BAKI UNİVERSİTETİNİN XƏBƏRLƏRİ

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

KİBERTERRORÇULUQ – TERRORÇULUĞUN YENİ FORMASI KİMİ: ANLAYIŞI, İCTİMAİ TƏHLÜKƏLİLİYİ, CİNAYƏT-HÜQUQİ VASİTƏLƏRLƏ MÜBARİZƏ MƏSƏLƏLƏRİ

E.NAĞIZADƏ
Bakı Dövlət Universiteti
eminnaghizade84@gmail.com

Məqalədə terrorçuluğun yeni forması kimi kiberterrorçuluğun ictimai təhlükəliyi, anlayışı, səciyyəvi xüsusiyyətləri, törədilmə üsulları ilə bağlı məsələlər nəzərdən keçirilmişdir. Hüquq doktrinasında kiberterrorçuluğun anlayışı ilə bağlı mövcud fikir və mülahizələrin, mövqelərin təhlili aparılmış, kiberterrorçuluğun anlayışı təklif edilmişdir. Bir çox xarici ölkələrin cinayət qanunvericiliklərində bilavasitə kiberterrorçuluğa görə məsuliyyət nəzərdə tutan normaların olmadığı qeyd olunmuş, eyni zamanda bəzi ölkələrdə (Böyük Britaniya, ABŞ, Pakistan, Macarıstan, İtaliya, Gürcüstan və s.) İnternet ehtiyatlarından, informasiya-telekommunikasiya şəbəkələrindən istifadə etməklə törədilən terrorçuluqla bağlı müəyyən müddəaların təsbit olunduğu göstərilmişdir. Qeyd olunmuşdur ki, «Kibercinayətkarlıq haqqında» 2001-ci il tarixli Budapeşt Konvensiyasında kiberterrorçuluğun kriminallaşdırılması zəruriliyi ilə bağlı müddəaların əks olunmaması bu Konvensiyanın ciddi boşluğu kimi qiymətləndirilməlidir. Bu boşluğun tez bir zamanda aradan qaldırılması məqsədilə xüsusi beynəlxalq konfransın çağırılması, Konvensiyanın iştirakçı ölkələrinə və digərlərinə öz milli qanunvericiliklərində kiberterrorçuluğa görə məsuliyyət müəyyən edən normaların və müddəaların daxil edilməsinin tövsiyə olunması, qeyd olunan bu və digər məsələləri tənzimləyən və Budapeşt Konvensiyasına Əlavə olunan Xüsusi Protokolun qəbul edilməsi, ümumiyyətlə isə yaxın illərdə Kibercinayətkarlığa qarşı mübarizə haqqında vahid Konvensiyanın hazırlanması və qəbuluna istiqamətlənmiş işlərin başlanması zəruriliyi vurğulanmışdır. Məqalədə kiberterrorçuluqla bağlı əməllərin kriminallaşdırılması məqsədilə CM-in 214-cü maddəsinə «İnternet informasiya ehtiyatlarından, informasiya-telekommunikasiya şəbəkələrindən, digər texniki-texnoloji və rəqəmsal vasitələrdən istifadə etməklə törədildikdə (kiberterrorçuluq)» kimi yeni tövsifedici tərkibin əlavə edilməsi məqsədəuyğun hesab edilmişdir.

Açar sözlər: terrorçuluq, kiberterrorçuluq, kiberterrorçuluğun ictimai təhlükəliliyi, kiberterrorçuluğun anlayışı, səciyyəvi xüsusiyyətləri, xarici ölkələrin cinayət qanunvericiliyi, Kibercinayətkarlıq haqqında Konvensiya

https://doi.org/10.30546/209300.305.2025.3.012

Məlum olduğu kimi, qloballaşmış müasir dünyanın xarakterik meyllərindən biri də rəqəmsal texnologiyaların sürətli inkişafı, ictimai həyatın bütün sahələrinə informasiya-telekommunikasiya texnologiyalarının, İnternet və di-

gər şəbəkələrin geniş tətbiqidir. «Rəqəmsal iqtisadiyyat», «bitkoinlər» «süni intellekt» kimi terminləri eşidəndə artıq heç kim təəccüblənmir. Qeyd olunan və elmi-texniki tərəqqi ilə bağlı olan bu və ya digər hadisələr dövlətin və cəmiyyətin inkişafı parametrlərini, sosial-iqtisadi və hüquqi münasibətlərin inkişafı istiqamətlərini də əhəmiyyətli dərəcədə dəyişdirmişdi [20, s.157]. Sosial-iqtisadi, hüquqi-siyasi, habelə şəxsiyyətlərarası münasibətlərin rəqəmsal transformasiyası şəraitlərində informasiya-kommunikasiya texnologiyalarının geniş yayılması və intensiv tətbiqi informasiya məkanında törədilən kriminal əməllərin genişlənməsində ifadə olunan cinayətkarlığın mahiyyətcə təbiətində, kəmiyyət və keyfiyyət parametrlərində, struktur və dinamikasında bir sıra ciddi neqativ dəyişikliklərin baş verməsini şərtləndirən əsas amillərdən birinə çevrilmişdir [21, s.287]. Təsadüfi deyildir ki, hüquq doktrinasında cinayətkarlar tərəfindən hakimiyyət orqanlarına qanunsuz təsir göstərmək, cəmiyyətdə qorxu atmosferini yaratmaq məqsədilə internet məkanından və informasiya-telekommunikasiya texnologiyalarından istifadə edilməsi hallarının yarandığını, yaxın illərdə terrorçuluğun yeni forması kimi kiberterrorçuluğun cəmiyyət və dövlət üçün böyük təhlükə kəsb edən sosial-hüquqi hadisəyə çevriləcəyini xüsusi narahatlıqla vurğulanır [11, s.4-6]. B.Əliyev və C.Əlizadə qeyd edirlər ki, «kiberməkanda fəaliyyət göstərən gizli sosial şəbəkələrin həyata keçirdikləri mütəşəkkil ciniayətkarlıq dövlət və cəmiyyətə qarşı, ilk növbədə isə, ölkə iqtisadiyyatına dağıdıcı təsir gücünə malikdir. Bu gün kiberməkanda «qaranlıq veblər» (dark webs), «gizli iqtisadiyyat» (underground economy), gizli şəbəkə (covert network) kimi yeni problemlər yaranmışdır. Gizli şəbəkələr heç bir dövlət tərəfindən nəzarət olunmayan şəbəkələrdir və insan alveri, kibercinayətkarlığın və terrorçuluğun yayılmasında əsas əlaqələndirici vasitədir» [9, s.342]. F.M.Cavadov və Y.S.Abdullayev beynəlxalq ekspertlərin fikir və mövqelərinə əsaslanaraq qeyd edirlər ki, «cinayətkar məqsədlərlə informasiya sistemlərindən (uçuşların idarə olunması sistemləri, AES-in idarə olunması və nəzarəti sistemləri, xüsusi dövlət idarəetmə və rabitə sistemləri, böyük maliyyə və sənaye müəssisələrinin informasiya sistemləri və s.) istifadə öz nəticələrinə görə kütləvi qırğın silahlarının tətbiqi nəticələri ilə müqayisə oluna bilər» [4, s.32-33]. B.S.Zahidov düzgün olaraq qeyd edir ki, «kompüter texnologiyalarından istifadə etməklə hərbi sirlərin ələ keçirilməsi, təyyarələrin, atom elektrik stansiyalarının, metroların, nəqliyyat-kommunikasiya sistemlərinin terrorçular tərəfindən öz maraqları xatirinə istifadə edə bilmək imkanları bu gün böyük təhlükələrdən xəbər verir» [5, s.18].

