UOT 004.49;004.056

Ələkbərova İ.Y.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
depart17@iit.ab.az

KOMPYUTER ŞƏBƏKƏSİNDƏ İNFORMASİYA HÜCUMLARI VƏ ONLARIN REALLAŞDIRILMASI MEXANİZMLƏRİ

Məqalədə kompyuter şəbəkəsində informasiya hücumları problemlərinə baxılmış, hücumların həyata keçirilməsi üsulları tədqiq edilmişdir. İnformasiya hücumlarının təsnifatı aparılmış, həmçinin hücumlarda istifadə olunan proqram vasitələri təsnif edilmiş, onların kompyuter şəbəkəsində fəaliyyəti araşdırılmışdır.

Açar sözlər: *informasiya müharibəsi, informasiya hücumları,informasiya sistemi, məntiqi bombalar, şəbəkə soxulcanları, viruslar.*

Giriş

Müasir cəmiyyətdə informasiyanın həcmi və rolu sürətlə artmaqdadır. Cəmiyyətin bütün sahələrində informasiya-kommunikasiya texnologiyalarının (İKT) imkanlarına əsaslanan intensiv informasiyalaşma prosesləri gedir. İKT-nin son nailiyyətlərinin tətbiqi nəticəsində dövlətin sosial-iqtisadi inkişafı, vətəndaşların hüquq və azadlıqlarının qorunması, rifah halının yüksəldilməsi üçün əvvəllər mövcud olmayan imkanlar yaranır.

Bu imkanlardan səmərəli istifadə etmək üçün informasiya mühitinin təhlükəsizliyinin təmin edilməsi vacib məsələdir. Belə ki, informasiya texnologiyalarının inkişafı ilə əlaqədar yaranan informasiya mühiti etibarlı şəkildə mühafizə olunmadıqda yeni növ informasiya əməliyyatı sayılan informasiya təcavüzünə şərait yaranmış olur.

Mütəxəssislər bildirirlər ki, elmi-texniki inkişafa uyğun olaraq, müharibələrin metod və silahları da dəyişməkdədir. Gələcəkdə dövlətə əsas təhlükə müxtəlif ölkələrin nizami ordusu tərəfindən deyil, müasir İKT vasitələri ilə silahlanmış, yüksək hazırlıq görmüş, əsas məqsədi qarşı tərəfin informasiya resurslarını ələ keçirmək və ya nəzarətdə saxlamaq olan xüsusi qruplar tərəfindən gözlənilir [1]. Son dövrdə müxtəlif cinayətkar qruplar informasiya hücumlarında elm və texnikanın ən yeni nailiyyətlərindən fəal istifadə etməkdədirlər.

Elektron vasitələrdən istifadə etməklə həyata keçirilən informasiya hücumlarının artması ilk növbədə, İnternetin yayılması ilə sıx bağlıdır. Kompyuter və şəbəkə texnologiyalarından istifadə etməklə bir neçə saniyə ərzində müxtəlif məxfi məlumatlar yerləşdiyi məkandan asılı olmayaraq oğurlanır, nəzarətdə saxlanılır və ya məhv edilir. Kompyuter şəbəkəsindən istifadə etməklə həyata keçirilən bu əməliyyatların transmilli xarakter alması belə deməyə əsas verir ki, informasiya hücumları ilə mübarizədə istənilən strategiyanın əsas hissəsi problemlərin həlli ilə əlaqədar ümumi siyasətin işlənməsidir.

Təqdim olunan məqalənin məqsədi kompyuter şəbəkələrində sürətlə artmaqda olan informasiya hücumları ilə əlaqədar mövcud problemləri analiz etmək və tədqiqat istiqamətlərini müəyyənləşdirməkdir.

İnformasiya hücumlarının mahiyyəti

Adi müharibələrdə olduğu kimi, informasiya müharibəsində də əməliyyatlar iki istiqamətdə yerinə yetirilir: hücum və müdafiə [2]. Hücum əməliyyatlarında əsasən informasiya silahlarından istifadə edilir. İnformasiya silahını adi döyüş silahlarından fərqləndirən cəhət ondan ibarətdir ki, informasiya silahında əsas diqqət özündə baza biliklərini cəmləmiş alqoritm və texnologiyalardan istifadəyə yönəlmişdir. İnformasiya silahı insanın şüuruna təsir edərək şəxsiyyətin identifikasiyasının üsul və formalarını dağıdır, təfəkkür matrisini [3] dəyişərək əvvəlcədən verilmiş parametrlər (düşünmə tərzi, mənəvi ehtiyac, özünüifadə formaları və s.) üzrə şəxsiyyəti formalaşdırır, qarşı tərəfin idarəetmə sistemlərini məhv edir və ya nəzarətdə saxlayır.

