UDK 004.9:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

YENİ NƏSİL MİLLİ KİBERTƏHLÜKƏSİZLİK STRATEGİYALARI

Müasir dövrdə kibertəhlükəsizlik cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir. Kibertəhdidlərə qarşı çevik, operativ və effektli 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.*

Giriş

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. Daim yeni kibertəhdidlərin meydana çıxdığı və təkamül 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-kommunikasiya texnologiyaları (İKT) sürətlə inkişaf edir, kiberhücum metodları və ssenariləri avtomatlaşdırılır və sənayeləşdirilir, kiberhücum alətlərinin qiyməti getdikcə aşağı düşür. Bu səbəblərdən də, kibertəhdidləri real zaman rejimində 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 davam edə bilər. Bir çox hallarda 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 informasiya resurslarına kiberhücumların qarşısını almaqdır.

Hazırda dövlət orqanlarına və özəl şirkətlərə qarşı kiberhücum və kibercasusluq halları sürətlə artmaqdadır. Qarşılıqlı əlaqəli və qarşılıqlı asılı informasiya infrastrukturuna yönələn 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 də 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.

"Kibertəhlükəsizlik" anlayışı

Ölkələrin milli strategiyalarında "kibertəhlükəsizlik" terminінə və digər əsas terminlərə verilən tərifl ər 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.

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

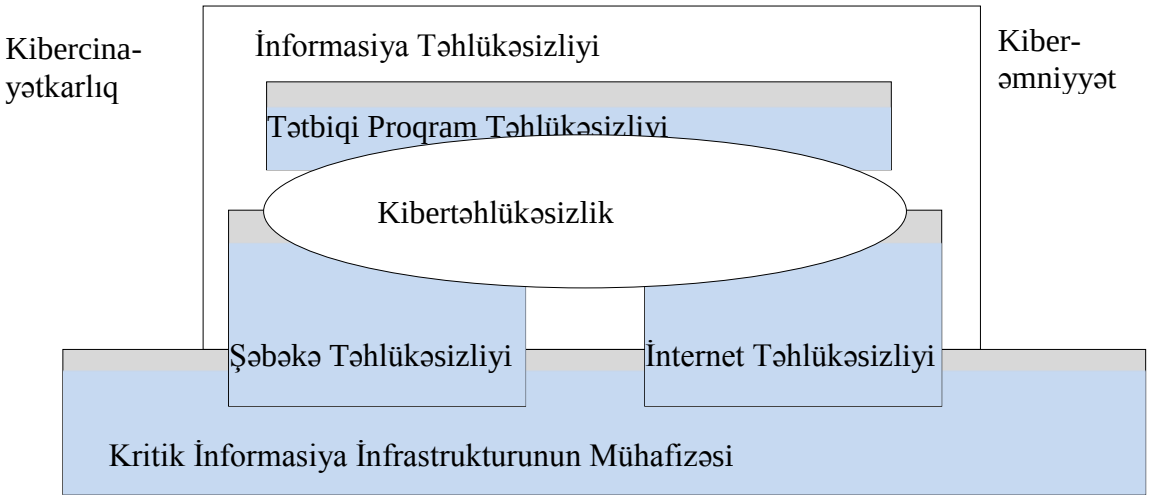
"Kiber" sözü "kibernetika" sözündən törəmədir. "Kibernetika" termini qədim yunan dilində "kibernetes" sözündən yaranıb, mənası sükançı, idarə edən deməkdir. Güman edilir ki, bu termin ilk dəfə qədim yunan filosofu Platon tərəfindən işlədilib. 19-cu əsrdə bu söz A.Amper və ondan sonra bəzi Avropa müəllifləri tərəfindən işlədilmişdir. "Kibernetika" termini 1948-ci ildə amerikan alimi N.Vinerin "Kibernetika" kitabı çap olunduqdan sonra geniş yayılmağa başladı. N.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 U.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].

ISO/IEC 27032 standartında "kibertəhlükəsizlik" və ya "kiberfəzada təhlükəsizlik" kiberfəzada informasiyanın konfidensiallığının, tamlığının və əlyetərliliyinin təmin edilməsi kimi müəyyən edilir. Öz növbəsində, kiberfəza – qlobal paylanmış qurğular və İKT-ni 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 daha geniş olan "kibernetik fəza" anlayışı ilə əvəz etmək cəhdi də var [7].

Şəkil 1-ə 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.



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

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 infrastrukturun əlyetərliliyi) 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 risklərin azaldılması üçün maraqlı tərəflərin iştirakına əsaslanaraq birgə həllər təklif edir.

