Əlizadə C. Ş., Əliyev B.Ə.♦

DOI: 10.25108/2304-1730-1749.iolr.2018.55.21-37

Kibertəhlükəsizlik dövlət təhlükəsizliyinin tərkib hissəsi kimi

Xülasə: Qloballaşma dövründə insanları ən çox narahat edən məsələlərdən biri və birincisi təhlükəsizlik və onun təminatı məsələsidir. Artıq qeyd etmək olar ki, kibertəhlükəsizlik dövlətin, cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir.

Son illər informasiya-kommunikasiya texnologiyaları (İKT) elə bir sürətlə inkişaf edir ki, onun sonrakı fəsadlarının əvvəlcədən dəqiq müəyyən edilməsi çox zaman mümkün olmur və sonradan yaranan neqativ vəziyyətin aradan qaldırılmasına yetərincə vəsait, zaman və bilik sərf etmək lazım gəlir. Əsasən də, Internet qlobal şəbəkəsində tətbiq edilən yeni texnologiyalar, layihələr və müxtəlif proqramlar ilk baxışdan faydalı və zərərsiz görünsə də, təcrübə göstərir ki, bir çox hallarda onların yaratdığı problemlərin qarşısını tam almaq mümkün olmur.

Kompüter şəbəkələrinin genişlənməsi kibermünaqişələrdə şəbəkə texnologiyalarının imkanlarından daha geniş istifadə etməyə, şəbəkə istifadəçilərinin fəaliyyətlərində koordinasiyanın, əhatəliliyin və mürəkkəbliyin artmasına şərait yaradır. Bu isə kibercinayətlərin çoxalmasına, onların daha təcrübəli və müasir İKT vasitələri ilə təmin olunmuş istifadəçilər tərəfindən aparılmasına səbəb olur.

Yuxarıdakılara əsaslanaraq deyə bilərik ki,kibertəhlükəsizliyin təmin edilməsi vacib məsələdir. Bu məsələ ilə bağlı milli siyasət vəbu siyasət çərçivəsində hazırlanmış bir kibertəhlükəsizlik strategiyası tələb olunur. Kiber hücumların,

♦**Əlizadə Cavid Şirzad oğlu** - AMEA-nın Hüquq və İnsan Haqları İnstitutunun "Dövlət təhlükəsizliyinin hüquqi təminatı" şöbəsinin elmi işçisi (Azərbaycan). E-mail: cavid6455@mail.ru
Əliyev Bəxtiyar Əbdürəhman oğlu- AMEA-nın Hüquq və İnsan Haqları İnstitutunun "Dövlət təhlükəsizliyinin hüquqi təminatı" şöbəsinin müdiri, h.ü.f.d.,dosent (Azərbaycan). E-mail:antiterror-baku@mail.ru

ümumiyyətlə mala və ehtimal daxilində də olsa cana təsir edən nəticələri ola biləcək olduğundan kiber təhlükəsizliyin təmin edilməsində bu nəticələrin və bu nəticələrə gətirib çıxaran hərəkət vəüsulların cinayət olaraq təyin olunması və cəzalandırılmasıböyük əhəmiyyət kəsb edir.

Açar sözlər: kibertəhlükəsizlik; beynəlxalq kibertəhlükəsizlik strategiyaları; kiber müdafiə.

Kibertəhlükəsizlik anlayışı və onunla bağlı anlayışlar son vaxtlar sürətlə inkişaf etmiş və inkişafı davam edir. İnformasiya və informasiya texnologiyalarındakı inkişafa paralel olaraq bu sahədəki anlayışlar da olduqca dinamik və sürətli şəkildə çoxalmaqdadır.

Kibertəhlükəsizlik ilk dəfə 1990-cı illərdə kompüter mühəndisləri tərəfindən, şəbəkəyə bağlı kompüterlərlə əlaqədar təhlükəsizlik problemlərini ifadə etmək üçün istifadə edilmiş, lakin bu təhlükəsizlik problemlərinin dağıdıcı sosial nəticələr yarada biləcəyi ortaya çıxdıqda zamanla nüfuzlu şəxslər və media tərəfindən qərb dünyasına qarşı böyük bir təhdid olaraq qiymətləndirilmiş və "elektron Kiber Pörl Harbor"lar olaraq dilə gətirilmişdir. ABŞ-da 2001-ci il 11 sentyabr tarixində baş vermiş terror aktı informasiya texnologiyalarına, kompüterlər təhlükəsizliyinə diqqət artırılmasını təmin etmiş, xüsusilə də informasiya texnologiyaları infrastrukturlarının qorunması, elektron müşahidəetmə, terrorçuların Interneti rabitə vasitəsi olaraq istifadə etməsi məsələləri diqqət çəkmişdir.

