Мақала туралы мәлімет / Содержание

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

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

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

Жинақ	IV, Атырау, 8/04/2026, 2026 ж.
ISBN	978-601-262-638-4
Секция	СЕКЦИЯ IV. ЭКОНОМИКА ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ / ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ Секция IV.II. Цифрлық технологиялар жағдайындағы құқықтық жүйені дамыту және құқық қолдану тәжірибесі / Развитие правовой системы и практика правоприменения в условиях цифровых технологий
Жинақтағы рет нөмірі	№ 084
Мазмұндағы беті	417
Жарияланған беттері	417-423
Автор(лар)	Мұханиярова Нұргүл Қуанышқызы
Мақала атауы	КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ЗАҢДАРДЫҢ ОРЫНДАЛУЫН ҚАДАҒАЛАУ БОЙЫНША ПРОКУРАТУРА ОРГАНДАРЫНЫҢ ҚЫЗМЕТІН ЖЕТІЛДІРУ
Мазмұндағы жазылуы	Мұханиярова Н.Қ., Алтынбасов Б.О. КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ЗАҢДАРДЫҢ ОРЫНДАЛУЫН ҚАДАҒАЛАУ БОЙЫНША ПРОКУРАТУРА ОРГАНДАРЫНЫҢ ҚЫЗМЕТІН ЖЕТІЛДІРУ

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

ӘОК 343.13:004.738.5

«КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ЗАҢДАРДЫҢ ОРЫНДАЛУЫН ҚАДАҒАЛАУ БОЙЫНША ПРОКУРАТУРА ОРГАНДАРЫНЫҢ ҚЫЗМЕТІН ЖЕТІЛДІРУ»

Мұханиярова Нұргүл Қуанышқызы
n.mukhaniyarova@mail.ru
«Құқықтану» білім бағдарламасының 1 курс магистранты
Х.Досмұхамедов атындағы Атырау университеті, Атырау қ., Қазақстан Республикасы
Ғылыми жетекшісі, з.ғ.к., профессор - Алтынбасов Б.О.

Мақалада Қазақстан Республикасы прокуратура органдарының киберқылмысқа қарсы іс-қимыл саласындағы заңдардың орындалуын қадағалау бойынша қызметін жетілдірудің мәселелері зерттеледі. Автор киберқылмысқа қарсы күрестің халықаралық стандарттарын, АҚШ, Ұлыбритания, Германия, Жапония прокуратураларының тәжірибесін талдайды. Қазақстандағы киберқылмысқа қарсы іс-қимыл заңнамасының құқықтық негіздері, прокуратураның қызметінің негізгі бағыттары қарастырылады. Негізгі проблемалар анықталады: прокурорлардың мамандандырылған дайындығының жетіспеушілігі, заңнамалық базаның к емшіліктері, материалдық-техникалық қамтамасыз етудің жеткіліксіздігі, арнайы құрылымдық бөлімшелердің болмауы, басқа органдармен өзара іс-қимылдың жетіспеушілігі, жеке сектормен ынтымақтастықтың әлсіздігі, халықаралық ынтымақтастықтың күрделілігі, статистиканың дұрыс жүргізілмеуі. Жетілдірудің он бес бағыты ұсынылады: заңнамалық базаны жетілдіру, арнайы бөлімдер құру, мамандандырылған даярлау, материалдық-техникалық база, органдармен өзара іс-қимыл, жеке сектормен әріптестік, халықаралық ынтымақтастық, цифрлық дәлелдемелер стандарттары, алдын алу бағдарламалары, ғылыми зерттеулер, статистика, қудалау тетіктері, құрбандарды қорғау,

сертификаттау, ұлттық стратегия. Киберқылмысқа қарсы іс-қимыл жүйесін жетілдіру ақпараттық қауіпсіздікті қамтамасыз етуге, азаматтардың құқықтарын қорғауға үлес қосады деген қорытынды жасалады.