Rəqəmsal idarəetmə metodlarına sürətli keçid artıq yaxın zamanlarda aviasiya, kosmik, atom enercisi obyektlərinin, digər həyati əhəmiyyətli infrastrukturun idarə edilməsi sisteminin ələ keçirilməsi ilə bağlı prinsipcə yeni terrorçuluq təzahürləri ilə müşayiət oluna bilər. Belə ki, rəqəmsal şəbəkələrin bütün üstünlükləri terrorçu təşkilatların da diqqətindən yayınmamışdır.

L.A.Bureyeva hərbi obyektlərin, nüvə, energetika, maliyyə, nəqliyyat və s. kimi sahələrin idarə edilməsini həyata keçirən kompüter sistemləri və onların şəbəkələri terrorçuların diqqətini cəlb edən əsas obyektlər sırasında olduğunu qeyd edir [16, s.35-36].

Deyə bilərik ki, şəxsiyyətin, cəmiyyətin və dövlətin təhlükəsizliyi üçün ciddi təhdid olan terrorçuluq qloballaşan dünyanın ən mürəkkəb və çoxaspektli neqativ təzahürlərindən birinə, ictimai təhlükəliliyi olduqca yüksək olan hadisəyə çevrilmişdir. F.Babaşov müasir terrorçuluğun kiberterrorçuluq kimi formasının ictimai təhlükəliliyinin yüksək olduğunu qeyd edərək yazır ki, «….nəzərə alsaq ki, bu gün atom elektrik stansiyalarına nəzarət kompüter vasitəsilə həyata keçirilir, onda təhlükənin nə qədər real olduğunu görərik» [1, s.319]. F.M.Cavadov və Y.S.Abdullayevin qeyd etdikləri kimi, «informasiya-kompüter texnologiyalarının geniş yayılması, ictimai həyatın bütün sahələrinə nüfuz etməsi, texnoloji proseslərin elektron idarə olunması metoduna keçid yeni terrorizm növünün, kiberterrorizmin yaranmasına şərait yaratmışdır» [4, s.85]. V.Ə.Qasımov terrorçuların elmi-texniki tərəqqinin son nailiyyətlərindən istifadə etmələrini, «onların dağıdıcılıq imkanlarının genişləndiyini, insanları daim qorxu altında saxlamağa imkan verdiyini qeyd edir [2, s.62]. Müəllif hesab edir ki, «Ənənəvi terrorçuluqdan fərqli olaraq, kiberterrorçuluq yalnız insanların və onlara məxsus olan əmlakın məhvinə (və ya məhvi təhlükəsinə), mühüm strateji və iqtisadi obyektlərin dağıdılmasına deyil, həmçinin maliyyə və kommunikasiya şəbəkələrinin və sistemlərinin işinin geniş miqyasda pozulmasına, iqtisadi infrastrukturun dağıdılmasına və hakimyyət strukturlarına öz iradələrinin qəbul etdirilməsinə yönəlmiş ola bilər» [2, s.62-63].

Qeyd edək ki, «kiberterrorçuluq» teminini ilk dəfə ABŞ-nın Kaliforniya Təhlükəsizlik və Kəşfiyyat İnstitutunun elmi əməkdaşı B.Kollin tərəfindən 1980-ci illərdə işlədilmişdir. Tədqiqatçı gələcəkdə kiberşəbəkələrin imkanlarından terrorçuların da istifadə edəcəklərinə əmin idi. Onun fikrincə, bu XXI əsrin ilk onilliyində baş verəcəkdir. Lakin zaman onun proqnozlarını xeyli qabaqlamışdır. İnternetdən qanunazidd məqsədlərlə istifadə etməklə bağlı ilk cəhdlər XX əsrin 90-cı illərindən həyata keçirilməyə başlamışdır. Belə ki, hüquq-mühafizə orqanları tərəfindən ilk kiberhücum cəhdi artıq 1990-cı illərdə qeydə alınmışdır (məsələn, 1993-cü ildə terrorçular «troya atı» zərərli virus proqramının köməyi ilə Litvanın ərazisində yerləşən İqnalinsk AES-in idarə olunmasını həyata keçirən kompüter sisteminin normal işini pozmaqla texnogen fəlakət yaratmaq, stansiyada partlayış törətməklə hədələmişlər [3, s.84]. Müasir şəraitdə isə terrorçuluq fəaliyyətini həyata keçirmər üçün informasiya-telekommunikasiya texnologiyalarından, rəqəmsal texniki vasitələrdən daha geniş şəkildə istifadə edilməyə başlanmışdır. Rəqəmsal (virtual) mühitdən, qlobal şəbəkələrdən terror qruplarına yeni üzvlərin cəlb edilməsi; terror ideologiyasının, terror çağırışlarının, təbliğat və təşviqat materiallarının yayılması; ter-

ror aktlarının törədilməsində istifadə olunan vasitələrin (silah, partlayıcı maddələr, kompüter virusları) hazırlanması ilə bağlı informasiyanın yayılması; daha təhlükəsiz şəraitdə ünsiyyyət və təmasların qurulması; terror təşkilatlarının fəaliyyətinin maliyyələşməsi üçün vəsaitlərin toplanması; potensial hədəflər (insanlar, infrastruktur obyektləri) haqqında informasiyanın toplanması üçün istifadə edilir. Müasir terrorçular elmi-texniki tərəqqinin ən yeni nailiyyətlərindən əsasən daha təhlükəsiz şəraitdə qarşılıqlı əlaqə və təmasların qurulması, təbliğat və informasiyanın ötürülməsi vasitəsi kimi istifadə etsələr də, yaxın gələcəkdə kiberterrorçuluğun cəmiyyət və dövlət üçün real təhlükə kəsb edəcəyini proqnozlaşdırmaq o qədər də çətin deyildir [22, s.41].

