Milli kibertəhlükəsizlik strategiyalarının analizi

Yadigar İmamverdiyev

AMEA İnformasiya Texnologiyaları İnstitutu

yadigar@lan.ab.az

***Xülasə*— Müasir dövrdə kibertəhlükəsizlik cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir. Kibertəhdidlərə qarşı çevik, operativ və effektiv mübarizə müəyyən zaman müddətində əldə edilməli olan milli hədəflərin və prioritetlərin, maraqlı tərəflərin rollarının və məsuliyyətinin düzgün müəyyən edilməsini tələb edir. Kibertəhlükəsizlik üzrə milli strategiya bu yolda ilk addımdır. Bu işdə milli kibertəhlükəsizlik strategiyalarının işlənilməsi sahəsində ən yaxşı təcrübənin aşkarlanması məqsədi ilə mövcud milli kibertəhlükəsizlik strategiyaları analiz edilir.**

Açar sözlər*— *kibertəhlükəsizlik; informasiya təhlükəsizliyi; kiberfəza; kiberhücum; kibertəhlükəsizlik strategiyası

I. GİRİŞ

Qlobal informasiya cəmiyyətinə keçid şəraitində dövlətlər, cəmiyyətlər, biznes strukturları və fərdlər kiberfəzada informasiyanın və onun mənbəyinin həqiqiliyi, e-servislərdən təhlükəsiz istifadə, fərdi məlumatların qorunması, verilənlərin tamlığı və konfidensiallığı sahəsində kritik problemlərlə qarşılaşırlar. Yeni kibertəhdidlərin daim meydana çıxdığı və evolyusiya etdiyi mühitdə ölkələrin qlobal kibertəhdidlərə qarşı çevik, operativ kibertəhlükəsizlik strategiyalarına malik olması mühüm əhəmiyyət daşıyır.

Kiberhücumların aktorları çox vaxt anonim qalırlar, kiberfəzada ölkələr arasında sərhədlər aradan qalxır və şəffaflaşır, informasiya və kommunikasiya texnologiyaları (İKT) sürətlə inkişaf edir, kiberhücum metodları və ssenariləri avtomatlaşdırılır və sənayeləşdirilir, kiberhücum alətlərinin qiyməti getdikcə aşağı düşür. Bu səbəblərdən kibertəhdidləri real vaxtda monitorinq və analiz etmək, əks-təsir göstərmək ənənəvi təhlükəsizlik təhdidləri ilə müqayisədə olduqca çətinləşir.

Son illər təşkilatların informasiya infrastrukturuna kiberhücumların təşkilində mühüm dəyişikliklər baş vermişdir. Bu paradiqma dəyişikliyi məqsədyönlü və davamlı hücumlar (Advanced Persistent Threat, APT) adı ilə xarakterizə olunur [1]. APT-nin kiberhücumların ənənəvi növlərindən fərqi yaxşı təşkil olunmuş layihə yanaşması, planlaşdırma, yaxşı maliyyələşdirmə və davamlı yerinə yetirilməsidir. Bu növ hücumlar icraçıların qarşısında qoyulmuş məsələlərdən asılı olaraq, aylarla və hətta illərlə sürə bilər. Bir çox halda hədəf olaraq şəbəkəni dağıtmaq və ya ona sarsıdıcı zərbə endirmək məsələsi qoyulmur, informasiyanın uzun müddət əldə edilməsi və analizi, sonra isə məqsədyönlü istifadəsi nəzərdə tutulur [2].

Mütəxəssislər qeyd edirlər ki, kiberfəza da tezliklə quru, su və hava kimi döyüş əməliyyatlarının səhnəsinə çevriləcək. Artıq bəzi dövlətlərin hərbi qurumları nəzdində kibertəhlükəsizlik üzrə xüsusi bölmələr yaradılıb. Onların vəzifələrindən biri də dövlət infromasiya resurslarına kiberhücumların qarşısını almaqdır.

