектісін, яғни құқық бұзушылық бағытталатын нақты ақпараттық жүйелерді, мәліметтер қорын және компьютерлік желілерді қарастырамыз. Сонымен қатар, қылмыс жасау үшін пайдаланылатын аппараттық және мамандандырылған бағдарламалық құралдар талданады. Қылмыс жасау тәсілдері, орны мен уақыты, сондай-ақ киберқылмыстарға тән анонимдік пен аумақтық белгісіздік мәселелері де қарастырылады. Соңында, мұндай қылмыстық құқық бұзушылықтарды анықтау және құжаттау қиындықтары, оның ішінде дәлелдемелерді жинау және тергеу әдістері талқыланады.

1. Қылмыстық құқық бұзушылықтың объектісі

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объектісі – ақпараттық жүйелер, деректер қоры және компьютерлік желілер, сондай-ақ цифрлық деректер. Бұл жүйелер мен деректерге жасалған құқыққа қайшы әрекеттер олардың тұтастығына, қолжетімділігіне және құпиялылығына зиян келтіреді [68].

Ақпараттық жүйелер – деректерді жинау, сақтау, өңдеу және беру мақсатында қолданылатын аппараттық және бағдарламалық құралдар жиынтығы.

Деректер қоры – мәліметтерді сақтауға және басқаруға арналған құрылымдалған жүйе.

Компьютерлік желілер – пайдаланушылар арасында деректер алмасуды қамтамасыз ететін өзара байланысты құрылғылар кешені.

Киберқылмыстардың нысанасы ретінде электронды түрде сақталған цифрлық деректер де қарастырылады. Мысалы, жеке ақпарат, коммерциялық құпиялар немесе мемлекеттік құпия мәліметтер құқық бұзушылықтың объектісі болуы мүмкін.

2. Қылмыстық құқық бұзушылық жасау құралдары

Киберқылмыстарды жасау үшін әртүрлі аппараттық және бағдарламалық құралдар қолданылады:

Аппараттық құралдар: желілік шабуылдар жасауға арналған құрылғылар (мысалы, серверлерді бұзу үшін қолданылатын арнайы құралдар).

Бағдарламалық құралдар: зиянды бағдарламалар (вирустар, трояндар, ransomware), фишингтік қосымшалар және тыңшылық бағдарламалар.

Бұл құралдар қылмыс жасау кезінде заңсыз рұқсат алуға, деректерді бұзуға немесе жоюға қолданылады. Сонымен қатар, кейбір кибершабуылдар автоматтандырылған ботнеттерді пайдаланумен жүзеге асырылады, бұл

шабуылдардың ауқымын арттырады.

3. Қылмыстық құқық бұзушылық жасау тәсілдері мен ерекшеліктері

Киберқылмыстардың объективтік жағы олардың жасалу тәсілдерінен көрінеді. Мұндай қылмыстық құқық бұзушылықтың жиі кездесетін түрлері:

- Деректерді ұрлау: Жеке деректер немесе коммерциялық құпияларға рұқсатсыз қол жеткізу арқылы жүзеге асырылады. Бұл ақпарат кейіннен сатылуы немесе басқа мақсатта пайдаланылуы мүмкін.
- Кибер тыңшылық: Мемлекеттік немесе коммерциялық деректерге рұқсатсыз қол жеткізу және оларды үшінші тұлғаларға беру.
- Зиянды бағдарламаларды қолдану: Вирустар мен басқа да зиянды бағдарламаларды қолдану арқылы жүйелерді зақымдау немесе мәліметтерді жою.
- Фишинг: Қолданушыларды алдау арқылы олардың жеке деректерін немесе қаржылық мәліметтерін иемдену.

Бұл қылмыстық құқық бұзушылықтардың ерекшелігі – олардың анонимділігі және аумақтық белгісіздігі. Қылмыскерлер әртүрлі елдерден әрекет ете алады, бұл құқық қорғау органдарына тергеу жүргізуді күрделендіреді. Сонымен қатар, қылмыс нақты бір орында жасалмайтындықтан, оның орнын және уақытын анықтау қиынға соғады.

4. Қылмыстық құқық бұзушылықтарды анықтау және дәлелдемелерді жинау

Киберқылмыстарды анықтау және тергеу барысында көптеген қиындықтар туындайды. Дәлелдемелерді жинау қиын болуы мүмкін, себебі қылмыс барысында цифрлық іздер тез жойылады немесе шифрланады. Сонымен қатар, қылмыскерлер VPN немесе анонимайзерлерді қолданып, өздерінің IP мекенжайларын жасыруға тырысады.

Мұндай қылмыстық құқық бұзушылықтарды тергеу үшін арнайы білім мен техникалық құралдар қажет. Киберқылмыстарды анықтау әдістері мыналарды қамтиды:

Желілік трафикті талдау: Шабуылдың қайдан жасалғанын және қандай деректерге қол жеткізілгенін анықтау.

Цифрлық криминалистика: Құрылғылардағы жойылған немесе шифрланған деректерді қалпына келтіру.

Мониторинг және ескерту жүйелері: Кибершабуылдарды алдын ала анықтау үшін желілерді үнемі бақылау [69].

Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объективтік жағы қылмыстың жасалу тәсілдері, құралдары және нысаналары арқылы сипатталады. Киберқылмыстарда заңсыз әрекеттер тек физикалық құрылғыларға ғана емес, сонымен қатар материалдық емес активтерге – цифрлық деректерге бағытталады.

Киберқылмыспен тиімді күресу үшін құқық қорғау органдары ақпараттық жүйелер мен деректердің ерекшеліктерін ескеруі және қорғау шараларын үнемі жетілдіріп отыруы қажет. Жаңа технологиялардың дамуы қылмыстық құқық

бұзушылықтардың жаңа түрлерін тудыратынын ескере отырып, заңнама мен құқық қолдану тәжірибесінде үнемі өзгерістер енгізу маңызды.

Киберқылмыстарда *қылмыстың құралдары* басты рөл атқарады, өйткені олар заңсыз әрекеттерді жасаудың әдістері мен құралдарын анықтайды. Номоконов пен Тропинаның зерттеуіне сәйкес киберқылмыстарға компьютерлік жүйелерді, желілерді және киберкеңістікке қол жеткізудің басқа құралдарын пайдалану арқылы жасалған қылмыстық құқық бұзушылықтар жатады. Мұндай қылмыстық құқық бұзушылықтардың негізгі құралдары шабуылдаушыларға жүйелерге енуге, деректерді шығаруға және зиян келтіруге мүмкіндік беретін аппараттық және арнайы бағдарламалық қамтамасыз ету болып табылады [70].

Киберқылмыс жасау үшін қолданылатын технология аппараттық және бағдарламалық қамтамасыз етудің әртүрлі түрлерін қамтиды. Бозе атап өткендей, компьютерлер, серверлер, желілер және желілік құрылғылар сияқты құрылғылар көбінесе қылмыстық шабуылдардың нысанасы немесе құралдары болып табылады. Шабуылшылар деректерді ұстау немесе таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдары сияқты шабуылдарды жүзеге асыру үшін бұзылған маршрутизаторларды, жалған серверлерді және басқа құрылғыларды пайдаланады. Бұл техникалық құралдар жүйеге жасырын ену және ақпаратпен манипуляциялау мүмкіндігін қамтамасыз етеді [71].

Жеке бағдарламалық қамтамасыз ету киберқылмыскерлердің ең маңызды құралдарының бірі болып табылады. Кучерковтың айтуынша, шабуылдаушылар жүйелерді бұзу және деректерді ұрлау үшін вирустарды, трояндарды, құрттарды және шпиондық бағдарламаларды қоса, зиянды бағдарламалардың әртүрлі түрлерін белсенді пайдаланады. Зиянды бағдарламалық қамтамасыз ету қорқытып алу мақсатында деректерді шифрлау (қарсылық бағдарламалық құрал), құпия сөздерді және басқа да құпия деректерді ұстау (клавиатура) және жаппай шабуылдар үшін пайдаланылатын ботнеттерді жасау сияқты нақты тапсырмаларды орындау үшін әзірленуі мүмкін. Бұл бағдарламалық қамтамасыз ету қылмыскерлерге өз әрекеттерін қашықтан және анонимділіктің жоғары дәрежесімен жүзеге асыруға мүмкіндік береді [72].

Осылайша, киберқылмыс саласындағы қылмыс құралдары шабуылдаушыларға киберкеңістікте заңсыз әрекеттер жасауға мүмкіндік беретін техникалық құралдарды да, арнайы бағдарламалық қамтамасыз етуді де қамтиды. Техникалық құралдар жүйелерге және олардың осалдықтарына қол жеткізуді қамтамасыз етеді, ал мамандандырылған бағдарламалық қамтамасыз ету шабуылдарды жүзеге асыру және деректермен манипуляциялау құралдарын ұсынады. Бұл құралдарды түсіну және талдау киберқылмыстың алдын алу және тергеу бойынша тиімді шараларды әзірлеудің кілті болып табылады.

Қылмыстың факультативті белгілері, мысалы, оның жасалу әдісі, орны және уақыты киберқылмыстарды саралау мен тергеуде маңызды рөл атқарады. Бұл белгілер қылмыстық құқық бұзушылықтарды жасау механизмдерін егжей-

тегжейлі сипаттауға және олардың ерекше белгілерін анықтауға көмектеседі, бұл құқық бұзушылықтарды неғұрлым тиімді ашуға және жолын кесуге ықпал етеді.

Киберқылмыстарды жасау әдісі зиянды бағдарламаны пайдаланудан әлеуметтік инженерияға дейін болуы мүмкін. Оганов атап өткендей, қылмыскерлер өз мақсаттарына жету үшін фишинг, DDoS шабуылдары және желіні бұзу сияқты әртүрлі техникалық құралдар мен тактикаларды пайдаланады. Мұндай қылмыстық құқық бұзушылықтардың орны көбінесе виртуалды болып табылады, бұл оларды тергеуді қиындатады және цифрлық дәлелдемелермен жұмыс істеудің арнайы әдістерін талап етеді. Құқық бұзушылықтарды жасау уақыты да маңызды рөл атқарады, өйткені көптеген шабуылдар жүйелер ең осал кезеңдерге жоспарланады, мысалы, жаңартулар немесе инфрақұрылымды өзгерту кезінде [73].

Киберқылмыстардың негізгі белгілерінің бірі олардың аумақтық белгісіздігі және анонимділіктің жоғары дәрежесі болып табылады. Қылмыскерлер әлемнің кез келген жерінде орналаса алады және өз елінен шықпай-ақ қылмыс жасай алады, бұл юрисдикция мәселелерін және әртүрлі елдердің құқық қорғау органдары арасындағы үйлестіруді қиындатады. VPN және анонимді желілер (мысалы, Tor) сияқты технологиялармен қамтамасыз етілген анонимдік қылмыскерлерге өздерінің жеке басын және орналасқан жерін жасыруға мүмкіндік береді, бұл оларды анықтау мен қудалауды қиындатады. Марас атап өткендей, трафикті анонимдеу және шифрлау тергеушілердің міндетін қиындатады, өйткені олар шабуылдардың көзін оңай анықтай алмайды немесе қылмыскерлерді анықтай алмайды [74].

Осылайша, киберқылмыстың әдісі, орны мен уақыты, аумақтық белгісіздік пен анонимділік сияқты факультативтік белгілер құқық қорғау органдарына айтарлықтай қиындықтар туғызады. Осы аспектілерді түсіну бізге киберқылмыспен күресудің тиімді әдістерін әзірлеуге және осындай құқық бұзушылықтарды ауыздықтау үшін халықаралық органдар арасындағы үйлестіруді жақсартуға мүмкіндік береді.

Киберқылмыстарды анықтау және құжаттау олардың техникалық күрделілігіне және шабуылдаушылардың анонимділігіне байланысты құқық қорғау органдарына айтарлықтай қиындық тудырады. Оганов А.А. атап өткендей, киберқылмыстар құпияның жоғары дәрежесімен және озық технологияларды қолданумен сипатталады, бұл оларды ашуды қиындатады. Сонымен қатар, қылмыскерлер әртүрлі елдерде орналасуы мүмкін, бұл мемлекеттер арасындағы юрисдикция мен үйлестіру үшін қосымша мәселелерді тудырады [75].

Киберқылмыстарды тергеу әдістеріне электронды құрылғылардан деректерді қалпына келтіруге және талдауға бағытталған сандық сот сараптамасын қолдану кіреді. Осы саладағы сарапшылар сандық дәлелдемелерді алу, сақтау және талдау үшін әртүрлі әдістер мен құралдарды пайдаланады. Маңызды аспект – дәлелдемелерді сақтау тізбегін сақтау, бұл оның сотта қабылдануы үшін қажет.

Тергеу процесі бірнеше кезеңдерді қамтиды: медиа таңдау, деректерді сақтау, талдау және есеп беру.

Киберқылмыстағы дәлелдер кіру журналдары, метадеректер, электрондық пошталар және файлдар сияқты сандық деректерді қамтуы мүмкін. Негізгі аспектілердің бірі – деректерді талдау және маңызды дәлелдерді ашу процесін автоматтандыру үшін жасанды интеллектті пайдалану. Жасанды интеллект интеллектталдау процесін айтарлықтай жылдамдатады, бұл тергеушілерге қылмыскерлерді тезірек анықтауға және одан әрі шабуылдардың алдын алуға мүмкіндік береді. Дегенмен, Зак Амос өз жұмысында атап өткендей, ЖИ қолдану ашықтық пен сотта ЖИ негізіндегі тұжырымдардың рұқсат етілуі сияқты қиындықтарды тудырады [76].

Осылайша, киберқылмыстарды анықтау және құжаттау мәселелері озық технологиялар мен мамандандырылған тергеу әдістерін қолдануды талап етеді. Жасанды интеллект пен цифрлық криминалистикалық сараптаманы қолдану қылмысты талдау мен ашу процесін айтарлықтай жақсартуға мүмкіндік береді. Дегенмен, сәтті тергеу дәлелдемелерді сақтау тізбегін қатаң сақтауды және алынған деректердің заңға сәйкестігін талап етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағын талдау киберқылмыспен тиімді күресу үшін аса маңызды. Ол қылмыс жасаудың әдістері, орны мен уақыты, сондай-ақ қылмыскерлердің аумақтық белгісіздігі мен анонимділігі сияқты қылмыстық әрекеттердің негізгі аспектілері мен белгілерін анықтауға мүмкіндік береді. В.В.Григорьев атап өткендей, қазіргі заманғы тергеу әдістері, соның ішінде киберкриминалистика қылмыстық құқық бұзушылықтардың цифрлық іздерін анықтау және құжаттауда шешуші рөл атқарады [77].

Киберқылмыспен күресу әдістерін жетілдіру үшін озық технологиялар мен пәнаралық тәсілді енгізу қажет. А.А.Оганов киберқылмыстар IT-технологиялар саласында арнайы білім мен дағдыларды қажет ететінін, бұл жасырын деректерді тиімдірек тергеуге және анықтауға мүмкіндік беретінін атап көрсетеді. Зак Амос жасанды интеллект пен автоматтандыруды пайдалану киберқауіптерді талдау және анықтау процесін айтарлықтай жылдамдатуы мүмкін екенін атап өтеді [78].

Киберқылмыспен күресу жолын жақсарту бойынша ұсынымдарға құқықтық базаны әзірлеу, құқық қорғау органдары қызметкерлерінің біліктілігін арттыру, озық технологиялар мен тергеу әдістерін енгізу, халықаралық ынтымақтастықты нығайту кіреді. Мемлекеттер бейімделген құқықтық негіздерді құруы, ақпарат алмасуды жақсартуы және халықты хабардар ету бойынша ағымдағы бағдарламаларды жүзеге асыруы керек. Цифрлық криминалистика мен деректерді талдаудың заманауи әдістерін тиімді пайдалана алатын мамандарды даярлауға ерекше назар аудару қажет.

«Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағының мәселелері» 2.2 бөлімін қорытындылай келе, олармен тиімді күресу үшін киберқылмыстардың объективтік жағын кешенді

талдаудың маңыздылығын атап өту қажет. Объективтік жағын талдау қылмыс жасаудың әдісі, орны, уақыты сияқты факторларды, сондай-ақ аумақтық белгісіздікпен және қылмыскерлердің анонимділігімен байланысты белгілерді ескеруді қамтиды. Бұл аспектілер қылмыстық құқық бұзушылықтарды ашу және құжаттандыру және тиімді қарсы шараларды әзірлеу үшін өте маңызды.

Киберқылмыстың жасалу тәсілі үнемі дамып отырады, бұл құқық қорғау органдарынан озық әдістер мен технологияларды қолдануды талап етеді. Бұл контексттегі маңызды құрал сандық дәлелдемелерді жинауға, талдауға және түсіндіруге мүмкіндік беретін киберкриминалистика болып табылады. Жасанды интеллект пен процестерді автоматтандыру сияқты заманауи әдістер тергеуді айтарлықтай жылдамдатады және тиімділігін арттырады.

Киберқылмыспен байланысты мәселелерді шешу тек технологиялық жаңалықтарды ғана емес, сонымен қатар халықаралық деңгейде құқықтық нормаларды үйлестіруді талап етеді. Киберқылмыстың ерекше сипатын ескеретін және тиімді халықаралық ынтымақтастықты қамтамасыз ететін құқықтық негіздерді әзірлеу қажет . Мемлекеттер белсенді түрде ынтымақтасуы, ақпарат пен тәжірибе алмасуы, мемлекеттік-жекеменшік әріптестік үшін жағдай жасауы керек.

Киберқылмыспен күресу әдістерін жетілдіру бойынша ұсыныстар келесі негізгі бағыттарды қамтиды:

1. Бейімделетін құқықтық базаны дамыту – киберқылмыстың тез өзгеретін сипатын ескеретін заңнаманы жасау қажет.
2. Мамандардың біліктілігін арттыру – IT-технологиялар және цифрлық сот сараптамасы саласында құқық қорғау органдары қызметкерлерін даярлау және қайта даярлау.
3. Жетілдірілген технологияларды қолдану – жасанды интеллект енгізу, процестерді автоматтандыру және деректерді талдаудың заманауи әдістерін қолдану.
4. Халықаралық ынтымақтастық – мемлекеттер арасындағы өзара іс-қимылды нығайту, ақпарат алмасу және киберқылмыспен күресу бойынша стратегияларды бірлесіп әзірлеу.
5. Мемлекеттік-жекешелік әріптестік – электрондық дәлелдер мен инфрақұрылымның көп бөлігін иеленетін жеке сектормен ынтымақтастық.

Осылайша, киберқылмыспен тиімді күресу технологиялық, құқықтық және ұйымдастырушылық шараларды, сондай-ақ халықаралық ынтымақтастық пен жеке сектормен серіктестікті қамтитын кешенді тәсілді қажет етеді [79].

Құқық қорғау органдарының киберқылмыстармен күрестегі тиімділігін арттыру үшін міндетті оқу бағдарламасын әзірлеу – маңызды қадамдардың бірі. Бұл бағдарлама құқық қорғау қызметкерлерінің біліктілігін арттырып, олардың заманауи киберқауіптерге тиімді әрекет етуіне мүмкіндік береді. Жаңа оқу жоспары төмендегідей негізгі бағыттарды қамтуы тиіс.

Цифрлық сараптама киберқылмыстарды тергеу және дәлелдемелерді жинау процесінде маңызды рөл атқарады. Бұл бағытта қызметкерлерге цифрлық іздерді

анықтау және талдау әдістерін меңгерту қажет. Сонымен қатар, шабуылдаушылардың ізін жасыруға бағытталған техникалық құралдарды қолдану арқылы жасырылған деректерді қалпына келтіру, кибершабуылдардың типологиясын түсіну және компьютерлік желілердегі заңсыз әрекеттерді дер кезінде анықтау қабілеті де осы курстың негізгі бөлігі болуы тиіс. Қызметкерлерді цифрлық криминалистика құралдарымен және ақпараттық жүйелердегі шабуылдарды талдаудың заманауи тәсілдерімен таныстыру олардың кәсіби дайындық деңгейін арттыруға септігін тигізеді.

Халықаралық киберқауіпсіздік заңнамасы туралы бөлімде құқық қорғау органдарының қызметкерлері әлемдік стандарттар мен халықаралық құқықтық актілерді меңгеруі қажет. Бұл оларға трансшекаралық қылмыстық құқық бұзушылықтарды тергеуде өзге елдердің құқықтық жүйелерімен үйлесімді жұмыс істеуге және халықаралық серіктестермен тиімді ынтымақтастық орнатуға мүмкіндік береді. Сонымен қатар, қызметкерлер Будапешт конвенциясы сияқты халықаралық келісімдермен жұмыс істеуді, шетелдік құқық қорғау органдарымен ақпарат алмасуды және кибершабуылдарды бірлесіп тергеу әдістерін игеруі тиіс. Бұл олардың халықаралық тәжірибені қолдану және өзара әрекеттесу қабілетін дамытады.

Тергеу әдістері бойынша оқыту бағдарламасы заманауи технологияларды қолдана отырып ақпараттық қылмыстық құқық бұзушылықтарды анықтау және тергеу тәсілдеріне бағытталуы керек. Қызметкерлерге кибершабуылдардан кейінгі қалпына келтіру жұмыстарын жүргізу, ботнеттерді анықтау, фишингтік шабуылдарды тергеу және шифрланған деректермен жұмыс істеу әдістерін меңгерту аса маңызды. Тергеу барысында қолданылатын арнайы бағдарламалық құралдар мен аналитикалық платформаларды үйрену арқылы құқық қорғау органдарының қызметкерлері күрделі киберқылмыстарды тиімді әрі жылдам тергеуге бейімделеді.

Бұл оқу бағдарламалары тұрақты түрде жаңартылып, жаңа қауіптер мен технологияларға сәйкес жетілдіріліп отыруы тиіс. Бұл қызметкерлерге ағымдағы киберқылмыстық трендтер мен қауіп-қатерлерден хабардар болуға мүмкіндік береді. Оқу курстарын үздіксіз жаңарту олардың кәсіби біліктілігін арттырып, киберқауіптерге шұғыл әрі тиімді әрекет ету қабілетін нығайтады.

2.3 Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъективтік жағының мәселелері

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъективтік жағының мәселелері осы салада қылмыстық құқық бұзушылық жасайтын адамдардың ниеттері мен әрекеттеріне қатысты. Негізгі мәселелердің бірі киберқылмыстарды жасау кезінде, әсіресе олар анонимді немесе маскировка технологияларын қолдану арқылы жасалғанда ниетті анықтаудың

қиындығы болып табылады. Кейде киберқылмыс жасаушылар зиянды әрекеттермен айналысуға ғана емес, сонымен қатар сынақ ретінде ақпараттық жүйелерге енуге итермелеуі мүмкін. Бұл олардың ниетін анықтауды және әрекеттерін қылмыстық құқық бұзушылық ретінде саралауды қиындатады.

Сонымен қатар, киберқылмыс контекстінде зиянды бағдарламаларды әзірлеушілер немесе кибершабуылдардағы делдалдар сияқты үшінші тұлғалардың әрекеттері үшін жауапкершілік мәселелері жиі туындайды. Олардың кінәлілігі мен қылмыстық құқық бұзушылыққа қатысу дәрежесін анықтау олардың іс-әрекеттері мен келтірілген залал арасында нақты тікелей байланыстың болмауына байланысты қиынға соғуы мүмкін. Бұл киберқылмыспен тиімді күресу және цифрлық кеңістікте әділеттілікті қамтамасыз ету үшін заңнаманы жетілдіру және қудалаудың жаңа әдістерін әзірлеу қажеттілігі туралы сұрақтарды тудырады.

Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъективтік жағы адамның жасалған әрекетке және оның зардаптарына психикалық қатынасымен байланысты. Мұндағы негізгі элементтер – ниет, мақсат және мотив. Киберқылмыскерлердің ниетін анықтау қиын болуы мүмкін, әсіресе қылмыстық құқық бұзушылықтар анонимді немесе бүркемелеу технологиялары арқылы жасалғанда. Мотивтерге қаржылық пайда, бәсекелестік артықшылық, саяси немесе идеологиялық мақсаттар, сондай-ақ қарапайым қызығушылық немесе өз дағдыларын тексеру жатады. Мұндай қылмыстық құқық бұзушылықтардың нысанасы көбінесе қылмыскерлер өз пайдасына пайдаланғысы келетін белгілі бір ақпараттық ресурстар немесе жүйелер болып табылады. Осы саладағы қылмыстық құқық бұзушылықтардың субъективтік жағын түсіну олардың алдын алу мен күресудің тиімді шараларын әзірлеу үшін, сондай-ақ әрекеттерді барабар саралау үшін маңызды.

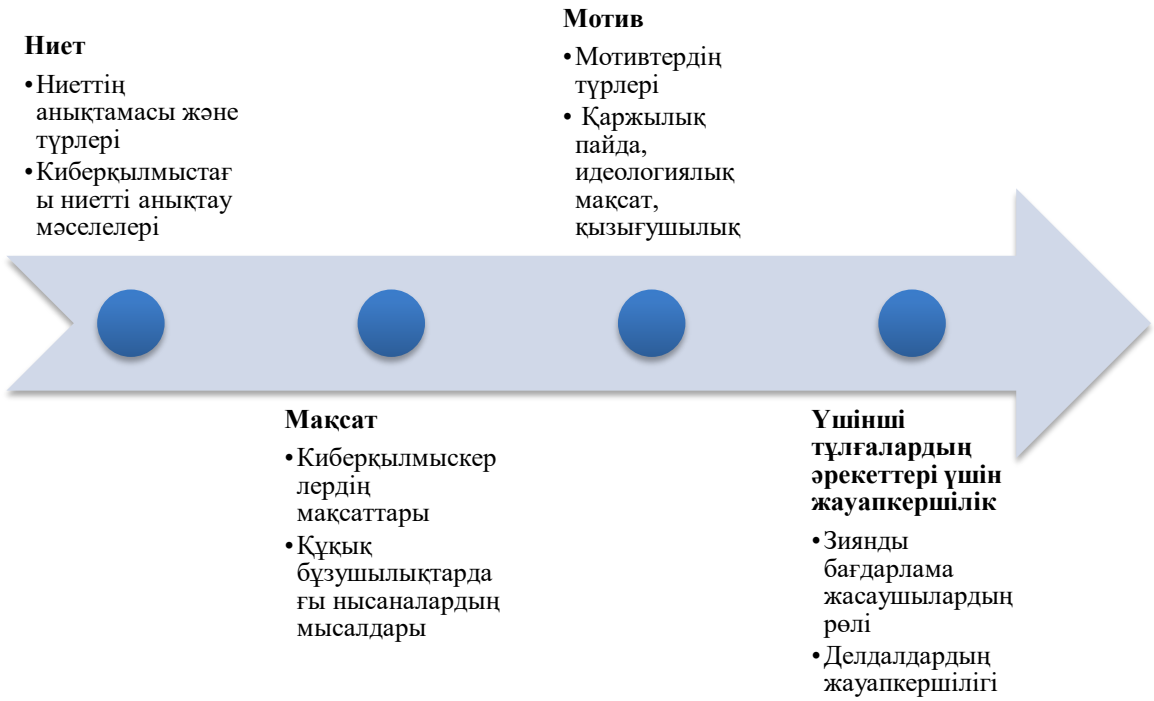
Қылмыстық құқық бұзушылықтың субъективтік жағын анықтау адамның жасалған әрекетке және оның зардаптарына психикалық қатынасын ескеруді қамтиды, ол қылмыстың кінәсі, мотиві мен мақсаты сияқты элементтерді қамтиды [80].

Қылмыстық құқықта субъективтік жағы шешуші рөл атқарады, өйткені ол әрекеттің қоғамдық қауіптілік дәрежесін және қылмыскердің жеке басын бағалауға мүмкіндік береді. Бұл, өз кезегінде, әрекеттің біліктілігіне, жазаны таңдауға және жауаптылықты жеңілдететін немесе ауырлататын мән-жайларды қолдану мүмкіндігіне әсер етеді. Киберқылмыс контекстінде субъективтік жағы ерекше маңызға ие, өйткені мұндай қылмыстық құқық бұзушылықтардың себептері мен мақсаттары көбінесе заңсыз пайда алумен, ақпараттық жүйелерге зиян келтірумен немесе деректердің құпиялылығын бұзумен байланысты.

Киберқылмыстың субъективтік жағының мәселелері мұндай әрекеттердің жоғары күрделілігі мен ерекшелігіне байланысты ерекше назар аударуды қажет етеді. Мысалы, ақпараттық-коммуникациялық технологияларды пайдалану қылмыскерлерге жасырын әрекет етуге және олардың іздерін жасыруға мүмкіндік береді, бұл кінәні және мотивтерді дәлелдеуді. Оның үстіне киберқылмыс көбінесе

трансұлттық сипатқа ие, бұл тергеу мен қудалауда қосымша құқықтық қиындықтар [81].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардағы субъективті жақтың рөліне аумақтық белгісіздік және құқық бұзушылардың анонимділігі сияқты аспектілерді де қарастыру кіреді. Бұл факторлар кінәні анықтау және мотивтерді анықтау процесін қиындатады, бұл құқық қорғау органдарынан арнайы тергеу және талдау әдістерін қолдануды талап етеді. Осылайша, киберқылмыстардың субъективтік жағын талдау олармен тиімді күресудің құрамдас бөлігі болып табылады. Бұл құқықтық, техникалық және ұйымдастырушылық шараларды, сондай-ақ халықаралық ынтымақтастық пен мемлекеттер арасындағы тәжірибе алмасуды қамтитын кешенді тәсілді қажет етеді [82].



Сурет 4 – Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъективтік жағының мәселелері

Бұл бөлімде біз қылмыстық құқық бұзушылықтың субъективтік жағының анықтамасын және оның қылмыстық құқықтағы маңызын қарастырамыз, сонымен қатар киберқылмыскерлердің ниетінің, мақсаты мен мотивінің түрлері мен ерекшеліктерін талдаймыз. Біз зиянды бағдарлама жасаушылардың рөліне және делдалдардың жауапкершілігіне ерекше назар аударамыз. Қорытындылай келе, әрекеттерді дұрыс саралау үшін субъективтік жағын талдаудың маңыздылығын талқылап, қылмыстық заңнаманы жетілдіру бойынша ұсыныстарды ұсынамыз (4-сурет).

Қылмыстық құқықта ниет деп адамның қылмыстық құқық бұзушылық

құрамы бар әрекетті жасауға саналы және мақсатты түрде ұмтылуы түсіндіріледі. Киберқылмыс жағдайында ниет қылмыскердің әрекетінің сипаты мен мақсатына қарай әртүрлі формада болуы мүмкін. Француз заң шығарушысы да ниетті қылмыстың қажетті элементі ретінде қарастырады, ерік-жігердің болуын және әрекеттің заңсыздығын білуді білдіреді [83].

Ниеттің екі негізгі түрі бар: тікелей және жанама. Тікелей ниет адамның өз іс-әрекетінің заңсыз сипатын білуін және қылмыстық нәтижеге жетуге ұмтылуын білдіреді. Жанама ниет, керісінше, адамның негізгі мақсаты болмаса да, оның іс-әрекеті барысында қылмыстық нәтиже болуы мүмкін екендігін сезінуімен сипатталады.

Киберқылмыстағы ниетті анықтау қиын, себебі қылмыскерлердің әрекеттері жиі жасырылады және заңды әрекеттер ретінде жасырылады. Жүйелер мен деректерге рұқсатсыз қол жеткізуге бағытталған хакерлердің шабуылдары әртүрлі мақсаттарда, соның ішінде зиян келтіру, деректерді ұрлау немесе экономикалық пайда алу үшін жүзеге асырылуы мүмкін. Мысалы, 2014 жылы британдық хакер Лори Лав веб-сайттарды бұзып, АҚШ үкіметінің жүйелеріне қол жеткізіп, құпия ақпаратты ұрлап, айтарлықтай зиян келтірді [84].

Киберқылмыс туралы Еуропа Кеңесінің конвенциясы киберқылмыс жасауға арналған құрылғыларды өндіруге, сатуға және пайдалануға, егер олар қылмыс жасау мақсатында пайдаланылса, тыйым салады. Дегенмен, 6(2)-бапқа сәйкес, бұл құралдарды компьютерлік жүйелерді тестілеу немесе қорғау сияқты заңды мақсаттарда пайдалану қылмыс болып табылмайды, бұл киберқылмыстарды тергеуде ниетті анықтауды қиындатады.

Киберқылмыскерлер қаржылық пайдадан саяси және идеологиялық себептерге дейін әртүрлі мақсаттарды көздейді. Артемий Владимирович Зык өз мақаласында киберқылмыскерлердің негізгі мақсаттары жұмыс процестерін бұзу, деректерді ұрлау, ақпаратты манипуляциялау, қорқыныш пен хаос себу, қаржылық зиян келтіру, діни немесе саяси идеяларды таңу және әскери мақсаттарға жету екенін көрсетеді. Киберқылмыскерлер өздерінің шоттарына ақша аудару үшін банктік шоттарға немесе қаржылық деректерге қол жеткізу үшін әртүрлі әдістерді пайдаланған кезде қаржылық пайда ең көп таралған мақсаттардың бірі болып қала береді [85].

Сонымен қатар, тану мен жетістікке жету маңызды мақсат болып табылады. Кейбір хакерлер күрделі жүйелерді бұзу арқылы келетін жетістік сезіміне итермелейді. Олар топта немесе өз бетінше әріптестер арасында тану үшін жұмыс істей алады.

Қаржылық пайданы көздеген киберқылмыстың бір мысалы британдық хакер Лори Лавтың ісі болып табылады, ол 2014 жылы АҚШ үкіметінің жүйелерін бұзып, құпия ақпаратты ұрлап, айтарлықтай зиян келтірген. Басқа мысал – қаржылық пайда алу немесе ұйымдардың жұмысын бұзу үшін деректерді ұрлау және манипуляциялау үшін вирустар мен троян аттары сияқты зиянды

бағдарламаларды пайдалану.

Саяси астарлы шабуылдар да жиі кездеседі. «Хактивистер» деп аталатын хакерлер топтары адам құқықтарына немесе басқа саяси мәселелерге назар аудару үшін ірі ұйымдарға шабуыл жасау үшін өз дағдыларын пайдалана алады. Мысалы, DDoS (үлестірілген қызмет көрсетуден бас тарту) шабуылдары веб-сайттарды шамадан тыс жүктеу және оларды бұзу үшін қолданылады, бұл айтарлықтай бұзылулар тудыруы мүмкін. Осылайша, киберқылмыскерлердің мақсаттары әртүрлі болуы мүмкін және қаржылық пайдадан саяси және идеологиялық себептерге дейін болуы мүмкін. Осы мақсаттарды түсіну сізге кибершабуылдардан қорғануға жақсы дайындалуға және тиімді қарсы шараларды әзірлеуге көмектеседі.

Киберқылмыскерлердің *әртүрлі мотивтері бар*, оларды бірнеше негізгі санаттарға бөлуге болады: қаржылық пайда, идеологиялық мақсаттар және қызығушылық. Бұл мотивтердің әрқайсысының өзіндік ерекшеліктері мен мақсаттары бар.

Қаржылық пайда – адамдарды киберқылмыспен айналысуға итермелейтін ең көп таралған себептердің бірі. С.С.Витвицкая, А.А.Витвицкий, Ю.И.Исаковалардың мақаласында қаржылық мотивтерге деректерді ұрлау, алаяқтық, бопсалау және бопсалау жатады. Қылмыскерлер банк шоттарына, қаржылық құжаттарға қол жеткізу немесе төлем бағдарламалық құралын орнату үшін өз дағдыларын пайдалана отырып, деректердің құлпын ашу үшін төлемді талап ете алады [86].

Идеологиялық мақсаттар немесе «хактивизм» жиі киберқылмыстардың мотиві болып табылады. Бұл қылмыскерлер әлеуметтік, саяси немесе экологиялық мәселелерге назар аудару үшін өздерінің дағдыларын қолдануға тырысады. Мысалы, олар мемлекеттік ұйымдардың веб-сайттарын бұзып, олардың көзқарасын баса көрсететін немесе белгілі бір саясатқа наразылық білдіретін ақпаратты жариялауы мүмкін. Бұл қылмыстық құқық бұзушылықтар серверлерді шамадан тыс жүктеуге және веб-сайттарды бұзуға бағытталған DDoS шабуылдарын қамтуы мүмкін.

Киберқылмыскерлерді ынталандыруда қызығушылық пен өзін-өзі растауға ұмтылу да маңызды рөл атқарады. Базоров пен Сагарев киберқылмыспен айналысатын көптеген жастар өз іс-әрекеттерін қызығушылықтан және өз дағдыларын сынауға ұмтылудан бастайтынын атап өтті. Бұл мотив көбінесе зиян келтірудің нақты мақсаты жоқ жүйені зерттеу мақсатында бұзу түрінде көрінеді, дегенмен бұл ақыр соңында ауыр зардаптарға әкелуі мүмкін.

Осылайша, қаржылық пайда қылмыскерлерді деректерді ұрлау мен алаяқтық жасауға итермелейді. Мысалы, британдық хакер Лори Лав 2014 жылы АҚШ үкіметінің жүйелеріне шабуыл жасап, құпия ақпаратты ұрлап, айтарлықтай зиян келтірген. Басқа жағдайда, төлем үшін ұйымдарды бопсалау үшін төлем бағдарламалық құралын пайдалану қаржылық негізделген шабуылдардың айқын мысалы болып табылады. Идеологиялық мақсаттар белгілі бір мәселеге назар

аудару үшін мемлекеттік сайттарға немесе инфрақұрылымға шабуылдарды қамтуы мүмкін. Мысалы, хактивистер кейбір үкімет саясаттарына немесе әрекеттеріне қарсы материалдарды жариялау үшін веб-сайттарды бұзуы мүмкін. Қызығушылығы мен өзін-өзі растау көбінесе нақты материалдық пайдасыз бұзуға әкеледі. Мұндай әрекеттерге олардың осалдықтарын зерттеу немесе жай ғана өз дағдыларын көрсету үшін хакерлік жүйелер кіруі мүмкін. Бұл әрекеттер зиянсыз болып көрінгенімен, олар көбінесе жүйелер мен деректер қауіпсіздігі үшін ауыр зардаптарға әкеледі [87].

Зиянды бағдарламалық жасақтаманы әзірлеушілер киберқылмыста басты рөл атқарады, өйткені олар әртүрлі заңсыз әрекеттерді жасау үшін қолданылатын құралдарды жасайды.

Зиянды бағдарламалық жасақтаманы әзірлеушілер үшін жауапкершілік мәселесі халықаралық құқық контекстінде жиі талқыланады. Мысалы, Ресей Федерациясының Қылмыстық кодексінің 273-бабына түсініктемелерде жауапкершілік зиянды бағдарламалардың бастапқы кодтарын жасағаны үшін де жүктелетіні көрсетілген, бұл әзірлеушілерді өз әрекеттері үшін толық жауапты етеді. Бұл осындай бағдарламаларды әзірлеумен айналысатындарға жүктелетін жауапкершіліктің жоғары деңгейін көрсетеді.

Зиянды бағдарламаларды тарататын немесе пайдаланатын жеке тұлғалар немесе ұйымдар сияқты делдалдар да қылмыстық жауапкершілікке тартылады. Ресей Федерациясының Қылмыстық кодексінің 273-бабында зиян келтіруге бағытталған зиянды бағдарламаларды тарату немесе пайдалану оларды жасау сияқты жазаланады. Бұл әзірлеуге тікелей қатысы жоқ, бірақ мұндай бағдарламаларды таратуға немесе пайдалануға қатысы бар адамдар да жазаға тартылады дегенді білдіреді [88].