Müasir dövrdə informasiya hücumları ilə bağlı iki fikir formalaşmaqdadır. Tədqiqatçıların bir hissəsi informasiya hücumları dedikdə elə informasiya əməliyyatlarını nəzərdə tuturlar ki, bu zaman kompyuter informasiya müharibəsində bir silah kimi istifadə edilir [4]. 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 informasiya müharibəsi zamanı informasiya hücumlarını təmin edən vasitə kimi qəbul edilir [5, 6]. Bir çox dövlətlərdə informasiya təhlükəsizliyi ilə bağlı qanunlarda bu yanaşma üstünlük təşkil edir.

İnformasiya hücumları iki cür olur: informasiya-texniki və informasiya-psixoloji hücum. Hər iki halda informasiya əməliyyatları qarşı tərəfə maksimum ziyan vurmaq üçün nəzərdə tutulmuşdur [7].

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;
- kompüter sistemlərinin, texniki vasitələrin işlərinin pozulması və s. nəzərdə tutulur.

İnformasiya hücumları, adətən, mərhələlərlə yerinə yetirilir [8]:

1. İnformasiya hücumundan öncə informasiyanın toplanması;
2. İnformasiya hücumunun həyata keçirilməsi;
3. 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 təcrübə 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 edilir və hədəf seçilir. 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 edilir. Bütün bu əməliyyatlar xüsusi metodlarla həyata keçirilir.

İnformasiya hücumunun ikinci mərhələsi olan hücumun həyata keçirilməsi əməliyyatı özü də iki mərhələdə baş verir: nüfuz etmə və nəzarət.

Nüfuzetmə 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 nəzarətə alınır. Bu isə xüsusi troyan proqramlar (NetBus, BackOrifice və s.) vasitəsi ilə həyata keçirilir.

Yalnız bundan sonra informasiya hücumunu həyata keçirmək mümkündür. Bu mərhələdə cinayətkar iki məqsəd güdür: şəbəkəyə və orada saxlanılan informasiyaya icazəsiz müdaxilə və şəbəkəni ələ keçirəndən sonra onunla informasiya mübadiləsi aparan digər şəbəkələrə icazəsiz müdaxilə. İkinci əməliyyat hücum edənin aşkar edilməsini çətinləşdirir və ya mümkünsüz edir.

Hücum başa çatdırıldıqdan 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 [9].

İnformasiya hücumlarının təsnifatı

Kompyuter şəbəkəsində baş verən informasiya hücumlarının təsnifatını aparmaq üçün şəbəkə təhdidlərinin təyin edilməsi vacibdir [10]:

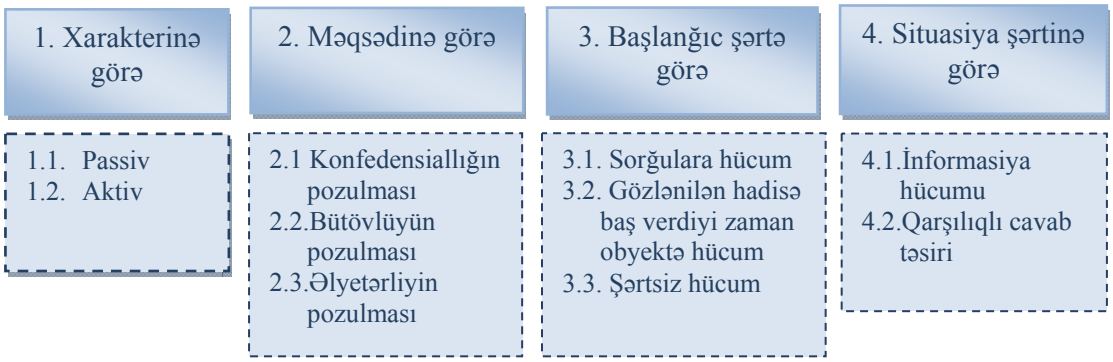
1. Uzaq məsafədən nüfuzetmə ***(remote penetration)***. Bu hücum nəticəsində şəbəkədən istifadə etməklə hücuma məruz qalmış kompyuteri idarə etmək mümkündür. Məsələn, NetBus və ya BackOrifice.
2. Lokal nüfuzetmə ***(local penetration)***. Bu tip hücumlar şəbəkəyə icazəsiz müdaxiləni təmin edir. Məsələn, GetAdmin.
3. Uzaq məsafədən xidmətdən imtina ***(remote denial of service)***. İnternetdən hücum nəticəsində serverin həddən artıq yüklənməsi və ya normal fəaliyyətinin pozulması. Məsələn, Teardrop və ya trin00.
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 müəyyən edilməsi xüsusi proqramlarla həyata keçirilir. Məsələn, Windows üçün L0phtCrack və ya Unix üçün Crack.
8. Protokol analizatoru ***(sniffers)***. Şəbəkə trafikini nəzarətdə saxlayan proqramlar. Onlar vasitəsilə lazım olan informasiya (kredit kartlar, istifadəçinin parolu haqqında informasiya və s.) əldə edilərək informasiya hücumlarında istifadə olunur. Məsələn, Microsoft Network Monitor, LanExplorer.

