EKSPRESS-İNFORMASİYA

Azərbaycan Milli Elmlər Akademiyası

İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

İradə Ələkbərova

İNFORMASİYA MÜHARİBƏSİ TEXNOLOGİYALARI

EKSPRESS-İNFORMASİYA

İNFORMASİYA CƏMİYYƏTİ SERİYASI

www.ikt.az

Azərbaycan Milli Elmlər Akademiyası

İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

İradə Ələkbərova

İNFORMASİYA MÜHARİBƏSİ TEXNOLOGİYALARI

EXPRESS – İNFORMASİYA

İNFORMASİYA CƏMİYYƏTİ SERİYASI

Bakı - 2012

Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyaları. Ekspress-informasiya. İnformasiya cəmiyyəti seriyası. Bakı: "İnformasiya texnologiyaları" nəşriyyatı, 2012, 108 səh.

Ekspress-informasiyada informasiya müharibəsi texnologiyaları araşdırılmış, informasiya qarşıdurması və şəbəkə müharibələri problemlərinə baxılmışdır. İnformasiya hücumlarının xüsusiyyətləri və məqsədləri təhlil edilmiş, reallaşdırılması mexanizmləri ilə bağlı təkliflər irəli sürülmüşdür.

AMEA İnformasiya Texnologiyaları İnstitutunun Elmi Şurasının qərarı ilə çapa tövsiyə olunmuşdur.

Elmi redaktor: AMEA İnformasiya Texnologiyaları İnstitutunun şöbə müdiri, f.-r.e.n., dosent Tofiq Kazımov

ISBN: 978-9952-434-31-6

MÜNDƏRİCAT

GİRİŞ

XX əsrin ortalarından başlayaraq informasiya həcminin durmadan artması dünyada paradoksal vəziyyətin yaranmasına səbəb oldu. Həddən artıq informasiyanın yığılması, insanların bu informasiyını toplamaq və emal etmək imkanlarının məhdud olması ilə əlaqədar problemlər yaranmağa başladı. Bütün bunlar yeni informasiya texnologiyalarının yaranmasına və inkişafına tələbi artırdı. İnformasiyanın emalı və ötürülməsi vasitələrinin yaradılması və inkişafı yeni inkişaf prosesinin başlanmasına şərait yaratdı ki, bu proses də öz növbəsində informasiya cəmiyyətinin (İC) yaranmasına və formalaşmasına təkan verdi [1].

Bu gün cəmiyyətin informasiya mühiti köklü şəkildə dəyişmiş, müasir informasiya texnologiyaları praktiki olaraq bütün sahələrə daxil olmuş, insanların informasiya mədəniyyətinin ayrılmaz bir hissəsinə çevrilmişdir. Telekommunikasiyaların, müasir informasiya texnologiyalarının inkişafı ilə əlaqədar informasiya resurslarının artması yeni informasiya münasibətləri, məşğulluq formaları yaratmışdır [2].

İnformasiya-kommunikasiya texnologiyalarının (İKT) inkişaf etdiyi ölkələrdə yeni informasiya texnologiyaları və sistemləri nəinki cəmiyyətin ayrılmaz hissəsinə çevrilmiş, eyni zamanda ayrı-ayrı vətəndaşların gündəlik həyatının bir hissəsi olmuşdur. Bunlara ilk növbədə kütləvi informasiya vasitələrində (KİV) istifadə olunan müasir avadanlıqlar, İnternet və müxtəlif növ radioelektron sistemlər (mobil əlaqə, qlobal yüksəkdəqiqlikli ötürülmə, verilənlərin ötürülməsində istifadə olunan naqilsiz şəbəkə və optik lifli kabel) aiddir. Bir sözlə

informasiya dövrü insanların həyat fəaliyyətlərinin bütün sahələrinə birbaşa və ya dolayısı yolla təsir etməkdədir.

İnkişaf edən İC yeni növ iqtisadiyyatı – ən ali əmtəə forması olan biliyə və informasiyaya əsaslanan iqtisadiyyatı formalaşdırmaqdadır [3, 4]. İC-nin normal fəaliyyəti, bütünlüklə inkişaf səviyyəsindən, funksionallığın keyfiyyətindən və informasiya mühitinin təhlükəsizliyindən asılıdır. Nəzərə almaq lazımdır ki, hər bir dövlətdə baş verən texnoloji nailiyyətlər, bu dövlətin müasir İKT vasitələrindən səmərəli istifadə etdiyini, güclü və dinamik iqtisadiyyata malik olduğunu sübut edən amildir. Bu gün informasiya texnologiyaları sahəsində bilik, informasiya resursları cəmiyyətin əsas iqtisadi, siyasi, elmi və mənəvi məhsulu kimi ön plana çəkilir. Nəticədə, hakimiyyət və güc maliyyə sahiblərinin deyil, informasiya sahiblərinin əlində toplanmaqdadır. İnformasiya qıtlığının aradan qaldırıldığı, dünyada informasiya resurslarının həddən artıq çoxaldığı bir şəraitdə dövlətlərin maraqlarının siyasi və iqtisadi sahələrdə toqquşması, beynəlxalq münasibətlərdə yeni böhranların yaranması, informasiya uğrunda mübarizələrin kəskinləşməsi baş verir.

Son zamanlar bir çox dövlətlər öz vətəndaşlarının və iqtisadi maraqlarının təhlükəsizliyi ilə yanaşı, mədəniyyətlərini, ənənələrini və mənəvi dəyərlərini qorumaq üçün xüsusi tədbirlər görmək məcburiyyətindədirlər. Bu baxımdan dövlətlər konseptual səviyyədə məqsədlərini həyata keçirmək, özlərini qorumaq, siyasi, iqtisadi və hərbi sahələrdə uğur əldə etmək üçün vacib olan informasiyanı əldə etməyə çalışırlar. 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. Odur ki, dövlətin informasiya resursu çox zaman strateji resurs hesab edilir və dövlətin vacib xammal ehtiyatı, enerji, faydalı qazıntılar və s. resurslarına analoji olaraq eyni səviyyədə baxılır [5, 6].

Deyilənlərdən belə nəticəyə gəlmək olar ki, dünyada cərəyan edən proseslər hər bir dövlətin ən başlıca vəzifələrindən birinin, onun öz informasiya məkanına ciddi nəzarət etməyə və informasiya resurslarının təhlükəsizliyini təmin etmək üçün informasiya texnologiyalarından səmərəli istifadə etməyə məcbur edir. *İnformasiya resursları* dedikdə, dövlətlərin informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda, verilənlər bankında və s.) hüquqi və fiziki şəxslərə aid ayrı-ayrı sənədlər və sənədlər toplusu nəzərdə tutulur. Eyni zamanda informasiya resursları kompyuterdə xüsusi təşkil edilmiş, istehsalatda, texnikada, dövlət strukturlarında istifadə olunan informasiyadır. Başqa sözlə, informasiya texnologiyaları vasitəsilə yaradılan və emal edilən informasiyadır. İnformasiya resurslarına informasiya və onun daşıyıcılarından əlavə İKT sahəsində realizə olunan texniki proseslər də aiddir.

İnformasiya texnologiyanın inkişafı ilə əlaqədar informasiyanın daha asan və tez əldə olunması dövlət və cəmiyyətlərin dünyadakı nüfuzunun artması baxımından ideal vasitə hesab olunur [7]. Bu səbəbdən, son zamanlar iqtisadiyyatda, siyasətdə və hərbidə "informasiya əməliyyatı" (information operations), "informasiya təhlükəsizliyi" (information security) və "informasiya müharibəsi"

(information warfare) terminləri geniş istifadə edilir. Müasir dünyada milli informasiya resurslarının mühafizəsi məsələsi çox aktualdır. İnkişaf etmiş dövlətlər tərəfindən informasiya silahının tətbiqi və qlobal informasiya infrastrukturunun yaradılması bu ölkələrin dünyada lider ölkə olmaq məqsədindən irəli gəlir. İnternet qlobal şəbəkəsinin genişlənməsi, kompyuter cinayətkarlığının artması, siyasi və iqtisadi məqsədlərə çatmaq üçün yüksək səviyyədə informasiya hücumları təhlükələrinin çoxalması informasiya müharibəsi (İM) probleminin aktuallığının artmasına səbəb olmuşdur.

Bildiyimiz kimi, idarəetmə sistemlərinin funksiyası əsas etibarı ilə informasiyadan asılı olur, bunun nəticəsində kompyuterin normal işinin hətta nəzərə çarpmayan pozulması idarəetmə sistemlərinə ciddi zərər vura bilər. Lakin əsas təhlükə kompyuterin normal iş rejiminin təsadüfən pozulması ilə deyil, informasiya resurslarına qəsdən və məqsədyönlü təsirlərdən yaranır.

Dünya telekommunikasiya şəbəkəsinin inkişaf etdiyi bir şəraitdə inkişaf etmiş və etməkdə olan ölkələrdə milli informasiya resurslarını qorumaq və informasiya mübadiləsində məxfiliyi saxlamaq üçün tədbirlər görülür. Xarici dövlətlərin təcrübəsi göstərir ki, vətəndaşın şəxsi həyatı ilə bağlı informasiya təhlükəsizliyi mexanizmi yaradılmadan, İM ilə əlaqədar problemlər həll edilmədən dövlətdə normal İC qurmaq mümkün deyil. Artıq aparıcı dövlətlər arasında dünya informasiya fəzası üzərində üstünlük əldə etmək üçün geostrateji informasiya qarşıdurmaları baş verir.

XX əsrin 80-ci illərinə kimi dövlətlərin milli təhlükəsizliyinin təmini məsələləri hərbi və xarici siyasət sahələrində görülən işlərlə müəyyən edilirdi. Lakin müasir

dövrdə insanların təhlükəsizliyini yalnız bunlarla təyin etmək düzgün olmazdı. İndi ölkə və onun vətəndaşları üçün əsas təhlükə iqtisadi, ekoloji, səhiyyə, təhsil, elm və informasiya sahələrindən gözlənilir. Çox zaman dövlətlər arasında baş verən münaqişələrin həllində hərbi silahlardan deyil, tamam fərqli üsullardan istifadə edilir. Bunlara maliyyə axınının kəsilməsi, siyasi təcrid, ticarət əlaqələrinin pozulması, elektrik enerjisinin ötürülməsinin dayandırılması, strateji vacib ehtiyatların (neft, kömür, qaz) eksportuna qadağaların qoyulması və s. aiddir.

Bu üsullardan ən təhlükəlisi isə qarşı tərəfə informasiya təsiridir. Bu gün informasiya təsiri ilə əlaqədar dövlətlərin informasiya təhlükəsizliyinin rolu xeyli artmışdır. Belə ki, dövlətin informasiya təhlükəsizliyi dedikdə, vətəndaşın, cəmiyyətin və dövlətin balanslaşdırılmış milli maraqlarının qorunması nəzərdə tutulur. Müasir cəmiyyətdə informasiyanın rolunun artması 80-ci illərdə dövlətlərin potensialında xüsusi resursların – informasiya resurslarının rolunun vacibliyini bir daha sübut etdi.

İnformasiya dünyada baş verən hadisələrdən asılı olaraq yaranır. Hadisələrin informsiyaya çevrilməsi üçün onlar xüsusi şəkildə şərh edilməli və dərk edilməlidir. Bu baxımdan hadisələrin (faktların) informasiyaya çevrilməsi üçün ilk növbədə onların informasiya daşıyıcılarında saxlanması vacibdir. İnformasiya daşıyıcısı informasiyanı müxtəlif ünvanlara ötürməklə yanaşı, onların emalnda əsas faktorlardan biridir.

Müasir dövrdə informasiya üstünlüyü əldə etmək, yüksək səviyyəli informasiya potensialına sahib olmaq üçün mübarizələrin kəskinləşməsi geosiyasi rəqabətin xarakterini dəyişmişdir. Geosiyasi mühit özündə informasiya mühitini də

əks etdirməklə yeni müstəviyə qədəm qoymuşdur. Təbii resursların azaldığı bir vaxtda informasiya resurslarının artması dünyadakı geosiyasi vəziyyətin dəyişməsinə səbəb olmuşdur. Aydındır ki, dövlətin informasiya resursuna kənardan təsir etməklə bu dövlətin infrastrukturuna təsir etmək mümkündür. Nəticədə, informasiya qarşıdurmasının spesifik xüsusiyyətləri həm hərbi nəzəriyyə, həm də dövlətin informasiya təhlükəsizliyi nəzəriyyəsinin əsaslarının hazırlanması məqsədi ilə bu qarşıdurmanın tərkibinin yenidən öyrənilməsinə tələbat yaratmışdır.

FƏSİL 1. İNFORMASİYA MÜHARİBƏSİ VƏ MÜASİR CƏMİYYƏT

1.1. "İnformasiya müharibəsi" termini haqqında

Son dövrlər İM ilə bağlı terminlərin müxtəlif sahələrdə geniş istifadə olunması və bununla bağlı konkret məsələlərin meydana çıxması yeni müharibə üsullarının reallaşdırılması problemlərini ortaya atdı. Həqiqətən də hər-hansı işi yerinə yetirməyə başlayarkən ilk növbədə istifadə olunacaq "alətin" əldə edilməsi vacibdir. Başqa sözlə, İM sahəsində terminologiyanın təyin olunması problemlərlə daha yaxından tanış olmaqla yanaşı, İM texnologiyalarının araşdırılmasında mühüm əhəmiyyət kəsb edir. Bütün bu deyilənlər "kibermüharibə", "şəbəkə müharibəsi", "informasiya müharibəsi", "informasiya qarşıdurması" və bu sahədə digər istifadə olunan terminlərə aiddir. Deyilənlərin təsdiqi olaraq Sun Szı tərəfindən hələ bizim eradan əvvəl yazılmış "Müharibə incəsənəti" traktatından sitatla tanış olaq: "Qabaqlayıcı bilik elə bir vasitədir ki, onun köməyi ilə məlumatlandırılmış hökmdarlar və müdrük sərkərdələr hücum edərək başqalarını fəth edirdilər... Qabaqlayıcı biliyi şeytandan və ya ruhdan almaq mümkün deyil... onu insanlardan almaq olar, belə ki, bu bilik düşmənin həqiqi vəziyyəti haqqındadır. Casusluğun beş növü var: yerli casuslar, daxili casuslar, ikili casuslar, geri dönməyən və geri dönən casuslar." [8]

Sun Szı öz traktatında casusluğu İM-də əsas istiqamət hesab edərək onun təsnifatını vermişdir: Yerli casuslar – uyğun yerdə yaşayan insanlardır. Daxili casuslar – düşmən dövlətdə vəzifə tutan insanlardır. İkili casusluq – düşmənin casuslarından istifadə etməkdir. Geri dönməyən casuslar – dövlət

sərhədlərindən kənarda dezinformasiyanın yayılmasını həyata keçirənlərdir. Onları yalan məlumatlarla təmin et və qoy onlar bu məlumatları düşmənin agentinə çatdırsınlar. Geri dönən casuslar – lazımi informasiya ilə geri dönənlərdir. Əgər hər beş üsul istifadə olunursa və onun yollarını heç kim bilmirsə, bu "sirli metod" adlanır. İnsan təbiətini nəzərdə tutsaq, o dövrdən bu günümüzə kimi heç nə dəyişməyib. Lakin bu gün informasiya münasibətlərinin instrumental realizəsinin təbiəti dəyişmişdir. Nəticədə, "yerli, daxili və geri dönən" casusların yerini şəbəkə informasiya resursları tutur, "geri dönməyən və dönmüş casusları" isə İnternet və intellektual agentlər əvəz etmişdir.

Tədqiqatlar göstərir ki, indiyə kimi informasiya texnologiyaları sahəsində İM-in ümumi universal anlayışı təyin edilməmişdir. Tarix boyu İM anlayışı təbliğat, təbliğata qarşı mübarizə, dezinformasiya metodları, psixoloji müharibə kimi hadisələrlə əlaqələndirilmişdir. Cəmiyyət inkişaf etdikcə, yeni həyat tərzi yarandıqca, "intellektual iqtisadiyyat" genişləndikcə, İKT inkişaf etdikcə, İC formalaşdıqca İM sosial hadisə kimi əhəmiyyətli dərəcədə avtonomluq statusu almaqdadır.

İlk dəfə "informasiya müharibəsi" terminini, 1976-cı ildə Tomas Rona "Boeing" kompaniyası üçün hazırladığı "Silah sistemləri və informasiya müharibəsi" adlandırdığı hesabatında istifadə etmişdir. Hesabatda o, sübut etmişdir ki, informasiya infrastrukturu Amerika iqtisadiyyatının əsas komponentinə çevrilmişdir [9].

ABŞ-ın Milli Müdafiə Universitetinin əməkdaşı Martin Libiki İM-in nə olduğunu anlatmağa çalışarkən demişdir: "İnformasiya müharibəsini bütün incəliyi ilə anlamaq təşəbbüsü kor adamların fili tanımaq üçün göstərdikləri cəhdləri xatırladır:

filin ayağına toxunan onu ağac, quyruğuna toxunan adam onu kəndir adlandırır və s. Bu üsulla tam təsəvvür almaq mümkündürmü? Ola bilsin ki, fil yoxdur, həqiqətən də ağac və kəndir vardır. Bir qrup mütəxəssislər bu anlayış altında bir çox istiqamətləri birləşdirmək istədikləri halda, digərləri İM-in hərhansı bir aspektini ümumi anlayış kimi qəbul edirlər...". Martin Libiki bu fikri ilə bir daha sübut etdi ki, İM anlayışı tam aydınlaşdırılmasa da bu proses davam etməkdədir [10].

İM-də demoqrafiya, təbliğat, "beyinlərin yuyulması", ictimai rəyin və şüurun manipulyasiyası kimi əməliyyatlardan geniş istifadə edilir. Qeyd etmək lazımdır ki, İM prosesində İnternet şəbəkəsindən istifadə etməklə qarşı tərəfin həyati əhəmiyyət kəsb edən vasitələrini (maliyyə, bank sistemi, rabitə, elektrik təchizatı və nəqliyyat) iflic etmək mümkündür. Bu məqsədlə İnternetdə veb-briqadalar və hakerlər fasiləsiz işləyirlər. Onlar xüsusi təşkil edilmiş, müəyyən hədəflərə yönəldilmiş peşəkarlar qrupudur. İM dezinformasiya, informasiya-kommunikasiya sistemlərinin normal iş fəaliyyətinin pozulması, psixoloji-ideoloji informasiyanın yayılması, informasiya blokadası, enerji təminatının pozulması, şayiələrin yayılması və s. proseslər daxildir.

İnformasiya təhlükəsizliyini təmin etmək üçün ilk növbədə İM-in mahiyyətini və xüsusiyyətlərini öyrənmək lazımdır. *İnformasiya təhlükəsizliyi* məlumatların bütövlüyünü və müxtəlifliyini, gizliliyini təmin edən, onu bütün qəbul edən, bəyənən istehlakçılar üçün anlaşılan, başa düşülən səviyyəyə uyğunlaşmasını təmin edən təşkilati-texniki tədbirlər kompleksidir [11]. Digər tərəfdən informasiya təhlükəsizliyi dedikdə, informasiya sistemi, kompyuter şəbəkəsi və onlara xidmət edən infrastrukturun təbii və ya süni xarakterli, təsadüfi

və ya qəsdli təsirlərdən mühafizəsi nəzərdə tutulur. *İnformasiyanın mühafizəsi* – informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir [12, 13].

ABŞ-ın Müdafiə Nazirliyinin (The Department of Defense) İM haqqında sənədlərində bildirilir ki, İM həm hakimiyyət, həm silah, həm də məqsəddir. ABŞ-ın hərbi dairələrində İM-i təsvir etmək üçün çox zaman onu, informasiya əməliyyatı ilə müqyisə edirlər. *İnformasiya əməliyyatı* – müəyyən məqsədə çatmaq üçün qarşı tərəfin informasiya fəzasına təsir etmək və eyni zamanda öz informasiya resurslarını qorumaq məqsədi ilə xüsusi metod və vasitələrdən (siyasi, iqtisadi, diplomatik, hərbi və s.) istifadəyə əsaslanan mübarizə formasıdır [14]. Rusiya mütəxəssisləri bu mübarizə formasını informasiya qarşıdurması kimi təsvir edirlər. *İnformasiya qarşıdurması* – tərəflərin xüsusi metodlardan, informasiya resurslarına təsir üsulları və vasitələrindən istifadə etməklə qarşı tərəfin informasiya resurslarının məhvinə və ya nəzarətdə saxlanmasına yönəlmiş informasiya əməliyyatıdır [15].

İnformasiya qarşıdurmasının məqsədi qarşı tərəfin şəbəkəyə icazəsiz müdaxilə vaxtını azaltmaqla, dezinformasiya və dezorentasiyanı həyata keçirmək və qarşı tərəfin informasiya da daxil olmaqla, bütün növ resurslarına təsir göstərməkdir. İnformasiya qarşıdurmasının effektivliyinin əsas meyarı kimi qarşı tərəfin informasiya şəbəkəsinə və kommunikasiya texnologiyalarına və nəhayət kompyuterlərinə icazəsiz müdaxilələr nəzərdə tutulur. İnformasiya qarşıdurmasında əsas əməliyyatlardan birini informasiya terrorizmi təşkil edir. *İnformasiya terrorizmi* – qabaqcadan planlaşdırılmış terror aktında informasiya sistemlərindən və kompyuter

şəbəkələrindən istifadə olunmasını nəzərdə tutulan kompleks əməliyyatlardır. Onu da qeyd etmək lazımdır ki, informasiya qarşıdurması və terrorizmi cinayətkar qruplarla, fırıldaqçılıq və zorakılıqla birbaşa bağlıdır.

İM özündə informasiya təcavüzü, qarşıdurması, terrorizmi kimi əməliyyatları birləşdirən daha təhlükəli informasiya təsiri formasıdır. İM bilik uğrunda müharibədir – nə, kim, nə zaman, harada, nə üçün və nə dərəcədə suallarına cavab tapmaq uğrunda müharibədir. İM qarşı tərəfin informasiyasını və informasiya sistemlərini məhv etməyə və ya ələ keçirməyə yönəlmiş hücumdur [16, 17]. Başqa sözlə, *informasiya müharibəsi* – qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir. İM-i son məqsəd hesab etmək olmaz, o yalnız vasitədir.

İM sahəsindəki təcrübələr, vasitələr və metodlar yalnız hərbi-siyasi sahələrdə deyil, dövlətin iqtisadi maraqlarında da geniş istifadə olunur və əsas məqsəd qarşı tərəfin informasiya resurslarının ələ keçirilməsinə, informasiya sistemlərinin məhv edilməsinə yönəlmişdir [18]. Hərbçilərin fikrincə, İM-də ilkin hədəf kimi silahlı qüvvələr, müdafiə müəssisələri kompleksi, ölkənin daxili və xarici təhlükəsizliyinə cavabdeh olan strukturlar nəzrdə tutulur. Ümumiyyətlə isə İM-in əsas hədəfi cəmiyyətin informasiya infrastrukturudur. Hərbi analitiklərin və İKT mütəxəssislərinin gəldiyi qənaətə görə, hazırkı dövrdə İM zamanı bütün informasiya vasitələri və texnologiyalarından istifadə edərək qarşı tərəfin siyasətinə qarşı narazılıq, şübhə,

inamsızlıq yaradılması, ordu və əhali arasında narazılıqların artması həyata keçirilir [19].

İM bəşər tarixinin 7-ci nəsil müharibəsi adlanır. Digər müharibələrdən fərqli olaraq, bu müharibənin sərhədi bilinmir və əsasən virtual xarakter daşıyır. İM-də iştirakçı tərəflərin sayı daha çoxdur və onun vurduğu zərərlər də daha dərindir. Həm də İM zamanı təhlükə hər tərəfdən – proqram vasitələri, texniki qurğular və s.-dən gələ bilər.

İM texnologiyaları inkişaf etdikcə şəbəkə müharibələri (Network War) ilə bağlı problemlər də artmaqdadır. Ümumiyyətlə isə elmi-texniki inkişafa uyğun olaraq, müharibənin metodları və silahları da dəyişməkdədir. "Şəbəkə müharibəsi" termini ilk dəfə 1993-cü ildə Con Arkuilla (John Arquilla) və Devid Ronfeldt (David Ronfeldt) tərəfindən "Kibermüharibə gəlir!" (Cyber War Is Coming!) məqaləsində istifadə edilmişdir. Məqalədə müəlliflər kibermüharibə və şəbəkə müharibəsi konsepsiyalarını (Network Centric Warfare NCW) irəli sürməklə müasir dövrdə İM-in təsəvvür ediləndən daha ciddi problemlər yaratmaq imkanına malik olduğunu göstərmişdilər [20].

