UOT 341:004.9

***Məmmədov B.N.*[1]*, Əsgərova A.N.*[2]**
[1,2]Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyi, Bakı, Azərbaycan
[1]law@mincom.gov.az, [2]law-aysel@mincom.gov.az

QLOBAL KİBERTƏHLÜKƏSİZLİK KONVENSİYASININ ZƏRURİLİYİ VƏ YA BUDAPEŞT KONVENSİYASININ QLOBAL STANDARTA ÇEVRİLMƏSİ İMKANLARI

Dövlətlərin coğrafi sərhədlərini aşmış kibercinayətkarlıqla mübarizənin effektiv olması və kiberməkanda təhlükəsizliyin təmin edilməsi üçün qlobal çoxtərəfli saziş və ya konvensiyanın olması zəruridir. Avropa Şurası çərçivəsində qəbul edilmiş və artıq 10-cu ildir ki, qüvvədə olan Budapeşt Konvensiyası regional xarakter daşıması, kiberməkanda yeni təhdidləri əhatə etməməsi və digər səbəblərdən qənaətbəxş hesab edilmir. Bir sıra dövlətlər BMT çərçivəsində yeni qlobal kibertəhlükəsizlik konvensiyasının işlənib hazırlanması təşəbbüsü ilə çıxış edir.Bu araşdırmalarda Budapeşt Konvensiyasının üstünlükləri və çatışmazlıqları təhlil edilir, qlobal kibertəhlükəsizlik konvensiyası üzərində razılığa gəlinməsi ilə bağlı dünyanın aparıcı dövlətləri arasında yaranmış fikir ayrılıqlarına nəzər salaraq, hadisələrin gələcək inkişafı üzrə proqnoz və mümkün həll yolları təklif edilir.

Açar sözlər: *kibertəhlükəsizlik, kibercinayətkarlıq, kiberməkan, Budapeşt Konvensiyası, qlobal kibertəhlükəsizlik konvensiyası.*

Giriş

İnformasiya cəmiyyətinin çoxsaylı risklər qarşısında müdafiəsizliyi cinayət hüququ sistemini yeni çətinliklərlə üz-üzə qoymuşdur. Sərhədsiz kiberməkan fərdlərə və qruplara dövlətlərin yurisdiksiyalarındakı boşluqlardan cinayətkar məqsədlər üçün istifadə etməyə şərait yaradır. Transmilli fenomen olan kibercinayətkarlıq əksər hallarda cinayətkar və zərərçəkənin müxtəlif yurisdiksiyalarda yerləşməsi səbəbindən hüquq-mühafizə orqanları tərəfindən bu cür cinayətlərin istintaqı və mühakimə olunmasına maneə törədir [1]. Dövlətlər daxili qanunvericiliyin lazımi səviyyədə olmaması və ya zəruri texniki resursların çatışmazlığı ilə əlaqədar kibercinayətlərin hədəfinə çevrilirlər. Bu sahədə ölkələr arasında beynəlxalq əməkdaşlığın qənaətbəxş olmaması isə həmin çətinliklərin aradan qaldırılmasına əngəl törədir. Bu səbəbdən kibercinayətkarlıqla mübarizədə beynəlxalq əməkdaşlıq, əlaqələndirmə və minimum harmonizasiya zəruridir.

Beynəlxalq əməkdaşlıq dövlətlərin qanunvericiliklərində kiberməkandakı risklərin və təhdidlərin cinayət əməli kimi təsbit olunmasını və bu qanunvericiliklərin uyğunlaşdırılmasını tələb edir. Əməkdaşlıq ekstradisiya və qarşılıqlı hüquqi yardımı özündə ehtiva etməlidir. Belə ki, ən azı, ağır kibercinayətlər ekstradisiyaya səbəb olan cinayət əməlləri olmalı, qarşılıqlı hüquqi yardım isə kiberməkanda təhqiqat tədbirlərinə geniş yer verməlidir. Kibercinayətkarlığın təhqiqatı çox vaxt iki və daha çox dövləti əhatə etdiyindən iş bölgüsünü özündə ehtiva edən əlaqələndirmə mexanizmi də çox vacibdir. Lakin maddi və prosessual hüquq normalarının minimum harmonizasiyası olmadan əməkdaşlıq və əlaqələndirmə cəhdləri uğursuzluğa məhkumdur. Minimum harmonizasiya milli qanunvericiliyin cavab verməli olduğu tələblərin minimum həddini müəyyən edir. Bu prinsip əsasında hazırlanmış qanun layihələri üzərində razılığa gəlmək maksimum harmonizasiya əsasında hazırlanmış qanun layihələrinin razılaşdırılmasından daha asandır. Belə ki, sonuncu milli qanunun qanunvericiliyin tələblərini aşmasına icazə vermir. Dövlətlər əksər hallarda bu məsələni öz aralarındakı qarşılıqlı hüquqi yardım haqqında razılaşmaları ikili cinayət prinsipi (əməlin hər iki yurisdiksiyada cinayət hesab olunaraq cəzalandırılması) əsasında qurmaqla həll etməyə çalışsalar da, onların coğrafi sərhədlərini aşmış kibercinayətkarlıqla mübarizənin optimal yolu bu sahədə qlobal çoxtərəfli saziş və ya konvensiyanın olmasıdır.