Son illərdə terrorçuluq fəaliyyətini həyata keçirən kriminal strukturlara təhsilə və savada malik, kompüter texnikası və şəbəkə texnologiyaları sahəsində bilik və təcrübəyə yiyələnmiş gənc mütəxəssislər də qoşulmağa başlamışlar. Bu da terror strukturlarına xeyli dərəcədə cinayətkar fəaliyyət üsullarını təkmilləşdirməyə, yeni, daha yüksək kriminal peşəkarlıq səviyyəsini əldə etməyə, kimi müasir texnologiyalardan istifadə olunmaqla terror fəaliyyətini həyata keçirməyə imkan verir. İnternet informasiya ehtiyatlarından, digər telekommunikasiya şəbəkələrindən istifadə edilməklə terror ideologiyası bəyan edilir, terrorçuluq fəaliyyətinin həyata keçirilməsi üçün maliyyə vəsaitələrinin toplanılması həyata keçirilir, yeni iştirakçılar cəlb olunur, terrorçuluğa çağırışlar təbliğ edilir, terror fəaliyyəti planlaşdırılır və hazırlanır. Rəqəmsal texnologiyalar, qlobal telekommunikasiya şəbəkəlıri vasitəsilə reallaşdırılan terror aktlarını geniş işıqlandırılır ki, bunda da məqsəd böyük sayda insanlar arasında «məşhurlaşmaq», cəmiyyəti qorxutmaq, insanlar arasında vahimə yaratmaq, özləri ilə hesablaşmağa məcbur etmək, kütləvi şüura bilavasitə qorxuducu sosial-psixoloji təsir göstərməkdir [23, s.84].

Eyni zamanda, terrorçuluğun bu yeni formasının, yəni kiberterrorçuluğun ictimai təhlükəliyinə, yaxın gələcəkdə sürətlə yayılma təhlükəsinin mövcudluğuna baxmayaraq bu gün də hüquq elmində «kiberterrorçuluq» anlayışı ilə bağlı vahid nöqteyi-nəzər mövcud deyildir.

Hüquq ədəbiyyatında da bu amilə diqqət yetirilmişdir. Belə ki, C.Brinckey, müasir şəraitlərdə kriminogen xarakterli prinsipcə yeni hadisə olan kiberterrorçuluğun hüquq doktrinasında dəqiq anlayışının, əlamətlərinin, xarakterik cəhətlərinin işlənilmədiyini qeyd etməklə yazır ki, bu amil kiberterrorçuluğun kibermüharibə, kibercəsusluq, kompüter informasiyası sahəsində cinayətlər və sair kimi oxşar anlayışlardan fərqləndirilməsində çətinlik və mürəkkəbliklərin yaranmasına gətirir [10, s.4-6]. Terrorizmə qarşıdurma sahəsində qəbul edilmiş beynəlxalq konvension mexanizmlər sistemində kiberterrorçuluğun leqal anlayışının təsbit edilməməsi vəziyyəti daha da mürəkkəbləşdirir [15, s.127].

Düzdür, informasiya təhlükəsizliyi ilə bağlı məsələlərin beynəlxalq-

hüquqi aspektlərini tənzimləyən bir sıra regional konvensiyalarda bəzi hallarda terrorizmin ayrı-ayrı təzahürlərini kibercinayətlərin bir növü olan kompüter cinayətləri ilə əlaqələndirən müddəalar təsbit olunmuşdur. Məsələn, 2010-cu il tarixli «İnformasiya texnologiyaları sahəsində cinayətlərlə mübarizə haqqında» Ərəb dövlətləri Liqasının Konvensiyasında informasiya texnologiyalarından istifadə etmək yolu ilə törədilmiş terrorizmlə bağlı cinayətlərin hüquqi məzmununun açılmasına cəhd edilmişdir. Belə ki, Ərəb konvensiyasının 15-ci maddəsində informasiya texnologiyalarından istifadə etməklə terror qruplarının ideyalarını və prinsiplərini təbliğ etmə və yayma; terror əməliyyatları üçün təlim keçmə və terrorçuluğu maliyyələşdirmə, terror təşkilatları arasında əlaqənin təmini; partlayıcı maddələri hazırlama üsullarını, onlardan terror əməliyyatlarında istifadə metodlarını yayma kimi əməllər (hərəkətlər) terrorçuluq əməllərinə aid edilmişdir. Oxşar vəziyyət 27 iyun 2014-cü il tarixli «Kibertəhlükəsizlik və fərdi məlumatların müdafiəsi haqqında» Afrika İttifaqı Konvensiyasında müşahidə olunur.

Xüsusi ədəbiyyata nəzər salsaq, görərik ki, hüquqşünaslar tərəfindən kiberterrorçuluğun anlayışı, mahiyyət və məzmunu, əlamətləri, törədilmə üsulları ilə bağlı çoxsaylı fikir və mülahizələr bildirilmişdir. Məsələn, 1997-ci ildə ABŞ-ın FTB-nin xüsusi agenti M.Pollit hüquqi dövriyyəyə yeni «kiberterrorizm» terminini daxil edərək kiberterrorizmə həyati əhəmiyyətli infrastuktur obyektlərin ciddi ziyan vurma, əhali qrupuna və ya məxfi agentlərə münasibətdə zorakılığa gətirən informasiyaya, kompüter sistemlərinə, kompüter proqramlarına və elektron məlumatlara siyasi cəhətdən motivləşdirilmiş qəsdən törədilən hücum kimi anlayış vermişdir [13, s.8-10]. R.İ.Dremlyuqa, A.İ.Korabeyev və A.V.Fedorovun fikrincə, kiberterrorizm dedikdə, terror aktlarının informasiya şəbəkələri vasitəsilə törədilməsi (bu halda İnternet cinayətin törədilməsi üsulu və vasitəsi kimi çıxış edir) və ya kompüter informasiya texnologiyalarından istifadə etməklə terrorçuluğun reallaşdırılmasına kömək edən kriminal fəaliyyət (məsələn, terrorçuluq fəaliyyətinə cəlb etmək, terrorçuluğun təbliği, terrorçular üçün vəsaitlərin toplanması, terror qruplarının üzvləri arasında qarşılıqlı əlaqəli fəaliyyətin təşkili və s.) başa düşülür [17, s.608]. A.A.Panenkov hesab edir ki, kiberterrorizm - siyasi və ya sosial-iqtisadi məsələlərin həlli üçün hakimiyyət orqanlarına təsir göstərmək məqsədilə kompüter sistemlərinə, şəbəkələrinə və ya onlarda saxlanılan informasiyaya qanunazidd müdaxilələrlə bağlı hərəkətlərdir [24, s.12-19].