Маңызды аспект, делдалдар таратылатын бағдарламалық қамтамасыз етудің сипатын толық түсінбеген жағдайда да жауапкершілікке тартылуы мүмкін. Заңға сәйкес бағдарламаның зиянды сипаты туралы ниеттің немесе алдын ала білімнің болуы негізгі критерий болып табылады. Сондықтан зиянды бағдарламаларды тарату тізбегіне қатысы бар кез келген адам өз әрекеттерінің ықтимал заңды салдарын білуі керек. Сондықтан үшінші тұлғалардың, соның ішінде әзірлеушілер мен делдалдардың әрекеттері үшін жауапкершілік киберқылмыспен күресте маңызды аспект болып табылады. Ресей Федерациясының Қылмыстық кодексінің 273-бабы сияқты заңдар бұл мәселенің маңыздылығын көрсетеді және зиянды бағдарламаларды жасау және тарату процесінің барлық қатысушыларына қатаң жаза белгілейді. Бұл ақпараттық жүйелер мен деректердің қауіпсіздігін қамтамасыз ету, сондай-ақ болашақта киберқылмыстардың алдын алу үшін маңызды [89].

Қылмыстың субъективтік жағын талдау, әсіресе, ақпараттандыру және байланыс саласындағы әрекеттерді дұрыс саралау және әділ сот төрелігін қамтамасыз ету үшін өте маңызды. Субъективті жағына қылмыскерлердің мотивтері, ниеттері мен мақсаттары жатады, олар көбінесе кінәнің дәрежесін және

жазаның ауырлығын анықтауда негізгі элементтер болып табылады. Кириленко мен Алексеев атап өткендей, киберқылмыстар мемлекет пен қоғамның ақпараттық қауіпсіздігіне елеулі қатер төндіреді, бұл мұндай қауіп-қатерлерге неғұрлым тиімді қарсы тұру үшін қылмыстық құқық бұзушылықтардың субъективтік жағының барлық аспектілерін мұқият талдау қажеттігін атап көрсетеді. [90].

Үнемі өзгеріп отыратын цифрлық орта жағдайында қылмыстық құқық бұзушылықтардың субъективтік жағын талдау ғана емес, жаңа сын-қатерлерге барабар жауап беру үшін қылмыстық заңнаманы жетілдіру маңызды. Киберқылмыс туралы E4J модулінде ұсынылған, киберқылмыспен күресуде заңдар мен халықаралық ынтымақтастықты үйлестіру қажеттілігін көрсететін халықаралық тәжірибе мен ұсыныстарды ескеру маңызды. Сондай-ақ қауіпсіздікті қамтамасыз ету мен негізгі құқықтар мен бостандықтарды сақтау арасындағы тепе-теңдікті сақтауға мүмкіндік беретін цифрлық ортада адам құқықтарын қорғаудың заманауи тәсілдеріне де назар аудару қажет.

Заңнамаларды жетілдіру бойынша негізгі ұсыныстарға мыналар жатады:

1. Заңнамалық нормаларды киберқылмыстың жаңа түрлеріне бейімдеу: Заңнамаға маңызды инфрақұрылымға шабуылдар және зиянды бағдарламаларды тарату сияқты киберқылмыстың жаңа түрлерін нақты сипаттайтын және қылмыстық жауапкершілікке тартатын нормаларды енгізу.
2. Халықаралық ынтымақтастық: киберқылмыспен бірлесіп күресуге және елдер арасында ақпарат алмасуға бағытталған халықаралық келісімдерді әзірлеу және жүзеге асыру.
3. Құқық қорғау органдарын оқыту және дамыту: Құқық қорғау органдарына киберқылмысты жақсырақ түсіну және оған қарсы тұру үшін мамандандырылған тренингтер мен курстарды қамтамасыз ету.
4. Жұртшылықтың хабардар болуын арттыру: киберқауіптер және олардан жалпы жұртшылық пен ұйымдар үшін хабардар болуды арттыруға арналған науқандар [91].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың субъективтік жағын талдау әрекеттерді дұрыс саралау және әділ сот төрелігін қамтамасыз ету үшін маңызды аспект болды. Бұл бөлімде біз құқық бұзушылықтың субъективтік жағының анықтамасын және оның қылмыстық құқықтағы маңызын қарастырдық, сонымен қатар киберқылмыскерлердің ниетінің, мақсаты мен мотивінің түрлері мен сипаттамаларын қарастырдық. Зиянды бағдарлама жасаушылардың рөлі мен делдалдардың жауапкершілігіне ерекше назар аударылды. Қорытындылай келе, біз әрекеттерді дұрыс саралау үшін субъективтік жағын талдаудың маңыздылығын талқылап, қылмыстық заңнаманы жетілдіру бойынша ұсыныстар бердік.

Қылмыстық құқықта қасақана адамның қылмыс құрамын құрайтын әрекетті саналы және мақсатты түрде жасауға ұмтылуы ретінде анықталған. Киберқылмыс контекстінде қасақана құқық бұзушының әрекетінің сипаты мен мақсатына қарай әртүрлі формада болуы мүмкін. Ниеттің екі негізгі түрі болды: тікелей және

жанама. Тікелей ниет адамның өз іс-әрекетінің заңсыз сипатын білуін және қылмыстық нәтижеге жетуге ұмтылуын білдіреді. Жанама қасақана адамның негізгі мақсаты болмаса да, оның іс-әрекеті барысында қылмыстық нәтиже болу мүмкіндігін сезінуімен сипатталды.

Киберқылмыскерлер әртүрлі мақсаттарды көздеді, олар қаржылық пайдадан саяси және идеологиялық себептерге дейін болуы мүмкін. Киберқылмыскерлер банк шоттарына немесе қаржылық деректерге қол жеткізу үшін әртүрлі әдістерді пайдаланған кезде қаржылық пайда ең көп таралған мақсаттардың бірі болып қала берді. Сонымен қатар, тану мен жетістікке жету хакерлерді күрделі жүйелерді бұзуға итермелейтін маңызды мақсат болды. Саяси астарлы шабуылдар да жиі болды.

Киберқылмыскерлердің мотивтерін бірнеше негізгі санаттарға бөлуге болады: қаржылық пайда, идеологиялық мақсаттар және қызығушылық. Қаржылық артықшылықтарға деректерді ұрлау, алаяқтық, бопсалау және бопсалау кіреді. Идеологиялық мақсаттар немесе «хактивизм» әлеуметтік, саяси немесе экологиялық мәселелерге назар аударуға бағытталған. Қызығушылығы мен өзін-өзі растауға деген ұмтылыс көбінесе нақты материалдық пайдасыз бұзуға әкелді.

Зиянды бағдарламалық жасақтаманы әзірлеушілер киберқылмыста басты рөл атқарды, өйткені олар заңсыз әрекеттерді жүзеге асыруға арналған құралдарды жасады. Ресей Федерациясының Қылмыстық кодексінің 273-бабында мұндай бағдарламаларды жасағаны, таратқаны немесе пайдаланғаны үшін жаза қарастырылған. Зиянды бағдарламаларды таратқан немесе пайдаланған делдалдар да жауапкершілікке тартылды. Негізгі критерий ниеттің болуы немесе бағдарламаның зиянды сипаты туралы алдын ала білу болды.

Қылмыстың субъективтік жағын талдау, әсіресе ақпараттандыру және байланыс саласындағы әрекеттерді дұрыс саралау және әділ сот төрелігін қамтамасыз ету үшін маңызды болды. Халықаралық ынтымақтастық пен жаңа сын-қатерлерге бейімделуге негізделген қылмыстық заңнаманы жетілдіру қауіпсіз цифрлық кеңістікті құру жолындағы басты қадам болды. Негізгі ұсыныстарға құқықтық бейімдеу, халықаралық ынтымақтастық, құқық қорғау органдарын оқыту және халықтың хабардарлығын арттыру кіреді.

Қорытындылай келе, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың субъективтік жағын талдаудың маңыздылығын асыра бағалауға болмайды. Бұл әділ сот төрелігін қамтамасыз ету және киберқылмыспен тиімді күресудің маңызды элементі болып табылады. Халықаралық ынтымақтастық пен жаңа сын-қатерлерге бейімделуге негізделген қылмыстық заңнаманы жетілдіру қауіпсіз цифрлық кеңістікті құру жолындағы басты қадам болып табылады.

2.4 Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық субъектісінің мәселелері

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың субъектілері жалпы және арнайы субъектілер болуы мүмкін. Жалпы субъектілер – белгілі бір жасқа толған және әрекет қабілеттілігі бар адамдар. Мамандандырылған субъектілерге күрделі киберқылмыстарды жасауға мүмкіндік беретін ақпараттық технологиялар саласында арнайы білімі мен дағдылары бар тұлғалар жатады. Киберқылмыс субъектілерінің сипаттамалары оларды анықтауға және қылмыстық жауапкершілікке тартуға ерекше көзқарасты талап етеді. Сондай-ақ зиянды бағдарлама жасаушылар немесе кибершабуылдардың делдалдары сияқты қылмыстық құқық бұзушылықтарға жанама түрде қатысы бар адамдарды жауапқа тартуға байланысты қиындықтар бар. Бұл ақпараттық саладағы қылмыстық схемалардың барлық қатысушыларының әрекеттерін тиімді анықтау және жолын кесу үшін құқықтық база мен тергеу әдістерін жетілдіру қажеттілігін көрсетеді.

2.4 бөлімінде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар пәніне қатысты мәселелерді зерттейміз. Қылмыстық құқықта құқық бұзушылықтың мәнін түсіну және анықтау басты рөл атқарады, өйткені олар әрекетті дұрыс саралауға және жауапкершілік шараларын белгілеуге мүмкіндік береді.

Қылмыстық құқық бұзушылықтың субъектісі – қылмыстық жауаптылыққа тартылатын жасқа толған, есі дұрыс және қылмыстық заңда көзделген әрекетті жасаған жеке тұлға. Киберқылмыстар контекстінде субъекті жеке тұлға немесе алдын ала сөз байласу бойынша әрекет ететін адамдар тобы немесе ұйымдасқан топтың құрамында болуы мүмкін. Кейбір жағдайларда құқық бұзушылықтың субъектісі заңды тұлғалар да болуы мүмкін екенін атап өткен жөн, әсіресе егер әрекеттер серіктестіктің мүддесі үшін немесе оны пайдалану арқылы жасалса.

Қылмыстық құқық бұзушылықтың субъектісі – қылмыстық жауаптылыққа тартылатын жасқа толған, есі дұрыс және қылмыстық заңда көзделген әрекетті жасаған жеке тұлға. Киберқылмыстар контекстінде субъекті жеке тұлға немесе алдын ала сөз байласу бойынша әрекет ететін адамдар тобы немесе ұйымдасқан топтың құрамында болуы мүмкін. Кейбір жағдайларда құқық бұзушылықтың субъектісі заңды тұлғалар да болуы мүмкін екенін атап өткен жөн, әсіресе егер әрекеттер серіктестіктің мүддесі үшін немесе оны пайдалану арқылы жасалса. Витвицкая және оның әріптестері киберқылмыстарды көбіне жоғары техникалық білімі мен дағдысы бар адамдар жасайтынын, бұл оларға құқықтық баға беруде ерекше көзқарасты талап ететінін атап көрсетеді [92].

Қылмыстық құқықтағы субъектінің маңыздылығы оның жасаған қылмысы үшін кінәсі мен жауаптылығында болып табылады. Субъектсіз құқық бұзушылықтың өзі де болмайды, өйткені қылмыстық құқық абстрактылы әрекеттерді емес, адамдардың мінез-құлқын реттеуге бағытталған. Сондай-ақ

субъектінің жасы, есі дұрыстығы, рөлі мен қылмыстық құқық бұзушылыққа қатысу дәрежесі сияқты ерекшеліктерін ескеру қажет, өйткені бұл факторлар әрекеттің жазасы мен біліктілігіне әсер етеді.

Ақпараттандыру және байланыс саласында жоғары техникалық білімі мен дағдысы бар, хакерлік шабуылдар, зиянды бағдарламаларды тарату, деректерді ұрлау және т.б. сияқты қылмыстық құқық бұзушылықтарды жасау үшін өз дағдыларын пайдаланатын адамдар құқық бұзушылық субъектілері болуы мүмкін. Бұл құқық қорғау органдары мен заң шығарушылардан мұндай субъектілерді анықтауға және реттеуге, сондай-ақ киберқылмыспен күресу және алдын алу бойынша арнайы шараларды әзірлеуге ерекше көзқарасты талап етеді.

Қылмыстық құқықтағы субъектінің маңыздылығы оның жасаған қылмысы үшін кінәсі мен жауаптылығында болып табылады. Субъектсіз құқық бұзушылықтың өзі де болмайды, өйткені қылмыстық құқық абстрактылы әрекеттерді емес, адамдардың мінез-құлқын реттеуге бағытталған. Сондай-ақ субъектінің жасы, есі дұрыстығы, рөлі мен қылмысқа қатысу дәрежесі сияқты ерекшеліктерін ескеру қажет, өйткені бұл факторлар әрекеттің жазасы мен біліктілігіне әсер етеді. Сауд Арабиясының заңы бойынша киберқылмыс жасаған қылмыскерлер әрекеттің ауырлығы мен ниетіне байланысты елеулі айыппұлдар мен ұзақ мерзімге бас бостандығынан айырылуы мүмкін [93].

Сонымен, осы бөлімнің аясында біз құқық бұзушылықтың субъектісін анықтаудың негізгі аспектілерін және оның қылмыстық құқықтағы маңызын қарастырамыз. Бұл ақпараттандыру және байланыс саласында қылмыстық заңнаманы тиімді қолданудың кілті болып табылатын құқық бұзушылықтарды саралауға және жазаларды белгілеуге субъектілердің әртүрлі сипаттамалары мен әрекеттері қалай әсер ететінін жақсы түсінуге мүмкіндік береді. Басқаша айтқанда, бұл бөлімде біз келесі тақырыптарды әрі қарай қарастырамыз: құқық бұзушылықтың жалпы субъектілері, оның ішінде жасы мен әрекет қабілеттілігі, сондай-ақ осы субъектілердің негізгі сипаттамалары; мысалдармен АТ саласында арнайы білімі мен дағдылары бар арнайы пәндер; Интернеттегі анонимділікке байланысты субъектіні анықтау мәселелері және бұзушыларды анықтау әдістері; және ақырында, әзірлеушілер мен делдалдар сияқты жанама қатысушылардың міндеттері, олардың рөлдері мен жауапкершіліктерінің мысалдары болып табылады.

Әрекет қабілеттілігі бар және заңда белгіленген жасқа толған жеке тұлға ғана *қылмыстық құқық бұзушылықтың субъектісі бола алады.* Көптеген елдердің, соның ішінде Ресейдің заңнамасына сәйкес, қылмыстық жауапкершілік 16 жастан басталады. Алайда, аса ауыр қылмыс жасағаны үшін жауапкершілік 14 жастан басталуы мүмкін (РФ Қылмыстық кодексінің 20-бабы). Қабілеттілік адамның өз іс-әрекетінің мәнін түсініп, оны бағыттай алу қабілеті ретінде анықталады. Бұл адамның есі дұрыс болуы және өз әрекетінің заңсыздығын түсінуі керек дегенді білдіреді.

Құқық бұзушылықтың жалпы субъектілері 5-суретте көрсетілген келесі

негізгі белгілермен сипатталады:

Сурет 5 – Құқық бұзушылықтың жалпы субъектілерінің сипаттамасы

Сонымен, құқық бұзушылықтың жалпы субъектілері мынадай негізгі белгілермен сипатталады:

– Қылмыстық жауаптылықтың ең төменгі жасы жасалған қылмыстың ауырлығына байланысты өзгереді. Көптеген юрисдикцияларда қылмыстық жауапкершілік 16 жастан басталады, бірақ аса ауыр қылмыстық құқық бұзушылықтар үшін жауапкершілік 14 жастан басталуы мүмкін.

- Құқық бұзушылықтың субъектісі тек өз іс-әрекетін жүзеге асыруға және оған бағыт беруге қабілетті, есі дұрыс адам бола алады. Психикалық бұзылулардың болуы немесе психикалық дамуының жеткіліксіз деңгейі адамды есі дұрыс емес деп тану үшін негіз бола алады, бұл оның қылмыстық жауаптылығын болдырмайды.

- Адам өз әрекетінің заңсыз екенін және қылмыстық жауапкершілікке әкеп соғуы мүмкін екенін білуі керек. Бұл әрекеттің фактілерін де, оның құқықтық салдарын да түсінуді қамтиды.

– Қылмысты жасауға кінәлі деп тану үшін оның әрекеті үшінші тұлғалардың мәжбүрлеуінсіз өз еркімен жасалғанын дәлелдеу қажет. Әйтпесе, жауапкершілік қайта жіктелуі немесе толығымен алынып тасталуы мүмкін.

Бұл сипаттамалар кінәні анықтауда және үкім шығаруда шешуші рөл атқарады. Олар сондай-ақ қылмыстық құқық бұзушылықтардың жалпы және ерекше субъектілерін ажыратуға көмектеседі, бұл әрекеттерді дұрыс саралау және әділ сот талқылауы үшін маңызды.

Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық субъектілеріне сауалнама жүргізу ақпараттық технологиялар саласында арнайы білімі мен дағдылары бар арнайы субъектілерге ерекше назар аударуды талап етеді. Арнайы актерлер кәсіби дайындықтың жоғары деңгейімен сипатталады, бұл олардың әрекеттерін анықтау мен алдын алуды қиындатады.

Арнайы субъектілердің негізгі сипаттамаларының бірі – олардың *IT*-

технологияларды терең білуі және оларды қылмыстық мақсаттарында пайдалана білуі. Бағдарламашылар, тестерлер, жүйелік талдаушылар, веб-дизайнерлер және желі әкімшілері сияқты АТ мамандары цифрлық кеңістікте кибершабуылдарды, хакерлік және басқа да қылмыстық әрекеттерді жүзеге асыруға мүмкіндік беретін құралдар мен әдістерге қол жеткізе алады [94].

Мұндай мамандар иеленетін арнайы білім мен дағдыларға сценарийлерді кодтау және жазу қабілеті, қауіпсіздік және ақпаратты қорғау жүйелерін білу, мәліметтер базасымен және желі архитектураларымен жұмыс істеу қабілеті жатады. Бұл дағдылар оларды ерекше қауіпті етеді, өйткені олар кибершабуылдар жасап қана қоймайды, сонымен қатар зиянды бағдарламаларды жасай алады , ботнеттерді басқара алады және күрделі бұзу операцияларын орындай.

Арнайы актерлердің мысалдары ретінде кибер тыңшылықпен және деректерді ұрлау үшін бұзумен айналысатын хакерлер, сондай-ақ мемлекеттік және корпоративтік жүйелерге кибершабуыл жасау үшін қылмыстық топтарда жұмыс істейтін мамандар жатады. Мысалы, киберқауіпсіздік мамандарының киберқылмыскерлерге ауысу жағдайлары жиілеп барады. Мұндай адамдар желілік технологияларды терең меңгерген және қауіпсіздік жүйелерін айналып өтіп, шабуылдар жасау үшін өз дағдыларын пайдалана алады [95].

Осылайша, киберқылмыспен күресудің тиімді шараларын әзірлеу үшін арнайы субъектілердің ерекшеліктерін және олардың уәждерін білу маңызды. Олардың кәсіби дағдыларын түсіну оларға ықтимал қауіптерді жақсы болжауға және тиісті қорғаныс шараларын әзірлеуге мүмкіндік береді.

Интернеттегі анонимділік киберқылмыстарды тергеу кезінде құқық қорғау органдарына маңызды қиындықтардың бірі болып табылады. Бір жағынан, анонимділік пайдаланушылардың және олардың деректерінің құпиялылығын қорғайды, бірақ екінші жағынан, құқық бұзушыларды анықтауға үлкен кедергілер жасайды. Желідегі анонимді әрекеттер псевдонимдерді, прокси-серверлерді және басқа да техникалық құралдарды қолдану арқылы жүзеге асырылуы мүмкін, бұл сәйкестендіру процесін әлдеқайда қиындатады [96].

Хакерлерді олардың жеке басын жасыруға тырысқанына қарамастан, желіде анықтаудың бірнеше әдістері бар. Осындай әдістердің бірі - пайдаланушының орналасқан жері туралы ақпаратты бере алатын IP мекенжайларын қадағалау. Дегенмен, прокси-серверлер мен VPN желілерін пайдалану бұл процесті қиындатады, өйткені олар пайдаланушының нақты IP мекенжайын жасырады. Басқа әдіс – файл метадеректері, веб-сайттардағы және әлеуметтік желілердегі әрекет журналдары сияқты интернетте пайдаланушылар қалдырған сандық іздерді талдау. Бұл деректер пайдаланушы бүркеншік атын пайдаланса да, оны анықтауға көмектеседі.

Блокчейн сияқты үлестірілген бухгалтерлік технологиялар да пәнді сәйкестендіру контекстінде ерекше қызығушылық тудырады. Блокчейн қауіпсіздік пен мөлдірліктің жоғары деңгейін қамтамасыз етеді, сонымен бірге

пайдаланушыларға жасырын қалуға мүмкіндік береді. Бұл құқық бұзушыларды анықтауды қиындатады, өйткені блокчейндегі транзакцияларды бақылауға болады, бірақ қатысушыларды әрқашан анықтау мүмкін емес [97].

Интернетте субъектілерді анықтау тиімділігін арттыру үшін әртүрлі технологиялар мен әдістерді қолдануды қамтитын кешенді тәсілді қолдану қажет. Бұған халықаралық ынтымақтастық және киберқауіпсіздік заңнамасын үйлестіру сияқты техникалық құралдар да, құқықтық тетіктер де кіреді.

Зиянды бағдарламалық жасақтаманы әзірлеушілер мен делдалдар киберқылмыс экожүйесінде басты рөл атқарады. Бұл субъектілер әрқашан тікелей қылмыстық әрекеттерді жасамайды, бірақ олардың қызметі басқаларға кибершабуыл жасау мүмкіндігін береді. Әзірлеушілердің рөлі қылмыс жасау үшін қолданылатын құралдарды жасау болып табылады, мысалы, вирустар, трояндар, шпиондық бағдарламалар және т.б. Мысалы, Солтүстік Кореяның Кимсуки хакерлер тобы Оңтүстік Кореядағы саяси және дипломатиялық ұйымдарға шабуылдарымен танымал. әзірленген зиянды бағдарлама.

Делдалдар, өз кезегінде, бұл құралдарды таратуға, оларды сатуға және қолдауға жағдай жасайды, сондай-ақ қылмыс іздерін жасыру қызметтерін көрсете алады. Бұл делдалдарға қара нарықта немесе көлеңкелі интернет форумдар арқылы қызметтерін ұсынатын жеке тұлғалар да, тұтас ұйымдар да кіреді. Мысал ретінде ұрланған деректер базасымен сауда жасайтын RaidForums платформасын жабуды келтіруге болады. Форум пайдаланушылары кибершабуылдар нәтижесінде ұрланған деректерді сату және алмасу бойынша өз қызметтерін көрсетті [98].

Бұл жанама субъектілердің жауапкершілігі киберқылмыспен тиімді күресу үшін маңызды. Түрлі елдердің заңнамасы тек тікелей кінәлілерді ғана емес, сонымен қатар кибершабуылға арналған құралдарды жасайтын және тарататындарды да жауапкершілікке тартуға көбірек көңіл бөлуде. Мысалы, Қазақстан Республикасының Қылмыстық кодексінің 273-бабы компьютерлік ақпаратқа рұқсатсыз қол жеткізуге арналған бағдарламаларды жасағаны, таратқаны немесе пайдаланғаны үшін жауапкершілікті белгілейді, бұл зиянды бағдарламалық жасақтаманы әзірлеушілерді жауапкершілікке тартудың маңыздылығына баса назар аударады.

Мысалы, Канададағы хакерлер басқа хакерлер тобы әзірлеген зиянды бағдарламаны пайдаланып, энергетикалық компанияға шабуыл жасады. Бұл жағдайда жауапкершілік тек шабуылды жасағандарға ғана емес, сонымен қатар пайдаланылған бағдарламалық жасақтаманы жасаған және таратқандарға да жүктеледі.

Сондықтан әзірлеушілер мен делдалдарды жауапкершілікке тарту киберқылмыспен күресте маңызды қадам болып табылады. Бұл мұндай әрекеттерді анықтау мен жолын кесудің техникалық құралдарын да, жазалаудың құқықтық тетіктерін де қамтитын кешенді тәсілді қажет етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық

бұзушылықтарды талдау киберқылмысты түсіну және онымен күресу үшін өте маңызды. Пәнді зерделеу нақты кімнің заңсыз әрекеттерді жасайтынын, қандай мотивтер мен мақсаттарды көздейтінін, сондай-ақ оның қандай білімі мен дағдысы бар екенін анықтауға мүмкіндік береді. Бұл тәсіл әрекеттерді дәлірек жіктеуге және кінәлілерді барабар жазалауға ықпал етеді. Киберқылмыскерлер жеке шабуылдаушылар немесе өз мақсаттарына жету үшін күрделі технологиялар мен әдістерді қолданатын ұйымдасқан топтар болуы мүмкін екенін ескеру маңызды. Осы субъектілердің сипаттамаларын түсіну бізге киберқылмыстардың алдын алу және онымен күресудің тиімді стратегияларын жасауға мүмкіндік береді.

Киберқылмыстарды қудалау тәсілдерін жақсарту үшін бірнеше негізгі аспектілерді ескеру қажет. Біріншіден, ақпараттық қауіпсіздік саласындағы заңнаманы заманауи шындықтар мен сын-қатерлерге сәйкес келетіндей етіп жаңарту маңызды. Зиянды бағдарламаларды әзірлеушілер мен делдалдардың жауапкершілігін реттейтін нақты ережелерді енгізу олардың қызметін тиімдірек тежеуге көмектеседі. Екіншіден, киберқылмыспен күресте халықаралық ынтымақтастықты күшейту қажет. Бірлескен жұмыс топтарын құру, ақпарат пен тәжірибе алмасу, сондай-ақ халықаралық келісімдерді әзірлеу трансшекаралық киберқылмыстармен тиімді күресуге мүмкіндік береді.

Үшіншіден, киберқылмыстарды анықтау мен жолын кесудің техникалық және аналитикалық әдістерін әзірлеу маңызды. Заманауи технологияларды инвестициялау, мамандарды оқыту және кибершабуылдарды талдау мен қадағалаудың жаңа құралдарын енгізу құқық қорғау органдары қызметінің тиімділігін арттыруға ықпал етеді. Соңында, киберқауіптер мен сақтық шаралары туралы халықтың хабардар болуын арттыру қажет. Науқандар мен білім беру бағдарламалары ықтимал құрбандардың санын азайтады және киберқылмыскерлердің жұмысын қиындатады.

Қорытындылай келе, ақпараттық қауіпсіздікті қамтамасыз етуде құқық бұзушылық субъектісін талдау және жауапкершілікке тарту әдістерін жетілдіру басты рөл атқарады. Заңнамалық, техникалық және білім беру шараларын қамтитын кешенді тәсіл киберқылмыспен тиімдірек күресіп, қоғамды цифрлық ортадағы қауіптерден қорғайды.

Сонымен, құқық бұзушылықтың жалпы субъектілері мынадай негізгі белгілермен сипатталады:

Кесте 3 – Құқық бұзушылықтың жалпы субъектілері

Қол қою	**Сипаттама**
Қылмыстық жауаптылықтың ең төменгі жасы	Қылмыстың ауырлығына қарай қылмыстық жауаптылық 16 жастан, ал аса ауыр қылмыстар үшін 14 жастан басталады.

Саналылық	Құқықбұзушылықтың субъектісі тек өз іс-әрекетін жүзеге асыруға және оларға бағыт беруге қабілетті, есі дұрыс адам бола алады. Психикалық бұзылулардың болуы немесе психикалық дамуының жеткіліксіз деңгейі адамды есі дұрыс емес деп тану үшін негіз бола алады, бұл оның қылмыстық жауаптылығын болдырмайды.
Іс-әрекеттердің заңсыздығын білу	Адам өз әрекетінің заңсыз екенін және қылмыстық жауаптылыққа әкеп соғуы мүмкін екенін білуі керек. Бұл әрекеттің фактілерін де, оның құқықтық салдарын да түсінуді қамтиды.
Іс-әрекеттердің еріктілігі	Қылмысты жасауға кінәлі деп тану үшін оның әрекеті үшінші тұлғалардың мәжбүрлеуінсіз өз еркімен жасалғанын дәлелдеу қажет. Әйтпесе, жауапкершілік қайта жіктелуі немесе толығымен алынып тасталуы мүмкін.

Бұл сипаттамалар кінәні анықтауда және үкім шығаруда шешуші рөл атқарады. Олар сондай-ақ қылмыстық құқық бұзушылықтың жалпы және ерекше субъектілерін ажыратуға көмектеседі, бұл әрекеттерді дұрыс саралау және әділ сот талқылауы үшін маңызды.

Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың субъектілерінің мәселелері ақпараттық технологиялар саласында арнайы білімі мен дағдылары бар арнайы субъектілерге ерекше назар аударуды талап етеді.

Арнайы субъектілердің негізгі сипаттамаларының бірі – олардың IT-технологияларды терең білуі және оларды қылмыстық мақсаттарында пайдалана білуі. Бағдарламашылар, тестерлер, жүйелік талдаушылар, веб-дизайнерлер және желі әкімшілері сияқты IT мамандары цифрлық кеңістікте кибершабуылдарды, бұзу және басқа да қылмыстық әрекеттерді жүзеге асыруға мүмкіндік беретін құралдар мен әдістерге қол жеткізе алады.

Мұндай мамандар иеленетін арнайы білім мен дағдыларға сценарийлерді кодтау және жазу қабілеті, қауіпсіздік және ақпаратты қорғау жүйелерін білу, мәліметтер базасымен және желі архитектураларымен жұмыс істеу қабілеті жатады. Бұл дағдылар оларды ерекше қауіпті етеді, өйткені олар кибершабуылдар жасап қана қоймайды, сонымен қатар зиянды бағдарламаларды жасай алады, ботнеттерді басқара алады және күрделі бұзу операцияларын жүргізе алады.

Арнайы актерлердің мысалдары ретінде кибер тыңшылықпен және деректерді ұрлау үшін бұзумен айналысатын хакерлер, сондай-ақ мемлекеттік және корпоративтік жүйелерге кибершабуыл жасау үшін қылмыстық топтарда жұмыс істейтін мамандар жатады. Мысалы, киберқауіпсіздік мамандарының киберқылмыскерлерге ауысу жағдайлары жиілеп барады. Мұндай адамдар желілік технологияларды терең біледі және қауіпсіздік жүйелерін айналып өту және шабуылдар жасау үшін өз дағдыларын пайдалана алады.

Осылайша, киберқылмыспен күресудің тиімді шараларын әзірлеу үшін

арнайы субъектілердің ерекшеліктерін және олардың уәждерін білу маңызды. Олардың кәсіби дағдыларын түсіну оларға ықтимал қауіптерді жақсы болжауға және тиісті қорғаныс шараларын әзірлеуге мүмкіндік береді. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъектісіне қатысты мәселелерді талдау әрекеттерді дұрыс саралау және кінәні анықтау үшін шешуші маңызы бар бірнеше негізгі аспектілерді бөліп көрсетуге мүмкіндік береді. Ең алдымен құқық бұзушылық субъектілерінің жасы мен әрекет қабілеттілігіне ерекше назар аудару қажет. Тәжірибе көрсеткендей, қылмыстық жауаптылықтың ең төменгі жасы жасалған қылмыстың ауырлығына, сондай-ақ нақты юрисдикцияға байланысты өзгереді. Әдетте, қылмыстық жауапкершілік 16 жастан басталады, бірақ аса ауыр қылмыстар үшін жауапкершілік 14 жастан басталуы мүмкін.

Маңызды элемент – құқық бұзушылық субъектісінің есінің дұрыстығы. Қылмысқа өз әрекетін жүзеге асыруға және оны басқаруға қабілетті есі дұрыс адам ғана кінәлі деп танылады. Психикалық бұзылулардың болуы немесе психикалық дамуының жеткіліксіз деңгейі адамды есі дұрыс емес деп тану үшін негіз бола алады, бұл оның қылмыстық жауаптылығын болдырмайды.

Сондай-ақ адам өз іс-әрекетінің заңсыздығын және оның құқықтық салдарын білуі тиіс екенін ескеру қажет. Қылмыстық құқық бұзушылықтың субъективтік жағының негізгі элементі әрекеттің фактілік және заңды жақтарын білу болып табылады. Адамды кінәлі деп тану үшін оның әрекетінің үшінші тұлғалардың мәжбүрлеуінсіз өз еркімен жасалғанын дәлелдеу маңызды.

Құқық бұзушылық субъектісін талдаудың маңыздылығы оның әрекеттерді дәлірек саралауға және әділ жаза белгілеуге мүмкіндік беретіндігінде. Сонымен қатар, жалпы және арнайы субъектілердің сипаттамаларын білу олардың арасындағы айырмашылықты анықтауға көмектеседі, бұл әсіресе ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін маңызды, мұнда әрекеттер техникалық күрделі және жасырын болуы мүмкін.

Киберқылмыстар үшін жауапкершілікке тарту әдістерін жетілдіру үшін ақпараттық қауіпсіздік саласындағы заңнаманы жаңарту, халықаралық ынтымақтастықты нығайту және кибершабуылдарды анықтау мен тоқтатудың техникалық және аналитикалық әдістерін әзірлеу қажет. Заңнамалық, техникалық және білім беру шараларын қамтитын кешенді тәсіл киберқылмыспен тиімдірек күресіп, қоғамды цифрлық ортадағы қауіптерден қорғайды.

2.5 Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық үшін жаза тағайындау мәселелері

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жаза тағайындау мәселелері цифрлық ортаның ерекшеліктерін ескере отырып мұқият қарауды талап ететін күрделі мәселе болып

табылады. Басты қиындықтардың бірі жасалған қылмыстық құқық бұзушылықтардың сипаты мен зардаптарын ескере отырып, барабар жазаларды анықтау болып табылады.

Осы саладағы негізгі мәселелердің қатарында:

1. Жазаның әділ және болжамды болуы үшін қылмыстың сипаты мен жазаның сәйкестігін орнату маңызды. Бұл жағдайда тек материалдық шығынды ғана емес, жәбірленушілер үшін ықтимал әлеуметтік және психологиялық зардаптарды да ескеру қажет.

2. Киберқылмыстардың ерекшеліктерін және оларды тергеудің күрделілігін ескере отырып, мұндай қылмыстық құқық бұзушылықтардың алдын алуға және жолын кесуге бағытталған арнайы жаза түрлерін енгізуге болады. Бұл айыппұлдарды, ақпараттық технологияларға қол жеткізу құқығынан айыруды, міндетті алдын алу шараларын және оқытуды қамтуы мүмкін.

3. Киберқылмыстар көбінесе халықаралық сипатқа ие және үкім шығаруда экстрадиция және халықаралық үйлестіру мәселелері туындауы мүмкін. Бұл халықаралық ынтымақтастықты дамытуды және киберқылмыспен тиімді күресу үшін елдер арасындағы нормативтік құқықтық актілерді үйлестіруді талап етеді.

4. Сондай-ақ киберқылмыс жасаған тұлғалардың алдын алу және оңалту мүмкіндіктерін қарастырған жөн. Бұл қайталанудың алдын алуға және қоғамға интеграциялануға бағытталған білім беру және қайта даярлау бағдарламаларын, психологиялық қолдауды және әлеуметтік оңалтуды қамтуы мүмкін [99].

Әлеуметтік даму мен технологиялық прогресс киберқылмыспен тиімді күресті қамтамасыз ету және цифрлық кеңістіктің қауіпсіздігін қамтамасыз ету мақсатында ақпараттандыру және байланыс саласындағы заңнаманы және жаза тағайындау тәжірибесін үнемі жаңартуды және бейімдеуді талап етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жаза тағайындау цифрлық ортаның ерекшеліктері мен қылмыстық құқық бұзушылықтардың сипатын ескеруді талап етеді. Негізгі міндет – киберқылмыстардың алдын алу мен жолын кесуде тиімді болатын әділ және барабар жазаларды анықтау. Материалдық зиян, сондай-ақ жәбірленушілер үшін әлеуметтік және психологиялық зардаптар ескерілуі керек. Айыппұлдар, ақпараттық технологияларды пайдалануға тыйым салу немесе міндетті алдын алу шаралары сияқты нақты жазаларды енгізу киберқылмыспен тиімді күресуге көмектеседі. Көптеген киберқылмыстардың халықаралық сипаты халықаралық ынтымақтастықты дамытуды және елдер арасындағы нормативтік құқықтық актілерді үйлестіруді талап етеді. Сондай-ақ оқыту бағдарламаларын, психологиялық қолдауды және әлеуметтік оңалтуды қамтуы мүмкін киберқылмыс жасаған тұлғалардың алдын алу және оңалту маңызды құрамдас бөлігі болып табылады. Цифрлық кеңістіктің қауіпсіздігін қамтамасыз ету ақпараттандыру және байланыс саласындағы заңнама мен жазалау тәжірибесін үнемі жаңартып, бейімдеуді талап етеді.

Сонымен, бұл бөлім ақпараттандыру және байланыс саласындағы қылмыстық

құқық бұзушылықтар үшін жаза тағайындау мәселелерін қарастыруға арналған. Жаза қылмыстық құқықта алдын алу және жазалау функцияларын орындай отырып, шешуші рөл атқарады. Кінәлі үшін жауапкершіліктің көлемін анықтау ғана емес, сонымен қатар келешекте осыған ұқсас құқық бұзушылықтардың алдын алуға көмектесетін тежеу мен тепе-теңдіктің тиімді жүйесін құру маңызды.

Қылмыстық құқықтағы жазаның маңызы оның көп функциялылығында. Жаза тек жасалған қылмыс үшін жазалау құралы болып қана қоймайды, сонымен қатар басқа адамдарды заңсыз әрекеттерден аулақ болуға шақыратын тәрбиелік қызмет атқарады. Сонымен қатар, сот төрелігін қалпына келтіру мен жәбірленушілердің құқықтарын қорғауда, қоғамдық тәртіп пен қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады.

Киберқылмыстар үшін жазалардың ерекшеліктері бөлек талдауды қажет етеді. Киберқылмыстар техникалық күрделіліктің жоғары дәрежесімен, трансшекаралық сипатымен және елеулі залал ауқымымен сипатталады. Осыған байланысты мұндай құқық бұзушылықтар үшін жазалар істің нақты мән-жайларын, мысалы, қылмысты жасау тәсілін, қылмыскердің себептері мен мақсаттарын, оның әрекетінің ықтимал және нақты салдарын ескеруі тиіс. Бұл заң шығарушылар мен құқық қорғау органдарының қызметкерлерінен IT-технологияларды біліп, түсінуді ғана емес, жаза қолдануда икемді болуын талап етеді.

Бұл бөлімде біз киберқылмыстар үшін жаза тағайындаудың негізгі принциптері мен тәсілдерін қарастырамыз, сонымен қатар әртүрлі юрисдикциялардағы құқық қолдану тәжірибесінің мысалдарын талдаймыз. Бас бостандығынан айыру және айыппұлдар сияқты дәстүрлі қылмыстық санкцияларды, сондай-ақ белгілі бір технологияларды пайдалануға тыйым салу немесе жәбірленушілерге өтемақы төлеу міндеттемесі сияқты арнайы шараларды қамтуы мүмкін нақты жазаларға ерекше назар аударылады.

Жаза бірнеше негізгі функцияларды атқара отырып, қылмыстық-құқықтық жүйеде негізгі рөл атқарады. Біріншіден, жаза жасалған қылмыс үшін жазалау, әділдікті қамтамасыз ету және қоғамдық әділеттілік сезімін қанағаттандыру құралы ретінде қызмет етеді. Екіншіден, келешекте қылмыстың алдын алуға бағытталған профилактикалық сипатқа ие. Жазаның алдын алу әсері әлеуетті қылмыскерлерді қорқыту және оларда қылмыстық іс-әрекеттер үшін жазаның бұлтартпас екендігіне сенім туғызу арқылы қол жеткізіледі. Үшіншіден, жаза сотталғандарды оңалтуға және қайта тәрбиелеуге, олардың әлеуметтік бейімделуіне және қоғамға кірігуіне жәрдемдесуге бағытталған түзеу функциясын орындайды [100].

