BAKI UNİVERSİTETİNİN XƏBƏRLƏRİ

№1 ***Sosial-siyasi elmlər seriyası*** ***2025***

UOT 343.1

KİBERCİNAYƏTKARLIQLA MÜBARİZƏNİN HÜQUQİ ƏSASLARI: MÖVCUD PROBLEMLƏR VƏ HƏLL YOLLARI

F.M.ABBASOVA, K.İ.XƏLİLOV
Bakı Dövlət Universiteti
firuza.abbasova@gmail.com
kamran.khalilov.isa@bsu.edu.az
https://orcid.org/0000-0002-0086-009X

Yaşadığımız dövrdə kibercinayətkarlıq informasiya texnologiyalarının sürətli inkişafı ilə paralel olaraq geniş yayılmış və istər beynəlxalq, istərsə də milli təhlükəsizlik üçün ciddi təhdidə çevrilmişdir. Kibercinayətlərin çoxşaxəli və spesifik xarakterdə olması onunla mübarizənin üsul və qaydalarını da çətinləşdirir. Məhz bu mənada hüquq mühafizə orqanları və beynəlxalq təşkilatların qarşısında duran ən vacib vəzifə kibercinayətkarlıqla mübarizə üsullarını dərindən bilmək, mövcud üsulları təkmilləşdirmək və ya yeni yollar axtarmaq, eləcə də bu istiqamətdə qarşıya çıxan çətinlikləri operativ və səmərəli şəkildə həll etməkdir. Bu məqsədlə araşdırma kibercinayətkarlıqla mübarizənin hüquqi əsaslarını müəyyən edərək, bu fəaliyyətin həyata keçirilməsində hansı çətinliklərin olduğunu təhlil edir. Həmçinin bu tədqiqat işi kibercinayətkarlıqla mübarizədə ortaya çıxan problemlərin həlli üçün alternativ həll yollarını araşdıraraq təqdim edir. Bu mübarizənin gücləndirilməsi üçün normativ-hüquqi bazanın təkmilləşdirilməsi, müasir istintaq üsullarından istifadə edilməsi, beynəlxalq əməkdaşlığın artırılması və hüquq mühafizə orqanlarının kibertəhlükəsizlik sahəsində ixtisaslaşmasının vacibliyi qeyd edilir.

Açar sözlər: kibercinayət, mübarizə, beynəlxalq əməkdaşlıq, yurisdiksiya, problemlər.

Giriş. Texnologiyanın və internetin inkişafı insanların qarşılıqlı əlaqə, ünsiyyət və işləmə tərzini dəyişdi. Bu irəliləyişlər çoxsaylı faydalar gətirsə də, həm də kibercinayət kimi tanınan cinayətkar fəaliyyətin yeni formasına səbəb oldu. Kibercinayətkarlıq kompüterlərdən, şəbəkələrdən və internetdən istifadə etməklə asanlaşdırılan və ya törədilən qeyri-qanuni fəaliyyətləri ehtiva edir. Kibercinayətkarlar geniş spektrli qeyri-qanuni fəaliyyətlər həyata keçirmək üçün kompüter sistemlərində, şəbəkələrdə və onlayn platformalardakı boşluqlardan istifadə edirlər. Bu fəaliyyətlərə xakerlik, fişinq, ransomware hücumları (zərərli proqram təminatı), məlumatların pozulması, onlayn fırıldaqçılıq, əqli mülkiyyət oğurluğu daxildir. Heç şübhə yoxdur ki, kibercinayətlərin maliyyə, sosial və psixoloji nəticələri fərdlərə, bizneslərə, hö-

kumətlərə və hətta milli təhlükəsizliyə təsiri yüksək həddədir. Buna görə də kibercinayətkarlıq transsərhəd xarakterinə və texnologiyanın sürətli təkamülünə görə unikal hüquqi problemlər yaradır. Yurisdiksiya məsələləri, rəqəmsal sübutların toplanması və qorunmasında çətinliklər, həmçinin yenilənmiş qanunvericiliyə ehtiyac kibercinayətkarlığın mürəkkəb hüquqi aspektlərindən yalnız bir neçəsidir. Bu problemlərin təhlili hüquqşünaslara və mütəxəssislərə kibercinayətkarlıqla effektiv mübarizə aparmaq üçün daha səmərəli hüquqi çərçivələr hazırlamağa kömək edir [5, s.4]. Kibercinayətlərin hüquqi nəticələrinin təhlili əməkdaşlığın təkmilləşdirilməsi, qanunların uyğunlaşdırılması, məlumat mübadiləsinin artırılması və hüquqi prosesləri sadələşdirmək üçün beynəlxalq çərçivələrin və müqavilələrin işlənib hazırlanması sahələrini müəyyən etməyə kömək edir. Kibercinayətkarlığın hüquqi nəticələrini öyrənməklə mövcud qanunlardakı boşluqları aradan qaldıra, zəruri islahatlar təklif edilə və kibercinayətkarlıqla mübarizə üçün effektiv strategiyalar təşviq oluna bilər.

Kibercinayətkarlıqla mübarizədə çətinliklər. Texnologiyanın sürətli inkişafı və son illərin təcrübəsi kibercinayətkarlıqla mübarizənin nə qədər çətin olduğunu bir daha sübut etdi. Bu mübarizənin hüquq sisteminə hansı dərəcədə təsir etməsini bir neçə amillə əlaqələndirmək olar. Hər şeydən öncə, kibercinayətkarlıq nisbətən yeni bir hadisə olduğundan, cinayətlərin necə törədildiyinə dair şablonlar yaratmaq mümkün deyil [1, s.555]. Bütün bunlar kibercinayətlərlə mübarizə üçün resursların necə ayrılması lazım olduğunu göstərən informasiya bazasının hazırlanmasına mane olur [27]. Problemin həqiqi miqyası haqqında biliklərimiz məhdud olsa da, aydındır ki, cinayətkarlığın sürətlə artan forması var. Digər tərəfdən, kiber məkanda törədilən bu növ cinayətlər cinayətin yeni növü olduğundan, istintaq orqanları və ədalət mühakiməsini həyata keçirən məhkəmələr üçün anlaşılması və alışılması vaxt aparan fenomendir. Xüsusilə hüquq mühafizə orqanları əməkdaşlarının və hakimlərin bu mövzuda ciddi və mütəmadi təlimlərə ehtiyacı var. Üstəlik, cinayətlərin törədilməsinin yeni üsulları sürətlə ortaya çıxdığından, bu orqanların öz biliklərini daim yeniləmələri vacibdir [25, s.140]. Bundan başqa, müqayisəli hüquqda kibercinayətlərin tərifi vahid deyil və mövcud tərifl ər həmişə aydın deyil. Bununla belə, maddi cinayət hüququ baxımından müşahidə edilən fərqlər də effektiv hüquqi yardımın qarşısını alır. Buna görə də kibercinayətlərə görə tətbiq edilən cəzaların unifikasiyası vacibdir. Qanunvericilik yenilənmədikdə və informasiya texnologiyalarının aşkar etdiyi cinayət növlərinə klassik cinayət növləri tətbiq olunduqda, cinayətkarı cəzalandırmaq heç də həmişə mümkün olmur. Sürətlə inkişaf edən texnologiya kibercinayətkarlığın yeni formalarını ortaya qoyur ki, bu da mövcud qanunvericilik bazasının, hətta yeni qaydalar qəbul edən dövlətlər üçün də eyni sürətlə dəyişdirilməsini və inkişaf etdirilməsini tələb edir [13]. Digər tərəfdən, kiber-