S.T.Məcidli hesab edir ki, kiberterrorçuluq dedikdə, kompüterdə emal olunan informasiyaya, kompüter sisteminə və şəbəkələrinə, informasiya infrastrukturuna düşünülmüş, siyasi məqsədlərə əsaslanan, siyasi, dini, ideoloji və digər motivlərlə törədilən, dağıdıcı, təxribatçı və qorxu aşılayan nəticələrə səbəb olan hücum başa düşülür. Müəllif qeyd edir ki, «əgər belə hərəkətlər ictimai təhlükəsizliyin pozulması, əhalinin qorxudulması, hərbi konfliktlərin,

təxribatların törədilməsi məqsədilə həyata keçirilmiş olarsa, onda bu hücum insanların həyatı və sağlamlığı və ya digər ağır fəsadların baş verməsi üçün daha böyük təhlükə yaradır» [7, s.61-62]. K.A.Qable əhalini qorxutma, siyasi fəaliyyətə təsir göstərmə, ictimai qaydanı pozma məqsədləri ilə kompüter məlumatlarına və ya kompüter proqramlarının, sistemlərinin, şəbəkələrinin işinə ciddi zərər vurma yolu ilə törədilən qanunazidd əməllər kiberterrorçuluq kimi nəzərdən keçirilə biləcəyini qeyd edir [12(15, s.72]. O.A.Sokolovanın mövqeyinə görə, kiberterrorçuluq, terrorçuluğun yeni yaranan forması olmaqla, kompüter və informasiya texnologiyaları sahəsində elm və texnikanın nailiyyətlərindən istifadə etməklə müxtəlif dövlət strukturlarının, beynəlxalq təşkilatların qərar qəbul etmələrinə təsir göstərməyə istiqamətlənmişdir [26, s.114]. «Kibertəhlükəsizliyin təmininin əsas prinsipləri haqqında» 21 iyun 2018-ci il tarixli Ukrayna Qanunun 1-ci maddəsinə görə, kiberterrorçuluq - kiberməkanda və ya kiberməkandan istifadə etməklə həyata keçirilən terrorçuluq fəaliyyətidir. Böyük Britaniyanın 2006-cı il tarixli «Terrorizm haqqında» Qanunun 2-ci maddəsinə uyğun olaraq kompüterlərə, onların sistemləri və ya şəbəkələrinə qanunsuz daxil olma əhəmiyyətli ziyana səbəb olduqda və ya kompüterlərdən və onlarda olan informasiyadan kütləvi zorakılıq hərəkətlərinin təşkili üçün istifadə edildikdə, bu əməllər terror aktı hesab edilir. E.B.Eyyubova kiberterrorçuluğu «kompüterdə emal olunan informasiyaya, kompüter sisteminə və şəbəkəsinə düşünülmüş, siyasi motivlərə əsaslanmış hücum» olduğunu qeyd edərək yazır ki, «belə hərəkətlər ictimai təhlükəsizliyin pozulması, əhalinin qorxudulması, hərbi konfliktlərin, təxribatların törədilməsi məqsədilə həyata keçirilmiş olarsa, onda bu hücum insanların həyatı və sağlamlığı və ya digər ağır fəsadların baş verməsi üçün daha böyük təhlükə yaradır» [3, s.84].

Beləliklə, kiberterrorçuluq - ictimai təhlükəsizliyi pozmaq, əhali arasında vahimə yaratmaq, dövlət hakimiyyəti orqanları və ya beynəlxalq təşkilatlar tərəfindən qərar qəbul edilməsinə təsir göstərmək məqsədilə kiberməkanda informasiya-telekommunikasiya texnologiyalarından və İnternet ehtiyatlarından, digər texniki-texnoloji və rəqəmsal vasitələrdən istifadə etməklə insanların həlak olması, onların sağlamlığına zərərin yetirilməsi, əhəmiyyətli əmlak ziyanının vurulması və ya başqa ictimai təhlükəli nəticələrin baş verməsi təhlükəsi yaradan partlayış, yanğın, subasma, daşqın kimi hərəkətlərin törədilməsi, nəqliyyat sisteminin, hərbi obyektlərin, səhiyyə müəssisələrinin, digər həyati əhəmiyyətli infrastruktur obyektlərinin normal fəaliyyətini pozmaqla onlara əhəmiyyətli ziyan vurmaqla reallaşdırılan, habelə digər ciddi ictimai-təhlükəli nəticələrə gətirən hərəkətlər (hərəkətlər kompleksi) və ya eyni məqsədlərlə bu cür hərəkətləri törətməklə hədələməkdir.

Kiberterrorçuluq anlayışını belə ifadə edərkən bu kriminal əməllər kompleksinin törədilməsi üsullarını iki bir-birindən asılı olmayan müstəqil

qruplara ayırmaq olar. Birinci qrupa kompüter infrastukturu obyektlərinə və informasiya şəbəkələrinə edilən cinayətkar qəsdləri aid etmək olar. Məsələn, informasiya sistemlərinin sıradan çıxarılması ki, bu hücuma məruz qalan obyektin nəzarətsiz işləməsinə (bu da atom və kimyəvi istehsalat sahələrində, həmçinin hərbi müdafiə sistemləri sahəsində, xüsusilə təhlükəlidir) və ya dağıdıcı hücumların təşkilinə (məsələn, informasiya ehtiyatlarının və ya kommunikasiya xətlərinin məhv edilməsi və ya informasiya sistemlərinin qoşulduğu strukturun fiziki məhvi) gətirib çıxaracaqdır [22, s.43]. Kiberterrorçuluğun törədilməsi üsullarının ikinci qrupuna, insanlara qorxuducu və vahimə yaradıcı təsir göstərmək məqsədilə törədilmiş terrorçuluqla bağlı (məsələn, Yaxın Şərqdə və digər yerlərdə jurnalistlərin edam edilməsi ilə bağlı videogörüntülərin İnternetdə yayılması) informasiyanın qlobal şəbəkədə yerləşdirilməsi üçün kompüter texnologiyalarından istifadə edilməsi ilə bağlı hərəkətləri və digərlərini aid etmək olar [18, s.33-34]. L.A.Bureyeva hesab edir ki, spektri ildən ilə genişlənən kibercinayətlərin bütün növləri arasında kiberterrorçuluğun iki əsas növünü fərqləndirmək olar: 1) kompüterlərdən və kompüter şəbəkələrindən istifadə etməklə törədilən terrorçuluq (hücum edilən şəbəkəyə qanunsuz olaraq daxil olmağa və ya şəbəkənin idarə edilməsini ələ keçirməyə imkan verən müxtəlif növ hücumlar; kompüter sistemlərinin işini bloklayan və ya onlarda olan informasiyanı dəyişdirən və məhv edən kompüter viruslarını yayma; müəyyən şərait və şərtlərdə işə düşən məntiqi bombanın kompüter proqramında yerləşdirilməsi və s.); 2) terrorçu qruplar tərəfindən təşkilati-kommunikasiya məqsədləri üçün qlobal informasiya məkanından istifadə etmə (terror aktlarının planlaşdırılması üçün informasiyanın toplanması; terror təşkilatlarına və terror ideologiyasına dəstək məqsədilə pul vəsaitlərinin yığılması; terrorçuluğun təbliği; şantaj, vahimə, təlaş yaratmaq məqsədilə kütləvi şüura informasiya-psixoloji təsirin göstərilməsi; təşkilati fəaliyyətin həyata keçirilməsi; terrorçuluqla bağlı hərəkətlərin planlaşdırılması və əlaqələndirilməsi üçün kommunikasiya texnologiyalarını tətbiq etməklə daha kiçik terrorçu qruplara öz potensiallarını genişləndirməkdə kömək göstərilməsi və s. [16, s.35-36].