Киберқылмыстар үшін жазалардың ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың ерекшеліктерімен анықталатын өзіндік белгілері бар. Киберқылмыс техникалық күрделіліктің жоғары дәрежесімен, трансшекаралық сипатымен және жеке адамға да , жалпы қоғамға да келтіруі мүмкін елеулі зиянмен сипатталады. Осыған байланысты

жазалауда істің нақты мән-жайлары, мысалы, қылмысты жасау тәсілі, қылмыскердің себептері мен мақсаттары, сондай-ақ оның әрекетінің ықтимал және нақты салдары ескерілуі тиіс.

Киберқылмыс үшін жазаның негізгі белгілерінің бірі дәстүрлі қылмыстық жазалау шараларын да, қайталанатын қылмыстардың алдын алуға бағытталған арнайы шараларды да қолдану қажеттілігі болып табылады. Атап айтқанда, мұндай шаралар белгілі бір технологияларды пайдалануға тыйым салуды, ақпараттық қауіпсіздік бойынша міндетті оқытуды, сондай-ақ зардап шеккендерге өтемақы төлеу міндеттемесін қамтуы мүмкін. Сонымен қатар, киберқылмыстың трансшекаралық сипатын ескере отырып, халықаралық ынтымақтастық пен әртүрлі елдердің құқық қорғау органдарының күш-жігерін үйлестіру ерекше маңызға ие. Осылайша, қылмыстық құқықтағы жазаның маңызын және киберқылмыстар үшін жазалардың ерекшеліктерін талдау ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершілікке тарту мәселелерін шешу үшін кешенді тәсіл қажет деген қорытынды жасауға мүмкіндік береді. Бұл заңнаманы үнемі жаңартып отыруды, құқық қолдану тәжірибесін жетілдіруді және халықаралық ынтымақтастықты нығайтуды талап етеді.

Қылмыстық құқықта жаза бірнеше функцияларды орындайды, олардың ішінде негізгілері жазалау, алдын алу және оңалту болып табылады. Үкім шығаруға негіз болатын принциптердің бірі – әділеттілік. Әділ жазада тек жасалған қылмыстың ауырлығы ғана емес, сонымен бірге қылмыскердің жеке басы, оның қылмыстан кейінгі мінез-құлқы, сондай-ақ іс-әрекеттің әлеуметтік салдары да ескерілуге тиіс [101].

Қылмыстық құқық бұзушылықтар үшін жаза тағайындау кезінде, оның ішінде ақпараттандыру және байланыс саласында бірқатар критерийлерді ескеру қажет. Біріншіден, бұл әрекеттің сипаты мен қоғамдық қауіптілік дәрежесімен анықталатын қылмыстың ауырлығы. Екіншіден, сот қылмыс жасаған адамның жеке басын, оның жасын, денсаулық жағдайын, отбасылық жағдайын және бұрын соттылығын ескеруі керек. Үшіншіден, маңызды фактор қылмыскердің қылмыс жасағаннан кейінгі мінез-құлқы, атап айтқанда оның өкінуі және тергеумен ынтымақтастығы сияқты факторлар.

Жазаны тағайындау кезінде қылмыстың материалдық зияны мен әлеуметтік зардаптарына ерекше назар аудару қажет. Киберқылмыс саласында бұған құрбандарға, компанияларға немесе мемлекеттік органдарға келтірілген залал кіруі мүмкін. Бұған қоса, әлеуметтік тұрақтылық пен цифрлық технологиялар мен инфрақұрылымға деген сенімнің салдары ескерілуі керек.

Материалдық залалды есепке алу кінәлінің өзінің қылмыстық әрекетімен келтірілген зиянды өтеуі тиіс деп есептейді. Бұл жәбірленушілерге тікелей өтемақы төлеуді немесе тиісті сомаларды мемлекеттік бюджетке аударуды қамтуы мүмкін. Қылмыстың әлеуметтік салдары қоғамдық қауіпсіздікке әсер ету, цифрлық жүйелерге сенім және компаниялар мен мемлекеттік органдар үшін

ықтимал беделді жоғалтуды қамтиды. Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін әділ жазаны белгілеу кезінде қылмыстың ауырлығын, қылмыскердің жеке басын, материалдық залал мен әлеуметтік зардаптарды қоса алғанда, факторлардың кең ауқымын ескеру қажет. актінің. Осы факторларды бағалаудың кешенді тәсілі қылмыстық жазаның әділдігі мен тиімділігін қамтамасыз етуге мүмкіндік береді [102].

Арнайы жазалар киберқылмыспен күресте маңызды рөл атқарады, өйткені олар ақпараттық-коммуникациялық технологияларды қолданумен байланысты қылмыстық әрекеттердің алдын алуға және жолын кесуге бағытталған. Арнайы жазаларға айыппұлдар, ақпараттық технологиялар саласындағы қызметке тыйым салу және алдын алу шаралары жатады.

Айыппұл – киберқылмыс үшін қолданылатын арнайы жазалардың ең көп тараған түрлерінің бірі. Олардың артықшылығы салыстырмалы түрде қолданудың жеңілдігінде және жасалған қылмыстың ауырлығына және келтірілген залалға байланысты айыппұл мөлшерін бейімдеу мүмкіндігінде. Айыппұл дербес жаза немесе басқа жаза түрлеріне қосымша болуы мүмкін [103]. Айыппұлдың тиімділігі олардың алдын алу функциясымен анықталады, өйткені материалдық шығын қаупі әлеуетті қылмыскерлерді тежеуші фактор бола алады.

Ақпараттық технологиялар секторындағы қызметке тыйым салу киберқылмыскерлерге қолданылатын тағы бір маңызды шара болып табылады. Бұл жаза компьютерлерді пайдалануға, интернетке кіруге немесе IT қатысты кейбір кәсіби әрекеттерге тыйым салуды қамтуы мүмкін. IT тыйымдары қылмыскерлерге жаңа қылмыстық құқық бұзушылықтар жасау үшін қажетті құралдарға қол жеткізуден бас тарту арқылы қылмыстың қайталануының алдын алуға бағытталған. Мұндай шаралар IT саласындағы арнайы білім мен дағдыларды пайдалана отырып, қылмыс жасалған жағдайларда тиімді.

Алдын алу шараларына киберқауіптер және олардың алдын алу жолдары туралы хабардарлықты арттыруға бағытталған білім беру бағдарламалары, тренингтер мен кеңестер кіреді. Бұл шаралар сотталғандарға да, киберқылмыстың ықтимал құрбандарына да қатысты болуы мүмкін. Профилактикалық іс-шаралар цифрлық кеңістікте қауіпсіздік мәдениетін қалыптастыруға және ақпараттық қауіпсіздік саласындағы білім мен дағдылардың жалпы деңгейін арттыру арқылы киберқылмыс деңгейін төмендетуге бағытталған [104].

Киберқылмыс үшін арнайы жазалардың тиімділігі олардың қайта қылмыс жасаудың алдын алу және әлеуетті қылмыскерлерді болдырмау қабілетімен анықталады. Зерттеулер көрсеткендей, жазаның ауырлығы қылмысқа тосқауыл немесе профилактикалық әсер етпейді, ал айыппұлдар мен ақпараттық технологияларға тыйым салу сияқты баламалы санкциялар бірдей табысты болуы мүмкін, бірақ қоғамға шығыны аз болып табылады. Айыппұлдар мен тыйым салуларды, сондай-ақ алдын алу шараларын қолдануды қоса алғанда, киберқылмыс үшін жаза тағайындаудың кешенді тәсілі киберқылмыспен күресте ең жақсы нәтижелерге қол жеткізуге ықпал етеді. Әрбір жағдайдың жеке

ерекшеліктерін ескеру және нақты жағдайға барынша сәйкес келетін шараларды қолдану маңызды.

Халықаралық ынтымақтастық киберқылмыспен күресте маңызды рөл атқарады, өйткені олар көбінесе трансұлттық сипатқа ие және оларды тергеу әртүрлі мемлекеттердің күш-жігерін үйлестіруді талап етеді. Бұл ынтымақтастықтың маңызды аспектілері экстрадициялау және халықаралық үйлестіру мәселелерін қамтиды.

Экстрадициялау – қылмыс жасағаны үшін айыпталған немесе сотталған адамды қылмыстық қудалау немесе жазалау үшін бір мемлекеттен екінші мемлекетке ауыстыру процесі. Киберқылмыстар контекстінде экстрадициялау ерекше маңызға ие болады, өйткені қылмыскерлер көбінесе ғаламдық интернет мүмкіндіктерін пайдалана отырып, әртүрлі мемлекеттердің аумағында өз әрекеттерін жасайды. Экстрадициялау рәсімі мемлекеттер арасындағы келісімдерді және өзара міндеттемелерді нақты анықтауды талап етеді [105]. Киберқылмыстар бойынша экстрадициялау мәселелерінің бірі әртүрлі елдердің заңдарын үйлестіру және қосарлы қылмыстылықты қамтамасыз ету, яғни әрекетті екі юрисдикцияда да қылмыс деп тану қажет.

Киберқылмыспен күресудегі халықаралық үйлестіру әртүрлі мемлекеттердің құқық қорғау органдары мен сот жүйелері арасындағы өзара іс-қимылдың әртүрлі нысандарын қамтиды. Бұл ынтымақтастық ресми және бейресми арналар арқылы жүзеге асуы мүмкін. Ресми шараларға өзара құқықтық көмек, қылмыстық қудалауды ауыстыру және халықаралық полиция ынтымақтастығы жатады. Интерпол және Еуропол сияқты ұйымдар ұлттық құқық қорғау органдарының күш-жігерін үйлестіруге көмектесе отырып, халықаралық үйлестіруде маңызды рөл атқарады [106].

Халықаралық ынтымақтастықтың көрнекті мысалы ретінде Будапешт конвенциясы деп аталатын Еуропа Кеңесінің Киберқылмыс туралы конвенциясы болып табылады. Ол киберқылмыспен күресу үшін ортақ құқықтық базаны құруды көздейді және қатысушы мемлекеттер арасында ақпарат пен дәлелдеме алмасу арқылы халықаралық ынтымақтастыққа жәрдемдеседі. Осы конвенцияға сәйкес елдер киберқылмыскерлерді тергеу мен қудалауда, сондай-ақ электрондық дәлелдемелерге қол жеткізуді қамтамасыз етуде бір-біріне көмектесуге міндеттенеді [107].

Тағы бір мысал, екі тараптың құқық қорғау органдары мен сот жүйелері арасындағы өзара іс-қимылды жеңілдететін АҚШ пен Еуропалық Одақ арасындағы құқықтық көмек және экстрадиция туралы келісім. Бұл келісім киберқылмыскерлерді тергеу және қудалау процесін айтарлықтай жеделдететін ақпарат пен дәлелдемелерді жылдам алмасу туралы ережелерді қамтиды [108].

Киберқылмыспен тиімді күресу әртүрлі мемлекеттер арасындағы экстрадицияны және үйлестіруді қамтитын халықаралық ынтымақтастықты талап етеді. Өзара құқықтық көмек көрсету және халықаралық ұйымдарға қатысу

сияқты шаралар киберқылмыстың алдын алу және қылмыстық жауапкершілікке тартуда басты рөл атқарады. Будапешт конвенциясы және АҚШ-ЕО келісімі сияқты табысты халықаралық ынтымақтастық мысалдары осы саладағы бірлескен күш-жігердің маңыздылығын көрсетеді.

Киберқылмыстың қарқынды өсуі жағдайында пайдаланушылардың да, ақпараттық қауіпсіздік мамандарының да білімдері мен дағдыларын арттыруға бағытталған *оқыту және қайта даярлау бағдарламалары басты рөл атқарады.* Мұндай бағдарламалардың маңыздылығы адамдардың ақпараттық-коммуникациялық технологияларды қолданумен байланысты қауіптер және олардан өзін қалай қорғау керектігі туралы түсініктерін дамыту болып табылады [109].

Жалпы халыққа, соның ішінде кәмелетке толмағандарға, қарт адамдарға және әртүрлі ұйымдардың қызметкерлеріне арналған білім беру бағдарламалары олардың киберқылмыстық әрекеттерге қатысу немесе осындай қылмыстық құқық бұзушылықтардың құрбаны болу ықтималдығын айтарлықтай төмендете алады. Мұндай бағдарламалар аясында студенттер киберқауіпсіздік негіздерімен, жеке деректерді қорғау әдістерімен, сондай-ақ интернетте қауіпсіз мінез-құлық қағидаларымен таныстырылады [110].

Ақпараттық қауіпсіздік мамандары үшін біліктілікті арттыру курстары, соның ішінде киберқауіптерді анықтау және алдын алудың заманауи әдістері, деректерді қорғаудың соңғы технологиялары және басқа елдердегі әріптестермен тәжірибе алмасу бағдарламалары жүргізіледі. Мұндай қайта даярлау мамандардың кәсіби деңгейін және олардың киберқылмыспен тиімді күресуге дайындығын арттыруға көмектеседі [111].

Киберқылмыстардың алдын алудың тиімді әдістерінің бірі халықтың әртүрлі санаттарын, соның ішінде жастарды, ұйымдардың қызметкерлерін және ақпараттық қауіпсіздік мамандарын оқыту және қайта даярлау бағдарламаларын жүзеге асыру болып табылады. Мұндай бағдарламалар киберқауіпсіздік саласындағы білім мен дағдылар деңгейін арттыруға бағытталған, бұл киберқылмысқа тартылу немесе осындай қылмыстық құқық бұзушылықтардың құрбаны болу қаупін азайтуға көмектеседі [112].

Сәтті бастаманың мысалы ретінде жас киберқылмыскерлерге арналған оңалту лагерлерін өткізуді қамтитын Ұлыбританиядағы Ұлттық қылмыс агенттігінің пилоттық жобасы болып табылады. Екі күндік лагерь барысында қатысушылар техникалық дағдыларды қалай қауіпсіз пайдалану керектігін үйренді, киберқауіпсіздік бойынша жұмыс мүмкіндіктері туралы ақпарат алды және әртүрлі оқыту іс-шараларына қатысты [113].

Компания қызметкерлеріне арналған оқыту бағдарламалары киберқауіпсіздік негіздері, деректерді қорғау әдістері және кибершабуылдарға әрекет етудің тәжірибелік аспектілері бойынша курстарды қамтиды. Бұл бағдарламаларға сонымен қатар басқа елдердегі әріптестермен тұрақты оқыту және тәжірибе

алмасу кіреді, бұл мамандарға соңғы қауіптер мен олардың алдын алу әдістерінен хабардар болуға көмектеседі [114].

Киберқылмыстан зардап шеккен *адамдарды психологиялық қолдау және әлеуметтік оңалту* маңызды . Кибербуллингтен, қаржылық шығындардан немесе жеке ақпараттың жоғалуынан туындаған күйзеліс құрбандардың психологиялық денсаулығын қалпына келтіруге кешенді көзқарасты талап етеді [115].

Психологиялық қолдау стресстің әсерін жеңуге, өзін-өзі бағалауды арттыруға және қалыпты жұмысты қалпына келтіруге бағытталған жеке және топтық кеңестерді қамтиды. Психологтар жәбірленушілердің әртүрлі санаттарының, соның ішінде кәмелетке толмағандар мен қарт азаматтардың ерекше қажеттіліктерін ескеретін қолдау бағдарламаларын әзірлейді.

Әлеуметтік оңалту жәбірленушілерді қоғамға біріктіру үшін жағдай жасауды, олардың әлеуметтік мәртебесін қалпына келтіруді және киберқылмыстық әрекеттерге қайта тартылудың алдын алуды көздейді. Осындай бағдарламалар аясында жоғалған құжаттарды қалпына келтіру, материалдық шығынды өтеу және заңгерлік көмек көрсету бойынша жұмыстар жүргізілуде [116].

Киберқылмыс құрбандарын сауықтыруда психологиялық қолдау және әлеуметтік оңалту маңызды рөл атқарады. Кибербуллингтен, қаржылық шығындардан немесе жеке ақпараттың жоғалуынан туындаған күйзеліс құрбандардың психологиялық денсаулығын қалпына келтіруге кешенді көзқарасты талап етеді [117].

Психологиялық қолдау стресстің әсерін жеңуге, өзін-өзі бағалауды арттыруға және қалыпты жұмысты қалпына келтіруге бағытталған жеке және топтық кеңестерді қамтиды. Психологтар жәбірленушілердің әртүрлі санаттарының, соның ішінде кәмелетке толмағандар мен қарт азаматтардың ерекше қажеттіліктерін ескеретін қолдау бағдарламаларын әзірлейді [118].

Әлеуметтік оңалту жәбірленушілерді қоғамға біріктіру үшін жағдай жасауды, олардың әлеуметтік мәртебесін қалпына келтіруді және киберқылмыстық әрекеттерге қайта тартылудың алдын алуды көздейді. Осындай бағдарламалар аясында жоғалған құжаттарды қалпына келтіру, материалдық шығынды өтеу және заңгерлік көмек көрсету бойынша жұмыстар жүргізілуде.

Киберқылмыс саласындағы тиімді профилактика және оңалту үшін оқыту және қайта даярлау бағдарламаларын, психологиялық қолдауды және зардап шеккендерді әлеуметтік оңалтуды қамтитын кешенді тәсіл қажет. Мемлекеттің, оқу орындарының және қоғамдық ұйымдардың бірлескен күш-жігері киберқылмыс деңгейін айтарлықтай төмендетіп, ақпараттық кеңістіктегі қауіпсіздікті арттыруға мүмкіндік береді.

Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін тиімді жазалар ақпараттық кеңістіктің қауіпсіздігін қамтамасыз етуде және азаматтардың құқықтарын қорғауда басты рөл атқарады. Олар жасалған қылмыстық құқық бұзушылықтар үшін жазалау құралы ретінде

ғана емес, сонымен бірге ықтимал бұзушыларды заңсыз әрекеттерден тежейтін профилактикалық функцияны орындайды. Жазаның тиімділігі олардың қатаңдығымен ғана емес, сонымен бірге әділеттілігімен, барабарлығымен және қолданудың бұлтартпастығымен де анықталатынын атап өткен жөн. Жазалар қылмыстың ауырлығына сәйкес келуі және қылмыскерлердің түзелуіне және қайта әлеуметтенуіне ықпал ету үшін олардың жеке ерекшеліктерін ескеруі тиіс.

Жаза жүйесін жетілдірудің бірінші қадамы ықпал ету шараларын саралау болып табылады. Қылмыскерлердің кінә дәрежесі мен жеке ерекшеліктерін ескере отырып, икемді жазалау жүйесін енгізу олардың тиімділігін айтарлықтай арттыруға мүмкіндік береді. Бұған қоғамдық жұмыстар, айыппұлдар және міндетті білім беру және қайта даярлау бағдарламалары арқылы сынақ мерзімі сияқты баламалы жазаларды қолдану кіреді.

Келесі маңызды бағыт – оңалту және қайта әлеуметтендіру бағдарламаларын әзірлеу. Қаржыландыруды ұлғайту және киберқылмыскерлерді оқыту мен қайта даярлауға бағытталған осындай бағдарламаларды кеңейту қылмыстың қайталануын азайтады. Бұл бағдарламалар киберқауіпсіздік бойынша оқытуды, жұмыс дағдыларын дамытуды және психикалық денсаулықты қолдауды қамтуы керек [119].

Халықаралық ынтымақтастықты нығайту да киберқылмыспен күрестің маңызды элементі болып табылады. Ақпарат алмасуды, үйлестіруді және өзара құқықтық көмекті қоса алғанда, халықаралық ынтымақтастықтың тиімді тетіктерін әзірлеу және енгізу трансұлттық қауіптерге қарсы тұруға және ұлттық юрисдикциялардан тыс әрекет ететін киберқылмыскерлерді қудалауға көмектеседі.

Ақпараттық саладағы қылмыстық құқық бұзушылықтың алдын алудың маңызды аспектілері халықтың хабардарлығын арттыру және киберқылмыстардың алдын алу болып табылады. Киберқауіптер мен қорғау әдістері, әсіресе балалар мен қарттар сияқты осал топтар арасында, сондай-ақ құпия ақпаратқа қол жеткізу мүмкіндігі бар ұйымдар қызметкерлерінің арасында хабардарлықты арттыруға бағытталған тұрақты білім беру науқандарын ұйымдастыру ықтимал құрбандардың санын азайтуға көмектеседі.

Сайып келгенде, заңнамалық базаны жетілдіру басым бағыт болуы керек. Заңнамалық нормаларды ақпараттық қауіпсіздіктің заманауи талаптарына сәйкес бейімдеу және жаңарту киберқылмыстардың әртүрлі түрлерін қамтитын жаңа баптарды енгізуді және оларды жасағаны үшін барабар санкцияларды белгілеуді қамтиды. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жазалау жүйесін жетілдіру алдын алу, оңалту және халықаралық ынтымақтастық шараларын қамтитын кешенді көзқарасты талап етеді. Бірлескен күш-жігер арқылы ғана біз ақпараттық қоғамның қауіпсіздігі мен тұрақты дамуының жоғары деңгейін қамтамасыз ете аламыз.

Сонымен, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объектісі оны дәстүрлі қылмыстық құқық бұзушылықтар

объектілерінен ерекшелейтін ерекше белгілерге ие. Ең алдымен, бұл ақпараттың материалдық емес сипатымен және оны цифрлық ортада қорғаудың қиындығымен байланысты. Ақпараттық ресурстар, жүйелер мен желілер тұтастығын, құпиялылығын немесе қолжетімділігін бұзу жеке тұлғаларға да, жалпы мемлекетке де елеулі зиян келтіруі мүмкін құнды активтер болып табылады. Бұл объектілерді тиімді қорғау мамандандырылған көзқарасты және құқықтық нормаларды қазіргі заманғы шындыққа бейімдеуді талап етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың объективтік жағы ақпараттық жүйелерді мақсатсыз пайдалануға немесе олардың жұмыс істеуін бұзуға бағытталған арнайы әрекеттермен немесе әрекетсіздіктермен сипатталады. Мұндай құқық бұзушылықтардың объективтік жағын анықтауға байланысты негізгі мәселелерге қылмыс фактісін, оның ауқымын және зардаптарын анықтаудағы қиындықтар жатады. Фишинг, хакерлік және зиянды бағдарламаларды тарату сияқты киберқылмыс жасаудың заманауи әдістері құқық қорғау органдарынан жоғары біліктілікті және кінәні тиімді тергеу және дәлелдеу үшін соңғы технологияны пайдалануды талап етеді. Осылайша, цифрлық орта объектілерін тиімді қорғау осы құқық бұзушылықтардың объективті аспектілерін егжей-тегжейлі талдаусыз және түсінусіз мүмкін емес.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъективтік жағына қылмыскерді бағыттайтын мотивтер мен мақсаттар жатады. Маңызды аспект ниетті анықтау болып табылады, өйткені киберкеңістікте көптеген әрекеттер кездейсоқ немесе абайсызда жасалуы мүмкін. Субъективтік жағын анықтау қылмыскердің мінез-құлқы мен ниеттерін жан-жақты талдауды, сондай-ақ әрекеттер жасырын және жасырын болуы мүмкін цифрлық ортаның ерекшеліктерін түсінуді талап етеді. Субъективтік жағын түсіну қылмыскердің шынайы ниетін анықтауға және оның кінәсінің дәрежесін анықтауға көмектеседі, бұл әділ жаза тағайындаудың кілті болып табылады.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың субъектісі ақпараттық ресурстар, жүйелер, деректер мен технологиялар болып табылады. Цифрлық технологиялардың әртүрлілігі мен динамикасы құқық қорғау органдарына жаңа міндеттер тудырады. Қылмыстың субъектісі деректер де, өңдеу және беру құралдары да бола алатынын ескерген жөн. Бұл заң шығарушылардан жылдам өзгеретін цифрлық ортада деректер мен технологияны лайықты қорғау үшін заңды стандарттарды үнемі жаңартып, бейімдеуді талап етеді. Сонымен, қылмыстық құқық бұзушылықтың субъектісі оның объектісімен және объективтік жағымен тығыз байланысты, бұл оларды қорғаудың кешенді тәсілінің қажеттілігін көрсетеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жаза қолдану киберқылмыстардың алдын алуға және деңгейін төмендетуге бағытталған құқық қолдану тәжірибесінің маңызды элементі болып табылады. Тиімді жазалар цифрлық ортаның ерекше ерекшеліктері мен жасалған қылмыстық құқық бұзушылықтардың сипатын ескере отырып, әділ және

барабар болуы керек. Құқық бұзушыларды, әсіресе жастарды оқыту және қайта даярлау бағдарламалары, сондай-ақ психологиялық қолдау арқылы оңалту және әлеуметтендіру мәселелеріне ерекше назар аудару қажет. Халықаралық ынтымақтастық пен тәжірибе алмасу трансұлттық киберқылмыспен күрестің негізгі факторлары болып табылады. Осылайша, жаза тағайындау мәселелері ақпараттандыру және байланыс саласындағы құқық бұзушылықтардың объектілерін, объективті және субъективті жақтарын, сондай-ақ субъектісін түсінумен тығыз байланысты [120].

Сонымен, 2-тарау ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың әртүрлі аспектілерін, оның ішінде объектілердің ерекшеліктерін, объективті және субъективті жақтарының мәселелерін, пәндік және жаза тағайындау мәселелерін жан-жақты талдауға арналған. Ақпараттық ресурстар мен жүйелерді тиімді қорғау құқықтық нормаларды заманауи сын-қатерлерге бейімдеуді, қылмыстық құқық бұзушылықтарды тергеуге және әділ жаза тағайындауға мамандандырылған көзқарасты талап етеді. Алдын алу, оңалту және халықаралық ынтымақтастық шараларын қамтитын кешенді және пәнаралық тәсіл ғана ақпараттық кеңістікті сенімді қорғауды қамтамасыз етеді және киберқылмыс деңгейін төмендетуге көмектеседі.

3 ТАРАУ АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ КРИМИНОЛОГИЯЛЫҚ АСПЕКТІЛЕРІ

Киберқылмыстардың криминологиялық аспектілері қылмыстық құқық бұзушылықтардың сипатын, олардың қоғамға әсерін, динамикасын, құрылымын, себептерін және қылмыстық әрекеттердің алдын алу мен оларға қарсы тұру механизмдерін терең түсінуге бағытталған. Бұл аспектілерді зерттеу киберқылмыстардың ерекшеліктерін ашып, олармен күресу үшін тиімді стратегияларды жасауға мүмкіндік береді.

Киберқылмыстардың ерекшеліктері оларды дәстүрлі қылмыстық құқық бұзушылықтан ажыратып тұратын бірқатар маңызды сипаттарға ие. Біріншіден, киберқылмыстардың виртуалды сипаты оларға тән ерекше белгі болып табылады. Бұл қылмыстық құқық бұзушылықтар физикалық кеңістікте емес, ақпараттық жүйелер мен деректер арқылы жүзеге асады. Екіншіден, киберқылмыстардың трансшекаралық сипаты олардың әлемнің кез келген нүктесінен жасалатынын көрсетеді. Бір мемлекет аумағында жасалған қылмыс басқа елдің заңдарына қатысты болуы мүмкін, бұл құқықтық қиындықтар туғызады. Үшіншіден, киберқылмыскерлердің әрекеттері көбінесе анонимді болып келеді, бұл оларды анықтауды қиындатады. Ақпаратты шифрлау және анонимдеу технологияларын пайдалану құқық қорғау органдарының тергеу жұмыстарын қиындатады. Төртіншіден, киберқылмыстарды жасау үшін жоғары техникалық дайындық қажет. Бұл қылмыстық құқық бұзушылықтарды көбінесе кәсіби хакерлер мен ұйымдасқан қылмыстық топтар жүзеге асырады.

Киберқылмыстарды талдауда олардың криминологиялық себептерін анықтау маңызды рөл атқарады. Экономикалық пайда табу киберқылмыстардың ең кең таралған мотивацияларының бірі болып табылады. Банктік алаяқтық, деректерді ұрлау және ransomware секілді бағдарламаларды пайдалану арқылы ақша талап ету – осындай қылмыстардың мысалы. Сонымен қатар, саяси немесе идеологиялық мақсаттарға жету үшін жасалатын киберқылмыстар да жиі кездеседі. Бұл жағдайда шабуылдар мемлекеттік жүйелерге немесе белгілі бір ұйымдарға бағытталуы мүмкін.

Киберқылмыстардың құрылымы мен динамикасы үнемі өзгеріп отырады. Бұл қылмыстық құқық бұзушылықтардың саны жыл сайын артып келеді, әсіресе цифрландырудың өсуі мен интернетке қолжетімділіктің кеңеюі жағдайында. COVID-19 пандемиясы кезінде қашықтан жұмыс істеу және онлайн қызметтердің өсуі киберқылмыстардың таралуына ықпал етті. Қылмыстардың кең таралған түрлері фишинг, зиянды бағдарламалар тарату, деректерді ұрлау, DDoS шабуылдары және банктік алаяқтық болып табылады. Бұл қылмыстық құқық бұзушылықтардың ерекшелігі – оларды жасау әдістері үнемі жетілдіріліп, жаңа технологиялар мен осалдықтарды пайдаланады.

Криминологиялық тұрғыдан алғанда, киберқылмыстармен тиімді күрес үшін

бірқатар тұжырымдар жасауға болады. Біріншіден, профилактикалық шаралардың маңызы зор. Бұл халықты ақпараттық қауіпсіздік негіздеріне оқыту және құқық қорғау органдары қызметкерлерінің кәсіби біліктілігін арттыру арқылы жүзеге асуы тиіс. Екіншіден, қылмыстық жауапкершілік шараларын күшейту қажет. Ұйымдасқан киберқылмыстық топтардың әрекеттері үшін қатаң санкцияларды енгізу қылмыстардың алдын алуға мүмкіндік береді. Үшіншіден, құқық қорғау органдарын заманауи технологиялармен жабдықтау маңызды. Киберқылмыстарды анықтау және тергеу үшін арнайы бағдарламалық қамтамасыз ету мен техникалық құралдар қажет. Төртіншіден, киберқауіптерді зерттеу мен мониторинг жүргізетін орталықтарды құру маңызды. Мұндай орталықтар киберқауіптердің алдын алу және қылмыстық әрекеттерді дер кезінде анықтау үшін ақпаратты талдауға мүмкіндік береді.

Халықаралық ынтымақтастықты нығайту киберқылмыстармен күресте негізгі рөл атқарады. Киберқылмыстардың трансшекаралық сипаты оларды жекелеген елдердің күш-жігерімен ғана емес, халықаралық деңгейде бірлескен әрекеттер арқылы жеңуге болатынын көрсетеді. Қазақстанның Будапешт конвенциясына қосылуы, трансшекаралық қылмыстармен күресу үшін халықаралық серіктестермен ақпарат алмасуды және бірлескен операциялар жүргізуді қамтиды. Сонымен қатар, халықаралық тәжірибе мен заңнамаларды зерделеу киберқылмыстарға қарсы ұлттық стратегияны жетілдіруге мүмкіндік береді.

Криминологиялық аспектілерді зерттеу киберқылмыстарды тиімді бақылау және алдын алу шараларын әзірлеу үшін қажет. Бұл зерттеулер қоғамды ақпараттық қауіпсіздікке дайындап, ұлттық және халықаралық деңгейде құқық қорғау органдарының жұмысын жетілдіруге мүмкіндік береді. Қазақстанның құқық қорғау органдары, заң шығарушылары және жеке сектордың бірлескен күші ғана киберқылмыстардың өсу қарқынын тоқтатып, ақпараттық инфрақұрылымды сенімді қорғауға қол жеткізе алады.

3.1 Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылыққа қарсы іс-қимылдың криминологиялық сипаттамасы

Ақпараттық технологиялардың қарқынды дамуы және қоғамның цифрлық трансформациясы жағдайында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық аспектілерінің маңыздылығы арта түсуде. Ақпараттық қауіпсіздік мемлекет үшін де, жеке сектор үшін де негізгі міндеттердің біріне айналуда. Бұл саладағы бұзушылықтар айтарлықтай экономикалық шығындарға, маңызды инфрақұрылымның бұзылуына және ұлттық қауіпсіздікке қатер төндіруі мүмкін. Осыған байланысты мұндай құқық бұзушылықтардың криминологиялық аспектілерін зерттеу өзекті және маңызды міндет болып табылады.

Ақпараттық қауіпсіздік мәліметтердің құпиялылығын, тұтастығын және

қолжетімділігін қорғауды қамтиды. Бұл саладағы бұзушылықтар елеулі зардаптарға, соның ішінде қаржылық шығындарға, мемлекеттік және жеке құрылымдарға деген сенімнің жойылуына, ұлттық қауіпсіздікке қатер төндіруі мүмкін. Үкімет үшін бұл тиімді қорғау тетіктерін құру және қолдау, ал жеке сектор үшін сенімді киберқауіпсіздік жүйелерін енгізу және деректерді қорғау процедураларын жүйелі түрде жаңарту қажеттілігін білдіреді.

Сондай-ақ, қазіргі жағдайда ақпараттық қауіпсіздік тұрақтылықты қамтамасыз етуде және мемлекеттік және жеке мүдделерді қорғауда шешуші рөл атқаратынын атап өткен жөн. Киберқылмыстың өсуі озық технологиялар мен халықаралық ынтымақтастыққа негізделген тиімді қарсы шараларды әзірлеуді және енгізуді талап етеді. Бұл бөлімде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимыл әрекеттерінің криминологиялық сипаттамаларына жан-жақты талдау жасалады.

Бұл бөлім киберқылмыспен күресудің негізгі тәсілдері мен әдістерін қарастырудан басталады. Заң шығару және орындау сияқты дәстүрлі әдістер жасанды интеллект пен үлкен деректерді талдауды қоса алғанда, заманауи технологиялық шешімдермен үйлеседі. Бұл әдістер қылмыстық құқық бұзушылықтың алдын алуға және құқық бұзушылықты жедел ашуға бағытталған. Төмендегі бөлімде киберқылмыспен күресу бойынша үкімет шаралары қарастырылады. Киберқауіпсіздікті нығайтуға бағытталған ұлттық стратегиялар мен бағдарламаларға ерекше назар аударылады. Жедел-іздестіру іс-шараларын жүргізетін және киберқылмыстардың алдын алу мен ашумен айналысатын құқық қорғау органдары мен арнайы қызметтер маңызды рөл атқарады. Осы құқық бұзушылықтардың жаһандық сипатын ескере отырып, халықаралық ынтымақтастық киберқылмыспен күрестің құрамдас бөлігі болып табылады. Халықаралық үйлестіру және мемлекеттер арасында ақпарат алмасу, сондай-ақ бірлескен операциялар мен келісімдер киберқауіптерге тиімді қарсы тұруда маңызды рөл атқарады. Бөлім киберқылмыспен күресу бойынша қолданыстағы шаралардың тиімділігін талдаумен аяқталады. Қолданылатын әдістер мен бағдарламалардың тиімділігін бағалау қолданыстағы жүйенің күшті және әлсіз жақтарын анықтауға мүмкіндік береді. Технологиялық прогресс басқару әдістеріне айтарлықтай әсер етеді, ол стратегияларды үнемі жаңартып отыруды және жаңа міндеттерге бейімдеуді талап етеді. Осылайша, бұл бөлім киберқылмыспен күресу бойынша кешенді іс-қимылдарды зерделеуге және талдауға бағытталған, бұл қолданыстағы шараларды жетілдіру және ақпараттық қауіпсіздік деңгейін арттыру бойынша ұсыныстар әзірлеуге мүмкіндік береді.

Киберқылмыспен күресудің дәстүрлі әдістеріне құқық бұзушыларды қудалау мен жазалаудың құқықтық негіздерін жасауға бағытталған заңнамалық шаралар жатады. Заңдар мен ережелер ақпараттық технологияларды пайдалануды реттейді, киберқылмыстың әртүрлі түрлері үшін жауапкершілікті белгілейді, деректер мен жүйелерді қорғау шараларын қарастырады. Дәстүрлі тәсілдің маңызды элементі киберқылмыскерлерді тергеу мен қудалауды қамтитын құқық қорғау қызметі

болып табылады. Бұл тәсіл киберқылмыстың алдын алу және онымен күресу үшін негіз болып табылады, бірақ ол әрқашан технологияның қарқынды дамуымен қатар келе бермейді [121].

Киберқылмыстардың алдын алудың заманауи әдістері озық технологиялар мен инновациялық тәсілдерді қолдануды қамтиды. Бұл әдістер үлкен деректерді талдау және күдікті әрекеттерді анықтау үшін жасанды интеллект пен машиналық оқыту жүйелерін енгізуді қамтиды. Бұл жүйелер ықтимал кибершабуылдарды болжай алады және олардың алдын алу шараларын автоматты түрде қабылдай алады. Заманауи стратегияның маңызды элементі бағдарламалық жасақтаманы жүйелі түрде жаңартуды, пайдаланушыларды қауіпсіз онлайн тәртібі туралы оқытуды және көп факторлы аутентификацияны енгізуді қамтитын кибергигиена болып табылады. Дәстүрлі және заманауи әдістерді біріктіретін кешенді тәсіл киберқауіптерден күшті қорғауды қамтамасыз етеді.

Киберқылмыстық құқық бұзушылықтардың себептері мен криминологиялық ерекшеліктері

Киберқылмыстың негізінде жатқан себептер мен факторларды терең талдау – бұл саладағы құқық бұзушылықтармен күресудің алғашқы қадамдарының бірі. Киберқылмыстардың ерекше ерекшелігі – олардың жасаушыларының жасырын әрекет ету мүмкіндігі, шекаралардың болмауы және қолжетімді технологиялық құралдардың көптігі. Бұл қылмыстық құқық бұзушылықтардың жасалуын жеңілдететін негізгі факторлар мыналар:

Анонимдік: Интернет пайдаланушыларының көпшілігі өздерінің әрекеттерін анонимдік жағдайда жүзеге асыруы мүмкін. Бұл қылмыскерлерге заңсыз әрекеттерді еркін жүргізуге мүмкіндік береді, өйткені олардың шынайы тұлғаларын анықтау күрделі.

Трансұлттық сипат: Киберқылмыс бір елдің аумағымен шектелмейді. Қылмыскерлер бір елден әрекет етіп, басқа мемлекеттерге зиян тигізуі мүмкін. Бұл құқық қорғау органдары үшін киберқылмыстарды тергеуде қосымша қиындықтар тудырады.

Технологиялық қолжетімділік: Интернеттегі заңсыз әрекеттерге арналған құралдар мен бағдарламалар кеңінен қолжетімді. Зиянды бағдарламаларды немесе кибер шабуыл жасау үшін қажетті құралдарды сатып алу немесе әзірлеу оңайға соғады.

Қаржылық пайда: Киберқылмыскерлердің көпшілігі материалдық пайда табуды көздейді. Криптовалюталардың таралуы бұл қылмыстық құқық бұзушылықтарды жасауды жеңілдетті, себебі криптовалюталарды анонимді түрде пайдалану мүмкіндігі бар.

Ақпараттық технологияларды пайдалану арқылы жасалатын қылмыстық құқық бұзушылықтарды жіктеу

Киберқылмыстардың жіктелуі олардың сипатына, қылмыскердің мотивациясына және зиян келтіру әдістеріне байланысты әртүрлі болуы мүмкін. Ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды

келесі топтарға бөлуге болады:

Компьютерлік жүйелерге рұқсатсыз қол жеткізу: Компьютерлік желілерге заңсыз кіру және оларды пайдалану арқылы деректерді ұрлау немесе жүйені зақымдау.

Зиянды бағдарламаларды тарату: Вирустар, трояндық бағдарламалар, рансомвар сияқты зиянды бағдарламаларды тарату арқылы жүйелерге шабуыл жасау.

Интернет арқылы алаяқтық жасау: Фишинг, интернет-банкинг жүйелеріне шабуыл жасау, жалған веб-сайттар арқылы деректерді ұрлау.

Деректерді ұрлау және заңсыз пайдалану: Жеке және корпоративтік деректерді рұқсатсыз алу және оларды заңсыз мақсатта пайдалану.

Зияткерлік меншік құқықтарын бұзу: Пираттық бағдарламаларды, фильмдер мен музыкаларды заңсыз тарату, авторлық құқықты бұзу [122].

