AZƏRBAYCAN RESPUBLİKASI
TƏHSİL NAZİRLİYİ

AZƏRBAYCAN RESPUBLİKASI
RABİTƏ VƏ İNFORMASİYA
TEXNOLOGİYALARI NAZİRLİYİ

ESTONİYA ELEKTRON
İDARƏETMƏ AKADEMİYASI

AZƏRBAYCAN
TEXNİKİ UNİVERSİTETİ

AMEA İNFORMASİYA
TEXNOLOGİYALARI İNSTİTUTU

Republic of Azerbaijan
AKTAM
non-governmental organization

ELEKTRON HÖKUMƏT AZƏRBAYCANDA: NAİLİYYƏTLƏR VƏ PERSPEKTİVLƏR

BEYNƏLXALQ KONFRANSI

MƏRUZƏ MATERİALLARI

Azərbaycan Texniki Universiteti

Bakı, 26-28 aprel 2010

Elektron kommersiya sistemlərinin təşkilati-iqtisadi modelləri

Xülasə. *Material innovasiya iqtisadiyyatının formalaşmasının əsas istiqamətlərdən biri olan elektron kommersiya sistemlərinin təşkilati-iqtisadi modellərinin təhlilinə həsr olunmuşdur. Əsas diqqət biznes-biznes (B2B), biznes – istehlakçı (B2C), istehlakçı - istehlakçı (C2C), biznes – dövlət (B2G), dövlət - biznes (G2B), istehlakçı – dövlət orqanları (C2A), dövlət orqanları - istehlakçı (A2C) və s. kimi modellərin təhlilinə verilmişdir.*

İNFORMASIYA MÜHARIBƏSININ DÖVLƏTIN INFORMASIYA MÜHITINƏ TƏSIRI PROBLEMLƏRI

.Ələkbərova İ.Y, AMEA İTİ.

Today, information war, combining the characters of defense and attack, becomes a strategic project of many nations. For the protection of information space of Azerbaijan from information attacks from the outside, you must first analyze the technologies of information warfare. Trends in the information wars, which are offered in the article help to solve these problems more effectively.

Giriş. Telekommunikasiyaların, müasir informasiya texnologiyaların inkişafı ilə əlaqədar informasiya resursları artır, yeni informasiya münasibətləri, mühitə görə paylanmış yeni məşğulluq formaları yaranır. İndiki şəraitdə cəmiyyətin əsas iqtisadi, siyasi, elmi və mənəvi məhsulu kimi elmi bilik və informasiya resursları hesab edilir [1]. Bu baxımdan müasir dövrdə hakimiyyət və güc pul sahiblərinin yox, informasiya sahiblərinin əlində toplanmaqdadır.

Konseptual səviyyədə hər bir dövlət məqsədini həyata keçirmək, özünü qorumaq, siyasi, iqtisadi və hərbi sahələrdə müvəffəqiyyət əldə etmək üçün vacib olan informasiyanı əldə etməyə çalışır. Əks tərəfin informasiya resurslarını ələ keçirən dövlət üçün bu resurslar və onlardan əldə edilən bilik, öz gücünü artırmaq, bütün sahələrdə rəqibdən üstün olmaq və gələcəkdə onun istənilən sahədə hücumlarına qarşı tab gətirmək, eyni zamanda, öz maddi-mənəvi dəyərlərini qorumaq üçün bir vasitədir.

İnformasiya müharibəsində məqsəd. Terminoloji cəhətdən "informasiya müharibəsi" anlayışı son zamanlar informasiya resurslarının, informasiya kommunikasiya texnologiyalarının (İKT), elektron kütləvi informasiya vasitələrinin sürətli inkişafı ilə əlaqədar geniş istifadə olunmağa başlanmışdır. Bütün bu amillər indiki dövrdə cəmiyyətin elmi-texniki, hərbi, siyasi, iqtisadi, sosial və mənəvi sahələrində nailliyyətlər əldə etməsi üçün yüksək effektli vasitələr sayılır

İnformasiya müharibəsi əks tərəfin informasiyasını və informasiya sistemlərini məhv etməyə və ya ələ keçirməyə yönəlmiş hücumdur. İnformasiya müharibəsini son məqsəd hesab etmək olmaz, o yalnız vasitədir. İnformasiya müharibəsində demoqrafiya, təbliğat, "beyinlərin yuyulması", ictimai rəyin və şüurun manipulyasiyası, veb-briqadalar və s. geniş istifadə edilir.

İlk dəfə Tomas Rona "informasiya müharibəsi" terminini 1976-cı ildə "Boeing" kompaniyası üçün hazırladığı "Silahların sistemi və informasiya müharibəsi" adlandırdığı hesabatında istifadə etmişdir [3]. Öz hesabatında o, göstərmişdir ki, müasir dözrdə informasiya infrastrukturu Amerika iqtisadiyyatının əsas komponentinə çevrilmişdir və dövlətin iqtisdiyyatına təsir edəcək əsas təhlükə informasiya təcavüzüdür. Belə ki, gizli materialların ələ keçirilməsi, araşdırılması və məqsədli istifadəsi iqtisadi, siyasi və hərbi sahədə əsas istiqamətdir.