cinayətlərin aşkar edilməsi üçün lazım olan sübutların növü və xarakteri, habelə onun əldə edilməsi üsulları ənənəvi cinayətlərdən fərqlidir. Sübutların əldə edilməsi çətin olsa da, həm də onların məhkəmələr üçün məqbul olan və mövcud prosessual qaydalara uyğun toplanması vacibdir. Bu, "potensial hüquqi sübutların əldə edilməsi üçün kompüter müayinəsi və təhlil üsullarından istifadə" ilə məşğul olan "rəqəmsal məhkəmə ekspertizası" adlı sahənin əhəmiyyətini ortaya qoyur. Bu baxımdan, bu cinayətləri araşdıracaq kadrların çox ciddi təcrübəyə malik olması vacibdir [14, s.33-34]. Digər tərəfdən, rəqəmsal sübutların hər an itirilə bilməsi ehtimalı qarşısında milli və beynəlxalq əməkdaşlıq prosesinin sürətlə davam etdirilməsi vacibdir. Məsələn, mobil telefonlarda mövcud olan və istintaq üçün sübuti əhəmiyyət daşıyan rəqəmsal sübutların əldə edilməsi zamanı müstəntiq və mütəxəssislər bir neçə metoddan istifadə edir. Bu metodların hansı dərəcədə effektiv olması və əldə edilmə prosesində rəqəmsal sübuta ziyan vurulmaması ən prioritet addım hesab olunmalıdır [15, s.371].

Göründüyü kimi, kibercinayətkarlıqla mübarizə özlüyündə bir çox cəhətləri ilə seçilən və həddindən çox diqqət, peşəkar bilik və bacarıq tələb edən mürəkkəb prosesdir. Təbii ki, qeyd olunan problemlər bu prosesin sadəcə bir hissəsidir. Məhz bu konteksdə, kibercinayətlərlə mübarizə aparılmasında üzləşilən prioritetik çətinlikləri xarakterinə görə aşağıdakı kimi qruplaşdıra bilərik:

Kibercinayətlərin mürəkkəb təbiəti. Kibercinayətlərin araşdırılması və təqib edilməsində çətinliklərdən biri kibercinayətkarların şəxsiyyətlərinin anonimliyidir. Cinayətkarlar istifadəsində heç bir məhdudiyyəti olmayan informasiya sistemlərindən istifadə etməklə dünyanın hər tərəfinə çata bilirlər [6]. Buna görə də kiberməkanda cinayətkarları aşkar etmək çox çətindir və onları izləmək üçün heç bir mexanizm yoxdur. Kibercinayətkarların müəyyən edilməsinə İP (Internet Protocol Address) ünvanları vasitəsilə nail olmaq olar. Lakin cinayətkarın həqiqi ünvan məlumatını əldə etmək həmişə mümkün olmur. Cinayətkar başqasının kompüter sistemindən, internet kafedəki kompüterdən və ya hava limanlarında, restoranlarda və ya otellərdə ictimai internet bağlantılarından istifadə etməklə cinayət törədə bilər. Üstəlik, İP ünvanı aşkarlansa belə, cinayətkarın şəxsiyyəti haqqında məlumatın xidmət təminatçısına açıqlanmaması və ya real məlumatın verilməməsi problemi yarana bilər [11, s.3]. Şəxsiyyətləri gizlətmək üçün "TOR (The Onion Router)" və ya "Psiphon" kimi müxtəlif rabitə vasitələrindən istifadə olunması isə başqa bir problemi ortaya çıxarır. Bu, İP ünvanını izləməyi demək olar ki, qeyrimümkün edir. Məsələn, zərərli proqramlar istehsal edən və bütün dünyada kriptovalyutaları idarə edən platforma olan Avalanche, pozulmaların qarşısını almaq və şəxsiyyətini gizlətmək üçün sürətli axın texnikasından istifadə etdi. Sürətli axın vasitəsilə İP ilə əlaqəli məlumatlar bir və ya bir neçə internetə qoşulmuş kompüterdən botnetlər vasitəsilə tez bir zamanda bir çox müxtəlif

kompüterlərə ötürülür. Beləliklə, o, həm kompüterin İP ünvan qeydlərini, həm də İP ünvanını yaradan xidmətləri dəyişir [3, s.117].

Bir dövlətin kibercinayətkarlıqla bağlı qanunvericilik bazası nə qədər təkmil olsa da, kibercinayətkarlar aşkar edilmədikcə bu qanunlar tətbiq edilməyəcək. Başqa sözlə, kibercinayətkarlıqla bağlı qanunlar boşluqda həyata keçirilə bilməz. Bu çətinliyi aradan qaldırmaq üçün istifadəçinin informasiya sistemlərindən istifadə edərkən özünü tanıması məcburi olmalıdır. Lakin insan haqları müdafiəçiləri bu vəziyyətin fərdlərin şəxsi toxunulmazlıq hüquqlarını pozduğunu əsas gətirərək buna qarşı çıxırlar [11, s.4]. Digər problem hüquq-mühafizə orqanları tərəfindən kibercinayətlərlə bağlı sübutların əldə edilməsi və qorunmasıdır. Əsl kibercinayətkarı müəyyən etmək üçün onu törədənin törətdiyi cinayət də sübuta yetirilməlidir. Bu cinayətləri sübut edən sübutların növləri və toplanma üsulları klassik cinayətlərdən tamamilə fərqlidir. Kibercinayətin törədildiyi yer informasiya sistemidir. Bu səbəbdən bu sistemlərdə cinayətin törədilməsinə dair sübutlar axtarılır. Lakin bu qeyri-maddi sübutların xarakteri müvəqqətidir və istənilən vaxt tamamilə və ya qismən itirilə bilər. Eyni zamanda, bu sübutlar asanlıqla dəyişdirilə və ya kodlaşdırıla bilər [21, s.32].