Құқықтық реттеу және заңнамалық бастамалар

Киберқылмыстардың алдын алу және олармен күресу үшін құқықтық нормалар мен заңнамалық бастамалар басты рөл атқарады. Қазіргі уақытта көптеген елдер ақпараттық жүйелерді қорғауға бағытталған заңдарды әзірлеп, қолданысқа енгізіп жатыр. Мысалы, Қазақстан Республикасында қабылданған «Ақпараттандыру туралы» заң ақпараттық қауіпсіздікке ерекше көңіл бөледі. Бұл заң деректерді қорғауға қатысты міндеттемелерді күшейтеді және киберқылмыстарға қарсы күресудің құқықтық негіздерін айқындайды.

Сонымен қатар, Қазақстанның Қылмыстық кодексінде ақпараттық жүйелерге рұқсатсыз кіру, деректерді жою немесе өзгерту, зиянды бағдарламаларды тарату сияқты әрекеттер үшін жауапкершілік қарастырылған. 205-213-баптарда ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін нақты жазалар көзделген.

Халықаралық ынтымақтастық және трансұлттық қылмыстық құқық бұзушылықтар

Киберқылмыстардың жаһандық сипатын ескере отырып, халықаралық ынтымақтастықтың маңыздылығы артып отыр. Трансұлттық қылмыстық құқық бұзушылықтарға қарсы тұру үшін мемлекеттер арасында ақпарат алмасу, құқықтық көмек көрсету және бірлескен операциялар жүргізу қажет. Будапешт конвенциясы – киберқылмыстарға қарсы күрестегі халықаралық келісімдердің бірі болып табылады. Бұл конвенция трансұлттық қылмыстық құқық бұзушылықтарды тергеу барысында мемлекеттер арасында құқықтық көмек көрсету және қылмыскерлерді экстрадициялау мүмкіндігін қамтамасыз етеді.

Еуропа, Азия, АҚШ сияқты елдерде киберқылмыстарға қарсы күресудің әртүрлі құқықтық және техникалық тәсілдері енгізілген. Мысалы, Еуропалық Одақ киберқауіпсіздік саласындағы ынтымақтастықты күшейту үшін арнайы директивалар қабылдады, ал АҚШ-та Computer Fraud and Abuse Act (CFAA) заңы киберқылмыстармен күресуге бағытталған маңызды құжаттардың бірі болып табылады. Азия елдерінде, соның ішінде Оңтүстік Корея, Жапония және Қытайда

да ақпараттық қауіпсіздікті қамтамасыз ету үшін күрделі құқықтық жүйелер құрылуда [123].

Киберқауіпсіздікті қамтамасыз етудің техникалық шаралары

Ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін тек заңнамалық шаралар ғана жеткіліксіз. Киберқылмыстармен тиімді күресу үшін техникалық құралдарды қолдану қажет. Бұл құралдарға мыналар кіреді:

Шифрлау және деректерді қорғау технологиялары: Деректерді шифрлау арқылы олардың қауіпсіздігін қамтамасыз ету және рұқсатсыз қол жеткізуге жол бермеу.

Фаерволлдар және желіаралық қалқандар: Желіаралық қалқандар арқылы жүйелерге сырттан кіру әрекеттерін шектеу және кибершабуылдарға қарсы қорғау.

Антивирустық бағдарламалар: Вирустар мен зиянды бағдарламаларға қарсы жүйелерді қорғау үшін антивирустық бағдарламаларды пайдалану.

Мультфакторлы аутентификация: Пайдаланушылардың жеке мәліметтерін қорғау үшін көп факторлы аутентификацияны енгізу [124].

Киберқылмыстардың алдын алу және халықты оқыту

Киберқылмыспен тиімді күресу үшін халықтың киберсауаттылығын арттыру маңызды. Бұл бағытта арнайы білім беру бағдарламаларын, семинарлар мен тренингтерді ұйымдастыру арқылы қоғамның киберқауіптер туралы хабардарлығын арттыру қажет. Мысалы, Қазақстанда киберқауіпсіздік туралы арнайы курстар мен тренингтер өткізіліп, мемлекеттік органдар мен жеке сектор қызметкерлеріне киберқауіптермен қалай күресуге болатыны туралы нұсқаулықтар беріледі.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимылдың криминологиялық сипаттамасын жан-жақты талдау бұл мәселені шешу үшін кешенді тәсілді қолданудың маңыздылығын көрсетеді. Құқықтық, техникалық және профилактикалық шараларды үйлестіре отырып, киберқылмыстардың алдын алу және олармен күресу мүмкіндігі артады. Трансұлттық қылмыстық құқық бұзушылыққа қарсы күресте халықаралық ынтымақтастықтың рөлі ерекше, себебі бұл құқық бұзушылықтар жаһандық қауіпсіздікке үлкен қауіп төндіреді.

Киберқылмыстарды шешуде *технологияны қолдану* қазіргі жағдайда басты рөл атқарады. Ең тиімді құралдардың бірі - нақты уақытта күдікті әрекетті анықтауға және бақылауға мүмкіндік беретін үлкен деректерді талдау. Машиналық оқыту және жасанды интеллект технологиялары деректерді талдау процесін автоматтандыруға көмектеседі, кибершабуылдарды анықтау мен жауап беруді жеделдетеді. Бұл технологияларды қолдану құқық қорғау органдарына қылмыстық заңдылықтарды жылдам анықтауға және ықтимал қауіптердің алдын алуға мүмкіндік береді.

Сонымен қатар, маңызды аспект сотта цифрлық дәлелдемелерді жинау, талдау және ұсыну үшін цифрлық сот сараптамасын пайдалану болып табылады.

Сандық криминалистика мамандары киберқылмыскерлер жойылған немесе бүлінген деректерді қалпына келтіру және талдау әдістері мен құралдарын әзірлейді. Бұл құқық бұзушылардың кінәсін дәлелдеуге ғана емес, сонымен қатар қорғау әдістерін жетілдіру бойынша олардың әрекетінің тетіктерін түсінуге мүмкіндік береді. Заманауи технологиялар сонымен қатар сандық дәлелдемелердің тұтастығы мен шынайылығын қамтамасыз ету үшін блокчейн технологияларын қолдануды қамтиды, осылайша сот төрелігі процесіне сенімді арттырады. Осылайша, дәстүрлі және заманауи әдістерді үйлестіру, сондай-ақ озық технологияларды белсенді пайдалану ақпараттық қауіпсіздік деңгейін арттыруға көмектесетін киберқылмыстардың алдын алу мен анықтауға кешенді көзқарасты қамтамасыз етеді.

Ұлттық стратегиялары мен бағдарламалары ақпараттық қауіпсіздік саласындағы мемлекеттік саясаттың негізі болып табылады. Түрлі елдер киберқылмыстың алдын алуға, анықтауға және онымен күресуге бағытталған кешенді жоспарларды әзірлеп, жүзеге асыруда. Бұл стратегиялар заңнамалық бастамаларды, маңызды инфрақұрылымды қорғау шараларын және халықтың киберсауаттылық деңгейін арттыру бағдарламаларын қамтиды. Маңызды аспект – киберқауіпсіздік жөніндегі күш-жігерді үйлестіруді қамтамасыз ету үшін мемлекеттік органдар мен жеке сектор арасындағы ынтымақтастық болып табылады. Мұндай бағдарламаларды іске асыру киберқылмыспен күресте жүйелі көзқарасты құруға және ұлттық мүдделерді қорғаудың жоғары деңгейін қамтамасыз етуге мүмкіндік береді [125].

Киберқылмыспен күресте *құқық қорғау органдары мен арнайы қызметтер басты рөл атқарады.* Олар жедел-іздестіру шараларын жүргізеді, ақпарат және байланыс саласындағы қылмыстық құқық бұзушылықтарды тергейді, сондай-ақ кінәлілерді жауапқа тартады. Олардың жұмысының маңызды элементі қызметкерлерді үздіксіз оқыту және киберқауіптерді талдау және анықтау үшін заманауи технологияларды пайдалану болып табылады. Полиция, қауіпсіздік қызметі және басқа да құқық қорғау органдары құрамында киберқылмыспен күресетін арнайы бөлімшелер құрылуда. Бұл бөлімшелер халықаралық ұйымдармен және басқа елдердің әріптестерімен трансшекаралық киберқылмыспен күресте күш-жігерді үйлестіру үшін ынтымақтасады.

Сонымен қатар, құқық қорғау органдары азаматтар мен ұйымдарды киберқауіптерден қорғау жолдары туралы ақпараттандыруға бағытталған профилактикалық жұмыстарды жүргізеді. Бұған білім беру бағдарламаларын, семинарлар мен тренингтерді өткізу, сондай-ақ ақпараттық материалдарды тарату кіреді. Маңызды аспект жеке сектормен, соның ішінде киберқауіпсіздік компанияларымен ақпарат алмасу және киберқылмысты анықтау және тоқтату үшін бірлесіп жұмыс істеу болып табылады. Осылайша, құқық қорғау органдары мен арнайы қызметтердің рөлі ақпараттық қауіпсіздікті қамтамасыз ету және киберқылмыспен тиімді күресу жөніндегі кешенді тәсілдің құрамдас бөлігі болып табылады.

Халықаралық үйлестіру және ақпарат алмасу киберқылмыспен күрестің маңызды элементтері болып табылады. Киберқылмыс көбінесе трансшекаралық сипатқа ие және қылмыскерлер әртүрлі елдерде орналасқан инфрақұрылым мен ресурстарды пайдалана алады. Бұл құқық қорғау органдарына күрделі құқықтық және операциялық қиындықтар туғызады. Халықаралық деңгейде күш-жігерді үйлестіру мұндай қылмыстық құқық бұзушылықтарды тиімді анықтауға және жолын кесуге, ағымдағы қауіптер мен олардың алдын алу әдістері туралы ақпаратпен неғұрлым жылдам алмасуды қамтамасыз етуге мүмкіндік береді. Бірлескен күш-жігер цифрлық кеңістіктегі жалпы қауіпсіздікті айтарлықтай жақсартатын киберқауіптерді бақылау және алдын ала ескертудің жаһандық жүйесін құруға ықпал етеді.

Киберқылмысқа қарсы күресте елдер арасындағы тиімді ынтымақтастықты қамтамасыз етуде *халықаралық келісімдер мен бірлескен операциялар шешуші рөл атқарады.* Киберқауіпсіздік жөніндегі күш-жігерді үйлестіруге бағытталған әртүрлі халықаралық шарттар мен конвенциялар бар, мысалы, Киберқылмыс туралы Будапешт конвенциясы. Бұл келісімдер киберқылмыстарды тергеу мен қудалаудың ортақ стандарттары мен рәсімдерін белгілейді және экстрадиция мен мемлекеттер арасындағы құқықтық көмекті жеңілдетеді.

Интерпол және Еуропол сияқты халықаралық ұйымдар жүргізген бірлескен операциялар ынтымақтастықтың жоғары деңгейін көрсетеді және ірі киберқылмыстық желілерді сәтті анықтап, бұзды. Мұндай операцияларға барлау мәліметтерін алмасу, елдер бойынша құқық қорғау күштерін үйлестіру, үйлестірілген рейдтер мен тұтқындаулар жүргізу кіреді. Табысты халықаралық операциялардың мысалдары тығыз ынтымақтастық пен ресурстарды біріктіру арқылы ғана жаһандық киберқауіптермен тиімді күресуге және халықаралық деңгейде ақпараттық кеңістікті қорғауға болатынын көрсетеді.

Құқық қорғау органдарының статистикасы мен есептері киберқылмыстың динамикасын бағалап, қазіргі жүйенің осал тұстарын анықтай алады. Іс жүзінде қандай әдістер мен шаралардың нақты жұмыс істейтінін түсіну үшін кибершабуылдарды бастан өткерген ұйымдар мен жеке тұлғалардың пікірлерін ескеру де маңызды. Тек жүйелі талдау және стратегияларды түзету арқылы киберқауіптерге қарсы күресте тұрақты жақсартуларға қол жеткізуге болады [126].

Технологиялық жетістіктер біздің киберқылмыспен күресуге айтарлықтай әсер етеді. Бір жағынан, жаңа технологиялардың дамуы киберқылмыскерлерге қосымша мүмкіндіктер туғызады, олардың құралдары мен әдістері арсеналын арттырады. Екінші жағынан, дәл сол технологиялар құқық қорғау органдарына қылмыстық құқық бұзушылықты анықтау, тергеу және алдын алудың жетілдірілген құралдарымен қамтамасыз етеді. Заманауи мониторинг және деректерді талдау жүйелері, жасанды интеллект пен машиналық оқытуды пайдалану күдікті әрекеттерді жылдам анықтауға және ықтимал қауіптерді болжауға мүмкіндік береді. Сонымен қатар, технологиялық инновациялар шифрлау жүйелері, желіаралық қалқандар және антивирустық бағдарламалар

сияқты киберқауіпсіздік құралдарын жақсартуда. Бұл құралдарды үнемі жаңартып, жаңа міндеттерге бейімдеу ақпараттық қауіпсіздіктің жоғары деңгейін сақтаудың негізгі факторы болып табылады [127].

Төмендегі 4-кесте киберқылмыспен күресудің негізгі тәсілдері мен әдістерін, қылмыстық құқық бұзушылықты ашуда технологияларды пайдалануды, мемлекеттік шараларды, халықаралық ынтымақтастықты және қолданыстағы шаралардың тиімділігін бағалауды көрсетеді. Бұл ақпараттық қауіпсіздікті қамтамасыз етуге және киберқауіптерге қарсы тұруға бағытталған іс-әрекеттердің күрделілігі мен жан-жақтылығын елестетуге мүмкіндік береді.

Кесте 4 – Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықпен күрестің негізгі аспектілері

Санат	Сипаттама
Негізгі тәсілдер мен әдістер	*Дәстүрлі әдістер:* Алдын алу, тәртіпті сақтау, халықтың хабардарлығын арттыру. *Қазіргі заманғы әдістер:* Киберпатрульдеу, кибергигиена.
Технологияны қолдану	Мониторинг және деректерді талдау жүйелерін қолдану, киберқылмыстарды анықтау және алдын алу үшін жасанды интеллект пен машиналық оқытуды пайдалану.
Үкімет шаралары	*Ұлттық стратегиялар:* Киберқауіпсіздік бағдарламалары, заңнамалық бастамалар. *Құқық қорғау органдарының рөлі:* Мамандандырылған бөлімшелер, жедел шаралар.
Халықаралық ынтымақтастық	*Үйлестірудің маңыздылығы:* Ақпарат алмасу, бірлескен әрекеттер. *Халықаралық келісімдер:* Шарттар мен конвенциялар, жаһандық операциялар.
Іс-шаралардың тиімділігі	*Тиімділікті бағалау:* Статистикалық мәліметтер, тәжірибелік нәтижелерді талдау. *Технологияның әсері:* жаңа қауіптерге бейімделу, қорғанысты жақсарту.

3.1-бөлім шеңберінде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықпен күрестің негізгі аспектілері қарастырылды. Киберқылмыстардың алдын алу және шешу үшін қолданылатын негізгі тәсілдер мен әдістер, соның ішінде дәстүрлі және заманауи әдістер көрсетілген. Құқық қорғау қызметінің тиімділігін айтарлықтай арттыратын технологиялардың рөліне ерекше назар аударылады.

Киберқауіпсіздікті нығайтуда ұлттық саясат пен бағдарламалар, сондай-ақ мамандандырылған құқық қорғау бөлімшелерінің рөлі сияқты үкімет саясаты маңызды рөл атқарады. Халықаралық келісімдермен және бірлескен

операциялармен қолдау көрсетілетін халықаралық ынтымақтастық пен үйлестіру киберқауіптерге қарсы жаһандық күрестің ажырамас элементтері болып табылады.

Қолданыстағы шаралардың тиімділігін бағалау және оларды тез өзгеретін технологиялық ландшафтқа бейімдеу ақпараттандыру және байланыс саласындағы жаңа сын-қатерлер мен қауіптерге тиімді әрекет етуге мүмкіндік береді. Сайып келгенде, барлық деңгейдегі ынтымақтастықты, озық технологияларды пайдалануды және күресу стратегиялары мен әдістерін үздіксіз жетілдіруді қамтитын кешенді тәсіл киберқылмыспен сәтті күресудің негізі болып табылады.

3.2 Қазақстан Республикасының ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық жасаудың себептері мен жағдайлары, қылмыскер тұлғасы

3.2-бөлім Қазақстан Республикасындағы ақпараттандыру және байланыс саласында қылмыстық құқық бұзушылықтар жасауға ықпал ететін себептер мен жағдайларды егжей-тегжейлі талдауға арналған. Осы факторларды түсіну киберқылмыстың алдын алу және онымен күресу бойынша тиімді шараларды әзірлеудің кілті болып табылады. Бұл бөлімде қылмыскерлердің ынтасы мен мінез-құлқына әсер ететін әртүрлі аспектілер қарастырылады. Ең алдымен қылмыстық ниеттің пайда болуына қолайлы жағдай тудыруы мүмкін әлеуметтік-экономикалық жағдайлар, білім деңгейі және мәдени орта сияқты әлеуметтік факторлар. Экономикалық факторлар да маңызды, оның ішінде қаржылық мотивтер, заңсыз баю мүмкіндіктері, жұмыссыздық пен экономикалық тұрақсыздықтың қылмыстық әрекетке әсері.

Сонымен қатар, психологиялық факторлар, соның ішінде киберқылмыскерлердің тұлғалық ерекшеліктері мен мотивациялары талданады. Бұл тұрғыда типтік қылмыскерлердің психологиялық портреттері маңызды болып табылады, бұл олардың мінез-құлқын және қылмыстық құқық бұзушылық жасау себептерін жақсы түсінуге көмектеседі. Қылмыскерлердің жасы мен жынысы, білім деңгейі мен кәсіби дағдылары сияқты спецификалық сипаттамалары да ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықты әрекетті қалыптастыруда маңызды рөл атқарады.

Қазақстандағы киберқылмыстың себептері мен жағдайларын кешенді зерттеуге бағытталған , ол қылмыстық әрекетке әсер ететін негізгі факторларды анықтап қана қоймай, оның алдын алудың тиімді стратегиялары мен шараларын әзірлеуге мүмкіндік береді.

Сонымен, қылмыскерлерді ынталандыруға әлеуметтік-экономикалық жағдайлардың әсері айтарлықтай. Экономикалық тұрақсыздық пен жоғары жұмыссыздық кезінде адамдар ақша табудың жылдам әрі оңай жолын іздеп

қылмысқа бет бұруы мүмкін. Қаржы ресурстарының жетіспеушілігі, өмір сүру деңгейінің төмендігі және әлеуметтік қауіпсіздік киберқылмыстың дамуына қолайлы жағдай жасайды. Мұндай жағдайларда қылмыскерлер көбінесе киберқылмысты қаржылық жағдайын жақсартудың жалғыз жолы ретінде қарастырады. Бұл әсіресе техникалық дағдылары бар, оларды онлайн режимінде заңсыз әрекеттер үшін пайдалана алатын жастарға қатысты.

Киберқылмыскерлердің мотивациясын қалыптастыруда білім мен мәдени ортаның рөлі де маңызды рөл атқарады. Сапалы білімнің болмауы және цифрлық сауаттылықтың төмен деңгейі киберқылмысқа қатысуға ықпал етуі мүмкін. Мәдени сипаттамалар мен әлеуметтік нормалар киберқылмыстың заңдылығы мен моральдық қолайлылығын қабылдауға әсер ететінін атап өткен жөн. Құқықтық мәдениет пен заңды құрметтеу жеткіліксіз дамыған қоғамдарда қылмыстық әрекетке тартылу ықтималдығы артады. Сондай-ақ киберқылмыстың қауіптері мен салдары туралы хабардарлықты арттыруға бағытталған білім беру ресурстары мен бағдарламаларына қолжетімділік маңызды фактор болып табылады.

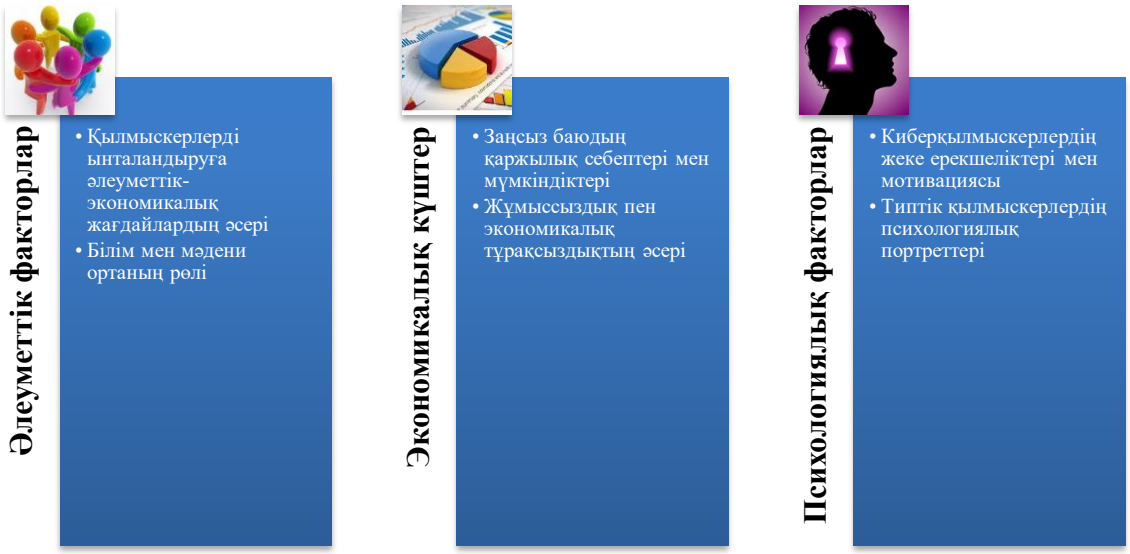
Қаржылық мотивтер мен заңсыз баю мүмкіндіктері көбінесе киберқылмыскерлердің негізгі қозғаушы күштері болып табылады. Киберкеңістікте заңсыз байлыққа қол жеткізудің көптеген жолдары бар, мысалы, деректерді ұрлау, банк жүйелерін бұзу, зиянды бағдарламаларды тарату және бопсалау. Бұл әрекеттер салыстырмалы түрде төмен шығындармен және ұсталудың ең аз қаупімен айтарлықтай табыс әкеле алады, бұл киберқылмысты тез байып кеткісі келетін адамдар үшін тартымды етеді. Қылмыскерлер өз әрекеттерін жасыру және жауапкершіліктен жалтару үшін интернеттің анонимділігі мен трансұлттық сипатын жиі пайдаланады.

Жұмыссыздық деңгейі мен экономикалық тұрақсыздықтың әсері де киберқылмыстардың өсуінде маңызды рөл атқарады. Жұмыссыздықтың жоғары деңгейі, әсіресе жастар арасында, үмітсіздік пен келешектің жоқтығы сезімін тудырады , бұл адамдарды ақша табудың балама, оның ішінде заңсыз жолдарын іздеуге итермелейді. Экономикалық тұрақсыздық пен экономикадағы дағдарыстар негізгі қажеттіліктерін қамтамасыз ету үшін қылмыстық құқық бұзушылық жасауға дайын адамдар санының артуына ықпал етуі мүмкін. Мұндай жағдайларда киберқылмыс өмір сүру тәсілі ғана емес, жалпы экономикалық құлдырау жағдайында қаржылық тұрақтылыққа қол жеткізу құралына айналады.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды жасауда киберқылмыскерлердің жеке ерекшеліктері мен мотивациялары басты рөл атқарады. Көптеген киберқылмыскерлердің интеллектінің жоғары деңгейі, техникалық сауаттылығы және қораптан тыс ойлау қабілеті бар. Олар жиі қиындықтар мен қиын мәселелерді жеңудің қанағаттануын іздейді. Кейбір қылмыскерлер үшін өзін-өзі жүзеге асыру және кішігірім топтарда тану маңызды, ал басқалары қаржылық пайдаға ұмтылу немесе билік пен бақылауға ұмтылумен байланысты болуы мүмкін. Мотивация әділетсіздік сезімі немесе қорлау үшін кек алу және өзіне назар аударту ниеті сияқты жеке

сенімдерді де қамтуы мүмкін [128].

Типтік киберқылмыскерлердің психологиялық профильдері әдетте қоғамға жат мінез-құлық, эмпатияның болмауы және жазаланбау сезімі сияқты жалпы қасиеттерді қамтиды. Олардың көпшілігі басқаларға зиян келтіруден қанағат алады және артықшылық пен бақылау сезімін сезінеді. Типтік киберқылмыскер оқшауланууға және девианттық тенденциялардың дамуына ықпал ететін шынайыдан гөрі виртуалды өзара әрекеттесуді ұнататын интроверт болуы мүмкін. Көбінесе мұндай құқық бұзушылардың әлеуметтік бейімделу мәселелері бар және тұлғааралық қарым-қатынас орнатуда қиындықтар туындауы мүмкін. Осы психологиялық факторларды түсіну киберқылмыскерлердің алдын алу мен оңалтудың тиімді әдістерін әзірлеу үшін маңызды.



Сурет 6 – Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың жасалуына әсер ететін факторлар

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды жасауға ықпал ететін күрделі себептер мен жағдайларды түсіну үшін факторлардың үш негізгі тобын қарастыру қажет: әлеуметтік, экономикалық және психологиялық. Осы факторлар тобының әрқайсысы қылмыскерлерді ынталандыруға және олардың мінез-құлқына айтарлықтай әсер етеді. Бұл диаграмма осы факторлармен байланысты негізгі аспектілерді ұсынады, бұл олардың қылмыстық ниеттер мен әрекеттерді қалыптастырудағы рөлін тереңірек түсінуге мүмкіндік береді.

Әлеуметтік факторларды талдау қылмыскерлердің мотивациясын қалыптастыруда білім деңгейі, мәдени орта және жалпы әлеуметтік орта сияқты әлеуметтік-экономикалық жағдайлардың маңызды рөл атқаратынын көрсетті. Білім беру мүмкіндіктерінің жоқтығы және қоғамның кері әсері киберқылмыс жасауға бейім адамдар санының артуына ықпал етуі мүмкін.

Қылмыскерлерді ынталандыруға экономикалық факторлар да айтарлықтай әсер етеді. Қаржылық қиындықтар, жоғары жұмыссыздық және экономикалық тұрақсыздық заңсыз баюға ұмтылуға негіз жасайды. Экономикалық белгісіздік кезінде адамдар табыс табудың жылдам және оңай жолдарын іздеу үшін қылмыстық әрекетке бет бұруы мүмкін, бұл әсіресе әлеуетті сыйақылар айтарлықтай болуы мүмкін киберқылмысқа қатысты.

Киберқылмыскерлердің тұлғалық ерекшеліктері мен мотивациясы сияқты психологиялық факторлар да маңызды. Тәуекелге, манипуляцияға және техникалық дағдыларға бейім адамдар ақпараттандыру және байланыс саласында қылмыскерге айналуы ықтимал. Типтік қылмыскерлердің психологиялық портреттері олардың жиі интеллектінің жоғары деңгейіне ие екенін көрсетеді, бірақ әлеуметтік бейімделу мен моральдық стандарттарда мәселелер болуы мүмкін.

Осылайша, әлеуметтік, экономикалық және психологиялық факторларды кешенді талдау ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды жасауға ықпал ететін себептер мен жағдайларды жақсы түсінуге мүмкіндік береді. Бұл түсіністік Қазақстан Республикасындағы киберқылмыс деңгейін төмендетуге және ақпараттық қауіпсіздікті арттыруға бағытталған тиімді стратегиялар мен алдын алу шараларын әзірлеу үшін қажет.

Ақпараттандыру және байланыс саласындағы қылмыскерлердің жас және жыныстық ерекшеліктері олардың профильдерін түсіну үшін маңызды аспект болып табылады. Зерттеулер көрсеткендей, киберқылмыскерлердің көпшілігі 18 бен 35 жас аралығындағы жастар. Жастар киберқылмысқа ең алдымен технологиялық сауаттылығы мен тәуекелге бел буғандықтан тартылады. Гендер де маңызды: IT секторына әйелдердің қатысуының артуына қарамастан, киберқылмыскерлердің басым көпшілігі ер адамдар. Бұл әлеуметтік және мәдени факторларға, сондай-ақ адамдардың технологиядағы тарихи рөлдеріне байланысты болуы мүмкін [129].

Қылмыскерлердің ақпараттандыру және байланыс саласындағы білімі мен кәсіби дағдылары олардың қызметінде басты рөл атқарады. Қылмыскерлер көбінесе, әсіресе ақпараттық технологиялар, информатика және инженерия саласында білім деңгейі жоғары. Мұндай білім мен дағдылар оларға күрделі шабуыл үлгілерін жасауға және қауіпсіздік жүйелерін айналып өтуге мүмкіндік береді. Бағдарламалау, желіні басқару және киберқауіпсіздік техникасын білу сияқты кәсіби дағдылар қылмыскерлер өздерінің қылмыстық әрекеттерін жүзеге асыру үшін қолданатын негізгі құралдар болып табылады. Олардың көпшілігінің IT компанияларында немесе киберқауіпсіздік саласында жұмыс тәжірибесі бар, бұл оларға қылмыстық құқық бұзушылық жасауға қажетті білім мен ресурстарға қол жеткізуге мүмкіндік береді.

Осылайша, жас және жыныс ерекшеліктері, сондай-ақ жоғары білім деңгейі мен кәсіби дағдылар киберқылмыскерлердің маңызды сипаттамалары болып табылады. Осы аспектілерді түсіну бізге киберқылмыстың алдын алу және онымен

күресу, сондай-ақ цифрлық кеңістіктегі қауіпсіздік деңгейін арттыру бойынша дәлірек және тиімді шараларды әзірлеуге мүмкіндік береді.

«Қазақстан Республикасының ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық жасаудың себептері мен жағдайлары, қылмыскердің жеке басы» 3.2-бөлімінде елдегі киберқылмыстардың пайда болуына және дамуына әсер ететін күрделі факторлар қарастырылған. Қылмыскерлерді ынталандыруда, олардың жеке қасиеттері мен кәсіби дағдыларын қалыптастыруда әлеуметтік, экономикалық және психологиялық аспектілер басты рөл атқарады [130].

Әлеуметтік-экономикалық жағдайлар, мысалы, өмір сүру деңгейі, білімге қол жетімділік және мәдени орта қылмыскерлердің мотивациясына айтарлықтай әсер етеді. Экономикалық тұрақсыздық пен жоғары жұмыссыздық кезінде адамдар ақша табудың заңсыз жолдарын іздеуі мүмкін, бұл киберқылмыстардың өсуіне ықпал етеді. Білім және мәдени орта да ақпараттық технологияларды заңды және заңсыз мақсаттарда түсіну және пайдалану үшін негіз болып табылады.

Экономикалық факторлар, оның ішінде қаржылық мотивтер мен заңсыз баю мүмкіндіктері қылмыс жасауға күшті ынталандыру болып табылады. Жылдам және айтарлықтай қаржылық пайда табу адамдарды киберқылмыс жасауға итермелейді, әсіресе экономикалық тұрақсыздық кезінде. Жұмыссыздықтың жоғары деңгейі бұл тенденцияны күшейтіп, қылмыстық әрекеттер жасауға дайын адамдар санын көбейтеді.

Киберқылмыскерлер профилін қалыптастыруда тұлғалық сипаттамалар мен мотивация сияқты психологиялық факторлар маңызды рөл атқарады. Типтік қылмыскерлердің психологиялық портреттері олардың ішкі мотивтері мен заңсыз әрекеттерге бейімділігін түсінуге көмектеседі. Тәуекелге бару, жоғары интеллект және технологияны меңгеру сияқты жеке қасиеттер көбінесе киберқылмыскерлермен байланысты.

Құқық бұзушылардың жасы мен жынысын қоса алғанда, ерекше сипаттамалары, сондай-ақ білім деңгейі мен кәсіби дағдылары жалпы көріністі толықтырады. Киберқылмыскерлердің көпшілігі – білімі жоғары және IT саласындағы маңызды дағдылары бар жас жігіттер. Бұл сипаттамалар оларға қылмысты сәтті жасауға және ашылмауға көмектеседі.

Тұтастай алғанда, киберқылмыстың себептері мен жағдайларын, сондай-ақ кінәлілердің тұлғалық ерекшеліктерін түсіну киберқылмыспен күресудің тиімді стратегияларын әзірлеудің кілті болып табылады. Әлеуметтік, экономикалық және психологиялық аспектілерді қамтитын кешенді тәсіл киберқылмыстың алдын алу және онымен күресу бойынша неғұрлым дәл және тиімді шараларды жасауға мүмкіндік береді, бұл өз кезегінде Қазақстан Республикасында ақпараттық қауіпсіздік деңгейін арттыруға ықпал етеді.

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық жасайтын қылмыскер тұлғасының әлеуметтік портреті әртүрлі сипаттамалар мен белгілерді қамтиды. Негізгі аспектілеріне:

- Жас мөлшері: 18-35 жасындағы адамдар.
- Техникалық дағдылар: Киберқылмыскерлер әдетте техникалық білім мен бағдарламалау дағдыларының жоғары деңгейіне ие. Олар өз білімдерін зиянды бағдарламаларды, бұзу жүйелерін және басқа кибершабуылдарды жасау үшін пайдалана алады.
- Мотивация: Киберқылмыскерлердің мотивтері қаржылық пайдадан саяси немесе идеологиялық себептерге дейін болады. Кейбір киберқылмыскерлер жеке дұшпандықтан немесе назар аударту ниетінен әрекет етеді.
- Әлеуметтік байланыстар: Киберқылмыскерлер көбінесе жәбірленушілермен және әріптестермен тікелей байланысқа түспей, көлеңкеде әрекет етеді. Олар өздерінің жеке басын жасыру үшін анонимді желілер мен бүркеншік аттарды пайдаланады.
- Психологиялық қасиеттер: Кейбір киберқылмыскерлер кінәнің болмауы, эмоционалды салқындық және манипуляциялық бейімділік сияқты қоғамға қарсы бұзылу белгілерін көрсетеді.
- Қоршаған орта және білім: киберқылмыскерлердің білімі мен шығу тегі әртүрлі болады. Олар студенттер, ақпараттық технология саласындағы мамандары немесе арнайы білімі жоқ хакерлік дағдыларды өз бетімен үйренген адамдар болып табылады.

Қазақстан Республикасының ақпараттандыру және байланыс саласындағы қылмыстық құқықбұзушылықтарға қарсы іс-қимылдың криминологиялық сипаттамасын толық түсіну үшін қосымша аспектілерді қарастыру қажет [131].

Технологиялық дамудың қылмысқа ықпалы

Қазіргі уақытта Қазақстанда киберқылмыс деңгейінің өсуі технологиялық дамудың жылдамдығымен тығыз байланысты. Жоғары жылдамдықтағы интернеттің қолжетімділігі, цифрлық технологиялардың дамуы және ақпараттық-коммуникациялық құралдардың кеңінен таралуы құқықбұзушылықтарға жаңа мүмкіндіктер берді. Бұл факторлар, әсіресе халықтың цифрлық сауаттылығы төмен деңгейде болғанда, қылмыскерлер үшін тиімді құралдарға айналады.

Технологиялық дамудың екі негізгі бағыты киберқылмыстардың көбеюіне ықпал етеді:

1. Цифрлық құралдардың кең таралуы: Әлеуметтік желілер, интернет-банкинг жүйелері, онлайн-сауда платформалары, бұлтты қызметтер секілді цифрлық құралдардың кеңінен қолданылуы ақпараттық қауіпсіздікке қауіп төндіретін жаңа алаңдар пайда болуына алып келеді. Мұндай құралдар қылмыскерлерге жеке ақпаратты ұрлауға, алаяқтық жасауға және зиянды бағдарламаларды таратуға мүмкіндік береді.
2. Интернеттегі анонимдік: Интернеттегі анонимдік қылмыскерлерге құқық қорғау органдарынан жасырыну мүмкіндігін береді. Бұл жағдай оларды жауапкершіліктен жалтаруға ынталандырады, себебі көптеген қылмыстық құқық бұзушылықтарды ізін суытпай тергеу қиынға соғады. Интернеттегі анонимдік, әсіресе, қара нарықтық операциялар, кибералаяқтық және хакерлік шабуылдар

үшін тиімді құралға айналған.

Білім және мәдени факторлар

Қазақстанда киберқылмыстардың дамуына білім беру жүйесі мен жалпы мәдени орта да әсер етуде. Цифрлық сауаттылықтың төмен деңгейі және ақпараттық қауіпсіздік туралы хабардарлықтың жеткіліксіздігі халықтың қорғаныссыздығын арттырады. Көптеген адамдар өздерінің жеке мәліметтерін қалай қорғау керектігі туралы түсініктері жоқ немесе жеткілікті деңгейде ақпараттандырылмаған.

Мәдени факторлар да маңызды рөл атқарады. Қазақстан қоғамында заң бұзушылыққа немқұрайлы қарау немесе оның мәнін жеткілікті түрде түсінбеу қылмыскерлерді заңды айналып өтуге итермелеуі мүмкін. Бұл қылмыстық құқық бұзушылықтардың кейбір түрлері, мысалы, авторлық құқықты бұзу немесе интернеттегі пираттық материалдарды тарату, кейбіреулер үшін «қылмыс» ретінде қарастырылмауы мүмкін, сондықтан мұндай әрекеттер қоғамда жиі кездеседі [132].

Қылмыскерлердің әлеуметтік-психологиялық ерекшеліктері

Киберқылмыс жасаушылардың көпшілігі жоғары деңгейдегі интеллектке ие және техникалық тұрғыдан сауатты адамдар болып келеді. Олар көбінесе IT саласындағы мамандар немесе хакерлік дағдыларды өз бетімен үйренген адамдар болып табылады. Осы факторларға байланысты олар қоғамдағы әдеттегі қылмыскерлерден ерекшеленеді, себебі олардың қылмыстық әрекеттері интеллектуалды сипатта болады.

Қылмыскерлердің көпшілігінің ортақ мінез-құлқы олардың қылмыстық әрекетке қатысуының психологиялық себептерін түсінуге көмектеседі. Бұл қылмыскерлер, әдетте:

- Қоғамға қарсы шығуға бейім болады;
- Жасалған қылмыстық құқық бұзушылықтың ықтимал салдарлары туралы ойланбайды;
- Өздерін жазадан қорғалған сезінеді.

Сонымен қатар, қылмыскерлердің жас ерекшеліктері де маңызды. Зерттеулер көрсеткендей, киберқылмыстардың көпшілігі 18-35 жас аралығындағы адамдармен жасалады. Бұл адамдардың ақпараттық технологиялар саласында білімдері жоғары және интернетте жұмыс істеу дағдылары жақсы дамыған.

Жағдайға әсер ететін қосымша факторлар

Қазақстан Республикасында ақпараттық қауіпсіздік пен деректерді қорғаудың жеткіліксіз деңгейі киберқылмыскерлерге жаңа мүмкіндіктер береді. Компаниялар мен мемлекеттік органдардың киберқауіпсіздікке жеткілікті назар аудармауы, тиісті техникалық құралдардың жоқтығы және ақпараттық қауіпсіздік саясаттарының жеткіліксіздігі қылмыскерлердің шабуылдарын жеңілдетеді.

Бұл жағдайлар қылмыскерлерге ақпараттық жүйелерге рұқсатсыз қол жеткізу және оларды бұзу арқылы қаржылық пайда табуға мүмкіндік береді. Мысалы, банктердегі немесе басқа қаржылық ұйымдардағы ақпараттық жүйелердің

қорғалмағандығы қылмыскерлерге осындай ұйымдардың ішкі жүйелеріне шабуыл жасау арқылы қаржылық алаяқтық жасауды жеңілдетеді [133].

Ақпараттық жүйелердің осал тұстарын пайдалану

Қазақстанда ақпараттық жүйелерді қорғау бойынша заманауи техникалық шешімдердің болмауы көптеген мекемелерді киберқылмыскерлердің мақсаттарына айналдырады. Ақпараттық қауіпсіздікке жеткілікті көңіл бөлмеу нәтижесінде хакерлер осы осал тұстарды пайдаланып, мекемелерге шабуыл жасайды. Мұндай шабуылдар көбінесе қаржылық алаяқтық, деректерді ұрлау, жүйелерді бұзу және маңызды ақпаратты жою сияқты әрекеттерге әкеледі.