Tədqiqatlar göstərir ki, "kibermüharibə", "şəbəkə müharibəsi" və "informasiya müharibəsi" terminləri sinonim deyillər, lakin nəzərə alsaq ki, onların hər biri İnternetlə sıx bağlıdır, demək, bu terminlər arasında ümumi cəhətlər çoxdur. *Kibermüharibə* dedikdə, ilk növbədə kiberfəzada baş verən müharibə nəzərdə tutulur. Digər tərəfdən nəzərə almaq lazımdır ki, bu gün kibermüharibə müxtəlif formalarda – dövlətin milli dəyərlərini əks etdirən domen adların ələ keçirilməsindən, domen mübahisələri ilə bağlı məhkəmələrdən başlamış sosial

şəbəklərdə baş verən qarşıdurmalara, haker hücumlarına kimi bütün istiqamətlərdə həyata keçirilir.

"Kibermüharibə" termininin ilk dəfə Con Akilla və Devid Ronfeldt tərəfindən "Cyber War Is Coming!" məqaləsində istifadə olunmasına baxmayaraq, bu mövzuda geniş araşdırmalara və kütləvi nəşrlərə 1997-ci ildə həmin müəlliflərin "Afina düşərgəsində: informasiya əsrində münaqişələrə hazırlaşarkən" kitabının nəşrindən sonra başlanmışdır [21]. Kitabda göstərilən ideyalar daha sonra onların "Şəbəkələr və şəbəkə müharibələri: terrorun, cinayətlərin və silahlı mübarizələrin gələcəyi" kitabında daha geniş işıqlandırıldı [22].

Kitabda yazılanlardan belə məlum olur ki, müəlliflər "kibermüharibə" və "şəbəkə müharibəsi" anlayışları arasında fərq qoymurlar. Müəlliflər lokal və qlobal münaqişələrə yalnız sosial-siyasi aspektdən baxmaqla kifayətlənirlər. Onların əsas məqsədi "şəbəkə müharibəsi" anlayışına ciddi instrumental təyinat vermək deyil, yalnız şəbəkə müharibəsi zamanı meydana çıxan problemləri işıqlandırmaqdır. Kitabda deyilir: "*Şəbəkə müharibəsi* (netwar) iştirakçıların şəbəkədə təşkilindən, şəbəkə strategiyasından və texnologiyalarından istifadə etdikləri sosial münaqişə formasıdır. Şəbəkə müharibəsi iştirakçıları böyük olmayan quruplar şəklində şəbəkədə yayılmışlar. Bu qruplar şəbəkədə bir-birlərinə təsir göstərməklə, hər-hansı mərkəzləşdirilmiş sistemdən kənar öz hərəkətlərini koordinasiya edir, ünsiyyət saxlayır və birgə tədbirlər həyata keçirirlər. Şəbəkə müharibəsində çox zaman İM iştirakçılarının və şəbəkə cinayətkarlarının (kibercinayətkarların) coğrafi yerini təyin etmək mümkün deyil".

Ötən əsrin 80-ci illərindən başlayaraq kibercinayətkarlığın sayının kəskin artması müşahidə edilməyə başladı. Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik yeni və daha təhlükəli kompyuter viruslarının yaradılması və yayılması üçün yeni imkanlar, yollar açdı. İnternet məkanının genişlənməsi ilə əlaqədar şəbəkə vasitəsilə viruslara yoluxma halları daha da çoxaldı. Kompyuter şəbəkəsindən istifadə etməklə həyata keçirilən informasiya hücumlarının sayının kəskin artması, eləcə də bu hücumların daha təhlükəli şəkil alması İM-ə qarşı şəbəkə cəmiyyətlərinin və formalarının yaranmasına səbəb olmuşdur. Bu səbəbdən qlobal kompyuter şəbəkəsi olan İnternet müasir dövrdə təkcə əlaqə vasitələrini deyil, insanların həyat tərzini, sosial münasibət və siyasi baxışları dəyişməklə İM meydanına çevrilmişdir.

1.2. İnformasiya müharibəsi texnologiyalarının inkişaf mərhələləri

İM texnologiyalarının inkişafını informasiyanın cəmiyyətdəki rolunun artması və hissediləcək dərəcədə hakim mövqe tutması ilə bağlamaq daha düzgün olardı. İM texnologiyaları bu gün cəmiyyətin elmi-texniki, hərbi, siyasi, iqtisadi, sosial və mənəvi sahələrində nailliyyətlər əldə etmək üçün yüksək effektli vasitələrdən sayılır [23].

İM və onun tətbiqi texnologiyalarının kökü qədim dövrlərə təsadüf edir. İnsanlar yaşadıqca İM və informasiya təcavüzü bu və ya digər formada hər zaman mövcud olmuşdur. Ən qədim tarixi və dini kitablarda təsvir edilən hadisələr insanlar arasında informasiya qarşıdurmaları və təcavüzlərinin üzərində qurulmuşdur. Məsələn, Çingiz xanın yürüşləri zamanı ordunun önündə xüsusi hazırlıq görmüş müəyyən qrup atlılar çapırdılar. Onlar Çingiz xanın opdusunun hədsiz dərəcədə güclü və

amansız əsgərlərdən təşkil olunduğu haqqında xəbərlər verərək əhalidə qorxu, ruh düşkünlüyü yaradırdılar. Bu cür psixoloji təsir üsulları digər məşhur sərkərdələr tərəfindən də istifadə edilmişdir (Makedoniyalı İsgəndər, Teymur Ləng və s.).

Fiziki müharibə etmədən İM aparmaq olur, amma İM olmadan fiziki müharibə aparılmır. Başqa sözlə, fiziki müharibə aparılarkən, eyni zamanda onun tərkib hissəsi kimi İM-in aparılması zəruridir. Hələ çox qədimlərdən müharibələr zamanı hərbçilər vuruşda güclərini effektiv idarə etmək üçün qarşı tərəfin informasiya mənbəyinə təsir etməyə, insanların fikrini lazım olan istiqamətə yönəltməyə çalışmışlar.

II Dünya müharibəsi zamanı Adolf Hitler və Stalin də informasiya-psixoloji təsirin əhəmiyyətini yaxşı anlayırdılar. Ötən əsrin 40-cı illərində informasiya texnologiyalarının inkişafı öz ilkin dövrünü yaşayırdı. Bu səbəbdən İM-də təbliğat və dezinformasiyadan istifadə daha effektli vasitə sayılırdı. İM-də üstünlüyü əldə saxlamaq məqsədi ilə Alman ordusunda xüsusi təbliğat qoşunu yaradılmışdı. Təbliğat qoşununun təşkilinə qərar 1938-ci ildə Qebbelsin təklifi ilə verildi. Təbliğat qoşununa hərbi jurnalistlər, foto-, kino- və radiomüxbirlər, radioavtomobillərə və kinoqurğulara xidmət edən heyət, təbliğat xarakterli ədəbiyyatın (vərəqə, plakat və s.) yaradılması və yayılmasında iştirak edən mütəxəssislər daxil idi. Təbliğat və dezinformasiya yalnız düşmən tərəf üçün deyil, eyni zamanda daxili qoşun və əhali üçün də nəzərdə tutulmuşdu.

II Dünya müharibəsinin ilk dövrləri göstərdi ki, informasiya təbliğatında çap edilmiş vərəqələrdən istifadə digər çap məhsulları (qəzet, jurnal, kitabça) ilə müqayisədə daha çox üstünlüyə malikdir. Təbliğat xarakterli vərəqələr daha operativ

idi və baş verən hadisələrə daha tez uyğunlaşdırılaraq qısa və oxunaqlı mətnə malik idilər. Eyni zamanda ölçülərinin kiçik olduğu üçün onları çap edib yaymaq, gizlətmək, başqalarına ötürmək də asan idi [24].

Tarix göstərir ki, müharibələr zamanı informasiya təbliğatı müxtəlif manevrlər və yayındırıcı hərəkətlərin köməyi ilə edilirdi. Bu zaman qarşı tərəfə yanlış informasiyanı ötürərək üstünlüyü ələ keçirmək üçün aşağıdakı şərtlər yerinə yetirilməli idi [25]:

- qarşı tərəfin hərəkətlərinin müşahidə edilməsi;
- yalanın həqiqət kimi qəbul edilməsi;
- ötürülmüş yanlış informasiyalardan istifdə etməklə nəzərdə tutulan əməliyyatların yerinə yetirilməsi.

Keçən əsrin ortalarına kimi həyata keçirilən informasiya əməliyyatlarının indiki informasiya əməliyyatlarından yeganə fərqi ondan ibarət idi ki, əvvəllər informasiya əməliyyatlarına hərbi əməliyyatların bir hissəsi kimi baxılmırdı. Bu da qədim dövrlərdə informasiyanın ötürülməsində istifadə olunan vasitələrin primitiv olması, informasiya təhlükəsizliyi baxımından texnologiyaların tələbatı tam ödəməməsi ilə izah olunurdu.

Müasir dövrdə informasiyanın emalı və ötürülməsində istifadə edilən maddi-texniki bazanın inkişafı ilə İM-in tətbiqi və texnologiyaları köklü şəkildə dəyişmiş, informasiya şəbəkəsinin yaranması və geniş yayılması, informasiyanın ötürülmə sürətinin min dəfələrlə artması İM-in əhəmiyyətini artırmışdır.

İqtisadi cəhətdən inkişaf etmiş ölkələrdə İKT-nin inkişaf tempinin daha da yüksək olması milli təhlükəsizlik sistemində İM-in rolunun vacibliyini bir daha sübut edir. Digər tərəfdən,

İM-in rolunun artması nəinki ayrı-ayrı dövlətlərin milli və hərbi təhlükəsizliyinin, eyni zamanda beynəlxalq təhlükəsizliyin təmin edilməsi məsələlərinin vacibliyini təsdiq edir. İnformasiya axınları üçün sərhədlərin şəffaflığı dövlət hakimiyyət institutlarının funksialarında prinsipial olaraq başqa bir situasiya yaradır. İnformasiya sistemlərinin dövlətlərin infrastrukturuna (bank-maliyyə, nəqliyyat, elekrtik şəbəkələri, neft və qaz xətləri) tətbiq edilməsi isə onları İM-də potensial obyektlərə çevirməkdədir. Belə bir şəraitdə praktiki olaraq informasiya fəzası mənsub olduğu ölkə tərəfindən idarə oluna bilmirsə, bu ölkənin suverenliyində məhdudiyyətlər yarana bilər və hətta ölkənin gələcəkdə müstəqil fəaliyyəti sual altına alınmış olar.

İM və informasiya təhlükəsizliyi məsələləri ilə məşğul olan alimləri üç qrupa bölmək olar:

- Birinci qrup alimlər İM ilə bağlı əməliyyatları ayrı-ayrı informasiya tədbirlərinə, informasiya rəqabəti vasitələrinə, dövlətlərarası münaqişə və silahlı mübarizələrin aparılmasına, kütləvi şüura təsir texnologiyalarna uyğunlaşdırırlar (sosial-kommumikativ yanaşma) [26, 27, 28, 29, 30, 31, 32].
- İkinci qrup alimlərə hərbi mütəxəssislər aiddir ki, onların fikrincə, İM hərbi münaqişələrlə birbaşa bağlıdır və bu münaqişələrə informasiya-hərbi mübarizə vasitələrinin və gücün kompleks birgə tətbiqi kimi baxılmalıdır (hərbi-tətbiqi yanaşma) [33, 34, 35, 36]. Lakin bir qisim alimlər bu yanaşma ilə razılaşmır və bildirirlər ki, "informasiya müharibəsi" ifadəsi hərbi əməliyyatların aparılması zamanı müasir informasiya texnologiyalarına münasibətdə hər zaman uyğun olmur və bu növ hərbi

əməliyyatları informasiya mübarizəsi adlandırmaq daha düzgün olardı [37, 38, 39].
- Üçüncü qrup tədqiqatçılar İM dövlətlərarası münaqişələrdən yaranan hadisə kimi baxırlar. Onların fikrincə, dövlətlər arasında yaranan siyasi münaqişələri hərbi yolla deyil, müasir İKT vasitələrindən istifadə etməklə həll etməyə çalışırlar. Bu baxımdan bir çox tanınmış alimlər İM-i geosiyasi münaqişəyə aid edərək ona dövlətlər arasında xüsusi münasibət növü kimi baxırlar. Bu halda mövcud olan münaqişəni aradan qaldırmaq üçün bu ölkənin informasiya mühitinə güc təsirlərinin müxtəlif metod, vasitə və texnologiyalarından istifadə olunur (geosiyasi yanaşma) [40, 41]. Bu qrup mütəxəssislər İM zamanı əməliyyatların zorakılıq xarakterini qabardaraq onu açıq hərbi münaqişənin aparılmadığı şəraitdə müharibənin ən vacib əlaməti hesab edirlər.

Bu gün İM problemləri İKT-nin inkişaf etdiyi bir çox ölkələrdə (ABŞ, Rusiya, İngiltərə, Fransa, İsveçrə, Yaponiya və s.) araşdırılmaqdadır. Bu ölkələrdə dövlətin informasiya infrastrukturunun kompleks müdafiəsi konsepsiyasının həyata keçirilməsi aktiv yerinə yetirilir.

Müasir İM texnologiyalarının yaranmasının müxtəlif izahları var:

1. İnformasiya texnologiyalarının, kommunikasiyanın sürətli inkişafı cəmiyyətdə əsas resurs kimi informasiyanın rolunun artmasına səbəb oldu. Effektivliyinə görə informasiya maddi resurslardan daha yuxarıda dayandı. Elmi texniki nəaliyyətlər İM-də istifadə edilən ənənəvi silahlarla yanaşı, gələcək müharibələrdə istifadəsi nəzərdə

tutulan istər insanlar, istərsə də bütün təbiət üçün çox böyük təhlükə yarada biləcək yeni-yeni fiziki-kimyəvi silahların kəşfinə şərait yaratdı [28].

2. İnsanların beyninin və davranışlarının öyrənilməsində əldə edilən nəaliyyətlər onlara müxtəlif istiqamətlərdən göstərilən psixofizioloji təsirlərin yollarını və vasitələrini daha yaxşı başa düşməyə imkan verdi.

Dünyada İKT-nin inkişafı və dövlətlər arasında baş verən hərbi və siyasi qarşıdurmalar belə söyləməyə əsas verir ki, yaxın gələcəkdə rəqib üzərində üstünlük informasiyanın ələ keçirilməsi, informasiya təsirinə tez reaksiya verilməsi, real zaman rejimində qarşı tərəfin informasiya mənbələrinin məhv edilməsi ilə əldə olunacaqdır.

İM sahəsində qabaqcıl mütəxəssislərdən biri kimi tanınan Martin Libiki hesab edir ki, gələcəkdə İM texnologiyaları, informasiya, informasiya sistemləri hərbi münaqişələrin gedişatında və sona çatmasında da əsas vasitələrdən olacaqdır.

Onun ilk dəfə 1995-ci ildə ABŞ-ın Milli Müdafiə Universiteti (National Defense University) tərəfindən nəşr edilmiş "İnformasiya müharibəsi nədir?" məqaləsində İM anlayışı tam açıqlanmır. Məqalədə təsvir edilən və "Information Warfare" adlanan sxemdə Libiki İM-in formalarını və onlar arasındakı əlaqələri göstərir [42].

Libikinin "Information Warfare" sxemi ABŞ Hərbi Hava Qüvvələri Universitetinin (Air University, Maxwell Airforce Base, Alabama) mütəxəssislərinin təklif etdikləri konsepsiya ilə kəsişsə də hər iki baxışda ümumi bir fikir vardır ki, İM-də psixoloji deyil, iqtisadi və hərbi aspektlərə üstünlük verilir. Libikinin fikrincə, gələcəkdə izləyici kosmik peyk şəbəkəsində yerləşdirilən torpaq üzərində, dəniz və havada baş verən

dəyişiklikləri qeyd edən vasitələrdən ibarət əlaqəli informasiya sistemləri dünyada baş verən istənilən hərbi aktivliyi nəzarətdə saxlamaq imkanına malik olacaqdır. Eyni zamanda bu sistemlərin köməyi ilə hərbi aktivliyi iflic etmək, qarşı tərəfin iqtisadi və informasiya sistemlərini dünyadakı digər sistemlərdən ayırmaq mümkün olacaqdır. Libiki bildirir ki, İM texnologiyalarının kosmik vasitələrlə birgə istifadəsi informasiya əməliyyatlarının effektivliyinin dəfələrlə artırılmasına şətait yaradır. Hal-hazırda ABŞ-ın Milli Təhlükəsizlik Agentliyi tərəfindən yaradılmış "Eşalon" qlobal sistemi radioelektron kəşfiyyat kosmik aparatlar orbital qrupunda yerləşdirilmişdir. Pentaqonun "Gələcəyin hərbi sistemləri" layihəsi 2010-cu ilə qədər ABŞ-ın silahlı qüvvələrinin istənilən qarşı tərəf üzərində tam informasiya üstünlüyünün əldə edilməsinə yönəlmişdir. İnternet istifadəçilərinin sürətli artımı bu layihənin həyata keçməsinə şərait yaradan əsas amillərdən biridir.

Martin Libiki "İnformasiya müharibəsi nədir?" məqaləsində İM-in yeddi formasını göstərmişdir:

1. *Komanda nəzarət (Command and control)* – komandanlıq və icraçılar arasındakı əlaqə kanallarına istiqamətlənmiş İM-dir. Aydındır ki, informasiya hücumu nəticəsində qarşı tərəfin əlaqə kanallarının funksiyası pozularsa İM-də qələbənin təmin olunması reallaşar.

2. *Kəşfiyyat müharibəsi (Information Based Warfare)* – mühüm informasiyanın toplanması və eyni zamanda özünə məxsus informasiyasının mühafizəsi prosesidir.

3. *Elektron müharibə (Electronic War)* – elektron kommunikasiya vasitələrinə qarşı yönəlmiş müharibədir. Elektron kommunikasiya vasitələri dedikdə, radioəlaqə, radar

qurğular, kompyuter şəbəkələri nəzərdə tutulur. Elektron müharibənin əsas bölməsi kriptoqrafiyadır (elektron informasiyanın şifrələnməsi və ya şifrənin açılması).

4. *Psixoloji müharibə (Psychological War)* – təbliğat, "beyinlərin yuyulması", əhalinin davranışlarına nəzarət və vətəndaşlar üçün nəzərdə tutulmuş informasiyanın emalıdır.

Libiki psixoloji müharibəni 4 hissəyə ayırır:

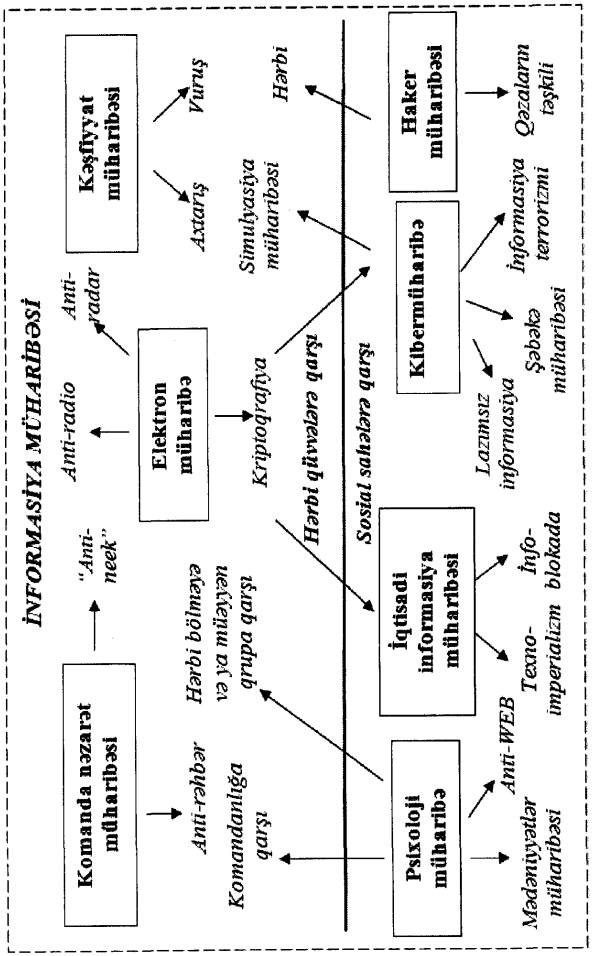
- Vətəndaşların mənəvi durumuna təsir;
- Hərbi qüvvələrdə mənəvi duruma və əhval-ruhiyyəyə nəzarət;
- Komandanlığın bilərəkdən səhv istiqamətləndirilməsi (Disorientation Command);
- Mədəniyyətlər mübarizəsi (Kulturkampf).

5. *Haker müharibəsi (Hacker War)* – qarşı tərəfin vətəndaşlarına, sosial sahələrə yönəlmiş diversiya əməliyyatlarıdır. Libiki haker fəaliyyətlərindən danışarkən onların törətdiyi fəsadları belə sadalayır: şəbəkənin total iflici, informasiya əlaqələrində fasilələr, verilənlərin ötürülməsi zamanı təsadüfi səhvlərin çoxalması, informasiyanın oğurlanması, informasiya xidmətlərinin oğurlanması (şəbəkəyə icazəsiz müdaxilə), şəbəkənin gizli monitorinqinin aparılması, şantaj məqsədi ilə gizli verilənlərin icazəsiz ələ keçirilməsi. Libikiyə görə hakerlərin silahı viruslardır – "troyan atları", məntiqi bombalar, sniferlər (izləyiçilər), şəbəkə soxulcanları və s. Libiki hakerləri ABŞ üçün ciddi təhlükə hesab edir və bunu da onunla izah edir ki, Amerika digər ölkələrlə müqayisədə şəbəkədən daha çox istifadə edir. Libiki birmənalı olmayaraq göstərir ki, ABŞ-da kompyuterlə bağlı elmlər üzrə Amerika universitetlərində müdafiə edən doktorantların 60%-ni

əcnəbilər təşkil edir ki, onların da 2/3 hissəsi müsəlman ölkələrindən və Hindistandan gələnlərdir.

6. *İqtisadi informasiya müharibəsi (Economic Info-Warfare)* – Libiki bu müharibəni iki formada təsvir edir: İnformasiya blokadası (ABŞ-a qarşı yönəlmiş) və informasiya imperiolizmi (ABŞ tərəfindən). İnformasiya blokadası dedikdə, ilk növbədə informasiya və ticarət əlaqələrinin kəsilməsi (fiziki ticarətə qadağanın qoyulması) nəzərdə tutulur. Bank şəbəkələrinin sındırılması bu kateqoriyaya daxil deyil və haker fəaliyyəti hesab olunur. İmperializm müharibəsi ümumi iqtisadi imperializm siyasətinin bir hissəsidir. Libiki bildirir ki, "ticarət özü də müharibədir".

7. *Kibernetik müharibə və ya kibermüharibə (Cyberwar)* fəaliyyətini analiz edərkən Libiki onları adi haker müharibələrindən fərqləndirir. Onun fikrincə, əgər nəzərə alsaq ki, terrorizm ayrı-ayrı insanlara və ya qruplara qarşı müharibədir, o zaman informasiya terrorizmi İM-in bir istiqaməti kimi, ilk növbədə kibercinayətkarlıq və ya şantaj üçün bir vasitədir. Libiki semantik hücumları təhlil edərkən onları haker müharibələrindən tam fərqləndirir və bildirir ki, əgər haker informasiya hücumu zamanı sistemi qeyri-düzgün işləməyə məcbur edirsə, semantik hücum zamanı kompyuter sisteminin fiziki göstəricilərinə təsir edilir və bu zaman semantik hücum vasitələri kompyuterin hər hansı bir hissəsinə nəzarət edən obyektə yönəlmiş olur. Sistemin fiziki göstəricilərini və ya digər giriş vasitələrini "aldatmaq", sistemdə heç nəyə toxunmadan və sistemə texniki zərər vurmadan bu sistemi sıradan çıxarmaq semantik hücumun əsas məqsədidir.



Şəkil 1. Martin Libiki tərəfindən təqdim edilən "İnformasiya müharibəsi" sxemi

Kibermüharibənin bir növü də simulyasiya müharibəsidir. *Simulyasiya müharibəsi* – real döyüş meydanında baş verə bilən hərbi əməliyyatların kompyuter modeli ilə əvəz olunmasıdır. Məsələn, təyyarəçilər kompyuterdə xüsusi oyun proqramlardan istifadə etməklə səmaya qalxmadan vuruş təçrübəsi əldə edirlər. Simulyasiya müharibəsi, əsasən nümayiş effekti yaradır və dünyanın virtuallaşmasının əyani nümunəsidir. Dünyanın virtuallaşması, daha doğrusu, dünyanın kompyuter versiyasının yaradılması ona gətirib çıxaracaq ki, gələcəkdə simulyasiya müharibəsi real müharibə ilə eyni məna kəsb edəcək və bir statusda olacaqdır.