BMT çərçivəsində yeni qlobal kibertəhlükəsizlik konvensiyasının hazırlanması təşəbbüsü

Beynəlxalq Telekommunikasiya İttifaqı (BTİ) 2011-ci ilin oktyabr ayında 2 illik müddətə BMT Təhlükəsizlik Şurasının qeyri-daimi üzvü seçilmiş, Şərqi Avropa və postsovet ölkələri arasında İKT sektorunun inkişafına görə aparıcı mövqe tutan ölkə kimi Azərbaycanın qlobal xarakter daşıyan kibertəhlükəsizlik üzrə konvensiyanın hazırlanmasında təşəbbüskar mövqe tutmasını təklif etmişdir. BTİ Azərbaycanın bu prosesdə aparıcı rol oynamasını beynəlxalq aləmdə kibertəhlükəsziliyin təmin olunması üzrə qanunvericilik bazasının formalaşmasında stimul olacağına, İKT-nin qlobal miqyasda inkişafına müsbət təsir göstərəcəyinə, yalnız ölkəmizdə deyil, bütün dünyada innovativ texnologiyaların tətbiqi üçün əlverişli şərait yaradacağına inamını ifadə etmişdir. 19-cu Beynəlxalq Telekommunikasiya və informasiya texnologiyaları sərgi və konfransı "Bakutel-2013" çərçivəsində BTİ-nin dəstəyi ilə 2-3 dekabr tarixlərində Bakıda keçirilmiş Kibertəhlükəsizlik üzrə Konfransın məruzəçiləri qlobal xarakter daşıyan kibertəhlükələrə qarşı əks-tədbirlərin də qlobal miqyaslı olması zərurətini, Budapeşt Konvensiyasının yalnız regional səviyyədə tənzimləmədə effektiv olduğunu, həqiqətən, beynəlxalq xarakter daşıyan konvensiyanın işlənib hazırlanmasının vacibliyini konfrans iştirakçılarının diqqətinə çatdırdılar [2]. BTİ-nin Baş katibi Hamadun Ture kibertəhlükəsizliyin təmin edilməsi sahəsində bir sıra mühüm tədbirlərin artıq həyata keçirildiyini və bu prosesin davam etdiyini, lakin kiberməkanda etimad və etibarın təsbit edilməsinin "bir neçə ölkənin təcrid olunmuş şəkildə" əldə etməsinin qeyri-mümkün olmasını xüsusi qeyd edərək, Budapeşt Konvensiyasının bu sahədəki roluna diqqət çəkmişdir [3]. Daha geniş beynəlxalq konvensiyanın işlənib hazırlanması zərurəti "Bakutel-2013" sərgi-konfransından təxminən 2 ay öncə Seul Kiberməkan Konfransında BMT Baş katibi Pan Gi Munun video mesajinda da vurğulanmışdır [4].

Qeyd edilən məsələnin ölkələr arasında ikitirəliyə gətirib çıxardığını "Bakutel-2013" sərgi-konfransı ilə eyni vaxtda Strasburqda təşkil edilmiş Oktopus Konfransı əyani olaraq göstərdi. Belə ki, konfrans Avropa, Amerika, Asiya-Sakit Okean hövzəsi ölkələri və Afrikada qanunvericilik sisteminin Budapeşt Konvensiyasının standartlarına uyğun şəkildə harmonizasiyasını təqdirəlayiq hal hesab edir və həmin ölkələr müvafiq konvensiyaya qoşulmağa dəvət olunurdu [5].