Kibertəhlükəsizliyə istiqamətlənmiş, şəbəkələr vasitəsilə təhdid meydana gətirən əsas hücum vasitələri nisbətən fərqlidir.Belə ki, dövlətlərin kibertəhlükəsizliyinə istiqamətlənmiş təhdid meydana gətirən hücumlar dövlətlərin bir-birilərinə qarşı meydana gətirdiyi kibertəhdidlər və xarici aktorlar tərəfindən dövlətlərin kibertəhlükəsizliyinə istiqamətlənmiş təhdidlər şəklində 2 kateqoriyaya ayırmaq olar. Kiber qarşıdurmalar, iqtisadi casusluq və kəşfiyyat təhdidləri birinci

kateqoriyaya aid edilir. Kiber şəbəkələr vasitəsilə işlənilən cinayətlər və kiberterrorçuluq isə ikinci kateqoriyaya aid təhdidlərdir [4].

Qeyd etmək olar ki, kiber məkanın kompleks və çox ölçülü özünəxas mühiti kiber təhlükəsizliyi prioritetli təhlükəsizlik sahələrindən biri halına gətirmişdir. Kiber mühitdəki hər cür məlumatın qorunması şəklində təyin olunan kiber təhlükəsizlik, eyni zamanda məlumatın istehsalını və saxlanılmasını özündə əks etdirir.Ən ümumi mənada kibertəhlükəsizlik kiber mühitdə təşkilat, quruluş və istifadəçilərin varlıqlarını qorumaq məqsədi ilə istifadə edilən vasitələr, təhlükəsizlik konsepsiyaları, təhsil və texnologiyanı ümumi şəkildə özündə əks etdirir [6]. Kiber mühitdə bəzi təhlükəsizlik meyarlarının təmin edilməsi lazımdır. Bunlar gizlilik, düzgünlük, bütünlük, ardıcıllıq, etibarlılıq, davamlılıq şəklində olmalıdır [1]. İnformasiya sistemlərinə olan hücumlar nəticəsində gizli məlumatların yayılması, xaosun baş verməsi dövlətləri çətin vəziyyətə sala bilər.Məsələn, 2007-ci ildə Estoniyada meydana gələn kiber hücum, bir ölkənin mühüm infrastrukturlarının Internetdən gələn təhlükələr qarşısında nə qədər müdafiəsiz ola biləcəyini göstərmişdir. Estoniyada bu təhdidin həyati məna kəsb etməsinin səbəbi, ölkədəki ictimai və özəl sektorla bağlı bir çox fəaliyyət sahəsininInternet vasitəsilə icra edilməsidir [2]. Yenə, Avstraliyada hirsli bir işçinin kompüter sistemlərini manipulyasiya edərək çay və parklara saldığı tullantı sular, proqramlar vasitəsilə ABŞ-da 11 adamın ölümünə gətirib çıxaran və 50 milyon adamın çarəsiz qalmasına səbəb olan elektrik kəsintisi və İran nüvə təsislərinə istiqamətli şəkildə reallaşdırılan "Stuxnet" hücumları ağıla gələn nümunələr arasındadır.

Kibertəhlükəsizliyin təbəqələrini tətbiq təhlükəsizliyi, xidmət təhlükəsizliyi və infrastruktur təhlükəsizliyi şəklində qeyd etmək olar. Unver M.Kiber tədid və hücumlarınistiqamətli yoxetmə, ziyan vermə, silmə, ifşa etmə, maneə törətmə şəklində təsnifatını vermişdir [7]. Bütün bunlara əsaslanaraq demək olar ki, təhlükəsizliyin təmin edilməsi sahəsində edilən işlər milli siyasət və bu siyasət