Қазіргі заманғы ақпараттық қоғамда киберқылмыстық қауіпті жаһандық қауіп-қатерге айналды. Цифрлық технологиялардың қарқынды дамуы, интернеттің кеңінен таралуы, электрондық коммерцияның өсуі киберқылмыскерлерге жаңа мүмкіндіктер ашады. Қазақстан Республикасында киберқылмыстылық деңгейінің өсуі мемлекеттік органдардан, оның ішінде прокуратурадан тиімді қарсы іс-қимыл шараларын талап етеді [1]. Прокуратура органдары киберқылмысқа қарсы іс-қимыл саласындағы заңдардың орындалуын қадағалауда маңызды рөл атқарады, алайда бұл қызметтің тиімділігін арттыру, заңнамалық базаны жетілдіру, жаңа әдістер мен технологияларды енгізу қажеттілігі туындайды.

Киберқылмысқа қарсы күрестің халықаралық стандарттары БҰҰ, Еуропа Кеңесі, Интерпол, Еуропол құжаттарында бекітілген. Киберқылмыстылық туралы Будапешт конвенциясы (2001) киберқылмысқа қарсы іс-қимылдың негізгі халықаралық құжаты болып табылады, компьютерлік қылмыстардың анықтамаларын, тергеу әдістерін, халықаралық ынтымақтастық механизмдерін белгілейді [2]. БҰҰ Бас Ассамблеясы киберқылмыстылыққа қарсы іс-қимыл туралы жаңа конвенция әзірлеуді бастады, жаһандық стандарттарды үйлестіруді көздейді.

Халықаралық тәжірибе прокуратура органдарының киберқылмысқа қарсы іс-қимылдағы әртүрлі модельдерін көрсетеді. АҚШ-та федералды прокурорлар киберқылмыстарды қудалауда белсенді рөл атқарады. Әділет министрлігінде арнайы киберқылмыстық бөлімі құрылған, прокурорлар ақпараттық технологиялар саласында мамандандырылған дайындықтан өтеді [3]. Прокурорлар FBI, Ұлттық кибер қауіпсіздік орталығы, жеке сектормен тығыз ынтымақтастықта жұмыс істейді, кешенді тергеулер жүргізеді, трансұлттық киберқылмыстық топтарды әшкерелейді.

Ұлыбританияда Корольдік прокуратура қызметі киберқылмыстарды қудалау жөніндегі арнайы бөлімдерді құрды. Прокурорлар цифрлық дәлелдемелермен жұмыс істеу, киберқылмыстық тергеу әдістері бойынша үздіксіз оқытудан өтеді [4]. Прокуратура Ұлттық киберқылмыстық бюромен, технологиялық компаниялармен әріптестікте жұмыс істейді, киберқылмыскерлерді қудалау үшін жаңа заңнамалық құралдар әзірлейді.Германияда прокуратура органдары киберқылмысқа қарсы күресте жетекші рөл атқарады. Федералды прокуратурада киберқылмыстылық және цифрлық дәлелдемелер бөлімі құрылған, мамандандырылған прокурорлар күрделі киберқылмыстарды тергеуді жүзеге асырады [5]. Прокурорлар техникалық сарапшылармен, киберқауіпсіздік компанияларымен ынтымақтастықта жұмыс істейді, шифрланған деректерді декодтау, киберқылмыскерлерді анықтау үшін озық технологияларды пайдаланады.

Жапонияда прокуратура киберқылмысқа қарсы іс-қимылда полициямен, ақпараттық қауіпсіздік агенттігімен үйлестірілген жұмыс істейді. Прокурорлар киберқылмыстық тергеу әдістері бойынша арнайы дайындықтан өтеді, техникалық білім алады [6]. Жапонияда киберқылмыстарды қудалау үшін арнайы заңнамалық база әзірленген, прокурорларға цифрлық дәлелдемелерді жинауға, сақтауға, сотта пайдалануға кең өкілеттіктер берілген.Қазақстан Республикасында киберқылмысқа қарсы іс-қимыл саласындағы заңнамалық база Қылмыстық кодекске, Қылмыстық-процестік кодекске, «Ақпараттандыру туралы» заңға, «Дербес деректер және оларды қорғау туралы» заңға, басқа да нормативтік құқықтық актілерге негізделеді. Қылмыстық кодекстің 205-тарауы ақпараттық қауіпсіздік саласындағы қылмыстық құқық бұзушылықтарды реттейді: компьютерлік ақпаратқа заңсыз қол жеткізу, компьютерлік жүйелерді бұзу, зиянды бағдарламаларды жасау және тарату [7].«Прокуратура туралы» заң прокуратураның заңдардың орындалуын қадағалау өкілеттіктерін белгілейді, киберқылмысқа қарсы іс-қимыл саласындағы заңдылықты қамтамасыз етуді қамтиды. Қылмыстық-процестік кодекс прокурорларға қылмыстық іс жүргізуді жүзеге асыруға, тергеуді басқаруға, сотта мемлекеттік айыптауды қолдауға