Milli kibertəhlükəsizlik strategiyalarının qısa xülasəsi

Kibertəhlükəsizliyi milli strateji məsələ kimi qəbul edən ilk ölkə ABŞ-dır. 1998-ci ildə bu ölkədə qəbul edilmiş "Kritik infrastrukturun mühafizəsi" sənədində kritik infrastruktur obyektlərinin, o cümlədən informasiya obyektlərinin təhlükəsizliyi üzrə əsas fəaliyyət istiqamətləri təsbit edilmişdi. ABŞ-da 2001-ci ilin 11 sentyabr tarixində baş verən terror hadisəsindən sonra İnternet təhlükəsizliyi siyasətinin təkrar gözdən keçirilməsi üzrə ətraflı bir layihə həyata keçirildi. Nəticədə 2003-cü ildə "Kiberfəzanın təhlükəsizliyi üzrə Milli Strategiya" qəbul edildi. Bu strategiya həmin terror hadisəsindən sonra qəbul edilmiş "Milli Təhlükəsizlik üzrə Milli Strategiya"nın tərkib hissəsidir [8].

2008-ci ildə ABŞ-in kibertəhlükəsizlik strategiyası təkrar yenilənərək, "Müfəssəl Milli Kibertəhlükəsizlik Təşəbbüsü" (*Comprehensive National Cybersecurity Initiative, CNCI*) adlı strategiya təsdiq edildi. *CNCI* 12 məxfi təşəbbüsdən ibarət idi. Zaman keçdikcə konfranslarda onun bəzi detalları haqqında məlumatlar verildi. *CNCI* bir neçə böyük- miqyaslı dəyişikliyi nəzərdə tuturdu. Birincisi, federal agentliklər və xarici təminatçılar arasında olan şəbəkə bağlantılarının 4 ay ərzində 4000-dən 50-ə qədər azaldılması tələb edilirdi.

İkincisi, federal veb-saytlardan digər veb-saytlara olan İnternet trafikini müşahidə edən *EINSTEIN* adlı proqramın səlahiyyətinin Milli Təhlükəsizlik Agentliyinə (*National Security Agency*) verilməsi idi. Bu proqramın yeni versiyasında isə trafiklə yanaşı, kontentin də

saxlanılması və izlənilməsi federal şəbəkələrlə bərabər, proaktiv olaraq özəl şəbəkələrin də müşahidə edilməsi kimi özəlliklər vardı.

CNCI kibertəhlükəsizlik sahəsində elmi-praktiki işlərə investisiyaların artırılması, kibertəhlükəsizlik üzrə kəşfiyyat çalışmalarının koordinasiya edilməsi və hökumət agentlikləri arasında məlumat paylaşımının təşviq edilməsi kimi mövzuları da əhatə edirdi [9].

2009-cu ilin mayında *CNCI* strategiyası yenidən təftiş edilmiş və *CNCI* təşəbbüsləri haqqında daha geniş şəffaflığın təmin edilməsinin gərəkliyi bildirilmişdi. Hazırlanan hesabatda Ağ Ev tərkibində Kibertəhlükəsizlik İdarəsinin yaradılması tövsiyə edilmişdi. Yaradılacaq bu qurumda bir nəfərin direktor olaraq vəzifə alması, onun Milli Təhlükəsizlik Şurasının üzvü olması və prezidentə asan və sürətli çıxış imtiyazına sahib olmasının lazım olduğu ifadə edilmişdir.

Həmin 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 AB üzvü olan 10 ölkə milli kibertəhlükəsizlik strategiyası qəbul edib, bir neçə AB üzvü isə oxşar milli strategiyalar işləyib hazırlamaqdadır [10].

Estoniya 2008-ci ildə geniş milli kibertəhlükəsizlik strategiyası qəbul etməklə, müvafiq addım atan 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 əks etdirilir.

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

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

Avstraliyanın kibertəhlükəsizlik strategiyası (2009) İnternetdə təhlükəsizlik üçün zəruri tədbirləri, həmçinin İnternetdə maraqların qorunması sahəsində hökumətin, biznes sektorunun və ictimaiyyətin rolunu müəyyən edir.

Birləşmiş Krallığın 2011-ci ilin noyabrından qüvvəyə minmiş kibertəhlükəsizlik strategiyasının 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 riskləri istisna etmək nəzərdə tutulur. Birləşmiş Krallığın kibertəhlükəsizlik strategiyasının səciyyəvi cəhəti detallı fəaliyyət planının təklif edilməsidir [11].

Almaniyada 2011-ci ilin fevralında "Kiberfəzada təhlükəsizlik strategiyası" qəbul edilmiş və Milli Kiber Müdafiə Agentliyi yaradılmışdır. Bu Agentlik polis, kəşfiyyat və İnformasiya Təhlükəsizliyi üzrə Federal İdarə ilə əməkdaşlıq edir. Alman strategiyasında da, amerikan strategiyasında olduğu kimi, məxfi hissə vardır. Güman edilir ki, həmin hissə informasiya hücumlarına qarşı əks-tədbirlərə həsr olunub.