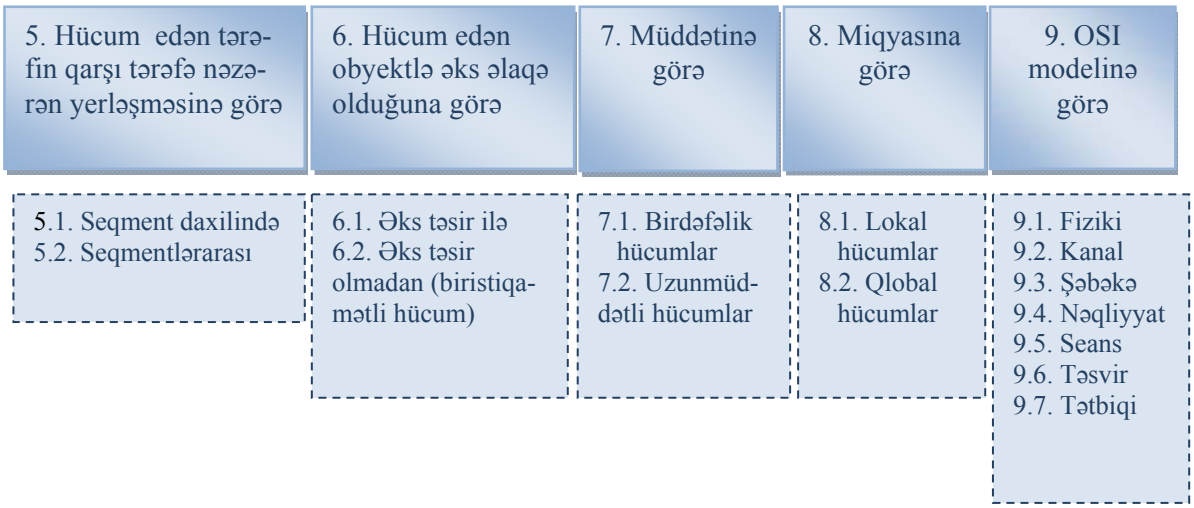
Internet Security Systems, Inc. şirkəti informasiya hücumlarını təsnif edərkən onları beş kateqoriyaya ayırmışdır [10]:

1. İnformasiyanın toplanması;
2. İcazəsiz müdaxilə təşəbbüsləri;
3. Xidmətdən imtina;
4. Şübhəli aktivlik;
5. Sistem hücumları.

İlk 4 kateqoriya üzaq məsafədən hücumlara, sonuncu kateqoriya isə şəbəkədə həyata keçirilən xidmətdən lokal imtina hücumlarına aiddir.

İnformasiya müharibəsinin əsas istiqamətlərindən sayılan informasiya hücumlarının növləri və səbəbləri müxtəlif olduğundan onların təsnifatı da müxtəlif istiqamətlərdə aparılmalıdır [11]: hücum xarakterinə, məqsədinə, başlanğıc şərtə, situasiya şərtinə, yerləşməsinə, hücum müddətinə, hücum miqyasına və OSI modelinə görə (şəkil 2).





Şəkil 2. İnformasiya hücumlarının təsnifatı

İnformasiya hücumları

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. Ziyanverici əməliyyatlara və informasiya hücumlarına davamlı informasiya sistemlərinin yaradılması müəyyən 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.