Қорытындылай келе, Қазақстан Республикасында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың себептері мен жағдайларын толық түсіну үшін әлеуметтік, экономикалық, мәдени және психологиялық факторларды жан-жақты талдау қажет. Бұл қылмыстық құқық бұзушылықты тиімді алдын алу және олардың зардаптарын азайту үшін кешенді шаралар қолдану керек.

3.3 Ақпараттандыру және байланыс саласында жасалатын қылмыстық құқық бұзушылықтармен күресудің шетелдік тәжірибесі

Ақпараттандыру және байланыс саласында жасалған қылмыстық құқық бұзушылықтар саласындағы шетелдік тәжірибені талдау жаһандық киберқауіпсіздік мәселеріне жауап ретінде бейімделуі немесе ұлттық құқықтық жүйелерге енгізілуі мүмкін халықаралық трендтер мен тәсілдерді түсіну үшін қажет. Әртүрлі елдердің заңнамасын салыстырмалы талдау киберқылмыспен байланысты қауіптерге барабар жауап бере алатын құқықтық реттеудің неғұрлым тиімді стратегиялары мен тетіктерін анықтауға мүмкіндік береді.

Ақпараттық технологиялар шекараны білмейді, бұл киберқылмысты халықаралық деңгейде үйлестірілген күш-жігерді қажет ететін трансұлттық құбылысқа айналдырады. Шетелдік тәжірибе көрсеткендей, бұл саладағы қылмыстық құқық бұзушылықпен табысты күресу тек қатаң заңнамалық базаны ғана емес, сонымен қатар мемлекеттік органдардың, жеке сектордың және халықаралық ұйымдардың белсенді ынтымақтастығын қажет етеді. Еуропа, Солтүстік Америка, Азия және басқа аймақтардағы мысалдар деректерді қорғау туралы заңдардан ақпараттық қауіпсіздік инциденттеріне әрекет ету тетіктеріне дейін осы мәселені реттеудің әртүрлі тәсілдерін көрсетеді.

Киберқылмыспен күрес саласындағы шетелдік тәжірибені зерттеу Қазақстан үшін осы бағытта тиімді заңнамалық және ұйымдастырушылық шараларды әзірлеу тұрғысынан маңызды. АҚШ, Еуропалық Одақ, Азия және Ресей мемлекеттеріндегі киберқауіпсіздікті қамтамасыз етудегі тәжірибе ақпараттық қауіпсіздікті нығайтуға бағытталған кешенді тәсілдердің мысалдарын көрсетеді. Әрбір елдің заңнамасы, халықаралық ынтымақтастыққа бағытталған қадамдары

және ұйымдық құрылымдары киберқауіптерге тиімді жауап беру үшін маңызды рөл атқарады.

АҚШ-та киберқылмыспен күресуге бағытталған негізгі заңдардың бірі – 1986 жылы қабылданған Computer Fraud and Abuse Act (CFAA). Бұл заң компьютерлік жүйелерге рұқсатсыз қол жеткізу, деректерді бұзу немесе жою сияқты әрекеттерді қылмыс ретінде қарастырады. Сондай-ақ, АҚШ-та Cybersecurity Information Sharing Act (CISA) заңын қабылдау арқылы мемлекеттік органдар мен жеке сектор арасындағы киберқауіптер туралы ақпарат алмасу тетіктері дамытылды. АҚШ үкіметі бұл салада Federal Bureau of Investigation (FBI) және Department of Homeland Security (DHS) сияқты агенттіктердің рөлін күшейтті. Бұдан бөлек, Cybersecurity and Infrastructure Security Agency (CISA) мемлекеттік және жеке сектордағы маңызды инфрақұрылымдарды қорғауға бағытталған іс-шараларды үйлестіреді. АҚШ тәжірибесінде мемлекеттік және жеке ұйымдар арасындағы серіктестік ерекше маңызға ие. Мысалы, технологиялық корпорациялар (Google, Microsoft, Amazon) өздерінің жүйелерін қорғау үшін озық қауіпсіздік технологияларын енгізіп, кибершабуылдардың алдын алу шараларын жүзеге асырады.

Еуропалық Одақта киберқауіпсіздікті реттеудегі негізгі құжаттардың бірі – General Data Protection Regulation (GDPR). 2018 жылы қабылданған бұл заң жеке деректердің қауіпсіздігін қамтамасыз етуге ерекше назар аударады және деректерді заңсыз пайдаланған ұйымдарға қатаң айыппұлдар қарастырады. Сондай-ақ, Network and Information Security Directive (NIS) ЕО-ға мүше елдерде киберқауіпсіздік стандарттарын күшейтуге бағытталған. ЕО-ның European Cybercrime Centre (EC3) және Europol ұйымдары трансұлттық кибершабуылдармен күресуде жетекші рөл атқарады. Бұл ұйымдар мемлекеттер арасында ақпарат алмасу және бірлескен операцияларды үйлестіру жұмыстарын жүргізеді. ЕО тәжірибесі көрсеткендей, киберқауіптерге қарсы күресте халықаралық ынтымақтастық пен стандарттарды үйлестіру маңызды.

Азия елдерінде де киберқауіпсіздік саласында айтарлықтай шаралар қабылданған. Жапонияда 2014 жылы қабылданған Cybersecurity Basic Act мемлекеттік және жеке сектордағы киберқауіпсіздік шараларын реттейді. Бұл елде National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ұйымы мемлекеттік мекемелерге және бизнеске кибершабуылдардың алдын алу бойынша кеңес береді. Оңтүстік Кореяда қабылданған Cybersecurity Act мемлекеттік және жеке секторларда ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуді міндеттейді. Korea Internet & Security Agency (KISA) бұл елде киберқауіптерге жедел жауап беретін және кибершабуылдарды болдырмауға бағытталған жұмыстарды жүргізеді. Үндістанда 2000 жылы қабылданған Information Technology Act елдегі ақпараттық қылмыстық құқық бұзушылыққа қарсы күреске негіз болды. Бұл заң рұқсатсыз қол жеткізу, деректерді бұзу және интернет арқылы алаяқтық жасау сияқты әрекеттерді қылмыс ретінде қарастырады. Үндістанның Indian Computer Emergency Response Team (CERT-In) агенттігі

киберқауіптерге жедел жауап беру және алдын алу жұмыстарымен айналысады.

Ресейде де киберқылмыспен күрес саласында бірқатар заңнамалық шаралар қабылданған. Ресей Федерациясының Қылмыстық кодексінің 272-бабы рұқсатсыз қол жеткізу және компьютерлік жүйелерге зиян келтіру әрекеттері үшін жауапкершілікті белгілейді. Сонымен қатар, 273-бап компьютерлік вирустарды жасау және тарату үшін қылмыстық жаза қарастырады. Ресейде «Ақпарат, ақпараттық технологиялар және ақпаратты қорғау туралы» заң қабылданып, мемлекеттік және жеке секторлардағы ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуге бағытталған шаралар жүйеленді. Елдің Федералдық қауіпсіздік қызметі (ФСБ) және Гостехкомиссиясы ақпараттық инфрақұрылымды қорғау және мемлекеттік мекемелерге қатысты кибершабуылдардың алдын алу шараларымен айналысады.

Шетелдік тәжірибе көрсеткендей, киберқауіпсіздікті қамтамасыз ету үшін заңнамалық базаны үнемі жетілдіру, халықаралық ынтымақтастықты нығайту және мемлекеттік органдар мен жеке секторлар арасындағы серіктестікті дамыту маңызды. Әрбір елдің заңнамалық жүйесі осы саладағы сын-қатерлерге жауап беруге бағытталған, ал халықаралық тәжірибе бұл бағыттағы шаралардың тиімділігін арттыруға мүмкіндік береді. Қазақстан үшін осы тәжірибелерді зерттеу және оларды ұлттық заңнамаға енгізу киберқауіптерге қарсы тиімді күрес шараларын әзірлеу үшін маңызды қадам болып табылады.

Бұл бөлімде заң шығару бастамалары, технологиялық инновациялар, киберқауіпсіздік қатерлері туралы оқыту және хабардар ету бағдарламалары сияқты киберқылмыстың алдын алуға бағытталған шараларға шолу жасалады. Сондай-ақ киберқылмысқа қатысты құқықтық саясатты қалыптастыруға мәдени және саяси сипаттамалардың әсері туралы мәселе қарастырылады.

Киберқылмыспен күресудегі кешенді тәсілдің маңыздылығы және технологиялық аспектілерді де, құқықтық, әлеуметтік және мәдени факторларды да ескеретін икемді киберқауіпсіздік жүйелерін құруға ұмтылу ерекше атап өтіледі. Сайып келгенде, халықаралық тәжірибе ақпарат алмасудың барлық қатысушыларын барабар қорғауды қамтамасыз ететін киберқылмыспен күресудің жаһандық және жергілікті стратегияларын әзірлеуге негіз болуы тиіс.

Ақпарат және байланыс саласында жасалатын қылмыстық құқықбұзушылықтар шетелдік тәжірибеде ерекше назарда және күрделі мәселе болып табылады. Киберқылмыстардың трансұлттық сипаты, оларды жасаудағы технологиялардың жедел дамуы мемлекеттердің ақпараттық қауіпсіздік пен құқықтық реттеу саласында жаңа тәсілдер мен әдістерді қабылдауын талап етеді. Бұл бөлімде шетелдік тәжірибенің негізгі элементтері мен ерекшеліктері талқыланады, оның ішінде халықаралық ынтымақтастықтың маңыздылығы мен киберқылмыстарға қарсы күрестің тиімді стратегиялары қарастырылады.

1. АҚШ-тағы киберқылмыспен күресу тәжірибесі

АҚШ-тағы киберқылмыспен күресу тәжірибесі әлемдегі ең озық және жан-жақты болып табылады. Америка Құрама Штаттары киберқылмыстардың алдын

алу және оларға қарсы шараларды қабылдауда бірқатар құқықтық және технологиялық қадамдар жасап, халықаралық ынтымақтастықты нығайтуға белсенді түрде қатысып келеді. Киберқылмыстардың жедел дамып, әртүрлі бағытта кеңейе түсуіне байланысты АҚШ-тағы тәжірибе құқықтық жүйелерді жетілдіру және киберқауіпсіздік шараларын үнемі жақсартуды талап етеді [134].

АҚШ-та киберқылмыстармен күресудің құқықтық негізі 1986 жылы қабылданған Computer Fraud and Abuse Act (CFAA) заңымен бастау алды. Бұл заң компьютерлік жүйелерге рұқсатсыз қол жеткізу, оларды бұзу және деректерді ұрлау секілді әрекеттер үшін қылмыстық жауапкершілікті белгілейді. CFAA қазіргі уақытта да киберқылмыстық істерде кеңінен қолданылады, әрі компьютерлік жүйелерге заңсыз кіру немесе оларды зақымдау әрекеттеріне қатаң жаза көзделген.

АҚШ-тағы киберқылмыстармен күресуде жетекші рөл атқаратын екі маңызды ұйым бар: Federal Bureau of Investigation (FBI) және Department of Homeland Security (DHS). Бұл екі ұйымның құрылымында киберқауіпсіздікке бағытталған арнайы бөлімдер жұмыс істейді. Мысалы, Cyber Division – FBI аясындағы киберқылмыстарға қатысты істерді зерттейтін және тергейтін бөлімше. Ол хакерлік шабуылдарды, деректердің заңсыз таралуын, интернет алаяқтықтарын және басқа да киберқылмыстық әрекеттерді тергеп, оларға қарсы шаралар қолданумен айналысады. DHS құрамындағы National Cybersecurity and Communications Integration Center (NCCIC) АҚШ-тағы киберқауіпсіздік инциденттерін анықтау және оларға жедел жауап беру орталығы болып табылады. NCCIC мемлекеттік, жеке және қоғамдық секторлар арасында байланыс орнатып, кибершабуылдардың алдын алу және оларды жою бойынша үйлестіру жұмыстарын жүргізеді.

АҚШ-тағы киберқауіпсіздік шараларының тағы бір маңызды аспектісі – Cybersecurity and Infrastructure Security Agency (CISA) агенттігінің қызметі. Бұл агенттік АҚШ-тың маңызды инфрақұрылым нысандарын, оның ішінде энергетика, көлік, қаржы және денсаулық сақтау салаларындағы жүйелерді қорғауға бағытталған. CISA агенттігі кибершабуылдардан туындайтын қатерлердің алдын алу және оларды болдырмау үшін жаңа технологиялар мен қауіпсіздік шараларын енгізумен айналысады.

АҚШ киберқылмыспен күресуде құқықтық шаралар қабылдап қана қоймай, киберқауіпсіздікке қатысты білім беру және ақпараттық-түсіндіру бағдарламаларын жүзеге асырады. Мысалы, Stop.Think.Connect кампаниясы – АҚШ үкіметі мен жеке сектордың бірлескен жобасы болып табылады. Бұл бағдарлама киберқауіпсіздік туралы қоғамның ақпараттылығын арттыру және интернетте қауіпсіз әрекеттерді үйрету мақсатында құрылған.

Халықаралық ынтымақтастық АҚШ-тың киберқылмыспен күресу тәжірибесінде маңызды орын алады. АҚШ киберқылмыстарға қарсы жаһандық деңгейде әрекет ету үшін көптеген халықаралық ұйымдармен тығыз байланыс орнатқан. Соның ішінде INTERPOL, Europol және басқа да халықаралық

қауіпсіздік ұйымдарымен бірлесе отырып, трансұлттық киберқылмыстарға қарсы операциялар жүргізеді. Сонымен қатар, АҚШ үкіметі бірнеше маңызды халықаралық келісімдерге қол қойған, оның ішінде Будапешт конвенциясы ерекше орын алады. Бұл конвенция киберқылмыстарға қарсы халықаралық ынтымақтастықты күшейтуге бағытталған.

АҚШ-тағы киберқылмыспен күресу саласында үкіметтік шаралардан басқа, жеке сектордың да рөлі үлкен. Жеке компаниялар, әсіресе технологиялық компаниялар, киберқауіпсіздікке инвестиция салып, жаңа қорғау технологияларын әзірлейді. Мысалы, Google, Microsoft және Amazon сияқты корпорациялар өздерінің ақпараттық жүйелерін қорғау үшін озық технологияларды қолдана отырып, кибершабуылдарға қарсы күресте жетекші рөл атқарады.

Сонымен қатар, АҚШ үкіметі Ақ үй арқылы киберқауіпсіздік бойынша ұлттық стратегияларды дамытып келеді. 2018 жылы қабылданған National Cyber Strategy құжаты АҚШ-тың киберқауіпсіздік саласындағы мақсаттары мен міндеттерін айқындады. Бұл стратегия елдің маңызды инфрақұрылымын қорғауды күшейтіп, кибершабуылдардың алдын алу шараларын жақсарту және жаңа қауіптерге жедел жауап беру үшін қажетті ресурстарды бөлуге бағытталған.

АҚШ-тағы тағы бір маңызды қадам – Cybersecurity Information Sharing Act (CISA) заңын қабылдау. Бұл заң киберқауіпсіздікке қатысты ақпарат алмасуды күшейтуді көздейді. Ол мемлекеттік органдар мен жеке компаниялар арасындағы ақпараттық қауіпсіздік инциденттері туралы мәліметтермен бөлісу механизмін жақсартуға бағытталған. CISA заңы киберқауіптердің алдын алу үшін ақпарат алмасуды жеңілдетіп, киберқауіпсіздік саласындағы ынтымақтастықты күшейтуге мүмкіндік береді [135].

Қорытындылай келе, АҚШ-тағы киберқылмыспен күрес саласындағы тәжірибе кешенді құқықтық, технологиялық және ұйымдастырушылық шараларға негізделген. Бұл мемлекет киберқауіптерге қарсы әрекет ету үшін заңнамалық базаны жетілдіріп қана қоймай, жаңа технологияларды енгізіп, халықаралық деңгейде ынтымақтастық орнатуға да ерекше мән береді.

2. Еуропалық Одақтағы киберқылмысқа қарсы күрес

Еуропалық Одақ (ЕО) киберқылмыспен күрес саласында бірқатар маңызды шараларды қабылдаған және әлемдік деңгейде алдыңғы қатарда тұрған құқықтық және ұйымдастырушылық механизмдерге ие. Еуропалық Одақтың бұл саладағы негізгі мақсаты – мүше мемлекеттердің ақпараттық қауіпсіздігін қамтамасыз ету және киберқылмыстарға қарсы тиімді күресті ұйымдастыру болып табылады. ЕО-да киберқылмыстардың таралуы тек технологиялық дамудың салдары ғана емес, сонымен қатар құқықтық реттеудің маңыздылығын арттыратын фактор ретінде қарастырылады. Осыған орай, ЕО киберқылмыстарға қарсы кешенді стратегияларды дамытып, киберқауіптерге төтеп беру үшін бірқатар заңнамалық актілер мен институционалдық механизмдер қабылдаған [136].

ЕО-ның негізгі құқықтық құжаты – Будапешт конвенциясы. Бұл құжат 2001 жылы Еуропа Кеңесі тарапынан қабылданған және ол әлемдегі алғашқы

киберқылмыстарға қарсы халықаралық келісім болып табылады. Будапешт конвенциясы Еуропалық Одақтың барлық мүше елдері мен басқа да мемлекеттер үшін үлгі бола алады. Конвенцияда киберқылмыстарды заңды түрде реттеу, олардың алдын алу және қылмыстық жауапкершілікке тарту бойынша нақты ережелер бар. Бұл құжат трансұлттық киберқылмыстармен күресудегі ынтымақтастықты күшейтіп, ЕО елдері арасында киберқылмыстар бойынша ақпарат алмасуды жеңілдетуге бағытталған.

Еуропалық Одақтағы киберқылмысқа қарсы күрестің тағы бір маңызды институты – Europol. Europol құрамында European Cybercrime Centre (EC3) жұмыс істейді, бұл орталық ЕО-дағы киберқылмыстарға қарсы күресте жетекші рөл атқарады. EC3 орталығы кибершабуылдарды анықтау, олардың алдын алу және киберқылмыстық әрекеттерді тергеу бойынша мүше мемлекеттерге қолдау көрсетеді. Орталық интернеттегі алаяқтық, деректерді ұрлау, зияткерлік меншік құқықтарын бұзу және басқа да қылмыстық әрекеттерді тергеуге мамандандырылған. Europol-дың EC3 орталығы мүше мемлекеттердің құқық қорғау органдарымен тығыз байланыста жұмыс істейді, сондай-ақ INTERPOL және басқа да халықаралық ұйымдармен ынтымақтастықта болып, киберқылмыстарға қарсы бірлескен операциялар жүргізеді.

ЕО-да киберқауіпсіздікті қамтамасыз ету үшін қабылданған маңызды заңдардың бірі – Network and Information Security (NIS) Directive. Бұл директива 2016 жылы қабылданып, ЕО елдерінде киберқауіпсіздік стандарттарын күшейтуге бағытталған. NIS директивасы мүше мемлекеттерге маңызды инфрақұрылымдарды қорғауға арналған шараларды әзірлеуге және киберқауіпсіздік инциденттеріне жауап беретін ұлттық органдар құруға міндеттейді. Бұл директиваның басты мақсаты – ақпараттық жүйелер мен желілердің сенімділігін арттыру және кибершабуылдардың алдын алу үшін ұйымдастырушылық және техникалық шаралар енгізу.

ЕО-ның тағы бір маңызды заңнамалық құжаты – General Data Protection Regulation (GDPR). GDPR 2018 жылы күшіне енген және деректерді қорғау саласындағы ең қатаң заңдардың бірі ретінде белгілі. Бұл заң жеке тұлғалардың жеке деректерін қорғауға ерекше көңіл бөледі және деректерді заңсыз пайдаланған немесе сақтаған ұйымдарға айтарлықтай қатаң жазалау шараларын қарастырады. GDPR компаниялар мен ұйымдардан деректерді өңдеу және сақтау кезінде жоғары қауіпсіздік стандарттарын талап етеді. Бұл заң ЕО-дағы деректердің қауіпсіздігін қамтамасыз етуге, жеке деректердің құпиялығын сақтауға және киберқылмыстық әрекеттердің алдын алуға бағытталған.

ЕО-дағы киберқауіпсіздік саясатының тағы бір маңызды аспектісі – ENISA (European Union Agency for Cybersecurity) агенттігінің қызметі. ENISA – киберқауіпсіздік бойынша ЕО-ның негізгі агенттігі, ол мүше мемлекеттерге киберқауіпсіздік стратегияларын әзірлеуге және оларды жүзеге асыруға көмектеседі. Агенттік ақпараттық қауіпсіздік инциденттеріне жедел жауап беру және олардың алдын алу үшін кеңес береді, сондай-ақ ЕО-дағы киберқауіпсіздік

саласындағы ғылыми зерттеулер мен талдауларды ұйымдастырады. ENISA агенттігі киберқауіпсіздік сертификаттау жүйесін құрып, ақпараттық жүйелер мен өнімдердің қауіпсіздігін тексеру бойынша стандарттар әзірлейді.

ЕО-ның киберқылмыспен күрес саласындағы халықаралық ынтымақтастығы да ерекше маңызды рөл атқарады. ЕО халықаралық ұйымдармен, оның ішінде INTERPOL, NATO, Council of Europe және басқа да елдермен бірлесе отырып, киберқауіптерге қарсы бірлескен шаралар қабылдайды. Бұл ынтымақтастық трансұлттық кибершабуылдарды анықтау және олармен күресу мақсатында ақпарат алмасу мен құқық қорғау органдарының іс-қимылдарын үйлестіруді күшейтуді көздейді. ЕО-ның киберқылмыспен күрес саласындағы халықаралық стратегиялары трансұлттық қылмыстық құқық бұзушылықты алдын алу үшін маңызды қадам болып табылады.

Цифрлық біртұтас нарық (Digital Single Market) стратегиясы да ЕО-дағы киберқылмыспен күресуде маңызды рөл атқарады. Бұл стратегия Еуропалық Одақтағы цифрлық экономика мен онлайн-қызметтерді дамытуға арналған, сондай-ақ киберқауіпсіздік стандарттарын жетілдіруге бағытталған. ЕО елдері арасында цифрлық нарықтағы қызметтерге қатысты қауіпсіздік шараларын күшейту және онлайн-бизнестің қауіпсіздігін қамтамасыз ету үшін құқықтық нормалар мен реттеу механизмдерін енгізу осы стратегияның бір бөлігі болып табылады [137].

Сонымен қатар, ЕО-да киберқауіпсіздікке қатысты білім беру және ақпараттандыру саласында да маңызды шаралар қабылданған. ЕО-ның көптеген елдерінде киберқауіпсіздік бойынша арнайы білім беру бағдарламалары ұйымдастырылып, қоғамға интернет қауіпсіздігі туралы ақпарат берілуде. Бұл бағдарламалар интернеттегі қауіп-қатерлер туралы халықты хабардар етіп, олардың киберқауіпсіздік саласында сауаттылығын арттыруға бағытталған.

Қорытындылай келе, Еуропалық Одақ киберқылмыспен күрес саласында кешенді құқықтық, ұйымдастырушылық және технологиялық шаралар қабылдаған. ЕО-дағы киберқылмыспен күрес саласындағы негізгі заңнамалар мен институттар киберқауіптерге жедел жауап беруге, ақпараттық жүйелердің сенімділігін қамтамасыз етуге және трансұлттық қылмыстық құқық бұзушылықтарға қарсы халықаралық ынтымақтастықты нығайтуға бағытталған. ЕО елдері үшін киберқауіпсіздікті қамтамасыз ету тек заңнамалық реттеумен шектелмей, сонымен қатар қоғамды ақпараттандыру, техникалық стандарттарды жетілдіру және халықаралық деңгейде әрекет етуді талап ететін маңызды міндет болып табылады.

3. Азия елдеріндегі киберқылмыспен күрес тәжірибесі

Азия елдеріндегі киберқылмыспен күрес тәжірибесі әр елдің экономикалық және технологиялық даму деңгейіне, құқықтық жүйесіне, сондай-ақ киберқауіпсіздікке деген көзқарасына байланысты ерекшеленеді. Соңғы онжылдықта Азия елдері ақпараттық технологиялардың жедел дамуына байланысты киберқауіптердің күрт өсуін байқады. Осыған орай, аймақтағы

мемлекеттер киберқылмыстарға қарсы заңнамаларды жетілдіріп, қауіпсіздік шараларын күшейтуге бағытталған ұлттық және халықаралық деңгейдегі бастамалар қабылдады. Бұл тәжірибелер әр елде түрлі жолмен жүзеге асуда, дегенмен барлық елдерге ортақ міндет – ақпараттық инфрақұрылымды қорғау және киберқылмыстардың алдын алу.

Жапониядағы киберқылмыспен күрес тәжірибесі

Жапония киберқауіпсіздік саласында көшбасшы елдердің бірі болып табылады және бұл елде киберқауіптерге қарсы құқықтық және технологиялық шаралар кеңінен дамыған. Жапонияда 2014 жылы Cybersecurity Basic Act заңы қабылданды, ол елдегі киберқауіпсіздік саясатының негізін құрады. Бұл заң киберқауіптерге жауап беру үшін мемлекеттік және жеке сектордағы жауапкершіліктерді анықтап, кибершабуылдарға қарсы тұру мақсатында түрлі шаралар қабылдауды міндеттейді.

Жапонияда киберқауіпсіздікті қамтамасыз етуге арналған National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ұйымы жұмыс істейді. Бұл орталық мемлекеттік органдар мен жеке компанияларға киберқауіптерден қорғануға көмектесіп, кибершабуылдарға қарсы әрекет етеді. Сонымен қатар, Жапониядағы Cybersecurity Strategy Headquarters сияқты құрылымдар ұлттық деңгейде киберқауіпсіздік саясатын әзірлеумен айналысады. Бұл орталықтар киберқылмыстардың алдын алу шараларын жетілдіріп, жаңа технологияларды қолдану арқылы ақпараттық жүйелерді қорғауға баса назар аударады [138].

Жапония киберқауіпсіздік саласында халықаралық ынтымақтастыққа үлкен мән береді. Ел халықаралық деңгейде INTERPOL, Europol, және ASEAN ұйымдарымен тығыз байланыс орнатып, киберқауіптерге қарсы ортақ шаралар қабылдайды. Жапония үкіметі киберқауіптерді болдырмау үшін жаһандық серіктестіктер арқылы ақпарат алмасуды жетілдіру мақсатында түрлі келісімдерге қол қойған.

Оңтүстік Кореядағы киберқылмыспен күрес тәжірибесі

Оңтүстік Корея да киберқауіпсіздік саласында көшбасшы елдердің бірі болып табылады. Елдің цифрлық экономикасы мен жоғары технологиялық инфрақұрылымының дамуы Оңтүстік Кореяның киберқауіпсіздік мәселелеріне ерекше назар аударуына себеп болды. Кореяда 2015 жылы Cybersecurity Act заңы қабылданып, ол ақпараттық жүйелер мен желілердің қауіпсіздігін қамтамасыз ету бойынша құқықтық нормаларды бекітті. Бұл заң жеке және мемлекеттік секторларда киберқауіптерге қарсы қауіпсіздік шараларын күшейтуді талап етеді.

Оңтүстік Кореяда Korea Internet & Security Agency (KISA) жұмыс істейді, ол елдегі киберқауіптерге жауап беру және оларды болдырмау бойынша басты агенттік болып табылады. KISA түрлі кибершабуылдарға қарсы зерттеулер жүргізіп, ақпараттық жүйелерді қорғау үшін жаңа технологиялар мен қауіпсіздік жүйелерін әзірлейді. Бұл агенттік сондай-ақ K-CERT/CC (Korea Computer Emergency Response Team/Coordination Center) сияқты орталықтар арқылы кибершабуылдарға жедел әрекет ету және олардың алдын алу бойынша жұмыстар

атқарады [139].

Оңтүстік Кореядағы киберқауіпсіздік мәселесі тек ұлттық деңгейде ғана емес, халықаралық ынтымақтастықты қажет етеді. Корея үкіметі INTERPOL, APEC, және ASEAN ұйымдарымен серіктестік орнатып, трансұлттық киберқылмыстарға қарсы бірлескен шараларды жүзеге асырады. Сонымен қатар, Корея үкіметі киберқауіптер туралы ақпарат алмасуды күшейту мақсатында жаһандық деңгейде келісімдерге қол қойып, халықаралық деңгейде қауіпсіздік шараларын жетілдіруді көздейді.

Қытайдағы киберқылмыспен күрес тәжірибесі

Қытай киберқауіпсіздік саласында қатаң бақылау мен реттеуді жүзеге асыратын мемлекеттердің бірі болып табылады. Қытай үкіметі ақпараттық қауіпсіздікке қатысты қатал заңдар мен ережелер қабылдап, елдегі интернет пен ақпараттық жүйелерді қатаң бақылауда ұстайды. 2017 жылы Қытайда Cybersecurity Law қабылданды, ол ақпараттық жүйелерді қорғауға және жеке деректердің қауіпсіздігін қамтамасыз етуге бағытталған. Бұл заң мемлекеттік органдарға ақпараттық инфрақұрылымды қатаң бақылауға алуға және елдегі интернет пайдаланушылардың іс-әрекеттерін реттеуге мүмкіндік береді.

Қытайдағы киберқауіпсіздікке жауап беретін негізгі ұйымдардың бірі – Cyberspace Administration of China (CAC). Бұл агенттік елдегі интернет жүйелерін бақылайды, киберқауіптерге жауап беру шараларын ұйымдастырады және интернетті реттеу бойынша ережелерді әзірлейді. Қытай үкіметі киберқылмыстарға қарсы тұру мақсатында ақпараттық қауіпсіздікті күшейтіп, елдегі интернетке қатысты қатаң шаралар қабылдаған. Соның ішінде шетелдік компаниялар мен сервистердің Қытайда жұмыс істеуі үшін арнайы талаптар енгізіліп, деректердің ел ішінде сақталуы және өңделуі міндеттелген.

Қытайда интернет қолданушыларының іс-әрекеттерін қадағалау күшейтіліп, үкімет киберқауіптерді болдырмау үшін ұлттық қауіпсіздік шараларын күшейтуге бағытталған. Сонымен қатар, Қытайдың Ұлы Брандмауэр деп аталатын интернет сүзгісі арқылы елдегі интернет ресурстары мен желілердің сыртқы әсерден қорғалуы қамтамасыз етіледі.

Үндістандағы киберқылмыспен күрес тәжірибесі

Үндістан киберқылмыспен күрес саласында соңғы жылдары айтарлықтай жетістіктерге жетті. Елдегі интернет пайдаланушылардың санының артуы және цифрлық технологиялардың дамуы киберқауіптерге қарсы күрестің өзектілігін арттырды. 2000 жылы Үндістанда Information Technology Act қабылданды, ол интернет және ақпараттық жүйелер арқылы жасалатын қылмыстық құқық бұзушылықтарға қатысты заңнамалық нормаларды бекітті. Бұл заң ақпараттық жүйелерге рұқсатсыз қол жеткізу, деректерді ұрлау және интернет арқылы алаяқтық жасау секілді қылмыстық құқық бұзушылықтарға жауапкершілік көздейді [140].

Үндістандағы киберқауіпсіздікті қамтамасыз етуге арналған Indian Computer Emergency Response Team (CERT-In) басты агенттік болып табылады. CERT-In

киберқауіптерге жауап беру, олардың алдын алу және зерттеу жұмыстарымен айналысады. Сонымен қатар, агенттік интернет қолданушыларына киберқауіптерден қорғану бойынша нұсқаулықтар береді және ақпараттық қауіпсіздікке қатысты ұлттық саясатты әзірлеуге қатысады.

Үндістандағы киберқауіпсіздік саясаты Digital India бастамасы аясында дамытылып келеді. Бұл бастама елдің цифрлық инфрақұрылымын жетілдіруді және интернетке қолжетімділікті арттыруды көздейді, бірақ сонымен қатар киберқауіптерден қорғану мәселелеріне де ерекше назар аударылады. Үндістан үкіметі ақпараттық қауіпсіздікке қатысты халықаралық ұйымдармен ынтымақтастық орнатып, киберқауіптерге қарсы жаһандық деңгейде әрекет етуді көздейді.

Азия елдеріндегі киберқылмыспен күрес тәжірибесі әртүрлі, әр елдің өзіндік ерекшеліктеріне сай құқықтық және ұйымдастырушылық шаралар қабылданған. Жапония, Оңтүстік Корея, Қытай және Үндістан сияқты елдер киберқауіпсіздікке қатысты ұлттық және халықаралық деңгейде ауқымды шаралар қабылдап, жаңа технологиялар мен заңнамалық механизмдерді енгізуде. Бұл елдерде киберқауіптерге қарсы тұру үшін мемлекеттік органдар, жеке сектор және халықаралық ұйымдар арасындағы ынтымақтастықты нығайту маңызды рөл атқарады. Киберқылмыстардың өсуі және олардың күрделілігі Азия елдеріндегі киберқауіпсіздік саясатын үнемі жетілдіруді талап етеді.

4. Ресей Федерациясындағы киберқылмыспен күрес тәжірибесі

Ресей Федерациясындағы киберқылмыспен күрес тәжірибесі соңғы жылдары айтарлықтай дамып, құқықтық және ұйымдастырушылық шаралармен бекітілген. Ақпараттық технологиялардың қарқынды дамуы және олардың қоғам өмірінің барлық саласына енуі Ресейде киберқауіптерге қарсы тиімді күрес қажеттілігін тудырды. Осыған орай, Ресей үкіметі киберқауіпсіздікті қамтамасыз ету және киберқылмыстарды болдырмау үшін кешенді құқықтық және техникалық шараларды қабылдады.

Ресейдегі киберқылмыспен күрестің құқықтық негізі

Ресейде киберқылмыстарға қатысты алғашқы заңнамалық қадамдар 1990-жылдардың соңында басталды. Ресей Федерациясының Қылмыстық кодексінде ақпараттық жүйелер мен деректерді қорғауға байланысты арнайы баптар енгізілген. Атап айтқанда, Ресей Қылмыстық кодексінің 272-бабы компьютерлік ақпаратқа рұқсатсыз қол жеткізгені және оны зақымдағаны үшін қылмыстық жауапкершілікті қарастырады. Бұл бап ақпараттық жүйелерді бұзу, деректерді жою немесе өзгерту секілді әрекеттерді қылмыстық құқық бұзушылық ретінде қарастырып, айыппұлдар мен бас бостандығынан айыруды қамтитын жазалау шараларын белгілейді [141].

2000-жылдардың басында қабылданған 273-бап компьютерлік вирустар және зиянды бағдарламаларды тарату үшін жауапкершілікті көздейді. Бұл бап арқылы Ресейдегі ақпараттық жүйелерге бағытталған хакерлік шабуылдар мен вирустарды таратушылар қатаң жазаланады. Компьютерлік жүйелерге зиян келтіруге

бағытталған кез келген әрекет ауыр қылмыс ретінде қарастырылады және кінәлі тұлғаларға айыппұл салу немесе түрмеге қамау сияқты қатаң жазалар тағайындалады.

Ресейде киберқауіпсіздікті қамтамасыз ету үшін "Ақпарат, ақпараттық технологиялар және ақпаратты қорғау туралы" заң (2006 жылы қабылданған) маңызды рөл атқарады. Бұл заң ақпараттық жүйелер мен деректердің қауіпсіздігін қорғауды қамтамасыз етуге бағытталған. Ол мемлекеттік органдар мен жеке секторға ақпараттық қауіпсіздік шараларын күшейту бойынша міндеттер жүктейді және ақпараттық жүйелердің сенімділігін арттыруға бағытталған құқықтық тетіктерді белгілейді.

Киберқауіпсіздік бойынша мемлекеттік органдар және агенттіктер

Ресейде киберқауіптерге қарсы тұру үшін бірнеше мемлекеттік органдар мен агенттіктер жұмыс істейді. Ресей Федерациясының Қауіпсіздік Кеңесі мен Федералдық қауіпсіздік қызметі (ФСБ) елдегі киберқауіпсіздік мәселелерін реттейтін негізгі органдар болып табылады. Бұл ұйымдар киберқылмыстарға жауап беріп, оларды болдырмау үшін қажетті шаралар қабылдайды.

ФСБ киберқауіптерге қарсы тұру бойынша маңызды рөл атқарады, әсіресе елдің ақпараттық инфрақұрылымын қорғау және ұлттық қауіпсіздікке бағытталған кибершабуылдарды болдырмау саласында. ФСБ киберқауіпсіздік саласында ақпарат жинау, талдау және қылмыстық әрекеттерді анықтау бойынша жұмыстарды жүргізеді. Сонымен қатар, мемлекеттік ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін арнайы бағдарламалар мен технологиялық шешімдер әзірлейді.

Ресейдегі тағы бір маңызды ұйым – Мемлекеттік техникалық комиссия (Гостехкомиссия). Бұл агенттік елдегі ақпараттық қауіпсіздік стандарттарын әзірлейді және ақпараттық жүйелердің сенімділігін тексеруге жауапты. Мемлекеттік органдар мен стратегиялық маңызды компаниялардың ақпараттық қауіпсіздігін қамтамасыз ету Гостехкомиссияның басты міндеті болып табылады [142].

Киберқылмыстарға қарсы күресте халықаралық ынтымақтастық

Ресей киберқылмыспен күресте халықаралық ынтымақтастыққа да үлкен мән береді. Ел трансұлттық киберқылмыстарға қарсы әрекет ету үшін халықаралық ұйымдармен, оның ішінде INTERPOL, Шанхай ынтымақтастық ұйымы (ШЫҰ) және BRICS елдерімен бірлесіп жұмыс істейді. Ресей киберқауіпсіздік бойынша бірқатар халықаралық келісімдерге қол қойған және бұл елдің жаһандық қауіпсіздікке қосқан үлесі ретінде қарастырылады.

Сонымен қатар, Ресей Федерациясы киберқауіпсіздік мәселелері бойынша БҰҰ деңгейінде де белсенді жұмыс істейді. Ресей БҰҰ шеңберінде қабылданған киберқауіпсіздікке қатысты резолюциялар мен келісімдерге қолдау көрсетіп, әлемдік деңгейде киберқауіптерге қарсы күресте маңызды рөл атқарады [143].

Киберқылмыстарды болдырмауға бағытталған техникалық және білім беру шаралары

Ресейде киберқауіпсіздікке қатысты техникалық және білім беру шаралары да ерекше маңызды. Мемлекетте «Цифрлық экономика» бағдарламасы аясында киберқауіпсіздік мәселелері бойынша арнайы жобалар жүзеге асырылуда. Бұл бағдарлама цифрлық инфрақұрылымды дамыту және қорғау, ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету бойынша стратегиялық мақсаттарды көздейді.

Сонымен қатар, Ресейде білім беру және оқыту бағдарламалары арқылы қоғамның киберқауіпсіздік туралы хабардарлығын арттыруға ерекше көңіл бөлінеді. Ресей үкіметі киберқауіпсіздік саласында жаңа мамандарды даярлау мақсатында оқу орындарымен және ғылыми-зерттеу институттарымен тығыз ынтымақтастық орнатады. Жоғары оқу орындарында киберқауіпсіздік бойынша мамандар даярлау курстары енгізіліп, арнайы бағдарламалар әзірленуде. Бұл шаралар киберқауіптерге жедел әрекет ету және оларды болдырмау үшін жоғары білікті кадрлар даярлауға мүмкіндік береді [144].

Цифрлық инфрақұрылымды қорғау және жеке деректердің қауіпсіздігі

Ресей Федерациясы киберқауіпсіздік саясатын жетілдіру мақсатында жеке деректердің қауіпсіздігіне ерекше мән береді. 2006 жылы қабылданған «Жеке деректер туралы» заң жеке тұлғалардың деректерін өңдеу және қорғау саласындағы құқықтық негіздерді айқындады. Бұл заң жеке деректерді заңсыз өңдеуден, ұрлаудан және өзгертуден қорғауды қамтамасыз етуге бағытталған. Сонымен қатар, мемлекеттік органдар мен жеке секторларға деректерді өңдеу және сақтау бойынша қатаң талаптар енгізілген [145].