Almaniyanın kibertəhlükəsizlik strategiyasında 10 əsas strateji sahə müəyyən edilir:

1. kritik informasiya infrastrukturunun mühafizəsi;
2. informasiya texnologiyaları sistemlərinin təhlükəsizliyi;
3. dövlət təşkilatlarında informasiya texnologiyalarının təhlükəsizliyinin gücləndirilməsi;
4. Milli Kiber-cavablandırma Mərkəzi;
5. Milli Kibertəhlükəsizlik Şurası;
6. kiberfəzada cinayətlərə effektli nəzarət;
7. Avropada və dünyada kibertəhlükəsizliyin təmin edilməsi üçün əlaqələndirilmiş fəaliyyət;
8. etibarlı və etimad doğuran informasiya texnologiyalarından istifadə;
9. federal idarələrdə kadr hazırlığı;
10. kiberhücumlara cavab alətləri.

Türkiyənin "Milli Kibertəhlükəsizlik Strategiyası və 2013-2014-cü illər üçün Fəaliyyət Planı" 2013-cü ilin iyun ayında təsdiq edilmişdir [12]. Fəaliyyət Planında kiber risqlərin nədən ibarət olduğu xarakterizə olunmuş, təşkilatlararası əməkdaşlıq yolu ilə planlaşdırılan dövrdə aşağıdakı 7 istiqamət üzrə 29 fəaliyyətin həyata keçirilməsi müəyyən edilmişdir:

1. Hüquqi bazanın təkmilləşdirilməsi;
2. Məhkəmə proseslərinə yardımçı olacaq çalışmaların həyata keçirilməsi;
3. Kiber insidentlərin emalı üzrə milli təşkilatın yaradılması;
4. Milli kibertəhlükəsizlik infrastrukturunun gücləndirilməsi;
5. Kibertəhlükəsizlik sahəsində insan resurslarının inkişafı və maarifləndirmə fəaliyyəti;
6. Kibertəhlükəsizlik sahəsində milli texnologiyaların inkişaf etdirilməsi;
7. Milli kibertəhlükəsizlik mexanizmlərinin əhatə dairəsinin genişləndirilməsi (milli təhlükəsizlik sistemi ilə inteqrasiya).

Yaponiya kibertəhlükəsizlik strategiyasının (2010) əsas istiqamətləri mümkün kütləvi kiberhücumlarla mübarizəyə yönəlmiş siyasətlərin gücləndirilməsi, informasiya təhlükəsizliyi sahəsində dəyişikliklərə asanlıqla adaptasiya olunan siyasətlərin həyata keçirilməsi və hücumların qarşısının alınmasına cavabdeh orqanın təsis edilməsidir. Strategiyada aşağıdakı əsas tədbirlər nəzərdə tutulur:

- Cəmiyyət həyatının təhlükəsizliyini təmin etmək üçün İT risqlərinin idarə edilməsi;
- Milli təhlükəsizliyi gücləndirən, kiberfəzada böhranların idarə edilməsini yaxşılaşdıran və sosial-iqtisadi fəaliyyət üçün əsas təşkil edən informasiya-kommunikasiya sistemlərinin istifadəsi siyasətinə zidd olmayan siyasətlərin həyata keçirilməsi;
- Milli təhlükəsizlik, böhranların idarə edilməsi, cəmiyyətin və şəxsiyyətin müdafiəsi problemlərini kompleks əhatə edən üçhissəli siyasətin həyata keçirilməsi. Xüsusilə, cəmiyyətin və şəxsiyyətin informasiya təhlükəsizliyi siyasəti vacibdir;
- İqtisadi artım strategiyasına zidd olmayan informasiya təhlükəsizliyi siyasətinin həyata keçirilməsi;
- Beynəlxalq əməkdaşlığın inkişaf etdirilməsi.

Hindistanda kibertəhlükəsizlik sahəsində strategiya 2013-cü ildə qəbul edilmişdir. Bu strategiyanın əsasında hökumət agentlikləri şəbəkəsi yaradılacaq, əlavə vəsaitlər kibertəhlükəsizlik sahəsində tədqiqat proqramlarına yönəldiləcək.