Budapeşt Konvensiyası: üstünlüklər və çatışmazlıqlar

Avropa Şurasının (AŞ) 2001-ci ildə Budapeştdə imzalanmış və 2004-cü ildə qüvvəyə minmiş Kibercinayətkarlıq və ya Budapeşt Konvensiyası kibercinayətkarlıqla mübarizədə tarixi nailiyyət hesab oluna bilər və bu günə qədər müvafiq sahədə aparıcı və ən çox istinad olunan beynəlxalq sənəddir [6]. 2014-cü ilin fevral ayına qədər Budapeşt Konvensiyası 49 ölkə tərəfindən imzalanmış, 41 ölkə tərəfindən ratifikasiya edilmişdir [7]. Azərbaycan da Budapeşt Konvensiyasını 30 iyun 2008-ci ildə imzalamış, 30 sentyabr 2009-cu ildə ratifikasiya etmişdir. Milli qanunvericiliyin Konvensiyaya uyğunlaşdırılması məqsədilə Azərbaycan Respublikası Cinayət Məcəlləsinə və digər normativ hüquqi aktlara müvafiq əlavə və düzəlişlər edilmişdir [8]. Layihəsinin hazırlanması və qəbul edilməsi AŞ tərəfindən həyata keçirilməsinə baxmayaraq, Budapeşt Konvensiyası AŞ üzvü olmayan ölkələr üçün də açıqdır və regional saziş hesab olunmur. AŞ üzvü olmayan ABŞ, Kanada, Yaponiya və Cənubi Afrika onu imzalamış, ABŞ və Yaponiya, Avstraliya, Dominikan Respublikası və Mavriki Respublikası isə ratifikasiya etmişdir.

Budapeşt Konvensiyası kibercinayətkarlıqla mübarizədə ən geniş əhatə dairəsinə malik sənəddir. Belə ki, bu Konvensiya bütün dünya üzrə İnternet istifadəçilərinin üçdə bir hissəsini əhatə edir. Bu sənəddə kibercinayətkarlıq üzrə maddi və prosessual hüquqlar, yurisdiksiya sahəsində qabaqcıl təcrübə öz əksini tapıb. Ən vacib cəhətlərindən biri odur ki, Konvensiyanın müddəaları əksər üzv ölkələr tərəfindən milli qanunvericiliyə tətbiq edilmişdir.

Budapeşt Konvensiyasının ən mühüm çatışmazlığı kimi onun Avropa sərhədlərindən kənara çıxmaması göstərilir. Belə ki, Konvensiyanı ratifikasiya etmiş 41 dövlətdən yalnız 5-i

(ABŞ, Yaponiya, Avstraliya, Dominikan Respublikası və Mavriki Respublikası) AŞ üzvü deyildir. Bu səbəbdən regional səviyyədə (Karib hövzəsi, Qərbi Afrika və s.) kibercinayətkarlıq üzrə qanunvericilik formalaşdırılmağa başlanmışdır [7]. Lakin 2014-cü ilin yanvar ayında Afrika Birliyi tərəfindən hazırlanmış Kibertəhlükəsizlik Konvensiyası İnternetdə ifadə azadlığını məhdudlaşdıracağı, qitə ölkələrinin iqtisadiyyat və mədəniyyətinə mənfi təsir göstərə biləcəyi səbəbindən qəbul edilmədi. Bundan başqa, Budapeşt Konvensiyasına qoşulma tələblərinin BMT konvensiyaları ilə müqayisədə daha sərt olması ona daha çox ölkələrin qoşulması üçün maneə hesab olunur. Konvensiyaya üzv olmaq üçün ona üzv olan bütün ölkələrin yekdil razılığı vacibdir. Budapeşt Konvensiyasının 37-ci maddəsinə görə, AŞ Nazirlər Şurası konvensiya üzrə razılığa gəlmiş tərəflərlə məsləhətləşmələrdən və onların anonim razılığını aldıqdan sonra Şuranın üzvü olmayan və ya Konvensiyanın hazırlanmasında iştirak etməyən istənilən dövləti Konvensiyaya qoşulmağa dəvət edə bilər [6].

Bundan başqa, inkişaf etməkdə olan ölkələr Konvensiyanın layihəsinin hazırlanmasında iştirak etməmişdir. Hazırda inkişaf etməkdə olan ölkələrin İnternet istifadəçilərinin sayı inkişaf etmiş ölkələrinkindən daha çoxdur və birincilərin kiberməkandakı risklərə məruz qalması ehtimalı daha böyükdür. Bu səbəbdən, kibercinayətkarlıqla mübarizəyə inkişaf etməkdə olan ölkələrin cəlb edilməsi zəruridir.