Hazırda dövlət orqanlarına və özəl şirkətlərə kiberhücum və kibercasusluq halları sürətlə artmaqdadır. Qarşılıqlı əlaqəli və qarşılıqlı asılı informasiya infrastrukturuna yönəlik yaxşı planlaşdırılmış və uğurla yerinə yetirilmiş kiberhücumların nəticəsi çox ağır ola bilər. Fərdi məlumatların kibertəhlükəsizliyi və gizlilik cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir. Buna görə kibertəhlükəsizlik informasiya cəmiyyətinin inkişafının zəruri şərtinə çevrilir.

İnformasiya təhlükəsizliyi Azərbaycan Respublikasında dövlət siyasətinin prioritet məsələlərindən biridir və bu sahədə məqsədyönlü işlər aparılır. Azərbaycan Respublikası Prezidenti cənab İlham Əliyevin imzaladığı "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Fərman informasiya təhlükəsizliyinin, o cümlədən kibertəhlükəsizliyin təmin edilməsi probleminə yeni strateji yanaşmanın formalaşdırılmasını nəzərdə tutur [3].

Məqalədə uğurlu milli kibertəhlükəsizlik strategiyasının işlənib hazırlanması, həyata keçirilməsi və təkmilləşdirilməsi üçün ən yaxşı təcrübənin aşkarlanması məqsədi ilə bu sahədə mövcud olan milli strategiyalar analiz edilir, onların ümumi və fərqli cəhətləri müəyyən edilir, bir sıra tövsiyələr verilir.

II. KİBERTƏHLÜKƏSİZLİK ANLAYIŞI

Ölkələrin milli strategiyalarında "kibertəhlükəsizlik" terminə və digər əsas terminlərə verilən tərifləri xeyli fərqlənir, beynəlxalq səviyyədə də kibertəhlükəsizliyin razılaşdırılmış tərifi mövcud deyil. Nəticədə kibertəhlükəsizlik strategiyalarının işlənilməsinə yanaşmalar da fərqlənir [4]. Bunu nəzərə alaraq, bu bölmədə "kibertəhlükəsizlik" anlayışına yanaşmalar analiz edilir.

Qeyd edək ki, "kibertəhlükəsizlik" termini rus elmi ədəbiyyatında geniş yayılmayıb. Rusdilli normativ-hüquqi sənədlərdə və elmi ədəbiyyatda, adətən, "kibertəhlükəsizlik" əvəzinə, mənasına görə ona yaxın olan "informasiya təhlükəsizliyi" termini istifadə edilir. Lakin "informasiya təhlükəsizliyi" daha geniş anlayışdır, "kibertəhlükəsizlik" "informasiya təhlükəsizliyi"nin tərkib hissəsidir, yalnız kibermühitdə olan informasiyanı əhatə edir.

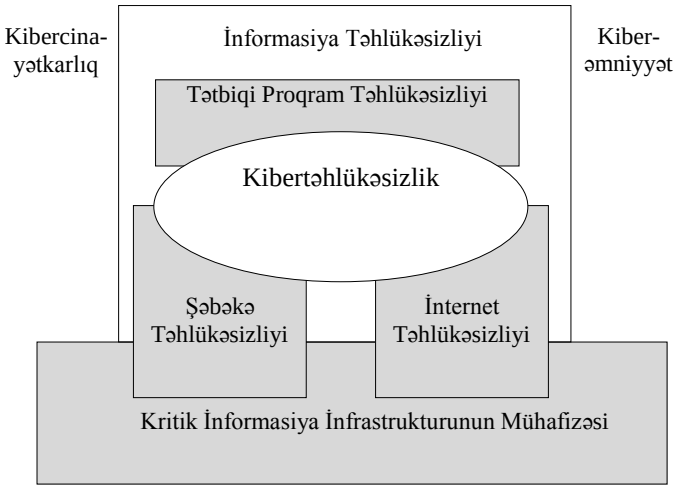
İngilis dilli ədəbiyyatda da bu terminin birmənalı tərifi yoxdur. İngilis dilində "kiber" sözü ilə başlayan onlarla terminə təsadüf etmək olar: kibertəhlükəsizlik, kiberfəza, kiberhücum, kibertəhdid, kibersilah, kibermüharibə, kibermühafizə və s.