Q.Veyman, terrorçuluğun yeni forması kimi kiberterrorçuluğun aşağıdakı xarakteristik xüsusiyyətlərini qeyd edir: kiberterror metodları ənənəvi terror vasitələrindən daha ucuz başa gəlir; kiberterrorçuluq yüksək anonimliklə səciyyələnir, dövlətlərin xüsusi xidmət orqanları üçün şəbəkədə terrorçunun şəxsiyyətini eyniləşdirmək olduqca çətin və mürəkkəbdir; qlobal şəbəkə effektiv kiberhücum hədəflərinin seçilməsi üçün daha geniş imkanlar təqdim edir; kiberror aktları məsafədən həyata keçirilə bilər ki, bununla da terrorçuların fiziki və psixoloji hazırlığı üçün xərclər, həmçinin onlar arasında itkilər də azalır; kiberterrorçuluq Şəbəkə istifadəçilərinin olduqca böyük sayına hücumları həyata keçirmək hesabına daha geniş birbaşa təsir imkanlarına

malikdir, həmçinin bu əməllər mediada da geniş işıqlandırılır ki, bu da terrorçular üçün əhəmiyyətli amildir [22]. D.V.Puçkov da kiberterrorçuluğun daşıdığı ciddi təhlükənin bu növ kriminal əməllərin həyata keçirilməsi zamanı milli sərhədlərin heç bir rol oynamamasını, bu əməllərin dünyanın istənilən nöqtəsindən törədilməsinin mümkünlüyünü qeyd edir. Müəllif, kiberterrorçuların potensial məqsədləri qismində dövlət strukturları, telekommunikasiya şəbəkələri, hava, dəniz və dəmir yolu nəqliyyatının idarə olunması sistemləri, energetika və maliyyə sistemləri çıxış edə bildiyini göstərir, bütün bunların məcmu halda adekvat hüquqi qiymətləndirilməsi və bu əməllərə görə cinayət məsuliyyətinin müəyyən olunması zəruriliyini şərtləndirdiyini göstərir [25, s.382-390].

Təhlil və araşdırma, xüsusi ədəbiyyatın, xarici ölkələrin kibercinayətkarlıqla mübarizə təcrübəsinin öyrənilməsi göstərir ki, bu gün informasiya-telekommunikasiya texnologiyalarından, İnternet ehtiyatlarından, rəqəmsal texniki vasitələrdən istifadə etməklə törədilən və daha geniş yayılan kiberterrorçuluq əməllərinə aid edilə bilərlər: kompüter-texniki vasitələrin sıradan çıxarılması məqsədilə ziyanverici proqramlardan istifadə (məsələn, nüvə reaktorlarının işində pozğunluqların yaradılması üçün ziyanverici proqramların tətbiqi); yüksək ictimai əhəmiyyət kəsb edən infrastrukturun (məsələn, maliyyə, nəqliyyat, sosial təminat, səhiyyə və s.) idarə edilməsini təmin edən kompüter sistemlərini və onların şəbəkələrini sıradan çıxarma; dövlətin siyasi-diplomatik xarakterli fəaliyyəti ilə, hərbi obyektlərlə bağlı məxfi xarakterli məlumatların, dövlət sirri olan digər qapalı informasiyanın "kilidini" açma və yayma; əhali arasında qorxu və vahimə yaradan məlumatları və videogörüntüləri yayma, tələblərini elan etmək məqsədilə internet-saytları ələ keçirmə; avtomatlaşdırılmış rabitə-telekommunikasiya xətlərini sıradan çıxarma; elektrik, su, qaz təchizatı şəbəkələrinin idarəetmə sistemlərinin işində ciddi pozğunluqlar yaratma; süni surətdə yüksək yüklənmə yaratmaqla İnternet şəbəkəsinin ayrı-ayrı seqmentlərinin və ya saytlarının, habelə digər informasiya-telekommunikasiya şəbəkələrin, texnoloji rəqəmsal sistemlərin işini iflic etmə [17, s.608].

Eyni zamanda, problemin müstəsna əhəmiyyət kəsb etməsinə baxmayaraq, kiberterrorçuluğun qarşısının alınmasının cinayət-hüquqi vasitələrinin işlənib hazırlanmasına hələ də lazımi səviyyədə diqqət yetirilmir.

Xarici ölkələrin cinayət qanunvericiliyinin təhlili göstərir ki, bir çox ölkələrdə kompüter texnologiyalarından və İnternet şəbəkəsindən istifadə etməklə terror aktının törədilməsinə görə cinayət məsuliyyətini müəyyən edən norma və müddəalar qüvvədə olan cinayət qanunvericiliyində öz əksini tapmamışdır. Məsələn, Gürcüstan istisna olmaqla pstsovet ölrələrinin CM-də kiberterrorçuluğa görə məsuliyyət nəzərdə tutan xüsusi maddə yoxdur. Müqayisəli-hüquqi təhlil bir çox xarici ölkə qanunvericilərinin CM-də kiberterror-

çuluğa görə cinayət məsuliyyəti nəzərdə tutan xüsusi tərkibləri daxil etməyə tələsmədiklərini göstərir.