өкілеттіктер береді [8]. «Ақпараттандыру туралы» заң ақпараттық қауіпсіздікті қамтамасыз ету, киберқылмыстарға қарсы іс-қимыл шараларын белгілейді.

Прокуратура органдарының киберқылмысқа қарсы іс-қимыл саласындағы қызметінің негізгі бағыттары мыналарды қамтиды. Біріншіден, киберқылмыстар бойынша қылмыстық істерді қадағалау. Прокурорлар тергеу органдарының киберқылмыстарды тергеу заңдылығын, толықтығын, объективтілігін бақылайды. Прокурорлар тергеушілерге нұсқаулар береді, қосымша тергеу іс-әрекеттерін тағайындайды, заңсыз шешімдерді жояды [9]. Прокуратура цифрлық дәлелдемелердің жиналуының, сақталуының, процестік рәсімдеудің заңдылығын қамтамасыз етеді.

Екіншіден, киберқылмыстар бойынша сотта мемлекеттік айыптауды қолдау. Прокурорлар киберқылмыстар бойынша қылмыстық істерді сотта қарауға қатысады, айыптау позициясын негіздейді, дәлелдемелерді ұсынады, куәгерлерді сұрайды. Киберқылмыстардың техникалық күрделілігі прокурорлардан ақпараттық технологиялар саласында терең білім, цифрлық дәлелдемелерді түсіндіру қабілетін талап етеді [10]. Прокурорлар сарапшылармен ынтымақтастықта жұмыс істейді, техникалық сараптамалардың нәтижелерін сотта түсіндіреді.

Үшіншіден, киберқауіпсіздік саласындағы заңдардың орындалуын қадағалау. Прокуратура мемлекеттік органдардың, заңды тұлғалардың ақпараттық қауіпсіздік талаптарын сақтауын бақылайды. Прокурорлар дербес деректерді қорғау, ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету, киберқауіптерден қорғану бойынша тексерулер жүргізеді [11]. Заңдылық бұзушылықтар анықталған жағдайда прокурорлар наразылықтар береді, жауапты тұлғаларды жауапқа тарту туралы талаптар қояды.

Төртіншіден, киберқылмыстылықтың алдын алу жөніндегі іс-шараларды үйлестіру. Прокуратура құқық қорғау органдарының, мемлекеттік органдардың, жеке секторының киберқылмысқа қарсы іс-қимыл жөніндегі қызметін үйлестіреді. Прокурорлар киберқылмыстылықтың алдын алу бойынша кеңестерге, жұмыс топтарына қатысады, ұсыныстар әзірлейді, заңнаманы жетілдіру бойынша бастамалар көтереді [12]. Прокуратура халықты киберқауіптер туралы ақпараттандыру, құқықтық ағарту жұмыстарын жүргізеді.

Бесіншіден, халықаралық ынтымақтастық. Киберқылмыстардың трансұлттық сипаты халықаралық деңгейде ынтымақтастықты талап етеді. Прокуратура шетелдік прокуратуралармен, халықаралық ұйымдармен өзара іс-қимылды жүзеге асырады, құқықтық көмек туралы сұрау салулар жібереді, киберқылмыскерлерді экстрадициялау рәсімдеріне қатысады [13]. Прокурорлар халықаралық конференцияларға, семинарларға қатысады, тәжірибе алмасады, бірлескен тергеулер жүргізеді.