"Kiber" sözü "kibernetika" sözündən törəmədir. "Kibernetika" termini qədim yunan dilində "kibernetes" sözündən yaranıb, mənası sükançı, idarə edən deməkdir.

Güman edilir ki, bu termin ilk dəfə qədim yunan filosofu Platon tərəfindən işlədilib. 19-cu əsrdə bu söz A.Amper tərəfindən və ondan sonra bəzi Avropa müəllifləri tərəfindən işlədilmişdir. "Kibernetika" termini 1948-ci ildə amerikan alimi N.Vinerin "Kibernetika" kitabı çap olunduqdan sonra geniş yayılmağa başladı. Viner metodoloji ortaqlığı əsas götürərək kommunikasiya və idarəetməyə aid müxtəlif elmlərin bir ad altında birləşdirilməsi üçün "kibernetika" terminini işlətmişdi. Müasir tərifl ərə görə, kibernetika canlı orqanizmlər (və onların komponentləri) və texniki qurğular da daxil olmaqla mürəkkəb sistemlərdə idarəetmə və kommunikasiya proseslərini öyrənir [5].

İnternet texnologiyalarının inkişafı ilə "kiber" əsaslı yeni sözlər yaranmağa başladı, bu sözlərdə "kiber" sözü "İnternet və virtual reallığa aid olan" mənasında işlənir. Qeyd edək ki, "kiberfəza" sözü ilk dəfə kanadalı yazıçı-fantast Uilyam Qibson tərəfindən 1982-ci ildə işlədilmişdi və 1984-cü ildə onun «Neuromancer» romanı ilə populyarlaşmışdı.

ISO/IEC 27032:2012 "İnformasiya texnologiyaları – Təhlükəsizlik üsulları – Kibertəhlükəsizlik üçün qaydalar" standartında kibertəhlükəsizlik anlayışı və onun digər anlayışlarla əlaqəsi təsvir olunur [6].



Şək. 1. Kibertəhlükəsizlik ilə digər təhlükəsizlik domenləri arasındakı münasibət [6]

ISO/IEC 27032 strandartında "kibertəhlükəsizlik" və ya "kiberfəzada təhlükəsizlik" kiberfəzada informasiyanın konfidensiallığının, tamlığının və əlyetənliyinin təmin edilməsi kimi müəyyən edilir. Öz növbəsində kiberfəza – qlobal paylanmış qurğular və İKT tətbiq edilməklə insanlar, proqram təminatları və xidmətlər arasında əlaqələri gerçəkləşdirməyə imkan verən, hər hansı fiziki formada mövcud olmayan vahid mühit kimi müəyyən edilir. Qeyd edək ki, "kiberfəza" anlayışını "kibernetik fəza" anlayışına genişləndirmək cəhdi də var [7].

Şəkil 1-ə [6] görə kibercinayətkarlıq nə informasiya təhlükəsizliyinə, nə də kibertəhlükəsizliyə daxil deyil. Kiberəmniyyət də eyni statusdadır, onun mahiyyəti – kiberfəzada təhlükəsiz davranış, ilk növbədə uşaqların İnternetdə neqativ informasiyadan qorunmasıdır.

Kibertəhlükəsizlik əsas tikinti blokları kimi informasiya təhlükəsizliyi, şəbəkə təhlükəsizliyi və İnternet təhlükəsizliyinə söykənir. Kritik informasiya infrastrukturunun təhlükəsizliyi kibertəhlükəsizliklə əlaqəli olsa da, onunla qismən kəsişir. Kibertəhlükəsizlik kritik informasiya infrastrukturunun mühafizəsi üçün zəruridir. Kritik infrastruktur servislərinin adekvat mühafizəsi də (məsələn, kritik infratstrukturun əlyetənliyi) kibertəhlükəsizliyin baza ehtiyaclarına kömək edir.