Libikinin "İnformasiya müharibəsi nədir?" məqaləsində İM-in əsas məqsədi kimi aşağıdakılar göstərilir:

1. Öz informasiyasını və informasiya sistemlərini qorumaqla qarşı tərəfin informasiya məkanına nəzarət;
2. Qarşı tərəfin informasiyasını nəzarətdə saxlamaqla informasiya hücumuna başlamaq (İM texnologiyalarından istifadə etməklə qarşı tərəfin iqtisadiyyatını ələ keçirmək və ya məhv etmək);
3. İnformasiyadan istifadə etməklə özünün ümumi güc potensialını yüksəltmək;
4. İnformasiya-psixoloji təsir vasitələrindən istifadə etməklə qarşı tərəfə psixoloji təsir.

FƏSİL 2. İNFORMASİYA MÜHARİBƏSİ TEXNOLOGİYALARININ XÜSUSİYYƏTLƏRİ

2.1. İnformasiya müharibəsi texnologiyalarının tətbiqində məqsəd və hədəflər

İM zamanı maraq obyektləri insanların psixoloji durumu ilə yanaşı, informasiya sistemləri və kompyuter şəbəkəsi olur. Kompyuter şəbəkəsinə müxtəlif sahələr üzrə verilənlər bazasının idarəetmə sistemlərini emal edən uyğun ötürmə xətləri, İM-də iştirak edən İKT vasitələri də aid edilir.

Aydındır ki, İM təhlükəsinin get-gedə artdığı şəraitdə kompyuter şəbəkələri ilk növbədə informasiya hücumlarına tab gətirmək imkanına malik olmalıdır. Yəni həm şəbəkələr, həm də bu şəbəkələrlə əlaqədar fəaliyyət göstərən informasiya sistemləri qarşı tərəfin informasiya təsirinə adekvant reaksiya göstərərək qarşı tərəf üzərində üstünlük əldə etmək məqsədi ilə informasiya qarşıdurmasında müəyyən məsələləri həll etmək qabiliyyətinə malik olmalıdırlar. Bu isə öz növbəsində informasiya resurslarının təhlükəsizliyini təmin etmək, şəbəkə ilə ötürülən informasiyaya kənar müdaxilələrin zərərli nəticələrini azaltmaq üçün vacibdir.

Müasir dövrdə proqram məhsullarına və kompyuter şəbəkələrinə müxtəlif növ cəsus proqramların daxil edilməsinə külli miqdarda vəsait sərf edilir. ABŞ və Qərbi Avropa ölkələrinin kəşfiyyat strukturlarında "İnternetdən istifadə" və ya "kompyuter kəşfiyyatı" şöbələri fəaliyyət göstərir. Bu şöbələrin qarşısında əsas məqsəd kimi elmi-texnoloji və maliyyə sirlərinin əldə olunması, informasiya şəbəkəsi vasitəsilə vacib informasiya sistemlərinə hücum, informasiya resurslarının təhlükəsizliyinin dəf edilməsi, təşkilatlarda cavabdeh şəxslərə psixoloji təsir və s. məsələlər durur. Bunları nəzərə alaraq deyə

bilərik ki, müasir İM texnologiyalarının tətbiqində əsas strateji əsasların təyin edilməsi bu sahədə görüləcək ilkin vəzifələrdəndir:

- İM-in həyata keçirilməsində çəkilən maliyyə xərclərinin informasiya təhlükəsizliyinin təmini üçün istifadə olunan vəsaitələrdən az olması;
- informasiya əməliyyatları zamanı ənənəvi dövlət sərhədlərinin maneəsiz dəf edilməsi;
- informasiya manipulyasiyası nəticəsində real vəziyyətin düzgün qiymətləndirilməməsi;
- informasiyanın ələ keçirilməsi və ya dəyişdirilməsi zamanı strateji kəşfiyyat fəaliyyətində prioritetlərin dəyişdirilməsi;
- İM, ümumiyyətlə, müxtəlif informasiya əməliyyatlarının başlaması vaxtının aşkar edilməsinin çətin olması (bəzən də mümükünsüzlüyü);
- İM-ə başlayan tərəfə qarşı təhlükəsizlik tədbirlərinin həyata keçirilməsinin mürəkkəbliyi və s.

İnformasiya və telekommunikasiya sahələri üzrə geri qalan ölkələr üçün informasiya resurslarının təhlükəsizliyinin təmin edilməsi və İM-nə tap gətirə bilmə problemlərinin vaxtında həlli məsələləri ABŞ və Qərbi Avropa ölkələri ilə müqayisədə daha aktualdır.

Tədqiqatlar göstərir ki, İM texnologiyalarının araşdırılması ilə məşğul olan mütəxəssislərin işində müxtəlif yanaşmalar və baxışlar mövcud olsa da, müəyyən məsələlərdə fikirlər eynidir: İM-də əsas məqsəd qarşı tərəfi fiziki məhv etmək deyil, onu səhv addım atmağa sövq edərək siyasi, hərbi, iqtisadi, psixoloji və sosioloji sahələrdə qələbə qazanmaq, rəqibdən üstün olmaqdır. Öz istəklərini həyata keçirmək

məqsədi ilə mübarizə aparan tərəflər biri-birinin informasiya və intellektual sahələrinə təsir göstərə biləcək hər bir vasitələrdən istifadə edir.

Son illərin lokal müharibələri və dünyanın müxtəlif yerlərində baş verən silahlı münaqişələr hərbi mütəxəssislər tərəfindən informasiya vasitələrinin hərbi sistem və qurğulara təsirinin geniş analizini aparmağa məcbur etmişdir. İM bir dövlətin daxilində qruplar, partiyalar, şirkətlər arasında, həmçinin müxtəlif dövlətlər arasında aparıla bilər. İM anlayışına müxtəlif təriflər verilsə də informasiya texnologiyaları və psixologiya üzrə mütəxəssislərin çoxu təsdiq edir ki, İM əsasən hakimiyyət və kapital, insanları idarə etmək uğrunda müharibədir [43].

Beynəlxalq sisyasətdə informasiya təsirinin iki forması mövcuddur: fasiləsiz (kontaktlı) və fasiləli (distant) informasiya təsiri. Fasiləli informasiya təsiri elə situasiyanı xarakterizə edir ki, bu zaman iki münaqişə edən beynəlxalq qüvvələrin birbaşa kontaktı mümkün deyil və ya arzu olunmazdır.

Distant formada informasiya təsirinə misal olaraq Almaniyanın xüsusi xidmət orqanlarının 2001-ci ildə verdiyi xəbəri göstərmək olar. Bu xəbərə görə, ABŞ-ın Milli Təhlükəsizlik Agentliyi "Microsoft" firmasının proqram məhsullarına malik açarlardan istifadə edərək AFR-nin Müdafiə Nazirliyinin şifrələnmiş informasiyasına müdaxilə etmişdi. Milli informasiya resurslarını qorumaq üçün Almaniyanın Müdafiə Nazirliyi kriptoqrafik texnikanın işlənməsi ilə məşğul olan yerli Almaniya firmalarına müraciət etmək məcburiyyətində qalmışdı. Bu hadisə bir daha sübut etdi ki, artıq "Microsoft" firmasının məhsulları informasiya silahı, qarşı tərəfə informasiya-texniki və informasiya-psixoloji müharibədə

maksimum ziyan vermək üçün nəzərdə tutulmuş vasitə kimi istifadə olunmaqdadır [44, 45].

İnformasiya təsiri obyektlərini şərti olaraq texniki (informasiya-texniki təsir) və sosial (informasiya-psixoloji təsir) hissəyə bölmək olar (cədvə 1.):

İnformasiya-texniki təsir – müxtəlif növ informasiya sistemlərinə (verilənlər bazası, verilənlər bankı, analitik sistemlər və s.), telekommunikasiya vasitələrinə, kompyuter şəbəkəsinə və s. texniki vasitələrə təsirdir. İnformasiya-texniki təsir dedikdə, radioelektron mübarizə, radioelektron kəşfiyyat, kompyuter şəbəkələrinə müdaxilə, haker müharibələri və s. nəzərdə tutulur. Texniki obyektlər kimi əlaqə və idarəetmə sistemləri, dövlətin maliyyə-iqtisadi fəaliyyətləri və s. ola bilər.

Cədvəl 1. İnformasiya müharibəsində üsullar

İnformasiya müharibəsi	*Obyekt*	*Məqsəd*
İnformasiya-texniki təsir	Kompyuterlər və informasiya sistemləri	İnformasiya sistemlərinə, kompyuter şəbəkəsinə nəzarət və ya onların məhv edilməsi
İnformasiya-psixoloji təsir	Ayrı-ayrı insanların və ya kütlənin şüuru	Hər-hansı ideologiyanın təbliği və davranışların idarə edilməsi

İnformasiya-psixoloji təsir – siyasi elita və əhalinin psixoloji durumuna, davranışına, cəmiyyətin informasiya mühitinin inkişafına, funksionallığına birbaşa təsir göstərən

xüsusi informasiyanın istehsalı və yayılmasıdır. Təbliğat, "beyinlərin yuyulması" və psixoloji təsir informasiya-psixoloji təsirin növləridir. İnformasiya-psixoloji təsir zamanı hansı üsuldan istifadə olunacağı ilk növbədə məqsədin təyin olunması və hədəflərin düzgün seçilməsindən asılıdır.

İnformasiya-psixoloji müharibə zamanı birinci yerdə ictimai fikrin formalaşdırılması prosesi dayanır. Bu halda azlıq təşkil edənlərin fikirlərini çoxluğun fikri kimi təqdim etmək informasiya psixoloji müharibələrdə ən çox istifadə olunan təsir növlərindəndir. İM zamanı psixoloji müharibə vasitələrindən istifadə bir tərəfdən mövcud informasiya sistemini dağıtmağa, digər tərəfdən isə onu digər informasiya-kommunikasiya sistemi ilə əvəz etməyə imkan verir ki, nəticədə, cəmiyyətin maraqları bu cəmiyyətə qarşı İM aparan tərəfin maraqlarına tabe etdirilir və ya uyğunlaşdırılır.

İnformasiya-psixoloji təsirdə ən təsirli vasitə kimi xəbərlər sayılır. Amerikalı mütəxəssislər xəbərlərə belə təyinat verirlər: "Xəbər – cəmiyyət tərəfindən qəbul edilmiş, hər zaman simmetrik olan ümumi normanın pozulması haqqında informasiyadır". Buradan nəticə çıxartmaq olar ki, İM texnologiyalarının müvəffəqiyyətli tətbiqi onun assimmetrikliyinin dərəcəsindən asılıdır [46].

Digər tərəfdən xəbər – müxtəlif hadisələr haqqında çap materiallarında, İnternetdə, radio və televiziyada, dedi-qodularda yayılan ən yeni informasiyadır. Xəbərin informasiya-psixoloji təsirinə onun təqdim edilmə üsulu da daxildir. Dünya təcrübəsi göstərir ki, ictimai rəy xəbərlərin təqdim edilmə üsulu əsasında formalaşır.

İctimai rəyin məhz xəbər mənbəyinə sərfəli şəkildə formalaşdırılmasının bir neçə yolu var. İnformasiya mənbəyi

KİV-in xəbərə hansı prizmadan baxmasını istəyirsə, məhz o tərəfi də qabardır. Çox zaman mənbənin niyyətindən bixəbər media da, öz növbəsində, xəbərin görünən (əslində göstərilən) tərəfini qabartmaqla ona informasiya ilə manipulyasiya xidməti göstərmiş olur və nəticədə bilərəkdən, bəzən də bilmədən İM-də iştirak etmiş olur.

Müasir jurnalistikada tez-tez informasiya ilə manipulyasiyadan söz açılır. Manipulyasiya İM-in əsas silahlarından biridir. Xəbərdən özü üçün sərfəli formada yararlanmaq istəyində olan mənbə hədəfi vurmaq üçün məhz media strukturlarından, kütləvi vasitədən yararlanır. Son illər bir sıra kütləvi informasiya şirkətləri müxtəlif psixoloji verlişlər, zorakılığı təbliğ edən və milli, dini ədavəti qızışdıran filmlər və verlişlər hazırlamaqla informasiya-psixoloji müharibələrin aparılmasında daha effektli vasitələrdən istifadə etməkdədir.

KİV-in ictimai rəyin formalaşmasında oynadığı rolun əhəmiyyəti bir çox ölkə rəhbərlərinin diqqətindən də yayınmayıb. Hətta vaxtilə ABŞ prezidenti Riçard Nikson Milli Təhlükəsizlik Şurasının iclasında büdcə xərcləriylə bağlı məsələlərin müzakirəsində çıxış edərkən silah sisteminin yaradılmasına 9 dollar qoymaqdansa informasiya və təbliğata 1 dollar sərf etməyi daha sərfəli saymışdır. R.Nikson bildirirdi ki, silaha nadir hallarda əl atılırsa, informasiyadan istifadə məkan və zamandan asılı olmayaraq hər zaman baş verir.

2010-cu ilin noyabr ayında İnternet qlobal şəbəkəsində yerləşdirilmiş WikiLeaks saytında ABŞ-a məxsus bəzi məxfi məlumatların nəşr olunması bir daha sübut etdi ki, son illər informasiya bolluğu elə bir həddə gəlib çatmışdır ki, insanlar və dövlətlər informasiya axınını nəzarətdə saxlaya bilmir.

"Rusiya-Avroasiya" Mərkəzinin xarici siyasət üzrə direktoru Aleksandr Rar müsahibələrinin birində bildirdi ki, dövlət sirlərinin dünya ictimaiyyətinə təqdim olunması iqtisadi böhrandan sonra ABŞ dövlətinə vurulan ikinci zərbədir: "Dünya dəhşət içində gördü ki, ABŞ kimi nəhəng dövlət öz sirlərini nəzarətdə saxlaya bilmir..." Analitiklər WikiLeaks saytı ilə bağlı qalmaqala qiymət verərək bəyan etdilər ki, bu cür gizli məlumatların nəşr edilməsi ABŞ-ın bir dövlət kimi təhlükəsizliyini sual altında qoyur: "Bu gün informasiya texnologiyaları dövlətlərdən də güclü olub və artıq bu prosesi dayandırmaq mümkün deyil. Bu gün informasiyaya qoyulan məhdudiyyətin sərhədinin harada olmasını anlamaq olmur" [47].

Bir çox ölkələrdə vətəndaşlar hələ də müasir informasiya texnologiyaları vasitələrindən gələn, əsasən də siyasi məqsədlərə xidmət edən gizli informasiya-psixoloji təhlükələri tam anlamırlar. Müxtəlif sosial proseslərdə istifadə edilən İKT vasitələri və informasiya sistemlərinin informasiya münaqişələrində tətbiqi İM texnologiyalarını təhlükəli həddə yüksəltmişdir. İKT vasitələrinin cəmiyyətə, müəyyən qrup insanlara, hər-hansı fərdi şəxsə qarşı tətbiqi, məqsədyönlü informasiya və informasiya-psixoloji təsiri insanlar arasında informasiya münasibətlərinin sosial müxtəlifliyini qabardaraq daha gizli forma almaqdadır. Bu gün insan psixikasına güclü təsir edən müxtəlif yeni mədəniyyət növləri inkişaf etməkdədir (məsələn, kompyuter mədəniyyəti, veb-texnologiyalar, perfomans, qraffiti (divar şəkilləri) və s.). Müasir dövrdə informasiya mədəniyyətinin müəyyən hissəsini təşkil edən bu sahələrdə fərdi ilə yanaşı, kütləvi şüuru dəyişdirməyə qadir həssas və təkmilləşdirilmiş texnologiyadan istifadə edilir.

İnformasiya mədəniyyəti, ilk növbədə, cəmiyyətdə informasiya fəaliyyəti və insanın informasiyaya (biliyə) münasibəti, cəmiyyətin informasiya resurslarından və informasiya kommunikasiya vasitələrindən effektli istifadə etmək, müasir texniki vasitə və metodlardan, kompyuter texnologiyalarından istifadə etməklə informasiyanın əldə edilməsi və ötürülməsi bacarığıdır. Bu nöqteyi-nəzərdən informasiya mədəniyyəti insana informasiya məkanında sərbəst hərəkət etməyə və İKT vasitəsilə başqalarına qarşılıqlı təsir göstərməyə imkan verən müəyyən bilik səviyyəsidir.

İM-də əməliyyatlar əsas iki istiqamətdə aparılmalıdır: informasiya hücumu və informasiya hücumlarından müdafiə:

1. İnformasiya hücumu – qarşı tərəfin informasiya infrastruktrunun tam məhv edilməsi və qarşı tərəfə öz qüvvəsindən istifadə imkanı verməməkdir. Digər tərəfdən informasiya hücumu dedikdə, şəbəkələrarası birləşmələr vasitəsi ilə informasiya sistemlərinə təsir, şəbəkədə aktiv axtarış, icazəsiz fəaliyyət və nəhayət informasiya qarşıdurması nəzərdə tutulur. İnformasiya hücumunda əsas məqsəd radioelektron vəsaitlərin və informasiya bazalarının məhvi, qarşı tərəfin kompyuter şəbəkəsinin, informasiya sistemlərinin normal fəaliyyətinin pozulması və s. daxildir. Son illər İnternetin dünyada yayılması ilə əlaqədar qarşı tərəfin elektron informasiya bazalarının kiberməhvi xüsusi önəm daşıyır.
2. İnformasiya hücumlarından müdafiə dedikdə, strateji vacib məlumatlarının və informasiya strukturlarının kənar təsirlərdən və icazəsiz müdaxilələrdən müdafiəsi nəzərdə tutulur. Bura informasiyanın strateji maskalanması, informasiya infrastruktrunun fiziki qorunması,

dezinformasiya, radioelektron mübarizə və s. daxildir. İM zamanı informasiyanın xarici təsirlərdən müdafiəsi informasiya təhlükəsizliyinin təminatı metodları ilə realizə olunur.

İM-də əməliyyatların müxtəlif istiqamətlərdə aparılması onun xüsusiyyətinə də təsirini göstərir:

- Təsir obyekti – informasiyanın və ya informasiya sistemlərinin bütün formaları. Sərbəst obyektlər kimi bütün növ informasiya və informasiya sistemləri istifadə mühitindən ayrılmaqla təsir altında saxlanılır.
- Təsir obyekti həm silah, həm də müdafiə obyekti kimi istifadə edilir.
- Müharibə aparılan ərazi və mühit genişlənmiş olur. İM həyat fəaliyyətinin müxtəlif sahələrində həm müharibə elan edilərkən, həm də böhran vəziyyətlərdə aparılır.
- İM həm müharibə şəraitində, həm də sülh şəraitində aparıla bilir.
- İM-də həm xüsusi təlim görmüş hərbçilər, həm də mülki şəxslər iştirak edir.

Bu xüsusiyyətləri nəzərə alaraq bir çox ölkələr İM-in potensialının təkmilləşdirilməsinin vacibliyini anlayırlar. Əgər İM-in hüçum hissəsi informasiya silahının işlənib hazırlanması və istifadəsindən asılıdırsa, müdafiə hissəsinin əsas aspekti təhlükələrin aşkar edilməsi və vaxtında qarşısının alınmasıdır.

İM zamanı məqsədyönlü informasiya təsiri nəzərdə tutulmuş obyektlərə uyğun olaraq informasiya hədəflərini 4 qrupa bölmək olar:

1. Qərarların qəbulu və idarəetmə sistemləri (vətəndaş, hərbi, sosial, mədəni);

2. Vətəndaş informasiya infrastrukturu (telekommunikasiya sistemləri, nəqliyyatın, energetikanın, maliyyənin, sənayenin informasiya sistemləri);
3. Hərbi informasiya infrastrukturu (nəzarət, idarə və əlaqə sistemləri, kəşfiyyat);
4. Silahlanma sistemləri.

Konkret informasiya əməliyyatları zamanı göstərilən hədəflər müxtəlif təsirlərə məruz qala bilər. Qeyd etmək lazımdır ki, bu yanaşma keçən əsrin 90-cı illərində daha populyar idi. Bu gün baş verən informasiya prosesləri və qarşıdurmaları sübut edir ki, informasiya sistemlərinə uzaqdan təsir müəyyən maliyyə itkilərinə və cəmiyyətdə psixoloji abu-havanın dəyişməsinə səbəb olsa da, onlar mühüm strateji sistemlərin fiziki məhvinə və insan itkilərinə səbəb olmurlar. Məsələn, haker fəaliyyəti özü-özlüyündə təhlükəli olsa da İM-də heç də həlledici rol oynamır. Odur ki, kibermüharibələrə ənənəvi hərbi əməliyyatların effektivliyini artıran faktor kimi baxmaq daha düzgün olardı.

Bununla yanaşı, nəqliyyat, energetika, maliyyə və həbi sahələrlə bağlı informasiya sistemlərinə hücum imkanlarını da nəzərdən qaçırmamaq lazımdır. ABŞ və Qərbi Avropada informasiya təhlükəsizliyi üzrə mütəxəssislər bu informasiya sistemlərini kritik mühüm infrastruktur (critical infrastructures) adlandıraraq İM-in əsas hədəfləri adlandırırlar.

Bu hücumların mümkünlüyü iqtisadi sahədə böyük itkilərə səbəb ola bildiyinə görə, 90-cı illərin ortalarından başlayaraq kibernetik mübarizə aktı kimi hərbi və mülki ekspertlərin əsas araşdırma predmetinə çevrilmişdir.

2. 3. İnformasiya müharibəsi sahəsində xarici ölkələrin təcrübəsi

İM probleminin obyektiv və tam təhlilini aparmaq üçün xarici mənbələrin analizi və qabaqcıl ölkələrin (ABŞ, Rusiya, Avropa ölkələri, Çin və s.) mütəxəssislərinin, alimlərinin, praktiklərinin fikirlərinin müqayisəsi tələb olunur. ABŞ-da İM problemi son 15 ildə digər ölkələrlə müqayisədə daha geniş araşdırılmış və öyrənilmişdir. Bunu ABŞ administrasiyasının, konqresin, Müdafiə Nazirliyinin rəsmi sənədlərində, rəsmi şəxslərin açıq bəyanatlarında, İM problemləri ilə məşğul olan təşkilatların hesabatlarında görmək mümükündür. ABŞ-da İM-ə hazırlıq 3 istiqamətdə aparılır [48, 49]:

1. Hərbi qüvvələr;
2. Xüsusi xidmət orqanları;
3. Elmi təşkilatlar və korporasiyalar.

Hərbi dairələrdə hazırlıq nəzəri, təşkilati və maddi-texniki fəaliyyətlərlə əlaqədardır. Orduda İM problemləri ilə məşğul olan zabitlərin (Info War Officers) hazırlığı həyata keçirilir. İM-in aparılması üzrə hər il onlarla qərargah oyunları keçirilir [50].

ABŞ-ın hərbi dairələrində İM ilə bağlı əməliyyatlarda informasiya sistemlərinin və kompyuter şəbəkələrinin məhvi vacib məqamlardan sayılır və xüsusi qurğuların, proqram təminatlarının və mütəxəssislərin köməyi ilə həyata keçirilir. Təsdiq olunmuşdur ki, İM-də avtomatik idarəetmə sistemlərinə (AİS) hücum vasitələrinin effektivliyi informasiyanın mühafizəsi sistemlərinin effektivliyindən daha yüksəkdir. Amerikalı ekspertlər tərəfindən bildirilir ki, 2010-cu ildən başlayaraq İM yeni və daha təhlükəli forma alacaqdır. Onların fikrincə, informasiya tədricən təminedici vasitədən çıxaraq döyüş növünə çevrilir [51]. Təəssüf ki, bu proqnozlar son illər

özünü doğrultmaqdadır. Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik, virusların yaradılması və yayılması üçün yeni imkanlar, İnternet məkanının genişlənməsi ilə əlaqədar şəbəkə müharibələrinin sürətlə artmasına şərait yaratmışdır.

Gizli materialların əldə keçirilməsi, araşdırılması və məqsədli istifadəsi hərbdə əsas istiqamətlərdəndir. 1980-ci ildən başlayaraq ABŞ-ın hərbi-hava qüvvələrində İM predmeti geniş öyrənilməyə başlandı. "Soyuq müharibə" sona çatdıqdan sonra "informasiya müharibəsi" termini ABŞ-ın Müdafiə Nazirliyinin sənədlərinə daxil edildi [52]. Fars körfəzi uğrunda müharibədə həyata keçirilən «Səhrada Tufan» əməliyyatından sonra isə İM texnologiyalarına münasibət həm ABŞ, həm də digər aparıcı ölkələrdə dəyişdi. Belə ki, bu əməliyyatdan sonra informasiya texnologiyaları ilk dəfə olaraq hərbi vasitə kimi sınaqdan keçirildi və "informasiya müharibəsi" termini rəsmi olaraq ABŞ Müdafiə Nazirliyinin 21 dekabr 1992-ci il tarixli 3600.1 saylı direktivində istifadə edildi.