Bundan əlavə, bu gün kibercinayətkarlığın aləti olan informasiya sisteminin yaddaş tutumunun xeyli artdığı görünür. Sübut tapmaq üçün yüz minlərlə məlumat axtarılmalıdır. Bəzi hallarda kibercinayətlərlə bağlı məlumatlar bir çox müxtəlif ərazilərdə yerləşən informasiya sistemlərində saxlanıla bilər. Bu vəziyyət hüquq-mühafizə orqanları üçün yeni problem yaradır və həmçinin sübutların əldə edilməsi prosesini çox mürəkkəbləşdirir. Digər tərəfdən, məlumatlar şifrələnə bilər. Buna görə də hüquq-mühafizə orqanlarının məlumatların şifrəsini açmadan oxuması qeyri-mümkün olur. Daha doğrusu, parolları deşifrə etmək üçün çox vaxt ayırmaq lazımdır. Buna görə də bu virtual dünyada sübut əldə etmək və təhlil etmək üçün kompüter kriminalistikası sahəsində yüksək səviyyədə biliyə malik ciddi İT təcrübəsi tələb olunur [10, s.95].

Yurisdiksiya problemi. Kibercinayələtlərlə mübarizədə digər çətinlik cinayəti törədən şəxsin yerinin müəyyən edilməsi və onun hansı qanunvericilik ilə məsuliyyətə cəlb edilməsindədir. Bu baxımdan, yurisdiksiyanın müəyyən edilməsi vacib əhəmiyyətə malikdir. Beynəlxalq hüquqda səlahiyyət dövlətin şəxslərə və əşyalara təsir və ya sərəncam vermək gücü kimi müəyyən edilə bilər. Bu mənada səlahiyyət üç əsas anlayışı əhatə edir: qanunvericilik orqanı, icra hakimiyyəti və məhkəmə hakimiyyəti. Klassik olaraq bu üç səlahiyyət növü əsasən ərazi prinsipinə əsaslanır [20, s.88] Bununla belə, bəzi hallarda bu prinsip qeyri-kafi olur və şəxsiyyət prinsipi, müdafiə prinsipi və ya universal yurisdiksiya prinsipi ərazi prinsipini tamamlayır. Ərazi prinsipinə uyğun olaraq, dövlətin səlahiyyəti onun öz coğrafi

sərhədləri daxilində quru, su, hava və kosmos sahələrində həyata keçirilə bilər. Başqa sözlə, dövlətin bu sahələr üzrə əməlin cinayətin maddi tərkibi olub-olmadığını müəyyən etmək, səlahiyyətli məhkəmə orqanlarını və tətbiq olunacaq qanunları müəyyən etmək səlahiyyəti var [16]. Ona görə də dövlətlər bu səlahiyyətdən başqa dövlətlərin yurisdiksiyasında istifadə edə bilməzlər. Bu klassik yurisdiksiyalar quruda, suda, havada və kosmosda müəyyən və sabit sərhədlərə malikdir. Bu ərazilərdə cinayət törədildikdə onun harada törədildiyini və son nəticədə hansı dövlətin yurisdiksiyasına düşəcəyini müəyyən etmək çətin deyil. Lakin kibercinayətlər heç bir sərhəd tanımayan və heç bir dövlətin yurisdiksiyasında olmayan kiberməkanda törədilir. Bu cür cinayətləri dünyanın istənilən yerində evdə oturan, informasiya şəbəkələrinə qoşulmuş kompüterdən istifadə edən şəxs törədə bilər. Bu zaman tətbiq olunan qanunun və səlahiyyətli məhkəmənin müəyyən edilməsi üçün cinayətin harada törədildiyi sualı yarana bilər. Kibercinayətkarlığın hərəkətlərini dəqiq müəyyən etmək çox çətindir. Yurisdiksiya məsələsi, xüsusilə kibercinayəti təşkil edən maddi elementlər müxtəlif dövlətlərdə törədildikdə daha da mürəkkəbləşir [9, s.45].

Cinayətin hansı elementlər üzrə törədilmiş hesab ediləcəyi (cinayətin motivi, səbəb-nəticə əlaqəsi və s.) və cinayətin harada törədilmiş hesab ediləcəyi ayrı-ayrı məsələlərdir. Məsələn, informasiya texnologiyaları vasitəsilə nifrət nitqi və ya uşaq pornoqrafiyası kimi məzmunla bağlı cinayətlərdə maddi elementin harada baş verdiyini və informasiya sisteminin harada yerləşdiyini müəyyən etmək kimi çətinliklərlə qarşılaşılır. Bundan əlavə, məzmun bir yerə yüklənməyə başlaya və başqa ölkədə sonlana bilər və ya cinayətkar bir ölkədə olarkən, məzmunu yaradaraq onu başqa ölkədə ictimaiyyətə təqdim etmiş ola bilər. Kiberhərəkət birdən çox ölkənin yurisdiksiyasına daxil ola bilər. Belə problemləri həll edə biləcək beynəlxalq orqan və ya məhkəmə olmadığı üçün dövlətlər bu problemi öz milli qanunlarına daxil edilmiş səlahiyyət qaydaları ilə həll etməyə çalışır [2].

Hazırda kibercinayətkarlıqla bağlı beynəlxalq səviyyədə fəaliyyət göstərən xüsusi orqan və ya məhkəmə yoxdur. Beynəlxalq Cinayət Məhkəməsinin (BCM) yurisdiksiyasına daxil olan cinayətlər, Roma Statutunun 5-ci maddəsinə əsasən, soyqırım cinayətləri, müharibə cinayətləri, insanlığa qarşı cinayətlər və beynəlxalq ictimaiyyəti təhdid edən təcavüz cinayətləridir [30]. Bu kontekstdə, kibercinayətlər Roma Statutuna açıq şəkildə daxil edilmir. Bununla belə, bəzi müəlliflərin fikrincə, o, kiber hərəkətlər adlanan cinayətlərin törədilməsi üçün yeni üsul yarada və onların törədilməsini asanlaşdıra və ya həvəsləndirə bilər. Buna görə də sözügedən hərəkətlər BCM-in 414-cü hissəsinin yurisdiksiyasına aid ola bilər. İlk baxışdan, kiber hərəkətlərin hücum cinayəti çərçivəsində nəzərdən keçirilə biləcəyini görmək olar [4, s.320]. Kiberhücum hücum cinayəti təşkil etmək üçün müəyyən meyarlara

cavab verməlidir. Roma Statutuna əlavə edilmiş 8-ci maddənin birinci bəndinə görə, təcavüz cinayətinin baş verməsi üçün bu, dövlətin hərbi və siyasi hərəkətlərini effektiv şəkildə idarə etmək və ya idarə etmək səlahiyyətinə malik olan şəxs tərəfindən törədilməlidir. Bu rəhbərlik şərti ümumiyyətlə kiberhücumlarda yerinə yetirilmir. Lakin DOS hücumlarında (Denial-of-service attacks) bu şərt yalnız müstəsna hallarda qarşılana bilər. Məsələn, 2008-ci ildə rusların Gürcüstan hökumətinə qarşı həyata keçirdikləri DOS hücumları nəticəsində Gürcüstan hökumətinin öz vətəndaşları ilə ünsiyyətinin qarşısı alınıb [26, s.200].

