UOT 004.351

Ələkbərova İ.Y.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
airada.09@gmail.com

İNFORMASİYA MÜHARİBƏSİNİN BƏZİ MODELLƏRİ HAQQINDA

Məqalədə informasiya müharibəsi ilə əlaqədar müəyyən terminlər şərh edilmiş, informasiya müharibəsinin məqsəd və hədəfləri göstərilmişdir. İnformasiya müharibəsində istifadə olunan bəzi modellər analiz olunmuşdur.

Açar sözlər: *informasiya hücumu, kritik infrastruktur, informasiya müharibəsi modeli, psixoloji təsir, kibermüharibə.*

Giriş

İnformasiya cəmiyyətinin (İC) formalaşması, e-dövlət quruculuğunda istifadəsi nəzərdə tutulan layihələrin çoxalması və təkmilləşdirilməsi nəticəsində dövlət strukturlarına aid kompüter şəbəkələrinin və virtual məkanın təhlükəsizliyi məsələləri aktuallaşmışdır. Müxtəlif illərdə İnternet protokolunun universallığından ortaya çıxan imkanlar, veb-texnologiyaların inkişafı və onlardan geniş istifadə nəticəsində real təhlükələr artmışdır. Belə bir şəraitdə dövlətin və cəmiyyətin idarə olunmasında informasiya təhlükəsizliyinin rolu mühüm əhəmiyyət kəsb edir.

Bu gün informasiya resursları, informasiya-kommunikasiya texnologiyaları (İKT) sahəsində biliklər cəmiyyətin əsas iqtisadi, siyasi, elmi və mənəvi məhsulu kimi ön plana çəkilir. Hakimiyyət və güc maliyyə sahiblərinin deyil, informasiya sahiblərinin əlində toplanmaqdadır. Dünyada informasiya resurslarının həddən artıq çoxaldığı bir şəraitdə siyasi və iqtisadi sahələrdə dövlətlərin maraqlarının toqquşması, beynəlxalq münasibətlərdə yeni böhranların yaranması, İKT-dən istifadə etməklə qarşı tərəfin informasiya resurslarının nəzarətdə saxlanması uğrunda mübarizələrin kəskinləşməsi müşahidə olunur.

Dövlətin informasiya resursları tez-tez hücumlara məruz qaldığından hər bir dövlət öz informasiya məkanının təhlükəsizliyini təmin etmək məcburiyyətindədir. Bu baxımdan, informasiya müharibəsi sahəsində əsas tədqiqatlar informasiya müharibəsi texnologiyaları, modelləri, informasiya hücumu metodları və informasiya təhlükəsizliyi ilə bağlıdır. İnformasiya müharibəsinin modelləşdirilməsi dedikdə, iki istiqamət nəzərdə tutulur:

- İnformasiya əməliyyatını araşdırmaq üçün nəzərdə tutulan modellər;
- İnformasiya hücumunu həyata keçirmək üçün nəzərdə tutulan modellər.

Məqalədə müxtəlif informasiya sistemlərinə və insanlara psixoloji təsir etməklə onların davranışlarını idarə etməyə yönəlmiş informasiya hücumunu nəzərdə tutan bəzi modellər araşdırılmışdır. Dövlətin informasiya təhlükəsizliyi məsələlərinin həllində sistemin müxtəlif təyinatlı informasiya hücumlarına qarşı dayanıqlığını təmin etmək üçün informasiya müharibəsi modellərinin öyrənilməsi vacib məsələlərdəndir. İnformasiya müharibəsi modellərinin araşdırılması informasiya müharibəsinin ilkin mərhələlərindən başlayaraq qarşı tərəflərin məqsədini, informasiya əməliyyatlarının xarakterini, informasiya hücumu hədəflərini və dövlətə vurulacaq zərəri müəyyən etməyə imkan verə bilər.

