Mündəricat

GİRİŞ

Elmi – tərəqqi tərəqqi informasiya mədəniyyətinin qloballaşması və formalaşması istiqamətində bəşəriyyətin təkamülünü misilsiz dərəcədə sürətləmmişdir. Nəticədə, milli – dövlət sərhədləri informasiya resurslarının axını, telekommunikasiya sistemlərinin qlobal kompüter şəbəkələrinin fəaliyyəti, transmilli biznes üçün şəffaf olmuşdur. Müasir dövrdə informasiya texnologiyalarının inkişaf səviyyəsi elə həddə çatmışdır ki, dünyada informasiya resursları, habelə pul vasitələri yer kürəsinin bir neçə saniyəyə dövr etmək imkanına malikdir.

Belə bir fikir mövcuddur ki, hər hansı kritik həddi aşdıqdan sonra, hətta elmi – texniki tərəqqi də, bəşəriyyətin mənfinə işləməyə başlayır. Misal olaraq, müasir dağıdıcı silahları, nüvə texnologiyasını və.s göstərmək olar. Elmi – texniki tərəqqi bu gün elə sürətlə inkişaf edir ki, onun doğuracağı bəzi fəsadlar cəmiyyət tərəfində çox gec başa düşülür. Vaxtı ilə sənayenin inkişafı ekologiya sahəsində ciddi problemlər doğurmuşdur.

Analoji situasiya hazırda informasiya texnologiyaları sahəsində də yaranmışdır. Yeni informasiya texnologiyalarının inkişafı şəxsi, təşkilar və dövlət səviyyəsində informasiya resursları üçün təhlükələrin meydana gəlməsinə səbəb olmuşdur. Bu gün İnternet şəbəkəsi bütün yer kürəsini hörümçək toru ilə örtmüşdür. Yer kürəsinin istənilən nöqtəsindən İnternet şəbəkəsinə qoşulmaq, onun vasitəsilə müxtəlif növ məlumatları ötürmək və almaq mümkündür. Paylanmış kompüter şəbəkələrindən ibarət olan İnternet

şəbəkəsinin xidmətləri istifadəçilərə öz iş yerlərini və evlərini tərk etmədən dünyanın, praktiki olaraq, istənilən nöqtəsində olan müxtəlif informasiya sistemlərinə və ya məlumat bazalarına qoşulmaq eləcə də onları

maraqlandıran zəruri informasiya ilə tanış olmaq və məlumatları əldə etmək imkanları verir.

İnternet şəbəkəsinin istifadəçilərinin sayı astronomik sürətlə artır. Açıq informasiya mənbələrinin məlumatlarına görə, bu gün İnternet dünyanın 160 – dan artıq ölkəsini əhatə edir. 1998 – ci ildə İnternet şəbəkəsinə, təxminən, 143 milyon istifadəçi qoşulmuşdusa, 2002 – ci ildə onların sayı 700 milyonu ötüb keçmişdir. Hazırda İnternetin istifadəçilərinin sayı ABŞ – da 158, Avropada – 95, Asiyada – 90, Latın Amerikasında – 14, Afrikada – 3, Rusiyada – 8, Ukraynada isə 1 milyondan çoxdur. Azərbaycanda İnternet şəbəkəsinin xidmətlərindən istifadə edənlərin sayı yüz minlərlə ölçülür.

Qeyd olunduğu kimi müasir informasiya texnologiyalarının tətbiqi ilə bağlı olan elmi – texniki tərəqqinin inkişafı yeni növ ciddi problemlərin meydana gəlməsinə səbəb olmuşdur. Xüsusi halda bu problemlərə kompüterlərin, komptüer sistemlərinin və şəbəkələrinin işinə qeyri – qanuni müdaxilə, kompüter informasiyasının oğurlanması, mənimsənilməsi, zorla, şantaj yolu ilə alınması kimi təhlükəli yeni sosial təzahürləri aid etmək olar. Bu təhlükələr “kompüter cinayətkarlığı” və “kompüter terrorçuluğu” adlarını almışdır.

Yeni texnologiyalar inkişaf etdikcə cinayətlərin struktutu da dəyişir. Baş verməsi, gizlədilməsi mexanizmlərinə və üsullarına görə kompüter cinayətləri müəyyən xüsusiyyətlərə malik olur. Bu cinayətlər ənənəvi cinayətlərdən fərqli olaraq, gizli qalmasının yüksək, açılmasının isə aşağı səviyyəsi ilə xarakterizə olunur.