Beynəlxalq hüquqda beynəlxalq və ya hər hansı bir milli məhkəmənin kibercinayətlərlə bağlı yurisdiksiyaya malik olmasının iki yolu var. Birincisi, universal yurisdiksiya və ya universallıq prinsipi, digəri isə tamamlayıcılıq prinsipidir. Beynəlxalq əməkdaşlıq tələb edən transmilli cinayətlərə tətbiq edilərkən universallıq prinsipi vacibdir [26, s.223]. Bu prinsipə əsasən, dövlətlər bütövlükdə beynəlxalq ictimaiyyəti təhdid edən cinayətlərin harada törədilməsindən, cinayəti törədənin və ya qurbanın vətəndaşlığından asılı olmayaraq, onların yurisdiksiyasına malik ola bilərlər. Başqa sözlə, ərazi, şəxsiyyət və ya müdafiə prinsiplərinə görə yurisdiksiyaya malik olmayan və piratçılıq və beynəlxalq terrorizm kimi insanlığa qarşı mütəşəkkil transmilli cinayətlərin təqibində özünü səlahiyyətli hesab edən dövlətdir [19, s.126]. Universallıq prinsipi istənilən dövlətin beynəlxalq və ya milli məhkəmələrinə cinayətkar üzərində yurisdiksiya axtarmağa imkan verir və kibercinayətlərin yaratdığı problemlərin həllini təmin edə bilər. Bəşəriyyətin düşməni olan "hostis humani generis" hesab edilən pirat cinayətləri törədildiyi yerdə mühakimə oluna bilər. Birləşmiş Millətlər Təşkilatının 1982-ci il tarixli "Dəniz Hüququ Konvensiyası"na və beynəlxalq adət-ənənələrə əsasən, açıq dənizdə törədilən dəniz quldurluğu cinayətləri istənilən dövlət tərəfindən mühakimə oluna bilər [31]. Eynilə, kibercinayətkarları bəşəriyyətin, kiberməkanı isə açıq dəniz kimi düşmən hesab etmək olar. Pirat cinayətləri üzərində universal yurisdiksiyanın tətbiqi üçün əsas odur ki, beynəlxalq ticarət təhlükə altındadır və DOS hücumları da böyük kommersiya veb-saytlarını sıradan çıxara və zədələyə bilər. Bu halda universal yurisdiksiyanın tətbiqində kibercinayətlərə üstünlük verilməlidir. Bununla belə, kibercinayətlərin əhatə dairəsinin müəyyən edilməsi universallıq prinsipinin kibercinayətlərə tətbiq edilməsində çətinlik yarada bilər. Sözügedən kibercinayətlərin əhatə dairəsi diqqətlə müəyyən edilərsə, bu, kibercinayətlərə qarşı mübarizədə çəkindirici vasitə ola bilər. Tamamlayıcılıq prinsipinə əsasən, milli məhkəmələr cinayətlər üzərində öz yurisdiksiyasını həyata keçirərkən üstünlüyə malikdirlər. Bu prinsip Roma Konfransından əvvəl "beynəlxalq cinayət mühakiməsinin milli cinayət ədalət mühakiməsi ilə tamamlanması" ifadəsi ilə vurğulanmışdır [12, s.171]. Bununla belə, milli məhkəmələrin təqib etmək istəmədiyi (istəksizliyi) və ya təqib etmək

üçün texniki imkanlarının olmadığı (qeyri-kafi) hallarda BCM cinayətlə bağlı yurisdiksiyaya malik ola bilər. Beləliklə, tamamlayıcılıq prinsipi dövlətlərin milli suverenliyinə hörmət edir. Tamamlayıcılıq prinsipi bəzi dövlətlərin kibercinayətkarları təqib etməməsi və ekstradisiya etməməsi problemini həll edə bilər. Bununla belə, bir çox müxtəlif dövlətlərin qanunlarının əhatə dairəsinə düşən kibercinayətkarlıq problemini yenə də tam şəkildə həll etmir. Bu zaman həmin məsələni yalnız dövlətlərüstü məhkəmə və ya orqan həll edə bilər.

Beynəxlalq əməkdaşlıqla bağlı çətinliklər. Kibercinayətlərlə mübarizədə üzləşilən digər bir problem beynəxlalq səviyyədə əməkdaşlığın istənilən səviyyədə olmamasıdır. Beynəlxalq əməkdaşlığın əsas məqsədi müxtəlif ölkələrdə cinayət törədənlərin cəzasız qalmasının qarşısını almaqdır. Cinayətkarlara qarşı mübarizə, günahkarların törətdikləri cinayətlərə görə alacaqları cəzaların proqnozlaşdırılmasını tələb edir. Cinayət təkcə törədildiyi ölkənin deyil, bütün ölkələrin təhlükəsizliyini təhdid edə bilər. Xüsusilə kibercinayətlər barədə danışsaq, o, dövlətin öz ərazi sərhədlərini keçir və bu cür cinayətləri törədənlərin cəzasız qalma ehtimalı daha yüksəkdir. Ona görə də bütün dövlətlər, beynəlxalq təşkilatlar bir-biri ilə əməkdaşlıq etmək üçün birgə fəaliyyət göstərməlidirlər. Hətta dövlətlər kibercinayətlərlə bağlı dayanıqlı və effektiv maddi və prosessual qaydalar qəbul etsələr belə, bu kifayət etməyəcək. Bu cinayətlərə qarşı mübarizə dövlətlər arasında əməkdaşlıq mexanizmlərinə əsaslanır. Doktrinada qeyd edildiyi kimi, kibercinayətkarlıqla mübarizə "ya qlobal xarakter daşıyacaq, ya da heç bir məna kəsb etməyəcək" [23, s.188]. Başqa sözlə, beynəlxalq əməkdaşlığa "vacib olmayan" şərt kimi baxılır. Bir neçə dövlət iştirak etmədikdə, cinayətkarlar ekstradisiya və qarşılıqlı hüquqi yardım müqavilələrində iştirak etməyən dövlətlərdən sığınacaq kimi istifadə edib, oradan öz hərəkətlərini davam etdirə bilərlər. Lakin beynəlxalq əməkdaşılqda mövcud çətinliklərin bir neçə təbii səbəbi vardır. Bunlardan ən vacibi kimi 3 əsas problemi qeyd edə bilərik: 1) dövlətlərin hüquq sistemlərindəki fərqliliklər; 2) beynəxlalq müqavilələrin natamamlığı; 3) prosessual qaydaların həddindən çox uzun və vaxt aparan olması.