İnformasiya müharibəsində məqsəd və hədəflərin, müharibə metodlarının araşdırılması e-dövlət quruculuğunda və İC-nin inkişafında informasiya təhlükəsizliyi problemlərinin effektiv həlli üçün vacib məsələlərdəndir. Belə ki, kompüter şəbəkələrində informasiya əməliyyatları ilə əlaqədar pozuntuların təyin edilməsində, konkret vəziyyət üçün daha çox ehtimal olunan təhlükələrin təyinində və informasiya təhlükəsizliyi ilə əlaqədar informasiya müharibəsi modellərinin təşkilində mühüm əhəmiyyətə malikdir.

İnformasiya müharibəsi ilə bağlı anlayışlar

İKT-nin inkişafı və informasiyanın rolunun cəmiyyətdə həddən artıq artması nəticəsində informasiya texnologiyaları ilə bağlı tədqiqatlarda "informasiya əməliyyatları" (*information operations*), "informasiya təhlükəsizliyi" (*information security*), "informasiya qarşıdurması" (*information confrontation*), "informasiya hücumu" (*information attack*) və "informasiya müharibəsi" (*information warfare*) terminlərindən daha tez-tez istifadə olunur. İnformasiya texnologiyalarında əsas işin məlumatların toplanması, saxlanması, emalı və ötürülməsi təşkil etsə də, bu gün "informasiya müharibəsi" anlayışını İKT-dən, əsasən də, İnternetdən kənarda təsəvvür etmək mümkün deyil [1].

İnformasiya qarşıdurması tərəflərin xüsusi metodlardan, informasiya resurslarına təsir üsulları və vasitələrindən istifadə etməklə qarşı tərəfin informasiya resurslarının məhvinə və ya nəzarətdə saxlanmasına yönəlmiş informasiya əməliyyatlarıdır [2]. İnformasiya hücumu - icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, həmçinin proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatlardır. İnformasiya müharibəsi isə özündə informasiya hücumu və informasiya qarşıdurması kimi əməliyyatları birləşdirən daha təhlükəli informasiya təsiri formasıdır [3].

İnformasiya müharibəsi qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək, ictimai şüura informasiya təsiri göstərməklə insanların davranışlarını dəyişmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir. İnformasiya müharibəsində informasiya həm silah, həm də məqsəddir [4, 5].

Müasir informasiya müharibəsi texnologiyalarının yaranması, inkişafı və geniş tətbiqinin müxtəlif izahları var [3]:

1. Hesablama texnikası və kommunikasiya vasitələrinın sürətli inkişafı, şəbəkə texnologiyasının təkmilləşdirilməsi cəmiyyətdə əsas resurs kimi informasiyanın rolunun artmasına səbəb olur.
2. Elmi-texniki nailiyyətlər hərbi sahədə istifadə edilən ənənəvi silahlarla yanaşı informasiya müharibəsi üçün nəzərdə tutulan İKT vasitələrinin kütləvi istehsalına və onlardan informasiya təhlükəsizliyinin təmini üçün geniş istifadəsinə şərait yaradır.
3. İnsanların beynlərinin və davranışlarının öyrənilməsində əldə edilən nailiyyətlər insanlara müxtəlif istiqamətlərdə psixo-fizioloji təsirlərin yollarını və vasitələrini daha yaxşı başa düşməyə imkan verir.

"İnformasiya müharibəsi" terminini ilk dəfə, 1976-cı ildə amerikalı mütəxəssis Tomas Rona "Boeing" şirkəti üçün hazırladığı "Silah sistemləri və informasiya müharibəsi" *(Weapon Systems and Information War)* adlı hesabatında istifadə etmişdir. T.Rona hesabatında sübut etmişdir ki, İKT-nin inkişafı dövlətin iqtisadiyyat və hərbi sahələrdə güclənməsinin əsas komponentinə çevrilməsinə səbəb olmuşdur [2].