Kiberfəzanın təhlükəsizliyini təmin etmək üçün qarşılıqlı təsir vacib rol oynayır. Lakin kiberfəzada maraqlı tərəflər arasında yetərsiz kommunikasiya nəticəsində çoxsaylı təhlükəsizlik məsələləri yaranır. Kiberfəzanı dəstəkləyən qurğuların və əlaqədar şəbəkələrin sahibləri müxtəlifdir, onların hər birinin öz maraqları var, istismar və tənzimləmə məsələlərini özünəməxsus şəkildə həll edirlər. İstifadəçilər və provayderlər təhlükəsizliyin təmin edilməsi problemlərinə müxtəlif bucaqlardan baxırlar. Belə fraqmentar yanaşma kiberfəzanın təhlükəsizliyində boşluqlar yaradır, ISO/IEC 27032:2012 standartı belə risqlərin azaldılması üçün maraqlı tərəflərin iştirakına əsaslanaraq birgə həllər təklif edir.

III. MİLLİ KİBERTƏHLÜKƏSİZLİK STRATEGİYALARININ QISA XÜLASƏSİ

İlk milli kibertəhlükəsizlik strategiyaları 2000-ci illərdə meydana çıxmışdır. Kibertəhlükəsizliyi milli strateji məsələ kimi qəbul edən ilk ölkə ABŞ olmuşdu. 2003-cü ildə "Kiberfəzanın təhlükəsizliyi üzrə Milli Strategiya" qəbul edildi. Bu strategiya 11 sentyabr 2011-ci il terror hücumlarından sonra qəbul edilmiş "Milli Təhlükəsizlik üzrə Milli Strategiya"nın tərkib hissəsidir [8].

Sonrakı illərdə Avropada da fəaliyyət planları və strategiyalar qəbul edilməyə başladı. 2005-ci ildə Almaniya "İnformasiya infrastrukturunun mühafizəsi üçün Milli Plan" qəbul etdi. 2007-ci ildə İsveç İnternet təhlükəsizliyinin təkmilləşdirilməsi üçün strategiya işləyib hazırladı. 2007-ci ildə Estoniyanın və 2008-ci ildə Gürcüstanın informasiya infrastrukturlarını iflic edən bir sıra ciddi kiberhücumlardan sonra bir sıra Avropa Birliyi (AB) ölkələri milli kibertəhlükəsizlik strategiyaları işləyib hazırlamağa və qəbul etməyə başladılar. Hazırda 10 AB üzvü milli kibertəhlükəsizlik strategiyası qəbul edib, bir neçə AB üzvü oxşar milli strategiyalar işləyib hazırlamaqdadır [9].

Estoniya 2008-ci ildə geniş milli kibertəhlükəsizlik strategiyası qəbul edən ilk AB ölkəsi oldu. Estoniya təhlükəsiz kibertəhlükəsizliyin zəruriliyini vurğulayır və informasiya sistemlərində cəmləşdirir. Tövsiyə edilən tədbirlərin hamısı mülki xarakterlidir və tənzimləmə, təhsil və əməkdaşlıq üzərində fokuslanır.

Fransa (2011-ci il) informasiya sistemlərinin kiberfəzada verilənlərin əlyetənliyini, tamlığını və konfidensiallığını poza bilən hadisələrə müqavimət göstərmək qabiliyyətinə fikir verir. Fransa informasiya sistemlərinin təhlükəsizliyinə yönəlmiş texniki vasitələr və kibercinayətkarlığa qarşı mübarizə üçün kibermüdafiə sisteminin qurulmasını vurğulayır.