Eyni zamanda terrorçuluğun bu olduqca təhlükəli formasının bir sıra ölkələrin milli qanunvericiliyində öz hüquqi qiymətini almağa və bu əməllərin müxtəlif təzahürlərinə görə cinayət məsuliyyəti nəzərdə tutulmağa başladığı da qeyd edilməlidir. Bununla belə, bu prosesin olduqca ləng getdiyi, müasir reallıqları tam şəkildə əks etdirmədiyi də vurğulanmalıdır. Bəzi ölkələrdə yalnız terrorçuluq məqsədləri ilə telekommunikasiya sistemlərindən istifadə ilə bağlı müəyyən qeydlər öz əksini tapmışdır. Məsələn, Fransa CM-in 421-1-ci maddəsində terrorçuluq aktına görə məsuliyyət nəzərdə tutularkən sadəcə olaraq qeyd olunur ki, bu əməllər məqsəd və istiqamətliyi terrorçuluq olan informatika sahəsində cinayətkar əməlləri də əhatə edir. XXİ əsrin əvvəllərində Fransa qanunvericisi İnternet şəbəkəsinin geniş yayılmağa başladığını nəzərə alaraq CM-ə 421-1.2-ci maddə daxil etmişdir ki, bu maddə də terrorçuluq idealogiyasının İnternet vasitəsilə yaymaq, terrorçuluq məqsədilə insanlara edilən hücumları əks etdirən müəyyən təsvirləri, məlumatları saytlarda yerləşdirmək kimi əməllərə görə cinyət məsuliyyəti nəzərdə tutulmuşdur. Makedoniya CM-nin 394a-3-cü maddəsində terror təşkilatını yaratmaq üçün açıq çağırışlar, bu növ təşkilatları yaratmağa təhrik etmə və sair kimi əməllərə, o cümlədən İnternet vasitəsilə belə çağırışların ifadə edilməsinə görə cinayət məsuliyyəti müəyyən edilmişdir [19, s.103]. İtaliya CM-də terrorçuluqla bağlı xüsusi tərkiblərlə yanaşı, terrorçuluq məqsədilə istənilən digər cinayətin törədilməsini terrorçuluq əməli kimi qiymətləndirən ümumi 280-ci maddə vardır. 2005-ci ildə İtaliya CM-nə terrorçuluq fəaliyyəti ilə bağlı təlim keçmə əməllərinə görə cinayət məsuliyyəti nəzərdə tutan maddə daxil edilmiş, 2015-ci ildə isə bu maddəyə mühüm əlavələr edilmişdir və bu dəyişikliyə görə, terror məqsədilə təlim keçmə zamanı informasiya texnologiyalarından istifadə etmə 280-ci maddəyə tövsifedici tərkib kimi daxil edilmişdir. Pakistanın Elektron cinayətlərin qarşısının alınması haqqında 2016-cı il tarixli Qanunun 10-cu maddəsində kibirterrorizmə görə cinayət məsuliyyəti nəzərdə tutulmuşdur. Həmçinin Estoniya (maddə 237), Avstriya (maddə 278 s), Belçika (maddə 137.2), Niderland (maddə 354 a), Böyük Britaniya (Terroroizm haqqında 2000-ci tarixli Qanunun 1.2-ci maddəsi) kimi ölkələrdə əhalini qorxutmaq, siyasi fəaliyyətə təsir göstərmək, ictimai qaydanı pozmaq məqsədləri ilə kompüter məlumatlarına və ya kompüter proqramlarına, sistemlərinə, şəbəkələrinə ciddi zərər vurma, habelə terrorçuluğun törədilməsi üçün istifadə olunan və ya belə aktları təşviq edən materialları qlobal informasiya şəbəkələrində yerləşdirmə və yayma əməlləri kriminallaşdırılmışdır [20, s.158-159]. 2006-cı ildə Gürcüstan qanunvericisi kiberterrorizm əməllərini kriminallaşdırmışdır (maddə 324.1). Bu maddənin dispozisiyasında kiberterrorizm olaraq əhalini qorxutmaq və ya (və) hakimiyyət orqanlarına təsir

göstərmək məqsədilə törədilən, ağır nəticələrin baş verməsi təhlükəsi yaradan qanunla qorunan kompüter informasiyasının qanunsuz olaraq ələ keçirilməsi, ondan istifadə edilməsi və ya istifadə edilməsi ilə hədələmə başa düşülür.

Cinayət qanunvericiliyinin təkmilləşdirilməsi istiqamətlərindən birini D.V.Lobaç və digərləri təklif edirlər. Müəlliflərin fikrincə, insanların ölümü, əhəmiyyətli əmlak ziyanının vurulması və ya digər ictimai təhlükəli nəticələrin (məsələn, elektrik təchizatı sistemində nasazlıqların yaranması, hərbi-sənaye kompleksinə daxil olan müəssisələrin, nəqliyyatın normal işinin pozulması və s.) başvermə təhlükəsi yaradan informasiya-telekommunikasiya texnologiyalarından qanunsuz istifadə etməklə dövlətin həyati əhəmiyyətli infrastrukturunda kompüter informasiyasına, kompüter sistemlərinə və şəbəkələrinə qanunsuz müdaxilə terrorçuluğun törədilməsinin ictimai təhlükəliliyi yüksək olan üsullardan biri kimi nəzərdən keçirilməli və bu əməllər cinayət məcəlləsinin uyğun maddəsində tövsifedici əlamət keyfiyyətində müəyyən edilməlidir [21, s.292].

S.Rzayeva və V.Sadiqlinin qeyd etdikləri kimi, «hazırda Cinayət Məcəlləsində kiber xarakterli cinayətlər kiberləşmə əlaməti üzrə əməlin ictimai təhlükəliliyinin dərəcəsi ilə müəyyən edilən əsas tərkiblərdə və cinayət məsuliyyətini ağırlaşdıran və xüsusilə ağırlaşdıran halı ehtiva edən tərkiblər kimi təsbit olunur. Bu spesifik əlamət, bir qayda olaraq, cinayətin törədilmə üsulu ilə müşayiət olunur ki, bu da «adi» növdən olan eyni cinayət əməlini onun kiber xarakterli növündən fərqləndirmədə əsas kimi çıxış edir» [8, s.55]. Məsələn, Azərbaycan Respublikasının CM-in bir sıra normalarına kompüter-informasiya texnologiyalarından istifadə etməklə ictimai təhlükəli əməllərin kiber məkanda törədilməsinə görə məsuliyyət nəzərdə tutan cinayət tərkibləri daxil edilmişdir (məsələn, CM-in 177.2.3-1-ci maddəsi – elektron məlumatlar daşıyıcılarından, yaxud informasiya texnologiyalarından istifadə etməklə törədilən oğurluq; CM-in 234.4.4-cü maddə – internet informasiya ehtiyatlarından və ya informasiya-telekommunikasiya şəbəkələrindən istifadə etməklə qanunsuz olaraq narkotik vasitələri, psixotrop maddələri və ya onların prekursorlarını hazırlama, istehsal etmə, əldə etmə, saxlama, daşıma, göndərmə və ya satma). B.S.Zahidov da düzgün olaraq yazır ki, «…bu və ya digər cinayət əməllərinin informasiya texnologiyalarından istifadə edilməklə törədilməsi halları ağırlaşdırıcı hallar kimi ayrı-ayrı tərkiblərdə nəzərə alınmalıdır» [5, s.19].