İnformasiya müharibəsinin ilk tədqiqatçılarından biri, ABŞ-ın Milli Müdafiə Universitetinin əməkdaşı Martin Libiki 1995-ci ildə yazdığı "İnformasiya müharibəsi nədir?" *(What Is Information Warfare?)* məqaləsində informasiya müharibəsi texnologiyalarının təsnifatını vermiş və göstərmişdir ki, son dövrlərdə İKT-nin inkişafı nəticəsində artıq informasiya müharibəsində yalnız psixoloji deyil, həm də iqtisadi və hərbi aspektlərə üstünlük verilir. İnformasiya müharibəsinin mərhələləri aşağıdakılardır [4]:

- Məqsədin müəyyən edilməsi. İnformasiya müharibəsi nə üçün lazımdır və nəticədə nə əldə ediləcək?
- Strategiyanın müəyyən edilməsi. Burada İKT-nin dörd baza komponenti nəzərə alınmalıdır: informasiyanın hazırlanması, informasiyanın yönələcəyi kommunikasiya kanalının təyin edilməsi, informasiyanın təsiri altına düşəcək auditoriyanın

müəyyənləşdirilməsi, informasiya müharibəsi metodunun seçilməsi.

– Taktiki fəaliyyət planının hazırlanması.

1993-cü ildə Stenford Universitetinin professorları Con Arkuilla və Devid Ronfeldt tərəfindən yazılan "Kibermüharibə gəlir!" adlı məqalədə "Şəbəkə müharibəsi" (*Network War*) termini istifadə edilmişdir. Məqalədə müəlliflər kibermüharibə və şəbəkə müharibəsi konsepsiyalarını (*Network Centric Warfare, NCW*) irəli sürməklə müasir dövrdə informasiya müharibəsinin ənənəvi müharibədən daha ciddi problemlər yaratmaq imkanına malik olduğunu göstərmişlər [5].

Konsepsiyada informasiya müharibəsinin əsas məqsədləri kimi aşağıdakılar göstərilir [5]:

1. Öz informasiyasını və informasiya sistemlərini qorumaqla qarşı tərəfin informasiya məkanına nəzarət;
2. Qarşı tərəfin informasiyasını nəzarətdə saxlamaqla informasiya hücumuna başlamaq;
3. Müxtəlif yollarla əldə olunan informasiyadan istifadə etməklə özünün ümumi güc potensialını yüksəltmək;
4. İnformasiya-psixoloji təsir vasitələrindən istifadə etməklə qarşı tərəfə psixoloji təsir etmək.

İnformasiya müharibəsinin fundamental paradiqması və ya dörd strategiyası aşağıdakı informasiya əməliyyatlarından ibarətdir [6, 7]:

1. İnformasiya təqdimatından imtina (*Denial of Information*) (Dağıtma və ya məhv etmə (*Degradation or Destruction*)).
2. Aldatma və imitasiya (*Deception and Mimicry*) (Təhrif (*Corruption*)) – bilərəkdən yanlışlığa yönəldən informasiyanın ötürülməsi əməliyyatı nəzərdə tutulur.
3. Ayırma və məhv etmə (*Disruption and Destruction*) (İmtina (*Denial)) –* daxildən dissfunksiya yaradan və informasiyanın məhvinə yönəlmiş əməliyyat.
4. Təxribat əməliyyatları (*SUBversion*) (İmtina (*Denial)) –* destruktiv prosesə səbəb olan informasiyanın daxil edilməsi əməliyyatı.

Dövlətə qarşı informasiya müharibəsi zamanı müşahidə olunan əsas informasiya əməliyyatları dövlət orqanları, maliyyə sistemləri və sosial əlaqələrin normal fəaliyyətini təmin edən şəbəkələrə qarşı yönəlmiş müxtəlif hücumlardır. Dövlət orqanları, maliyyə sistemləri və s. sahələrə qarşı informasiya hücumu dedikdə, elektron sənədlərin dəyişdirilməsi, məhvi və ya serverlərdəki proqram təminatlarına, verilənlərin saxlandığı texniki qurğulara, ötürücü vasitələrə və şəbəkəyə yönəlmiş informasiya əməliyyatları nəzərdə tutulur [8]. Dövlətə qarşı reallaşdırılan informasiya müharibəsinin əhatə etdiyi sahələr aşağıdakılardır:

– dövlətin maddi rifahını təmin edən kritik infrastruktur;
– iqtisadi sahələr;
– vətəndaşların şəxsi məlumatları: şifrələr, bank hesabları və s;
– İnternet şəbəkəsi.