Kanadanın 2010-cu ildə nəşr edilmiş kibertəhlükəsizlik strategiyasında üç istiqamət götürülmüşdür. Birinci istiqamətin məqsədi dövlət sistemlərinin təhlükəsizliyi üzrə aydın rolları və məsuliyyəti müəyyən etmək, federal kibersistemlərin təhlükəsizliyini gücləndirmək və hökümətdə kibertəhlükəsizlik

biliklərini təkmilləşdirməkdir. İkinci istiqamətə federal hökümətə aid olmayan vacib sistemlərin kibertəhlükəsizliyini təmin etmək üçün özəl və kritik infrastruktur sektorları cəlb edilməklə, əyalətlərlə bir sıra tərəfdaşlıq təşəbbüsləri daxildir. Üçüncü istiqamət kibercinayətkarlıqla mübarizəni və Kanada vətəndaşlarının onlayn mühitdə mühafizəsini əhatə edir.

Avstraliya kibertəhlükəsizlik strategiyası İnternetdə təhlükəsizlik üçün zəruri tədbirləri, həmçinin İnternetdə maraqların qorunması sahəsində hökümətin, biznesin və ictimaiyyətin rolunu müəyyən edir.

Birləşmiş Krallığın kibertəhlükəsizlik strategiyasının (2011-ci il) məqsədi ölkəni İKT sahəsində innovasiyalar, investisiyalar və servislərin keyfiyyəti üzrə lider mövqeyinə çıxartmaq və bununla da kiberfəzanın bütün üstünlüklərindən tam şəkildə istifadə etməkdir. Kiberfəzanı vətəndaşlar və iqtisadiyyat üçün təhlükəsiz etmək məqsədi ilə cinayətkarların, terrorçuların və digər dövlətlərin kiberhücumları kimi risqləri istisna etmək nəzərdə tutulur. Birləşmiş Krallığın kibertəhlükəsizlik strategiyasının səciyyəvi cəhəti detallı fəaliyyət planının təklif edilməsidir [10].

Almaniyanın kibertəhlükəsizlik strategiyasında 10 əsas strateji sahə müəyyən edilir – kritik informasiya infrastrukturunun mühafizəsi; Almaniyada informasiya texnologiyaları sistemlərinin təhlükəsizliyi; dövlət təşkilatlarında informasiya texnologiyalarının təhlükəsizliyinin gücləndirilməsi; Milli Kiber-cavablandırma Mərkəzi, Milli Kibertəhlükəsizlik Şurası, kiberfəzada cinayətlərə effektiv nəzarət, Avropada və dünyada kibertəhlükəsizliyin təmin edilməsi üçün əlaqələndirilmiş fəaliyyət, etibarlı və etimad doğuran informasiya texnologiyalarından istifadə, federal idarələrdə kadr hazırlığı, kiberhücumlara cavab alətləri.

IV. MİLLİ KİBERTƏHLÜKƏSİZLİK STRATEGİYALARININ ÜMUMİ CƏHƏTLƏRİ

Beynəlxalq Telekommunikasiya İttifaqının təklif etdiyi milli kibertəhlükəsizlik strategiyasının nümunəvi modelində [11] aşağıdakılar nəzərdə tutulur:

- Milli strategiyanın məqsədləri, miqyası və fərziyyələrinin aydın şəkildə bəyan edilməsi;
- Milli kibertəhlükəsizliyin strateji konteksti – kibertəhdidlər və risqlər;
- Aydın, qısa və əldə edilə bilən kibertəhlükəsizlik hədəfləri;
- Milli kibertəhlükəsizlik prioritetləri;
- Kibertəhlükəsizlik prioritetləri üzrə tədbirlər;
- Zaman bölgüsü və yerinə yetirilmə metrikaları.

Bir qayda olaraq, milli kibertəhlükəsizlik strategiyalarında aşağıdakı mövzulara toxunulur [12].