Tam əminliklə demək olar ki, bu gün telekommunikasiya sistemləri və kompüter şəbəkələri, o cümlədən İnternet şəbəkəsi siyasətçilər, iş adamları, dini təşkilatlar, terrorçu qruplar, cinayətkar qruplaşmalar, habelə rəqib (düşmən) ölkələrin xüsusi xidmət orqanları tərəfindən informasiya mübarizəsi, qarşıdurması, hətta müharibəsi vasitəsi və aləti kimi istifadə olunur.

Aydındır ki, İnternet şəbəkəsi istifadəçi qismində onun xidmətlərindən istifadə edə biləcək hər bir şəxsə o cümlədən, cinayətkara və terrorçuya da öz cinayətkar niyyətlərini həyata keçirmək üçün tamamilə eyni imkanlar yaradır.

Ümumiyyətlə, kompüter cinayətlərini iki kateqoriyaya bölmək olar:

- kompüterlərin kriminal fəaliyyətə kömək vasitəsi kimi istifadə olunduğu cinayətlər, məsələn, saxta şəxsiyyət vəsiqələrinin istehsalı, müəllif materiallarının başqasının adından verilməsi və.s;

- kompüterlərin hücumunun məqsədi, hətta silahı kimi istifadə olunduğu cinayətlər, məsələn, informasiyanın oğurlanması və ya korlanması məqsədilə təşkilatlara hücum edilməsi qeyri-qanuni maliyyə əçəliyyatlarının aparılması, kredit kartlarının kodlarının oğurlanması və digər hərəkətlər;

Dövlətin milli təhlükəsizliyinin vacib tərkib hissələrindən biri kimi informasiya təhlükəsizliyinin təmin edilməsi məsələsi transmilli (sərhədsiz) kompüter cinayətkarlığının və kiberterrorçuluğunun meydana gəlməsi kontekstində xüsusi ilə kəskin şəkildə ortaya çıxır.

Bu gün kompüter cinayətkarlığı və kiberterrorçuluq hüquq mühafizə orqanlarının nəzarətindən çıxaraq dövlət və beynəlxalq səviyyədə ciddi problemə, təhlükəyə çevrilmişdir. Beynəlxalq cinayətlərə aid edilən bu növ cinayətləri öz miqyasına görə yalnız nüvə, bakterioloji və kimyəvi silahlarla müqayisə edirlər.

Beynəlxalq cinayətlərə aid edilən bu növ cinayətləri öz miqyasına görə yalnız nüvə, bakterioloji və kimyəvi silahlarlamüqayisə edirlər.Eyni zamanda nəzərə almaq lazımdır ki, bu təhlükənin səviyyəsi hələ də insanlar tərəfindən sonadək dərk olunmamış və öyrənilməmiş qalır.

FƏSİL I. KOMPÜTER SİSTEMLƏRİNDƏ VƏ ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ ƏSASLARI

§1.1. İnformasiya təhlükəsizliyi problemi və onu xarakterizə edən əsas amillər

Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyinin pozulmasının bütün mümkün hallarını, əsasən, üç kateqoriyaya ayırmaq olar:

- informasiyanın məxfiliyinin pozulması təhlükəsi;
- informasiyanın tamlığının pozulması təhlükəsi;
- sistemin iş qailiyyətinin pozulması (xidmətin göstərilməsindən imtina) təhlükəsi.

Məxfiliyin pozulması təhlükələri məxfi informasiyanın və ya sirlərin açılmasına yönəlmiş olur. Bu növ təhlükələr reallaşdıqda informasiya ona giriş hüququ olmayan şəxslərin əlinə keçə və ya onlara bəlli ola bilər. Kompüter sistemlərində və şəbəkələrində saxlanılan və ya ötürülən məxfi informasiyaya hər dəfə icazəsiz giriş əldə edildikdə və ya buna cəhd göstərildikdə onun gizliliyinin pozulması təhlükəsi yaranır.

Kompüter sistemlərində və şəbəkələrində saxlanılan və ya ötürülən *informasiyanın tamlığının pozulması təhlükələri* onun təhrif olunmasına, keyfiyyətin polzulmasına və ya tam məhvinə gətirib çıxaran dəyişikliklərin edilməsi ilə xarakterizə olunur. İnformasiyanın tamlığı ziyankar (bədəməl) şəxslərin düşünülmüş fəaliyyəti, eləcə də ətraf mühitin obyektiv təsiri nəticəsində pozula bilər.