çərçivəsində hazırlanmış bir kibertəhlükəsizlik strategiyası tələb edir. Kiber hücumların, ümumiyyətlə mala və ehtimal daxilində də olsa cana təsir edən nəticələri ola biləcək olduğundan kibertəhlükəsizliyin təmin edilməsində bu nəticələrin və bu nəticələrə gətirib çıxaran hərəkət və üsulların cinayət olaraq təyin olunması və cəzalandırılması böyük əhəmiyyət kəsb edir.Texnologiyanın inkişafı ilə paralel olaraq kiber hücum vasitə və üsullarının dəyişdiyi nəzərə alınaraq ölkə qanunvericiliyinin nəzərdən keçirilməsi ehtiyac vardır. Nöqsanların aradan qaldırılması lazım olduğundan bu mövzuda qanuni bir çərçivənin yaradılması da vacib məsələdir. Bundan başqa proqram təminatı, aparat təminatı və iş proseslərinin keyfiyyəti artırılaraq daha etibarlı olması üçün texniki tədbirlərin inkişaf etdirilməsi ilə yanaşı, kiber təhlükəsizliyin təmin edilməsi barədə təşkilatın yaradılması, beynəlxalq iş birliyi və koordinasiyanın təmin edilməsi və inkişaf etdirilməsi, kibertəhlükəsizliyin təmin edilməsində əhəmiyyətli ünsürlər olaraq gözə dəyməkdədir.

Hazırda təhlükəsiz kiber mühit formalaşdırmaq imkanı olmayan dövlətlərdə var. Bu kimi dövlətlərə yardım göstərilməsi xüsusi əhəmiyyət kəsb edir. Bu da öz növbəsində kiberfəzada təhlükəsizliyin (kibertəhlükəsizlik) təmin edilməsi ilə bağlı strategiyaların hazırlanmasını tələb edir.

AB (Avropa Birliyi) orqanlarının kiberfəzada təhlükəsizliyin təmin edilməsi üzrə fəaliyyəti üç əsas istiqamətdə cəmlənib:

- normativ-hüquqi bazanın inkişaf etdirilməsi;
- institusional strukturların yaradılması;
- təşkilata üzv olan ölkələrin dövlət qulluqçuları və əhalisi arasında məlumat və təhsil kampaniyalarının həyata keçirilməsi.

Hazırda AB-də kiberfəzada təhlükəsizlik məsələləri üzrə minimal zəruri normativ-hüquqi baza yaradılmışdır. Məsələn, 2012-ci ildə Avropa Komissiyası AB üçün “Internetin təhlükəsizliyi strategiyası”nı işləyib hazırlamışdır. Layihədə əsas risklər və problemlərlə yanaşı, iqtisadi və geosiyasi imkanları aşkarlamaq,

üçüncü ölkələrdə Internetin təhlükəsizliyi probleminə hazırlıq səviyyəsini müqayisə etmək, həlli tələb edilən vacib problemləri müəyyənləşdirmək, cari və planlaşdırılan tədbirləri qiymətləndirmək məqsədləri qoyulur.

AB-nin kibertəhlükələrlə mübarizə potensialının gücləndirilməsi 2005-ci ilin sentyabrında yaradılmış Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyinə (European Network and Information Security Agency, ENISA) həvalə edilmişdir.

2013-cü ilin yanvar ayının 1-dən etibarən EuroPol-un tərkibində "Avropa kibertəhlükəsizlik Mərkəzi" fəaliyyətə başlamışdır, onun əsas məqsədi AB-ə üzv olan ölkə vətəndaşlarının artmaqda olan kibercinayətkarlıq hallarından müdafiəsini yaxşılaşdırmaqdır.

AB-ə üzv olan ölkələrin əhalisinin kiberfəzadakı təhdidlər barəsində məlumat səviyyəsini yaxşılaşdırmaq məqsədi ilə 2012-ci ilin oktyabrında ENISA tərəfindən "Avropa kibertəhlükəsizlik aylığı" pilot layihəsi həyata keçirilmişdir. Layihə televiziya və radioda, sosial şəbəkələrdə müvafiq reklam kampaniyalarının aparılmasını, bir sıra ölkələrdə konfransların və dəyirmi masaların təşkilini nəzərdə tuturdu.