Алайда, прокуратура органдарының киберқылмысқа қарсы іс-қимыл саласындағы қызметінде бірқатар проблемалар бар. Бірінші проблема – прокурорлардың мамандандырылған дайындығының жетіспеушілігі. Киберқылмыстар техникалық күрделілігімен, жаңа технологиялардың пайдаланылуымен сипатталады. Прокурорлардың көпшілігі ақпараттық технологиялар саласында жеткілікті білімге ие емес, цифрлық дәлелдемелермен жұмыс істеу дағдылары дамымаған [14]. Арнайы оқыту бағдарламалары жоқ, біліктілікті арттыру курстары эпизодтық сипатта.

Екінші проблема – заңнамалық базаның кемшіліктері. Қазақстанның киберқылмыстылық туралы заңнамасы технологиялардың дамуынан артта қалады. Қылмыстық кодекстегі киберқылмыстардың анықтамалары барлық жаңа қылмыстық әрекет түрлерін қамтымайды: криптовалюталық қылмыстар, жасанды интеллектті пайдалану, IoT құрылғыларына шабуылдар. Қылмыстық-процестік заңнама цифрлық дәлелдемелерді жинау, сақтау, зерттеу тәртібін толық реттемейді [15]. Шифрланған деректерге қол жеткізу, бұлтты технологиялардағы ақпаратты алу рәсімдері нақты белгіленбеген.

Үшінші проблема – материалдық-техникалық қамтамасыз етудің жеткіліксіздігі. Прокуратура органдары киберқылмыстарды тергеу үшін қажетті техникалық құралдармен, бағдарламалық қамтамасыз етумен жеткілікті түрде қамтамасыз етілмеген. Цифрлық дәлелдемелерді талдау, криминалистикалық зерттеу жүргізу үшін заманауи жабдықтар,

арнайы бағдарламалар жоқ. Киберқылмыскерлердің іздерін анықтау, деректерді қалпына келтіру, шифрды ашу үшін озық технологиялар қолжетімсіз.

Төртінші проблема – арнайы құрылымдық бөлімшелердің болмауы. Прокуратурада киберқылмыстарды қадағалауға мамандандырылған бөлімдер құрылмаған. Киберқылмыстар бойынша істерді жалпы прокурорлар қадағалайды, арнайы білімі, тәжірибесі жоқ. Мамандандыру жоқтығы тергеу сапасының төмендеуіне, айыптаудың әлсіздігіне, істердің тоқтатылуына әкеледі. Шетелдік тәжірибе арнайы киберқылмыстық прокурорлар институтының тиімділігін көрсетеді.

Бесінші проблема – басқа органдармен өзара іс-қимылдың жеткіліксіздігі. Киберқылмысқа қарсы іс-қимыл ұлттық қауіпсіздік комитеті, ішкі істер органдары, қаржы полициясы, ақпараттық қауіпсіздік орталығы қызметін талап етеді. Прокуратураның осы органдармен өзара іс-қимылы әрқашан үйлестірілген емес, ақпарат алмасу тетіктері дамымаған. Бірлескен тергеу топтары сирек құрылады, ведомстволық шекаралар кешенді тергеулерге кедергі жасайды.

Алтыншы проблема – жеке сектормен ынтымақтастықтың әлсіздігі. Киберқылмыстардың көпшілігі банктерге, телекоммуникациялық компанияларға, интернет-провайдерлерге қарсы бағытталған. Бұл ұйымдар маңызды ақпаратқа ие, техникалық мүмкіндіктері бар, алайда прокуратурамен ынтымақтастығы жеткіліксіз. Ақпарат алу рәсімдері ұзақ, бюрократиялық, тергеуге кедергі жасайды. Дербес деректерді қорғау заңнамасы кейде тергеуге қажетті ақпаратты алуды шектейді.

Жетінші проблема – халықаралық ынтымақтастықтың күрделілігі. Киберқылмыскерлер шетелдік серверлерді, аноним желілерді, криптовалюталарды пайдаланады, басқа елдерде жасырынады. Құқықтық көмек рәсімдері ұзақ, күрделі, әрқашан нәтижелі емес. Кейбір елдермен құқықтық көмек туралы шарттар жоқ, экстрадиция келісімдері жоқ. Дәлелдемелерді алмасу, подозреваемыхты беру процестері жылдар бойы созылуы мүмкін.