I - Dövlətlərin hüquq sistemlərindəki fərqliliklər. İlk olaraq, hüquq sistemindəki fərqliliklərdən danışsaq, deyə bilərik ki, hüquq sistemləri cəmiyyətlərin müxtəlif ehtiyaclarına və reallıqlarına uyğun olaraq formalaşır. Qanunlar cəmiyyətdə din, mədəniyyət, tarix, sosiologiya və coğrafiya kimi bir çox amillərin əksidir. Bunun təbii nəticəsi olaraq dövlətlərin müxtəlif maddi və prosessual cinayət qanunları mövcuddur [22]. Kibercinayətkarlığa gəldikdə isə problem daha da ciddiləşir. Maddi hüquq baxımından hansı hərəkətlərin cinayət sayılması məsələsi dövlətlər arasında çox dəyişir. Birinci fəsildə müzakirə edildiyi kimi, cinayətin termini və tərifi ilə bağlı konsensus yoxdur. Bu əməl qurbanın ölkəsində cinayət sayıla bilər, lakin onu törədənin ölkəsində cinayət sayıla bilməz və ya başqa cür təyin oluna bilər. Məsələn,

Almaniya və Avstriyada "milli-sosialist" təbliğatı cinayət hesab edilərək cəzalandırıldığı halda, ABŞ, Avstraliya və Kanadada fikir azadlığı çərçivəsində sayılır və cinayət təşkil etmir [32, s.113]. Eyni şəkildə, nifrət nitqi aktları Avropa ölkələrində nifrət cinayətləri təşkil edir, lakin ABŞ-da ifadə azadlığı hesab olunur. Məsələn, "Yahoo! LICRA-ya qarşı" işi bu baxımdan ən bariz nümunədir. Yahoo! şirkəti Üçüncü Reyxin xatirə əşyalarının fotoşəkilləri, satışı, mübadiləsi və ya nümayişi kimi nasistlərlə əlaqəli materiallara giriş Fransa cinayət qanunvericiliyinə zidd olaraq bu veb-saytlar vasitəsilə təmin edilirdi. Bu səbəbdən 2000-ci ildə Fransanın qeyri-kommersiya təşkilatı İrqçilik və Antisemitizmlə Mübarizə Beynəlxalq Liqası (LICRA) Yahoo! Şirkətinə qarşı açılan iddia nəticəsində Paris məhkəməsi Yahoo! şirkətin nasistlərlə əlaqəli bütün materiallara girişi əngəlləmək üçün lazımi tədbirlər görəcəyinə qərar verdi. Fransada Yahoo! (www.yahoo.fr) məhkəmənin qərarına uyğun olaraq bütün nasist materiallarını yığışdırdı. Bununla belə, Paris məhkəməsi sözügedən məzmunun fransızlar üçün əlçatan olan Yahoo!-nun qlobal saytından silinməsini istəmişdi. Yahoo bu sorğunu rədd etdi. Məhkəmə Kaliforniyanın Şimal Dairə Məhkəməsində iddia qaldıraraq, Paris Məhkəməsinin qlobal internet saytından (www.yahoo.com) məzmunu silmək qərarının ifadə azadlığını tənzimləyən ABŞ Konstitusiyasını pozduğunu iddia etdi. Bu məhkəmə Paris Məhkəməsinin qərarının Amerika Konstitusiyasına zidd olduğuna və ABŞ-da tətbiq edilə bilməyəcəyinə qərar vermişdir [24, s.214-220]. Dövlətlərin cinayət qanunvericiliyindəki maddi normalar fərqli olduğu kimi, nəzərdə tutulan prosedurlar da fərqlidir. Dövlətdə törədilmiş cinayətlərin araşdırılması, mühakimə olunması və müvafiq sübutların toplanması üsulları həmin dövlətdə səmərəli şəkildə həyata keçirilə bilər. Amma başqa dövlətdə qeyri-adekvat və ya qeyri-qanuni ola bilər. Bu uyğunsuzluq dövlətlərin milli qanunları arasında ziddiyyətlərin yaranmasına səbəb olur. Məsələn, uzaqdan axtarış tədbirləri Böyük Britaniya və ABŞ-da cinayətlərlə bağlı sübutların əldə edilməsinin hüquqi üsullarından biridir. Bununla belə, digər ölkələrdə bu, fərdin məxfilik hüquqlarının pozulmasını təşkil edən qeyri-qanuni tədbir hesab olunur [28]. Əslində kibercinayətin araşdırılmasında ən kritik məsələlərdən biri məlumatların saxlanmasıdır. Dövlətlərin məlumatların saxlanması üçün müxtəlif tələbləri var.

Dövlətlərin cinayət hüquq sistemlərindəki fərqlər kibercinayətlərlə bağlı müddəaların bir-biri ilə uzlaşmamasına və qanunların toqquşmasına səbəb olur. Bu, həm də beynəlxalq əməkdaşlığa əngəl törədir. İkili cinayət məsuliyyəti hüquqi yardım və ekstradisiya prosedurlarının həyata keçirilməsi üçün ilkin şərtdir. Bu şərtə görə, hüquqi yardım haqqında sorğunun predmeti olan cinayət həm sorğu edən dövlətin, həm də sorğu edilən dövlətin cinayət qanunvericiliyində cinayət kimi tənzimlənməlidir. İkiqat cinayət şərtinin yerinə yetirilməməsi beynəlxalq əməkdaşlıq çərçivəsində sübutların əldə edil-

məsi kimi əməliyyatların pozulmasına səbəb ola bilər [7, s.255]. Bundan əlavə, "yurisdiksiya alış-verişi" konsepsiyası həyata keçiriləcək. Müvafiq olaraq, cinayətkarlar kibercinayətləri cəzalandırmayan və ya daha az cəzalar təyin edən dövlətlərdə yerləşir və fəaliyyət göstərirlər. Başqa sözlə desək, bir ölkədə əməlin cinayət sayılması, digər ölkədə cinayət hesab edilməməsi cinayətin təqibi prosesini çətinləşdirir və beynəlxalq əməkdaşlığı mümkünsüz edir [8, s.477]. Bu problemi aradan qaldırmaq üçün dövlətlər kibercinayətkarlıqla bağlı qanunlarını uyğunlaşdırmalıdır. Lakin dövlətlərin quruluşu, tarixi, mədəniyyəti, sosial dinamikası və hüquqi ənənələri kimi müxtəlif amillərə görə uyğunlaşma prosesi kifayət qədər çətin görünür. Kibercinayətkarlığa gəldikdə "bir ölçü hamıya uyğundur" prinsipi uyğun deyil. Odur ki, bu cinayətlərə qarşı mübarizə dövlətlərin müxtəlif daxili şərtlərini nəzərə alan uyğunlaşma tələb edir. Yeri gəlmişkən, qeyd etmək lazımdır ki, qanunların uyğunlaşdırılması "eyniliyin" təmin olunması demək deyil. Bunun məqsədi mühüm tamamlayıcılıqdır. Başqa sözlə, milli və regional fərqlər mümkün qədər azaldılmalı və icra mexanizmlərinin səmərəli işləməsinə imkan verəcək şəkildə uzlaşdırılmalıdır.