Kibertəhlükəsizlik üzrə normativ-hüquqi bazanın yaradılması, institusional strukturların təsis edilməsi məsələlərində xeyli inkişafa baxmayaraq, AB-ə üzv olan ayrı-ayrı ölkələrin potensial kibertəhdidlərlə mübarizəyə hazırlığı yetərli deyil. Bu, xüsusilə, Avropa Parlamentinin 22 noyabr 2012-ci il tarixli “Kibertəhlükəsizlik və müdafiə məsələləri üzrə qətnamə”sində qeyd olunur [6]. Sənəddə terrorçu təşkilatların virtual fəzadan istifadəsi təhlükəsinin artması xüsusilə qeyd olunur.Bildirilir ki, onların AB üçün kritik nəticələri olan kiberhücumlar təşkil etmək imkanları vardır.

Göstərilən nöqsanların aradan qaldırılması məqsədi ilə Avropa Komissiyası 07 fevral 2013-cü ildə "Avropa Birliyinin Kibertəhlükəsizlik Strategiyası: Açıq, Etibarlı və Təhlükəsiz Kiberfəza" sənədini irəli sürmüşdür. Strategiya AB-nin beynəlxalq kibertəhlükəsizlik siyasəti üçün aydın prioritetlər təqdim edir:

•Azadlıq və açıqlıq: Bu strategiya əsas AB dəyərlərinin və fundamental hüquqların kiberfəzada tətbiqində baxışları və prinsipləri müəyyən edir.

•Qanunlar, normalar və AB-nin əsas dəyərləri fiziki dünyada olduğu kimi kiberfəzada da eyni səviyyədə tətbiq edilir: Daha təhlükəsiz kiberfəza üçün cavabdehlik vətəndaşlardan dövlətlərədək qlobal informasiya cəmiyyətinin bütün iştirakçılarının üzərinə düşür.

•Kiber təhlükəsizlik potensialının qurulması: AB üçüncü ölkələrdə qlobal potensialın qurulmasını dəstəkləmək üçün beynəlxalq tərəfdaşlarla və təşkilatlarla, özəl sektorla və vətəndaş cəmiyyəti ilə birlikdə çalışacaq. Bura informasiyaya və açıq Internetə çıxışın yaxşılaşdırılması və kibertəhdidlərin qarşısının alınması daxil olacaq.

•Kibertəhlükəsizlik məsələlərində beynəlxalq əməkdaşlığın inkişaf etdirilməsi: Açıq, azad və təhlükəsiz kiberfəzanın saxlanması qlobal çağırışdır və bu problemi AB müvafiq beynəlxalq tərəfdaşlarla və təşkilatlarla, özəl sektorla və vətəndaş cəmiyyəti ilə birlikdə həll etməyə çalışacaq.

Strategiyanın əsas müddəaları aşağıdakılardır:

•Bütün AB üzvü olan ölkələr tərəfindən milli kibertəhlükəsizlik strategiyalarının işlənilməsi;

•Kiberfəzada cinayətkarlıqla mübarizənin əsas beynəlxalq hüquqi aləti kimi "Avropa Birliyinin Kibercinayətkarlıq üzrə Konvensiyasının" siyasi təşkilatın bütün iştirakçıları tərəfindən məcburi ratifikasiyası;

•Ölkələrin kibertəhdidlərlə mübarizəyə hazırlığı üzrə vahid standartlar siyahısının tətbiq edilməsi;

•Avropa şirkətlərinin aşkarlanmış kiberinsidentlər barəsində müəyyən milli orqanı mütləq məlumatlandırması;

•Kibertəhlükəsizlik sahəsində vətəndaş və müdafiə sektorları arasında əməkdaşlığın yaxşılaşdırılması və s.

Avropa Birliyinin kibertəhlükəsizlik strategiyası 2013-cü ilin iyun ayının 19-da qüvvəyə minmişdir və bu sənədə əsasən, ENISA-nın səlahiyyətləri növbəti yeddi ilə qədər uzadılıb.AB ölkələrinin hökumətlərinə kibertəhlükəsizliyə cavabdeh orqanların yaradılması, maliyyə, nəqliyyat və enerji şirkətlərinə – kibertəhdidlərə qarşı tədbirlər işləyib hazırlamaq tapşırılıb.ABŞ strategiyasında olduğu kimi, AB proqramının yaradıcıları da özəl və dövlət sektorları arasında əməkdaşlığa arxalanırlar.