Təşkilati struktur. Kibertəhlükəsizlik strategiyalarında kibertəhlükəsizliyin təmin edilməsinə yönəlmiş çevik idarəetmə modelinin qurulması nəzərdə tutulur. Ölkələrin bir çoxunda kibertəhlükəsizlik üçün məsuliyyət bir neçə orqanın və müxtəlif qurumlardan ibarət təşkilatların üzərinə düşür. Bu faktor fərqli kibertəhlükəsizlik hədəfləri və koordinasiya rolları olan yeni təşkilatlar yaratmaqla mövcud strukturların yenidən təşkil edilməsini tələb edir.

Normativ hüquqi baza. Bəzi strategiyalarda kiberfəzanın mühafizəsi üçün qanunvericilik bazasının yaradılması zəruriliyi qeyd edilir. Normativ hüquqi bazaya zəruri siyasət və tənzimləmə mexanizmlərinin planlaşdırılması və müəyyən edilməsi, maraqlı tərəflərin rol, hüquq və məsuliyyətlərinin dəqiq müəyyənləşdirilməsi, informasiya təhlükəsizliyinin təmin edilməsinin baza tədbirləri və fəaliyyət təlimatları, yeni maddi-texniki təlimat normaları və s. aid edilir.

Maraqlı tərəflərin əməkdaşlığı. Kibertəhlükəsizlik strategiyalarının reallaşdırılması üçün özəl və dövlət sektoru sıx əməkdaşlıqda işləməlidir. Əməkdaşlıq informasiya və qabaqcıl təcrübə mübadiləsi ilə, dövlət səviyyəsində təlimlər vasitəsilə həyata keçirilməlidir. Dövlət və özəl sektor kimi maraqlı tərəflərə kibertəhlükəsizlik problemləri ilə bağlı siyasətləri müzakirə və təsdiq etməyə imkan verən müvafiq mexanizmlər də müəyyən edilməlidir.

Kibercinayətkarlıq. Kibercinayətkarlıqla beynəlxalq mübarizəyə qoşulmaq üçün dövlətin imkanlarının inkişafı və zəruri qanunvericilik bazasının müəyyən edilməsi nəzərdə tutulur. Bəzi strategiyalarda kibercinayətkarlığa xüsusi fikir verilir (məsələn, Hollandiya, Fransa).

Erkən xəbərdarlıq sistemi. İnsidentlərə hazırlığın yüksəldilməsi, reaksiya vaxtının azaldılması, qəzalardan sonra bərpa planının və kritik informasiya infrastrukturlarının mühafizəsi mexanizmlərinin işlənməsi (məsələn, xüsusi şəraitdə milli fəaliyyət planı, kiberfəzada davranış qaydası, situasiya barəsində məlumatlandırma) nəzərdə tutulur. Bu məsələlər Litvanın milli kibertəhlükəsizlik strategiyasında daha yaxşı əhatə olunur.

Elmi-tədqiqatlar. Həm mövcud, həm də gələcək sistem və servislərin təhlükəsizliyi və dayanıqlığı problemlərinin həllinə yönəlmiş kompleks elmi-praktiki tədqiqatların aparılması zəruridir. Bir sıra strategiyalarda kibertəhlükəsizlik üzrə elmi-tədqiqatlarda aparıcı mərkəzlərin müəyyən edilməsi və geriliyin aradan qaldırılması üçün onlara investisiyaların təmin edilməsi nəzərdə tutulur.

Kadr hazırlığı. IT mütəxəssislərinin və kibertəhlükəsizlik üzrə peşəkarların təhsilinə diqqət ayıran yeni təhsil proqramlarının zəruriliyi göstərilir. İstifadəçilərin vərdişlərini təkmilləşdirən treninqlər də zəruridir. Bəzi milli strategiyalarda kibertəhlükəsizliyin etibarlı təmin edilməsi üçün informasiya təhlükəsizliyi üzrə mütəxəssislərin təhsil proqramlarını təkmilləşdirmək məqsədi qarşıya qoyulur.