Amerika tədqiqatçılarının fikrincə, hərbi qüvvələrin hazırlığı və hərbi əməliyyatlar zamanı baş verən informasiya qarşıdurmalarında yalnız İM texnologiyalarından deyil, eyni zamanda informasiya təhlükəsizliyini təmin edən texnologiyalardan da istifadə olunmalıdır. Belə ki, kompyuter şəbəkələrinin və bu şəbəkələrdəki informasiya sistemlərinin iş qabiliyyəti yalnız qurğuların etibarlılığından deyil, həm də onun işini pozmağa yönəlmiş məqsədyönlü əməliyyatlara qarşı davam gətirmək qabiliyyətindən asılıdır.

İlk dəfə informasiya hücumları vasitəsi kimi informasiya texnologiyalarından 1991-ci ildə İraqa qarşı aparılan hərbi əməliyyatlarda istifadə edilmişdir. "İnformasiya müharibəsi"

termini isə ilk dəfə, rəsmi olaraq ABŞ Müdafiə Nazirliyinin direktivində istifadə edilsə də, Amerika administrasiyasının İM məsələləri ilə bağlı fəaliyyəti 1996-cı ildə vacib infrastrukturların mühafizəsi üzrə Prezident komissiyasının formalaşmasından başlamışdır.

ABŞ-ın hərbi dairələrində İM dedikdə, milli hərbi strategiyanı dəstəkləməklə, informasiya üstünlüyü əldə etmək üçün qarşı tərəfin kompyuter şəbəkəsinə və informasiya sistemlərinə təsir etməklə başlanan fəaliyyət nəzərdə tutulur [53]. Bildirilir ki, İM-ə başlayan tərəf əvvəlcə malik olduğu informasiya sistemlərinin təhlükəsizliyini təmin etməlidir. Belə ki, son illərin təctübəsi göstərir ki, hərbi əməliyyatlar zamanı baş verən itkilər əsasən, idarəetmə sistemlərinə və insan psixikasına qarşı tətbiq edilən informasiya silahlarının növündən və tətbiq üsulundan asılıdır.

1990-cı illərdə ABŞ-ın nüfuzlu RAND korporasiyasının həyata keçirdiyi əsas tədqiqatlar nəticəsində İM texnologiyalarının araşdırılması, informasiya silahının imkanlarının dərk edilməsi və bundan düzgün istifadə edilməsi zəruriyyəti ortaya çıxdı. Çox keçmədi ki, RAND şirkətinin İM üzrə tədqiqatlarının əsas nəticələri MR-661-OSD "Strategic Information Warfare. A new Face of War" (1996) [54], MR-963-OSD "The Day After... in the American Strategic Infrastructure" (1998) [55], MR-964-OSD "Strategic Information Warfare Rising" (1998) [56] hesabatlarında göstərildi və korporasiyanın əməkdaşları Con Arkvilla və Devid Ronfeldt kibermüharibə və şəbəkə müharibəsi konsepsiyalarına (Network Centric Warfare - NCW) əlavə edildi.

Bu konsepsiyada göstərilir ki, gələcək hərbi münaqişələrdə müvəffəqiyyət "informasiya üstünlüyü" hesabına əldə

ediləcəkdir. İnformasiya üstünlüyü isə yeni texnologiyaların hərbi idarəetmə və əlaqə sistemlərinə tətbiqi ilə əldə ediləcəkdir. Konsepsiyadakı bir çox təkliflər sonradan ABŞ Hərbi Hava Qüvvələrinin şəbəkə müharibələri və şəbəkə hərbi qüvvələrinin konsepsiyasının hazırlanmasında istifadə olunmuşdur.

Silahlı qüvvələrin informasiyalaşması və hərbi platformanın intellektuallaşdırılması bu nəzəriyyənin sürətlə praktikaya tətbiq olunmasına şərait yaratmışdır. Məhz bundan sonra beynəlxalq aləmdə SİW (Strategic Information Warfare - strateji informasiya əks-mübarizəsi) termini məşhurlaşdı. Bu anlayış dövlətlərin qlobal informasiya məkanından istifadə etməsi və strateji hərbi əməliyyatların keçirilməsi üçün infrastrukturun formalaşdırılması kimi izah olunurdu [57].

1992-ci ilin 21 dekabrında Pentaqonun bu problemə aid 3600.1 nömrəli "İnformasiya müharibəsi" direktivininin nəşrindən sonra 1993-cü ildə Qərargah Rəisləri Komitəsinin 30 nömrəli direktivi meydana çıxdı. Bu sənəddə İM-in aparılmasının əsas prinsipləri göstərilməklə, gələcək müharibələrin məhz informasiya xarakterli olacağı və özündə siyasi, iqtisadi, texniki və hərbi sahələrdəki məqsədləri birləşdirəcəkləri xüsusi ilə qeyd edilirdi. Məhz bu sənəddə ilk dəfə göstərildi ki, İM-in müharibə dövründə olduğu kimi sülh dövründə də aparılması mümkündür – İM həm dövlət səviyyəsində (diplomatik, iqtisadi, informasiya, xüsusi, başqa qüvvə və vasitələr), həm də hərbi səviyyədə (qüvvələr, döyüş idarəçiliyi sistemləri ilə mübarizə vasitələri) aparıla bilər.

1994-cü ildən başlayaraq ABŞ-da ölkənin görkəmli hərbi-siyasi rəhbərlərinin nümayəndələrinin iştirakı ilə "İnformasiya müharibəsi" üzrə elmi konfranslar keçirilməyə başladı. 5-ci

elmi konfrans (5th International Conference on Information Warfare and Security) 2010-cu ilin aprel ayında ABŞ-ın Ohayo şəhərində yerləşən Hərbi Hava Qüvvələrinin Texniki İnstitutunda (The Air Force Institute of Technology, Wright-Petterson Air Force Base, Ohio) keçirilmişdir [58].

Konfranslarda müzakirə edilən problemlər əsasında belə qənaətə gəlmək olar ki, kompyuter şəbəkəsinin təhlükəsizliyini təmin etmək üçün, ilk növbədə, bütün mümkün təhlükələri tədqiq etmək, daha sonra isə konkret vəziyyət üçün daha çox ehtimal olunan təhlükələri seçmək lazımdır. Bu zaman iki üsuldan istifadə etmək lazım gəlir:

1. Artıq baş vermiş informasiya hücumları haqqında məlumatların toplandığı verilənlər bankından istifadə edilməsi;
2. Ehtimal olunan bütün informasiya hücumlarını təhlil edən və nəzərə alan metodoloji vəsaitlərin hazırlanması.

Hələ 1995-ci ildə ABŞ Hərbi Hava Qüvvələri Universitetinin (Air University, Maxwell Airforce Base, Alabama) əməkdaşları Corc Steyn, Riçard Şafranski və Oyen Censen İM texnologiyalarını araşdırarkən belə qənaətə gəlmişdilər ki, gələcək hərbi münaqişələrdə həlledici rol hərbi silahların deyil, informasiyanın (biliyin) üzərinə düşəcəkdir. Onların elmi işlərində informasiya texnologiyalarına strateji informasiya üstünlüyünü təmin edən vasitə kimi baxılmışdır. İnformasiya təhlükələrini araşdıran mütəxəssislər bildirmişdilər ki, informasiya hücumunda istifadə olunan vasitələrin bütün növləri arasında kompyuter virusları daha çox təhlükəlidir. Ekspertlərin fikrincə, bu gün informasiya texnologiyalarından aktiv istifadə edən şirkətlərin 80%-ə qədəri kompyuter viruslarından əziyyət çəkir [59].

1996-cı ilin fevral ayında ABŞ-ın Müdafiə Nazirliyi "Nəzarət və idarəetmə sistemləri ilə mübarizə" doktrinasını həyata keçirməyə başladı. 1996-cı ilin sonunda Pentaqonun eksperti Robert Banker simpoziumların birində "XXI əsrdə ABŞ hərbi qüvvələrinin yeni hərbi doktrinası" mövzusuna həsr edilmiş məruzə ("Force XXI" konsepsiyası) ilə çıxış etdi. Məruzədə deyilirdi ki, müharibələr iki istiqamətdə getməlidir – ənənəvi ərazidə və kiberfəzada. Kiberfəzalardan istifadə İM-in digər istiqamətləri ilə müqayisədə daha çox əhəmiyyət kəsb edir. Burada Robert Banker "kibermanevr" doktrinasını təklif edirdi ki, bu doktrinada qarşı tərəfin hərbi qüvvələrinin neytrallaşdırılması və dəf edilməsi məqsədi ilə istifadə edilən İM ənənəvi hərbi konsepsiyanı tamamlayan əlavə kimi göstərilirdi [60].

Bu sənəd müasir hərbi əməliyyatlarda nəzarət və idarəetmə sistemlərinə qarşı mübarizənin prinsiplərini izah edirdi. Hərbi ekspertlərin qeyd etdiyi kimi, yeni müharibələrdə qarşı tərəfin əsas hədəf obyektləri informasiya infrastrukturları və psixika (human network) olacaqdır. Bununla da 1996-cı ildən başlayaraq təyin edildi ki, hərbi münaqişələrdə torpaq, su, hava və kosmosdan başqa informasiya mühiti (infomühit) də nəzarətdə olmalıdır.

1998-ci ilin sonunda ABŞ-ın Hərbi Qüvvələrinin Qərargah Rəisləri Komitəsində "İnformasiya əməliyyatlarının keçirilməsi doktrinası" (Joint doctrin of information operations) adlı sənəd çap edildi. Bu sənəddə ilk dəfə olaraq amerikalıların hücum xarakterli informasiya əməliyyatlarının (informasiya hücumu) keçirilməsinə hazırlaşdıqları bir fakt kimi təsdiq olunurdu [61].

Bundan əvvəlki çıxışlarında Pentoqonun nümayəndələri dünya ictimaiyyətini inandırmağa çalışırdılar ki, informasiya fəzasında ABŞ yalnız müdafiə xarakterli informasiya əməliyyatları yerinə yetirir. Amma bu sənəddə hücum xarakterli informasiya əməliyyatının təkcə müharibə zamanı deyil, sülh şəraitində də keçirilməsinin mümkünlüyü göstərilirdi.

1999-cu ildə informasiya sistemlərinin və kompyuterlərin aktiv mühafizə qabiliyyətinin artırılması məqsədi ilə ABŞ-ın Müdafiə Nazirliyində kompyuter şəbəkəsinin mühafizəsi üzrə xüsusi operativ qrup yaradıldı və 1999-cu il, oktyabr ayının 1-dən başlayaraq Müdafiə Nazirliyinin elektron hesablama maşınları (EHM) şəbəkəsinin mühafizəsi üzrə cavabdehliyi kosmik komandanlığın baş komandanı öz üzərinə götürdü [62]. 2000-ci il, yanvar ayının 7-də ABŞ-ın Prezidentinin göstərişlərinin yerinə yerirlməsi ilə bağlı "İnformasiya sistemlərinin mühafizəsi haqqında milli plan" işləndi. Bu planın həyata keçirilməsi üçün federal büdcədən birinci il 2,103 milyard dollar tələb olundu.

2006-cı il, fevralın 13-də ABŞ-ın Ştab Rəisləri Komitəsi tərəfindən "İnformasiya əməliyyatları" doktrinasının (JP 3-13) yeni variantı təsdiq edildi [63]. Bu doktrinada ABŞ hərbçilərinin informasiya əməliyyatlarının təşkili və keçirilməsinə yeni, əvvəlki doktrinalardan fərqli münasibət göstərilməklə, informasiya qarşıdurmasının məqsədi, əsas prinsipləri dəqiqləşdirilmiş, rəhbər şəxslərin istər müharibə, istərsə də sülh şəraitində informasiya əməliyyatlarının keçirilməsində qarşılarında duran vəzifələr sadalanmışdır. Yeni doktrinada aşağıdakı ümumi kompleks informasiya əməliyyatlarının həyata keçirilməsi nəzərdə tutulur:

- radioelektron mübarizə *(Electronic Warfare, EW)*;

- psixoloji əməliyyatlar *(Psychological Operations, PSYOPS)*;
- şəbəkə əməliyyatları *(Computer Network Operations, CNO)*;
- operativ maskalanma *(Military Deception, MILDEC)*;
- əks tərəfin mühüm informasiya infrastrukturlarına real hücum *(Physical Attack)*;
- təhlükəsizlik əməliyyatları *(Operations Security, OPSEC)*.

Doktrinada göstərilmiş ümumi kompleks informasiya əməliyyatlarından da görünür ki, bu gün informasiya sistemlərinin İM məsələsində əsas rolu təkcə qarşı tərəfi yüksək dəqiqliklə məğlubiyyətə uğratmaq deyil, eyni zamanda öz informasiya sistemlərinin təhlükəsizliyini yüksəldərək onları daha çevik və effektli etmək, onlarda əks tərəfin təsirinə qarşı cavab təsirini sürətləndirmək, yeni taktiki fəaliyyət tətbiq etməkdir.

ABŞ-ın hərbi dairələrində İM problemlərinə dair konsepsiyalar arasında amerikalı hərbi analitik Riçard Şafrinskinin İM konsepsiyası öz orijinallığı və qoyulan məsələlərə görə xüsusi ilə diqqəti cəlb edir. O, İM problemlərinə hərbi qarşıdurma (warfare) kontekstindən baxaraq onun qarşı tərəfin biliyinə və cari vəziyyətdə fəaliyyətinə qarşı yönəlmiş hərbi əməliyyat olduğunu göstərir.

90-cı illərin əvvəllərindən başlayaraq ABŞ-ın Müdafiə Nazirliyində informasiya qoşunlarının təşkilatı strukturunun formalaşması həyata keçirilir. Hal-hazırda ABŞ-ın Hərbi Qüvvələrinin hər bir növü öz İnformasiya Müharibəsi Mərkəzinə malikdir.

ABŞ-ın İnformasiya Müharibəsi Mərkəzlərindən biri 1993-cü ilin sentyabrında ölkənin Hərbi Hava Qüvvələrinin nəzdində yaradılmış AFIWC (Air Force Information warfare Center) mərkəzidir. AFIWC-in əsas proqramında mərkəz üzərinə düşən tapşırıqlar belə göstərilir: "AFIWC qarşı tərəfin operativ idarəetmə və komanda sistemləri ilə mübarizə vasitələrini işləyir və təkmilləşdirir, eləcə də onların analiz edilməsini və təcrübədən keçirilməsini təmin edir. AFIWC həm də informasiya əməliyyatları zamanı informasiya silahlarının operativ tətbiqinin planını hazırlayır" [64].

1994-cü ilin avqust ayında ABŞ-ın Hərbi Dəniz Qüvvələrinin nəzdində İnformasiya Müharibəsi Mərkəzi – NIWA (Navy Information Warfare Activity) yaradılmışdır. Bu mərkəzin əsas vəzifəsi gələcəkdə ABŞ-ın Hərbi Dəniz Qüvvələrinin iştirakı ilə baş verə biləcək münaqişələrin həllini təmin edən İM-in daha vacib aspektlərini tədqiq etməkdir.

ABŞ-ın quru qoşunlarında İM əməliyyatları yerüstü informasiya hərbi əməliyyatları xidməti LIWA (Land Information Warfare Activity) tərəfindən həyata keçirilir. LIWA Amerikanın Virciniya ştatının Belvuar limanında yerləşir. ABŞ-da İM problemləri ilə Müdafiə nazirliyi məşğul olur. İM ilə bağlı bütün məsələlərin həllində cavabdehlik ABŞ-ın Müdafiə nazirinin qoşunların idarə edilməsi, əlaqə və kəşfiyyat üzrə köməkçisinin üzərinə düşür. İnformasiya hücumları problemlərinin həlli üzrə birbaşa rəhbərliyi Müdafiə Naziri köməkçisinin İM məsələləri üzrə müavini yerinə yetirir.

ABŞ-da informasiya qoşunlarının düzgün tətbiqini təmin etmək üçün xüsusi təşkilatların yaradılması təklif olunur:

1. İnformasiya müharibəsi məsələləri üzrə planlaşdırma və koordinasiya mərkəsi. Mərkəzdə İM ilə bağlı bütün

məsələlər üzrə fəaliyyətin planlaşdırma sisteminin işlənməsi nəzərdə tutulmuşdur;
2. İnformasiya müharibəsinin başlanması əlamətlərinin təhlili üzrə strateji mərkəz. Mərkəz kəşfiyyat xarakterli informasiyanın toplanması və təhlili ilə məşğul olmalıdır;
3. İnformasiya silahlarından müdafiə mərkəzi. Mərkəz informasiya hücumları haqqında xəbərdarlıq etmək və informasiya hücumlarının yaradacağı fəsadları aradan qaldırmaq kimi məsələlərlə məşğul olacaqdır;
4. Avtomatik idarəetmə sistemlərinin (AİS) arxitektura və konstruksiyasının işlənməsi üzrə şöbə. Şöbədə informasiya silahlarından müdafiə olunmaq üçün sistem və vasitələrin birgə layihəsinin və texniki standartlarının işlənməsi nəzərdə tutulmuşdur;
5. Müstəqil ekspertlər qrupu – "Qırmızı komanda". Qrupa AİS-in zəif tərəflərini analiz etmək, İM zamanı hücuma məruz qalacaq ayrı-ayrı elementlərə və bütünlüklə AİS-ə eksperimental hücumların təşkilini həyata keçirmək həvalə olunur.

İnformasiya qoşunlarının təşkilati strukturu daima dəyişdirilir və inkişaf etdirilir. ABŞ-ın hərbi-siyasi rəhbərliyi çox zaman "sınaq və xəta" (Trial and error) metodu üzrə hərəkət edir. "Sınaq və xəta" problemlərin həlli, xətaların aradan qaldırılması, biliyin əldə edilməsinin ümumi metodudur. Bu metoda əsasən: struktur yaradılır, daha sonra onun effektivliyi yoxlanılır. Əgər struktur ona qoyulan tələblərə cavab vermirsə, o ləğv olunur və ya dəyişdirilir [65].

İnformasiya qoşununun təşkilati strukturunun təyini və bu ordunun ayrı-ayrı bölmələri tərəfindən həll ediləcək məsələlər bir daha sübut edir ki, həm sülh şəraitində, həm də hərbi

əməliyyatlar zamanı İM-in vacibliyini ABŞ-ın hərbi-siyasi dairələrində yaxşı anlayırlar. Bu gün Pentaqon informasiya silahlarının metod və texnologiyalarından istifadə etməklə, XXI əsrdə mümkün müharibələrin variantlarını superkompyuterlərdə modelləşdirməkdə davam edir.

İlk destruktiv proqram vasitələrinin yaranması ilə ABŞ rəhbərliyi bu proqramlardan siyasi və hərbi sahədə nəaliyyətlər əldə etmək üçün istifadə etməyi qərara aldı. Bu məqsədlə 1990-cı ildə ABŞ-ın Müdafiə Nazirliyində hərbi destruktiv proqram vasitəsinin yaradılması üzrə müsabiqənin keçirilməsi açıq elan edildi. Hərbi destruktiv proqram vasitəsinin yerinə yetirəcəyi funksiyalar bunlar idi:

- Hərbi təyinatlı AİS-in abonent komplekslərinin və əlaqə xətlərinin normal iş rejiminin pozulması;
- AİS-ə yalan informasiyanın daxil edilməsi (qarşı tərəfin dezinformasiyası);
- Proqram təminatının modifikasiyası.

Yaradılacaq destruktiv proqram vasitələrinin AİS-ə daxil edilməsi əməliyyatının qarşı tərəfin radioəlaqə sistemlərindən həyata keçirilməsi nəzərdə tutulurdu. Hal-hazırda ABŞ-da bu cür informasiya təsirləri vasitələrinin işlənməsi yüksək sürətlə həyata keçirilir və araşdırmalarda şəbəkə müharibələri problemlərinə daha çox diqqət ayrılır.

Şəbəkəsentrik müharibə və ya şəbəkə müharibəsi (Network Centric Warfare – NCW) konsepsiyası üzərində müntəzəm işlərin görülməsinə 1990-cı illərin ortalarında, "RAND Corporation" şirkəti tərəfindən başlanmışdır. Konsepsiya üzərində işləyən şirkət əməkdaşları C. Akvilli və D. Ronfeldt gələcəkdə baş verəcək şəbəkə müharibələri haqqında fikirlərini ilk dəfə "The Advent of Netwar" (Şəbəkə

müharibəsinin meydana çıxması) məqaləsində bildirdilər [66]. Sonradan NCW konsepsiyasının işlənməsinə Pentaqonun bir çox bölmələri və "beyin mərkəzləri" (think-tanks) qoşuldular. Beləliklə, ABŞ-ın Müdafiə Nazirliyində silahlı qüvvələrin şəbəkə mühafizəsi (network-centric defense) və şəbəkə müharibəsi (network-centric warfare) nəzəriyyələri meydana çıxdı.

"Şəbəkə müharibəsi" nəzəriyyəsinin prinsiplərinə əsaslanaraq ABŞ-ın hərbi sahəsində xüsusi bölmə – ABŞ-ın silahlı qüvvələrinin yeniləşdirilməsində, eləcə də müasir tələbatlara uyğun inkişafında cavabdehlik daşıyan Hərbi Qüvvələrin Yenidən Təşkili Departamenti (Office of Force Transformation) yaradıldı.

NCW konsepsiyasında göstərilən problemlərin çoxu 2001-ci il, iyul ayının 27-də ABŞ-ın Müdafiə Nazirliyi tərəfindən hazırlanmış "Şəbəkəsentrik hərb sənəti" məruzəsində, Hərbi Qüvvələrin Yenidən Təşkili Departamenti tərəfindən nəşr edilmiş "Şəbəkəsentrik hərb sənətinin realizə olunması" işində, eləcə də bir sıra amerikalı hərbçilərin və ekspertlərin monoqrafiyalarında, məqalələrində göstərilmişdir [67, 68, 69, 70].

Müharibələrin kompyuter şəbəkəsində aparılmasının modelləşdirilməsi və təsviri üçün amerikalı ekspertlər "baza-effektlər" əməliyyatının konsepsiyasını (effects-based operations) işlədilər. Konsepsiyada göstərilən əməliyyatların mənfi və müsbət cəhətlərini analiz edərək ekspertlər belə qənaətə gəldilər ki, "baza-effektlər" əməliyyatını "sülh, böhran və müharibə şəraitində dostların, neytral qüvvələrin və qarşı tərəflərin davranışlarının formalaşmasına istiqamətlənmiş əməliyyatlar yığımı" (sets of actions directed at shaping the

behavior of friends, neutrals, and foes in peace, crisis, and war) kimi təqdim etmək olar. Eyni zamanda "baza-effektlər" əməliyyatı istənilən vaxt və istənilən yerdə keçirilə bilər və şəbəkə müharibəsinin aparılmasının əsas forması hesab edilir [71].

NCW nəzəriyyəsində insanların emosiyası, psixoloji durumu və s. nəzərə alınmış, coğrafi anlayış öz mənasını itirmişdir. NCW nəzəriyyəsini işləyənlər müasir müharibənin mahiyyətini faktiki olaraq digər xalqlara öz mədəniyyətini, dəyərlər sistemini, dünyagörüşlərini təbliğ etməkdə görürlər. Belə bir nəzəriyyə bu gün silahdan istifadə edilərək həyata keçirilən müharibələrin ideyalar müharibəsinə keçməsi haqqında fundamental tezisdir. Müasir dövrdə idayaların özləri də effektli silaha çevrilmişdir.

2001-ci il, 11 sentyabr terror aktından sonra ABŞ-ın müdafiə naziri D. Ramsfeld elan etdi ki, Amerika yeni tip müharibəyə hazırlaşmalıdır. Bu müharibə XX əsrin müharibəsindən, həm də beynəlxalq terrorizmə qarşı müharibədən köklü surətdə fərqlənməlidir. Bununla da NCW nəzəriyyəsi öz aktuallığını bir daha sübut etmiş oldu. Nəzəriyyə 2010-cu ilə qədər ABŞ-da hərbi quruculuq proqramına («Joint Vision 2010») daxil edilmişdir. Bu proqramın həyata keçirilməsi üçün artıq bu gün Pentaqonun yeni qlobal informasiya müdafiəsi şəbəkəsi (Defense Information Grid) yaradılır. NCW qarşı tərəf üzərində informasiya üstünlüyü əldə etməyi nəzərdə tutur ki, bu da intellektual obyektlərin vahid informasiya fəzasında birləşməsi hesabına hərbi gücün artmasına səbəb olacaqdır.

NCW nəzəriyyəsinin müvəffəqiyyətlə həyata keçirilməsi Qərb alimlərinin fikrincə, yalnız Hərbi Dəniz Qüvvələrinin

idarəedilməsi sisteminin, silahların, İKT vasitələrin birləşmiş strukturu və ya Qərbdə "Hərbi Dəniz Qüvvələrinin vahid şəbəkəsi" (ForceNet) adlandırılan funksional konsepsiyası bazasında mümkündür.