Konvensiyanın müasir və gələcək texnologiyaları əhatə etməsi məqsədilə texnoloji baxımdan neytral dildə tərtib olunmasına baxmayaraq, ən mühüm arqumentlərdən biri onun kiberməkandakı müasir cinayət və riskləri əhatə etməməsidir. Bundan əlavə, elektron sübutların məhkəmə tərəfindən qəbul edilməsi qaydaları və İnternet provayderlərinin məsuliyyəti, təşkilati məsələlər, dövlət və özəl sektor əməkdaşlığı Konvensiyada öz əksini tapmamışdır.

Konvensiyasının 32b maddəsinin beynəlxalq hüququn hamılıqla tanınmış prinsiplərindən olan milli suverenlik prinsipi ilə ziddiyyət təşkil etməsi narahatlıq doğurur [6]. Belə ki, Konvensiyanı ratifikasiya edən dövlət digər dövlətlərə öz ərazisində təhqiqat aparmağa icazə verməklə milli suverenlik prinsipindən qismən imtina etmiş olur. Həmin maddəyə görə, hüquq-mühafizə orqanları məxsus olduqları ölkənin sərhədləri xaricində yerləşən, ictimaiyyətə açıq olmayan kompüter məlumatlarını bu cür məlumatları açıqlamaq üçün qanuni icazəsi olan şəxsin qanuni və könüllü icazəsi ilə əldə edə bilərlər.

Digər cəhdlər

Kibercinayətkarlıqla mübarizədə ümumi hüquqi çərçivənin təsbit olunmasında AŞ son dövrlərə qədər mühüm rol oynasa da, artıq bu təşəbbüsün istər qanunvericilik, istərsə də təcrübə baxımından Avropa Birliyinə (AB) keçdiyi iddia olunur. İstənilən halda kibercinayətkarlıqla mübarizədə Avropa mübarizə modeli dəyərlidir və gələcək qlobal inkişaf üçün baza rolunu oynaya bilər. Lakin ümumilikdə, kibercinayətkarlığın qlobal xarakteri ilə əlaqədar Avropa qitəsində həyata keçirilən tədbirlər qənaətbəxş hesab edilmir. Bu səbəbdən bir sıra dövlətlər BMT çərçivəsində yeni qlobal kibertəhlükəsizlik konvensiyasının işlənib hazırlanmasını zəruri hesab edir.

On ildən artıq bir müddətdə kibertəhlükəsizlik məsələlərinə öz gündəliyində geniş yer ayıran BMT bu rolu 1949-cu ildən telekommunikasiya və İKT sahəsində ixtisaslaşmış quruma çevrilmiş BTİ vasitəsilə həyata keçirir. BTİ kiberməkandakı təhdid və zəif nöqtələrə qarşı şəbəkə, xidmət və mexanizmlər işlənib hazırlanmasında dövlət və özəl sektor üçün qlobal mərkəz hesab olunur. BMT kibertəhlükəsizlik məsələləri ilə əlaqədar öz mövqeyini Baş Assambleya çərçivəsində qəbul edilmiş qətnamələrlə ifadə etmişdir [9].

İnformasiya Cəmiyyəti üzrə Ümumdünya Sammitinin ikinci - Tunis mərhələsində iştirak edən dövlətlər İKT-nin istifadəsinə inam və etibarı formalaşdırmaq üzrə vahid moderator rolunu BTİ-yə həvalə etmiş [10], 2006-cı ildə BTİ-nin yeni Baş katibi seçilmiş H.Ture BMT çərçivəsində qəbul edilmiş sənədlər arasında ən geniş əhatə dairəsinə malik olan və ən perspektivlisini - Qlobal Kibertəhlükəsizlik Gündəliyi və Qlobal Strateji Hesabatı təqdim

etmişdir [11]. BMT çərçivəsində kibertəhlükəsizlik üzrə qlobal konvensiyanın layihəsinin hazırlanmasında qeyd edilən sənədlərin danışıqlar üçün baza rolu oynayacağı gözlənilir.

Bundan başqa, bir sıra tədqiqat institutları və alimlər kibercinayətkarlıqla mübarizə üzrə mühüm layihələr işləyib hazırlamışlar. Amerika Huver İnstitutu tərəfindən 2001-ci ildə hazırlanmış və bu günə qədər kibercinayətkarlığa qarşı beynəlxalq sənəd üçün aparıcı akademik təklif hesab edilən "Kibercinayətdən və terrorizmdən müdafiəni gücləndirmək üçün Beynəlxalq Konvensiyanın Stanford Layihəsi 2000"dir [12]. Layihə kiberməkanda əsas cinayətlərin beynəlxalq səviyyədə tanınması, təhqiqatı, cinayətkarların ekstradisiyası və mühakiməsi sahəsində əməkdaşlıq edilməsi üçün universal sazişi təşviq etmək məqsədilə yaradılmışdır.