Ресейдегі ақпараттық жүйелер мен желілердің қауіпсіздігін қамтамасыз ету мақсатында «Критикалық ақпараттық инфрақұрылымды қорғау туралы» заң (2017 жылы қабылданған) ерекше рөл атқарады. Бұл заң елдегі маңызды инфрақұрылым нысандарын, оның ішінде энергетика, көлік, қаржы және мемлекеттік басқару салаларын қорғауды күшейтуді көздейді. Заңға сәйкес, маңызды инфрақұрылым нысандарына кибершабуылдар жасалған жағдайда жедел әрекет ету және алдын алу шаралары жүзеге асырылады.

Ресей Федерациясындағы киберқылмыспен күрес тәжірибесі кешенді құқықтық және техникалық шараларға негізделген. Елде киберқауіптерге қарсы тұру үшін құқықтық нормалар мен стандарттар жетілдіріліп, арнайы мемлекеттік органдар мен агенттіктер құрылған. Ресей үкіметі киберқауіптерге жедел жауап беру және алдын алу үшін жаңа технологиялар мен қауіпсіздік жүйелерін енгізуге бағытталған бағдарламаларды жүзеге асыруда. Сонымен қатар, Ресейдің киберқауіпсіздік саласындағы халықаралық ынтымақтастығы трансұлттық қылмыстық құқық бұзушылықпен күресте маңызды рөл атқарады.

5. Халықаралық ынтымақтастық және киберқылмысқа қарсы жаһандық стратегиялар

Халықаралық ынтымақтастық және киберқылмысқа қарсы жаһандық стратегиялар қазіргі таңда әлемдік қауіпсіздік жүйесінің маңызды элементтеріне айналды. Ақпараттық технологиялардың шекараларды білмейтіндігі және

киберқылмыстардың трансұлттық сипаты халықаралық деңгейде бірлескен күш-жігерді қажет етеді. Киберқылмыс қазір тек бір мемлекеттің ішкі мәселесі емес, ол жаһандық қауіпке айналды. Сондықтан киберқылмыспен тиімді күресу үшін әртүрлі елдер арасында ынтымақтастық орнату, ақпарат алмасу, заңнамалық және техникалық стандарттарды үйлестіру маңызды болып отыр [146].

Будапешт конвенциясы (Cybercrime Convention)

Киберқылмысқа қарсы халықаралық ынтымақтастықтың ең маңызды құжаты – 2001 жылы қабылданған Еуропа Кеңесінің Будапешт конвенциясы. Бұл конвенция киберқылмыстарға қарсы күрестегі алғашқы және ең маңызды халықаралық келісімдердің бірі болып табылады. Оның басты мақсаты – киберқылмыстарға қатысты заңнамаларды үйлестіру, құқық қорғау органдарының өзара әрекетін қамтамасыз ету және киберқылмыстар бойынша халықаралық құқықтық көмек көрсету. Конвенцияға қол қойған елдер киберқылмыстарды қылмыстық әрекет ретінде қарастырып, оларға қарсы құқықтық нормалар қабылдауға міндеттеледі. Конвенция сондай-ақ трансұлттық қылмыстарды тергеу барысында мемлекеттер арасында ақпарат алмасуды жеңілдетеді. Бұл құжаттың маңызды бөлігі киберқылмыстық әрекеттерді болдырмауға және олармен күресуге бағытталған құқық қорғау органдарының бірлескен күш-жігерін күшейтуге арналады [147].

Будапешт конвенциясына қосылудың маңызы

Қазақстанның Будапешт конвенциясына қосылуы киберқылмыспен күрес саласында ұлттық заңнаманы халықаралық стандарттарға сәйкестендіру және трансшекаралық қылмыстарға тиімді жауап беру үшін маңызды қадам болып табылады. Будапешт конвенциясы – бұл киберқылмыстарға қарсы күреске арналған ең ірі және бірегей халықаралық құқықтық құжат, ол киберқылмыстардың алдын алудағы, тергеудегі және жазалаудағы негізгі стандарттарды анықтайды. Конвенцияға қосылу Қазақстанға басқа елдермен ынтымақтастықты нығайтып, трансшекаралық қылмыстарға жедел әрі тиімді жауап беруге мүмкіндік береді.

Қазақстандағы цифрландырудың қарқынды дамуы мен ақпараттық инфрақұрылымның кеңеюі киберқауіптердің өсуіне әкелуде. Будапешт конвенциясына қосылу арқылы Қазақстан өз азаматтарының деректерін қорғауды күшейтіп, киберқауіпсіздікті қамтамасыз етуде халықаралық тәжірибені қолдана алады. Сонымен қатар, бұл қадам Қазақстанды цифрлық экономика мен ақпараттық қауіпсіздіктің сенімді серіктесі ретінде көрсетіп, халықаралық деңгейдегі беделін арттырады.

Будапешт конвенциясының артықшылықтары және оның Қазақстан үшін пайдасы

Будапешт конвенциясына қосылу Қазақстанға бірқатар артықшылықтар береді, олардың ішінде ең маңыздылары:

1. Халықаралық ынтымақтастықтың нығаюы: Конвенцияға мүше елдер арасында ақпарат алмасу, трансшекаралық киберқылмыстарға жедел әрекет ету,

және киберқылмыстарды тергеуде қажетті ресурстармен бөлісу мүмкіндігі артады. Бұл Қазақстанның құқық қорғау органдарына күрделі кибершабуылдарға жауап беру және оларды тергеу кезінде тиімді әрекет етуге мүмкіндік береді.

2. Құқықтық базаны жетілдіру: Конвенция стандарттарына сәйкес, Қазақстанның қылмыстық кодексіне жаңа ұғымдар мен баптарды енгізу арқылы заңнаманы жетілдіру қажет болады. Бұл киберқылмыстарға қарсы жазаларды күшейтіп, құқықтық құралдардың ауқымын кеңейтеді.

3. Цифрлық дәлелдемелерді жинау және сақтау: Конвенция электрондық дәлелдемелерді жинау және пайдалану үшін халықаралық стандарттарды бекітеді. Бұл киберқылмыстарды тергеу және сот процесінде дәлелдерді қабылдау жүйесін жетілдіруге ықпал етеді.

4. Экономикалық және инвестициялық тартымдылықтың артуы: Киберқауіпсіздік деңгейінің артуы шетелдік инвесторлар үшін Қазақстанды сенімді серіктес ретінде көрсетеді, бұл цифрлық экономика саласындағы инвестицияларды арттыруға ықпал етеді.

Халықаралық ынтымақтастықтың нақты мүмкіндіктері

Қазақстан Будапешт конвенциясы аясында трансшекаралық киберқылмыстарға қарсы ынтымақтастықты тереңдете алады. Құқық қорғау органдары арасында киберқауіптер туралы ақпарат алмасу және бірлескен тергеу шараларын жүргізу мүмкіндігі артады. Мысалы, Қазақстанның киберқауіпсіздік органдары INTERPOL, Europol сияқты халықаралық ұйымдармен және мүше мемлекеттердің құқық қорғау органдарымен байланыс орнатады. Бұл әртүрлі елдерде орналасқан қылмыстық топтарға қарсы бірлескен операцияларды тиімді жүргізуге мүмкіндік береді.

Бұдан бөлек, Қазақстан басқа елдердің құқық қорғау органдарымен өзара құқықтық көмек көрсету жүйесін жақсартады. Бұл кибершабуылдарды анықтау, дәлелдер жинау және қылмыскерлерді экстрадициялау бойынша үйлесімді жұмыс істеуге мүмкіндік береді. Сондай-ақ, халықаралық ынтымақтастық трансшекаралық қылмыстарды тиімді тергеу және алдын алу үшін шекаралық процедураларды жеңілдетуге көмектеседі.

Будапешт конвенциясынан Қазақстан заңдарына енгізілетін өзгерістер

Конвенцияның негізгі нормалары мен ұғымдарын Қазақстан заңнамасына енгізу елдегі киберқауіпсіздік деңгейін арттыруға және киберқылмыстармен күресте нақты құралдарды қолдануға мүмкіндік береді:

1. «Деректерге рұқсатсыз қол жеткізу» ұғымы: Бұл ұғым деректерді рұқсатсыз алу, өзгерту немесе жою әрекеттеріне нақты жауапкершілік енгізуді көздейді. Қазақстанның қылмыстық кодексінде осы бағытта арнайы баптарды қабылдау қажеттілігі туындайды.

2. Электрондық дәлелдемелерді рәсімдеу: Конвенция электрондық дәлелдемелерді жинау, сақтау және пайдалану рәсімдерін нақты реттейді. Бұл заңнамаға сәйкес электрондық деректердің дәлел ретінде қабылдануын қамтамасыз етеді.

3. Зиянды бағдарламалық қамтамасыз ету бойынша жауапкершілік: Конвенцияға сәйкес, зиянды бағдарламаларды жасау, пайдалану және тарату әрекеттеріне қатаң жазалар қарастыру қажет.

4. Халықаралық ынтымақтастықты реттеу: Қазақстан трансшекаралық киберқылмыстарға қарсы әрекеттерді үйлестіру үшін құқықтық негіздер енгізуі тиіс. Бұл басқа елдердің құқық қорғау органдарымен ынтымақтастықты заңды түрде бекітуге мүмкіндік береді.

Қазақстанның Будапешт конвенциясына қосылуы елдегі киберқауіпсіздік деңгейін арттырып, халықаралық стандарттарға сай құқықтық жүйені қалыптастыруға мүмкіндік береді. Бұл қадам киберқылмыстардың алдын алу, оларды тергеу және жазалау жүйесін жақсартып, халықаралық ынтымақтастықты нығайтады. Сонымен қатар, конвенция нормаларын заңнамаға енгізу арқылы Қазақстан өзінің ақпараттық қауіпсіздігін күшейтіп, халықаралық аренада беделін арттырады.

INTERPOL және Europol

INTERPOL және Europol халықаралық деңгейдегі құқық қорғау ұйымдары киберқылмысқа қарсы күресте негізгі рөл атқарады. INTERPOL киберқылмыстарға қарсы жаһандық ынтымақтастықты күшейту мақсатында 2015 жылы Global Complex for Innovation (IGCI) деп аталатын киберқылмыспен күрес орталығын ашты. Бұл орталық трансұлттық киберқылмыстарға қарсы күрес бойынша мемлекеттерге ақпарат алмасу, сараптама жасау және бірлескен операциялар жүргізу үшін қолдау көрсетеді. IGCI орталығы киберқылмыстарға қатысты зерттеулер жүргізіп, құқық қорғау органдары мен киберқауіпсіздік сарапшыларын біріктіреді. INTERPOL сондай-ақ кибершабуылдардың алдын алу үшін үнемі мониторинг жүргізіп, трансұлттық қылмыстық желілерді анықтау бойынша арнайы операциялар ұйымдастырады [148].

Europol аясындағы European Cybercrime Centre (EC3) киберқылмыстарға қарсы күрес бойынша Еуропалық Одақтың жетекші орталығы болып табылады. Бұл орталық киберқылмыстармен күресуде ЕО елдерінің құқық қорғау органдарына қолдау көрсетіп, трансұлттық кибершабуылдарға қарсы бірлескен шараларды жүзеге асырады. EC3 киберқауіптерді анықтау, талдау және болдырмау бойынша зерттеулер жүргізіп, ақпарат алмасуға мүмкіндік береді. Europol киберқылмыспен күрес бойынша жеке және мемлекеттік секторлар арасындағы серіктестікті нығайтып, интернеттегі қылмыстық әрекеттерді анықтауда үлкен рөл атқарады.

Халықаралық ынтымақтастықты қамтамасыз ету үшін қолданылатын жаһандық стратегиялар

Халықаралық ынтымақтастықтың негізгі жаһандық стратегиялары бірнеше бағытта жүзеге асырылады:

Құқықтық және институционалдық үйлестіру. Көптеген елдер киберқылмыспен күрес саласындағы құқықтық жүйелерін үйлестіру үшін бірлескен халықаралық келісімдерге қол қоюда. Бұл киберқылмыстарды

трансұлттық қылмыс ретінде қарастырып, құқық қорғау органдарының бір-біріне жедел құқықтық көмек көрсетуіне мүмкіндік береді. Будапешт конвенциясы осы бағытта маңызды рөл атқарады, бірақ оған қосылмаған елдер де халықаралық ынтымақтастыққа жүгінуде. Бұл елдер өздерінің заңнамаларын үйлестіру арқылы киберқылмыстарға қатысты жазалау шараларын бірдей қолдану мүмкіндігін қамтамасыз етуде.

Ақпарат алмасу және бірлескен операциялар. Киберқылмыстарды анықтау және болдырмау мақсатында мемлекеттер арасында ақпарат алмасуды жетілдіру өте маңызды. Халықаралық ұйымдар, соның ішінде INTERPOL, Europol, сондай-ақ АТ-компаниялар мемлекеттерге ақпараттық қауіптер туралы деректер беріп, олардың алдын алуға көмектеседі. Бірлескен операциялар киберқылмыстық желілерді анықтап, жою үшін жүргізіледі. Мысалы, Dark Web деп аталатын жасырын интернет желілерінде жүзеге асырылатын қылмыстық әрекеттерге қарсы бірлескен операциялар сәтті жүргізіліп келеді.

Халықаралық стандарттар мен келісімдер. Киберқауіпсіздікке қатысты жаһандық стандарттарды енгізу және қолдану маңызды қадам болып табылады. Халықаралық ұйымдар мен альянстар киберқауіпсіздік стандарттарын әзірлеу арқылы киберқылмыспен күресуді оңтайландыруға үлес қосуда. Мысалы, ISO/IEC 27001 стандарты киберқауіпсіздікті қамтамасыз етудің халықаралық стандарты ретінде танылған және көптеген елдерде қолданылады. Бұл стандарт ұйымдарға ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін қажетті шараларды әзірлеуді көздейді.

Білім беру және оқыту бағдарламалары. Киберқылмыстармен тиімді күресу үшін құқық қорғау органдарын, сондай-ақ жеке сектор мамандарын оқыту мен даярлау өте маңызды. Халықаралық ұйымдар мемлекеттерге киберқауіпсіздік саласында мамандарды оқыту бойынша арнайы бағдарламалар ұсынады. Бұл бағдарламалар киберқылмыстық әрекеттерді анықтау, алдын алу және тергеу саласында тәжірибе жинауға мүмкіндік береді. Сонымен қатар, халықты киберқауіптер туралы хабардар ету бойынша арнайы бағдарламалар мен науқандар жүргізіледі.

Халықаралық ынтымақтастықты жетілдіру үшін техникалық шаралар. Киберқылмыстарға қарсы күресте жаңа технологиялар маңызды рөл атқарады. Халықаралық ынтымақтастықтың бір бөлігі ретінде мемлекеттер мен ұйымдар арасында киберқауіптерге қарсы қолданылатын технологиялық шешімдер алмасу жүзеге асырылады. Кибершабуылдарды анықтау және болдырмау үшін мемлекеттер үнемі жаңа қауіпсіздік жүйелерін әзірлеп, бірлесіп пайдалануға тырысады. Мысалы, DDoS шабуылдарымен күресу үшін арнайы техникалық құралдар мен бағдарламалар қолданылады.

Халықаралық ұйымдардың рөлі

БҰҰ мен Дүниежүзілік банк сияқты халықаралық ұйымдар да киберқауіпсіздік саласында маңызды рөл атқарады. БҰҰ-ның Цифрлық қауіпсіздік стратегиясы жаһандық деңгейде ақпараттық қауіпсіздікті қамтамасыз

етуге бағытталған. Бұл стратегия киберқауіптерге қарсы халықаралық ынтымақтастықты күшейтуді, құқықтық жүйелерді үйлестіруді және жаңа технологияларды енгізуді көздейді. Дүниежүзілік банк киберқауіпсіздікке қатысты түрлі жобаларды қаржыландырып, мемлекеттерге киберқылмыспен күресуде қолдау көрсетеді.

G20 және BRICS елдері де киберқауіпсіздік бойынша ынтымақтастықты дамытуға ерекше көңіл бөлуде. Бұл топтар киберқылмыстарға қарсы бірлескен стратегияларды әзірлеп, халықаралық деңгейде ақпарат алмасуды күшейтуді көздейді. G20 саммиттерінде киберқауіптерге қарсы шаралар талқыланып, бұл мәселені шешуге бағытталған жаңа бастамалар қабылданады.

Киберқылмыспен күрес саласындағы халықаралық ынтымақтастық әлемдік қауіпсіздіктің маңызды аспектісі болып табылады. Будапешт конвенциясы, INTERPOL, Europol және басқа да халықаралық ұйымдар киберқылмыстарға қарсы бірлескен шараларды жүзеге асырып, құқық қорғау органдары мен жеке сектор арасындағы серіктестікті күшейтуге бағытталған. Трансұлттық қылмыстарға қарсы тұру үшін халықаралық стандарттарды енгізу, ақпарат алмасуды жетілдіру және бірлескен операциялар жүргізу киберқауіпсіздікті қамтамасыз етудің маңызды құралдарына айналды. Халықаралық ынтымақтастық киберқауіптерге қарсы күресте тиімді шешімдер қабылдауға мүмкіндік береді және жаһандық қауіпсіздікті нығайтуға ықпал етеді [149].

6. Киберқылмыспен күресудегі ұлттық құқықтық жүйелерге халықаралық тәсілдерді енгізу

Киберқылмыспен күрес саласында шетелдік тәжірибені ұлттық құқықтық жүйелерге енгізу өте маңызды қадам болып табылады. Әртүрлі елдердің заңнамаларын салыстырмалы талдау киберқылмыстарға байланысты қауіптерге жауап беруге мүмкіндік береді. Халықаралық тәжірибені қабылдай отырып, әрбір мемлекет ақпараттық қауіпсіздік пен деректерді қорғау саласында өзіне тиімді стратегияларды қалыптастыра алады.

Мысалы, Қазақстандағы Ақпараттандыру туралы заң ЕО-ның GDPR заңына ұқсас талаптар енгізіп, деректерді қорғау және жеке тұлғалардың ақпараттық қауіпсіздігін қамтамасыз ету үшін маңызды қадамдар жасады. Сондай-ақ, Қазақстан Республикасының Қылмыстық кодексінің VII тарауы АҚШ және Еуропа елдерінің киберқылмыстарға қарсы заңдарын үлгі етіп қабылдап, киберқылмыстарға қатысты жауапкершілікті күшейтті. Біздің ойымызша, «Ақпараттандыру туралы» заңына киберқауіпсіздік ұғымын енгізу маңызды, себебі, бұл компьютерлік жүйелерді, желілерді және деректерді рұқсатсыз қол жеткізуден, шабуылдардан және қауіптерден анықтауға бағытталған.

Шетелдік тәжірибе ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен тиімді күресудің жаһандық және жергілікті стратегияларын қалыптастыруға көмектеседі. Киберқылмыстардың трансұлттық сипаты халықаралық ынтымақтастық пен әртүрлі елдердің құқықтық жүйелерін біріктіруді талап етеді. Киберқылмыспен күресуде халықаралық

ынтымақтастықты күшейту, киберқауіпсіздік шараларын жетілдіру және ұлттық заңнамаларды халықаралық тәжірибеге бейімдеу – киберқылмыстардың алдын алудың маңызды қадамдары болып табылады [150].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың шетелдік тәжірибесі қылмыстық салада заманауи технологияларды қолданудан туындайтын мәселелерге назар аударады. Жарқын мысал ретінде өзінің өлім қаупімен жұртшылықтың назарын аударған «Көк кит» ойынын айтуға болады. Осы ойын аясында жүргізушілер мәжбүрлеген қатысушылар өз-өзіне қол жұмсады. Ресейлік БАҚ 2015 жылдың қарашасы мен 2016 жылдың сәуірі аралығында осы ойынға байланысты балалардың суицидінің 130 жағдайын хабарлады. Өзбекстанда осындай мәселелер суицидке апаратын букмекерлік кеңселер сияқты интернет-платформаларды пайдалануда байқалды. Тұтынушылардың құқықтарын қорғау агенттігі мұндай сайттарға кіруді шектеу шараларын қолданды және 2019 жылы Өзбекстан президенті бұл қызметті реттеу мақсатында елдегі букмекерлік кеңселерді заңдастыру туралы жарлыққа қол қойды. Мұндай шаралар азаматтардың өмірі мен денсаулығына төнетін қатерлердің алдын алуға бағытталған.

О.Лонге және т.б. «Сахараның оңтүстігіндегі Африка елдеріндегі ақпараттық және коммуникациялық технологияларды қылмыстық пайдалану: үрдістер, алаңдаушылықтар және перспективалар». Бұл аймақта АКТ-ның дамуы әлеуметтік-экономикалық дамуға айтарлықтай оң өзгерістер әкелді, алайда ол қылмыскерлердің қолындағы киберқылмыстардың әртүрлі түрлерін жасау қаупінің көзіне айналды. Мұндай қылмыстық құқық бұзушылық мысалдарына электрондық пошта арқылы алаяқтық, жеке басын ұрлау, балалар порнографиясы, ұйымдасқан қылмыс және жезөкшелікке шақыру жатады. Батыс африкалық интернетте кең тараған және нигериялық тамыры бар деп есептелетін «419 алаяқтыққа» ерекше назар аударылады. Авторлар бұл құбылыстың алдын алмаған жағдайда кибертерроризмнің трамплиніне айналуы мүмкін екенін ескертеді, бұл лаңкестерге қарапайым ноутбуктер мен Интернетке кіру арқылы шабуылдарды жинауға, үйретуге және жоспарлауға мүмкіндік береді. Мақалада Африканың оңтүстігінде АКТ-ны қылмыстық жолмен пайдалану туралы шолу берілген, әсіресе нигериялық «419» алаяқтығына сілтеме жасалған. Авторлар осы құбылыстардың тарихын, тенденцияларын, мәселелері мен салдарын қарастырады және осы мәселені шешу үшін стратегиялық саясат перспективаларын ұсынады. Ұсынылған стратегиялар осы қиындықтармен бетпе-бет келген Оңтүстік Сахара Африка сияқты дамушы елдер үшін жалпы тәсілдер жиынтығын ұсынады. Ол одан әрі зерттеулер мен тәжірибеге арналған салдарлармен және ұсыныстармен аяқталады [151].

А.Жаров жүргізген зерттеу Ресейдегі ақпараттық-коммуникациялық технологиялардың (АКТ) ақпараттық қауіпсіздігін реттейтін құқықтық нормалар мен техникалық стандарттарға талдау жасайды. Сондай-ақ бұл саладағы мемлекеттік саясатты айқындайтын стратегиялық құжаттар қамтылып, құқықтық

жүйедегі олқылықтар айқындалады. Автор АКТ-ның бағдарламалық және аппараттық құралдарын зерттейді, сонымен қатар «Ақпарат, ақпараттық технологиялар және ақпаратты қорғау туралы» және «Ресей Федерациясының маңызды ақпараттық инфрақұрылымының қауіпсіздігін қамтамасыз ету туралы» қоса алғанда, негізгі федералды заңдарға шолу жасайды [152].

Цюрих ашық репозиторийінде жарияланған мақаласында және 2015 жылғы мұрағат Еуропалық Одақтың қылмыстық заңнамасының ақпараттық және коммуникациялық технологияларды (АКТ) реттеуге әсерін зерттейді. ЕО-ның кибер әрекетке қатысты қылмыстық заңнамаға қатысуы нені және қандай дәрежеде қылмысқа жатқызу керектігі туралы консенсусқа қол жеткізуді қамтиды. ЕО-ның көптеген заңнамалық шаралары киберқылмысты реттеуге бағытталған, соның ішінде ақпараттық жүйелерге шабуылдар бойынша директивалар және алаяқтық пен жалған ақша жасау бойынша негіздік шешімдер. Терроризмге қарсы негіздік шешім немесе балаларды қанау жөніндегі директивалар сияқты БАҚ-ты реттеуге негізінен қатысы жоқ заңнамалық құралдар үшін де Интернет маңызды рөл атқарады. ЕО-да криминализациялануы тиіс киберқызмет түрлеріне қатысты әртүрлі көзқарастар бар. Балалар порнографиясын өндіру немесе көрсету сияқты белгілі бір әрекеттер үшін қылмыстық жауапкершілікке тарту қажеттілігі туралы кең консенсус бар. Дегенмен, кейбір басқа салаларда қылмыстық заңға жүгіну қажеттілігіне қатысты пікірлердің кең ауқымы бар. Бұл, әсіресе, ЕО-ның зияткерлік меншік құқығын бұзумен күресу үшін қылмыстық заңнаманы құру әрекеттері аясында байқалады. ЕО-ның осы саладағы қылмыстық заңнамаға итермелеуі ЕО деңгейіндегі қылмыстық құқық бұзушылыққа байланысты қиындықтарды көрсетеді [153].

Т.Элвес және С.Дрим жүргізген зерттеулер виртуалды кеңістіктегі қылмыстық құқық бұзушылықтың ауырлығын жеңілдету үмітімен бірқатар ұсыныстармен сүйемелденеді, өйткені ол көбінесе көптеген жағдайларда шынайы өмірмен байланыстырылады және жеке өмірге қол сұғылмаушылықты қорғауға алаңдамайды. индивидуалды және оның қауіпсіздігін қамтамасыз ету ақпараттық технологиялар дәуіріндегі жағымсыз құбылыстардан ақпараттық БАҚ араласып, БАҚ еркіндігі мен ашықтығы стандарттары инфильтрация және бұзылу мәселесімен араласады. Ұсыныстар келесідей болды:

- Электрондық ақпарат құралдарына қатысты заңдар мен ережелерді әзірлейтін заң шығарушылар жергілікті билік органдарымен және халықаралық ұйымдармен қазіргі заманғы коммуникацияларды пайдаланушылар мен оларды пайдалануды реттейтін мәселелер бойынша жақсы қарым-қатынас пен келісімді қамтамасыз ету үшін желіні басқару негіздері мен ережелерін құруы керек.

- Ақпараттық БАҚ пайдаланушыларын қауіпсіздік, құпиялылық және ақпараттық қылмыс туралы оқыту үшін жоспарлар мен стратегияларды әзірлеу бойынша жұмыс жасаңыз.

- Адамның рухын жоюға және оның табиғатынан айыруға шақыратын веб-сайттарды цензуралау және вирустар мен хакерлердің алдын алу және оларға

қарсы тұру үшін пайдаланушы желілерін бағдарламалық қамтамасыз етумен нығайту.

- Ұлттық үкіметтер электрондық БАҚ пайдаланушылары арасында зияткерлік меншік мәдениетін және құпиялылық туралы хабардарлықты таратуға және сақтауға назар аударуы керек.

- Жаңа медиа саласындағы академиялық зерттеулерді күшейту, олардың әлеуметтік құбылыстар мен оларға әсер ететін мәселелерді көрсетудегі рөлін және олардың қысқа және ұзақ мерзімді перспективада әсерін, сондай-ақ оларды виртуалды ортада қылмыстық әрекеттерді тарату үшін пайдаланбауын түсіндіру. ғарыш.

- Ақпараттық мәдениетті түсінуге және медиаконтентпен өзара әрекеттесуге адамды дайындау үшін әртүрлі білім беру, академиялық және кәсіби салаларда медиа сауаттылық деңгейін арттыру.

- Қажетті құқықтық реформаларды жүргізу және оларды жылдам жүзеге асыру үшін қажетті ресурстармен қамтамасыз ету, сондай-ақ сабақ алу және жағдайдың маңыздылығын түсіну үшін веб-сайттарды пайдаланатын қылмыскерлерді жазалау қажеттілігі.

- Электрондық БАҚ пайдаланушысының мінез-құлқын өзгерту үшін құндылықтар жиынтығын енгізу және оны тәуелділіктен және Интернетте көбірек уақыт өткізуден құтқарудың басқа нақты нұсқаларын жасау арқылы оның моральдық аспектісіне назар аудару [154].

Германиядағы Кавин С., Братсук И. және Литвиненко А. зерттеулері бойынша киберқауіпсіздікке қатысты заңнамалық база мониторинг жүргізу, анықтау, алдын алу, салдарларды азайту және оқиғаларды басқаруға арналған заңдарды қамтиды. Бұл заңдар деректерді қорғау және электрондық құпиялылық туралы заңдар, зияткерлік меншік туралы заңдар, құпиялылық туралы заңдар, ақпараттық қауіпсіздік туралы заңдар және импорт/экспортты бақылауды реттейді. Германиядағы киберқауіпсіздік бірнеше заңмен реттеледі, олардың негізгісі 2015 жылғы 25 шілдеде қабылданған Германияның Қауіпсіздік туралы заңы (IT-Sicherheitsgesetz). Бұл заң Телемедиа туралы заңға (Telemediengesetz), Телекоммуникациялар туралы заңға (Telekommunikationsgesetz), ЕО-ның Деректерді қорғау туралы жалпы ережесіне (Datenschutz-Grundverordnung), Деректерді қорғау туралы Федералдық заңға (Bundesdatenschutzgesetz) және Федералдық Ақпараттық қауіпсіздік басқармасы туралы заңға (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) өзгерістер енгізді [155].

Сонымен қатар, киберқауіпсіздікке қатысты заңнамалар банк қызметі туралы заң (Kreditwesengesetz) және бағалы қағаздар саудасы туралы заңмен (Wertpapierhandelsgesetz) реттеледі. Ресми заңдардан басқа, Германияда АТ қауіпсіздігіне қатысты бейресми ережелер де бар. Олардың қатарына Федералдық Ақпараттық қауіпсіздік агенттігінің (BSI) Ақпараттық технологиялар қауіпсіздігінің негіздері, ISO/IEC 15408 стандартына сәйкес Ақпараттық технологиялар қауіпсіздігін бағалаудың ортақ критерийлері және Ақпараттық

және байланысты технологияларды басқару (COBIT) жүйесі жатады.

Еуропалық Одақтың Киберқауіпсіздік ережесі (2019) Еуропалық киберқауіпсіздік агенттігіне (ENISA) киберқауіпсіздік сертификаттарын орнату құқығын береді. ENISA киберқауіпсіздік мәселелері бойынша негізгі байланыс орталығы болып саналады. Ақпараттық қауіпсіздік туралы федералдық заң маңызды инфрақұрылым үшін арнайы киберқауіпсіздік талаптарын белгілейді. Осыған сәйкес неміс және еуропалық заңнама ұйымдарға киберинциденттерді бақылау, анықтау, алдын алу және салдарын азайту бойынша бірқатар міндеттемелерді қарастырады. Мысалы, Телемедиа туралы заңның 13(7) тармағына сәйкес, телемедиа қызметтерін жеткізушілер пайдаланатын техникалық жабдыққа рұқсатсыз қол жеткізуге жол берілмеуі және жеке деректердің кибершабуылдардан қорғалуы қамтамасыз етілуі тиіс.

Сондай-ақ С.Кавин, И.Братсук және А.Литвиненко Франция киберқауіпсіздік саласындағы заңнамалық платформасының негізін құрайтын бірқатар заңдар бар екенін дәлелдейді . Ең маңыздыларының қатарына мыналарды жатқызуға болады: 1988 жылғы 15 қаңтардағы № 88-19 Годфрен заңы, 1978 жылғы 6 қаңтардағы № 78-17 «Деректерді қорғау туралы», 2016 жылғы 7 қазандағы № 2016-1321 «Цифрлық республика» заңы және 2018 жылғы 26 ақпандағы NIS № 2018-133 директивасын ауыстыратын желілік қауіпсіздік және ақпараттық жүйелер (NIS актісі). Сонымен қатар, қылмыстық заңнаманы киберқылмыстың жекелеген түрлеріне бейімдейтін және арнайы тергеу құралдарын жасайтын бірқатар заңдар бар. Мысалы, 2001 жылғы 15 қарашадағы «Күнделікті қауіпсіздік туралы» Заң (ТҚҚ), 2003 жылғы 18 наурыздағы № 2003-239 «Ішкі қауіпсіздік туралы» Заңы, № 2004 «Сот жүйесін қазіргі жағдайдағы қылмыстың дамуына бейімдеу туралы» Заңы. 2004 жылғы 9 наурыздағы 204 және 2006 жылғы 1 тамыздағы Давид заңы деп аталатын Ақпараттық қоғамдағы авторлық құқық туралы заң. Франциядағы маңызды инфрақұрылымдар заңмен анықталады және белгілі бір заңды талаптарға, әсіресе құпияны сақтау саласындағы кәсіби мамандарға, маңызды қызмет операторларына және цифрлық қызмет жеткізушілеріне қатысты талаптарға сәйкес келуі керек. GDPR бойынша контроллер мен процессор анықталған тәуекелге сәйкес қауіпсіздік деңгейін қамтамасыз ету үшін тиісті техникалық және ұйымдастырушылық шараларды қабылдауы керек. NIS ережелері сонымен қатар PSO және DSP маңызды/цифрлық қызметтерді көрсету және ақпараттық жүйелердің қауіпсіздік тәуекелдерін анықтау үшін қажетті желілік және ақпараттық жүйелердің тізімін құруды және жүргізуді талап етеді. Бұдан басқа, олар қауіпсіздіктің тиісті деңгейін қамтамасыз етуі, тәуекелдердің алдын алу, басқару және азайту үшін қажетті техникалық және ұйымдастырушылық шараларды жүзеге асыруы, сондай-ақ оқиғаларды болдырмау және олардың қызметтердің үздіксіздігіне әсерін барынша азайтуы керек. NIS ережелерін қолдану үшін ANSSI, Қорғаныс министрлігі және Ішкі істер министрлігі жауапты ұлттық орган болып табылады. Кейбір аймақтарда киберқауіпсіздікті бақылау айтарлықтай қатаң болуы керек, әсіресе маңызды

инфрақұрылымдар үшін [155,б.54-56].

Н.Мехта, П.Сангави, М.Паливал және М.Шукла сәйкес кибер құқық, көбінесе ***Интернет құқығы*** деп аталады, Интернеттегі ақпараттық технологиялардың заңдылығымен айналысатын құқықтық жүйенің саласы. Ол ақпаратты цифрлық тасымалдауды, онлайн-сауда қолданбаларын және ақпараттық қауіпсіздікті реттейді. Ол сот информатикасына және жүйелер, бағдарламалық қамтамасыз ету және аппараттық қамтамасыз ету сияқты электрондық компоненттерге қатысты. Бұл мақалада G20 елдері арасында ашық интернеттің болуы және сәйкестігі, сөз бостандығы және онлайн құпиялылық сияқты әртүрлі тақырыптар қарастырылады. G20 – 19 ел мен Еуропалық Одақ өкілдері бар әлемдегі ең ірі жиырма экономиканың халықаралық ұйымы. G20 мүшелеріне АҚШ, Қытай, Жапония, Германия, Франция, Ұлыбритания, Ресей, Үндістан және т.б. сияқты әртүрлі елдер кіреді. Бұл ұйым жаһандық сауда, қаржылық тұрақтылық және халықаралық қаржы институттарын реформалау сияқты маңызды экономикалық және қаржылық мәселелерді талқылайды. Стандарттар асимметриялық соғысқа қатысатын адамдар санын айтарлықтай қысқартуға ықпал етеді, сондай-ақ ақпаратқа заңсыз қол жеткізуден, интернетті пайдаланумен байланысты сөз бостандығынан, жеке кеңістікті, ақпарат алмасуды, электрондық пошта домендерін қорғау арқылы олардың қатысуын шектеуге көмектеседі, материалдық емес активтер, машиналар және интернет, соның ішінде сақтау құрылғылары. Интернет-трафик көбейген сайын бүкіл әлемде құқықтық мәселелердің саны да артып келеді. Интернет заңдары әр елде әртүрлі болғандықтан, жазалау айыппұлдардан бас бостандығынан айыруға дейін болуы мүмкін және полиция органдарына орындау қиын болуы мүмкін. Киберзаң Интернетті пайдаланатын немесе онлайн бизнес жүргізетін адамдарды қорғайды. Интернет пайдаланушылары желідегі әрекеттерге рұқсат етілген немесе тыйым салынғанын анықтау үшін өз елдерінің жергілікті қауымдастығын және киберзаңдарын түсінуі керек. Бұл сондай-ақ заңсыз әрекеттерге араласпауға көмектеседі [156].

Мусаткина А.А., Евдокимов К.Н., Ревина С.Н., Цельникер Г.Ф. және В.М.Реуф «Киберқылмыс Ресей Федерациясының цифрлық экономикасына қауіп ретінде: ағымдағы жай-күй, динамикалық үлгі және үрдістер» атты мақаласында киберқылмыстың Ресейдің цифрлық экономикасына тигізетін ықпалы туралы талдау жасалған. Мақала «Ресейдегі мемлекеттік басқару және аймақтық басқару» журналында жарияланған. Ресей Федерациясының Қылмыстық кодексінің 274-бабының 1-бөлігіне сәйкес, компьютерлік ақпаратты сақтау, өңдеу немесе беру құралдарын, сондай-ақ ақпараттық-телекоммуникациялық желілерді және терминалдық жабдықтарды пайдалану ережелерін бұзу нәтижесінде 1 миллион рубльден астам ірі залал келтірілген жағдайда, кінәлілер 2 жылға дейін бас бостандығынан айырылады. Ауыр зардаптар тудырған немесе олардың туындау қаупін тудырған жағдайда, санкция 5 жылға дейін бас бостандығынан айыру жазасын қарастырады (РФ Қылмыстық кодексінің 274-бабының 2-бөлігі). Ресми статистикаға сәйкес, компьютерлік ақпарат саласында жасалған қылмыстық құқық

бұзушылықтарды, оның ішінде Ресей Федерациясының Қылмыстық кодексінің 274-бабында көрсетілген әрекеттердің ағымдағы жағдайы мен динамикалық үлгісі регрессивті болып табылады. Атап айтқанда, осы түрдегі қылмыстық құқық бұзушылықтар бойынша тіркелген, тергелетін және сотқа жеткізілетін қылмыстық істердің саны жыл сайын тұрақты түрде азайып келеді. Ресей Федерациясы Ішкі істер министрлігінің Бас ақпараттық-талдау орталығының мәліметтері бойынша, 272, 273, 274-баптарында көрсетілген компьютерлік ақпарат саласындағы қылмыстық құқық бұзушылықтың жалпы саны (күнтізбелік жылдың ағымдағы кезеңінде тіркелген). Ресей Федерациясының Қылмыстық кодексі келесідей болды: 2009 жылы - тиісінше 9489, 2097 және 4; 2010 жылы – тиісінше 6132, 1010 және 0; 2011 - 2005 жылдары тиісінше 693 және 0; 2012 жылы - тиісінше 1930, 889 және 1; 2013 жылы – тиісінше 1799, 764 және 0; 2014 жылы – тиісінше 1151, 585 және 3; 2015 жылы – тиісінше 1396, 974 және 12; 2016 жылы – тиісінше 994, 751 және 3; 2017 жылы – тиісінше 1079, 802 және 2; 2018 жылы – тиісінше 1761, 733 және 5 [157].

Ақпараттандыру және байланыс саласында жасалған қылмыстық қылмыстық құқық бұзушылықтардың шетелдік тәжірибесі тенденцияларды талдау, мұндай қылмыстық құқық бұзушылықтың себептері мен салдарын анықтау, сондай-ақ олардың алдын алу және жолын кесу бойынша тиімді шараларды әзірлеу тұрғысынан маңызды зерттеу нысаны болып табылады. Әртүрлі елдерде жүргізілген зерттеулер киберқауіпсіздікті реттеудің ерекшеліктерін анықтауға, сондай-ақ қабылданған шаралар мен заңнаманың тиімділігін бағалауға мүмкіндік береді. Ақпараттық-коммуникациялық технологияларды қолданудың артуымен киберқылмыс деңгейі де артып отырғаны атап өтіледі, бұл ақпаратты қорғаудың құқықтық тетіктері мен техникалық құралдарын үздіксіз жетілдіру қажеттілігін көрсетеді. Сонымен қатар, әртүрлі елдердегі киберқауіпсіздікті реттеудің қолданыстағы тәсілдерін талдау осы саладағы перспективалар мен мәселелерді анықтауға мүмкіндік береді. Осылайша, шетелдік тәжірибені зерделеу киберқылмыспен күресудің тиімді стратегиясын қалыптастыруда және ақпараттық ортаның қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Әртүрлі елдерде қолданылатын құқықтық және техникалық тетіктерді талдау осы саладағы реттеудің ерекшеліктерін анықтауға, сондай-ақ киберқауіптермен күресудің тиімді әдістерін анықтауға мүмкіндік береді. Зерттеу киберқылмыстың даму тенденциялары мен динамикасын ғана емес, сонымен қатар оның алдын алу мен жолын кесудің табысты тәжірибелері мен инновациялық тәсілдерін ашады. Басқа елдердің тәжірибесі заңнаманы жетілдіру, ақпаратты қорғаудың техникалық құралдарын әзірлеу және киберқауіпсіздік мамандарының құзыреттілігін арттыру бойынша құнды сабақтар мен ұсыныстардың көзі бола алады. Осылайша, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың шетелдік тәжірибесі туралы қорытындыда жалпы ақпараттық ортаның қауіпсіздігін қамтамасыз ету үшін киберқауіптерге қарсы күресте халықаралық ынтымақтастық пен тәжірибе алмасудың маңыздылығы көрсетілген.