Nəzərdə tutulmuş bütün konsepsiyaların yerinə yetirilməsi informasiyanın əldə edilməsi, emalı, ümumiləşdirilməsi, paylanması və mühafizəsi üzrə əvvəllər mümkün olmayan imkanlar əldə etməyə şərait yaradır. ForceNet konsepsiyasının 2005-ci ildə qəbul olunmasına baxmayaraq Qərbdə bu konsepsiya üzrə mübahisələr hələ də davam edir. Bir qism analitiklər bu konsepsiyanı Hərbi Dəniz Qüvvələri tərəfindən həyata keçirilən informasiya əməliyyatlarının təşkilinin və operativ tətbiqinin əsası adlandırırlar, digərləri ona ABŞ-ın silahlı qüvvələrinin ümumi konsepsiyası hesab edilən NCW-nin əsası kimi baxırlar. Onların fikrincə, NCW nəzəriyyədir, şəbəkəsentrik əməliyyat isə (Net-centric Operations) konsepsiyadır, FORCEnet isə nəzəriyyəni praktika ilə birləşdirən prosesdir. Əslində hər iki anlayış vahid informasiya fəzasında hərbi əməliyyatların aparılmasını əvvəlcədən müəyyən edir. "XXI əsrin informasiya texnologiyaları" (IT-21 - Information Technology for 21-st Century) konsepsiyası sonradan "Hərbi Dəniz Qüvvələrinin vahid şəbəkəsi" (FORCEnet) funksional konsepsiyası ilə əvəz edilmişdir. Bu konsepsiya hərbi əməliyyatların bütün iştirakçılarını, idarəetmə və kəşfiyyat sistemlərini, hərbi platformaları (gəmilər, sualtı qayıqlar, təyyarələr və s.), silahlanma vasitələri və konplekslərini vahid qarşılıqlı əlaqədə olan strukturda birləşdirərək istənilən səviyyəli və ölçülü münaqişələrdə müvəffəqiyyətli əməliyyatlar keçirməyə qadirdir.

NCW proqramının və FORCEnet konsepsiyasının müvəffəqiyyətlə həyata keçirilməsi idarəetmə orqanlarının avtomatlaşdırılması vasitələrinin, silahlanma və hərbi təminat sistemi ilə qarşılıqlı əlaqəsindən, eləcə də müxtəlif şəbəkələrin effektiv inteqrasiyasından, ilk növbədə hərbi qərargahların, bu qərargahlar arasında əlaqələrin, kəşfiyyat və müşahidələrin avtomatlaşdırılması sistemlərindən asılıdır [72].

Bu gün NCW konsepsiyalarının həyata keçirilməsi prosesində yerinə yetirilən əsas proqramlar bunlardır [73]:

- Birgə komandanlıq və idarəetmə orqanlarının təkmilləşdirilməsi (Joint Command and Control - JC^2);
- Birgə çevik komandanlıq və mümkün idarəetmə orqanlarının təkmilləşdirilməsi (Deployable Joint Command and Control Capability – DJC^3);
- Hərbi Dəniz Qüvvələrinin və Quru Qoşununun kəşfiyyat informasiyasının toplanması, emalı, paylanması üzrə ümumi avtomatlaşdırılmış sistemin təkmilləşdirilməsi (Distributed Common Ground System-Navy - DCGS-N).

ABŞ mütəxəssislərinin fikrincə göstərilən proqramlar İM-in müvəffəqiyyətlə həyata keçirilməsində əsas şərtdir. Bu gün Pentaqon tərəfindən işlənmiş İM konsepsiyası iki istiqamətdə reallaşdırılır: dövlət strukturlarında və hərbi sahələrdə həyata keçirilən informasiya əməliyyatları.

Dövlətlər arasında aparılan İM-də əsas məqsəd rəqib dövlətlərin mövqelərinin zəiflədilməsi, onların milli-dövlət dayaqlarının dağıdılması, cəmiyyətin gündəlik həyatının siyasi, diplomatik, iqtisadi və sosial sahələrinə təsir etməklə dövlət idrəçiliyi sisteminin pozulması, psixoloji əməliyyatların, təxribatçı və digər pozucu təbliğat aksiyalarının aparılması təşkil edir. Dövlət səviyyəsində İM ABŞ-ın milli maraqlarının

qorunması, beynəlxalq münaqişələr haqqında əvvəlcədən xəbərdarlıq, provokasiya və terror aksiyalarının, eləcə də milli informasiya resurslarının təhlükəsizliyinin təminatı məsələlərində vacib faktordur.

Hərbi sahədə aparılan informasiya əməliyyatları hərbi qüvvələr daxilində zonalar üzrə komandanlıqların həyata keçirdikləri razılaşdırılmış kompleks tədbirlərin və hərbi əməliyyatların tərkib hissəsini təşkil edir. Hərbi komandanlıqların əsas vəzifəsi qarşı tərəf üzərində informasiya üstünlüyü əldə etməyə və öz idarəetmə sistemlərinin mühafizəsinə istiqamətlənir. Bunun üçün hüquqi, mənəvi, diplomatik, siyasi və hərbi normalara formal riayət olunmaqla sərəncamda olan istənilən hərbi və texniki vasitələrdən və güclərdən istifadə etməklə informasiya əməliyyatlarını daha uğurla həyata keçirmək mümkündür.

ABŞ-ın və NATO mütəxəssislərinin birgə işlədikləri İM konsepsiyalarının hazırlanmasında C^4I (Command, Control, Computer, Communications and Intelligence) və C^4IFTW (Command, Control, Computer, Communications and Intelligence For The Warrior) hərbi-texniki konsepsiyalarından geniş istifadə edilir [74].

C^4I – komandanlıq, idarəetmə, kompyuter, kommunikasiya və kəşfiyyat sistemlərinin razılaşdırılmış inkişafı konsepsiyasının əsas tərkibini informasiyanın toplanması, emalı, saxlanması və ötürülməsi üzrə müxtəlif əməliyyatların avtomatlaşdırılması təşkil edir.

Konsepsiya çərçivəsində müxtəlif tipli informasiyanın axtarışı, təyini, emalı və paylanması funksiyalarının avtomatlaşdırılmasının yüksək səviyyəsinə nail olmaq planlaşdırılır. Bununla yanaşı, konsepsiyada elektron poçt,

telekonferensiyalar və s. xidmətlərdə də yüksək effektə nail olmaq nəzərdə tutulmuşdur. C^4I konsepsiyasında həmçinin ekspert sistemlərin və hərbi əməliyyatların moddelləşdirmə vasitələrinə, neyrokompyuter və yüksək göstəricilərə malik kompyuter texnologiyalarından istifadə edən, avtomatlaşdırma üçün nəzərdə tutulmuş texniki vəsaitlər kompleksinin tətbiqinə böyük yer verilir.

C^4IFTW – müharibə şəraiti üçün nəzərdə tutulmuş komandanlıq, idarəetmə, kompyuter, kommunikasiya və kəşfiyyat sistemlərinin birgə və funksional inteqrasiyası konsepsiyası daha böyük ordu hissələrinin hərbi əməliyyatlara başlaması üçün müəyyən şəraiti təmin edən qlobal informasiya–idarəetmə infrastrukturunun təşkili nəzərdə tutur.

İM-in effektiv və minimum itki ilə aparılması, eyni zamanda informasiya silahından düzgün istifadə edilməsi üçün yüksək ixtisaslı kadrlar tələb olunur. ABŞ-da bu kadrların hazırlanması ilə Vaşinqtonda yerləşən Milli Müdafiə Universiteti məşğul olur. Universitetdə İM problemləri üzrə xüsusi ixtisas yaradılmışdır və həmin ixtisas üzrə ABŞ-ın silahlı qüvvələrinin bütün növlərindən nümayəndələr təhsil alır.

ABŞ-ın Milli Müdafiə Universitetinin proqramlarında İM-in aşağıdakı formalarına üstünlük verilir [75]:

- Radioelektron müharibə *(Electronic Warfare, EW)*;
- Psixoloji müharibə *(Psychological Operations, PSYOPS)*;
- Kəşfiyyat vasitələrindən istifadə etməklə aparılan İM *(Intelligence service)*;
- Hakerlərlə müharibə *(Hackerwar)*;
- Kibernetik müharibə *(Cyberwar)*.

Gələcəkdə ABŞ-ın Müdafiə Nazirliyinə aid təhsil müəssisələrində və bəzi mülki ali təhsil ocaqlarında İM-in və

informasiya hərbi əməliyyatlarının aparılması məsələləri üzrə kursların keçirilməsi planlaşdırılır. Bu kurslarda qarşı tərəfin tətbiq etdiyi informasiya silahının dəf edilməsi məsələləri ön plandadır. Odur ki, "informasiya silahından müdafiə" və "şəbəkə və sistemlərin administratoru" ixtisasları üzrə mütəxəssislərin hazırlanması planlaşdırılır. ABŞ müasir dövrdə siyasi və hərbi üstünlük əldə etmək üçün informasiya silahından düzgün istifadəyə xüsusi önəm verir.

ABŞ da daxil olmaqla bir sıra inkişaf etmiş ölkələrdə "İnformasiya Silahlı Qüvvələri"-nin yaradılması bir daha sübut edir ki, müasir dövrdə İM problemləri ölkələrin informasiya təhlükəsizliyində mühüm rol oynayır. Eyni zamanda son illər ABŞ-da kiberəsgərlər adlanan xüsusi təlim görmüş döyüşçülər də hazırlanır. Bu gün ABŞ-ın müdafiə nazirliyinin direktivlərində İM-ə hazırlıq qaydaları təffərrüatı ilə şərh edilir [72].

Nəticə etibari ilə, ABŞ hərbi dairələrində İM-in yaratdığı fəsadları kütləvi dağıntılarla eyniləşdirirlər. İnformasiya silahlarına olan münasibətdə isə bildirilir ki, bu silahların təsir spektri insanların psixi sağlamlığına vurulan zərbədən, kompyuter şəbəkələrinə virusların ötürülməsi və informasiyanın məhv edilməsinə qədər bütün sahələri əhatə edir.

Araşdırmaların nəticəsi olaraq İM konsepsiyasının reallaşdırılması məqsədi ilə (həm hücum, həm də müdafiə planında) ABŞ-da görülən tədbirləri müəyyən mərhələlərə bölmək mümkündür:

1. Təhlükəsizlik üzrə komissiya yaradılmışdır. Komissiya 1993-1994-cü illər üzrə İM problemlərini araşdırmış və bu qərara gəlmişdir ki, bu onillikdə və çox ehtimal var ki, gələcəkdə informasiya hücumlarına məruz qalan əsas

sahələr informasiya sistemləri və kompyuter şəbəkələri olacaqdır. Belə ki, "verilənlərin ötürülməsi şəbəkələri döyüş meydanına çevrilirlər. İnformasiya silahını, strategiyasını və tətbiq taktikasını gələcəkdə əsaslı surətdə tədqiq etmək lazım gələcəkdir. Onlar hücum və müdafiə zamanı "elektron sürəti ilə" istifadə ediləcəkdir. İnformasiya texnologiyaları bir güllə belə atmadan geosiyasi böhranların həllini təmin edəcək, insan itkisinin və dağıntıların qarşısını alacaqdır. Milli təhlükəsizliyin təmin olunması üzrə apardığımız siyasət və onun həyata keçirilməsi İM-də bizim imkanlarımızın qorunmasına və ABŞ-a qarşı çıxan bütün ölkələrin İM-də uduzması üçün mümkün şəraitin yaradılmasına istiqamətlənmişdir".

2. İM-ə hazırlıq və aparılması strategiyası araşdırılmış və təsdiq edilmişdir. ABŞ-ın hərbi qüvvələrinin bütün növlərində İM aparmaq üçün xüsusi mərkəzlər yaradılmışdır (İnformasiya hərbi əməliyyatlar mərkəzi).
3. ABŞ hərbi qüvvələrinin bütün növlərində İM-in aparılması üzrə xüsusu bölmələr yaradılmış və İM üzrə zabit vəzifələri təyin edilmişdir. Bütün hərbi təlim müəssisələrində İM üzrə xüsusu kurslar yaradılmış və İM aparmaq üçün mütəxəssislərin hazırlanması həyata keçirilir (ilk buraxılış 1995-ci ildə olmuşdur).
4. ABŞ-ın hərbi qüvvələrində İM ilə bağlı təlimlər və praktiki işlər həyata keçirilir. İnformasiya silahı tətbiq etməklə konkret əməliyyatlar işlənir.
5. ABŞ hökuməti tərəfindən İM problemləri üzrə 5 beynəlxalq konfrans keçirilmişdir.
6. Milli informasiya infrastrukturunun illik təkmilləşdirilməsi üzrə tədbirlər görülür. ABŞ hökuməti

nümayəndələrinin verdiyi qiymətə görə Milli informasiya infrastrukturunda gizli informasiyanın 80%-i dövr edir.

7. Yeni növ informasiya silahları və onların milli strukturlarda tətbiqi üçün nəzərdə tutulan maliyyə xərcləri hər il artırılır. Ekspertlərin hesablamalarına görə bu xərclər kosmik və nüvə-raket xərclərindən artıqdır.

İM nəzəriyyəsinə ABŞ tərəfindən yanaşmanın əsasını informasiya əməliyyatları ilə bağlı hərbi-nəzəri araşdırmalar və informatika sahəsində texnoloji nailiyyətlərdən kompleks istifadə təşkil edir. Müasir dövrdə ABŞ digər ölkələrlə müqayisədə ən yeni radioelektron sistemlərdən və kompyuter texnologiyalarından istifadədə üstünlük təşkil edir. Bu dövlət hər zaman siyasi, iqtisadi, sosial və hərbi sahələrdə olduğu kimi dünya informasiya infrastrukturunda da birinciliyi əldə saxlamağa səy göstərir.

Son zamanlar Rusiya Federasiyasında informasiya qarşıdurması və təcavüzü ilə bağlı müxtəlif araşdırmalar aparılır. Araşdırmalarda psixoloqlar, hərbçilər, siyasətçilər və informasiya texnologiyaları mütəxəssisləri iştirak edirlər. Rusiyada İM probleminin araşdırılması ilə əlaqədar nəşr olunan ədəbiyyatları bir-neçə qrupa bölmək olar.

Birinci qrupa daxil olan ədəbiyyata dövlətin ali orqanlarının fəaliyyətini reqlamentləşdirən hüquqi sənədlər və informasiya siyasəti sahəsində idarəçilik daxildir [75, 76]. Bu sənədlərdə İM-in ümumi konsepsiyası göstərilsə də, mülki şəxslərə və ölkənin müdafiə sisteminə qarşı yönəlmiş informasiya əməliyyatlarının mümkün fəsadların analizi verilməmişdir.

İkinci qrupa Rusiya alimlərinin təhlükəsizlik nəzəriyyəsi və RF-nın milli təhlükəsizliyi mövzusunda elmi araşdırmalarını

və hərbi təhlükəsizlik məsələləri ilə məşğul olan mütəxəssislərin fundamental tədqiqatlarını aid etmək olar. Burada əsas yeri elə elmi əsərlər tutur ki, onlarda nəzəri-metodoloji nəticələr daha konkretdir və informasiya təhlükəsizliyi probleminə yönəlib. Bu işlərin bəzilərində informasiya-psixoloji təhlükəsizliyin müxtəlif aspektlərinə baxılmışdır [33, 34, 35].

Üçüncü qrup elmi işlər informasiya siyasəti, informasiya qarşıdurması və hücumları problemlərinə aiddir. Problemlə bağlı elmi əsərlərdə informasiya fəzasında qarşıdurma məsələlərinin geniş spektrli analizi öz əksini tapmışdır [27, 28, 39, 63].

Belə tədqiqatlar bir daha sübut edir ki, artıq Rusiyada tətbiqi elmin yeni sahəsi – İM nəzəriyyəsi inkişaf etməkdədir. İM və informasiya təhlükəsizliyi məsələləri ilə əlaqədar 2006-cı ilin oktyabr ayından başlayaraq Rusiya Elmlər Akademiyası və Hərbi Elmlər Akademiyasının təsis etdikləri "Информационные войны" elmi jurnalı nəşr olunmağa başlamışdır.

İM yeni sahə olduğu üçün müxtəlif qabaqcıl ölkələrdə olduğu kimi, Rusiyada da İM texnologiyalarının araşdırılması və təhlili davam etməkdədir. Bununla əlaqədar Rusiya Federasiyasının İnformasiya Təhlükəsizliyi Doktrinasında bəzi ölkələrdə işlənmiş İM konsepsiyaları Rusiyanın təhlükəsizliyinə qarşı yönəlmiş xarici təsir mənbələrindən biri kimi göstərilmişdir [76].

Rusiya hərbi qüvvələrinin verdiyi qiymətə görə İM konsepsiyası aşağıdakıları nəzərə almalıdır [77]:

- dövlət və hərbi idarəetmənin infrastrukturunun elementlərinin məhv edilməsi *(komanda və idarə mərkəzlərinin məhvi);*
- informasiya və telekommunikasiya sistemlərinin elementlərinə elektromaqnit təsir *(radioelektron mübarizə);*
- əlaqə kanalları, eyni zamanda radiodalğalarla ötürülən informasiya axınlarının saxlanması və şifrə açma yolu ilə axtarılan informasiyasının əldə edilməsi, eləcə də xüsusi elektron qurğuların köməyi ilə informasiyaların oğurlanması və ya bloklanması *(radioelektron kəşfiyyat);*
- informasiya resurslarına icazəsiz müraciətin həyata keçirilməsi (proqram-aparat vasitələrindən istifadə etməklə qarşı tərəfin informasiya və telekommunikasiya sistemlərindəki müdafiə sisteminin sındırılması), sonradan onların dəyişdirilməsi, məhv edilməsi və ya oğurlanması, eləcə də bu sistemlərin normal fəaliyyətlərinin pozulması *(haker müharibəsi);*
- qərar qəbul edən şəxslərə və mülki əhalinin şüuruna, davranışına təsir etmək üçün qarşı tərəfin informasiya kanalları ilə və ya qlobal şəbəkələrdən istifadə etməklə dezinformasiyanın və təbliğat xarakterli informasiyanın təşkili və kütləvi yayılması *(psixoloji müharibə);*
- qorunmayan əlaqə kanalları vasitəsi ilə ötürülən açıq və marağa səbəb olan informasiyanın əldə keçirilməsi, eləcə də KİV-də nəşr olunan məlumatların emal edilməsi.

Rusiyanın Təhlükəsizlik Şurası tərəfindən işlənmiş "İnformasiya-psixoloji təhlükəsizliyin təmin olunması sahəsində dövlət siyasətinin əsasları" sənədində İM şəraitində dövlətin informasiya siyasətinə informasiya-psixoloji

təhlükəsizliyin təmini sisteminin mərkəzi komponenti kimi baxılır və bildirilir ki, bu gün kəskin informasiya-psixoloji münaqişələr şəraitində həyata keçirilən informasiya siyasətində istifadə olunan ümumi prinsip, vasitə və metodlardan istifadə effektiv deyil [24, 78].

Rusiya mütəxəssislərinin fikrincə, bu gün qloballaşma və informasiya qarşıdurmasının gizli formalarının inkişafı şəraitində informasiya siyasətində köklü dəyişikliklərə ehtiyac vardır.

İnformasiya münaqişələri və bu münaqişələrdən yaranan problemlər V.L. Manilovun, Y.L. Dosenko, Q.Q. Poçepsovun əsərlərində geniş tədqiq edilmişdir. Lakin bu sahədəki terminlər hələ də dəqiq təyin edilməmişdir. Hər bir müəllif mövzudan asılı olaraq müəyyən xüsusiyyətləri əsas götürərək bu və ya digər anlayışa öz tərifini təklif edir. Bu tərifləri müqayisə edərkən bəzən onların bir-birilərindən kəskin fərqləndiyi də müşahidə edilir.

İM sahəsində geniş araşdırmaları ilə məşhur olan Rusiyalı politoloq İ.N.Panarinin bildirdiyinə görə: "İM müasir dünya siyasəti və iqtisadiyyatında siyasi, maliyyə və iqtisadi sahələrdə hökmranlığı əldə etmək üçün əsas vasitədir". Panarinin fikrincə, hərbi münaqişələrdə ənənəvi silahların istifadəsi ilə yanaşı, informasiya vasitələri və üsullarından istifadə edilə bilər. Panarin əsərlərində sübut etməyə çalışır ki, İM informasiya texnologiyalarının və hərbi silahların, həmçinin güclərinin kompleks birgə tətbiqidir.

Rusiyada İM-in digər təyinatları da vardır: İM milli strateji maraqlar daxilində, üstünlüyü əldə etmək məqsədi ilə qarşı tərəfin informasiyasına və informasiya sistemlərinə təsir edən kommunikasiya texnologiyalarıdır. Bir şərtlə ki informasiya

hücumuna başlayan tərəf öz informasiyasını və informasiya sistemlərini qorumaq iqtidarında ola bilsin. Bu təyinat İM-in mahiyyətini daha dəqiq və dolğun təsvir etməklə, onun ilk növbədə dövlət qərarlarının qəbulu mexanizmlərinə və informasiya mühitinə nəzarətə yönəldiyini göstərir.

Rusiyalı mütəxəssislərin fikirlərinə görə, İM-i üç əsas mərhələyə bölmək olar [79]:

1. Məqsədin təyin edilməsi (İM nə üçün lazımdır və nəticədə nə əldə ediləcəyi gözlənilir);
2. Strategiyanın təyin edilməsi. Burada İKT-nin dörd baza kompanenti nəzərə alınmalıdır: informasiyanın hazırlanması, informasiyanın yönələcəyi kommunikasiya kanalının təyin edilməsi, informasiyanın təsiri altına düşəcək auditoriyanın müəyyənləşdirilməsi və İM texnologiyasının seçilməsi;
3. Taktiki fəaliyyət planının hazırlanması.

Rusiyada milli təhlükəsizlik məsələləri ilə əlaqədar informasiya təhlükəsizliyi üzrə bir sıra konseptual sənəd hazırlanmışdır. Bu sənədlərə ilk növbədə 2000-ci ilin sentyabr ayında qəbul olunmuş "Rusiya Federasiyasının informasiya təhlükəsizliyi doktrinası" və "Rusiya Federasiyasının milli təhlükəsizlik konsepsiyası" aiddir. Konsepsiyada ölkəyə qarşı gözlənilən informasiya təhlükəsi dəqiq təyin edilmişdir. Bunlara "bir sıra ölkələrin informasiya fəzasında qabaqcıl yerlərdən birini tutmağa can atması, Rusiyanı xarici və daxili bazardan sıxışdırıb çıxarması; bir sıra dövlətlər tərəfindən digər dövlətlərin informasiya fəzasına təhlükəli təsir vasitələrinin yaradılması; informasiya və kommunikasiya sistemlərinin normal fəaliyyətinin pozulması, eləcə də informasiya

resurslarının qorunması, onlara icazəsiz müdaxilənin həyata keçirilməsi" aiddir [80].

ABŞ-ın yanaşmasından fərqli olaraq bu doktrinada birinci yerdə əhalinin psixoloji təsirdən mühafizəsi problemi ön plana çəkilir. Doktrinanın həyata keçirilməsi və Rusiyanın informasiya təhlükəsizliyinin təmin edilməsi üçün RF-nın təhlükəsizlik şurasında İnformasiya Təhlükəsizliyi İdarəsi yaradılmışdır.

İM ilə bağlı problemlərin həllinə görə bu gün Rusiya Azərbaycandan öndə olsa da ABŞ-dan xeyli geri qalır. Rusiyanın informasiya infrastrukturu bir sıra səbəblərə görə ona qarşı ciddi təhlükə yarada biləcək İM texnologiyalarına qarşı davamsızdır. Rusiya Federasiyasının informasiya təhlükəsizliyi doktrinasında bu səbəblər açıq göstərilmişdir [76]:

- Rusiyanın informasiya təhlükəsizliyinin təmini sahəsində vahid dövlət siyasətinin olmaması;
- Rusiyanın informasiya təhlükəsizliyinin təmini ilə məşğul olan təşkilatların kifayət qədər maliyyələşdirilməməsi;
- Dünyanın aparıcı dövlətlərinin texnoloji sahədə inkişafının kəskin sürətlənməsi və bu dövlətlərlə rəqabətdə Rusiyanın informasiya texnologiyaları sahəsinin tab gətirə bilməməsi;
- Rusiyanın informasiya bazarının, onun ayrı-ayrı yerli və xarici informasiya infrastrukturlarının inhisara alınması;
- Rusiya informasiya infrastrukturunun yaradılması və inkişafı ilə əlaqədar yerli və xarici informasiya texnologiyalarından, informasiya mühafizəsi vasitələrindən, informasiyalaşma, telekommunikasiya və kommunikasiya vasitələrindən sertifikatsız istifadə.

Bu gün Rusiyada İM problemləri ilə Rusiyanın Müdafiə Nazirliyi, Xarici İşlər Nazirliyinin xüsusi şöbəsi, Rusiyanın Federal Təhlükəsizlik Xidməti, Rusiya Prezidenti yanında Hökumət Rabitəsi və İnformasiyası üzrə Federal Agentliyi və Rusiyanın informasiya texnologiyalarının yüksək texnoloji mühitində baş verən cinayətlərin araşdırılması ilə məşğul olan Daxili İşlər Nazirliyinin "P" idarəsi məşğul olur.