2014-cü ilin yanvar ayında Afrika Birliyi tərəfindən hazırlanmış Kibertəhlükəsizlik Konvensiyası İnternetdə ifadə azadlığını məhdudlaşdırmaq, qitə ölkələrinin iqtisadiyyat və mədəniyyətinə mənfi təsir göstərə bilmək ehtimalı səbəbindən Birlik üzvləri tərəfindən qəbul edilmədi [13]. Fikrimizcə, bu hadisə hətta regional səviyyədə konvensiya layihəsi üzrə ölkələr arasında razılığın əldə edilməsinin asan olmadığını və mövcud alətlərin təkmilləşdirilərək istifadə edilməsinin məqsədəuyğunluğunu bir daha sübut edir.

Qlobal kibertəhlükəsizlik konvensiyasının tərəfdarları və əleyhdarları

Kibercinayətkarlıqla mübarizə sahəsində yeni beynəlxalq konvensiyanın hazırlanması təşəbbüsü ilə bir neçə dəfə çıxış etmiş Rusiyanın bu məsələdə əsas arqumenti Budapeşt Konvensiyasının köhnəlmiş olması və dövlətlərin suverenliyini pozan müddəaları ehtiva etməsidir. Qeyd edək ki, Rusiya AŞ üzvü olmasına baxmayaraq, Konvensiyaya qoşulmamışdır. Konvensiyanın kiberterrorizmi tənzimləməməsi də Rusiyanı narahat edən məsələlərdəndir. Lakin Rusiya yeni Konvensiyanın AB və ya NATO deyil, məhz BMT çərçivəsində hazırlanmasının tərəfdarıdır [14]. 2011-ci ilin sentyabr ayında Rusiya, Çin, Tacikistan və Özbəkistan bu məsələ ilə bağlı BMT Baş Assambleyası çərçivəsində müfaviq qətnamənin qəbul edilməsi təşəbbüsü ilə çıxış etmişdir. Budapeşt Konvensiyasının qlobal standart kimi qəbul edilməsinin əleyhinə olan BTİ Baş katibi H. Turenin mövqeyi bu səbəbdən Rusiya tərəfindən dəstəklənir.

Lakin qeyd edilən məsələ ilə bağlı Rusiya ilə Qərb dövlətləri, xüsusilə, ABŞ arasında ortaq məxrəcə gəlinməsi real görünmür. İki dövlət arasında fikir ayrılığının əsas səbəbi onlar üçün müxtəlif mənalar daşıyan "informasiya təhlükəsziliyi" anlayışıdır. Kiberməkanın fiziki infrastrukturunu təşkil edən naqillər, serverlər, routerlər və s. kimi rəqəmsal informasiyadan hazırlanmış proqram təminatı informasiya texnologiyaları hesab olunur. Bu mənada, böyük ziyan vurmaq iqtidarında olan *Stuxnet* kimi proqram təminatı "informasiya silahı"dır. ABŞ informasiya təhlükəsizliyinin bu cür məhdud şərhinə üstünlük versə də, Rusiya informasiya, ideya və komminikasiya platformalarının hakimiyyət əleyhinə istifadə edilməsindən ehtiyat edərək, bu cür platformaların da "informasiya təhlükəsizliyi" termini ilə əhatə olunmasının tərəfdarıdır.

Hələ 1998-ci ildə Rusiya BMT Baş Assambleyasına "informasiya silahları"nın müəyyənləşdirilməsi və günahkarların cəzalandırılması ilə bağlı qətnamə layihəsi təklif edərkən ABŞ mövcud qanunların kiberməkandan hərbi məqsədlərlə istifadəni kifayət qədər tənzimləməsi səbəbindən Rusiyanın mövqeyini dəstəkləməmişdi. Ehtimal olunur ki, o dövrdə ABŞ-ın bunu etməsi üçün üç səbəb var idi. Birincisi, ABŞ digər dövlətlər tərəfindən özünə qarşı kibermüharibəni real hesab etməyərək, kiberməkanda milli təhlükəsizliyi üçün əsas təhlükəni terroristlərdən gözləyirdi. İkincisi, ifadə azadlığının məhdudlaşdırılması Amerika dəyərləri və rəsmi xarici siyasətlə bir araya sığa bilməzdi. Üçüncüsü, ən güclü kiberhücum imkanlarına malik olması ehtimal edilən bir dövlət kimi kibersilahların məhdudlaşdırılması ABŞ-ın maraqlarına uyğun olmazdı.