İnternet istifadəçilərinin sayının sürətlə artması ilə yanaşı, cəmiyyətin siyasi aktivliyi və narahatlığı yeni fəaliyyət sahəsinin – virtual məkanda informasiya hücumlarının və qarşıdurmalarının çoxalmasına səbəb olmuşdur. Belə ki, ictimai rəyin yaradılması və ya dəyişdirilməsində, siyasi, iqtisadi və hərbi qərarların qəbulunda, qarşı tərəfin informasiya resurslarına təsirində, dezinformasiyanın yayılması planında İnternet-texnologiyalar geniş imkanlara malikdir [3, 8].

İnternetdə informasiya qarşıdurması vasitələrinin universallığı, gizliliyi, çoxvariantlılığı, təsirin radikallığı, informasiya təminatında zaman və məkan seçiminin geniş olması onları həddən artıq təhlükəli edir və bu xüsusiyyətlər qlobal şəbəkədə informasiya müharibəsinin gizli aparılması üçün uyğun şərait yaradır.

Dövlətə qarşı informasiya müharibəsində əsas hədəf kimi kritik infrastruktur (*Critical infrastructures*) nəzərdə tutulur. Kritik və ya başqa sözlə, həyati əhəmiyyət kəsb edən

infrastrukturlar dedikdə, dövlətin və vətəndaşların normal fəaliyyətini və rifahını təmin edən əsas sahələr nəzərdə tutulur. Bu infrastrukturların dağıdılması və ya fəaliyyətində pozuntular dövlət strukturlarının və hökumətin işində böyük çətinliklər yarada bilər.

Kritik infrastrukturlara aiddir: informasiya və kommunikasiya (*Information and Communications*), bank və maliyyə (*Banking and Finance*), enerji sahələri (elektrik enerjisi, neft və qaz) və insan kapitalı (*Human Capital*) [9].

İnformasiya müharibəsinin əhatə etdiyi sahələri nəzərə alaraq, deyə bilərik ki, hər bir dövlətdə informasiya müharibəsi idarəetmə və qərarların qəbulu sistemlərinə (*Command & Control Warfare*), kompüter şəbəkələrinə və informasiya sistemlərinə (*Computer Network Attack*) qarşı yönəlmiş informasiya əməliyyatları ilə həyata keçirilir. İdarəetmə və qərarların qəbulu sistemlərinə destruktiv təsir zamanı qərarların qəbulunda iştirak edən məsul şəxslərə və işçi heyətinə qarşı psixoloji əməliyyatlar da (*Psychological Operations, PSYOP*) nəzərə alınmalıdır.

E-dövlətin formalaşması dövlət strukturlarının və vətəndaşların informasiya təhlükəsizliyinin təmin olunmasını tələb edir. E-dövlətə qarşı informasiya müharibəsində aşağıdakı əsas üç istiqamət nəzərə alınmalıdır:

- elektron hücum (*Electronic Attack*);
- elektron müdafiə (*Electronic Protect*);
- elekron müharibəyə dəstək (*Electronic Warfare Support*).

E-dövlətə qarşı informasiya müharibəsində bu istiqamətlərin hər biri üçün ayrılıqda metodlar işlənməlidir: elektron hücum metodları, elektron müdafiə metodları və elekron müharibəyə dəstək metodları.