3.4 Қазақстан Республикасының ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресу мәселелері

Ақпараттық технологиялардың қарқынды дамуы және киберқылмыстардың артуы жағдайында тиімді құқық қорғау және үйлестіру мәселелері өзекті бола түсуде.

Бұл бөлімде талқыланатын бірінші аспект құқықтық реттеуге қатысты. Киберқылмыспен күресті реттейтін қолданыстағы заңдар мен ережелер үнемі жаңартып отыруды және жаңа сын-қатерлер мен қауіптерге бейімделуді талап етеді. Құқықтық базаны қайта қарау және жетілдіру қажеттілігі технологияның қарқынды дамуы мен қылмыскерлер қолданатын әдістердің өзгеруіне байланысты.

Екінші аспект жедел-іздестіру жұмыстарын қамтиды. Онда құқық қорғау органдары киберқылмыстарды анықтау мен тергеуде кездесетін ұйымдастырушылық кемшіліктер мен қиындықтарды зерттейді. Киберқауіптерге тиімді қарсы тұру үшін қажетті мамандандырылған қызметкерлер мен заманауи құрал-жабдықтардың қажеттілігіне ерекше назар аударылады.

Үшінші аспект халықаралық ынтымақтастыққа арналған. Киберқылмысқа қарсы күрес шетелдік серіктестермен тығыз ынтымақтастықты қажет етеді, бірақ тиімді халықаралық үйлестіру үшін көптеген кедергілер мен қиындықтар бар. Өзара жұмыс істеу мәселелері, заңнамалық тәсілдер мен процедуралық нормалардағы айырмашылықтар трансшекаралық киберқылмыспен күресу бойынша бірлескен күш-жігерді қиындатады [158].

Бөлімнің қорытынды бөлігінде ағымдағы жағдайды жақсарту бойынша ұсыныстарға назар аударылады. Құқықтық базаны жетілдіру және заңнаманы заманауи шындыққа бейімдеу маңызды қадам болып табылады. Сондай-ақ Қазақстан Республикасындағы киберқылмыспен күрестің тиімділігін айтарлықтай арттыратын ұйымдық өзгерістер мен құқық қорғау органдары қызметкерлерінің біліктілігін арттыру бойынша шаралар ұсынылатын болады. Осылайша, 3.4-бөлім ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылыққа қарсы күреске байланысты мәселелер мен міндеттерді жан-жақты қарастыруға, сондай-ақ оларды еңсеру және елдегі ақпараттық қауіпсіздік деңгейін арттыру бойынша ұсыныстар әзірлеуге бағытталған.

Заңнамаларды бейімдеу қажеттілігі киберқылмыстың жаһандық сипатымен де байланысты. Қылмыстық құқық бұзушылықтың бұл түріне қарсы күрес халықаралық ынтымақтастықты және мемлекеттер арасында белсенді ақпарат алмасуды қажет етеді. Қазақстан трансшекаралық киберқылмыспен күресудің бірлескен стратегиялары мен әдістерін әзірлеуге белсене қатысуда, ол сондай-ақ басқа шетелдер қол қойған құқықтық құжаттарда және халықаралық келісімдерде көрініс табады. Осылайша, киберқылмыспен күрес саласындағы тиімді құқықтық реттеу тек қана қатаң талаптарды талап етпейді. қолданыстағы нормативтік-құқықтық актілерді сақтау, сонымен қатар оларды ақпараттық қоғамның және технологиялық прогрестің жаңа жағдайларына үнемі жаңартып отыру және

бейімдеу болып табылады [159].

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылыққа қарсы күрес саласындағы жедел-іздестіру жұмыстары бірқатар ұйымдастырушылық кемшіліктер мен мәселелерге тап болып отыр. Басты мәселелердің бірі – түрлі құқық қорғау органдары арасындағы үйлестіру мен ынтымақтастықтың жоқтығы. Бұл тергеулердің кешігуіне әкеледі және киберқауіптерге тиімді әрекет етуді қиындатады. Техникалық қамтамасыз ету деңгейіне және жоғары білікті мамандарды тарту мүмкіндігіне әсер ететін шектеулі қаржыландыру да маңызды аспект болып табылады. Ақпараттық қауіпсіздік инциденттеріне жедел әрекет ету үшін ресурстардың жетіспеушілігі киберқылмыспен күресу шараларының тиімділігін төмендетеді.

Қазақстанның құқық қорғау органдарының киберқылмыспен күресу бойынша жұмысында ұйымдастырушылық жағынан елеулі кемшіліктер анықталды. Негізгі мәселелердің бірі – қызметкерлердің ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтарды саралау мен тергеуде қиындықтарға әкелетін арнайы білімнің болмауы [160]. Киберқылмыстарды тергеу бойынша жеткілікті ғылыми негізделген әдістемелер мен ұсыныстардың жоқтығы да процесті қиындатады. Сонымен қатар, көптеген құқық қорғау органдарының қызметкерлері қылмыстық құқық бұзушылықты ашуда заманауи технологияларды тиімді пайдаланудың қажетті дағдыларына ие емес, бұл олардың тиімділігі мен тиімділігін төмендетеді.

Сонымен қатар, құқық қорғау органдарына арнайы мамандар мен заманауи құрал-жабдықтар өте қажет. Заманауи киберқылмыстар тек дәстүрлі тергеу әдістерін ғана емес, ақпараттық технологиялар саласындағы терең білімді де қажет етеді. Дегенмен, Қазақстанда киберқауіпсіздік саласында қажетті құзыреттерге ие мамандар тапшы. Бұл мәселені шешу үшін қоғамның цифрлық трансформациясы жағдайында олардың біліктілігін және жұмыс тиімділігін арттыратын құқық қорғау органдары қызметкерлерін даярлау және қайта даярлау бағдарламаларын әзірлеу және енгізу қажет. Тергеу жүргізу және цифрлық дәлелдемелерді талдау үшін озық технологиялар мен құралдарға қолжетімділікті қамтамасыз ету де маңызды. Осылайша, киберқылмысқа қарсы күресте жедел-іздестіру жұмыстарының тиімділігін арттыру үшін ұйымдық құрылымды жетілдіру, қаржыландыруды ұлғайту, кадрлық және техникалық ресурстарды дамытуды қамтитын кешенді тәсіл қажет.

Қазақстан Республикасында киберқылмыспен тиімді күресу үшін мамандандырылған кадрларды тарту және оқыту қажет. Бүгінгі таңда интернет-алаяқтықты тексеру үшін әр өңірде арнайы «Киберпол» топтары құрылып, жұмыс істейді. Бұл топтар IT білімі бар және заң ғылымының негіздерін білетін жоғары білікті мамандардың тапшылығына тап болып отыр. Жедел-іздестіру іс-шараларын жүргізуге қажетті заманауи құрал-жабдықтар да қажет. Мысалы, Астана қаласындағы алаяқтық байланыс орталықтарында тінту кезінде арнайы бағдарламалармен қорғалған құлаққаптары мен желілік жабдықтары бар

ноутбуктер алынды, бұл киберқылмыстарды тиімді тергеу үшін заманауи техникалық құралдардың қажеттілігін растайды [161].

Киберқылмыспен күресуде халықаралық ынтымақтастықтың негізгі қиындықтарының бірі – мемлекеттер арасындағы өзара үйлесімді іс-қимылдың жеткіліксіздігі. Қазақстанда да, басқа елдер сияқты, киберқауіптермен тиімді күресу үшін халықаралық ынтымақтастық пен ақпарат алмасудың маңызы артып келеді. Алайда бірыңғай стандарттар мен рәсімдердің болмауы ақпарат алмасу және бірлескен операцияларды ұйымдастыру үдерісін күрделендіреді. Бұл жағдай кибершабуылдарды уақытылы анықтап, олардың жолын кесу бойынша іс-қимылдарға кедергі келтіреді, сондай-ақ оқиғаларды толық тергеу мен кінәлілерді жауапқа тарту қажеттілігін күшейтеді. Мысалы, жеке деректердің таралуы немесе жүйелердің шифрлау вирустарымен зақымдануы кезінде халықаралық ынтымақтастық шешуші рөл атқарады.

Сонымен қатар, халықаралық үйлестірудегі басты қиындықтардың бірі – елдер арасындағы құқықтық айырмашылықтар мен бюрократиялық рәсімдердің көптігі. Бірыңғай деректер алмасу тетіктерінің болмауы киберқылмыскерлерге жазасыз қалуға мүмкіндік береді, өйткені мұндай құқықтық олқылықтар олардың қудалаудан оңай жалтаруына жағдай жасайды. Халықаралық келісімдерді үйлестіру және бекіту де айтарлықтай қиындық тудырады, бұл жаһандық киберқауіпсіздік жүйесін құруға тосқауыл қояды. Мәселен, 2023 жылы Қазақстанның «Мемлекеттік техникалық қызметі» халықаралық деңгейде араласуды талап ететін бірқатар киберқауіпсіздік инциденттерін тіркегенімен, үйлестірудегі қиындықтар бұл мәселелерді жедел әрі тиімді шешуге кедергі жасады.

Қазақстандағы киберқылмыспен күрестің тиімділігін арттырудың негізгі қадамы – заңнамалық базаны үнемі жетілдіріп отыру. Жаңа қауіптер мен қылмыстық әдістерді ескере отырып, заңдар мен нормативтік актілерді жаңарту қажет. Бұл тек шабуылдарды тиімді бақылау мен жолын кесуге мүмкіндік беріп қана қоймай, сондай-ақ цифрлық ортада азаматтар мен ұйымдардың құқықтарын қорғаудың берік негізін қалыптастырады. Сонымен қатар, киберқауіпсіздік мәселелерін реттейтін мамандандырылған заңдарды әзірлеп, халықаралық келісімдерді ратификациялау мүмкіндігін қарастыру қажет. Бұл қадамдар Қазақстанның ұлттық мүдделері мен құқықтық жүйесінің ерекшеліктеріне сәйкесжүзеге асырылуы тиіс [162].

Киберқылмыспен күрестің тиімділігін арттыру үшін бірқатар ұйымдастырушылық өзгерістерді енгізу қажет:

1. Киберқылмыскерлердің жаңа қауіптері мен әдістерін ескере отырып, киберқауіпсіздікке қатысты заңдарды жүйелі түрде қарап шығу және жаңарту.
2. Киберқылмысты қадағалауды және онымен күресуді жеңілдету үшін ережелерді енгізу.
3. Киберқауіпсіздік мәселелерін реттейтін арнайы заңдарды жасау.
4. Ұлттық мүдделерді ескере отырып, жаһандық киберқауіпсіздікті нығайтуға

бағытталған халықаралық келісімдер мен конвенцияларды ратификациялауды қарастыру.

5. Құқық қорғау органдарында тек киберқылмыстармен айналысатын мамандандырылған бөлімшелерді ұйымдастыру.

6. Киберқауіпсіздіктің соңғы әдістері мен технологияларына назар аудара отырып, құқық қорғау органдары қызметкерлеріне тұрақты курстар мен тренингтер өткізу.

7. Оқыту бағдарламаларында халықаралық тәжірибе мен озық тәжірибені зерттеуді қосу.

8. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды үйлестіруді жақсарту үшін ведомствоаралық ынтымақтастықты дамыту.

9. Оқиғаларға тезірек ден қоюға мүмкіндік беретін жеке сектормен ынтымақтастықты күшейту.

10. Киберқауіпсіздік мәселелері бойынша халықаралық форумдар мен конференцияларға белсенді қатысу.

11. Шетелдік киберқауіпсіздік органдарымен серіктестік орнату және дамыту.

12. Халықаралық серіктестермен жедел ақпарат алмасу механизмдерін құру.

13. Азаматтардың цифрлық кеңістіктегі сақтық шаралары туралы хабардарлығын арттыру үшін ақпараттық науқандарды өткізу.

14. Мектептер мен университеттерде киберқауіпсіздік бойынша білім беру бағдарламаларын әзірлеу.

15. Киберқауіпсіздік саласындағы отандық бағдарламалық шешімдерді әзірлеуге және енгізуге инвестициялау.

16. Барлық мемлекеттік және жеке құрылымдардың заманауи технологияларға қолжетімділігін қамтамасыз ету.

17. Қауіпсіздік жағдайын бақылау және барлық мүдделі тараптардың әрекеттерін үйлестіру үшін Ұлттық киберқауіпсіздік үйлестіру орталығын құру.

18. Ағымдағы қауіптер мен ақпараттық қауіпсіздік инциденттері туралы тұрақты ақпарат алмасуды ұйымдастыру [163].

Қазақстанның цифрлық дәуірге енуі барысында ақпараттандыру және байланыс саласындағы қылмыстық құқықбұзушылықтар өзекті мәселеге айналды. Бұл саладағы қылмыстық құқық бұзушылықтарға ақпараттық жүйелерге заңсыз қол жеткізу, деректерді ұрлау және тарату, зиянды бағдарламаларды қолдану және телекоммуникациялық инфрақұрылымға шабуыл жасау жатады. Осындай құқықбұзушылықтармен күресу үшін елдің құқықтық және институционалдық жүйесін жетілдіру қажет.

А.Н. Ағыбаевтың пікірінше, киберқылмыстарға қарсы күрес жүргізуде құқықтық базаның жетілуі және құқықтық реттеудің заманауи талаптарға сай болуы аса маңызды. Ол заңнамалық актілердің тұрақты түрде жетілдірілуі қылмыстық құқықтың тиімділігін арттырады деп атап көрсетеді. Бұл ретте Қазақстанда қабылданған «Киберқалқан» тұжырымдамасы ақпараттық қауіпсіздікті қамтамасыз етудің маңызды құралы болып табылады. Дегенмен,

елдегі құқық қолдану тәжірибесінде бірыңғай стандарттар мен ережелердің болмауы күрес тиімділігін төмендетуі мүмкін [164].

И.Ш. Борчашвили киберқылмыстармен күресте құқық қорғау органдарының мамандануына ерекше көңіл бөледі. Оның пікірінше, киберқылмысқа қарсы күресті күшейту үшін полиция, прокуратура және арнайы қызметтердің қызметкерлерін ақпараттық технологиялар саласында оқыту қажет. Бұл олардың ақпараттық қауіпсіздікке байланысты қылмыстық құқық бұзушылықтарды тиімді тергеу және алдын алу қабілетін арттырады. Сонымен қатар, құқықтық нормалар халықаралық тәжірибелермен үйлесуі керек, себебі киберқылмыстардың трансұлттық сипаты халықаралық ынтымақтастықты қажет етеді [165].

Ү.С. Жекебаев ақпараттық қауіпсіздікке байланысты қылмыстық құқықбұзушылықтарға құқықтық баға беруде нормалардың анықтығы мен қолдану бірізділігінің маңыздылығын атап өтеді. Оның пікірінше, ақпараттық кеңістіктегі қылмыстық құқық бұзушылықтарды дұрыс саралау және тиісті жазалау шараларын белгілеу – құқық бұзушылықтардың алдын алудың тиімді құралы. Қазақстандық құқықтық жүйе бұл бағытта әлі де жетілдіруді қажет етеді, себебі кейбір құқықтық олқылықтар қылмыскерлерге жауапкершіліктен құтылуға мүмкіндік береді [166].

Е.І. Қайыржановтың еңбектерінде көрсетілгендей, киберқылмыстармен күресте құқықтық жүйенің басты міндеттерінің бірі – цифрлық инфрақұрылымға нұқсан келтіретін әрекеттердің алдын алу. Ол заңнаманың киберкеңістіктегі заңсыз әрекеттерді қамту ауқымын кеңейту және жаңа қауіп-қатерлерді ескеретін нормативтік-құқықтық актілерді әзірлеу қажеттігін атап өтеді [167].

С.М. Рахметов ақпараттық жүйелерді қорғаудағы құқықтық және техникалық шаралардың қатар жүргізілуінің маңыздылығын көрсетеді. Ол цифрлық қауіпсіздікті қамтамасыз ету үшін заңнамалық шаралармен қатар технологиялық шешімдерге де назар аудару керектігін атап өтеді. Оның пікірінше, мемлекеттік органдар мен жеке сектордың бірлесе жұмыс істеуі ақпараттық қауіпсіздік саласындағы қылмыстық құқықбұзушылықтардың алдын алуда маңызды рөл атқарады [168].

К.Ж. Балтабаев киберқылмыстарға қатысты қылмыстық істер бойынша дәлелдемелерді жинау және сотқа дейінгі тергеу процесінің қиындықтарын талдайды. Ол дәлелдемелерді жинау кезінде қолданылатын әдістердің сенімділігін қамтамасыз ету қажеттігін баса айтады, себебі киберқылмыстардың күрделі құрылымы мен анонимдік сипаты тергеушілер үшін үлкен қиындық туғызады. Сонымен қатар, киберқылмыстардың көбіне трансұлттық сипатқа ие болуына байланысты халықаралық ынтымақтастықты дамыту қажеттілігіне тоқталады [169].

Қазақстанда ақпараттық және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы күресті жетілдіру үшін қылмыстық заңнаманы халықаралық стандарттармен үйлестіру, құқық қорғау органдарының кәсіби дайындығын арттыру және ақпараттық қауіпсіздікке қатысты кешенді стратегия

әзірлеу маңызды. Жоғарыда аталған ғалымдардың пікірлері мен талдаулары киберқылмыспен күресте құқықтық және институционалдық базаны нығайтудың маңыздылығын айқындайды. Бұл құқықбұзушылықтарға қарсы тиімді күрес жүргізу үшін заңнамалық реформаларды жалғастырудың, жаңа қауіптерге дер кезінде әрекет етудің және мемлекеттік органдар мен жеке сектор арасындағы ынтымақтастықты күшейтудің қажеттілігін көрсетеді.

Қазақстан Республикасында ақпараттандыру және байланыс саласындағы қылмыстық құқықбұзушылықтарға қарсы күрес барысында шешілмеген бірқатар мәселелер бар. Бұл мәселелердің ішінде құқықтық реттеу, мамандардың жеткіліксіздігі, құрал-жабдықтардың жетіспеушілігі және халықаралық ынтымақтастықтың жеткілікті деңгейде болмауы секілді аспектілерді ерекше атап өтуге болады. Бұл мәселелерді тиімді шешу үшін кешенді тәсілдер мен заманауи технологияларды қолдану қажет.

Құқықтық реттеу мәселелері: Киберқылмыспен күрес саласындағы құқықтық реттеу – күрделі әрі үнемі дамуды қажет ететін бағыт. Қазақстан Республикасында ақпараттық қауіпсіздік мәселелерін реттейтін бірқатар заңдар мен нормативтік актілер бар, мысалы, «Қазақстанның киберқалқаны» тұжырымдамасы. Алайда, ақпараттық технологиялар үнемі дамып отырғандықтан, заңдар да жылдам өзгеріп отыруы керек. Қазіргі таңда заңдар қылмыскерлер қолданатын кейбір жаңа әдістер мен құралдарға толық сәйкес келмеуі мүмкін, бұл киберқылмыстарды ашу мен тергеуді қиындатады.

Сонымен қатар, Қазақстандағы заңнамалық базаны жетілдіру халықаралық стандарттарға сәйкес келуі тиіс. Халықаралық тәжірибе көрсеткендей, киберқылмысқа қарсы тиімді күрес елдердің өзара ынтымақтастығын және қылмыстық жауапкершілікті ортақ ережелер негізінде белгілеуді қажет етеді.

Мамандар тапшылығы: Ақпараттық қауіпсіздік саласындағы негізгі мәселелердің бірі – білікті мамандардың жеткіліксіздігі. Қазақстандағы құқық қорғау органдары мен мемлекеттік мекемелерде киберқауіптерді анықтайтын, оларды тиімді тергеп, болдырмайтын жоғары білікті кадрлар жеткіліксіз. Көптеген қызметкерлер заманауи технологиялар мен әдістемелерді қолдануға толық дайын емес. Осыған байланысты, киберқауіпсіздік мамандарын даярлау және қайта даярлау курстарын ұйымдастыру қажеттілігі туындап отыр. Бұл курстарда құқық қорғау қызметкерлері мен мамандары халықаралық тәжірибелерге негізделген ең заманауи технологиялар мен құралдармен жұмыс істеуді үйренуі тиіс.

Құрал-жабдықтардың жетіспеушілігі: Қазақстандағы құқық қорғау органдарының тағы бір мәселесі – заманауи құрал-жабдықтардың жетіспеушілігі. Киберқылмыспен күресу үшін қажетті арнайы бағдарламалық және техникалық жабдықтар болмауы тергеулердің тиімділігіне кері әсер етеді. Ақпараттық қауіпсіздік инциденттерін ашу және қылмыскерлердің ізін кесу үшін қазіргі заманғы құралдарды қолдану аса маңызды. Бұл құралдар деректерді қалпына келтіру, желілік шабуылдарды талдау және зиянды бағдарламаларды анықтау сияқты күрделі тапсырмаларды орындауға мүмкіндік береді.

Халықаралық ынтымақтастықтың жеткіліксіздігі: Киберқылмыспен күрес – тек ұлттық деңгейде ғана шешілмейтін мәселе, өйткені киберқылмыстардың көпшілігі трансұлттық сипатқа ие. Қазақстан үшін халықаралық ынтымақтастықты күшейту маңызды, себебі кибершабуылдар жиі халықаралық деңгейде жүзеге асырылады. Бірақ, елдер арасында ортақ құқықтық механизмдер мен процедуралардың болмауы тиімді ақпарат алмасуды қиындатады. Халықаралық деңгейде бірыңғай стандарттар мен келісімдер жасау, бірлескен операциялар өткізу, сондай-ақ трансшекаралық киберқылмыстарды тергеуге мүмкіндік беретін құқықтық негіздерді бекіту қажет.

Интерпол және Еуропол секілді халықаралық ұйымдардың қатысуымен жүзеге асырылатын бірлескен операциялар трансұлттық киберқылмыстарды сәтті ашу үшін жақсы мысал болып табылады. Қазақстан осындай ынтымақтастықты күшейту арқылы киберқауіптерге төтеп беру бойынша халықаралық күш-жігерге үлес қоса алады.

Азаматтардың цифрлық қауіпсіздік мәселелеріне бейімделуі: Құқық қорғау органдары мен үкіметтік құрылымдардың жұмысы азаматтардың цифрлық қауіпсіздік туралы хабардарлығын арттыруға бағытталуы тиіс. Қарапайым интернет қолданушылары киберқауіптердің, интернет-алаяқтықтың, фишингтің және басқа да кибершабуылдардың құрбанына айналып жатыр. Осы орайда, халық арасында цифрлық сауаттылықты көтеру, интернеттегі қауіпсіз мінез-құлық туралы ақпараттық науқандар өткізу қажет. Мектептер мен университеттерде кибергигиена бойынша арнайы бағдарламалар енгізу арқылы болашақ ұрпақтың цифрлық қауіпсіздік туралы хабардарлығын арттыру мүмкін болады.

Құқық қорғау органдарының біліктілігін арттыру: Құқық қорғау органдарының қызметкерлерін тұрақты түрде оқыту және қайта даярлау қажеттілігі де маңызды. Халықаралық тәжірибе көрсеткендей, киберқылмыспен күресу үшін құқық қорғау қызметкерлері жаңа технологиялар мен әдістерді меңгеруі керек. Тек осылай ғана қылмыстық құқық бұзушылықтарды анықтау мен тергеу үдерісінде жетістікке жетуге болады. Құқық қорғау органдарының қызметкерлері киберқауіпсіздік бойынша халықаралық тренингтер мен курстарға қатысуы олардың кәсіби деңгейін арттырады.

Профилактикалық мониторинг жүйесін енгізу:

Киберқауіптерді ерте анықтау үшін «Мемлекеттік техникалық қызмет» базасында мониторинг орталықтары құрылып, олар заманауи талдау құралдарымен жабдықталуы тиіс. Бұл орталықтар:

1. Кибершабуылдарға жедел әрекет ету мүмкіндігін қамтамасыз етеді.
2. Қылмыстық құқық бұзушылықтарды жоспарлау сатысында анықтап, олардың алдын алады.
3. Трансшекаралық қауіптерге уақытылы шара қолдануды қамтамасыз етеді.

Осылайша, Қазақстан Республикасында киберқылмыспен күресу үшін құқықтық реттеуді жетілдіру, заманауи технологиялар мен құралдарды қолдану, халықаралық ынтымақтастықты дамыту және азаматтардың цифрлық

сауаттылығын арттыру қажет. Кешенді шаралар қолдану арқылы елдегі ақпараттық қауіпсіздік деңгейін арттыруға және киберқылмыстардың алдын алуға болады.

ҚОРЫТЫНДЫ

Бұл докторлық диссертация ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды қарастырып, олардың қылмыстық-құқықтық және криминологиялық аспектілеріне баса назар аударады. Тараудың негізгі тұжырымдарын қорытындылау ерекше назар аударуды және одан әрі зерттеуді қажет ететін бірнеше маңызды жайттарды бөліп көрсетуге мүмкіндік береді.

Зерттеу барысында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объектілері мен субъектілерінің негізгі белгілері, сондай-ақ мұндай қылмыстық құқық бұзушылықтардың объективті және субъективтік жақтарының мәселелері анықталды. Қазақстанның қолданыстағы заңнамасы ақпараттық технологиялардың қарқынды дамуы жағдайында айтарлықтай жетілдіруді және бейімделуді талап ететіні анықталды. Талдау заңнамалық базаны нығайту және құқық қорғау органдары қызметкерлерін оқытудың кешенді бағдарламаларын әзірлеу қажеттігін көрсетті.

Ұсынылған ұсыныстардың маңыздылығы олардың Қазақстандағы ақпараттық қауіпсіздік деңгейін арттыруға әлеуетті әсер етуінде. Ұсынылған шараларды іске асыру мыналарға мүмкіндік береді: құқықтық қорғауды күшейтуге және қылмыстық заңнаманы киберқылмыстардың жаңа түрлеріне бейімдеуге; үкімет пен халықаралық құрылымдар арасындағы үйлестіруді және өзара іс-қимылды жақсарту; құқық қорғау органдары қызметкерлерінің біліктілігін арттыру және оларды киберқылмыспен күресу үшін қажетті техникалық құралдармен қамтамасыз ету; профилактикалық шараларды күшейту және ақпараттық қауіптерден қорғау әдістері туралы халықтың хабардарлығын арттыру.

Әрі қарайғы зерттеулердің келешегі киберқылмыстарды жіктеу мен талдаудың жаңа тәсілдерін әзірлеуді, сондай-ақ тәжірибеде ұсынылған шаралардың тиімділігін зерделеуді қамтиды. Киберқылмыскерлерді ынталандыруға әлеуметтік, экономикалық және психологиялық факторлардың әсерін зерттеуді жалғастыру қажет. Ұсынылған шараларды іске асыру мемлекеттік органдардың, жеке сектордың және халықаралық серіктестердің белсенді ынтымақтастығын талап етеді. Сондай-ақ жедел технологиялық прогресс жағдайында ақпараттық қауіпсіздік стратегиялары мен әдістерін жүйелі түрде жаңарту маңызды болып табылады.

Осылайша, ұсынылған диссертация ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға байланысты мәселелерді түсінуге және шешуге елеулі үлес қосады және Қазақстандағы ақпараттық қауіпсіздік деңгейін арттыру бойынша нақты қадамдарды ұсынады.

Зерттеудің мақсаты мен міндеттері толығымен орындалды. Жұмыс барысында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық белгілеріне жан-жақты талдау жүргізіліп, құқық қорғау қызметінің мәселелері айқындалып, заңнаманы жетілдіру және осындай қылмыстық құқық

бұзушылықтармен күрестің тиімділігін арттыру бойынша ұсыныстар әзірленді. Зерттеу ақпараттық технологиялардың қарқынды дамуымен байланысты құқықтық тетіктерді жетілдіру және оларды жаңа міндеттерге бейімдеу қажеттілігін көрсетті.

Зерттеу объектісі ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар болды, ал пәні осындай қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық және криминологиялық аспектілері болды.

Осы мақсатқа жету үшін жұмыста келесі міндеттер орындалды:

1. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауаптылықтың тарихи аспектілері зерттелді.

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

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

4. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық сипаттамасы берілді.

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

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

Талдау негізінде тұжырымдалған зерттеу гипотезасы расталды. Зерттеу көрсеткендей, технологияның дамуына және қылмыс жасау әдістерінің өзгеруіне сәйкес ақпараттандыру және байланыс саласындағы құқықтық тетіктер жетілдірілсе, бұл осы саладағы қылмыстық құқық бұзушылық деңгейінің төмендеуіне әкеледі.

Осылайша, жұмыс ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға байланысты мәселелерді түсінуге және шешуге елеулі үлес қосады және Қазақстандағы ақпараттық қауіпсіздік деңгейін арттыру бойынша нақты қадамдарды ұсынады. Әрі қарайғы зерттеулердің келешегі киберқылмыстарды жіктеу мен талдаудың жаңа тәсілдерін әзірлеуді, сондай-ақ тәжірибеде ұсынылған шаралардың тиімділігін зерделеуді қамтиды. Ұсынылған шараларды іске асыру мемлекеттік органдардың, жеке сектордың және халықаралық серіктестердің белсенді ынтымақтастығын, сондай-ақ жылдам технологиялық прогресс жағдайында ақпараттық қауіпсіздік стратегиялары мен тәжірибелерін жүйелі түрде жаңартуды талап етеді.

Зерттеудің қорытындысы ретінде, Қазақстан Республикасында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға

қарсы күрес мәселелері жан-жақты зерттеліп, тиісті қорытындылар мен ұсыныстар әзірленді. Бұл жұмыс қылмыстық құқықтық және криминологиялық аспектілерді қарастыра отырып, киберқылмыстарға қарсы күресудің кешенді жүйесін құрудың қажеттілігін айқындады.

Сондықтан, ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың қылмыстық-құқықтық және криминологиялық аспектілерін зерттеу өзекті болды, осы бағытта диссертациялық зерттеу нәтижесі бойынша келесідей қорытындылар жасалды:

1. Ақпараттандыру және байланыс саласында жасалатын қылмыстық құқық бұзушылықтар үшін жауаптылықтың тарихи аспектілерін зерттеу нәтижесінде олардың келесі кезеңдері анықталды: 1 – кезең «Ең алғашқы құқық бұзушылықтар мен телекоммуникация саласындағы заң бұзушылықтар 1960-1970 жылдары телекоммуникация саласындағы құқық бұзушылықтар технологиялық революцияның алғашқы толқынының нәтижесінде пайда болды»; 2 – кезең «Компьютерлік жүйелердің дамуы және алғашқы компьютерлік қылмыстық құқық бұзушылықтар 1980-1990 жылдары ақпараттық технологиялар қарқынды дамып, компьютерлік жүйелер өмірдің көптеген салаларына ене бастады»; 3 – кезең «Интернеттің таралуы және жаңа қылмыс түрлері 1990-2000 жылдар аралығында интернеттің жаһандық таралуы ақпараттық технологиялар саласындағы қылмыстардың жаңа кезеңін ашты». 4 – кезең «Қазіргі кезең 2000 жылдан бастап қазіргі уақытқа дейінгі кезең интернет пен ақпараттық технологиялардың жаппай таралуымен және дамуының күрделі кезеңі болып саналады».

2. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар ұғымының қазіргі қалыптасуын ашып,және оған теориялық талдау жасалды. Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасы мен Киберқауіпсіздік тұжырымдамасының жүзеге асуын ескере отырып, қазіргі цифрлық технологиялар даму кезеңінде қылмыстық құқық бұзушылықтар да ерекше сипатқа ие автормен ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтың теориялық сипатта авторлық анықтамасы берілді. Осылайша, *Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар дегеніміз* - «*ақпараттық жүйелерді, мәліметтер базасын және телекоммуникация, компьютерлік коммуникация желілерін заңсыз пайдалану арқылы жүзеге асырылатын, жеке және мемлекеттік деректерге қол жеткізу, оларды өзгерту немесе жою мақсатындағы қылмыстық құқық бұзушылықтар*».

3. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар үшін жауапкершілікті реттейтін нормативтік құқықтық базаны талдау және оның кемшіліктерін анықтау бойынша бірқатар өзгерістер енгізлу ұсынылды. Соған сәйкес келесі ұсыныстар енгізілді. Қазақстан Республикасы Қылмыстық кодексінің жалпы бөлімінің 3-бабының 41-1 тармағын мынадай ұғымдармен толықтыру қажет: «*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». Бұл ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық ұғымдарының дефиниялар түріндегі қоғамдық қауіпті әрекеттер мен әрекетсіздіктердің, ықтимал немесе туындайтын ауыр және аса ауыр зардаптардың негізгі белгілерін уақтылы нақты анықтауға мүмкіндік береді. Компьютерлік коммуникация және киберқауіпсіздік ұғымдарын заңнамаға нақтылау және енгізу құқықтық реттеуді жетілдіру, ақпараттық қауіпсіздік деңгейін арттыру, инновациялар мен технологиялық дамуды ынталандыру, экономикалық және ұлттық қауіпсіздікті қамтамасыз ету мақсаттарына негізделеді. Осылайша, құқықтық жүйені және ақпараттық қоғамды дамытуға маңызды үлес қосады.

Сонымен қатар ҚР ҚК 3 бабының 38 тармағына ҚР ҚК 205,206,208 баптарымен толықтыру ұсынылды, *яғни ірі залал және ірі мөлшер ретінде айлық есептік көрсеткіштен бір мың есе асатын мүлік құны немесе залал мөлшері ретінде* өзгерістер енгізу ұсынылды. Осылайша, ірі залал және ірі мөлшер ұғымдары қылмыстық құқық бұзушылықтың қоғамға тигізетін зиянының дәрежесін объективті бағалауға мүмкіндік береді, қылмыстық құқық бұзушылықтың ауырлығын нақты анықтап, құқық қорғау органдарының дұрыс әрекет етуін қамтамасыз етеді.

4. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың объективтік немесе субъективтік белгілерін талдау көрсеткендей, келесі қылмыстық құқық бұзушылықтар құрамын келесі редакцияда беру ұсынылды:

ҚР Қылмыстық кодексі 205-бап. Ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу

4 бөлігі. «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

1) адамдар тобының алдын ала сөз байласуымен;

2) 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».

5. ҚР Қылмыстық кодексінің 206 бабы 1 бөлігінің диспозициясын «*компьютерлік коммуникация*» ұғымымен толықтыру ұсынылды. Себебі Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру әрекеттері *компьютерлік коммуникация* желісі арқылы беріледі. Сондықтан біздің ойымызша, ҚР ҚК 206 бабының диспозициясы мынадай түрде тұжырымдалады: «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».

Сонымен қатар, ҚР Қылмыстық кодексінің 208 бабы 1-бөлігін диспозициясын «*компьютерлік коммуникация*» ұғымымен толықтыру ұсынылды. Себебі Себебі, ақпаратты құқыққа сыйымсыз иеленіп алу әрекеттері *компьютерлік коммуникация* желісі арқылы беріледі. 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». Ақпараттық технологиялардың дамуы мен кеңінен қолданылуы ақпараттық жүйелер мен телекоммуникация желілерінің маңызды рөлін көрсетеді. Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру әрекеттері компьютерлік коммуникация желісі арқылы жиі жүзеге асырылады. Сондықтан бұл ұғымды енгізу ақпараттық қауіпсіздікті қамтамасыз ету үшін құқықтық реттеудің нақтылығын арттыруға және ақпараттық құқық бұзушылықтарды нақты анықтап, оларға қарсы шараларды тиімді түрде қабылдауға мүмкіндік береді.

6. 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 ұсынылды: «*Киберқауіпсіздік - бұл компьютерлік жүйелерді, желілерді және деректерді рұқсатсыз қол жеткізуден, шабуылдардан және қауіптерден қорғауға бағытталған шаралар мен процестер жиынтығы*» анықтама ұғымымен толықтыру ұсынылды. Киберқауіпсіздік ұғымын енгізу қажеттілігі заңнамалық актілерді жетілдіру, халықаралық стандарттарға сәйкестікті қамтамасыз ету, киберқылмыстардың алдын алу және қоғамның ақпараттық қауіпсіздік деңгейін арттыру мақсаттарына негізделеді. Келтірілген өзгерістер ақпараттық қауіпсіздікті қамтамасыз ету жүйесін нығайтып, құқықтық реттеуді одан әрі жетілдіруге

мүмкіндік береді.

7. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың криминологиялық сипаттамасын жан – жақты талдау жасалды. Криминологиялық тұрғыдан алғанда, киберқылмыстармен тиімді күрес үшін бірқатар тұжырымдар жасауға болады. Біріншіден, профилактикалық шаралардың маңызы зор. Бұл халықты ақпараттық қауіпсіздік негіздеріне оқыту және құқық қорғау органдары қызметкерлерінің кәсіби біліктілігін арттыру арқылы жүзеге асуы тиіс. Екіншіден, қылмыстық жауапкершілік шараларын күшейту қажет. Ұйымдасқан киберқылмыстық топтардың әрекеттері үшін қатаң санкцияларды енгізу қылмыстардың алдын алуға мүмкіндік береді. Үшіншіден, құқық қорғау органдарын заманауи технологиялармен жабдықтау маңызды. Киберқылмыстарды анықтау және тергеу үшін арнайы бағдарламалық қамтамасыз ету мен техникалық құралдар қажет. Төртіншіден, киберқауіптерді зерттеу мен мониторинг жүргізетін орталықтарды құру маңызды. Мұндай орталықтар киберқауіптердің алдын алу және қылмыстық әрекеттерді дер кезінде анықтау үшін ақпаратты талдауға мүмкіндік береді. Киберқылмыспен күресудің негізгі тәсілдері мен әдістерін қарастырылды. Киберқылмыспен күресудің дәстүрлі әдістеріне құқық бұзушыларды қудалау мен жазалаудың құқықтық негіздерін жасауға бағытталған заңнамалық шаралар жатады. Заңдар мен ережелер ақпараттық технологияларды пайдалануды реттейді, киберқылмыстың әртүрлі түрлері үшін жауапкершілікті белгілейді, деректер мен жүйелерді қорғау шаралары қарастырылды. Дәстүрлі тәсілдің маңызды элементі киберқылмыскерлерді тергеу мен қудалауды қамтитын құқық қорғау қызметі болып табылады. Киберқылмыстардың алдын алудың заманауи әдістері озық технологиялар мен инновациялық тәсілдерді қолдануды қамтиды. Бұл әдістер үлкен деректерді талдау және күдікті әрекеттерді анықтау үшін жасанды интеллект пен машиналық оқыту жүйелерін енгізуді қамтиды. Сонымен қатар, киберқылмыстардың пайда болуына және дамуына әсер ететін күрделі факторлар қарастырылған. Қылмыскерлерді ынталандыруда, олардың жеке қасиеттері мен кәсіби дағдыларын қалыптастыруда әлеуметтік, экономикалық және психологиялық аспектілері талданды. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылық жасайтын қылмыскер тұлғасының шамамен әлеуметтік портреті әртүрлі сипаттамалар мен белгілерді қамтиды. Бұл ретте:

- 18-35 жасындағы;
- техникалық білім мен бағдарламалау дағдыларының жоғары деңгейіне ие.
- білімдерін зиянды бағдарламаларды, бұзу жүйелерін және басқа кибершабуылдарды жасау үшін пайдалана алады;
- қаржылық пайда, саяси немесе идеологиялық себептерге дейін болады. Кейбір киберқылмыскерлер жеке дұшпандықтан немесе назар аударту ниетінен әрекет етеді;
- жеке басын жасыру үшін анонимді желілер мен бүркеншік аттарды

пайдаланады;

- киберқылмыскерлердің білімі мен шығу тегі әртүрлі болады. Олар студенттер, ақпараттық технология саласындағы мамандары немесе арнайы білімі жоқ хакерлік дағдыларды өз бетімен үйренген адамдар болып табылады;

8. 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 ұсынылды: Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресу бойынша іс-шаралары оның ішінде нақты Халықаралық ынтымақтастықты нығайту: киберқылмыспен күресудегі белсенді халықаралық ынтымақтастыққа, оның ішінде міндетті ақпарат алмасуды және шетелдік серіктестермен бірлескен операцияларды жүргізуге міндеттемені заңмен бекіту. Трансшекаралық киберқылмысқа қарсы күреске бағытталған халықаралық келісімдер мен конвенцияларды ратификациялау ұсынылды. Осыған, Будапешт конвенциясы сияқты халықаралық келісімдерге қосылуы ұсынылды, 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 процедулар 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.