NATO 2007-ci ildə Estoniyanın şəbəkə sisteminə edilən kütləvi kiberhücumlardan sonra - 2008-ci ildə Buxarest zirvə toplantısında kibertəhdidlərə qarşı tədbir görülməsi və kibertəhlükəsizlik sahəsində əməkdaşlıq üçün təhlükəsizlik mərkəzləri qurulmasını qərara almışdı.Bu görüşdə belə fikir ifadə edilmişdi ki, kibertəhlükəsizliyin təmin edilməsi, hər şeydən əvvəl, dövlətlərin vəzifəsidir. Lakin NATO-nun 2010-cu ildə Lissabonda keçirilən zirvə toplantısında kiberfəzadan gələn təhlükələr kütləvi qırğın silahlarının yayılması və terrorçuluqdan sonra NATO ölkələrini hədəfə alan təhdidlər sırasına daxil edildi. Artıq NATO "Kiber Müdafiə Siyasəti" və "Kiber Müdafiə Konsepsiyası" kimi sənədləri işləyib hazırlamışdır.Lakin bu sənədlər məxfidir, alyansın rəsmi veb-saytında onlar haqqında yalnız icmal məlumatları tapmaq olar. Kibermüdafiə prinsiplərinin müəyyən edilməsində alyans üzvləri müttəfiq həmrəyliyi və milli suverenliyin tanınması prinsiplərindən çıxış etmişlər. Başqa sözlə, ümumi məqsəd ondan ibarətdir ki, bütün NATO müttəfiqləri kiberhücumlara hazır olmalı və belə hücumlar zamanı bir-birini dəstəkləmək potensialına malik olmalıdırlar.Bu məqsədə çatmaq üçün müttəfiqlər öz ölkələri daxilində kibermüdafiə potensialını inkişaf etdirməlidirlər. Bu kontekstdə NATO çətiri altında tərəfdaş ölkələr arasında ikitərəfli və çoxtərəfli sıx əməkdaşlıq şəbəkələri qurulur.

Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər Birləşmiş Millətlər Təşkilatı (BMT) Baş Məclisinin 20 dekabr 2002-ci il tarixli 57/239 saylı qətnaməsi ilə təsdiq edilmişdir.

Hal-hazırda Azərbaycanın komputer infrastrukturlarına asılılığı artmaqdadır.Bu günə qədər computer sistemlərinə zərər vermiş hücumlar, hakerlərin dünya səviyyəsində computer viruslarından ibarət olsa da, kiberfəzada mövcud təhdidlər gələcəkdə genişlənə və narahatverici səviyyəyə çata bilər. Çünki texnologiya sistemlərinin təhlükəsizliyini qorumaq çətin məsələdir.Azərbaycanın rəsmi və qeyri-rəsmi texnologiya infrastrukturları daha təhlükəsiz hala gətirilməzsə bu gələcəkdə böyük fəsadlar yarada bilər.

Biblioqrafiya

1. Gorman, Sean P. (2006). A Cyber Threat to National Security? (Edited By: Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan). Seeds of Disaster, Roots of Response. Cambridge: Cambridge University Press, 239-257.

2. Gücüyener, Ayhan(2015). Kritik enerji Altyapılarına Yönelik Gerçekleşmiş Siber Saldırılara İlişkin Bir Değerlendirme. (Editör: Mesut Hakkı Caşın). Uluslararası Kritik Enerji Altyapı Güvenliği: Yeni Tehditler ve Fırsatlar. Hazar Strateji Enstitüsü.18-39

3. Lewis J.A. Assessing the risks of cyber terrorism, cyber war and other cyber threats // Center for Strategic and International Studies, 2002, pp. 3-12. Alekperova IY Information war technology, publishing house "Information Technologies", Baku, 2012, 108 p.

4. Nye, Joseph, Jr. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, Wınter-2011, p.18-38.

5. Sawyer P. Третья мировая может начаться в интернете // Computerworld Russia, Moscow, № 32, 2009, p. 29, Alakbarova I.Y. Information war technology, publishing house "Information Technologies", Baku, 2012, 108 p.

6. Stevens, Tim (2015). Cyber Security, Community, Time, Cyber Security and the Politics of Time. Cambridge: Cambridge University Press.

7. Ünver Mustafa ve Canbay Cafer. (2010). “Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik”, Elektrik Mühendisliği Dergisi, Sayı 438.