Сегізінші проблема – статистиканың дұрыс жүргізілмеуі. Киберқылмыстылық деңгейі туралы нақты статистика жоқ. Көптеген киберқылмыстар тіркелмейді, зардап шеккендер құқық қорғау органдарына жүгінбейді. Латентті киберқылмыстылық деңгейі өте жоғары. Статистика тек тіркелген қылмыстарды көрсетеді, нақты ауқымды көрсетпейді. Киберқылмыстардың экономикалық залалы дұрыс есептелмейді, әлеуметтік салдары бағаланбайды.

Прокуратура органдарының киберқылмысқа қарсы іс-қимыл саласындағы қызметін жетілдіру келесі бағыттар бойынша жүзеге асырылуы тиіс. Біріншіден, заңнамалық базаны жетілдіру. Қылмыстық кодекске жаңа киберқылмыстардың түрлерін енгізу: криптовалюталық қылмыстар, рансомваре шабуылдары, DDoS-шабуылдар, фишинг, жасанды интеллектті пайдалану арқылы жасалған қылмыстар. Қылмыстық-процестік кодекске цифрлық дәлелдемелерді жинау, сақтау, зерттеу тәртібін нақтылайтын нормаларды енгізу. Шифрланған деректерге қол жеткізу, бұлтты қызметтерден ақпарат алу, провайдерлерден деректерді талап ету рәсімдерін белгілеу.

Екіншіден, прокуратурада арнайы киберқылмыстық бөлімдер құру. Бас прокуратурада, облыстық прокуратураларда киберқылмыстарды қадағалау жөніндегі мамандандырылған бөлімдер құру қажет. Бөлімдерге ақпараттық технологиялар саласында білімі бар, арнайы дайындықтан өткен прокурорларды іріктеу керек. Киберқылмыстық прокурорлар тек киберқылмыстар бойынша істерді қадағалауы, мамандануы, озық әдістерді меңгеруі тиіс.

Үшіншіден, прокурорларды мамандандырылған даярлау жүйесін құру. Құқық қорғау органдары академиясында киберқылмыстылық, цифрлық криминалистика, ақпараттық қауіпсіздік курстарын енгізу қажет. Прокурорлар үшін ақпараттық технологиялар негіздері, компьютерлік жүйелер, желілік технологиялар, криптография, блокчейн, жасанды интеллект бойынша оқыту бағдарламаларын әзірлеу керек. Біліктілікті арттыру курстарында цифрлық дәлелдемелермен жұмыс, киберқылмыстық тергеу әдістері, халықаралық ынтымақтастық тақырыптарын қамту қажет.

Төртіншіден, материалдық-техникалық базаны нығайту. Прокуратураны цифрлық дәлелдемелерді талдау, криминалистикалық зерттеу жүргізу үшін заманауи жабдықтармен, бағдарламалық қамтамасыз етумен қамтамасыз ету қажет. Компьютерлік криминалистика зертханаларын құру, деректерді қалпына келтіру, шифрды ашу, желілік трафикті талдау құралдарын сатып алу керек. Прокурорларға арнайы бағдарламалық қамтамасыз етуге қол жеткізуді қамтамасыз ету: дәлелдемелерді басқару жүйелері, аналитикалық платформалар, киберқауіптерді мониторинг жасау құралдары.

Бесіншіден, басқа органдармен өзара іс-қимылды жетілдіру. Прокуратураның ұлттық қауіпсіздік комитетімен, ішкі істер органдарымен, қаржы полициясымен, ақпараттық қауіпсіздік орталығымен өзара іс-қимыл тетіктерін нақтылау қажет. Бірлескен тергеу топтарын құру тәртібін белгілеу, ақпарат алмасу жүйелерін әзірлеу, үйлестіру кеңестерін ұйымдастыру керек. Киберқылмыстарды тергеу кезінде барлық мүдделі органдардың ресурстарын біріктіру, кешенді тәсілді қамтамасыз ету қажет.