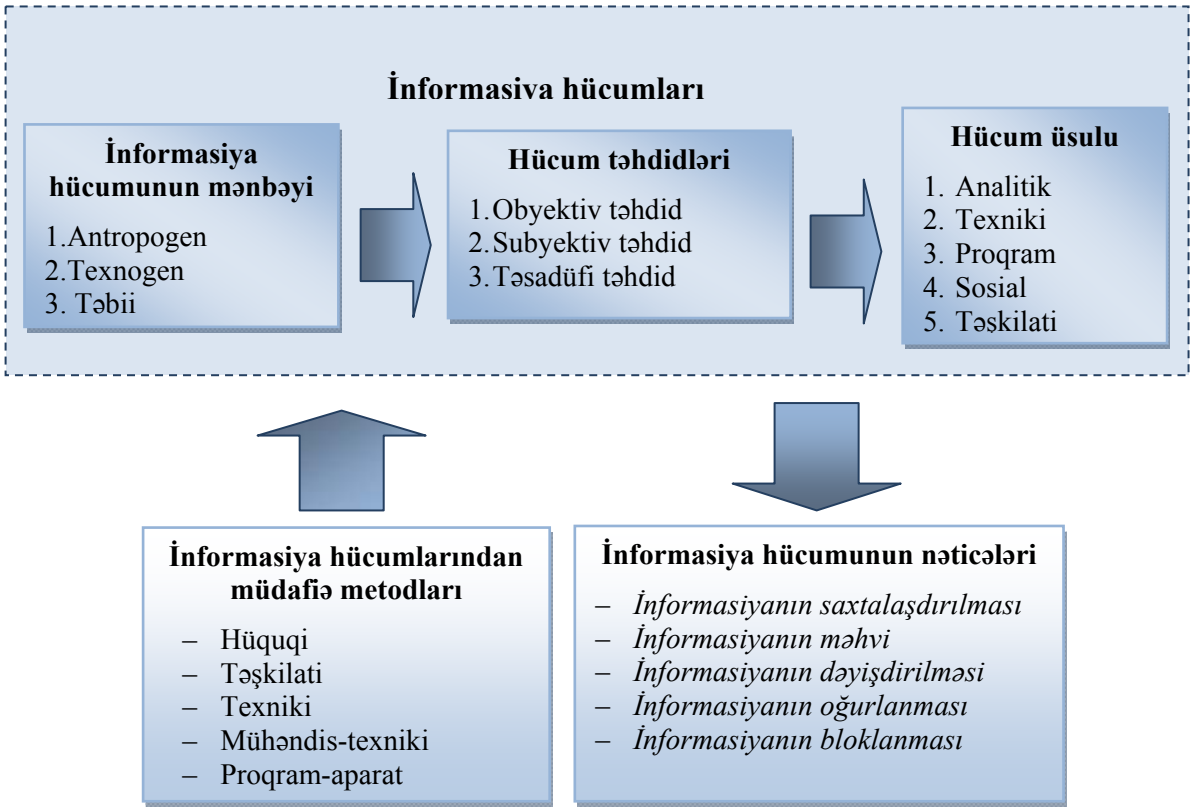
Kompyuter şəbəkəsinin təhlükəsizliyini təmin etmək üçün, ilk növbədə, bütün mümkün təhdidləri tədqiq etmək, daha sonra isə konkret vəziyyət üçün daha çox ehtimal olunan təhdidləri seçmək lazımdır. Bu zaman iki üsuldan istifadə etmək lazım gəlir [11]:

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.

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

1. Sistemə olan informasiya təhdidlərinin modelinin müəyyən edilməsi;
2. Sistemdəki boşluq kriterilərinin analiz edilməsi;
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 3).



Şəkil 3. İnformasiya hücumunda əməliyyatlar ardıcıllığı

İnformasiya hücumlarında istifadə olunan proqram və texniki vasitələr – informa-siya 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 kompüter virusları;
– məntiqi bomba – hərbi və ya mülki infrastruktura əvvəlcədən tətbiq edilmiş xüsusi proqram təminatıdır, siqnal və ya müəyyən edilmiş zamanda həmin proqram işə düşür;
– telekommunikasiya şəbəkələrində informasiya mübadiləsinin qarşısının alınması vasitələri, dövlət və hərbi idarə kanallarında informasiyanın saxtalaşdırılması;
– mətn proqramlarının neytrallaşdırılması vasitələri;
– obyektin proqram təminatlarına qarşı tərəfdən bilərəkdən müxtəlif növ səhvlərin daxil edilməsi.

İnformasiya hücumu vasitələri müxtəlif olduğu kimi, hücumun nəticələri də müxtəlif olur [12, 13]:

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 qoşulmasi 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.

İcazəsiz müdaxilə sistemdə baş verən nasazlıqlar vasitəsilə də həyata keçirilə bilər. Məsələn, istifadəçinin faylları açıq qalıbsa, hücum edən verilənlər bankının ona məxsus olmayan hissələrinə müdaxilə edə bilər.