ABŞ-dan sonra Yaponiyanın, Rusiyanın, Çinin və bir çox Avropa ölkələrinin ictimai və dövlət təşkilatlarında informasiya müharibəsi ilə bağlı araşdırılmalara başlandı [4]. Beləliklə, informasiya proseslərinə təsir göstərən məqsədyönlü, aktiv metod və vasitələrin inkişafına təkan verildi, dövlətlərin informasiya məkanına müdaxilə halları isə kütləvi xarakter aldı [5].

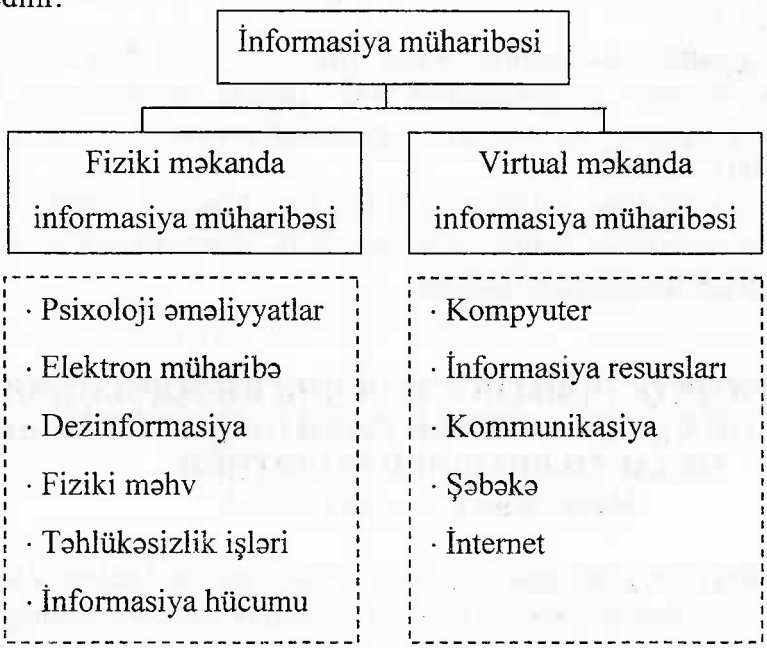
İnformasiya müharibəsinin istiqamətləri. Bu gün dünyada cərəyan edən proseslər hər bir dövlətin ən başlıca vəzifələrindən birinin onun öz informasiya məkanına nəzarət etməsi uğrunda mübarizəsi olduğunu deməyə əsas verir.

Digər mübarizə metodlarından fərqli olaraq informasiya müharibələri daha geniş spektrdə aparılır və onun həyata keçirilməsində müxtəlif vasitələrdən istifadə olunur. Bu vasitələrə kütləvi

ıformasiya vasitələrindən (KİV) başlayaraq qeybətə qədər bütün sahələr aid edilə bilər. ıformasiya müharibəsinin tərkib hissələri kimi: psixoloji əməliyyatlar, elektron informasiya məliyyatları, dezinformasiya və əkstəbliğat üzrə əməliyyatlar, təhlükəsizliyin təmin edilməsi və ıüqaviməti üzrə aparılan tədbirlər, açıq şəkildə olan informasiya hücumları, informasiya :surslarına fiziki təsirlər və digər amilləri göstərmək olar. İnformasiya müharibəsi dünyada hər iki ıəkanı – fiziki və virtual məkanı əhatə edir.

Fiziki məkanda informasiya müharibəsinin əsas istiqamətləri:

1. Psixoloji əməliyyatlar – informasiyadan əks tərəfin hərbi və mülki şəxslərinə təsir üçün istifadə edilir;
2. Elektron müharibə – əks tərəfə dəqiq informasiya əldə etmək imkanı verilmir;
3. Dezinformasiya – əks tərəfə yanlış informasiya ötürülür;
4. Fiziki məhv – informasiya sistemləri və kommunikasiyaların narmal funksiyası pozulur;
5. Təhlükəsizlik işləri – obyektin malik olduğu informasiyanın ələ keçirilməsinin və məhvinin qarşısı alınır;
6. İnformasiya hücumu – əks tərəfin malik olduğu informasiya birbaşa və ya dolayı yolla məhv edilir.



Şəkil. İnformasiya müharibəsinin əsas istiqamətləri

Virtual məkanda informasiya müharibəsinin əsas istiqamətləri:

1. Kompyuterlər – hakerlər və digər kompüter mütəxəssisləri tərəfindən kompyuterlər sıradan çıxarılır;
2. İnformasiya resursları – əks tərəfin sənədləşdirilmiş informasiyaları ələ keçirilir və ya məhv edilir;
3. Kommunikasiya – əks tərəfin informasiya-kommunikasiya sistemlərinin normal iş prinsipi pozulur;
4. Şəbəkə – informasiyanın ötürülməsi və qəbulu əməliyyatlarının normal aparılmasına imkan verilmir;
5. İnternet – müxtəlif İnternet-layihələrdən istifadə etməklə qlobal şəbəkədə müxtəlif təbliğat və dezinformasiya xarakterli məlumatlar yayımlanır.