Milli kibertəhlükəsizlik strategiyalarının ümumi cəhətləri

Beynəlxalq Telekommunikasiya İttifaqının təklif etdiyi milli kibertəhlükəsizlik strategiyasının nümunəvi modelində aşağıdakılar nəzərdə tutulur [13]:

- Milli strategiyanın məqsədləri, miqyası və fərziyyələrinin aydın şəkildə bəyan edilməsi;
- Milli kibertəhlükəsizliyin strateji konteksti – kibertəhdidlər və risklər;
- 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 [14]:

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 siyasəti 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 dayanıqlılığı 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. İT mütəxəssislərinin və kibertəhlükəsizlik üzrə peşəkarların təhsilinə diqqət ayıran yeni təhsil proqramlarının zəruriliyi göstərilir. İstifadəçilərin vərdişlərini təkmilləşdirən treyninqlər 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 riskləri də mövcuddur [15]. Beynəlxalq əməkdaşlıq qanunvericilik tədbirləri, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və proqram təminatının sertifikatlaşdırılması kimi sahələri əhatə edə bilər.

Beynəlxalq kibertəhlükəsizlik strategiyaları

Kibertəhlükəsizlik bir sıra ölkələrdə (məsələn, ABŞ, Avropa Birliyi, Rusiya) xarici siyasətin prioritetlərindən biri elan edilib. ABŞ 2011-ci ildə kibertəhlükəsizliyin azad ticarət və sosial-iqtisadi inkişaf üçün etibarlı, təhlükəsiz və açıq mühit qurmağa imkan verəcək beynəlxalq

əsaslarının formalaşdırılması haqqında 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 hücum-larından 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.

AB 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 "İnternetin təhlükəsizliyi strategiyası"nı işləyib hazırlamışdır. Layihədə əsas risklər 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.

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 [16]. 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" [17] 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 İnternetə 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.

Rusiya Federasiyası milli informasiya sistemlərinin mühafizəsi haqqında BMT Konvensiyasının layihəsini hazırlamışdır. Layihədə dünya informasiya fəzasının normal və stabil inkişafına əsas təhdidlər sadalanır. Bu sənədin müəlliflərinə görə, həmin 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 məsələlərinə qarışmaq üçün İKT-dən istifadə etməməli, digər dövlətlərin daxili işlərinə qarışmaq və müdaxiləni həyata keçirmək üçün böhtanlardan, təhqiredici və ya düşmən təbliğatdan çəkinməlidir.

Nəticə

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 ictimaiyyətin məqsədlərinə zidd olmadığı, qlobal səviyyədə kibertəhlükəsizlik problemləri ilə mübarizəni dəstəklədiyi də analiz edilməlidir.

Ədəbiyyat

1. Sood A.K., Enbody R.J., Targeted cyberattacks: a superset of advanced persistent threats / IEEE Security & Privacy, 2013, Vol. 11, No. 1, pp. 54-61.
2. Li F., Lai A., Ddl D., 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. Теслер Г.С., 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. The Comprehensive National Cybersecurity Initiative, http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf
10. ENISA: National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace, 2012, 15 p.
11. National Audit Office: The UK cyber security strategy: Landscape review, February 2013, 43 p.
12. Ulusal siber güvenlik stratejisi və 2013-2014 eylem planı, 2013, www.resmigazete.gov.tr,.
13. The ITU National cybersecurity strategy guide. Geneva, 2012, 122 p.

14. OECD: Non-governmental perspectives on a new generation of national cybersecurity strategies, OECD Digital Economy Papers, No.212, OECD Publishing. 2012.
15. Klimburg (Ed.), National cyber security framework manual, NATO CCD COE Publication,Tallinn, 2012, 253 p.
16. European Parliament: Report on cyber security and defence, №2012/2096 (INI). 14 p., http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0335&language=EN
17. European Commission: Cyber security strategy of the European Union: An open, safe and secure cyberspace, Brussels, 7.2.2013, 20 p.

УДК 004.9:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Национальные стратегии кибербезопасности нового поколения

На современном этапе кибербезопасность превращается в стратегическую национальную проблему, влияющую на все уровни общества. Гибкая, оперативная и эффективная борьба с киберугрозами требует правильного определения национальных целей и приоритетов, достигаемых за определенный период времени, а также ролей и ответственности заинтересованных сторон. Национальные стратегии кибербезопасности являются первым шагом в этом направлении. С целью выявления наилучших практик в области разработки национальных стратегий кибербезопасности в этой работе анализируются существующие национальные стратегии кибербезопасности.

Ключевые слова: *кибербезопасность, информационная безопасность, информационная война, киберпространство, кибератака, стратегия кибербезопасности.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

Next generation national cyber security strategies

In the modern era cyber security becomes the national strategic issue that affects all levels of society. A flexible, operative and effective struggle against cyber threats requires the national targets and priorities to be achieved within a certain timeline, and the roles and responsibilities of stakeholders to be correctly identified. A national cyber security strategy is the first step on this direction. In this paper, existing national cyber security strategies are analyzed with the aim of identifying the best practices in the development of national cyber security strategies.

Keywords: *cyber security, information security, information warfare, cyber space, cyber attack, cyber security strategy.*