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

3. *İnformasiyanın dəyişdirilməsi.* Son illər informasiya müharibələrində informasiyanın dəyişdirilməsi ilə bağlı əməliyyatlar daha çox yayılmışdır və icazəsiz müdaxilənin bir istiqaməti hesab edilir. Fərq yalnız ondan ibarətdir ki, bu növ informasiya hücumu ilə hər kəs yox, yalnız təcrübəli və yüksək ixtisaslaşmaya malik mütəxəssislər məşğul ola bilər. İnformasiya hücumu zamanı kompyuterdəki etibarlı informasiya digər saxta verilənlərlə əvəz edilir. Bu üsulla informasiya sistemindəki verilənləri dəyişərək müxtəlif cinayətlər həyata keçirmək mümkündür. Məsələn, sifarişçiyə tələb etdiyini deyil, başqa sənədin göndərilməsini, maliyyə hesablamalarında səhvlərin olmasını, səsvermələrdə səslərin dəyişdirilməsini həyata keçirmək olar.

4. *İnformasiyanın oğurlanması.* Ənənəvi oğurluğun qarşısını almağa xidmət edən cinayət məcəlləsinin qanunvericiliyi informasiya oğurluğu ilə bağlı hüquqi münasibətləri tənzimləyə bilmir. Bu sahədə informasiya hücumunun aşkar edilməsi və hücum edən tərəfin məsuliyyətə cəlb edilməsi müəyyən çətinliklər yaradır. Nəzərə almaq lazımdır ki, informasiya hücumu ilə məşğul olan şəxs çox zaman başqa ölkədə fəaliyyət göstərir.

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 [14].

İnformasiya hücumlarında istifadə olunan vasitələr

İnformasiya hücumlarında geniş istifadə olunan vasitələri realizə üsuluna görə üç sinfə bölmək olar [11]: *riyazi (alqoritmik), proqram və aparat* (şəkil 4).

Alqoritmik vasitələrə aiddir:

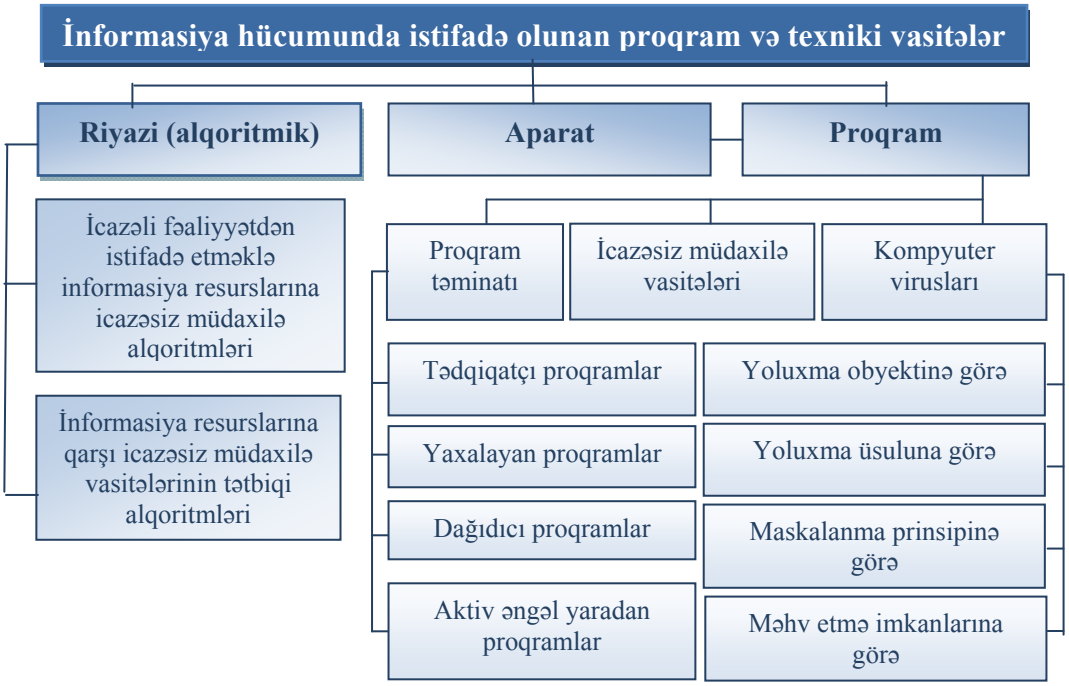
- İcazəli fəaliyyətdən istifadə etməklə informasiya resurslarına icazəsiz müdaxilə alqoritmləri;
- İcazəli proqram təminatından və icazəsiz müdaxiləyə imkan verən proqram vasitələrindən istifadə etməklə informasiya resurslarına icazəsiz müdaxilə alqoritmləri.