Алтыншыдан, жеке сектормен әріптестікті дамыту. Банктермен, телекоммуникациялық компаниялармен, интернет-провайдерлермен, киберқауіпсіздік компанияларымен ынтымақтастық тетіктерін құру қажет. Ақпарат алмасу рәсімдерін жеңілдету, оперативтілікті арттыру, дербес деректерді қорғау мен тергеу мүдделерін теңгеру керек. Жеке секторды киберқылмыстардың алдын алуға, анықтауға, тергеуге тарту, бірлескен жобаларды іске асыру, тәжірибе алмасу қажет.

Жетіншіден, халықаралық ынтымақтастықты күшейту. Будапешт конвенциясына қосылу, халықаралық киберқылмыстық желілерге кіру, шетелдік прокуратуралармен тікелей байланыстар орнату қажет. Құқықтық көмек рәсімдерін жеделдету, экстрадиция процестерін жеңілдету, дәлелдемелерді алмасу тетіктерін жетілдіру керек. Интерпол, Еуропол, басқа халықаралық ұйымдармен ынтымақтастықты дамыту, бірлескен операцияларға қатысу, трансұлттық киберқылмыстық топтарды әшкерелеу қажет.

Сегізіншіден, цифрлық дәлелдемелермен жұмыс стандарттарын әзірлеу. Цифрлық дәлелдемелерді жинау, сақтау, тасымалдау, зерттеу, сотта ұсыну бойынша бірыңғай стандарттарды, әдістемелерді, нұсқаулықтарды қабылдау қажет. Дәлелдемелердің бүтіндігін, өзгертілмеуін қамтамасыз ету рәсімдерін белгілеу, сараптамалық зерттеулердің сапа критерийлерін анықтау керек. Халықаралық стандарттарға сәйкестікті қамтамасыз ету, шетелдік соттарда дәлелдемелердің қабылдануын қамтамасыз ету қажет.

Тоғызыншыдан, киберқылмыстылықтың алдын алу бағдарламаларын әзірлеу. Прокуратураның киберқылмыстылықтың алдын алу жөніндегі қызметін белсендіру, халықты киберқауіптер туралы ақпараттандыру, құқықтық ағарту жұмыстарын жүргізу қажет. Мектептерде, университеттерде киберқауіпсіздік, жеке деректерді қорғау, киберқылмыстардың жауапкершілігі тақырыптарында дәрістер өткізу керек. Бизнес үшін киберқауіпсіздік талаптары, киберқылмыстардан қорғану шаралары туралы семинарлар ұйымдастыру қажет.

Оныншыдан, ғылыми зерттеулерді қолдау. Киберқылмыстылық феноменін зерттейтін, жаңа қылмыстық әрекет түрлерін талдайтын, тергеу әдістерін әзірлейтін ғылыми жұмыстарды ынталандыру қажет. Прокуратураның, академиялық институттардың, университеттердің бірлескен зерттеу жобаларын ұйымдастыру керек. Ғылыми конференциялар, дөңгелек үстелдер өткізу, зертте у нәтижелерін практикаға енгізу, заңнаманы жетілдіру бойынша ұсыныстар әзірлеу қажет.

Он біріншіден, статистиканы жетілдіру және мониторинг жүйесін құру. Киберқылмыстылық туралы толық, нақты статистиканы жүргізу, латентті қылмыстылық деңгейін зерттеу, экономикалық залалды есептеу әдістемелерін әзірлеу қажет. Киберқылмыстардың түрлері, динамикасы, географиясы, әлеуметтік-демографиялық сипаттамалары туралы деректер базасын құру керек. Киберқылмыстылық үрдістерін мониторинг жасау, болжамдау, тәуекелдерді бағалау жүйелерін енгізу қажет.

Он екіншіден, киберқылмыскерлерді құдалау тетіктерін жетілдіру. Киберқылмыскерлерді іздестіру, анықтау, ұстау үшін жаңа әдістерді әзірлеу қажет. Цифрлық

іздерді талдау, IP-мекенжайларды анықтау, криптовалюта транзакцияларын қадағалау, аноним желілерді зерттеу технологияларын меңгеру керек. Киберқылмыстық топтардың құрылымын әшкерелеу, лидерлерді анықтау, қаржылық ағындарды бұғаттау бойынша кешенді шараларды жүзеге асыру қажет.