Qeyd olunanlar nəzərə alınmaqla, eyni yanaşma kiberterrorçuluqla bağlı əməllərin kriminallaşdırılması zamanı da həyata keçirilməli, CM-in 214-cü maddəsinə «İnternet informasiya ehtiyatlarından, informasiya-telekommunikasiya şəbəkələrindən, informasiyanın emalı, ötürülməsi, dəyişdirilməsi üçün nəzərdə tutulmuş digər texniki-texnoloji və rəqəmsal vasitələrdən istifadə etməklə törədildikdə (kiberterrorçuluq)» kimi yeni tövsifedici tərkibin əlavə edilməsi məqsədəuyğun hesab edilməlidir.

Daha bir məsələyə toxunmaq istərdik. Məlum olduğu kimi, 2001-ci ilin noyabrında Avropanın və Amerikanın 30 dövləti tərəfindən qəbul edilmiş kibercinayətkarlıqla mübarizə haqqında Avropa Konvensiyanın (Budapeşt Konvensiyası) 2-ci fəslində kibercinayətlərin təsnifatı aparılmış, kibercinayətlər kateqoriyasına aid edilən bir sıra əməllərə görə iştirakçı-dövlətlərin milli qanunvericiliklərində cinayət məsuliyyətinin nəzərdə tutulması zəruri hesab edilmişdir.

Təəssüf ki, Budapeşt Konvensiyasında kiberterrorçuluqla bağlı müddəalar öz əksini tapmamışdır.

Halbuki, «Kibercinayətkarlıq haqqında» Konvensiyanın (Azərbaycan Respublikasının Milli Məclisi 30 sentyabr 2009-cu ildə ratifikasiya etmişdir) Preambula hissəsində digər tədbirlərlə yanaşı, rəqəmsal texnologiyaların həyatımıza daxil olması, kompüter şəbəkələrinin birləşməsini və qloballaşmasının səbəb olduğu əhəmiyyətli dəyişikliklərin dərk edilməsinin; kibercinayətkarlığa qarşı səmərəli mübarizə aparmaq üçün cinayət hüququ sahəsində geniş beynəlxalq əməkdaşlığın tələb olunduğunun nəzərə alınmasının vacibliyi qeyd olunmuşdur. A.N.İbrahimovanın düzgün olaraq qeyd etdiyi kimi, «texnoloji inkişaf, süni intellekt sistemlərindən istifadə, əşyaların interneti kimi tandemlər kibercinayətlərin təsnifatının tez-tez yenilənməsini tələb edir. Ənənəvi bölgüdə yeni subkateqoriyalar artırmaqla yeni kiber pozuntuların da kriminallaşdırılması və onlara qarşı mübarizə aparılması vacibdir» [6, s.5]. Müəllif, kiberterrorçuluğun, kompüter-informasiya texnologiyalarından, İnternet ehtiyatlarından istifadə etməklə törədilən və son illərdə ictimai təhlükəliliyi əhəmiyyətli dərəcədə yüksələn bir sıra texnoloji cinayətlərin Konvensiyanın normalarından kənarda qaldığını qeyd etməklə yazır ki, «Tvitter, Youtube və digər şəbəkələrdə müxtəlif terrorçuluğa açıq çağırışların (məsələn, İŞİD) yayılması kompüter vasitəsilə törədilən cinayətlərin siyahısının artırılmasını tələb edir» [6, s.7].

Qeyd olunan Konvensiyada kiberterrorçuluğun kriminallaşdırılması zəruriliyi ilə bağlı müddəaların əks olunmaması bu Konvensiyanın ciddi boşluğu kimi qiymətləndirilməlidir. Konvensiyanın yaradıcıları onun qəbul olunması ərəfəsində kiberterrorçuluğun yaxın gələcəkdə yüksək ictimai təhlükə kəsb edə biləcəyini proqnozlaşdıra bilməmişlər. Hesab edirik ki, bu nöqsan tez bir zamanda aradan qaldırılmalıdır. Bu məqsədlə xüsusi beynəlxalq konfrans çağırılmalı, Konvensiyanın iştirakçı ölkələrinə və digərlərinə öz milli qanunvericiliyində kiberterrorçuluğa görə məsuliyyət müəyyən edən normaların və müddəaların daxil etmələri tövsiyə olunmalı, qeyd olunan bu və digər məsələləri tənzimləyən və Budapeşt Konvensiyasına Əlavə olunan Xüsusi Protokol qəbul edilməlidir. Ümumiyyətlə isə yaxın illərdə Kibercinayətkarlığa qarşı mübarizə haqqında vahid Konvensiyanın hazırlanması və qəbuluna istiqamətlənmiş işlərə başlanılmalıdır.

ƏDƏBİYYAT

1. Babaşov F. Regional səviyyədə terrorçuluq cinayətinin kriminoloji xarakteri və onun profilaktikası // «Regional cinayətkarlığın kriminoloji tədqiqinin aktual problemləri» 3-cü beynəlxalq elmi-praktik konfransın materialları. - Bakı, - 2015.
2. Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq. - Bakı, - 2007.
3. Eyyubova E.B. Kiberterrorizmin mahiyyəti haqqında // Bakı universitetinin xəbərləri. sosial-siyasi elmlər seriyası. - 2015. - №1.
4. Cavadov F., Abdullayev Y. Qloballaşma şəraitində kibercinayətkarlığın ictimai təhlükəliliyi və onunla mübarizənin aktual problemləri // Məhkəmə ekspertizası, kriminalistika və kriminologiyanın aktual məsələləri. Elmi əsərlər məcmuəsi. - №58, - 2013.
5. Zahidov B. İnformasiya təhlükəsizliyinin cinayət-hüquqi vasitələrlə mühafizəsi problemləri // İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə 2-ci respublika elmi-prktiki konfransı, 14 may, 2015-ci il. - Bakı, - 2015.
6. İbrahimova A.N. Kibertəhlükələr və onların təsnifatı // Bakı Universitetinin xəbərləri. Sosisal-siyasi elmlər seriyası. - 2020. - №1.
7. Məcidli S.T. Kibercinayətlər. - Bakı, - 2019.
8. Rzayeva S., Sadiqli V. Cinayətin kiber üsulla törədilməsi – cəzanı ağırlaşdıran hal kimi // Polis Akademiyasının elmi xəbərləri. - 2022. - №4(36).
9. Əliyev B., Əlizadə J. Qloballaşma dövründə kiberterrorçuluq təzahürlərinin dövlət təhlükəsizliyi üçün yaratdığı təhdidlər // Məhkəmə ekspertizası, kriminalistika və kriminologiyanın aktual məsələləri. Elmi əsmərlər məcmuəsi. - Bakı, - 2018. - №66.
10. Brickey J. Defining Cyberterrorism Capturing a Broad Range of Activites in Cyberspace // Westpoint CTC Sentinel. - 2012.- Vol.5. -Iss.8. - p.4-6.
11. Colarik A.M. Cyber Terrorism: Political and Economic Implications. - Hershey, - 2006. - p.2-7.
12. Gable K.A. Syber-apocalypse now: securing the Internet against cyberterrorism using universal jurisdiction as a deterrent//Vanderbit J.of Transnat. Law. - 2010. - Vol.43, - №1. - p.57-118.
13. 18.Pollit M.M. Cybertorrorism – Fact of Fancy? // Computer Fraud & Security. - 1998.- iss.2. -p.8-10.
14. Weimann G. Cyberterrorism. How Real Is the Threat//United States Institute of Peace. Special Report. 12p.//http://www.usip.org/sites.
15. Амирова Д.К., Габдрахманова Р.И. Кибетерроризм как современная угроза безопасности граждан//Ученые записки Казанского юридического института МВД России. - 2021. – Т. 6. - №2(12).
16. Буреева Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма//Пробелы в российском законодательстве. 2017. №3.
17. Дремлюга Р.И., Коробеев А.И., Федоров А.В. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты//Всероссийский криминологический журнал. - 2017. - Т.11. - №3.
18. Капитонова Е.А. Особенности кибертерроризма как новой разновидности террористического акта//Известия высших учебных заведений. Поволжский регион. - 2015. - №2(34).
19. Кошенчкина Е.А., Новиков С.В. К вопросу о проблемах законодательства в сфере кибертерроризма//Омский научный вестник. Серия «Общество. История. Современность». - 2017, - №4.
20. Кулешова Г.П., Капитонова Е.А., Романовский Г.Б. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политичес-