II - Beynəlxalq müqavilələrin natamamlığı. Dövlətlər arasında əməkdaşlığın ən mühüm mexanizmləri ekstradisiya və qarşılıqlı hüquqi yardımdır. Ötən illərdə dar saxlanılan qarşılıqlı hüquqi yardımın əhatə dairəsi günügündən genişlənir. Bu gün hüquqi yardım məlumatların verilməsi və cinayət tərkibi haqqında məlumatların göndərilməsi, məhkəmə qərarlarının və məhkəmə prosesi ilə bağlı sənədlərin təqdim edilməsi, şahidlərin, ekspertlərin və təqsirləndirilən şəxslərin dindirilməsi, sübut məqsədi ilə axtarış və götürmənin təyin edilməsi, əşyaların və ya sənədlərin göndərilməsi və həbs edilmiş şəxsin başqa ölkəyə göndərilməsi kimi məsələləri əhatə edir. Dövlətlərarası müqavilələr olmadığı halda, dövlətlərin beynəlxalq hüquqa əsasən kibercinayətkarlıq və ya hər hansı digər cinayətlə bağlı digər dövlətlərlə əməkdaşlıq etmək öhdəliyi yoxdur [17, s.220]. Ona görə də bu məsələdə beynəlxalq hüquqda ciddi çatışmazlıqlar var. Başqa sözlə, sözügedən hüquqi yardım və ekstradisiya prosesləri yalnız dövlətlər arasında imzalanmış ikitərəfli və ya çoxtərəfli sazişlər vasitəsilə həyata keçirilir (məsələn, Avropa Şurasının Kibercinayətkarlıq haqqında Konvensiyası, Cinayət İşləri üzrə Qarşılıqlı Yardım haqqında Avropa Konvensiyası və s.). Bununla belə, hazırda kibercinayətkarlıqla mübarizə üzrə heç bir beynəlxalq saziş mövcud deyildir. İkitərəfli və ya çoxtərəfli regional sazişlərin effektivliyi iştirakçı dövlətlərlə məhdudlaşır. Buna görə də kibercinayətkarlıqla qlobal mübarizədə böyük çətinliklər yaranır.

Kibercinayətkarlıq sahəsində əməkdaşlıq haqqında razılaşmaların olmamasının ən mühüm nümunəsi 2000-ci ildə Gorşkov və İvanov hadisəsidir. Rusiyalı hakerlər Vasiliy Qorşkov və Aleksey İvanov Amerika şirkətlərinin İT sistemlərinə qanunsuz hücum edərək, onların məlumatlarını əldə edərək,

onları şantaj etmişdi [29]. ABŞ və Rusiya arasında ekstradisiya müqaviləsi olmadığı üçün Rusiyanın şübhəliləri təhvil verməsi mümkün olmayıb. Buna görə də, FTB cinayəti araşdırmaq və mühakimə etmək üçün şübhəliləri ABŞ-a gətirdi. FTB agentləri şübhəliləri "Invita" adlı saxta kompüter şirkəti vasitəsilə ABŞ-a gətirdilər və müsahibənin bir hissəsi olaraq, kompüter bacarıqlarını nümayiş etdirmək üçün FTB tərəfindən qurulan şəbəkənin hərfini yazmağı xahiş etdilər. Şübhəlilərin ABŞ-da istifadə etdikləri kompüterlərə daha əvvəl gizli proqram təminatı quraşdıran FTB Rusiyadakı kompüterlərə daxil olan parol və məlumatları əldə etmişdi. Bununla da, Rusiyadakı kompüterlərin məlumatlarından və sübutlarından istifadə edilərək təqsirləndirilən şəxslərin mühakimə olunmasına və həbsinə nail olunmuşdur. Rusiya tərəfi isə buna etiraz etdi və cinayətkarların ekstradisiyasını tələb etdi, lakin razılaşma olmadığından ABŞ bu tələbə məhəl qoymadı [18].

III - Prosessual qaydaların həddindən çox uzun və vaxt aparan olması. Kibercinayətlərlə bağlı ekstradisiya və qarşılıqlı hüquqi yardım haqqında sorğuların verilməsi, qəbulu və sonrakı prosedurları hər iki dövlətdə ənənəvi diplomatik və ya məhkəmə orqanları vasitəsilə həyata keçirilir. Bu alətlər (hüquqi əməliyyatlar, sənədlərin tərcüməsi və s.) uzun və mürəkkəbdir və buna görə də daim inanılmaz sürətlə inkişaf edən və sərhədləri aşan kibercinayətlərə qarşı aciz qalır. Başqa sözlə, ənənəvi beynəlxalq hüquqi yardım rejimi çox vaxt qeyri-adekvatdır və kibercinayətkarlıq zamanı yardım üçün müraciətləri yerinə yetirmək iqtidarında deyil. Məsələn, informasiya texnologiyaları sahəsində dünyanın ən qabaqcıl ölkəsi olan ABŞ elektron cinayətkarların qeydiyyatı ilə bağlı digər dövlətlərin sorğularını yerinə yetirmək üçün orta hesabla 10 ay və ya daha çox vaxt sərf edir [26, s.207].

Cinayət törədərkən cinayətkarın əlaqəsi bir çox ölkədən keçərsə, hüquqi yardım prosesi daha uzun olacaqdır. Bu vəziyyət cinayətlə bağlı məlumatların və sübutların itirilməsi ehtimalını da artırır. Bu səbəbdən dövlətlər arasında klassik əməkdaşlıq idarəçiliyindən imtina edilməli və yeni sürətli üsullar tapılmalıdır. Məsələn, beynəlxalq fövqəladə hallar üçün 24/7 şəbəkələrin inkişaf etdirilməsi, beləliklə, müstəntiqlərin digər ölkələrdəki ekspertlərlə əlaqə saxlamasını təmin edə bilər. Beynəlxalq əməkdaşlığın ənənəvi üsullarının qeyri-adekvat olması ilə yanaşı, hüquqi yardım əməliyyatları ilə bağlı sənədlərdəki hər hansı çatışmazlıqların geri qaytarılması üçün əsas kimi istifadə edilməsi, hüquqi yardım sənədlərinin göndərilməsi ilə bağlı məhkəmələrin birbaşa Ədliyyə Nazirliyi ilə əlaqə saxlamaması, hüquq-mühafizə orqanlarının kifayət qədər hüquqi biliklərə malik olmaması, istintaq proseslərinin kifayət qədər aparılmaması, xarici dildə kifayət qədər danışıq aparmaması kimi praktikada bir çox çətinliklər var.