Sistemin iş qabiliyyətinin pozulması (xidmətin göstərilməsindən imtina edilməsi) təhlükəsi müəyyən düşünülmüş hərəkətləri, eləcə də təsadüfi hadisə və proseslər nəticəsində kompüter sistemlərinin və şəbəkələrinin fəaliyyətinin pozulmasına, iş qabiliyyətinin zəifləməsinə, informasiya resurslarına icazəli və ya qanuni girişin məhdudlaşdırılmasına, tamamilə bağlanmasına gətirib çıxaran vəziyyətlərin reallaşdırılmasına yönəlmiş olur. Kompüter sistemlərinin və şəbəkələrinə, onların informasiya resurslarına yönəlmiş bu təhdidlərin təsnifatına uyğun olaraq onların qarşısının alınması və informasiya təhlükəsizliyinin təminedilməsi məsələsinə də, əsasən, üç aspektdən baxılır. Bu istiqamətlər informasiya təhlükəsizliyinin üç əsas baza prinsipini müəyyən edir:

- informasiyanın gizliliyinin təmin edilməsi;
- informasiyanın tamlığının təmin edilməsi;

- informasiyaya əl yetərliyinin təmin edilməsi (informasiyaya icazəli girişin təmin edilməsi və ya informasiyanın təcrid edilməsinin qarşısının alınması).

İnformasiyanın gizliliyinin təmin edilməsi dedikdə informasiyaya giriş hüququ olan istifadəçilər qrupunun müəyyənləşdirilməsi, informasiyaya, onun saxlandığı, emal olunduğu, ötürüldüyü sistem və şəbəkələrə kənardan, ələlxüsus icazəsiz müdaxilələrin və müdaxilə cəhdlərinin qarşısının alınması başa düşülür. İnformasiyanın gizliliyi – onun məzmununun icazəsi olmayan digər istifadəçilərdən və kənar şəxslərdən gizli saxlanılması xassəsidir. Bu, icazəsiz olaraq məxfi informasiyanın məzmununun açılması, proqramların, məlumat bazalarının sistem cədvəllərinin və parametrlərinin istifadəsi və onlara müdaxilə təhlükələrinin qarşısının alınmasının təmin edilməsini nəzərdə tutur.

İnformasiyanın tamlığının təmin edilməsi – sistemdə saxlanılan, emal olunan və ötürülən informasiyanın təhrif olunmamış (yəni onun hər hansı qeyd olunmuş vəziyyətinə münasibətdə dəyişilməmiş) şəkildə mövcud olmasının təmin edilməsinin özündə ehtiva edir. İnformasiyanın bu xassəsi onun icazəsiz olaraq qəsdən və ya təsadüfən dəyişdirilməsinə, korlanmasına, blokirovkasına və ya məhv edilməsinə, eləcə də informasiyanın itirilməsinə gətirib çıxaran proqram – texniki nasazlıqlar və sıradan çıxmalar kimi təhlükələrdən də qorunmasını tələb edir.

İnformasiyaya girişin təmin edilməsi – informasiyanın saxlanılması, emalı və ötürülməsi sistemlərinin (mühitinin, vəsaitlərinin və texnologiyalarının) etibarlılıq və sıradançıxmalara davamlılıq xassələrinə qoyulan başlıca tələb olub, informasiya və sistem resurslarına icazəli girişə rədd cavablarının verilməsinin qarşısının alınması, istifadəçilərin onları maraqlandıran və giriş hüquqları olan bütün informasiya resurslarına maneəsiz və vaxtında girişinin təmin edilməsi, eləcə də istifadəçilərdən daxil olan bütün sorğuların müvafiq avtomatlaşdırılmış xidmətlər tərəfindən yerinə yetirilməsi qabiliyyətini xarakterizə edir.