Proqram vasitələrinə informasiyanın saxlanması, emalı və ya göndərilməsi zamanı potensial təhlükəli sonluqla nəticələnən əməliyyatlara səbəb olan proqramlar aiddir. Potensial təhlükəli proqramlar dedikdə, aşağıdakı funksiyaları yerinə yetirə bilən bir çox proqramlar nəzərdə tutulur [15]:

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;
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 təhlükəsizlik sistemlərində test proqramlarının işini neytrallaşdıran proqramlar.

İnformasiya hücumlarında müxtəlif təhlükəli fəsadlar törədən proqramlar şərti olaraq 3 sinfə bölünür [11]:

– kompyuter virusları;
– icazəsiz müdaxilə vasitələri;
– ziyanlı proqramlar.



Şəkil 4. İnformasiya hücumlarında istifadə olunan proqram və texniki vasitələrin realizə üsuluna görə təsnifatı

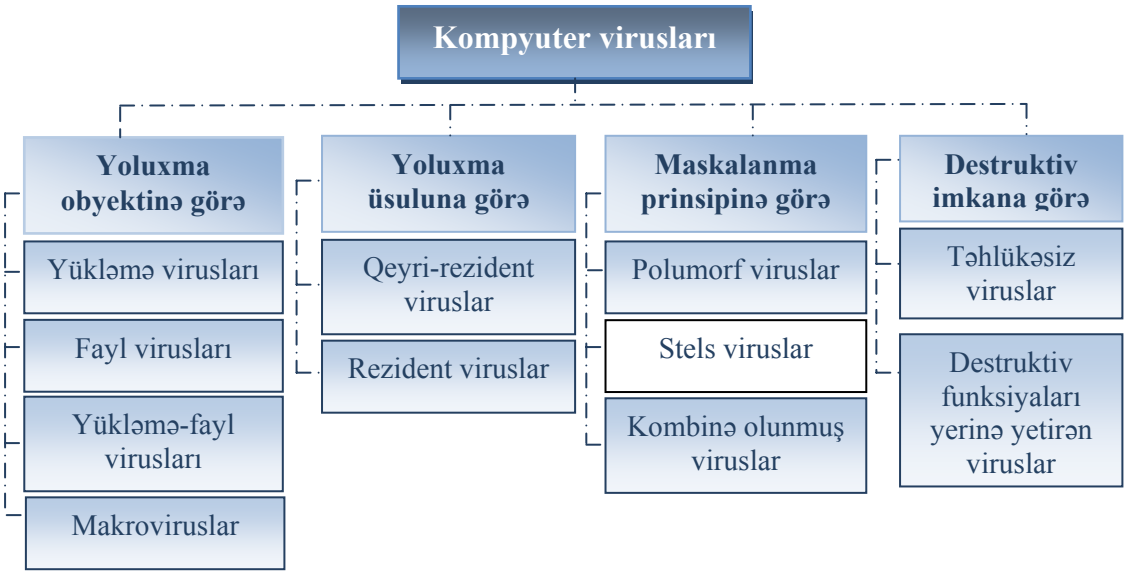
Kompyuter virusları

Kompyuter virusları müxtəlif vasitələrlə bir kompyuterdən digər kompyuterə keçməyə cəhd edən, verilənlərin dəyişdirilməsi və ya silinməsinə səbəb olan və ya istifadəçinin işinə mane olan, digər proqramlarda gizlənmiş kiçik həcmli proqramlardır [16]. Virus proqramları özlərini təxminən bioloji virus kimi aparır: çoxalır, maskalanır və ziyanlı təsirlər göstərir. Virus özgə informasiya daşıyıcılarından, elektron poçt və ya İnternet resurslardan istifadə edilən zaman təhlükə yarada bilər. Viruslar bütün kompyuter və şəbəkə mühitlərində yayıla bildiyindən, informasiya hücumlarında onlardan daha geniş istifadə edirlər [17].

Hal-hazırda informasiya hücumlarında istifadə olunan vasitələrin bütün növləri arasında kompyuter virusları daha çox təhlükəlidir. G Data Software şirkətinin 2010-cu ilin illik hesabatında bildirilmişdir ki, dünyada hər 15 saniyədə bir virus yaradılır və təhlükəli virusların sayı 2 mlyn.-dan artıqdır [18].