Nəticə. Kibercinayətkarlıqla mübarizədə üzləşilən çətinliklərin aradan qaldırılması üçün həyata keçirilməsi lazım olan tədbirlər həm milli, həm də

beynəxalq səviyyədə icra tətbiq olunmalıdır. Milli səviyyədə kibercinayətkarlıqla mübarizənin başlanğıc nöqtəsi məhz elə dövlətlərin yerli cinayət və cinayət-prosessual qanunveriliciyidir. Kibercinayətkarlığın güclü hüquqi tənzimlənməsi olmadığı halda, dövlətlər kibercinayətkarlar üçün təhlükəsiz sığınacaq təşkil edir. Buna görə də dövlətlər kibercinayətlərin inkişafı ilə paralel olaraq kibercinayətlərlə bağlı milli maddi və prosessual cinayət qanunlarını tənzimləməli, inkişaf etdirməli və yeniləməlidirlər. Həmçinin cinayətlərin araşdırılması və təqibi üçün klassik alətlər kibercinayətlərə qarşı qeyri-adekvatdır və xüsusilə rəqəmsal mühitdə sübutların əldə edilməsi və qiymətləndirilməsində xüsusi rəqəmsal sübut laboratoriyasına malik rəqəmsal məhkəmə ekspertizası infrastrukturu tələb olunur. Hüquq-mühafizə orqanları kibercinayətlərin təhqiqatı və ibtidai istintaqı üçün yeni və sürətli metodlar hazırlamalı, kibercinayətlərin qarşısının alınması üçün texniki cəhətdən hazır olmalı və təchiz olunmalıdırlar.

Bu məqsədlə, kibercinayətkarlıqla mübarizə üçün xüsusi təşkilatlar yaradılmalıdır. Bundan başqa, dövlətlər müxtəlif İT infrastrukturlarını inkişaf etdirməli və lazımi texniki tədbirlər görməlidirlər. Bu nöqtədə kiber sahədə təhlükəsizlik və məxfiliyin qorunması və kiberhücumların qarşısının alınması üçün hərtərəfli layihələr həyata keçirilməli və strateji planlar hazırlanmalıdır. Bundan başqa, əksər kibercinayətlər barədə məlumat verilmir. Bunun səbəbi, zərərçəkmişin kibercinayətə məruz qaldığını və bu barədə necə məlumat verəcəyini bilməməsi, həmçinin bəzi şirkət və qurumların onların reputasiyasının zədələnəcəyini düşünməsidir. Odur ki, kibercinayətlər və onların necə xəbər veriləcəyi barədə ictimaiyyəti məlumatlandırmaq üçün araşdırmalar və fəaliyyətlər təşkil edilməlidir. Milli səviyyədə hüquq-mühafizə orqanları arasında həm öz aralarında, həm də özəl sektorla səmərəli əməkdaşlıq qurulmalıdır. Xüsusilə internet provayderləri məlumatlara çıxışın təmin edilməsində çox mühüm rol oynayırlar. Bir tərəfdən, xidmət təminatçısı cinayətkarların müəyyən edilməsində hüquq-mühafizə orqanlarına yardım etməli, digər tərəfdən isə şəxslərin hüquqlarını və şəxsi toxunulmazlığını qorumalı və sui-istifadə hallarına yol verməməlidirlər.

Digər tərəfdən, kibercinayətlərlə beynəxlalq səviyyədə mübarizə aparılması da vacib əhəmiyyətə malikdir. Başqa sözlə desək, kibercinayətkarlıqla mübarizənin başlanğıc nöqtəsi milli qanundursa, çıxış nöqtəsi beynəlxalq hüquqdur. Qlobal cinayət qlobal mübarizə tələb edir. Milli qanun çox vaxt transsərhəd kibercinayətlərə qarşı qeyri-adekvatdır. Bu kontekstdə, beynəlxalq əməkdaşlığı tənzimləyən beynəlxalq səviyyədə məcburi sazişə ehtiyac vardır. Bunun üçün ən mühüm vasitə Birləşmiş Millətlər Təşkilatıdır. BMT çərçivəsində sözügedən beynəlxalq konvensiyanın məqsədi kibercinayətlərlə bağlı dövlətlərin maddi və prosessual qanunlarını birləşdirmək və uyğunlaşdırmaqdır. Bu halda beynəlxalq əməkdaşlığın ilkin şərti olan ikiqat cəza-

landırma şərti reallaşacaq və kibercinayətlərin araşdırılması və təqibi üsulları ilə bağlı ölkələr arasında yaranmış fikir ayrılığı aradan qaldırılacaq. Ənənəvi beynəlxalq üsullar kibercinayətkarlığın təbiətinə uyğun deyil, çünki onlar səmərəsiz və uzundur. Kibercinayətkarlıqla mübarizə effektiv, sürətli və təkmil beynəlxalq əməkdaşlıq mexanizmlərini tələb edir. Transmilli kibercinayətlər çox vaxt birdən çox dövlətin yurisdiksiyası daxilində törədilə bilər ki, yaranan yurisdiksiya problemini həll edən heç bir beynəlxalq orqan və ya norma yoxdur. Belə görünür ki, kibercinayətkarlıq Beynəlxalq Cinayət Məhkəməsinin yurisdiksiyasına aid deyil. Bu problem üçün iki həll yolu təklif edilə bilər. Birincisi, kibercinayətkarlığın Beynəlxalq Cinayət Məhkəməsinin yurisdiksiyasına malik olduğu müharibə, insanlığa qarşı cinayətlər, soyqırım və təcavüz cinayətlərinə beşinci cinayət kimi əlavə edilməsidir. Digəri isə Beynəlxalq Cinayət Məhkəməsinə bənzər kibercinayətlər üzrə xüsusi beynəlxalq məhkəmənin yaradılmasıdır. Dövlətlər arasında təkcə məhkəmə əməkdaşlığı deyil, həm də polis sahəsində əməkdaşlıq da həyata keçirilməlidir. Polis əməkdaşlığında isə fəal rol oynayan mexanizmlər INTERPOL, EUROPOL, ASEANAPOL və AMERİPOL-dur. Həmçinin onu da qeyd edək ki, inkişaf etmiş dövlətlərlə inkişaf etməkdə olan və ya zəif inkişaf etmiş dövlətlər arasında informasiya texnologiyaları sahəsində böyük uçurum var. Bu uçurumun aradan qaldırılması və texnoloji biliklərin paylaşılması ümumdünya səviyyəsində kibertəhlükəsizliyin qorunub saxlanılmasında və kibercinayətkarlığa qarşı effektiv mübarizə aparılmasında mühüm töhfələr verəcəkdir.

ƏDƏBİYYAT

1. Akbulut, B.B. “Bilişim Suçları”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Milenyum Armağanı, Cilt 8, Sayı 1-2, - 2000.
2. Albert I. Aldesco, “The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime”, Loyola of Los Angeles Entertainment Law Review, Vol.23, No.1, - 2002, p. 89.
3. Bell, R.E. “The Prosecution of Computer Crime”, Journal of Financial Crime, Vol. 9, No. 4, - 2002, p.314.
4. Cammack, C. “The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression”, Tulane Journal of International & Comparative Law, Vol. 20, No. 1, - 2011, p. 319-324.
5. Clough, J. Principles of Cybercrime. Second edition. Cambridge University Press, - 2015. p.513.
6. Clough, J. “Cybercrime”, Commonwealth Law Bulletin, Vol. 37, No. 4, - 2011, p. 673.
7. Clough, J. “A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation”, Monash University Law Review, Vol. 40, No.1, - 2014, p. 701.
8. Csonka, P. “The Council of Europe’s Convention on Cyber-crime and Other European Initiatives”, Revue İnternationale de Droit Penál , Vol. 77, No. 3, - 2006, p.620.
9. David L. Speer, “Redefining Borders: The Challenges of Cybercrime”, Crime, Law and Social Change, Vol. 34, No. 3, - 2000, p. 260.
10. Ehuan, A. “Cybercrime and Law Enforcement Cooperation”, CyberForensic Understanding Information Security Investigations, Ed. Jennifer Bayuk, Germany, Springer, - 2010, p. 138.