кого измерения//Всероссийский криминологический журнал. - 2020. - Т.14. - №1.
21. Лобач Д.В., Смирнова Е.А., Мирошниченко О.И. Национальный уголовно-правовой опыт противодействия кибертерроризму в современных условиях//Образование и право. - 2020. - №7.
22. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. - 2010. - №1(21).
23. Медов М.У. Кибертерроризм: новая угроза // Научный портал МВД России. - 2014. - №3.
24. Паненков А.А. Кибертерроризм как реальная угроза национальной безопасности России//Право и кибербезопасность. - 2018. - №1.
25. Пучков Д.В. Кибертерроризм как новая угроза // Виктимология. - 2021. - Т.8, - №4.
26. Соколова О.А. Кибертерроризм: понятие и меры борьбы // Вестник молодых ученых и специалистов Самарского государственного университета. - 2017. - №1(10).

КИБЕРТЕРРОРИЗМ-КАК НОВАЯ ФОРМА ТЕРРОРИЗМА: ПОНЯТИЕ, ОБЩЕСТВЕННАЯ ОПАСНОСТЬ, ВОПРОСЫ БОРЬБЫ УГОЛОВНО-ПРАВОВЫМИ СРЕДСТВАМИ

Э.НАГИЗАДЕ

РЕЗЮМЕ

В статье рассмотрены вопросы, связанные с общественной опасностью кибертерроризма как новой формы терроризма, его понятием, характерными особенностями, способами совершения. Проведен анализ существующих мнений и суждений, позиций относительно понятия кибертерроризма в правовой доктрине, предложено понятие кибертерроризма. Было указано, что в уголовном законодательстве многих зарубежных стран отсутствуют нормы, предусматривающие ответственность за непосредственный кибертерроризм, но в то же время в некоторых странах (Великобритания, США, Пакистан, Венгрия, Италия, Грузия и др.) установлены определённые положения относительно терроризма, совершенного с использованием интернет-ресурсов и информационно-телекоммуникационных сетей. Отмечено, что отсутствие в Будапештской Конвенции 2001 года "О киберпреступности" положений, касающихся необходимости криминализации кибертерроризма, следует рассматривать как серьезный пробел в настоящей Конвенции. В целях скорейшего устранения этого пробела подчеркнута необходимость созвать специальную международную конференцию, рекомендовать странам-участницам Конвенции и другим включить в национальное законодательство нормы и положения, устанавливающие ответственность за кибертерроризм, принять Специальный Протокол регулирующий указанные и другие вопросы и дополненный к Будапештской конвенции, а в целом начать работу, направленную на подготовку и принятие в ближайшие годы единой Конвенции о борьбе с киберпреступностью. В статье было сочтено целесообразным добавить к статье 214 УК Новый описательный состав, такой как «кибертерроризм, совершенный с использованием информационных ресурсов интернета, информационно-телекоммуникационных сетей, иных технико-технологических и цифровых средств» в целях криминализации деяний, связанных с кибертерроризмом.

Ключевые слова: терроризм, кибертерроризм, общественная опасность кибертерроризма, понятие кибертерроризма, его особенности, уголовное законодательство зарубежных стран, Конвенция о киберпреступности

CYBERTERRORISM AS A NEW FORM OF TERRORISM: CONCEPT, PUBLIC DANGER, ISSUES OF COMBATING CRIMINAL LAW MEANS

E.NAGIZADE

SUMMARY

The article examines the social danger, definition, distinctive characteristics, and methods of commission of cyberterrorism as a new form of terrorism. It analyzes existing opinions and legal doctrinal positions regarding the concept of cyberterrorism and proposes a definition for it. The criminal legislation of many foreign countries lacks provisions directly establishing liability for cyberterrorism. At the same time, it is demonstrated that certain countries (such as the United Kingdom, the United States, Pakistan, Hungary, Italy, Georgia, etc.) have specific provisions addressing terrorism committed through the use of Internet resources and information-telecommunication networks. The absence of provisions criminalizing cyberterrorism in the 2001 Budapest Convention on Cybercrime is emphasized as a significant gap. To urgently address this gap, the article stresses the necessity of convening a special international conference and recommends that the Convention's participant countries and others incorporate norms and provisions establishing liability for cyberterrorism into their national legislation. The adoption of a Special Protocol supplementing the Budapest Convention, regulating these and other related issues, is also urged. Moreover, initiating work aimed at preparing and adopting a unified Convention on combating cyberterrorism in the near future is highlighted as essential. The article concludes that, for the purpose of criminalizing acts related to cyberterrorism, it is appropriate to add a new descriptive element to Article 214 of the Criminal Code, specifying "when committed using Internet information resources, information-telecommunication networks, and other technical, technological, and digital means (cyberterrorism)."

Keywords: terrorism, cyberterrorism, the social danger of cyberterrorism, the concept of cyberterrorism, its specific features, criminal legislation of foreign countries, Convention on Cybercrime