Lakin 2010-cu ildə Rusiya və bir sıra digər dövlətlərlə birgə BMT Baş Assambleyasında qlobal səviyyədə kibertəhlükəsizliyi genişləndirən beynəlxalq normaların işlənib hazırlanması zəruriliyini bəyan edən qətnamə layihəsini dəstəkləyən ABŞ-ın mövqeyində dəyişiklik baş verdi.

Siyasi kursda bu cür kəskin dəyişikliyin baş verməsi səbəbləri tam aydın olmasa da, bunun ABŞ siyasətçiləri tərəfindən kiberməkanda öz ölkələrinin zəifliyinin dərk etmələri ilə əlaqələndirmək olar [15].

Ağ Evin kibertəhlükəszilik üzrə keçmiş müşaviri R.Klarke ölkənin milli kibertəhlikəsizliyi üçün güclü kiberhücum imkanlarına malik olmağı üç vacib faktordan yalnız biri hesab edir [16]. Kibermüdafiə imkanları və ölkənin kiberməkandan asılılığı dərəcəsi də milli kibertəhlükəszilik üçün vacib elementlərdir. Rusiya, Çin və İran ABŞ-dan daha zəif kiberhücum imkanlarına malik olmasına baxmayaraq, daha güclü kibermüdafiə imkanlarına malikdirlər və kiberməknadan daha az asılıdırlar. Hər üç faktoru vəhdət şəklində nəzərdən keçirən R.Klarke ABŞ-ın milli kibertəhlükəsziliyinin adıçəkilən dövlətlərdən daha zəif olması qənaətinə gəlir.

Lakin qeyd edilən cəhətlərin ABŞ-ın kibertəhlükəsziliklə bağlı dövlət siyasətində dəyişikliyə səbəb olması beynəlxalq kibersiyasətdə digər dövlətlər, o cümlədən Rusiya ilə ortaq məxrəcə gəlməsinə kömək etmədi. Belə ki, Rusiyanın yuxarıda adıçəkilən qətnamə layihəsi ABŞ və əsas Qərb dövlətləri tərəfindən ifadə azadlığını məhdudlaşdırması səbəbindən dəstəklənmədi [17]. Qətnamə layihəsi informasiyanın axtarılması, əldə edilməsi və yayılması hüquqlarının milli qanunlar əsasında tənzimlənməsini təklif etsə də, təşəbbüskar dövlətlərin (Rusiya, Çin, Tacikistan və Özbəkistan) nəşr, yayım və İnternet azadlığı sahəsində hüquqları məhdudlaşdıran ölkələr arasında ilk yerləri tutması Qərb dövlətlərinin qətnamə layihəsini qəbul etməməsi ilə nəticələndi.

Bundan başqa, siyasi məqsədlər üçün kibercinayətkarlığın müxtəlif növlərini maliyyələşdirməkdə ittiham olunan Rusiya və Çinin kibercinayətlərin istintaqı və mühakiməsi üzrə beynəlxalq əməkdaşlığın yüksək standartları ilə razılaşaraq öz üzərlərinə öhdəlik götürmələri şübhə ilə qarşılanır. Belə ki, Rusiya 2007-ci ilin aprel ayında Tallində Bürünc əsgər heykəlinin yerinin dəyişdirilməsindən sonra Estoniya və Rusiya arasında diplomatik qalmaqal yaranmışdır. Bu hadisədən sonra Rusiya Estoniyanın dövlət qurumlarına, banklarına, KİV-lərinə məxsus saytlara edilən *DDoS* hücumlarına görə məsuliyyət daşımadığını bəyan etmişdir. Lakin həmin insidentlərin araşdırılması üçün Estoniya hökuməti ilə əməkdaşlıq etməkdən imtina etməsi hücumların arxasında məhz Rusiyanın dayanmasını ehtimal etməyə əsas vermişdir [16].