İnformasiya müharibəsi texnologiyalarına aiddir: elektron müharibə (*Electronic Warfare),* psixoloji müharibə *(Psychological Warfare),* İnternet şəbəkəsində kəşfiyyat müharibəsi (*Information Based Warfare*), haker müharibəsi (*Hacker Warfare*) və kibermüharibə (*Cyberwar*) [4, 8, 9].

Nəzərə almaq lazımdır ki, informasiya müharibəsi iki istiqamətdə aparılır: informasiya-texniki müharibə və informasiya-psixoloji müharibə. İnformasiya-texniki müharibədə müxtəlif növ informasiya sistemlərinə (verilənlər bazası, analitik sistemlər və s.), telekommunikasiya vasitələrinə, kompüter şəbəkəsinə və s. texniki vasitələrə hücum əməliyyatları nəzərdə tutulur. Nəticədə informasiya sistemlərinin ələ keçirilərək nəzarətdə saxlanması və ya məhv edilməsi əməliyyatları həyata keçirilir. İnformasiya-psixoloji müharibədə isə hədəf ayrı-ayrı insanlar, sosial qruplar, təşkilatlar, bir və ya bir neçə dövlətin vətəndaşları, dünya ictimaiyyətidir. İnformasiya hücumu nəticəsində uyğun ideologiyanın təbliği və davranışların idarə edilməsi həyata keçirilir.

İnformasiya-texniki müharibə modelləri

Avstraliyanın Monaş Universitetinin professoru Borden və Amerikanın Aviasiya Universitetinin professoru Kopp tərəfindən işlənmiş Borden-Kopp modeli informasiya müharibəsində istifadə olunan riyazi modellərdəndir. K.Şennonun informasiya nəzəriyyəsinə əsaslanan Borden-Kopp modeli şəbəkə ilə ötürülən informasiyanın miqdarını təyin edir [10]. Model həm də şəbəkədə küylərin yaranmasını və küylü şəbəkədən ötürülən informasiyanın oxunmasını təmin edir. Borden-Kopp modelində küylərdən istifadə etməklə yalnız 4 növ hücum nəzərdə tutulur: deqredasiya (*degrade*), korlamaq (*corrupt*), imtina (*deny*) və istismar (*exploit*). İmtina etmək dedikdə, birbaşa hücumlardan istifadə etməklə informasiyanın qarışdırılması və dağıdılması nəzərdə tutulur. Modeldə informasiya əməliyyatları 4 mərhələdən ibarətdir: informasiya toplanır (*collected*), saxlanılır (stored), situasiya qiymətləndirilir (*situation assessment*) və nəhayət, informasiya dağıdılır (*moved*) [11, 12] (Cədvəl 1).

Valts modeli informasiya təhlükəsizliyinin əsas 3 aspektinə hücumları nəzərdə tutur: konfedensiallıq, tamlıq və əlyetərlik. Model informasiya müharibəsinin əksər istiqamətlərində istifadə olunur: informasiyanın ələ keçirilməsi, korlanması, dəyişdirilməsi və s. [13].

Hatçinson-Uorren modeli qarşı tərəfin informasiyasının məhvinə, oğurlanmasına və dağıdılmasına yönəlmişdir [14]. Model Borden-Kopp və Valts modellərinə oxşardır. Fərq yalnız ondadır ki, Hatçinson-Uorren modeli daha geniş imkanlara malikdir: qarşı tərəfə dəqiq informasiya əldə etmək imkanı verilmir, şəbəkənin normal funksiyası pozulur, qarşı tərəfin malik olduğu informasiya birbaşa və ya dolayı yolla məhv edilir.

Fliger-Fliger modeli informasiyanın ələ keçirilməsi və istismarını nəzərdə tutur. Bu model digər modellərlə müqayisədə daha sadə görünsə də, informasiyanın tamlığı, konfedensiallığı və əlyetərliliyinə qarşı hücum əməliyyatlarını uğurla yerinə yetirə bilir [15].