Virusun xüsusiyyətini onun konkret proqrama istiqamətlənmiş olmaması, öz-özünə çoxalma imkanına malik olması, proqramın daxilində yerləşməsi, əlaqə xətləri, kompyuter şəbəkəsi ilə ötürülməsi və informasiya sistemini sıradan çıxara bilməsi və s. təşkil edir. Kompyuter viruslarından informasiya təsiri sisteminin proqram modulu kimi istifadə olunması üçün virusların aşağıdakı əlamətlərə görə təsnifatı vacibdir (şəkil 5):

– 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: təhlükəsiz viruslar və destruktiv funksiyaları yerinə yetirən viruslar [16, 19].



Şəkil 5. Kompyuter viruslarının təsnifatı

İcazəsiz müdaxilə vasitələri

Ötən əsrin 90-cı illərindən başlayaraq İnternetdə informasiya müharibəsinin genişlənməsi ilə əlaqədar şəbəkə hücumlarının sayının kəskin artması müşahidə edilməyə başlandı. Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik icazəsiz müdaxilə vasitələrinin, kompyuter viruslarının yaradılması və tətbiqi üçün yeni imkanlar, yollar açdı. İnternet məkanından istifadə etməklə informasiya sistemlərinin və məxfi informasiyanın ələ keçirilməsi, kompyuter şəbəkələrinin viruslara yoluxma halları daha da çoxaldı [20].

İcazəsiz müdaxilə vasitələri müəyyən təhlükələrlə nəticələnən xüsusi proqramlar sinfidir və müasir informasiya müharibələrində onlardan geniş istifadə olunur. Belə proqramlara informasiya mübadiləsi şəbəkələrində mümkün proqram təminatları aid edilə bilər. Bu da qarşı tərəfin əməliyyat sistemlərinin işini və ya hesablama mühitinin bütövlüyünü pozmağa şərait yaradır. Çox zaman bu növ proqram təminatlarından müdafiə sistemlərinin analizi üçün istifdə edilir. Sonradan bu analizin nəticələrindən şəbəkədəki informasiya resurslarına icazəsiz müdaxiləni realizə etmək üçün istifadə olunur.

Ziyanlı proqram təminatı

Ziyanlı proqram təminatı – potensial təhlükəli nəticələrə səbəb olan proqramlardır. Bu proqramların icazəsiz müdaxilə vasitələrindən fərqi ondan ibarətdir ki, onlar mühafizəni dəf edə bilmirlər. Ziyanlı proqramları onların 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 proqramlarda, 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, şəbəkə soxulcanları aiddir [21].

Troyan proqramlar (Trojans) – sistemə qanuni 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. [21]:

- *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, sistem 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 resurslarına daxil olur. Bir qayda olaraq, spam tipli məlumatların yayılması 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 yoluxmuş kompyuterdən daxil edilən məlumatları, ekranın şəkillərini, aktiv proqram təminatları, ümumiyyətlə, istifadəçinin kompyuterdə gördüyü 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 ötürülməsi həyata keçirilir. Məntiqi bombalar müəyyən məntiqi əməliyyatlar zamanı bədniyyətli fəaliyyətləri 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 ziyanverici proqramın əməliyyat sistemi (proqram təminatı) daxilində imtiyazlı funksiyaları və ya ona icazə verilməyən iş rejimini idarə etməyə şərait yaradan xüsusi mexanizmdir. Məntiqi lyuka obyektin proqram təminatına bilərəkdən daxil edilən müxtəlif növ səhvləri 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 soxulcanı" hesab edilir [22]. 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 [23]:

- Təsir məqsədi ilə kompyuter şəbəkəsində axtarış (çox hallarda şəbəkə ünvanı məlum olan kompyuterin axtarışı);
- şəbəkə vasitəsilə informasiya sisteminə xüsusi proqram kodunun göndərilməsi;
- hücumuna məruz qalan kompyuterlərdəki informasiya sistemlərinin idarəetməsinin ələ keçirilməsi və s.

Analiz nəticəsində belə söyləmək olar ki, bütün proqram əlavələrini yaradılma məqsədlərinə görə siniflərə ayırmaq mümkündür: tədqiqatçı, ələ keçirici, dağıdıcı, aktiv maneə törədən proqramlar. Informasiya hücumlarında istifadə olunan proqram vasitələrinin universallığı, gizliliyi, çoxvariantlılığı, zaman və məkana görə qeyri-məhdud, ucuz başa gəlməsi bu vasitələri müasir dövrdə çox təhlükəli informasiya silahına çevirmişdir.