İM ifadəsi ilk dəfə hərbi sahədə yaransa da sonradan insan fəaliyyətinin digər sahələrini də əhatə etmişdir. İM ağır və təhlükəli fəaliyyət olub, həm sülh şəraitində, həm də qanlı, dağıdıcı hərbi əməliyyatlarla əlaqədar aparılır. Dünyanın müxtəlif dövlətlərində İM doktrinasını tərtib edən hərbi ekspertlər onun ayrı-ayrı istiqamətlərini çox aydın şəkildə təsəvvür edirlər: ştab müharibəsi, elektron müharibə, psixoloji əməliyyatlar və s.

Artıq dünya dövlətləri informasiyanın cəmiyyətdəki rolunu qiymətləndirərək özlərinə məxsus İM strategiyalarını yaratmağa nail olublar. Çin Xalq Respublikasında "informasiya müharibəsi" termini hərbi leksikonda çoxdan istifadə edilir. Çin mənbələrinin məlumatına görə, bu ölkənin İM strategiyasının hazırlanmasında tarixi, milli təsəvvürlər, strateji, operativ və taktiki səviyyədə döyüş planlaşdırılması, həmçinin Sun Tsızın 36 strateji məsləhətindən istifadə olunub. 2000-ci ildən isə Çinin hərbi məktəblərində bilavasitə informasiya əməliyyatlarının təşkilini həyata keçirən yüksək səviyyəli mütəxəssislərin hazırlanmasına başlanıb.

Bu gün Çin mütəxəssisləri İM-in vahid doktrinasının yaradılması üzərində işləyirlər. Faktiki olaraq, əgər hərbi sahədə inqilab hərbi təlimlərdə, strategiyada, ordunun təşkilində və hərbi əməliyyatlarda üstünlüyü əldə etmək imkanı yaradan

texnologiyaların köklü surətdə dəyişdirilməsi ilə bağlıdırsa, əminliklə söyləmək olar ki, dünyanın bütün ölkələri içərisində yalnız Çin və ABŞ kiberfəzada baş verən dəyişikliklərə təsir edə biləcək ölkələrdir.

Bu gün Çində İM sənaye cəmiyyətindəki texnoloji mübarizədən idarəetmə və qərarların qəbulu sistemləri uğrunda mübarizə, eləcə də bilik və intellekt uğrunda informasiya əməliyyatlarına keçid kimi qəbul edilir [81]. Çin "Şəbəkə gücləri" konsepsiyasını inkişaf etdirməkdədir [46]. Bu konsepsiyaya görə istənilən növ İM-də müvəffəqiyyətlə iştirak edə biləcək, sayları batalyondakı əsgərlərin sayı qədər olan, müxtəlif qabaqcıl dövlət universitetlərində, akademiyalarda və tədris mərkəzlərində təhsil almış yüksəkixtisaslı kompyuter ekspertlərindən ibarət "informasiya qoşunu"nun yaradılması vacibdir.

Böyük Britaniyada isə qeyd olunan məsələ ilə Dövlət Kommunikasiyalar Departamenti (State Department of Communications – SDC) məşğul olur. Bu departamentin şəxsi heyətinin sayı 6 min nəfərdir və ingilislər daha çox ABŞ-ın İM taktikasından istifadə edirlər. Bu taktikaya görə isə İM-də qarşı tərəfin informasiya sisteminə təsir göstərməklə öz informasiya infrastrukrunun və sisteminin mühafizəsi əsas şərtdir.

Böyük Britaniyada müəyyən dərəcədə kiberfəzadakı fəaliyyətlərə tətbiq edilməsi mümkün olan mövcud qanunlar əsasında ədliyyə strukturundan istifadə də nəzərdə tutulmuşdur (Regulation of Investigatory Powers Act – RIP). İM problemlərinin həlli üçün nəzərdə tutulmuş RIP konsepsiyası 2000-ci ildə qəbul edilmişdir. Bu konsepsiyaya görə informasiya sistemlərinə hücum əməliyyatına, nəticədən asılı olaraq adi cinayət hadisəsi kimi baxıla bilər. Bu isə Britaniya

hökumətinə istənilən elektron məktubun əldə edilməsinə, dövlət qulluqçusunun tələbi ilə şəxsi faylların şifrələrinin açılmasına icazə verir.

ABŞ mütəxəssislərindən fərqli olaraq almanlar İM-in tərkib hissəsi kimi KİV-in idarə olunmasına üstünlük verirlər, fransızlar isə İM konsepsiyasının – hərbi və iqtisadi olmaqla iki elementini əsas götürürlər. Əsasən iqtisadi sahəyə təsirləri nəzərə alan fransızlar ölkə və vətəndaşların kiberfəzadakı fəaliyyətinə nəzarət edən «Eşalon» aAdlı mühafizə sisteminin tətbiqinə nail olublar.

İnformasiya təhlükəsizliyi sahəsində ABŞ, Rusiya, Çin, Hindistan və Kuba daha inkişaf etmiş dövlətlərdən hesab olunurlar. Hazırda dünyanın bir çox ölkələri Birləşmiş Ştatların, Çinin və Rusiyanın informasiya-psixoloji təsirlərinə qarşı öz müdafiə sistemlərini işləyir və inkişaf etdirməkdədir. Məsələn, Fransada televiziya ilə nümayiş edilən xarici kinofilimlərin və verilişlərin həcmi ümumi proqramın 50 faizindən çox olmamalıdır. Bu metod bəzi Avropa dövlətləri tərəfindən də tətbiq edilir. Hesablamalara görə, hər il dünyada informasiya müharibələrinə 120 mlrd. dollar vəsait xərclənir.

Ekspertlərin fikrincə, bu gün ABŞ-ın dünya üzərində hegemon dövlətlərdən birinə çevrilməsi, onun informasiya fəzasında baş verən cinayətlərin və informasiya qarşıdurmalarının rolunun daha düzgün qiymətləndirilməsi ilə əlaqəlidir.

FƏSİL 3. İNFORMASİYA HÜCUMLARI

3.1. İnternet mühitində informasiya hücumlarının bəzi üsul və vasitələri haqqında

Bu gün informasiya qarşıdurmasında İnternetdən daha aktiv və hərtərəfli istifadə olunmaqdadır. Son illər İnternet istifadəçilərinin sıçrayışlı artımı ilə yanaşı cəmiyyətin siyasi aktivliyi və narahatlığı yeni fəaliyyət sahəsinin – İnternetdə informasiya hücumlarının çoxalmasına səbəb olmuşdur.

İctimai rəyin formalaşması və ya dəyişdirilməsində, siyasi, iqtisadi və hərbi qərarların qəbulunda, qarşı tərəfin informasiya resurslarına təsirində, dezinformasiyanın yayılması planında İnternet geniş imkanlara malikdir.

İnternetin nəhəng məlumat bazası hər saniyə yeni xəbərlərlə zənginləşir. İnternet genişləndikcə bu şəbəkə vasitəsilə dünyanın istənilən nöqtəsində yaşayan insanlarla virtual ünsiyyət qurmaq, məktublaşmaq, on-line rejimində keçirilən müxtəlif forumlarda iştirak etmək, kitab, jurnal və qəzetlərin elektron versiyalarını oxumaq, alış-veriş etmək, radio dinləmək, televiziya verilişlərinə tamaşa etmək, gündəlik hadisələr haqqında operativ məlumatlar almaq mümkündür. Bütün bunlar informasiya qarşıdurmasında və hücumunda İnternetdən ən geniş şəkildə istifadə etmək imkanları verir.

Müasir dövrdə informasiya hücumları ilə bağlı iki fikir formalaşmaqdadır. Tədqiqatçıların bir hissəsi informasiya hücumları dedikdə elə informasiya əməliyyatlarını nəzərdə tuturlar ki, bu zaman kompyuter İM-də bir silah kimi istifadə edilir [82]. İkinci qrup tədqiqatçılar isə informasiya hücumları dedikdə, informasiyanın avtomatlaşdırılmış emalında qanunsuz fəaliyyəti nəzərədə tuturlar. Bu zaman hücum obyekti kompyuter sistemində emal edilən informasiya hesab edilir,

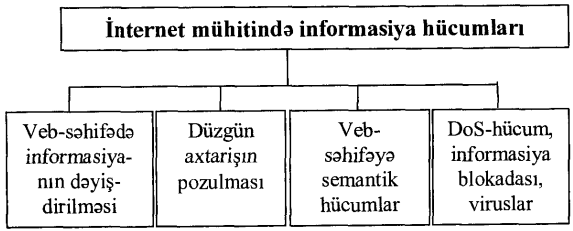
kompyuter isə İM zamanı informasiya hücumlarını təmin edən vasitə kimi qəbul edilir [83, 84]. Bir çox dövlətlərdə informasiya təhlükəsizliyi ilə bağlı qanunlarda bu yanaşma üstünlük təşkil edir.

İnformasiya hücumlarını ilk dəfə xüsusi informasiya təminatlarından istifadə edən hakerlər həyata keçirmişlər. Son dövrlərdə baş verən informasiya hücumları isə müxtəlif siyasi baxışların təbliği, dezinformasiya, "beyinlərin yuyulması" kimi məqsədlər üçün istifadə olunur. İnformasiya hücumları dedikdə:

- informasiya massivlərinin məhvi, təhrif edilməsi və ya oğurlanması;
- mühafizə sisteminin dəf edilməsi;
- qanuni istifadəçilərin müraciətlərinə məhdudiyyətlərin qoyulması;
- kompyüter sistemlərinin, texniki vasitələrin işlərinin pozulması;
- insan psixologiyasına təsir və s. nəzərdə tutulur.

İnternet mühitində informasiya hücumu dedikdə veb-səhifələrin dəyişdirilməsi, məhvi və ya serverlərdəki proqram təminatlarına, verilənlərin saxlandığı texniki qurğulara və şəbəkəyə yönəlmiş əməliyyatlar nəzərdə tutulur. Hücum əməliyyatlarında istifadə olunan informasiya silahlarını adi döyüş silahlarından fərqləndirən cəhət onların işlənməsi və tətbiqində baza biliklərini özündə cəmləmiş alqoritm və texnologiyalardan istifadəyə olunmasıdır. İnformasiya silahı insanın şüuruna təsir edərək təfəkkür matrisini [85] dəyişi, əvvəlcədən verilmiş parametrlər (düşünmə tərzi, mənəvi ehtiyac, özünüifadə formaları və s.) üzrə şəxsiyyəti formalaşdırır, qarşı tərəfin idarəetmə sistemlərini məhv edir və ya nəzarətdə saxlayır.

İnternet mühitində müşahidə olunan əsas informasiya əməliyyatları veb-səhifələrə və şəbəkənin normal fəaliyyətinə yönəlmiş müxtəlif tipli hücumlardır (şəkil 2):



Şəkil 2. İnternet mühitində informasiya hücumları

1. Veb-səhifələrdə informasiyanın bir hissəsinin və ya bütünlükdə digəri ilə əvəz edilməsi qlobal şəbəkədə ən geniş yayılan hücumlardandır. Bu üsuldan siyasi və hərbi münaqişələr zamanı daha geniş istifadə edilir. Bununla informasiya hücumuna başlayan tərəf nəzəri özünə cəlb edərək, informasiya qarşıdurmsında geniş imkanlara malik olduğunu nümayiş etdirməyə və ya siyasi mövqeyini əsaslandırmağa çalışır.

2. İnternet mühitində axtarışın pozulması zamanı şəbəkədə eyni açar sözə görə yanlış informasiya daşıyan saytların axtarış sistemlərində qeydiyyatdan keçməsi, eləcə də hiperkeçidlərin digər ünvanlara – qarşı tərəfin xüsusi hazırladığı səhifələrə yönəldilməsi müşahidə olunur.

3. İnternetdə baş verən informasiya qarşıdurmasında semantik hücumlar xüsusi yer tutur. Bu əməliyyat zamanı əvvəlcədən hazırlanmış xüsusi informasiyanın (hiperkeçidlərin, şəkillərin və s.) veb-səhifədə yerləşdirilməsi həyata keçirilir.

Belə hücumlara adətən tez-tez müraciət olunan saytlar məruz qalır.

4. İnternetdə təsadüf olunan digər əməliyyat şəbəkədə struktur elementlərinin funksionallığında effektivliyin azaldılması və ya sıradan çıxarılmasıdır. Şəbəkənin ayrı-ayrı elementlərinin fəaliyyətinin effektivliyini aşağı salan üsullardan ən çox istifadə edilənlər şəbəkənin elektron məktublarla "bombardıman" edilməsi, xidmətdən imtina ilə bağlı hücumlar (DoS hücumlar, *Denial of Service Attack*) və kompyuter viruslarının tətbiqidir [86]:

– şəbəkənin elektron məktublarla "bombardıman" edilməsi üsulu İnternetdə informasiya blokadasına səbəb olur. Belə ki, kiçik zaman intervalında eyni ünvana çoxlu sayda elektron məktubların göndərilməsi istifadəçilərin məxsus olduqları informasiyanı əldə etmək imkanını çətinləşdirir və ya sıfra endirir. Belə hücumlar zamanı şəbəkə istifadəçilərinə xidmət göstərən serverin normal fəaliyyətinin pozulması halları üstünlük təşkil edir;

– DoS hücumlar bir ünvana çoxlu sayda məktubların göndərilməsi və nəticədə veb-sayta olunan həddən artıq müraciətlərin generasiyasını nəzərdə tutur. DoS hücumlar nəticəsində xidmət göstərən serverin sürəti aşağı düşür və ya onun normal fəaliyyəti tamamilə pozulmuş olur;

– kompyuter viruslarının tətbiqi şəbəkə müharibələrində ən populyar üsullardandır. Bu gün müxtəlif növ xüsusi kompyuter virusları işlənməkdədir.

İnternetdə informasiya qarşıdurması vasitələrinin, yəni informasiya silahlarının universallığı, gizliliyi, çoxvariantlılığı, təsirin radikallığı, təminatın kifayət qədər zaman və məkan seçimi, nəhayət, əlverişli olması onları həddən artıq təhlükəli

edir. Bu xüsusiyyətlər qlobal şəbəkədə İM-in gizli aparılması üçün uyğun şərait yaradır. İnformasiya qarşıdurması hərbi, iqtisadi, bank, sosial və digər sahələri əhatə edir və aşağıdakı məqsədləri daşıya bilər:

- İdarəetmə strukturlarının, nəqliyyat axınının və kommunikasiya vasitələrinin normal fəaliyyətinin pozulması;
- çoxhissəli texnoloji əlaqələri və qarşılıqlı hesab sistemlərini pozmaqla, valyuta-maliyyə fırıldaqları həyata keçirməklə ayrı-ayrı müəssisələrin, bankların, müxtəlif istehsal sahələrinin fəaliyyətlərinin məhdudlaşdırılması və ya tamam təcrid edilməsi;
- təhlükəli maddələr və enerjinin yüksək konsentrasiyaları ilə əlaqəli olan texnoloji proseslərin və obyektlərin düzgün idarə olunmaması nəticəsində ərazidə iri texnogen qəzaların təşkili;
- insanların şüuruna müəyyən təsəvvürlərin, davranışların və əxlaqi stereotiplərin kütləvi yönəldilməsi və yayılması;
- əhali arasında hərcmərcliyin və narazılığın, eləcə də ayrı-ayrı sosial qruplar arasında destruktiv fəaliyyətlərin təşkil edilməsi.

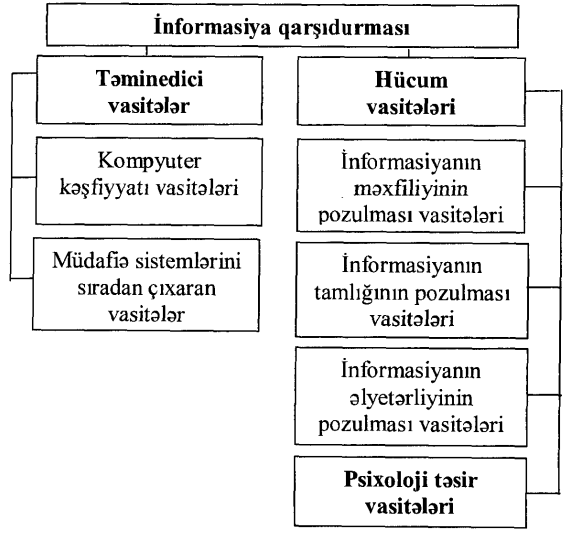
İnternet mühitində informasiya qarşıdurması müxtəlif strukturlar tərəfindən həyata keçirilir:

- dövlət təşkilatlarına aid kompyuter və əlaqə sistemlərində idarəetmə funksiyalarını yerinə yetirən strukturlar;
- ordunun və hərbi texnikanın idarə edilməsi məsələləri ilə, eləcə də hərbi qüvvələrin maraqlarına uyğun olan informasiyanın yığılması və emalı ilə məşğul olan hərbi informasiya infrastrukturları;

- bankların, nəqliyyat və istehsal müəssisələrinin informasiya və idarəetmə strukturları.

Ümumi halda informasiya qarşıdurması vasitələrini iki yerə ayırmaq olar: təminedici və hücum vasitələri.

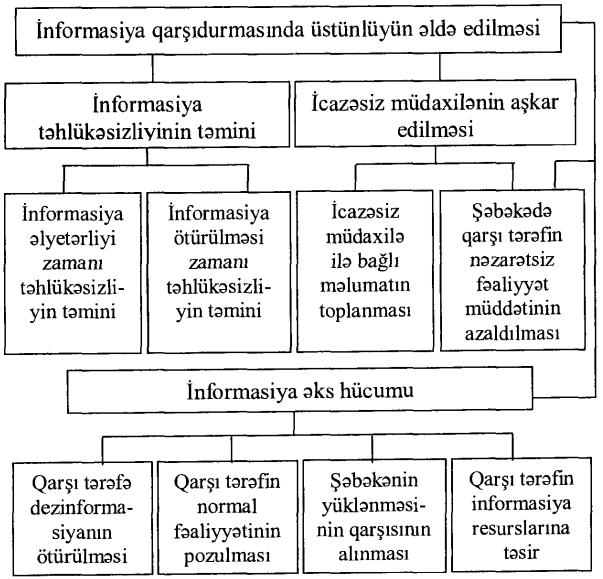
Təminedici informasiya vasitələri ilə əks tərəfin informasiya müdafiəsi vasitələrinə təsir həyata keçirilir. Təminedici informasiya vasitələrinin tərkibinə kompyuter kəşfiyyatı və kompyuter şəbəkəsinin müdafiə sistemlərini sıradan çıxaran vasitələr daxildir (şəkil 3).



Şəkil 3. İnformasiya qarşıdurması vasitələri

3.2. İnformasiya hücumlarının reallaşdırılması mexanizmləri

İnformasiya qarşıdurmasında üstünlüyün əldə edilməsi yalnız bir sıra şərtlərin ödənməsi nəticəsində həyata keçirilə bilər: informasiyanın təhlükəsizliyinin təmini, icazəsiz müdaxilələrin təyini və qarşı tərəfin informasiya hücumlarının qarşısını almaqla əks-hücumun həyata keçirilməsi. Bu məsələləri həll etmək üçün kompyuter şəbəkəsində informasiya qarşıdurmasının hər üç aspekti reallaşdırılmalıdır (şəkil 4).



Şəkil 4. İnformasiya qarşıdurmasıda məqsəd və vəzifələr

İnformasiya hücumları adətən əvvəlcədən müəyyən olunmuş mərhələlərlə yerinə yetirilməlidir: informasiyanın toplanması, informasiya hücumunun həyata keçirilməsi, hücumun başa çatdırılması. Çox zaman informasiya hücumu dedikdə ikinci mərhələ nəzərdə tutulur, informasiyanın toplanması və hücumun başa çatması əməliyyatları isə informasiya hücumuna aid edilmir. Lakin müşahidələr göstərir ki, bu mərhələlərin hər biri ayrı-ayrılıqda informasiya hücumunu təşkil edir. Məsələn, hücumdan öncə informasiyanın toplanması informasiya hücumunun nəticəsini müəyyən edən əsas amildir.

İnformasiya hücumuna keçməzdən öncə hücumun məqsədi müəyyən edilməli və hədəf seçilməlidir. Yalnız ondan sonra hədəf haqqında informasiya toplanır. Hədəf haqqında informasiya dedikdə əməliyyat sisteminin tipi, açıq portlar və şəbəkə serverləri, yüklənmiş sistem və tətbiqi proqram təminatları haqqında məlumat, şəbəkə topologiyasının öyrənilməsi və s. nəzərdə tutulur. Daha sonra hücum ediləcək sistemin "zəif" yerləri identifikasiya edilməlidir.

İnformasiya hücumunun ikinci mərhələsi olan hücumun həyata keçirilməsi əməliyyatı özü də iki mərhələdə baş verir: nüfuz etmə və nəzarət. Nüfuz etmə dedikdə şəbəkənin müdafiə vasitələrinin dəf edilməsi nəzərdə tutulur. Bu isə öz növbəsində müxtəlif üsullarla realizə edilir: serverin boşluqlarının müəyyən edilməsi, elektron poçtla zərərli proqramların göndərilməsi, Java apleti, adminstratorun parolunun ələ keçirilməsi və s. Nüfuz edildikdən sonra hücuma məruz qalan şəbəkə xüsusi proqram təminatlarının tətbiqi nəticəsində nəzarətə alınır.

İnformasiya hücumunu həyata keçirən tərəf iki məqsəd güdür: şəbəkəyə və orada saxlanılan informasiyaya icazəsiz

müdaxilə və şəbəkəni ələ keçirəndən sonra onunla informasiya mübadiləsi aparan digər şəbəkələrə nəzarət. İkinci əməliyyat hücum edənin aşkar edilməsini çətinləşdirir və ya mümkünsüz edir. Hücum başa catdırıldıqdan sonra görüləcək növbəti əməliyyat "hücum izlərinin" gizlədilməsidir. Bunun üçün şəbəkənin qeydiyyat jurnalında müəyyən yazıların pozulması, hücum edən sistemin ilkin vəziyyətə gətirilməsi və s. işlər görülməlidir.

Kompyuter şəbəkəsində baş verən informasiya hücumlarının təsnifatını aparmaq üçün şəbəkə təhdidlərinin təyin edilməsi vacibdir:

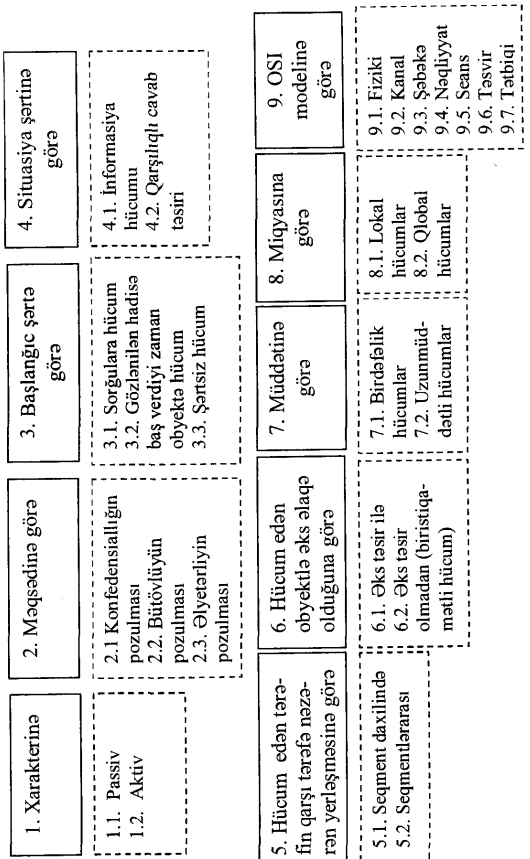
1. Uzaq məsafədən nüfuzetmə (*remote penetration*). Bu hücum nəticəsində şəbəkədən istifadə etməklə hücuma məruz qalmış kompyuteri idarə etmək mümkündür. Məsələn, NetBus və ya BackOrifice.
2. Lokal nüfuzetmə (*local penetration*). Bu tip hücumlar şəbəkəyə icazəsiz müdaxiləni təmin edir. Məsələn, GetAdmin.
3. Uzaq məsafədən xidmətdən imtina (*remote denial of service*). İnternetdən hücum nəticəsində serverin həddən artıq yüklənməsi və ya normal fəaliyyətinin pozulması.
4. Xidmətdən lokal imtina (*local denial of service*). Daxil olduqları kompyuterin normal fəaliyyətinin pozulması və ya həddən artıq yüklənməsi. Belə hücumlara mərkəzi prosessoru sonsuz sayda əməliyyatlarla yükləyən ziyanlı apletləri misal göstərmək olar. Nəticədə prosessorda sorğuların emalı mümkün olmur.
5. Şəbəkə skanerləri (*network scanners*). Bu proqramlar şəbəkə topologiyasını analiz edərək hücum üçün əlyetən serverləri aşkar edirlər. Məsələn, nmap sistemi.