Будапешт конвенциясына қосылу Қазақстанға бірқатар артықшылықтар береді, олардың ішінде ең маңыздылары:

- Халықаралық ынтымақтастықтың нығаюы: Конвенцияға мүше елдер арасында ақпарат алмасу, трансшекаралық киберқылмыстарға жедел әрекет ету, және киберқылмыстарды тергеуде қажетті ресурстармен бөлісу мүмкіндігі артады. Бұл Қазақстанның құқық қорғау органдарына күрделі кибершабуылдарға жауап беру және оларды тергеу кезінде тиімді әрекет етуге мүмкіндік береді.
- Құқықтық базаны жетілдіру: Конвенция стандарттарына сәйкес, Қазақстанның қылмыстық кодексіне жаңа ұғымдар мен баптарды енгізу арқылы заңнаманы жетілдіру қажет болады. Бұл киберқылмыстарға қарсы жазаларды күшейтіп, құқықтық құралдардың ауқымын кеңейтеді.
- Цифрлық дәлелдемелерді жинау және сақтау: Конвенция электрондық

дәлелдемелерді жинау және пайдалану үшін халықаралық стандарттарды бекітеді. Бұл киберқылмыстарды тергеу және сот процесінде дәлелдерді қабылдау жүйесін жетілдіруге ықпал етеді.

- Экономикалық және инвестициялық тартымдылықтың артуы: Киберқауіпсіздік деңгейінің артуы шетелдік инвесторлар үшін Қазақстанды сенімді серіктес ретінде көрсетеді, бұл цифрлық экономика саласындағы инвестицияларды арттыруға ықпал етеді.

10. Профилактикалық мониторинг жүйесін енгізу ұсынылды: Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен қарсы күресте тиімді әрекет ету үшін халықаралық серіктестермен ақпарат алмасу және бірлескен операцияларды ұйымдастыру міндеттелуі қажет. Киберқауіптерді ерте анықтау үшін «Мемлекеттік техникалық қызмет» базасында мониторинг орталықтары құрылып, олар заманауи талдау құралдарымен жабдықталуы тиіс. Осы ұсынып отырған орталықтарымыздың негізгі функциясы Кибершабуылдарға жедел әрекет ету мүмкіндігін қамтамасыз ету, қылмыстық құқық бұзушылықтарды жоспарлау сатысында анықтап, олардың алдын алу және Трансшекаралық қауіптерге уақытылы шара қолдануды қамтамасыз етеді.

11. Оқу бағдарламасын әзірлеу және осы бағытта оқыту ұсынылды: 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 ұсынылды. Бұл оқу бағдарламасы заманауи кибершабуылдарды анықтау және тергеудің соңғы әдістерін, сондай-ақ халықаралық құқық нормаларын қамтуы қажет.

12. Халықтың цифрлық сауаттылығын арттыру ұсынылды: 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. Бұл шаралар құқық қорғау органдарына келіп түсетін киберқылмысқа қатысты шағымдардың санын азайтуға да ықпал етеді.

Қосымша ретінде төмендегідей мәселелер мен ұсыныстарды ескеруге болады:

Заңнамалық реформалардың маңыздылығы: Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарды құқықтық реттеудің жаңартылуы тек заңдар мен нормативтік актілерді қабылдаумен шектелмей, қылмыстық жауапкершіліктің нақты механизмдерін жетілдіруді қажет етеді. Бұл құқық бұзушылықтардың жаңа түрлерін анықтау және оларға сәйкес жазалау шараларын қарастыру маңызды. Әсіресе, халықаралық тәжірибені ескере отырып, киберқылмысқа қарсы күрес заңнамасын халықаралық стандарттарға сәйкес бейімдеу керек.

«Құқықтану» және «Құқық қорғау қызметі» бағыты бойынша болашақ құқық қорғау органдарының мамандарын дайындайтын бакалавр оқу бағдарламаларына «Жаңа кәсіптер мен құзыреттер атласына» сәйкес «Кибертергеуші» оқу бағдарламасын енгізу бойынша оқыту. Бұл оқу бағдарламасы Цифрлық ортада жасалған қылмыстық құқық бұзушылықтарды зерттейді. Киберқылмыстарды жасаудың жаңа құралдарын, мақсаттары мен арналарын қадағалайтын және талдайтын, заманауи ақпараттық технологияларды пайдалана отырып, оларға қарсы әрекет ететін маман иесін дайындайды.

Киберқауіпсіздік мәдениетін дамыту: Елде киберқауіпсіздік мәдениетін қалыптастыру – маңызды міндеттердің бірі. Мемлекеттік мекемелер, жеке сектор, оқу орындары және жалпы қоғам кибергигиена және цифрлық қауіпсіздік ережелерін ұстануы қажет. Бұл мақсатта отандық IT-компаниялар мен үкімет бірлесе отырып, киберқауіпсіздікті сақтау бойынша стандарттар мен ережелерді әзірлеп, оларды қолдануды насихаттауы керек.

Технологиялық инновациялар мен отандық шешімдерді дамыту: Қазақстанда киберқауіпсіздік мәселелерін шешу үшін отандық технологиялық өнімдерді дамыту мен қолдауға баса назар аудару қажет. Шетелдік бағдарламалық қамтамасыз етуге толық тәуелді болудан бас тартып, отандық әзірлемелерді қолдау ақпараттық қауіпсіздік жүйелерінің қауіпсіздігін арттырады. Мемлекет пен жеке сектордың бірлескен күш-жігері арқылы ақпараттық технологиялар саласында инновациялық жобаларды жүзеге асыру – елдегі цифрлық қауіпсіздіктің ұзақ мерзімді перспективадағы кепілі.

Қорыта келе, бұл диссертациялық зерттеу ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтардың өзекті мәселелерін кешенді түрде талдап, Қазақстан Республикасында киберқауіпсіздікті қамтамасыз ету жолдарын қарастырды. Зерттеуде жасалған тұжырымдар мен ұсыныстар елдің құқық қорғау жүйесін жетілдіруге, заңнаманы жаңартуға және халықаралық деңгейде ынтымақтастықты арттыруға үлес қосуға мүмкіндік береді.

Зерттеу нәтижелері ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған мемлекеттік саясатты жетілдіру және цифрлық қауіп-қатерлерге қарсы тұруда құқық қорғау жүйесінің тиімділігін арттыру үшін бағалы ақпарат көзі бола алады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Тоқаев, Қ.К. (2024). «Әділетті Қазақстанның экономикалық серпіні» Қазақстан халқына Жолдау, 2024 жылғы 2 қыркүйек. Қол жеткізу режимі: https://www.akorda.kz. 30.10.2024

2. Қазақстан Республикасының Үкіметі. (2017). «Киберқауіпсіздік тұжырымдамасы – «Қазақстанның киберқалқаны»» бекітілген қаулысы, 30 маусым 2017 ж., № 407. «Әділет» ақпараттық-құқықтық жүйесі. Қол жеткізу режимі: https://adilet.zan.kz. 15.08.2024

3. Қазақстан Республикасының Президенті. (2021). Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасын бекіту туралы Жарлығы, 15 қазан 2021 ж., № 674. «Әділет» ақпараттық-құқықтық жүйесі. Қол жеткізу режимі: https://adilet.zan.kz. 13.05.2024

4. Қазақстан Республикасының Бас прокуратурасы. Қазақстан Республикасының Қылмыстық кодексі бойынша құқық бұзушылықтар статистикасы (205-213 бап 2020-2024 жж.). Қол жеткізу режимі: https://qaz.stat.gov.kz. 22.09.2024

5. Байтенова, Н.А. «Ақпараттық қауіпсіздіктің құқықтық аспектілері: Қазақстан тәжірибесі». Алматы: Қазақ университеті баспасы, 2021. – 105 б.

6. Мусаев, С.Т. «Киберқауіпсіздік және ақпараттық технологиялар саласындағы заңнамалық өзгерістер». Юрист журнал, №3, 2022. – 45-58 б.

7. Момынов, К.А. «Ақпараттық қоғам және киберқылмыстар: Қазақстандағы жағдай». Вестник Евразийского национального университета, №5, 2021. – 28-39 б.

8. Сидорова, О.В. «Законодательные меры борьбы с киберпреступностью в международной практике». Международное право, 2020. – 92-104 с.

9. Ахметов, Ж.Т. «Киберқылмыстар және олардың алдын алу шаралары». Құқық қорғау органдарының қызметі журналы, №6, 2021. – 17-25 б.

10. Ерғалиев, А.К. «Киберқауіпсіздік: Қазақстандағы нормативтік құқықтық актілер». Заң және қоғам, №2, 2022. – 63-74 б.

11. Серікбай, Е.Б. «Ақпараттық технологиялар және киберқауіпсіздік». Ғылым және технологиялар журналы, №4, 2020. – 45-59 б.

12. Темірханова, Ж.М. «Қазақстандағы ақпараттық қауіпсіздік мәселелері». Вестник КазНУ, Юридические науки, №1, 2021. – 102-115 б.

13. Иванов, П.Р. «Международный опыт борьбы с киберпреступностью». Москва: Юридическая литература, 2019. – 230 б.

14. Ким, А.С. «Кибершабуылдарға қарсы құқықтық реттеу». Қазақстан Республикасы Құқық және заң журналы, №5, 2022. – 82-96 б.

15. Жалғасова, М.Е. «Интернет-алаяқтықпен күресу әдістері». Заңгер журналы, №7, 2021. – 12-19 б.

16. Абдрахманова, Т.К. «Киберқылмыстардың алдын алу: халықаралық тәжірибе». Вестник Академии МВД, №9, 2020. – 95-110 б.

17. Захаров, И.И. «Законодательное регулирование кибербезопасности в ЕС

и СНГ». Международное право и политика, №6, 2019. – 73-85 с.

18. Джамалиев, С.А. «Правовые аспекты киберугроз». Алматы: Юридический институт МВД, 2021. – 210 б.

19. Берова Д.М. (2020). Правовое регулирование ответственности за преступления в сфере компьютерной информации: проблемы и перспективы развития. Пробелы в российском законодательстве, 13(3), 121-123 с.

20. Бычков В.В., Харченко С.В. (2021). О понятии компьютерного преступления. КБК 67.408 Б 83, - 26 с.

21. Қабылов, Н.К. «Киберқылмыспен күрес: Қазақстандағы құқықтық негіздер». Заң және құқық журналы, №4, 2022. – 31-45 б.

22. Бабанина В., Ткаченко И., Матиушенко О., Крутевич М. (2021). Киберпреступность: история становления, современное состояние и способы противодействия. Научно-практический журнал, Т. 10, № 38, б. 113. DOI: https://doi.org/10.34069/AI/2021.38.02.10. 22.07.2024.

23. Горбачева Е.В. (2016). История информационного законодательства. XX век. Начало. Правовая информатика, (3), 145-148 б.

24. Матвеев В., Никитченко О.Е., Стефанова Н., Хрипко С., Ищук А., Паско К. (2021). Киберпреступность как дискурс интерпретации: семантика речевого спокойствия и психологическая мотивация к актуальным проблемам. Международный журнал информатики и сетевой безопасности, Т. 21, №8, с. 203. DOI: 10.22937/IJCSNS.2021.21.8.27.

25. Амириан Фарсани А. Криминологиялық тұрғыдан киберқылмысты талдау // Бизнес және әлеуметтік ғылыми зерттеулер журналы. 2020. Т. 1, № 7. 79-84 б . ISSN 2690-0866 (басып шығару), ISSN 2690-0874 (онлайн).

26. Думчиков М., Юнин О., Несторова Н., Борко А., Ерменчук О. (2021). Криминологические и криминалистические характеристики форм хищений денежных средств с использованием информационных технологий. Международный журнал информатики и сетевой безопасности, Т. 10, № 41, б. 131. DOI: 10.34069/AI/2021.41.05.13.

27. Мұстафи М. Құқықтық әділеттілік және қылмыстың пайда болуының тарихи аспектілері // Еуропалық пәнаралық зерттеулер журналы. 2015. 1-том, № 3. Б. 79. ISSN 2411-958X (басып шығару), ISSN 2411-4138 (онлайн).

28. Харитонов Е., Харитонова О., Толмачевская Ю., Фасий Б., Ткалич М. Ақпараттың қауіпсіздігі және оны құқықтық қамтамасыз ету құралдары // Amazonia Investiga. 2019. 8-том, № 19. ISSN 2322-6307., - 255 б.

29. Ақшатаева Дж.Б. , Байдалы А.Ж. Ақпарат және коммуникация саласындағы қылмыстардың ерекшеліктері // ОҚМУ ғылыми еңбектері, бб.76-78

30. Пернебекова А.П. Ақпараттық қауіпсіздікті қамтамасыз етудегі Қазақстан мен Ресей заңнамасының ерекшеліктері // Хабаршысы Л.Н. Гумилев атындағы Еуразия Ұлттық университеттер . 2021. № 4(137). «Журналистика» сериясы. ISSN: 2616-7174 , eISSN : 2663-2500.

31. Сәулен Н., Жамбаев Е.С., Сағадиев А.Н. Цифрландыру және

ақпараттандыру конституциялық құндылықтарды өзгерту триггерлері ретінде // Хабаршы Л.Н. Гумилев атындағы Еуразия Ұлттық университеттер . 2021. № 4(137). «Журналистика» сериясы . Астана, Қазақстан: Еуразия Ұлттық университеттер . ISSN 2616-7174 , eISSN 2663-2500.-26 б.

32. Бижанова, А.Р., Мейірбекова, Г.Б., Жүнісова, Г.Ә. (2021). Ақпараттандыру мен байланыс саласындағы қылмыстық құқық бұзушылықтар: ComputerLik қауіпсіздікті қамтамасыз ету технологиясы. Қарағанды университетінің хабаршысы, №L3, 104-112 беттер. DOI: 10.31489/2021L3/104-112.

33. Рүстемова Г.Р. (2020). Профилактика уголовных правонарушений в сфере информации и коммуникаций в Республике Казахстан. Вестник Могилевского института Министерства внутренних дел, (1), бб. 58-63. http://elib.institutemvd.by/handle/MVD_NAM/4844. 10.06.2024

34. Середа Е.В., Чесноков Н.А. (2020). Цифровая трансформация органов прокуратуры Российской Федерации и стран СНГ. Вестник: Педагогические науки, (2), 835 с.

35. Қазақстан Республикасының Қылмыстық кодексі. – Астана: Қазақстан Республикасының Әділет министрлігі, 2023. 205-213-баптар. https://adilet.zan.kz/kaz/docs/K1400000226#z1703 15.09.2024

36. Council of Europe. Convention on Cybercrime (Budapest Convention), 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (жүгінген уақыты: 18.09.2024).

37. Есжанов, М.Қ. Ақпараттық технологиялар саласындағы қылмыстар: құқықтық реттеу және алдын алу шаралары. Заңгерлік зерттеулер журналы, 2022, №3, 58-64 б.

38. Сәдуақасов, А.Т. Кибералаяқтық және ақпараттық қауіпсіздікті қамтамасыз ету мәселелері. Құқық және мемлекет журналы, 2023, №2, 89-95 б.

39. Оразбеков, А.Б. Телекоммуникация саласындағы қылмыстық құқық бұзушылықтар және олардың алдын алу шаралары. Алматы: Қазақ университеті баспасы, 2022. 85-90 б.

40. Ерғалиев, С.М. Ақпараттық технологиялар және коммуникациялар саласындағы қылмыстар: құқықтық реттеу және халықаралық тәжірибе. Қазақстанның заңгерлік зерттеулер журналы, 2023, №1, 112-118 б.

41. Есжанов, М.Қ. Цифрландыру және ақпараттық қауіпсіздік: құқықтық және техникалық аспектілер. Қауіпсіздік және құқық журналы, 2023, №4, 45-52 б.

42. Феткулин Р.Р., Арюков А.К. Цифрлық ақпарат саласындағы қылмыстар: түсінігі мен түрлері // Байкал зерттеу журналы. 2019. Т. 10, № 3. – Қазан: Қазан инновациялық университеті атындағы. В.Г. Тимирясова (ХЭУ), Ресей Федерациясы. – DOI 10.17150/ 2411-6262.2019.10(3) .17. – ISSN 2411-6262. – ӘОЖ 343.3/.7. – Байкал мемлекеттік университетінің электронды ғылыми журналы. – Желіден кіру: http://brj-bguep.ru 10.02.2024

43. Бегишев И.Р. Цифрлық ақпарат айналымы саласындағы қылмыстардың түсінігі мен түрлері : реферат дисс. 12.00.08 – қылмыстық құқық және

криминология; қылмыстық атқару құқығы. – Қазан, 2017. – Қылмыстық құқық және криминология кафедрасы,- 69-74 б.

44. Рахманова Е.Н., Пинкевич Т.В. Цифрлық қылмыс концепциясы // Алғаштар Экономика, бизнес және менеджмент зерттеулерінде . - 2020. - Т. 138. - «Қазіргі заманғы менеджмент үрдістері және цифрлық экономика: аймақтық дамудан жаһандық экономикалық өсуге дейін» 2-ші Халықаралық ғылыми-практикалық конференция (MTDE 2020), 42-47 б.

45. Матвеев В., Никитченко О.Е., Стефанова Н., Хрипко С., Ищук А., Ищук О., Бондарь Т. Экономикалық кеңістіктегі киберқылмыс: Психологиялық мотивация және семантикалық-терминологиялық ерекшеліктер // Информатика және желілік қауіпсіздік халықаралық журналы. – 2021. – Т. 21, № 11. – 135-б.

46. Қазақстан Республика Қазақстан Республикасының 2016 жылғы 28 наурыздағы № 476-V Заңдары «Ақпарат саласындағы қылмыстық әрекетке қарсы іс-қимыл бойынша ұжымдық қауіпсіздік туралы шарттар. Ұйымға мүше мемлекеттердің өзара іс-қимылы туралы хаттамаларды ратификациялау туралы «[Электрондық ресурс]. – «Әділет» құқықтық анықтамалық жүйесінен қолжетімділік Қазақстан Республикалар . – Кіру режимі: https://adilet.zan.kz/kaz/docs/Z1600000476. 10.03.2024

47. Қазақстан Республикасының Қылмыстық кодексі. 205-бап. Ақпаратқа, ақпараттық жүйеге немесе телекоммуникация желісіне заңсыз қол жеткізу [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/205.htm 10.03.2024

48. Қазақстан Республикасының Қылмыстық кодексі. 206-бап. Ақпаратты заңсыз жою немесе өзгерту [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/206.htm 12.03.2024

49. Қазақстан Республикасының Қылмыстық кодексі. 207-бап. Ақпараттық жүйенің немесе телекоммуникация желілерінің жұмысын бұзу [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/207.htm 12.03.2024

50. Қазақстан Республикасының Қылмыстық кодексі. 208-бап. Ақпаратты заңсыз алу [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/208.htm

51. Қазақстан Республикасының Қылмыстық кодексі. 209-бап. Ақпаратты беруге мәжбүрлеу [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/209.htm 15.03.2024

52. Қазақстан Республикасының Қылмыстық кодексі. Мақала 210. Зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/210.htm 15.03.20214

53. Қазақстан Республикасының Қылмыстық кодексі. 211-бап. Қолжетімділігі шектелген электрондық ақпараттық ресурстарды заңсыз тарату [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-

kz.com/ka/ugolovnyj_kodeks/211.htm 16.03.2024

54. Қазақстан Республикасының Қылмыстық кодексі. 212-бап. Заңсыз мақсаттарды көздейтін интернет-ресурстарды орналастыру жөніндегі қызметтерді көрсету [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/212.htm 16.03.2024

55. Қазақстан Республикасының 2014 жылғы 3 шілдедегі No 226-V Қылмыстық кодексі. 213-бап. Абоненттік ұялы байланыс құрылғысының, абоненттік сәйкестендіру құрылғысының сәйкестендіру кодын заңсыз өзгерту, сондай-ақ абоненттік құрылғының сәйкестендіру кодын өзгертуге арналған бағдарламаларды жасау, пайдалану, тарату [Электрондық ресурс]. – Қол жеткізу режимі: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/213.html 16.03.2024

56. Қазақстан Республикасының Бас прокуратурасы. Қылмыстық құқық бұзушылықтар статистикасы (2020-2024). URL: https://qaz.stat.gov.kz 03.11.2024

57. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. – М.: Палеотип; Логос, 2009. – 148 с.

58. Борчашвили И.Ш. Комментарий к уголовному кодексу Республики Казахстан особенная часть, Том 2, Алматы «Жеті жарғы» 2021 г, - 1135 с.

59. С. М. Рахметова, И. И. Рогова Комментарий к УК Республики Казахстан — 4-е изд., доп. и перераб. — Алматы: Изд-во «Норма-К», 2016. — 752 с.

60. Қазақстан Республикасының «Ақпараттандыру туралы» Заңы. Қазақстан Республикасы Үкіметінің ресми порталы, 2024. URL: https://adilet.zan.kz/kaz 11.10.2024

61. Абылкасимова, Н.А. «Ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етудегі заңнамалық шаралар». Құқық және мемлекет журналы, №2, 2020. – 33-45 б.

62. Мусин, Б.К. «Қазақстандағы ақпараттық қауіпсіздіктің құқықтық аспектілері». Юрист журнал, №4, 2021. – 56-68 б.

63. Ермаков, Д.А. «Законодательное регулирование киберугроз в контексте международного права». Москва: Юридическая литература, 2020. – 185 б.

64. Лазарева, Т. Виртуалды объектілер және құқық: құқықтық аспектілер мен сын-қатерлер. Құқықтық хабаршы, 2023, 45-47 б.

65. Павлов, А. Инновациялық технологиялар және киберқауіпсіздікті қамтамасыз ету. Технологиялық журнал, 2022, 78-82 б.

66. Пандей, А., Сайяд, М. Киберқауіпсіздіктегі жасанды интеллект және заттар интернеті: сын-қатерлер мен мүмкіндіктер. Ақпараттық технологиялар журналы, 2021, 112-115 б.

67. Маштаков, И. В. Киберқылмыс және виртуалды объектілер: құқықтық мәселелер және олардың шешімдері. Құқық және қоғам, 2023, 61-64 б.

68. Кучин, А.В. (2017). Киберпреступность и информационная безопасность: теория и практика борьбы. Москва: Юрайт., С. 88-112.

69. Соловьев, А.В., Тихомиров, М.Н. (2019). Информационное право и кибербезопасность: современные вызовы. Санкт-Петербург: Проспект., С. 135-

148.

70. Номоконов, В., Тропина, Е. Киберқылмыстар және оларды жасау құралдары. Қылмыстық құқық журналы, 2022, 77-80 б.

71. Бозе, А. Компьютерлік жүйелер және желілердегі кибершабуылдар: қауіптер мен шешімдер. Киберқауіпсіздік журнал, 2023, 112-115 б.

72. Кучерков, В. Зиянды бағдарламалық қамтамасыз ету: киберқылмыстарды жасау құралдары. Ақпараттық технологиялар журналы, 2022, 56-60 б.

73. Оганов, А. Кибершабуылдарды зерттеу: әдістер мен тәсілдер. Құқықтық зерттеулер журналы, 2023, 92-95 б.

74. Марас, М. Трафикті шифрлау және анонимдеу: киберқылмыстардың тергеу мәселелері. Киберқауіпсіздік зерттеулері, 2022, 77-80 б.

75. Оганов, А. Киберқылмыстарды анықтау және құжаттау: негізгі мәселелер мен қиындықтар. Құқықтық зерттеулер журналы, 2023, 91-93 б.

76. Амос, Зак. Жасанды интеллекттің киберқылмыстарды тергеудегі рөлі және оның қиындықтары. Киберқауіпсіздік және жасанды интеллект, 2023, 33-35 б.

77. Григорьев, В.В. Современные методы расследования преступлений, совершенных с использованием информационных систем // Форум молодых ученых. 2023, 78-86 с.

78. Оганов, А.А. Оперативно-разыскная характеристика киберпреступлений в отношении несовершеннолетних с использованием информационно-телекоммуникационных сетей // Юридические науки. 2019, 19-21б.

79. Finprom.kz. (2023). Незримые: лишь 5% уголовных дел по хакерским преступлениям в Казахстане доходит до суда. (с. 35-50).

80. Қасымов, Ә.Б. «Ақпараттық қауіпсіздік және құқықтық жауапкершілік». Вестник КазНУ, Юридические науки, №2, 2021. – 63-74 б.

81. Наумов, В. Киберқылмыстың субъективтік жағы және оның құқықтық реттелу мәселелері. Құқықтық зерттеулер журналы, 2023, 152-155 б.

82. Павлов, А. Халықаралық ынтымақтастық және киберқылмыстарды тергеу. Киберқауіпсіздік және құқық журналы, 2022, 178-182 б.

83. Француз, Ж. Қылмыс ниеті және құқықтық жауапкершілік: француздық тәжірибе. Қылмыстық құқықтың халықаралық зерттеулері, 2023, 67-70 б.

84. Лав, Л. Лори Лав және АҚШ үкіметінің жүйелеріне хакерлік шабуыл: іс тарихы. Киберқылмыс және қауіпсіздік, 2014, 95-98 б.

85. Зык, А.В. Киберқылмыстардың мақсаттары: қаржылық пайдадан саяси және идеологиялық себептерге дейін. Киберқауіпсіздік зерттеулері, 2023, 85-89 б.

86. Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления: понятие, классификация, международное противодействие // Legal Order and Legal Values. 2023. Vol. 1. No. 1. URL: https://www.lawandorder-donstu.ru 22.02.2024

87. Байжанов, Қ.Т. (2024). Киберқылмыспен күрес саласындағы заңнамалық реформалар. Қазақстан құқықтық зерттеулер журналы, №1, 91-96 б.

88. Приказ ФАС России от 08.08.2019 N 1073/19 «Об утверждении методических рекомендаций».

89. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 12.06.2024) (с изм. и доп., вступ. в силу с 06.07.2024). Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

90. Кириленко, В.П., Алексеев, Г.В. Киберпреступность и цифровая трансформация (Cybercrime and Digital Transformation). Theoretical and Applied Law. 2021. No. 1(7). С. 39-53.

91. E4J University Module Series: Cybercrime. Module 3: Legal Frameworks and Human Rights. 2019. URL: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/legal-frameworks-and-human-rights.html (жүгінген уақыты: 07.07.2024).

92. Витвицкая, Е.А. Киберқылмыстар және олардың ресейлік қылмыстық құқықтағы біліктілігі. Мәскеу, 2019., 127-130 б.

93. Сауд Арабиясы. Киберқылмыстар туралы заң. Сауд Арабиясының Әділет министрлігі, 2017., 45-47 б.

94. Гончаренко, И.В. Компьютерлік ақпарат саласындағы қылмыстар: оқу құралы. Мәскеу: Юнити-Дана, 2020., 78-81 б.

95. Шарипов, Б.А. Ақпараттық қауіпсіздік және киберқылмыстар: қылмыстық-құқықтық және криминологиялық талдау. Алматы: Қазақ университеті, 2021., 92-95 б.

96. Лебедев, А.В. Киберқылмыстарды тергеу: соттық тәжірибе және құқықтық мәселелер. Санкт-Петербург: Питер, 2022., 56-159 б.

97. Смирнов, И.В. Блокчейн және киберқылмыстар: құқықтық реттеу мәселелері. Мәскеу: Норма, 2023., 66-68 б.

98. Трофимов, Н.А. Компьютерлік қылмыстар: құқықтық аспектілер. Екатеринбург: УрФУ, 2020., 09-112 б.

99. Темиралиев Т.С., Омаров Е.А. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения. УДК 343.00. Алматы, 2024. 143-146 б.

100. Гончаров А.А. Киберқылмыстар үшін жаза тағайындаудың ерекшеліктері. Заң ғылымдарының негіздері. Мәскеу: Юрайт, 2022. 154-157 б.

101. Жаңабаев Е.К. Қазақстан Республикасындағы қылмыстық құқық және киберқылмысқа қарсы күрес. Астана: Фолиант, 2023. 198-202 б.

102. Нұрғожаев С.Ж. Ақпараттық қылмыстарды тергеудің құқықтық аспектілері. Құқық қорғау саласындағы зерттеулер. Алматы, 2024. 88-91 б.

103. Маслов В.П. Киберқылмыстар үшін жаза тағайындаудың халықаралық тәжірибесі. Халықаралық құқық журналы. Мәскеу, 2021. 43-46 б.

104. Пак А.В. Киберқауіпсіздікті қамтамасыз етудегі профилактикалық шаралар. Құқық және технологиялар журналы. Алматы, 2023. 120-123 б.

105. Чернов В.А. Экстрадиция және халықаралық құқықтағы киберқылмыс мәселелері. Мәскеу, 2020. 74-77 б.

106. Интерпол. Cybercrime Report: Global Trends and Law Enforcement

Challenges. Interpol Annual Report. 2022. 59-63 б.

107. Council of Europe. Convention on Cybercrime (Budapest Convention). 2001.

108. Финансовые технологии и киберпреступность. Сборник материалов международной конференции. Москва: Научный центр, 2020. 55-58 б.

109. Kumar, A., Sinha, R. Cybercrime Legislation in India: Emerging Trends and Challenges. Journal of International Law, 2019. 91-94 б.

110. BBVA. Inside the Mind of a Cybercriminal. BBVA Blog, 2020. 44-46 p.

111. Jabara, A., Al-Shibli, M., & Abu Issa, H. (2020). The Specificity (Problems) of the Moral Element in Cyber Crimes. Jadara University. 53-55 p.

112. Parkin, S. (2017). The British hacker who was wanted by the FBI. The Guardian. 112-114 p.

113. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). 87-89 p.

114. Зак Амос. Как искусственный интеллект улучшает цифровую криминалистику. Unite.AI, 2024. С. 98-100.

115. Chetry, A., & Sharma, U. Anonymity in Decentralized Apps: Study of Implications for Cybercrime Investigations. International Journal of Experimental Research and Review, 2023. 44-46 p.

116. Maras, M. Cybercrime and its Challenges for Law Enforcement. Criminal Justice Review, 2016. 61-63 p.

117. Adu, M. K., Alese, B. K., & Adewale, O. S. Mitigating Cybercrime and Online Social Networks Threats in Nigeria. Proceedings of the World Congress on Engineering and Computer Science, 2014. 78-80 p.

118. Wheelans, A. Cybercrime: International Implications on New Zealand Strategy. Master's Dissertation, University of Canterbury, 2022. 121-123 p.

119. Улитин И.Н. Факультативные признаки субъективной стороны в составах преступлений против жизни и здоровья: теоретико-прикладное исследование. Краснодар: Кубанский государственный университет, 2021. С. 45-47.

120. Прохорова М.Л. Значение субъективной стороны в уголовном праве. Краснодар: Кубанский государственный университет, 2021. С. 72-75.

121. Оразов М.Қ. Ақпараттық қауіпсіздік: Қазақстандағы заманауи үрдістер мен технологиялық шешімдер. Алматы: ҚазҰУ баспасы, 2021. 120-123 б.

122. Иванов А.В. Киберпреступления: классификация и проблемы правоприменения. Вестник уголовного права, 2019. С. 87-92.

123. United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. New York: United Nations, 2020. 65-68 б.

124. Жұмағұлов А.Б. Қазақстандағы киберқауіпсіздік жүйесін нығайту: мәселелер мен шешімдер. Мемлекеттік басқару журнал, 2022. 101-105 б.

125. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2021: Mapping the Cybersecurity Threats. Athens: ENISA, 2021. 49-52 p.

126. Темирбаев С.Е. Киберқылмыспен күрес саласындағы заңнамалық реформалар. Қазақстан құқық журналы, 2023. 67-70 б.

127. Maras M.-H. Cybercrime and its Challenges for Law Enforcement. Criminal Justice Review, 2019. 112-115 p.

128. Власова, А.Ю. Психология киберпреступников: мотивация и особенности личности. Вестник психологии и права, 2021, №4, 145-150 б.

129. Жұмаділов, Қ.С. Киберқылмыстардағы жас ерекшеліктері және гендерлік аспектілер. Қазақстан криминологиясы журналы, 2023, №2, 89-94 б.

130. Оразғали, Ә.Б. Киберқылмыспен күрестегі әлеуметтік және экономикалық факторлардың рөлі. Қылмыстық құқық және криминология журнал, 2022, №3, 101-105 б.

131. Бекмұхамедов, Ж.С. Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз етудің құқықтық негіздері. Алматы: Заң, 2023, 130-135 б.

132. Ахметов, М.Ә. Киберқылмысқа әсер ететін мәдени және білім беру факторлары. Қоғам және заң, 2023, №5, 76-82 б.

133. Есенғазиев, Т.Қ. Киберқауіпсіздіктің техникалық аспектілері: Қазақстандағы жағдай. Ақпараттық технологиялар журналы, 2024, №1, 45-49 б.

134. United States Department of Justice. Computer Fraud and Abuse Act (CFAA), 1986. URL: https://www.justice.gov/criminal-ccips/computer-fraud-and-abuse-act 23.03.2024

135. United States Department of Homeland Security. Cybersecurity and Infrastructure Security Agency (CISA), 2018. URL: https://www.cisa.gov 29.03.2024

136. European Union Agency for Cybersecurity (ENISA). Network and Information Security (NIS) Directive, 2016. URL: https://www.enisa.europa.eu 20.04.2024

137. European Commission. General Data Protection Regulation (GDPR), 2018. URL: https://ec.europa.eu/info/law/law-topic/data-protection_en 20.04.2024

138. National Center of Incident Readiness and Strategy for Cybersecurity (NISC). Cybersecurity Basic Act, 2014. URL: https://www.nisc.go.jp 25.05.2024

139. Korea Internet & Security Agency (KISA). Korea Cybersecurity Act, 2015. URL: https://www.kisa.or.kr 15.08.2024

140. Ministry of Electronics and Information Technology, Government of India. Information Technology Act, 2000. URL: https://www.meity.gov.in/content/information-technology-act 13.08.2024

141. Ресей Федерациясының Қылмыстық кодексі. 272-бап: Компьютерлік ақпаратқа рұқсатсыз қол жеткізу. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/9e76877b7b27f2deeb8000cd7422b21c70f1066d 20.08.2024

142. Гостехкомиссия России. URL: https://www.gost.ru 20.05.2024

143. United Nations General Assembly. UN Resolution on Cybersecurity. URL: https://www.un.org/cybersecurity 20.05.2024

144. «Цифрлық экономика» бағдарламасы. Ресей Федерациясы Үкіметінің

ресми порталы. URL: http://government.ru/en/projects/selection/743/35804/ 20.08.2024

145. «Жеке деректер туралы» заң. Ресей Федерациясы. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ 22.09.2024

146. United Nations Office on Drugs and Crime (UNODC). International Cooperation on Cybercrime. URL: https://www.unodc.org 01.10.2024

147. Council of Europe. Convention on Cybercrime (Budapest Convention), 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 02.10.2024

148. INTERPOL. Global Complex for Innovation (IGCI), 2015. URL: https://www.interpol.int/en/Who-we-are/Global-complex-for-innovation 20.10.2024

149. European Union Agency for Cybersecurity (ENISA). ISO/IEC 27001 Standard on Information Security. URL: https://www.enisa.europa.eu 15.10.2024

150. Қазақстан Республикасы. «Ақпараттандыру туралы» заң. URL: https://adilet.zan.kz/kaz 20.09.2024

151. Лонге, О. «Қылмыстық мақсатта ақпараттық және коммуникациялық технологияларды қолдану: Африка тәжірибесі». Journal of African Law, №3, 2020. – 75-88 б.

152. Жарова, А. «Ақпараттық-коммуникациялық технологиялар қауіпсіздігін қамтамасыз етудегі құқықтық шаралар». Мәскеу: Юридическая наука, 2019. – 225 б.

153. Цюрих Ашық Репозиторийі. «Еуропалық Одақтың ақпараттық-коммуникациялық технологияларды реттеудегі қылмыстық заңнамасы». Zurich Open Repository, 2015. – 120 б.

154. Alves, T., Dream, S. «Виртуалды кеңістіктегі қылмыстар және ақпараттық қауіпсіздік стратегиялары». International Journal of Cybersecurity, №2, 2020. – 89-104 б.

155. Кавин, С., Братсук, И. «Германияның киберқауіпсіздікке қатысты заңнамалық базасы». Европейское право и политика, №4, 2021. – 42-56 б.

156. Мехта, Н. «Киберқұқық және ақпараттық технологиялар дәуіріндегі заңдылық мәселелері». Үндістан: Legal World Publishing, 2020. – 168 б.

157. Мусаткина, А.А. «Ресей Федерациясындағы ақпараттық қауіпсіздік және қылмыстық жауапкершілік». Құқық және экономика журналы, №5, 2021. – 63-77 б.

158. Жұмаділов, Қ.С., & Әлиев, А.Т. Киберқылмыстарға қарсы заңнамалық шаралар: Қазақстан мен халықаралық тәжірибені салыстыру. Қазақстанның құқықтық зерттеулер журналы, 2023, №2, 68-74 б.

159. Омаров, Б.Р. Киберқауіпсіздік саласындағы халықаралық ынтымақтастықтың құқықтық негіздері. ТМД құқықтық шолу, 2022, №4, 35-40 б.

160. Өтебеков, С.Қ. Қазақстандағы киберқылмыспен күрес: құқық қорғау органдарының рөлі және ұйымдастырушылық мәселелер. Заң журналы, 2023, №5, 56-62 б.

161. «Мемлекеттік техникалық қызмет» АҚ есебі. Қазақстандағы киберқауіпсіздік инциденттері және халықаралық ынтымақтастық. Нұр-Сұлтан, 2023. https://sts.kz/kz/ 22.09.2024

162. Қазақстан Республикасының «Мемлекеттік техникалық қызмет» АҚ. Ақпараттық қауіпсіздік инциденттері туралы есеп. Астана: Мемлекеттік техникалық қызмет, 2023. б.45.

163. Есенғазиев, М.Ә. Ұлттық киберқауіпсіздік жүйесін жетілдіру: Қазақстандағы құқықтық және техникалық аспектілер. Қауіпсіздік және құқық журналы, 2023, №3, 72-78 б.

164. Ағыбаев, А.Н. (2021). Қылмыстық құқық: Жалпы бөлім. Алматы: Жеті жарғы. – 152-168 б.

165. Борчашвили, И.Ш. (2020). Киберқылмыспен күрестің құқықтық негіздері. Алматы: Заң ғылымдары академиясы. – 74-89 б.

166. Жекебаев, Ү.С. (2019). Ақпараттық қауіпсіздік және құқықтық реттеу. Нұр-Сұлтан: Фолиант. – 98-115 б.

167. Қайыржанов, Е.І. (2022). Қылмыстық құқық: Ерекше бөлім. Алматы: Қазақ университеті. – 193-207 б.

168. Рахметов, С.М. (2020). Киберқұқық және ақпараттық қауіпсіздік мәселелері. Құқықтық зерттеулер журналы, №2, 34-42 б.

169. Балтабаев, К.Ж. (2023). Цифрлық қылмыстар және құқық қорғау органдарының қызметі. Астана: Фолиант. – 56-72 б.