11. Emmanuel Femi Gbenga Ajayi. “Challenges to Enforcement of Cyber-Crimes Laws and Policy”, Journal of Internet and Information Systems, Vol. 6, No.1, 2016, p. 4.
12. Erdal, S. “Uluslararası Ceza Mahkemesinin Ulus-Devlet Egemenliğine Etkisi”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi , C.XVIII, S. 1, - 2010, s. 195.
13. Gregor Urbas, Criminalising Computer Misconduct: Some Legal and Philosophical Problems, 14 Asia Pac. L. Rev. 95 (2006), p. 99.
14. Xəlilov, K. Rəqəmsal məhkəmə ekspertizasının müasir metodologiyası: Texnologiyanın rəqəmsal cinayət təqibində rolu. Qanun Nəşriyyatı, № 05 (355), - 2024, s.33-44.
15. Xəlilov, K. Kibercinayətlərin ibtidai istintaqında rəqəmsal sübutların əldə edilməsi və fərdi məlumatların mühafizəsi: qarşılıqlı əlaqə və müqayisəli təhlil. Doktorantların və gənc tədqiqatçıların XXVII r. elmi konfransı (NASCO XXVII). Materiallar toplusu – II hissə, - 2025. s.369-374.
16. Henriksen, A. International Law, 2. bs., United Kingdom, Oxford Universty Press, - 2019, p.85.
17. Inger Marie Sunde, “Cybercrime Law”, Digital Forensics, Ed.André Årnes, Hoboken John Wiley & Sons, - 2018, s. 111; Vatis, a.g.m., p.375.
18. Jean-Baptiste Maillart. “The limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”, ERA Forum, Vol. 19., No. 3., - 2019, p.384.
19. Keçeligl, M.D. “Evrensel Yargı Yetkisi: Ceza Hukuku Bağlamında Evrensellik İlkesine Bakış” Terazi Hukuk Dergisi, C.XIII, - 2018, s.143.
20. Khalilov, K. Extraterritorial Jurisdiction of the ECHR in the Context of Analysis of Relevant Cases: Which Model Is Effective? 10, Scopus Preview, Baku St. U. L.Rev.84, - 2024. p.84-120.
21. Kim-Kwang Raymond Choo. “Organised Crime groups in Cyberspace: a Typology”, Trends Organ Crim, Vol.11, No. 3, - 2008, p. 287.
22. Matthew R. Zakaras. “International Computer Crimes, General Report”, Revue internationale de droit pénal, Vol. 72, No. 3, 2001, p. 827.
23. Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 7. bs., Ankara, Seçkin Yayınları, - 2018, s. 256.
24. Okoniewski, E.A. “Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet”, American University International Law Review, Vol. 18., No.1, - 2002, p.380.
25. Özgür Uçkan/Yasin Beceni, Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, - 2004, s. 423.
26. Perloff-Giles, A. “Transnational Cyber Offenses: Overcoming Jurisdictional Challenges”, The Yale Journal of International Law, Vol. 43, No. 1, - 2018, p. 227.
27. Susan W. Brenner, Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?, 30, Rutgers Computer & Tech. L.J. 1 - 2004, p. 33.
28. Susan W. Brenner. “Law, Dissonance, and Remote Computer Searches”, North Carolina Journal of Law & Technology, Vol. 14, No.1, - 2012, p.124.
29. Susan W. Brenner, Joseph J. Schwerha IV, “Transnational Evidence Gathering and Local Prosecution of International Cybercrime”, The John Marshall Journal of Information Technology & Privacy Law, Vol. 20, No. 3, - 2002, p.347-348.
30. Ulusoy, O. Uluslararası Ceza Mahkemesi, Ed. Utku Kılınç, İzmir, Etki Matbaacılık Yayıncılık, - 2008, s. 22- 29.
31. United Nations Convention on the Law of the Sea. Available at: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf [accessed March 05, 2025].
32. Veli Özer Özbek, “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları”, DEÜHFD, C.IV, S.1., - 2002, s.130.

ПРАВОВЫЕ ОСНОВЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ: АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Ф.М.АББАСОВА, К.И.ХАЛИЛОВ

РЕЗЮМЕ

В наше время киберпреступность получила широкое распространение параллельно с бурным развитием информационных технологий и стала серьезной угрозой как международной, так и национальной безопасности. Многогранность и специфичность киберпреступности также усложняют методы и правила борьбы с ней. В этом смысле важнейшей задачей, стоящей перед правоохранительными органами и международными организациями, является глубокое понимание методов борьбы с киберпреступностью, совершенствование существующих методов или поиск новых путей, а также оперативное и эффективное решение возникающих на этом направлении трудностей. С этой целью в исследовании выявляются правовые основы борьбы с киберпреступностью и анализируются трудности в осуществлении этой деятельности. В данном исследовании также рассматриваются и представляются альтернативные решения проблем, возникающих в борьбе с киберпреступностью. В целях усиления этой борьбы отмечается важность совершенствования нормативно-правовой базы, использования современных методов расследования, расширения международного сотрудничества, специализации правоохранительных органов в области кибербезопасности.

Ключевые слова: киберпреступность, борьба, международное сотрудничество, юрисдикция, проблемы.

LEGAL BASIS OF COMBATING CYBERCRIME: CURRENT PROBLEMS AND SOLUTIONS

F.M.ABBASOVA, K.I.KHALILOV

SUMMARY

In our time, cybercrime has become widespread in parallel with the rapid development of information technologies and has become a serious threat to both international and national security. The multifaceted and specific nature of cybercrime also complicates the methods and rules of combating it. In this sense, the most important task facing law enforcement agencies and international organizations is to have a deep understanding of the methods of combating cybercrime, to improve existing methods or to look for new ways, as well as to solve the difficulties encountered in this direction in an operational and efficient manner. For this purpose, the study identifies the legal foundations of combating cybercrime and analyzes the difficulties in implementing this activity. This research also examines and presents alternative solutions to the problems arising in combating cybercrime. In order to strengthen this fight, the importance of improving the regulatory and legal framework, using modern investigative methods, increasing international cooperation, and specializing law enforcement agencies in the field of cybersecurity is noted.

Keywords: cybercrime, fight, international cooperation, jurisdiction, problems.