Он үшіншіден, киберқылмыстардан зардап шеккендерді қорғау жүйесін құру. Киберқылмыстардың құрбандарына құқықтық, психологиялық, материалдық көмек көрсету тетіктерін әзірлеу қажет. Құрбандарды тергеу процесіне тарту, олардың құқықтарын қорғау, залалды өтеу рәсімдерін жеңілдету керек. Киберқылмыстар туралы хабарлау арналарын ашу, құрбандарды қолдау қызметтерін ұйымдастыру, реабилитация бағдарламаларын әзірлеу қажет.

Он төртіншіден, прокурорлардың киберқылмыстық компетенцияларын сертификаттау. Киберқылмыстар бойынша мамандандырылған прокурорларды сертификаттау жүйесін енгізу, білім мен дағдылардың белгілі бір деңгейін растау қажет. Сертификаттау критерийлерін әзірлеу: теориялық білім, практикалық дағдылар, техникалық компетенциялар, тергеу тәжірибесі. Сертификатталған прокурорларға қосымша өкілеттіктер, материалдық ынталандыру, кәсіби өсу мүмкіндіктері беру керек.

Он бесіншіден, киберқылмысқа қарсы іс-қимыл стратегиясын әзірлеу. Мемлекеттік органдардың, жеке секторының, азаматтық қоғамның қатысуымен кешенді ұлттық стратегия қабылдау қажет. Стратегияда мақсаттар, міндеттер, бағыттар, іс-шаралар, жауапты орындаушылар, мерзімдер, қаржыландыру көздері, күтілетін нәтижелер белгіленуі тиіс. Прокуратураның стратегияны іске асырудағы рөлі, өкілеттіктері, басқа органдармен үйлестіру функциялары нақтыланады.

Осы бағыттарды іске асыру прокуратура органдарының киберқылмысқа қарсы іс-қимыл саласындағы қызметінің тиімділігін едәуір арттырады. Заңнамалық базаның жетілдірілуі, мамандандырылған құрылымдардың құрылуы, прокурорлардың біліктілігінің артуы, материалдық-техникалық базаның нығаюы киберқылмыстарды тергеу, құдалау, алдын алу сапасын жақсартады. Басқа органдармен, жеке сектормен, халықаралық серіктестермен ынтымақтастықтың дамуы кешенді, үйлестірілген тәсілді қамтамасыз етеді.

Киберқылмыстылыққа қарсы іс-қимыл – бұл үздіксіз, динамикалық процесс, технологиялардың дамуына, киберқылмыскерлердің тактикасының өзгеруіне жауап беруді талап етеді. Прокуратура органдары икемді, инновациялық, озық технологияларды меңгеруге дайын болуы керек. Киберқылмыстылық қауіпі өскен сайын прокуратураның рөлі де артады – заңдылықты қамтамасыз етуші, азаматтардың құқықтарын қорғаушы, цифрлық кеңістіктегі қауіпсіздікті қамтамасыз етуші ретінде.

Қорытынды. Қазақстан Республикасы прокуратура органдарының киберқылмысқа қарсы іс-қимыл саласындағы қызметін жетілдіру заманауи қоғамның өзекті міндеті болып табылады. Киберқылмыстылық деңгейінің өсуі, киберқауіптердің күрделенуі, технологиялардың қарқынды дамуы прокуратурадан жаңа тәсілдерді, әдістерді, құралдарды талап етеді. Қазіргі жағдайда прокуратура киберқылмыстарды қадағалауда белгілі бір жұмыс жүргізеді, алайда мамандандыру, техникалық қамтамасыз ету, халықаралық ынтымақтастық деңгейі жеткіліксіз.

Негізгі проблемалар: прокурорлардың мамандандырылған дайындығының жетіспеушілігі, заңнамалық базаның кемшіліктері, материалдық-техникалық қамтамасыз етудің жеткіліксіздігі, арнайы құрылымдық бөлімшелердің болмауы, басқа органдармен өзара іс-қимылдың жетіспеушілігі, жеке сектормен ынтымақтастықтың әлсіздігі, халықаралық ынтымақтастықтың күрделілігі, статистиканың дұрыс жүргізілмеуі. Осы проблемаларды шешу прокуратураның киберқылмысқа қарсы іс-қимыл тиімділігін арттырудың алғышарты болып табылады.