6. Boşluq skaneri (*vulnerability scanners*). Hücumu həyata keçirmək üçün istifadə olunan və şəbəkədə boşluqları axtaran xüsusi zərərli proqramalar. Məsələn, SATAN və ya ShadowSecurityScanner.
7. Parolların sındırılması (*password crackers*). İstifadəçi parollarının təyini xüsusi proqramlarla həyata keçirilir. Məsələn, Windows üçün L0phtCrack, Unix üçün Crack.
8. Protokol analizatoru (*sniffers*). Şəbəkə trafikini nəzarətdə saxlayan proqramlar vasitəsilə lazım olan informasiya (kredit kartlar, istifadəçi parolu haqqında informasiya və s.) əldə edilərək informasiya hücumlarında istifadə olunur. Məsələn, Microsoft Network Monitor, LanExplorer.

Internet Security Systems Inc. şirkəti informasiya hücumlarını təsnif edərkən onları beş əsas kateqoriyaya ayırmışdır [86]:

1. İnformasiyanın toplanması (*Information gathering*);
2. İcazəsiz müdaxilə təşəbbüsləri (*Unauthorized access attempts*);
3. Xidmətdən imtina (*Denial of service*);
4. Şübhəli aktivlik (*Suspicious activity*);
5. Sistem hücumları (*System attack*).

İlk 4 kateqoriya üzaq məsafədən hücumlara, sonuncu kateqoriya isə şəbəkədə həyata keçirilən xidmətdən lokal imtina hücumlarına aiddir. İnformasiya hücumlarının növləri və səbəbləri müxtəlif olduğundan onların təsnifatı da müxtəlif istiqamətlərdə aparılmalıdır: hücum xarakterinə, məqsədinə, başlanğıc şərtə, situasiya şərtinə, yerləşməsinə, hücum müddətinə, hücum miqyasına və OSI modelinə görə (şəkil 5).



Şəkil 5. İnformasiya hücumlarının təsnifatı

Kompyuter şəbəkələrinin və bu şəbəkələrdəki informasiya sistemlərinin iş qabiliyyəti yalnız qurğuların etibarlılığından deyil, həm də onun işini pozmağa yönəlmiş məqsədyönlü əməliyyatlara qarşı davam gətirmək qabiliyyətindən asılıdır. Çox zaman informasiya hücumlarına dayanıqlı sistemin yaradılması vaxt itkisinə və müəyyən resursların sərfinə səbəb olur. Digər tərəfdən, məlumdur ki, informasiya sistemi nə qədər möhkəm mühafizə olunursa, ondan istifadə də bir o qədər narahatlıq yaradır. Bu zaman informasiya sisteminin əsas funksiyalarından istifadə müəyyən çətinliklərə səbəb olur. Bu çatışmazlıqları aradan qaldırmaq üçün kompyuter şəbəkəsinin təhlükəsizliyini təmin edən sistemlərə qoyulan əsas tələblərdən biri qorunan informasiya sisteminin əlyetərliyinə mane olmamaqdır.

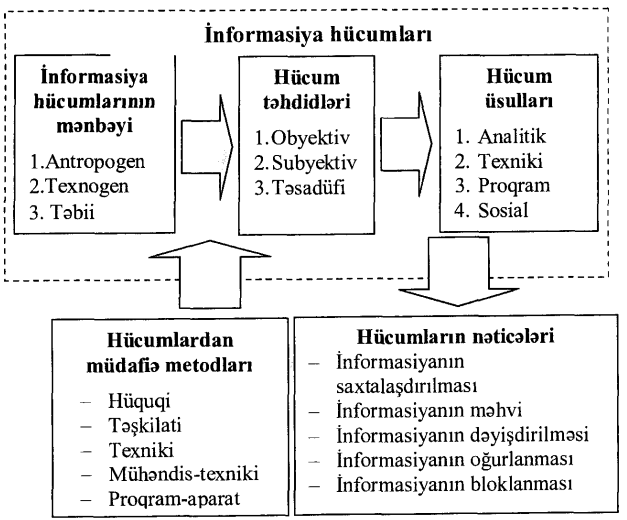
Kompyuter şəbəkəsinin təhlükəsizliyini təmin etmək üçün, ilk növbədə, bütün mümkün təhdidlər içindən konkret vəziyyət üçün daha çox ehtimal olunan təhdidləri seçmək və təsnifatlandırmaq lazımdır. Bunun üçün müəyyən üsuldan istifadə etmək lazımdır:

1. Artıq baş vermiş hücumlar haqqında məlumatların toplandığı verilənlər bankından istifadə edilməsi;
2. Müxtəlif mənbələrdə toplanmış hücumlar haqqında verilənlərin (metaverilənlərin) analitik emal edilməsi;
3. Ehtimal olunan bütün informasiya hücumlarını təhlil edən və nəzərə alan metodoloji vəsaitlərin hazırlanması.

İnformasiya hücumlarının analizi və mümkün variantların qiymətləndirilməsi metodologiyası bu hücumların modelinin yaradılması, onların analizi, təsnifatı və mənbələrinin müəyyənləşdirilməsi, qiymətləndirilməsi və realizə metodlarına əsaslanmalıdır. Bu zaman əsas üç məsələ həll edilməlidir:

1. Sistemə olan informasiya təhdidlərinin modelinin müəyyən edilməsi;
2. Sistemin iş prinsipində ən zəif nöqtələrin üzə çıxarılması;
3. Sistemdə baş verən icazəsiz müdaxilələrin müəyyən edilməsi.

İnformasiya hücumunu aşkarlamaq üçün ilk növbədə informasiya təhlükəsizliyini pozan prosesin ümumi sxemini müəyyənləşdirmək lazımdır. Bu sxemdə əməliyyatlar "hücum mənbəyi – təhdid – hücum üsulu – nəticə" məntiqi ardıcıllığına əsasən həyata keçirilir (şəkil 6).



Şəkil 6. İnformasiya hücumları zamanı proseslərin ardıcıllığı

İnformasiya hücumlarında istifadə olunan proqram və texniki vasitələr – informasiya silahları qarşı tərəfin informasiya resurslarına təcavüzü həyata keçirmək üçün nəzərdə tutulmuşdur. Hücum üçün nəzərdə tutulmuş informasiya silahı kimi aşağıdakıları göstərmək olar:

- proqramlara daxil olmaqla çoxalan, şəbəkə ilə ötürülən, idarə sistemlərini sıradan çıxaran kompyüter virusları;
- məntiqi bomba – hərbi və ya mülki infrastruktura əvvəlcədən tətbiq edilmiş xüsusi proqram təminatıdır, siqnal və ya müəyyən edilmiş zamanda həmin proqram işə düşür;
- kompyuter şəbəkəsində informasiya mübadiləsinin qarşısının alınması vasitələri, dövlət və hərbi idarə kanallarında informasiyanın saxtalaşdırılması;
- mətn proqramlarının neytrallaşdırılması vasitələri;
- obyektin proqram təminatına bilərəkdən müxtəlif növ səhvlərin daxil edilməsi.

İnformasiya hücumu vasitələri müxtəlif olduğu kimi, hücumun nəticələri də müxtəlif olur:

1. *İnformasiyanın saxtalaşdırılması.* İnformasiyanın saxtalaşdırılması kompyuterdə saxlanılan informasiyaya icazəsiz müdaxilə nəticəsində həyata keçirilir. İcazəsiz müdaxilə adətən, başqasının adından istifadə etməklə, texniki qurğuların fiziki ünvanlarını dəyişməklə, hər hansı məsələnin həllindən sonra yaddaşda qalan informasiyadan istifadə etməklə, proqram və informasiya təminatının modifikasiyası, informasiya daşıyıcısının oğurlanması, verilənlərin otürülməsi kanalına yazı aparatının qoşulması ilə həyata keçirilir.

Kompyuterdə saxlanılan informasiyaya müdaxilə edən şəxs çox zaman özünü qanuni istifadəçi kimi təqdim edir.

Autentifikasiyaya (məsələn, fiziologi xarakterlərə görə: barmaq izləri, gözün qüzeyli qişası, səs və s.) malik olmayan sistemlər bu növ müdaxilə qarşısında acizdirlər. Belə müdaxiləni həyata keçirmək üçün ən sadə üsul qanuni istifadəçilərdən parolun və ya digər identifikasiya məlumatlarının oğurlanmasıdır.

2. *İnformasiyanın məhvi.* İnformasiyanın məhvi onun tamamilə və ya qismən təyinatı üzrə istifadə üçün yararsız hala salınmasıdır. İnformasiyanın məhvi əsasən, müxtəlif kompyuter virusları vasitəsilə həyata keçirilir.

3. *İnformasiyanın dəyişdirilməsi.* Son illər İM-də informasiyanın dəyişdirilməsi ilə bağlı əməliyyatlar daha çox yayılmışdır. İnformasiyanın dəyişdirilməsi icazəsiz müdaxilənin bir istiqaməti hesab edilir. Fərq yalnız ondan ibarətdir ki, bu növ informasiya hücumu ilə yalnız təcrübəli və yüksək ixtisaslı mütəxəssislər məşğul ola bilər. İnformasiya hücumu zamanı informasiya digər saxta verilənlərlə əvəz edilir. İnformasiya sistemindəki verilənləri dəyişməklə müxtəlif cinayətlər həyata keçirmək mümkündür. Məsələn, sifarişçiyə tələb olunan deyil, yanlış sənədin göndərilməsi, maliyyə hesablamalarında saxtakarlıq, səsvermələrdə səslərin dəyişdirilməsi kimi halları misal göstərmək olar.

4. *İnformasiyanın oğurlanması.* Ənənəvi oğurluğun qarşısını almağa xidmət edən cinayət qanunvericiliyi informasiya oğurluğu ilə əlaqədar hüquqi münasibətləri tənzimləyə bilmir. Həm də onu nəzərə almaq lazımdır ki, informasiya hücumunu həyata keçirən şəxs çox zaman başqa ölkədə fəaliyyət göstərir və nəticədə hücum edən tərəfin məsuliyyətə cəlb edilməsi müəyyən çətinliklər yaradır.

5. *İnformasiyanın bloklanması.* İnformasiyanın bloklanması dedikdə informasiyaya çıxışın olmaması,

informasiya əməliyyatlarının ardıcıllıqla yerinə yetirilməsinə qoyulan qadağa və ya hər hansı qurğunun sıradan çıxması nəticəsində informasiyadan istifadənin mümkünsüzlüyü nəzərdə tutulur.

İnformasiya hücumlarında geniş istifadə olunan vasitələri realizə üsullarına görə üç sinfə bölmək olar: *riyazi (alqoritmik), proqram və aparat vasitələri* (şəkil 7).

Alqoritmik vasitələrə aiddir:

- İcazəli fəaliyyətdən istifadə etməklə informasiya resurslarına icazəsiz müdaxilə alqoritmləri;
- İcazəli proqram təminatından və icazəsiz müdaxiləyə imkan verən proqram vasitələrindən istifadə etməklə informasiya resurslarına icazəsiz müdaxilə alqoritmləri.

Proqram vasitələrinə informasiyanın saxlanması, emalı və ya ötürülməsi zamanı potensial təhlükəli sonluqla nəticələnən əməliyyatlara səbəb olan proqramlar aiddir. Potensial təhlükəli proqramlar dedikdə, aşağıdakı funksiyaları yerinə yetirən proqramlar nəzərdə tutulur [87]:

1. Kompyuter şəbəkəsinin proqram-aparat mühitində öz iştirakını gizlədən proqramlar;
2. Çoxalma qabiliyyətinə malik, özünü digər proqramlarla əlaqələndirən və ya xarici daşıyıcılarla ötürülən proqramlar;
3. Operativ yaddaşda proqram kodlarını məhv edən proqramlar;
4. Operativ yaddaşdan informasiya fraqmentlərini xarici yaddaşın bəzi hissələrində saxlayan proqramlar;

Şəkil 7. İnformasiya hücumlarında istifadə olunan proqram və texniki vasitələrin realizə olunma üsuluna görə təsnifatı

5. İnformasiya massivlərini təhrif edən, bloklayan və ya digər informasiya ilə əvəz edən proqramlar;
6. Telekommunikasiya şəbəkəsində həyata keçirilən informasiya mübadiləsini pozan, dövlət və hərbi idarələrdə informasiya mübadiləsini saxtalaşdıran proqramlar;
7. İnformasiya sistemlərinin təhlükəsizlini yoxlayan test proqramların işini neytrallaşdıran proqramlar.

İnformasiya hücumlarında müxtəlif təhlükəli fəsadlar törədən proqramları şərti olaraq 3 sinfə bölmək olar: kompyuter virusları, icazəsiz müdaxilə vasitələri, ziyanlı proqramlar.

Kompyuter virusları

Kompyuter virusları müxtəlif vasitələrlə bir kompyuterdən digər kompyuterə keçməyə cəhd edən, verilənlərin dəyişdirilməsi və ya silinməsinə səbəb olan, istifadəçinin işinə mane olan, digər proqramlarda gizlənmiş kiçik həcmli proqramlardır [88]. Virus proqramları özlərini təxminən bioloji virus kimi aparır: çoxalır, maskalanır və ziyanlı təsirlər göstərir. Virus özgə informasiya daşıyıcılarından, elektron poçt və ya İnternet resurslarından istifadə edilən zaman təhlükə yarada bilər.

Kompyuter viruslarından şəbəkə müharibələrində geniş istifadə olunur [89]. Kompyuter virusları müxtəlif şəbəkələrdə yayıla bildiyinə və aşkarlanması bir-çox hallarda çətin olduğuna görə daha çox təhlükəli hesab edilir. G Data Software şirkətinin 2010-cu ilin illik hesabatında bildirilmişdir ki, dünyada hər 15 saniyədə bir virus yaradılır və təhlükəli virusların sayı 2 mlyondan artıqdır [90].

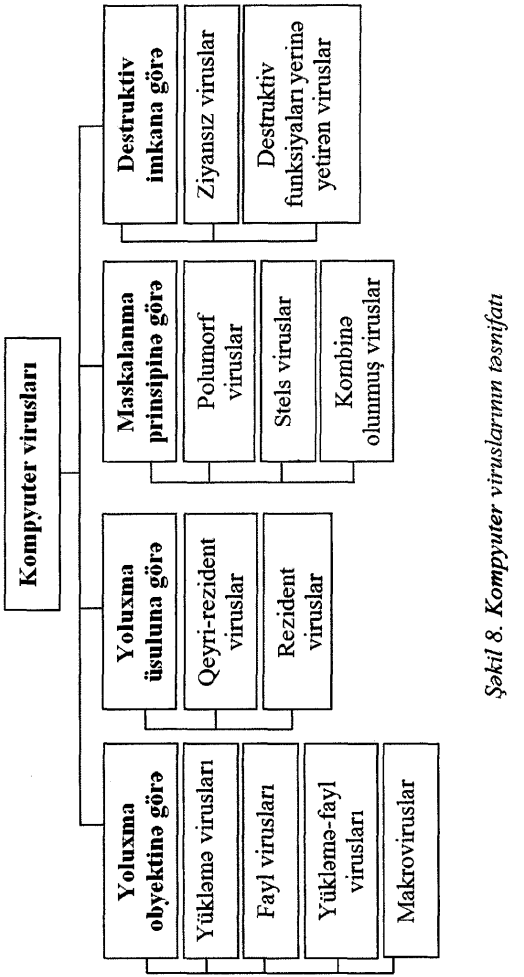
Kompyuter virusunun xüsusiyyəti onun öz-özünə çoxala bilməsi, hiss olunmadan sistemdə yayılması, proqramın daxilində gizlənməsi, əlaqə xətləri, kompyuter şəbəkəsi ilə gizli ötürülməsi, informasiya sisteminin normal fəaliyyətinə mane olması ilə müəyyən olunur. Virusları müxtəlif əlamətlərə görə təsnifatlandırmaq olar (şəkil 8):

- yoluxma obyektinə görə: yükləmə virusları, fayl virusları, yükləmə-fayl virusları, makroviruslar;
- yoluxdurma üsuluna görə: rezident və qeyri-rezident;
- maskalanma prinsipinə görə: polimorf viruslar (özüşifrlənən viruslar), stels viruslar (görünməz viruslar), kombinə olunmuş viruslar.
- destruktiv imkanlarına görə: ziyansız viruslar və destruktiv funksiyaları yerinə yetirən viruslar [88].

İcazəsiz müdaxilə vasitələri

İcazəsiz müdaxilə vasitələri müəyyən təhlükələrlə nəticələnən xüsusi proqramlar sinfidir və müasir İM-də onlardan geniş istifadə olunur.

Belə proqramlara kompyuter şəbəkəsi ilə ötürülən, qarşı tərəfin əməliyyat sisteminin işini və ya hesablama mühitinin bütövlüyünü pozmağa şərait yaradan xüsusi proqram təminatları aiddir. Çox zaman bu növ proqram təminatlarından müdafiə sistemlərinin işinin sınaqdan keçirilməsi üçün istifadə edilir. Sınaqdan keçirməklə şəbəkədə informasiya resurslarına icazəsiz müdaxiləyə səbəb ola biləcək boşluqları müəyyən etmək mümükündür.



*Şəkil 8. **Kompyuter** viruslarının təsnifatı*

Ziyanlı proqram təminatları

Ziyanlı proqram təminatları icazəsiz müdaxilə vasitələrindən fərqi olaraq mühafizə sistemlərini dəf edə bilmirlər. Onları tətbiq sahələrinə və metodlarına görə təsnifatlandırmaq mümkündür:

– proqram-aparat mühiti təsəvvürü yaradan proqramlar;

– ilkin yükləmə proqramları təsəvvürü yaradan proqram vasitələri;

– drayverlərin, komanda interpretatorunun, şəbəkə drayverlərinin, yəni əməliyyat sistemlərinin yüklənməsi təsəvvürünü yaradan proqram əlavələr;

– ümumi təyinatlı tətbiqi proqram təminatı (klaviatur və ekran drayverində, kompyuterin test proqramında, utilit və ya örtük proqramnlarda, məsələn, NORTON sistemində qurulmuş viruslar) təsəvvürü yaradan proqramlar;

– paket proqramlarda quraşdırılan, yalnız koda malik icraedici modullar;

– xarici görünüşünə görə gizli informasiyanın daxil edilməsini tələb edən bəzi proqramlara oxşar imitator modullar;

– optimizasiya təyinatlı proqram vasitələri kimi (arxivatorlar, sürətləndiricilər və s.) maskalanmış proqramlar;

– oyun və əyləncə təyinatlı proqram təminatı kimi maskalanmış (çox zaman tədqiqatçı proqram əlavələr istifadə edilir) proqramlar.

Ziyanlı proqramlara troyan proqramlar, məntiqi bombalar, məntiqi lyuklar, tələ proqramlar, müxtəlif şəbəkə soxulcanları və s. aiddir [91].

Troyan proqramlar (Trojans) – sistemə müdaxilə edərək, gizli funksiyaları yerinə yetirə bilən proqramlardır. Bu

proqramların ən özəl xüsusiyyəti, kompyuter sistemini tədricən, amma mükəmməl şəkildə məhv etməsidir.

"Troya atı" ifadəsi tarixi hadisə ilə əlaqədardır. Taxtadan düzəldilmiş at fiqurunun içərisində gizlənən əsgərlər Troya şəhəri uğrunda gedən müharibənin taleyini həll etmişlər. Troyan proqramlar iki hissədən ibarətdir. Birinci hissə kompyuterə yüklənir və ilkin əmri alan kimi (məsələn, şəklin, hər hansı faylın açılması) ikinci hissə ilə əlaqəni gözləyir. Digər kompyuterdə olan ikinci hissə virusla yoluxmuş kompyuterin İP-ünvanını (şəbəkəyə qoşulmuş hər bir kompyuterin identifikasiyası üçün unikal ünvan) müəyyən edir. Ünvan məlumdursa, artıq yoluxmuş kompyuter qarşı tərəfin nəzarətinə keçir – disk qurğuları özbaşına açılır, bağlanır, pəncərələr özbaşına işləyir, çağırılan əmrlər yerinə yetirilmir, proqramlar açılmır, "yenilənmə"(refresh) düyməsinin funksionallığı pozulur və s.

Troyanlar funksiya və məqsədlərinə görə müxtəlif olurlar: Backdoor, Trojan-DoS, Trojan-PSW, Trojan-Downloader, Trojan-Proxy, Trojan-Banker, Trojan-Spy, Trojan-ArcBomb, Trojan-Clicker, Trojan-Dropper, Trojan-GameThief, Trojan-IM, Trojan-Notifier, Trojan-Ransom, Trojan-SMS, Trojan-Spy və s. [91]:

– Backdoor – bu tip proqramlar ən təhlükəli hesab olunur və kompyuteri uzaqdan idarə etməyə şərait yaradır. Onları aşkar etmək çox çətindir. Nəticədə, istifadəçi kompyuterində virusun olduğundan şübhələnmir, eyni zamanda onun kompyuteri uzaqdan idarə üçün artıq açıq olur;

–Trojan-DoS (Denial of Service) – bu proqramdan istifadə etməklə həyata keçirilən informasiya hücumlarında subyektə çoxlu sayda sorğular göndərilir və əgər kompyuterin

resursları daxil olan bütün sorğuların emalı üçün yetərli deyilsə xidmətdən imtina baş verir;

– Trojan-PSW (Password Stealing Ware) – parolların oğurlanması üçün istifadə edilən troyandır. Bu tip troyanlar yoluxduğu kompyuterdən müxtəlif məlumatları, adətən, system parollarını oğurlamaq qabiliyyətinə malikdir. Yoluxmuş kompyuter barədə müxtəlif məlumatları (yaddaşının və disk sahəsinin həcmi, əməliyyat sisteminin versiyası və s.) toplayıb xüsusi elektron ünvana göndərən Trojan PSW-lər mövcuddur;

– Trojan-Downloader – müxtəlif proqramların yüklənməsində istifadə olunan troyandır. Bu tip troyanların köməyi ilə müxtəlif ziyanverici proqramların İnternet vasitəsi ilə kompyuterə yüklənməsi və işə salınması həyata keçirilir;

– Troyan-Proxy – proksi-server troyanları. Bu tip troyanlar anonim olaraq müxtəlif İnternet resusrlarına daxil olur. Bir qayda olaraq, spam tipli məlumatların yayılmasl üçün istifadə olunur;

–Trojan-Banker – bank sistemi, plastik kartlarla əlaqədar istifadəçiyə məxsus informasiyanın oğurlanmasında istifadə olunan ziyanlı proqramdır;

– Trojan-Spy – "ağent" troyanlar. Adətən on-layn ödənişlərdə və bank sistemlərində istifadə edilir. Əsas məqsədi kompyuterdə yerinə yetirilən işlər barədə məlumat toplamaqdır. *Trojan-Spy* fayl şəklində kompyuterin diskində saxlanılır və məlumatları müntəzəm şəkildə "troyanın sahibinə" ötürür.

Məntiqi Bombalar (Logic Bombs) – məntiqi bombaların proqram təminatına daxil edilməsi nəticəsində informasiyanın məhvi ilə yanaşı dəyişdirilməsi, saxtalaşdırılması və icazəsiz ötürülməsilə həyata keçirilir. Məntiqi bombalar müəyyən məntiqi əməliyyatlar zamanı bədniyyətli məqsədləri həyata

keçirən proqramlardır. Bu tip viruslara misal olaraq hərbi infrastrukturun informasiya-idarəetmə mərkəzlərinə daxil edilən və siqnalla, yaxud təyin edilmiş vaxtda işə düşən proqramları göstərmək olar. Müxtəlif texnogen qəzaların (su və ya atom elektrik stansiyalarında, kimyəvi laboratoriyalarda və s.) həyata keçirilməsində məntiqi bombaların təhlükəsi inkaredilməzdir.

Məntiqi lyuk – əməliyyat sistemi və ya proqram təminatında icazə verilməyən hər hansı funksiyanı yerinə yetirməyə çalışan xüsusi mexanizmdir. Məntiqi lyuka obyektin proqram təminatında bilərəkdən həyata keçirilən müxtəlif növ səhv əməliyyatları misal göstərmək olar.

Tələ-proqramlar – proqram təminatında baş verən səhvləri və ya anlaşılmazlıqları xüsusi məqsədlərlə istifadə edən proqramlardır.

Kompyuter soxulcanları (Computer worms) – viruslardan fərqli olaraq müstəqil proqramlardır. Bu tip proqramlar lokal və qlobal şəbəkələrdə yayılaraq bir kompyuterdən digərinə köçürülür. İlk yaradılmış kompyuter soxulcanı "Morris soxilçanı" hesab edilir [92]. Robert Morris tərəfindən yazılmış "Morrisa soxulcanı" 2 noyabr 1988-ci ildə şəbəkə vasitəsilə qısa müddətdə ABŞ-da altı mindən artıq kompyuteri yoluxdurmuşdu.