Budapeşt Konvensiyasının Asiya-Sakit Okean İqtisadi Əməkdaşlığı, AB, İnterpol, Amerika Dövlətləri Təşkilatı tərəfindən dəstəkləndiyini və kibercinayətkarlıqla mübarizədə aydın və hərtərəfli çıxış yolları təklif etdiyini bəyan edən AŞ Budapeşt Konvensiyasının layihəsinin hazırlanmasında iştirak etməmiş dövlətlərin siyasi səbəblərdən ona qoşulmaqdan imtina etmələrini anlayışla qarşılayır. Bununla belə, Konvensiyaya qoşulan ölkələrin Budapeşt Konvensiyasının Komitəsinə üzvlük əldə edərək onun gələcəkdə yenilənməsində iştirak edə biləcəyini bəyan edir. AŞ kibercinayətkarlıqla mübarizə üzrə yeni konvensiya layihəsinin hazırlanmasının deyil, BMT çərçivəsində Budapeşt Konvensiyasının təmin etdiyi prosessual hüquqlar və əməkdaşlıq imkanları üzrə konsensusun əldə edilməsini təklif edir [18].

Nəticə

Kibercinayətkarlıqla effektli mübarizə aparmaq və kiberməkanda təhlükəsizliyə nail olmaq üçün Budapeşt Konvensiyasına daha çox ölkənin qoşulması vacibdir. Yeni qlobal konvensiya layihəsinin hazırlanması illərlə davam edə, diplomatik mübahisələrlə müşayiət oluna və müsbət sonluqla nəticələnməsi qeyri-müəyyən olan bir proses ola bilər. Bu həm də üzv dövlətlər tərəfindən Budapeşt Konvensiyası əsasında artıq həyata keçirilməkdə olan qanunvericilik islahatlarını ləngidə, qanunvericilik və digər tədbirlərin həyata keçirilməsinin təxirə salınmasına səbəb ola bilər. Bundan başqa, artıq mürəkkəb qanunvericilik islahatları həyata keçirmiş və Konvensiyanı tətbiq etmiş ölkələr bu cəhdlərini yenidən təkrarlamaq məcburiyyətində qala bilərlər.

Budapeşt Konvensiyasının üzv ölkələr tərəfindən tətbiqinin effektli olması və onlara kibercinayətkarlıqla mübarizədə mühüm təcrübə qazandırması faktı inkar edilə bilməz. AŞ

Konvensiyanın yenilənməyə ehtiyacı olduğunu etiraf etmişdir və bu sənəd təşkilata üzv olmayan ölkələrin qoşulması və Konvensiyanın təkmilləşdirilməsində iştirak etməsi üçün açıqdır.

Yeni qlobal konvensiyanın Budapeşt Konvensiyasından fərqli tənzimləmə predmeti və istinad edəcəyi standartlar vacib aspektlərdir. Bu cür konvensiyanın inkişaf etməkdə olan ölkələr üçün daha aşağı standartlar təsbit edərək rəqəmsal uçurumu daha da dərinləşdirmək və effektli beynəlxalq əməkdaşlığa əngəl yaratmaq ehtimalı vardır. Bundan başqa, daha aşağı və daha az spesifik prosessual hüquq müddəalarının daha aşağı təhlükəsizlik tədbirləri nəzərdə tutması kiberməkanda mövcud vəziyyətin daha da gərginləşməsinə səbəb ola bilər.

İndiki mərhələdə artıq bir çox ölkələrdə başlanmış harmonizasiya prosesini və maliyyə imkanlarının çatışmazlığını nəzərə alaraq, harmonizasiya proseslərini təkrarlamaqdansa, resursları artıq mövcud olan alətlərin tətbiqinə yönəltmək, ölkələrə Budapeşt Konvensiyasının və əlaqədar tədbirlərin tətbiqi üçün texniki yardım göstərməyin kibertəhlükəsziliyin təmin edilməsi üçün daha effektli olduğu hesab edilir [20].

Qeyd olunanları nəzərə alaraq, mövcud Konvensiyanın kiberməkandakı müasir risklərə uyğun şəkildə yenilənməsi və ona daha çox ölkənin cəlb edilməsi daha rasional hesab olunur. Budapeşt Konvensiyası artıq 10-cu ildir ki qüvvədədir. Onun qlobal standarta çevrilə bilməsi üçün daha çox dövlət tərəfindən imzalanması və ratifikasiya edilməsi məqsədilə AŞ və BMT tərəfindən birgə tədbirlər həyata keçirilməli və Konvensiyaya qoşulma tələbləri yumşaldılmalıdır.