Nəticə

İnformasiya hücumunda proseslər ardıcıllığının ümumi sxeminin işlənməsi kompyuter şəbəkələrində informasiya hücumları ilə bağlı pozuntuların təyin edilməsində informasiya təhlükəsizliyi ilə əlaqədar işlərin görülməsində mühüm əhəmiyyətə malikdir. Göründüyü kimi, informasiya müharibəsində istifadə olunan hücum xarakterli proqramlar yalnız informasiya hücumları üçün deyil, eyni zamanda, hesablama mühitinin elementlərinin mühafizə sisteminin kəşfiyyatı və tədqiqatı üçün də nəzərdə tutulmuşlar. Məqalədə aparılan potensial informasiya hücumlarının təsnifi informasiya müharibəsində konkret vəziyyət üçün daha çox ehtimal olunan təhlükələrin seçilməsi üçün əhəmiyyətlidir.

Ədəbiyyat

1. Əliquliyev R.M., İmamverdiyev Y.N., E-dövlərin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2001, №1, s. 3-13.
2. Alan D., Douglas H. Cyberwar 3.0: Human factors in information operations and future conflict (Hardcover) // Afcea Intl Pr, 2000, 309 pp.
3. David Noel, Matrix Thinking Book I // BFC Press, Australia, 2004, 200 pp., http://www.aoi.com.au/matrix/MT.htm
4. Пархомов В.А. К определению понятия «Информационное преступление» // Вестник ИГЭА, 2001, № 2, с. 10–13.
5. Рассел Р. и др. Защита от хакеров коммерческого сайта: пер. с англ. – М.: Компания АйТи: ДМК пресс: ТЕТРУ, 2004, 552 стр.
6. 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.
7. Фефелова О., Фефелова И. Информационные войны как средство управления общественно-политическими процессами // Лаборатория рекламы, 2007, №1, с. 14–17.

8. Тестирование вычислительных сетей на проникновение. http://perimetr-ural.ru
9. Об атаках на компьютерные сети, http://www.i2r.ru
10. Способы нападений на компьютерные сети и защита от несанкционированного межсетевого доступа, http://library.tuit.uz
11. Гриняев С.Н. Интеллектуальное противодействие информационному оружию // М.: СИНТЕГ, 1999, 232 с.
12. Колесников Д.Г. Компьютерные атаки и технологии их обнаружения, http://web-protect.net
13. Вихорев С.В. Классификация угроз информационной безопасности. http://www.cnews.ru
14. Əliquliyev R.M., İmamverdiyev Y.M., Rəqəm imzası texnologiyası // "Elm", Bakı: 2003, 132 s.
15. Сердюк В.А**.** Вы атакованы – защищайтесь (методология выявления атак) // BYTE/Россия, 2003, №9 (61), с. 61–64.
16. Островский С.Л. Компьютерные вирусы, Выпуск 3.2 // М.: «Диалог Наука», 1997, 88 с.
17. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы // М.: «Диалог-МИФИ», 1996, 256 с.
18. G Data Malware Report, http://www.gdatasoftware.com/
19. J.Allen et al., State of the Practice of Intrusion Detection Technologies, Tech. Report CMU/SEI-99-TR-028, ESC-TR-99-028, Software Eng. Institute, Carnegie Mellon Univ., Pittsburgh; http://www.sei.cmu.edu
20. Əliquliyev R.M., Mahmudov R.Ş., İnternetin tənzimlənməsi problemləri // Ekspress-informasiya, Bakı: "İnformasiya Texnologiyaları", 2010, 116 s.
21. Виды угроз и атак – вирусы и черви // http://pc-secure.ru
22. Eugene H. Spafford, The Internet Worm Program: An Analysis // Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, 2004
23. 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 (5 July 2000), 1997.

УДК 004.49;004.056

Алекперова Ирада Я.
Институт Информационных Технологий НАНА, Баку, Азербайджан
depart17@iit.ab.az

Разработка общей схемы информационных атак в компьютерной сети на основе классификаций по разным аспектам

В статье рассмотрены существующие проблемы в связи с информационными атаками в компьютерных сетях, исследованы методы проведения атак. Проведена классификация информационных атак, а также классификация программных средств, использованная при атаках, исследована их активность в компьютерных сетях.

Ключевые слова: *информационная война, информационная атака, информационная система, логические бомбы, сетевые черви, аналитические системы.*

Irada Y. Alakparova
Institute of Information Technology ANAS, Baku, Azerbaijan
depart17@iit.ab.az

Development of a general scheme of information attacks in the computer network based on the classification of different aspects

The actual problems in relation to information attacks in the computer network were given in the article , the methods of carrying out of these attacks were investigated. There was held on the classification of information attacks, the classification of software applications used for information attacks and additionally was explored their activity in computer networks in the given article
Key words: *information warfare, information attack, information system, logic bombs, net worms, analytical systems.*