USAF (US Air Forse) modeli Valts tərəfindən təklif edilmişdir. Digər modellər informasiyanın dəyişdirilməsi və korlanması kateqoriyasına daxil olduqları halda, *USAF* modeli informasiyanın dağıdılması ilə yanaşı, kompromat informasiyanın toplanması məslələrini də həll etmək imkanına malikdir [9].

Cədvəl 1. İnformasiya müharibəsi üzrə bəzi modellərin müqayisəsi

İnformasiya müharibəsi modeli	**İnformasiya əməliyyatları**	**Nəticə**
Borden-Kopp (1999)	Keyfiyyətə təsir Deqradasiya İnformasiyadan imtina	İnformasiya korlanır
Waltz (1998)	Tamlığa təsir Məxfiliyin və əlçatarlığın pozulması	İnformasiya korlanır
Hutchinson- Warren (2001)	İnformasiyanın dəyişdirilməsi İnformasiyadan imtina Manipulyasiya	İnformasiya oğurlanır
Pfleeger- Pfleeger (2003)	İnformasiyanın ötürülməsinə mane olmaq	İnformasiya kəsilir
USAF (1998)	İnformasiyanın dağıdılması İnformasiyadan imtina Aldatmaq	Kompromat informasiya toplanır

İnformasiya-psixoloji müharibə modelləri

İnformasiya müharibəsinin ümumi modeli (*General Information Warfare models*) 2009-cu ildə Ventre tərəfindən təklif olunmuşdur. Ventre bildirir ki, kompüter şəbəkələri və İnternetdə baş verən informasiya müharibələrinin əsas səbəbi dünyada siyasi gərginliyin artmasıdır. Təklif olunan model kiberhücumlar üçün nəzərdə tutulsa da, istənilən insident üçün istifadə oluna bilər. Modeldən dövlətin vacib infrastrukturlarında və şəbəkələrində istifadə etmək mümkündür. Modeldə hədəflərə hücum informasiyanın dəyişdirilməsinə və yeni informasiyanın yaradılmasına əsaslanmışdır ki, bu da, əsasən, vətəndaşlara psixoloji təsir ilə nəticələnir [16].

Məlumatlar axını modeli (*The Message Flow Model*) Koks tərəfindən təklif olunmuşdur və bəzi hallarda "Psixoloji hücum modeli" də adlanır. Model vətəndaşların davranışlarının dəyişdirilməsinə yönəlmişdir. Psixoloji hücum zamanı insanlarda qorxu və gərginlik yaratmağa yönəlmiş model, eyni zamanda, insanların davranışlarına və hadisələrə reaksiyasına görə ötürülən məlumatları qiymətləndirir [17].

Həyat dövrü modeli (*Life Cycle Model*) müxtəlif insidentlərin təsvirini verir və informasiya müharibəsinin müxtəlif formalarına tətbiq oluna bilir. Metodların fərqliliyi, məsələn, psixoloji təsir və ya radioelektron müharibə onun fərqli məsələlərdə tətbiqinə mane olmur [18].

Araşdırmalar göstərir ki, informasiya müharibəsi ilə bağlı problemləri yalnız informasiya sisteminin və ya kompüter şəbəkəsinin təhlükəsizliyini gücləndirməklə həll etmək mümkün deyil. E-dövlət və İC quruculuğunda istənilən informasiya şəbəkəsinin layihələndirilməsini həyata keçirərkən artıq sabah onun informasiya əməliyyatları meydanına çevriləcəyini nəzərə almaq lazımdır.

Nəticə

Tədqiq edilən informasiya müharibəsi modelləri yüksək səviyyəli informasiya əməliyyatları üçün nəzərdə tutuldu üçün onlardan dövlət infrastrukturlarının müdafiəsində də istifadə edilə bilər. İnformasiya müharibəsi hədəfləri ilə kritik infrastruktur eyni deyil və bu səbəbdən informasiya müharibəsi modelinin bütün mümkün ssenarilərdə tətbiqini gözləmək düzgün deyil. Hər bir model, ilk növbədə, müəyyən konseptual səviyyədə, mühitə uyğun insidentlər üçün tətbiq oluna bilər.