Maarifləndirmə. İstifadəçilərə yeni davranış modelləri və iş modelləri aşılamağı nəzərdə tutan maarifləndirmə proqramlarının məqsədləri müəyyən edilir.

Beynəlxalq əməkdaşlıq. Beynəlxalq əməkdaşlıq həyati əhəmiyyət daşıyır, çünki hamı bir kiberfəzadan asılıdır və bir ölkədə olan kibertəhlükəsizlik boşluqları digər ölkələrə təsir edə bilər. Lakin bu strateji sahədə xarici ölkələrlə əməkdaşlıqda iqtisadi, siyasi, və milli təhlükəsizlik risqləri də mövcuddur [13]. Beynəlxalq əməkdaşlıq qanunvericilik tədbirləri, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və

proqram təminatının sertifikatlaşdırılması kimi sahələri əhatə edə bilər.

V. BEYNƏLXALQ KİBERTƏHLÜKƏSİZLİK STRATEGİYALARI

Kibertəhlükəsizlik bir sıra ölkələrdə (məsələn, ABŞ, Avropa Birliyi, Rusiya) xarici siyasətin prioritetlərindən biri elan edilib. ABŞ kibertəhlükəsizliyin azad ticarət və sosial-iqtisadi inkişaf üçün etibarlı, təhlükəsiz və açıq mühit qurmağa imkan verəcək beynəlxalq əsaslarının formalaşdırılması haqqında 2011-ci ildə sənəd hazırlamışdı. Bu sənəddə bir neçə əsas prinsip təsvir edilir.

Birinci yerə iqtisadi əlaqələr qoyulub. ABŞ kommersiya sirri daxil olmaqla bu və ya digər tərəfə məxsus olan informasiyanı qorumaqla İnternet üzərindən azad ticarət imkanı yaratmağı təklif edir. Digər vacib prioritet kiberfəzada beynəlxalq davranış kodeksinin yaradılmasıdır. Layihə müəlliflərinə görə, belə kodeksin varlığı xarici haker hücumlarından qorunmağa imkan verəcək. Daha bir bənd kibercinayətkarlıqla mübarizəyə həsr olunub. ABŞ diqqəti konkret cinayətlərə yönəltməyə və İnternetə girişi məhdudlaşdırmamağa çağırır.

Təhlükəsiz mühit formalaşdırmaq imkanı olmayan ölkələrə yardım göstərilməsi də nəzərdə tutulur. Strategiya ABŞ-ın bütün əsas nazirliklərini əhatə edir, onların hamısına xarici ölkələrdə analoji nazirliklərin iştirakı ilə qarşılıqlı əlaqə prinsiplərini yaratmaq tapşırığı verilib.

Hazırda AB üçün vahid kibertəhlükəsizlik strategiyası yoxdur. 2012-ci ildə Avropa Komissiyası AB üçün "İnternetin təhlükəsizliyi strategiyası"nı işləyib hazırlamışdır. Layihədə əsas risqlər və problemlərlə yanaşı, iqtisadi və geosiyasi imkanları aşkarlamaq, üçüncü ölkələrdə İnternetin təhlükəsizliyi probleminə hazırlıq səviyyəsini müqayisə etmək, həlli tələb edilən vacib problemləri müəyyənləşdirmək, cari və planlaşdırılan tədbirləri qiymətləndirmək məqsədləri qoyulur.

Rusiya Federasiyası milli informasiya sistemlərinin mühafizəsi haqqında BMT Konvensiyasınn layihəsini hazırlamışdır. Layihədə dünya infromasiya fəzasının normal və stabil inkişafına əsas təhdidlər sadalanır. Layihə müəlliflərinə görə, bu təhdidlər informasiya müharibəsinin elementləri hesab oluna bilər və beynəlxalq sülh və təhlükəsizliyə qarşı cinayət kimi tanınmalıdır.