Ədəbiyyat

1. Wall D. S. The Transformation of Crime in the Information Age, 2007, Wiley, 2007, 288 p.
2. http://www.bakutel.az/2013/?l
3. Speech by ITU Secretary-General, Dr Hamadoun I. Touré , Global Cybersecurity Cooperation: Challenges and Visions Opening Ceremony Opening Speech, 02 December 2013, Baku, Azerbaijan, http://www.itu.int/en/osg/speeches/Pages/2013-12-02.aspx
4. Secretary-General's video message to the Seoul Conference on Cyberspace, Seoul, Republic of Korea, 17 October 2013, http://www.un.org/sg/statements/?nid=7209 *l*
5. Key messages - Octopus Conference 2013 Strasbourg, 4-6 December 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571Octo2013_keymessages_v3short.pdf
6. Convention on Cybercrime, Budapest, 21 November 2011, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
7. http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
8. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, 30 sentyabr 2009-cu il, http://www.cert.az/konvensiya.html
9. Резолюции Генеральной Ассамблеи, http://www.un.org/ru/development/ict/res.shtml
10. Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16-18 November 2005, http://www.itu.int/wsis/docs2/tunis/off/ 9rev1.pdf
11. ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Global Strategic Report, http://www.cybercrimelaw.net/documents/Chairmans_Report.pdf
12. Draft International Convention To Enhance Protection from Cyber Crime and Terrorism, http://www.stanford.edu
13. Draft African Union Convention on the establishment of a credible legal framework for cyber security in Africa, http://www.au.int/en/cyberlegislation

14. Смирнов А.И. Геополитические вызовы информационной безопасности, http://www.нииглоб.рф
15. Yılmaz S. "Enhancing international cybersecurity: Will the UN reach a deal?" September 23, 2013, http://www.nationmultimedia.com
16. Clarke R.A., Knake R. Cyber War: The Next Threat to National Security and What to Do About It, HarperCollins Publishers, 2010, 304 p.
17. Baldor C.L. "Cyber weaknesses should deter US from waging war" 11 July 2011, http://www.nbcnews.com
18. Contribution of the Secretary General of the Council of Europe to the Twelfth United Nations Congress on Crime prevention and criminal justice Salvador, Brazil, 12-19 April 2010, http://www.coe.int

УДК 341:004.9

Мамедов Бахтияр Н.[1], Аскерова Айсел Н.[2]
Министерство Связи и Высоких Технологий Азербайджанской Республики, Баку, Азербайджан
[1]law@mincom.gov.az, [2]law-aysel@mincom.gov.az

Необходимость принятия глобальной конвенции по кибербезопасности, или возможности превращения Будапештской Конвенции в глобальный стандарт

В целях эффективной борьбы с киберпреступностью, перешагнувшей границы отдельно взятых государств и обеспечения безопасности на киберпространстве, необходимо подписание глобального многостороннего соглашения или Конвенции. Принятая в рамках Совета Европы и действующая более 10 лет, Будапештская конвенция носит региональный характер и не охватывает новые угрозы на киберпространстве, а потому не считается удовлетворительной. В связи с этим некоторые страны выступают с инициативой разработки и принятия новой конвенции по глобальной кибербезопасности в рамках ООН. В настоящем исследовании приводится анализ преимуществ и недостатков Будапештской конвенции, указаны причины разногласий между ведущими мировыми державами относительно конвенции по глобальной кибербезопасности, а также дается прогноз возможного развития событий и предлагаются пути разрешения разногласий.

Ключевые слова: *кибербезопасность, кибепреступление, киберпространство, Будапештская Конвенция, конвенция по глобальной кибербезопасности.*

Bachtiyar N. Mammadov[1], Aysel N. Asgarova[2]
[1,2]Ministry of Communications and High Technologies of the Republic of Azerbaijan, Baku, Azerbaijan
[1]law@mincom.gov.az, [2]law-aysel@mincom.gov.az

Necessity of global cybersecurity convention or the opportunities for Budapest Convention to become a global standard

Global multilateral agreement or convention is necessary to effectively combat cybercrimes that have crossed the geographical boundaries of states and to provide security in cyberspace. Budapest Convention, which was adopted in the framework of Council of Europe and has been in force for 10 years, now is not considered satisfactory by some national states, since it is of a regional character and does not cover new threats in cyberspace, and some states initiate elaborating new global cybersecutiry convention in the framework of the UN. The present research analyses the advantages and disadvantages of Budapest Convention, proposes forecast for future development of events and possible solutions by examining the disagreement among the leading states of the world on new global cybersecutiry convention.

Keywords: *cybersecurity, cybercrime, cyberspace, Budapest Convention, global cybersecutiry conventions.*