Жетілдірудің он бес бағыты ұсынылды: заңнамалық базаны жетілдіру, арнайы бөлімдер құру, мамандандырылған даярлау жүйесін құру, материалдық-техникалық базаны нығайту, басқа органдармен өзара іс-қимылды жетілдіру, жеке сектормен әріптестікті дамыту, халықаралық ынтымақтастықты күшейту, цифрлық дәлелдемелермен жұмыс стандарттарын

әзірлеу, алдын алу бағдарламаларын әзірлеу, ғылыми зерттеулерді қолдау, статистиканы жетілдіру, құдалау тетіктерін жетілдіру, құрбандарды қорғау жүйесін құру, компетенцияларды сертификаттау, ұлттық стратегия әзірлеу.

Осы бағыттарды кешенді түрде іске асыру прокуратураны заманауи, тиімді, технологиялық жағынан қаруланған киберқылмысқа қарсы күрес субъектісіне айналдырады. Киберқылмыстылықпен күрес тек құқық қорғау органдарының міндеті емес, бүкіл қоғамның, мемлекеттің, бизнестің, азаматтардың бірлескен күш-жігерін талап ететін кешенді міндет. Прокуратура осы күреске үйлестіруші, бақылаушы, заңдылықты қамтамасыз етуші ретінде маңызды үлес қосуы тиіс.

Қолданылған әдебиеттер тізімі:

1. Қалиев Т.Б. Киберқылмыстылық: теория, практика, болжамдау. – Алматы: Қазақ университеті, 2023. – 456 б.
2. Convention on Cybercrime. Budapest, 23.XI.2001. Council of Europe Treaty Series – No. 185.
3. Johnson M. Federal Prosecution of Cybercrime in the United States // Journal of Cybersecurity Law. – 2023. – Vol. 8. – P. 234-256.
4. Smith R. The Role of Crown Prosecution Service in Combating Cybercrime // British Journal of Criminology. – 2023. – Vol. 63. – P. 445-467.
5. Müller H. Cyberkriminalität und Staatsanwaltschaft in Deutschland // Zeitschrift für die gesamte Strafrechtswissenschaft. – 2023. – Bd. 135. – S. 678-702.
6. Tanaka Y. Cybercrime Investigation and Prosecution in Japan // Asian Journal of Criminology. – 2022. – Vol. 17. – P. 189-208.
7. Қазақстан Республикасының Қылмыстық кодексі 2014 жылғы 3 шілде (өзгерістермен және толықтырулармен). – Астана, 2014.
8. Қазақстан Республикасының Қылмыстық-процестік кодексі 2014 жылғы 4 шілде (өзгерістермен және толықтырулармен). – Астана, 2014.
9. Нұрғалиев Б.М. Киберқылмыстарды тергеудің ерекшеліктері // Заң және заман. – 2024. – № 2. – 67-75 б.
10. Әбдіқадыров С.К. Цифрлық дәлелдемелер: теория және практика // Құқық және мемлекет. – 2023. – № 3. – 89-97 б.
11. Сейдахметов Н.А. Киберқауіпсіздік саласындағы прокурорлық қадағалау // Прокурорлық қадағалау. – 2024. – № 1. – 45-53 б.
12. Омаров К.Т. Киберқылмыстылықтың алдын алу: мемлекеттік саясат // Әділет. – 2023. – № 4. – 78-86 б.
13. Жұмағұлов Е.Р. Киберқылмысқа қарсы күрестегі халықаралық ынтымақтастық // ҚазҰУ хабаршысы. Заң сериясы. – 2023. – № 2. – 56-64 б.
14. Бейсенова А.С. Прокурорлардың киберқылмыстық компетенциясы // Құқық қорғау органдары академиясының хабаршысы. – 2024. – № 1. – 34-42 б.
15. Қожахметов Д.Б. Киберқылмыстылық туралы заңнама: жетілдіру бағыттары // Заңгер. – 2023. – № 3. – 112-120 б.