Kompyuter soxulcanının funksionallığının əsas mərhələləri [93]:

– Təsir məqsədi ilə kompyuter şəbəkəsində axtarış (çox hallarda şəbəkə ünvanı məlum olan kompyuterin axtarışı);

– şəbəkə vasitəsilə informasiya sisteminə xüsusi proqram kodunun göndərilməsi;

– hücuma məruz qalan kompyuterlərdə informasiya sistemlərinin idarəedilməsinin ələ keçirilməsi və s.

İnformasiya hücumunda istifadə olunan proqram vasitələrini məqsədlərinə görə müxtəlif siniflərə ayırmaq mümkündür: tədqiqatçı, ələ keçirici, dağıdıcı, aktiv maneə törədən proqramlar. Universallığı, gizliliyi, çoxvariantlılığı, zaman və məkana görə məhdudiyyətsizliyi, ucuz başa gəlməsi bu vasitələri müasir dövrdə çox təhlükəli informasiya silahına çevirmişdir.

İM-də istifadə olunan hücum xarakterli proqramlar yalnız informasiya hücumları üçün deyil, eyni zamanda, hesablama mühiti elementlərinin mühafizə sisteminin kəşfiyyatı və tədqiqatı üçün də istifadə oluna bilər.

3.3. Nəticə

İnformasiya müharibəsi texnologiyalarının araşdırılması, informasiya hücumlarının analizi və təsnifatı, hücumda istifadə olunan proqram vasitələrinin təhlili kompyuter şəbəkələrində informasiya əməliyyatları ilə əlaqədar pozuntuların təyin edilməsində, konkret vəziyyət üçün daha çox ehtimal olunan təhlükələrin təyinində və informasiya təhlükəsizliyi ilə əlaqədar işlərin təşkilində mühüm əhəmiyyətə malikdir.

Kompyuter şəbəkələrində baş verən və günbəgün genişlənən informasiya qarşıdurmalarına qadağa qoymaq və ölkələrin ümumi qlobal informasiya fəzasında fəaliyyətlərini məhdudlaşdırmaq mümkün deyildir. Bununla belə öz informasiya fəzasını mühafizə etməyə çalışan hər bir dövlət İM vasitələrindən qorunmaq, informasiya hücumları təhlükəsini minimuma endirmək üçün beynəlxalq hüquqa söykənmiş müqavilələrə qoşulmaqla informasiya təhlükəsizliyi üzrə bir sıra tədbirlərdən istifadə edə bilər.

Respublikamızda dövlət qurumlarının informasiya sistemləri formalaşdıqca onların təhlükəsizliyini təmin etmək, hakerlərdən qorumaq ölkənin sosial təhlükəsizliyinin əsas şərtlərindən biridir. Çünki dövlət əhəmiyyətli məlumatların əks qüvvələrin əlinə düşməsi ölkənin gələcəyi üçün böyük təhlükələr yarada bilər. Belə təhlükələrin qarşısının alınması dövlətlərdən birgə tədbirlərin görülməsini tələb edir.

Nəzərə almaq lazımdır ki, informasiya texnologiyaları üzrə cinayətlər çox zaman beynəlxalq xarakter daşıyır. Belə ki, cinayətkar bir ölkədə fəaliyyət göstərirsə, onun potensial "qurbanları" digər bir ölkədə və ya ölkələrdə ola bilər. Kompyuter şəbəkəsindən istifadə etməklə həyata keçirilən hücum əməliyyatlarının transmilli xarakterli olması belə deməyə əsas verir ki, informasiya hücumları ilə mübarizədə istənilən strategiyanın əsas hissəsini problemlərin həlli ilə əlaqədar ümumi siyasətin işlənməsi təşkil edir.

2001-ci il noyabr ayının 23-də Avropa və Amerikanın 30-dan çox ölkəsi Avropa Şurasının kiberfəzada cinayətkarlıq üzrə ekspert komitəsinin dörd il ərzində işləyib hazırladığı "Kibercinayətkarlıq haqqında" Konvensiyanı (ETS N 185) imzaladı. Bu konvensiya fırıldaqçılıq, müəllif hüquqlarının pozulması, kompyuter proqramlarının sındırılması, uşaq pornoqrafiyası və digər bu kimi cinayətkarlıqla mübarizədə qarşılıqlı fəaliyyətə çağıran ilk beynəlxalq muqavilədir. Ayrıca protokolda İnternetdə irqçilik və antisemitizm xarakterli materialların yayılması qadağan edilmişdir [94].

"Kibercinayətkarlıq haqqında" Konvensiya, 2003-cü ildə "Kompyuter informasiyaları sahəsində cinayətkarlıq barədə" Konvensiyaya əlavə olunan protokol məhz dövlətlərin informasiya təhlükəsizliyini təmin etmək məqsədini daşıyır.

2008-ci ildə Azərbaycan "Kibercinayətkarlıq haqqında" Konvensiyaya qoşulmaq haqqında sənəd imzalamışdır [95].

"Kibercinayətkarlıq haqqında" Konvensiya kiberfəzada baş verən cinayətləri dörd qrupa bölür.

Birinci qrupa kompyuter verilənlərinin və sistemlərinin konfedensiallığına, bütövlüyünə və əlyetərliliyinə qarşı cinayətlər aiddir: qanunsuz müdaxilə (səh. 2), qanunsuz ələ keçirmə (səh. 3), kompyuter verilənlərinə təsir (qanunsuz, bilərəkdən kompyuter verilənlərinin zədələnməsi, silinməsi, keyfiyyətinin korlanması, dəyişdirilməsi və ya bloklanması) (səh. 4, 5). Bu cinayət qrupuna eyni zamanda xüsusi texniki qurğulardan qanunsuz istifadə də aiddir (səh. 6) – kompyuter cinayətlərində istifadə üçün nəzərdə tutulmuş kompyuter proqramları, kompyuter sisteminə və ya onun müəyyən hissəsinə müdaxilə etmək üçün nəzərdə tutulmuş kompyuter parolları, müdaxilə kodları, onların analoqları.

İkinci qrupa kompyuter vasitələrindən istifadə ilə əlaqəli cinayətlər daxildir. Onlara kompyuter texnologiyalarından istifadə etməklə həyata keçirilən saxtakarlıq və dələduzluq fəaliyyəti daxildir (səh. 7-8). Kompyuter texnologiyalarından istifadə etməklə elektron sənədlərdə saxtakarlıq, qərəzli və qanunsuz informasiyanın daxil edilməsi, informasiya sistemlərində verilənlərin dəyişdirilməsi, silinməsi və bloklanması daxildir ki, nəticədə informasiya təhlükəsizliyi pozulmuş olur.

Üçüncü qrupa uşaq pornoqrafiyasının istehsalı (kompyuter sistemləri vasitəsilə yaymaq məqsədi ilə), təklifi və ya verilməsi, yayılması və hazırlanması, eyni zamanda kompyuterdə saxlanılması aiddir (səh. 9).

Dördüncü qrupa müəlliflik hüququ ilə bağlı cinayətlər aiddir. Konvensiyadakı razılaşmaya görə hər bir iştirakçı dövlət kibercinayətkarlıqla mübarizədə müvafiq orqanlara müvafiq hüquq və vəzifələri vermək üçün vacib hüquqi şərait yaratmalıdır: kompyuter sisteminin, onun bir hissəsinin və ya informasiya daşıyıcısının zəbt edilməsi; kompyuter verilənlərinin sürətlərinin hazırlanması və ya müsadirə edilməsi; cinayət işində istifadə edilən saxlanılan kompyuter verilənlərinin tamlığının və qorunmasının təmin edilməsi; kompyuter sistemində saxlanılan kompyuter verilənlərinin məhv edilməsi və ya bloklanması.

Konvensiya həmçinin mövcud texniki vasitələrin köməyi ilə İnternet provayderlərə informasiyanın ələ keçirilməsi, yığılması və qeydiyyatı ilə bağlı lazım olan hüquqi şəraitin yaradılmasını tələb edir.

Son dövrlərdə kiberfəzada baş verən ciddi dəyişiklikləri, İnternetdən terrorçuluq, narkotik maddələrin yayılması və insan alveri məqsədilə istifadənin gücləndiyini nəzərə alaraq kompyuter cinayətkarlığı sahəsində Azərbaycan Respublikasının Cinayət Məcəlləsinin 271, 272 və 273-cü Maddələrində kompyuter informasiyasına qanunsuz müdaxiə, ziyanverici proqram yaratma, onlardan istifadə etmə və ya onları yayma, informasiya sistemlərinin və şəbəkələrinin istismarı qaydalarını pozmağa görə şərti maliyyə vahidi məbləğinin beş yüz misli miqdarda cərimədən başlayaraq beş ilədək müddətə azadlıqdan məhrum etmə cəzası nəzərdə tutulur.

Azərbaycan Respublikasının Milli Məclisi 2002-ci il iyulun 20-də Yalta şəhərində GUÖAM-ın Zirvə Toplantısında imzalanmış "Terrorizm, mütəşəkkil cinayətkarlıq və digər növ

təhlükəli cinayətlərlə mübarizə sahəsində GUÖAM iştirakçısı olan dövlətlərin Hökumətləri arasında əməkdaşlıq haqqında" Sazişi 10 iyun 2003-cü ildə təsdiq etdi. Qanunun 1-ci Maddəsində kompyuter texnologiyaları və kompyuter şəbəkələrinin istifadəsi sahəsində cinayətlərlə mübarizə və əqli mülkiyyət sahəsində cinayətlərlə mübarizə öz əksini tapmışdır [96].

İM problemlərini yalnız informasiya sisteminin və ya kompyuter şəbəkəsinin təhlükəsizliyini gücləndirməklə həll etmək mümkün deyil. Bu gün istənilən informasiya şəbəkəsinin layihələndirilməsini həyata keçirərkən, artıq sabah onun informasiya əməliyyatları meydanına çevriləcəyini nəzərə almaq lazımdır. İnformasiya təcavüzünün qarşısını almaq, informasiya qarşıdurmasında uğur əldə etmək üçün isə ilk növbədə İM mahiyyətini dərindən bilmək, informasiya hücumlarını analiz edərək onlara qarşı qabaqlayıcı tədbirlər görmək lazımdır.

Hər bir dövlətin iqtisadi və elmi-texniki siyasətinin bir istiqaməti kimi milli informasiya təhlükəsizliyi məsələsi həll edilməlidir. İnformasiya təhlükəsizliyinin təmin edilməsi sistematik, kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlərin aparılması müasir dövrün ən vacib məsələlərindəndir.

ƏDƏBİYYAT

1. Тоффлер Э., Третья волна, пер. с англ. М., 2002 776 с.
2. Алгулиев Р.М., Алиев А.Г., Экономические особенности информационных технологий, Баку, "ЭЛМ", 2002, с. 56
3. Иноземцев В.Л., Современное постиндустриальное общество: природа, противоречия, перспективы, М.: Логос, 2000, 86 с.
4. Белл Д., Грядущее постиндустриальное общество, М.: Академия, 1999, 949 с.
5. Toffler A., War and Anti-War: Survival at hte Daün of the 21st Century, N.Y., 1993, 302 pp.
6. Шапорев С.Д., Информатика, Теоретический курс и практические занятия, СПб., БХВ-Петербург, Учебная литература для вузов, 2008, 480 с.
7. Волковский Н.Л., История информационных войн, в 2ч/ч.1, СПб., ООО «Издательство «Полигон», 2003, 502 с.
8. Сунь Цзы., Искусство войны, http://cclib.nsu.ru/projects/satbi/satbi/books/sunzi/
9. Thomas P. Rona, "Weapon Systems and Information War" // Boeing Aerospace Co., Seattle, WA, 1976, pp. 14
10. Libicki M., What is Information Warfare? // National Defense University. ACIS, 1995, pp. 3
11. Əliquliyev R.M., Şükürlü S.F., Kazımova S., Elmi fəaliyyətdə istifadə olunan əsas terminlər, Bakı, "İnformasiya Texnologiyaları", 2009, 201 səh.

12. Əliquliyev R.M., İmamverdiyev Y.N., Rəqəm imzası texnologiyası, Bakı, "Elm", 2003. 132 səh.
13. Галатенко В.А., Основы информационной безопасности, Москва, Издательство: INTUIT.RU 2008, 264 с.
14. Colonel Alan D., Douglas H., Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Hardcover) // Afcea Intl Pr, 2000, pp. 309
15. Абдурахманов М.И., Баришполец В.А., Баришполец Д.В., Манилов В.Л., Геополитика, международная и национальная безопасность, Словарь-справочник. Под общей редакцией В.Л. Манилова, "Пробель", Москва, 1999, с. 127-130
16. Кара-Мурза С.Т., Манипуляция сознанием, М.: ЭКСМО, 2008. 864 с.
17. Присяжэнюк С.П., Сидак А.А., Анализ современного состояния теории и практики построения моделей систем защиты информации. / Тезиси докладов III Межведемственной научно-технической конференции «Проблемные вопросы сбора, обработки и передачи информации в сложных радиотехнических системах», Пушкин, 1997
18. Почепцов Г. Г, Информационные войны, М.: «Рефл-Бук», 2000, 576 с.
19. Forno R., Baklarz R., The Art of Information Warfare. Insight into the Knowledge of Warrior Philosophy, 1999.
20. Arguilla J., Ronfeldt D., Cyberwar is coming! // Comparative Strategy, 1521-0448, Volume 12, Issue 2, 1993, pp. 141 – 165

21. Arguilla J., Ronfeldt D., In Athena's Camp: Preparing for Conflict in the Information Age // War; Information society; Forecasting, Santa Monica, Calif., 1997, pp. 501
22. Arguilla J., Ronfeldt D., Networks and Netware: The Future of Terror, Crime, and Militancy // War; Information society; Forecasting, Santa Monica, Calif., 2001, pp. 375
23. Павлютенкова М.Ю., Информационная война: реальная угроза или современный миф? // "Власть", М., 2001, с.19-23
24. Волковский Н.Л., История информационных войн, в 2ч/1ч, СПб., «Полигон», 2003, 512 с.
25. Ржавский К.В., Информационная безопасность: Практическая защита информационных технологий и телекоммуникационных систем, Учебное пособие, ФГУ ГНИИ ИТТ "Информика", 2005, 120 с.
26. Брусницин Н.А., Информационная война и безопасность // М.: Вита-Пресс, 2001, с. 9
27. Почепцов Г.Г., Информационные войны, Киев: Ваклер, 2000. с. 20
28. Расторгуев С.П., Информационная война // М.: Радио и связь, 1998. с. 35-37
29. Пирумов В.С., Родионов М.А., Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. № 5, 1997, с. 43-47
30. Цыбмал В.И., О концепции информационной войны // Информационный сборник "Безопасность". М., 1995, № 9, с. 35

31. Прохожев А.А., Турко Н.И., Основы информационной войны // Анализ систем на пороге XXI века: теория и практика. М., 1996. с. 252-253
32. Веренцов А., Ненасильственное средство: США оттачивают приемы информационной борьбы // ЭВНВО, № 016 (139), 1999
33. Панарин И.Н., Технология информационной войны, М.: КСП, 2003, с. 320
34. Панарин И.Н., Информационные войны и Россия // Информация. Дипломатия. Психология. М.: Известия, 2002. с. 145
35. Панарин И.Н., Информационные войны: теория и практика // М.: Кадровая политика, №2, 2002, 71 с.
36. Комов С.А., Информационная борьба в современной войне: вопросы теории // "Военная мысль", 1996, № 3. с.73
37. Гриняев С.Н., Война в четвертой сфере: НВО // Независимое военное обозрение, № 42, 2000, с. 7
38. Модестов С.А., Война, к которой готовится Америка: Эволюция вооруженной борьбы в эпоху информатизации // ЭВНГ, № 048, 1996
39. Костин Н.А., Общие основы теории информационной борьбы // Военная мысль, №3, 1997, с. 44–50
40. Стрельцов А.А., Обеспечение информационной безопасности России, Теоретические и методологические основы, М.: МЦНМО, 2002, 286 с.
41. Принципы, касающиеся международной информационной безопасности, Проект, МИД РФ, 2000
42. Libicki M. What is Information Warfare. – National Defense University. ACIS, 1995, pp 3.

43. Давыдов Ю., Понятие «жесткой» и «мягкой» силы в теории международных отношений // Международные процессы. Т.: 2004, №1 (4), с. 74–76;
44. Ранних А. А., Информационная безопасность и дипломатическая служба России // Информация. Дипломатия. Психология., М.: Известия, 2002, с. 338–340
45. Фефелова О, Фефелова И., Информационные войны как средство управления общественно-политическими процессами // Лаборатория рекламы. 2007. №1, с. 14-17
46. Эксперты: Эпохе гостайн пришел конец, http://www.segodnya.ua/news/
47. Wikileaks готовит еще две сенсации, http://rupor.info/glavnoe/
48. Панарин И.Н., Панарина Л.Г., Информационная война и мир // М.: ОЛМА-ПРЕСС , 2003, 382 с.
49. Гриняев С.Н., Информационная война: история, день сегодняшний и перспектива, СПб.: Арлит, 2000, http://www.agentura.ru/equipment/psih/info/war/
50. Бедрицкий А. В., Информационная война: концепции и их реализация в США, Российский институт стратегических исследований, М., 2008, 188 с.
51. Arguilla J., Ronfeldt D., Zanini M., Networks, Netwar, and Information-Age Terrorism // The Changing Role of Information in Warfare, Rand Corporation, 1999, pp. 88–89
52. Colin S. Gray, Geoffrey R. Sloan, Geopolitics, geography, and strategy // Frank Cass Publishers, Landon, 1999, pp. 189

53. Stein G.J. Information warfare // Airpower Journal. Spring, 1995, pp. 30
54. Roger C. Molander, A. S. Riddile, Peter A. Wilson, Strategic Information Warfare: A New Face of War, Santa Monica, National Defense Research Institute, Calif.: RAND, MR-963-OSD, 1996
55. Roger C. Molander, Peter A. Wilson, The Day After...in the American Strategic Infrastructure, Santa Monica, National Defense Research Institute, Calif.: RAND, MR-963-OSD, 1998
56. Roger C. Molander, Peter A. Wilson, B. David Mussington, Richard Mesic, Strategic Information Warfare Rising, Santa Monica, Calif.: RAND, MR-964-OSD, 1998
57. Robert J. Bunker, Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI // 1996, pp. 108-120, http://www.carlisle.army.mil/
58. Robert E. Blackington, Major, USAF, Air Force information operations (IO) doctrine: consistent with joint io doctrine? // Air Command and Stoff college, Air University, Maxwell Air Force Base, Alabama, 2001
59. Деньщиков А.Л., Информационная стратегия США (анализ, стратегия, перспективы) // Диссертационная работа, Дипломатическая академия министерства иностранных дел РФ, М., 2008
60. Костюхин А., Горбунов Г., Сажин А., Информационные операции в планах командования ВС США // Зарубежное военное обозрение, № 5, 2007, с. 7-12
61. Joint doctrin of information operations, http://www.iwar.org.uk

62. Joint Task Force - Computer Network Operations, http://www.iwar.org.uk
63. Гриняев С.Н., Интеллектуальное противодействие информационному оружию, М.: СИНТЕГ, 1999, 232 с.
64. Air Force Information Warfare Center, http://www.fas.org/
65. Network-Centric Warfare: Department of Defense Report to Congress, 2001, http://cio-nii.defense.gov
66. Arguilla J., Ronfeldt D., The Advent of Netwar / In Athena's Camp: Preparing for Conflict in Information Age, RAND Corporation, National Defense research Institute, 1997
67. Arguilla J., Ronfeldt D., Swarming and Future of Conflict, RAND Corporation, National Defense research Institute, 2000
68. David S. Alberts, John J. Garstka, Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd edition (revised). Washington, DC: DoD CCRP, 2000
69. Edward A. Smith, Jr. Effects-based Operations. Applying Network-centric Warfare in Peace, Crisis and War, Washington, DC:DoD CCRP, 2002, pp.108
70. Garstka J., Network Centric Warfare Offers Warfighting Advantage, Signal Forum. Signal Magazine. 2003
71. Баулин В., Кондратьев А., Реализация концепции "Сетецентрическая война" в ВМС США // Зарубежное военное обозрение, №6, 2009, с. 61-67

72. Комарович В. Ф., Компьютерные информационные войны // «Защита информации. Конфидент», № 4-5, 2002, с. 84-88
73. Burnette G., Information: Battlefield of the Future // Surface Warfare, 1995
74. Жуков В., Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. № 1, 2001, с. 2-9
75. Конституция Российской Федерации, М. 1994, http://main-law.ru/
76. Доктрина информационной безопасности Российской Федерации. // Российская газета, М., №187, 2000
77. Военная Доктрина Российской Федерации, М. 2000, http://news.kremlin.ru/ref_notes/461
78. Манойло А.В., Информационное противоборство в условиях психологической войны. – М.: Закон и право, 2003, № 12, с. 31-34
79. Швец Д.А. Информационное управление как технология обеспечения информационной безопасности, Сб. "Массовая коммуникация и массовое сознание", М., МГИМО, 2003
80. Пархомов В.А. К определению понятия "Информационное преступление" // Вестник ИГЭА, 2001, № 2, с. 10-13.
81. Manuel Cerejo, "China, Cuba and Information Warfare, Signal Intelligence, Electronic Warfare and Cyber Warfare, http://www.futurodecuba.org/
82. Рассел Р. И др. Защита от хакеров коммерческого сайта: пер. с англ. – М.: Компания АйТи: ДМК пресс: ТЕТРУ, 2004, 552 с.

83. Balkin J., Grimmelmann J., Katz E., Kozlovski N., Wagman S. & Zarsky T., Cybercrime: Digital Cops in a Networked Environment // New York: New York University Press,, 2007, 268 pp.
84. David Noel, Matrix Thinking Book I // BFC Press, Australia, 2004, 200 pp, http://www.aoi.com.au
85. Changwang Zhang, Jianping Yin, Zhiping Cai, Weifeng Chen, RRED: Robust RED Algorithm to Counter Low-rate Denial-of-Service Attacks, IEEE Communications Letters, vol. 14, pp. 489-491, 2010
86. Способы нападений на компьютерные сети и защита от несанкционированного межсетевого доступа, http://library.tuit.uz
87. Сердюк В.А. Вы атакованы – защищайтесь (методология выявления атак) // BYTE/Россия, 2003, № 9 (61), с. 61-64.
88. Островский С.Л. Компьютерные вирусы, Выпуск 3.2 // М.: «Диалог Наука», 1997, 88 с.
89. Фролов А.В., Фролов Г.В., Осторожно: компьютерные вирусы // М.: «Диалог-МИФИ», 1996, 256 стр.
90. G Data Malware Report, http://www.gdatasoftware.com/
91. Белоусов С.А., Гуц А.К., Планков М.С., Троянские кони. Принципы работы и методы защиты, Омск: Издательство Наследие. Диалог-Сибирь, 2003. 84 с.
92. Eugene H. Spafford, The Internet Worm Program: An Analysis // Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, 2004
93. Howard J.D., An Analysis of Security Incidents on the Internet: 1989-1995, doctoral dissertation, Dept. Eng. and

Public Policy, Carnegie Mellon Univ., Pittsburgh, http://www.cert.org/research/JHThesis/Start.html, 2000
94. International Aspects of Computer Crime, http://www.cybercrime.gov/
95. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, http://archive.president.az/
96. "Terrorizm, mütəşəkkil cinayətkarlıq və digər növ təhlükəli cinayətlərlə mübarizə sahəsində GUÖAM iştirakçısı olan dövlətlərin Hökumətləri arasında əməkdaşlıq haqqında" Sazişin təsdiq edilməsi barədə, http://e-qanun.az/

Alakparova I.Y. Technologies of information warfare. Express information. Series of Information Society.
Baku: "Information Technologies" Publishing House, 2012, 108 pp.

The essence of technology information warfare was investigated in the rapid information and the problems of the information counter and the network war were considered. Properties were analyzed and the purpose of information attacks, put forward proposals in relation to the mechanisms of their realitsatsii.

Алекперова И.Я. Технологии информационных войн. Экспресс-информация, Серия Информационное общество. Баку: Изд. «Информационные Технологии», 2012, 108 с.

В экспресс-информации были исследованы технологии информационных войн, рассмотрены проблемы информационного противостояния и сетевых войн. Были анализированы свойства и цели информационных атак, выдвинуты предложения в связи с механизмами их реалицации.

İradə
Yavər qızı
Ələkbərova

AMEA İnformasiya Texnologiyaları İnstitutunun sektor müdiri.

depart17@iit.ab.az

Texniki redaktor: Anar Səmidov

Korrektor: Ləman Manahova

Kompyuter tərtibatı: Zülfiyyə Hənifəyeva

Kompyuter yığımı: Dinara Zeynalova

Çapa imzalanmışdır: 01.03.2012. Çap vərəqi: 60x84 16/1,
Sifariş №32, sayı 100 ədəd.