İnformasiya hücumlarının qarşısını almaq, informasiya qarşıdurmasında uğur əldə etmək üçün isə, ilk növbədə, informasiya müharibəsi modellərini öyrənmək, onlara qarşı qabaqlayıcı tədbirlər görmək lazımdır. İnformasiya müharibəsinin fundamental modellərinin bəzilərinin analizi və müqayisəsi dövlətdə kritik infrastrukturun müdafiəsində mühüm rol oynaya bilər.

Ədəbiyyat

1. Расторгуев С.П. Математические модели в информационном противоборстве. Москва. Экзистенциальная математика, 2014, 260 с.
2. Rona T. P. Weapon Systems and Information War // Boeing Aerospace Co., 1976, pp. 14.
3. Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyalarının analizi və təsnifatı // İnformasiya cəmiyyəti problemləri, 2010, №2, s. 80–91.
4. Libicki M., What is Information Warfare? // National Defense University. ACIS, 1995, pp. 3
5. Arguilla J., Ronfeldt D., Cyberwar is coming! // Comparative Strategy, 1993, vol. 12, no 2, pp. 141–165.
6. Kopp C. Shannon, Hypergames and Information Warfare // Journal of Information Warfare, 2002, vol. 2, no 2, pp. 108–118.
7. Moteff J., Parfomack P. Critical infrastructure and key assets: Definition and identification. CRS Report for Congress, 2004, http://www.fas.org/ sgp/crs/RL32631.pdf
8. Алекперова И.Я., Comparative analysis of information attacks in Internet // Информационные технологии и компьютерная инженерия, 2010, №3 (19), с. 81–87.
9. Brett N., Manoj S. M. Relevance of information warfare models to critical infrastructure protection // Journal of Military Studies, 2011, vol. 39, no 2, pp. 99–122.
10. Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal, 1948, vol. 27, no 3, pp. 379–423.
11. Poisel R.A. Information Warfare and Electronic Warfare Systems, Boston: Artech House, 2013, 414 p.
12. Kopp C. The four strategies of information warfare and their applications // IO Journal, 2010, vol. 1, no 4, p. 28–33.
13. Waltz K.N. International politics is not foreign policy // Security Studies, 1996, vol. 6, no. 1, p. 54–57
14. Hutchinson W. Warren M. The law and cyber terrorism // Journal of information warfare, 2003, vol. 2, no. 2, pp. 27-32.
15. Pfeeger P.C., Pfleeger S.L. Security in computing, 4rd edition. Upper Saddle River, NJ: Prentice Hall, 2007, 846 p.
16. Ventre D. Information Warfare, Wiley-ISTE, 2009, 320 p.
17. Cox L.V. Planning for psychological operations a proposal. The Research Department. Air Command and Staff College, 1997, 91 p.

18. Brett N., Manoj S.M. The Information Warfare Life Cycle Model // Journal of Information Management, 2011, vol. 13, no 1, pp. 11–20.

УДК 004.351

Алекперова Ирада Я.
Институт Информационных Технологий НАНА, Баку, Азербайджан
airada.09@gmail.com

О некоторых моделях информационной войны

В статье дан обзор определенных терминов, используемых в информационной войне, представлены ее цели и задачи. Проанализированы некоторые модели информационной войны.

Ключевые слова: *информационная атака, критическая инфраструктура, модели информационной войны, психологическое воздействие, кибервойна.*

Irada Y. Alakbarova
Institute of Information Technology of ANAS, Baku, Azerbaijan
airada.09@gmail.com

On some models of the information war

The article provides comments about certain terms in connection with the information war, demostrates the goals and objectives of the information war. some models used in information warfare are analyzed.

Key words: *information attack, critical infrastructure, models of information warfare, psychological effect, cyberwar.*