İnformasiya hücumu vasitələri. İnformasiya müharibəsində əsas istiqamət kimi informasiya ücumu nəzərdə tutulur. İlk dəfə informasiya hücumunu xüsusi informasiya təminatından istifadə dən xakerlər həyata keçirmişlər [5]. İnformasiya hücumu vasitələri aşağıdakılardır:

- əlaqə xətləri ilə ötürülən, proqramlara daxil olmaqla idarə sistemlərini sıradan çıxaran kompyüter virusları;
- məntiqi bomba – hərbi və ya vətəndaş infrostrukturuna əvvəlcədən tətbiq edilmiş xüsusi proqram təminatıdır ki, siqnal və ya təyin edilmiş zamanda həmin proqram işə düşmüş olur;
- telekommunikasiya şəbəkələrində informasiya mübadiləsinin qarşısının alınması vasitələri, dövlət və hərbi idarə kanallarında informasiyanın saxtalaşdılması;
- mətn proqramlarının neytrallaşdırılması vasitələri;
- obyektin proqram təminatlarına düşmən tərəfindən bilərəkdən müxtəlif növ səhvlərin daxil edilməsi.

Nəticə. Müdafiə və eyni zamanda hücum xarakteri daşıyan informasiya müharibəsi bir çox dövlətlərin strateji layihəsinə çevrilməkdədir. Bu dövlətlərdə informasiya müharibəsini texnologiyalarını, informasiya silahını hazırlayan xüsusi strateji-elmi laboratoriyalar, mərkəzlər fəaliyyət göstərirlər.

İnformasiya müharibəsi probleminin obyektiv və tam təhlilini aparmaq üçün xarici mənbələrin analizi və inkişaf etmiş ölkələrin (ABŞ, Rusiya, Avropa ölkələri, Çin və s.) mütəxəssislərinin, alimlərinin, praktiklərinin fikirlərinin müqayisəsi tələb olunur. Azərbaycanın informasiya fəzasının informasiya hücumlarından qorunması üçün ilk növbədə informasiya müharibəsi texnologiyalarının araşdırılması tələb olunur. İnformasiya müharibəsi istiqamətlərinin təyini bu problemin həllinin daha effektli aparılmasına xidmət edir. Azərbaycanın informasiya müharibəsindəki nəaliyyəylərinə görə qabaqcıl ölkələrlə bir sırada olması üçün əsas şərt, bu sahədə mütəxəssislərin hazırlanması və müasir İKT-dən səmərəli istifadədir. Azərbaycanın bu sahədə kifayət qədər kadrlarının olmasını nəzərə alaraq əminliklə deyə bilərik ki, Azərbaycan informasiya müharibəsi layihəsini tam realizə etmək iqtidarındadır.

Ədəbiyyat

1. Алигулиев Р.М., Алиев А.Г. Экономические особенности информационных технологий // Баку, «ЕЛМ», 2002, 56 с.
2. Почепцов Г.Г., Информационные войны // Киев, «Ваклер». 2000, 576 с.
3. Thomas Rona, Weapon Systems and Information War // Boeing Aerospace Co., Seattle, WA,
4. Павлютенкова М. Ю. Информационная война: реальная угроза или современный миф? // Москва, «Власть», 2001, с. 19-23.
5. Denning D.E. Information Warfare and Security // Reading, Mass.etc., 1999.
6. Гриняев С.Н., Информационная война: история, день сегодняшний и перспектива // http://www.agentura.ru/equipment/psih/info/war/.

АРХИТЕКТУРНЫЕ ОСНОВЫ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ВНЕШНЕЙ ПОЛИТИКИ

Набибекова Г.Ч.., ИИТ НАНА

Abstract. This article outlines the goals and objectives of Information Analysis Decision Support System (IA DSS) in the area of foreign policy. Standard architectural and technological scheme of IA DSS is shown. Five-tier architecture of IA DSS in the area of foreign policy is proposed, the tasks that need to be addressed at each level of the system are discussed in detail.

Цели и задачи ИАС ППР. Цели и задачи ИАС ППР в сфере внешней политики заключаются в обеспечении организаций или отделов, работающих в етой сфере, актуальной и значимой информацией, связанной с зарубежными поездками сотрудников организаций госструктур Азербайджана, необходимой для достижения оперативного принятия ефективных решений в области внешней политики страны, для прогнозирования в данной сфере, для выявления тенденций. Многоцелевой характер ИАС ППР – ето возможность решения задачи управления в различных аспектах – управление финансовыми, кадровыми, техническими ресурсами.

На рис.1 приведена стандартная архитектурно-технологическая схема ИАС ППР.

Рис. 1. Архитектурно-технологическая схема ИАС ППР