Konvensiya layihəsində kibertəhdidlərlə beynəlxalq səviyyədə mübarizə aparmağa imkan verən normalar sadalanır. Vurğulanır ki, dövlətlər təhlükəsizliyin bölünməzliyi prinsipinə əməl edəcəklər və öz təhlükəsizliklərini digər dövlətlərin təhlükəsizliyinin ziyanına gücləndirməyəcəklər.

Konvensiyaya görə dövlətlər "informasiya fəzasında təhdidlərin artmasına səbəb ola bilən planların işlənməsi və qəbulundan çəkinməli, digər dövlətin daxili səlahiyyətlərinə qarışmaq üçün İKT-dən istifadə etməməli, digər dövlətlərin daxili işlərinə qarışmaq və müdaxiləni həyata keçirmək üçün böhtanlardan, təhqiredici və ya düşmən təbliğatdan çəkinməlidir."

NƏTİCƏ

Ölkələrin kibertəhlükəsizliyə baxışları müxtəlifdir, kibertəhlükəsizliyə informasiya təhlükəsizliyi, milli təhlükəsizlik məsələsi, hüquq-mühafizə məsələsi, iqtisadi məsələ kimi baxışlar mövcuddur.

Bütün ölkələr kibertəhlükəsizlik sahəsində beynəlxalq əməkdaşlığın vacibliyini etiraf etsələr də, ortaq "dilin" və yanaşmanın olmaması beynəlxalq əməkdaşlığı çətinləşdirir. Buna görə ölkələrin kibertəhlükəsizlik termininin ümumi qəbul edilmiş tərifi haqqında razılığa gəlməsi zəruridir.

Kibertəhlükəsizliyin etibarlı təmin edilməsi dövlətin təkbaşına imkanları xaricindədir, bu problemin həlli bütün maraqlı tərəflərin – dövlətin, özəl sektorun və vətəndaşların tərəfdaşlığını və əməkdaşlığını tələb edir. Kibertəhdidlərin transsərhəd xarakteri ölkələri kibertəhlükəsizlik sahəsində sıx əməkdaşlığa sövq edir.

Kibertəhlükəsizlik strategiyasının beynəlxalq cəmiyyətin məqsədlərinə zidd olmadığı, qlobal səviyyədə kibertəhlükəsizlik problemləri ilə mübarizəni dəstəklədiyi də analiz edilməlidir.

ƏDƏBİYYAT

[1] A.K.Sood, R.J.Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," IEEE Security & Privacy, 2013, Vol. 11, No. 1, pp. 54-61.

[2] F. Li, A. Lai, D. Ddl, "Evidence of Advanced Persistent Threat: A case study of malware for political espionage," Proc. of the 6th International Conference on Malicious and Unwanted Software, 2011, pp.102-109.

[3] İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı. 26 sentyabr 2012-ci il.

[4] Luiijf H., Besseling K., Spoelstra M., de Graaf P., "Ten National Cyber Security Strategies: a comparison," Proc. 6th International Conference on Critical Information Infrastructures Security (CRITIS 2011), September 2011.

[5] Г.С. Теслер, Новая кибернетика. – Киев: Логос, 2004. – 401 с.

[6] ISO/IEC 27032:2012 - Information technology - Security techniques - Guidelines for Cybersecurity. 2012, 50 p.

[7] Mitra A., Schwartz R.L., "From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces," Journal of Computer-Mediated Communication's, 2001, Vol. 7, No. 1. http://jcmc.indiana.edu/vol7/issue1/mitra.html

[8] US Government Accountability Office. National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture, GAO-09-432T, 2009.

[9] ENISA: "National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace." May 2012, 15 p.

[10] National Audit Office: The UK cyber security strategy: Landscape review, February 2013, 43 p.

[11] The ITU National Cybersecurity Strategy Guide. Geneva, 2012, 122 p.

[12] OECD: "Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies," OECD Digital Economy Papers, No.212, OECD Publishing. 2012.

[13] Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012, 253 p.