Başqa sözlə, kənardan daxilolmanı (nüfuzetməni) və informasiyaya icazəsiz girişi reallaşdırmağa imkan verən boşluqların, spesifik kanalların və zəif yerlərin olması belə sistemlər üçün xarakterikdir. Bu isə əsasən, aşağıda göstərilən xüsusiyyətlərlə xarakterizə olunur:

- sistemin komponentləri bir-birindən ərazicə uzaq məsafədə yerləşir və onlar arasında intensiv informasiya mübadiləsi həyata keçirilir;

- informasiyanın saxlanılması, emalı və ötürülməsi üçün istifadə edilən üsulların, kompüter texnikasının, telekommunikasiya vasitələrinin və rabitə kanallarının, eləcə də proqram təminatının spektri genişdir;

- müxtəlif subyektlərə aid olan müxtəlif təyinatlı məlumatlar vahid məlumat bazası çərçivəsində inteqrasiya olunur və əksinə, hər hansı subyektə lazım olan informasiya kompüter şəbəkəsinin uzaq məsafələrdə olan müxtəlif qovşaqlarında yerləşir;

- informasiya sahibləri fiziki strukturlardan və informasiyanın saxlanması yerlərindən təcrid edilmiş olur;

- paylanmış informasiya emalı üsullarından istifadə edilir;

- avtomatlaşdırılmış informasiya emalı prosesində çoxlu sayda istifadəçi və müxtəlif kateqoriyalı personal iştirak edir;

- şəbəkədə olan resurslardan (o cümlədən informasiya resurslarından) çoxlu sayda və müxtəlif kateqoriyalı istifadəçilər birbaşa və eyni zamanda istifadə edir;

- informasiya emalı sistemlərində geniş istifadə edilən texniki vəsaitlərin çoxunda aparat səviyyəsində xüsusi qoruma vasitələri reallaşdırılmır.

§1.2. Kompüter sistemlərində və şəbəkələrində informasiyanın sızması yolları

Kompüter şəbəkələrində informasiya təhlükəsizliyi baxımından *zəif yerlər* dedikdə kompüter və şəbəkə resurslarının, o cümlədən proqram-texniki və informasiya təminatının, rabitə kanallarının təhlükəsizliyinin pozulmasının daha çox ehtimal edildiyi, sistemə və şəbəkə resurslarına qanunsuz və icazəsiz daxilolmaların (soxulmaların) mümkün olduğu yerlər (qovşaqlar, komponentlər) başa düşülür.

Müxtəlif kompüterləri, telekommunikasiya qurğularını, rabitə kanallarını, informasiyanın saxlanması, emalı və ötürülməsi vasitələrini özündə birləşdirən kompüter şəbəkələrində təhlükəsizliyin pozulmasma daha asan və tez-tez məruz qala biləcək əsas funksional struktur komponentlərə aşağıdakılar aid edilir:

- *işçi stansiyalar* - istifadəçilərin (abonentlərin, operatorların) avtomatlaşdırılmış iş yerlərinin reallaşdırıldığı ayrı-ayrı kompüterlər və ya uzaq məsafədə yerləşən terminallar;

- *serverlər* - böyük həcmdə məlumatların toplanması, saxlanılması, emal edilməsi, istifadəçilərə müxtəlif xidmətlərin göstərilməsi funksiyalarını reallaşdıran, böyük yaddaşa və sürətə malik olan kompüterlər;

- *telekommunikasiya qurğuları* - informasiyanın emalı və ötürülməsi şəbəkələrində və ya onlar arasında müxtəlif qarşılıqlı əlaqə protokolları ilə işləyən, bir neçə seqmentin birləşdirilməsini təmin edən elementlər (şəbəkələrarası körpülər, şlüzlər, kommutatorlar, konsentratorlar, kommutasiya mərkəzləri və.s);

- *rabitə kanalları* - lokal, telefon (ayrılmış və ya kommutasiya edilən) və optik rabitə xətləri, radio və peyk kanalları.

İnformasiyanın sızmasının və ona icazəsiz girişin əldə olunmasının əsas yolları aşağıdakılardır:

- şəbəkə avadanhqlarına və rabitə xətlərinə qoşulma;

- elektromaqnit şüalanmalarınuı tutulması;

- uzaq və yaxm məsafədən şəkilçəkmə;
- qulaqasma qurğularının tətbiq edilməsi;
- informasiya daşıyıcılarının, çap olunmuş vərəqlərin və istehsal məsrəflərinin oğurlanması və məhv edilməsi;
- icazəsi olan (həqiqi) istifadəçilər sistemdə işləyən zaman onun "ilişməsindən" istifadə edərək onun adı altında sistemə qoşulma;
- qeydiyyatdan keçmiş istifadəçilərin terminallarından icazəsiz istifadə edilməsi;
- parolların və girişi məhdudlaşdıran digər rekvizitlərin oğurlanması yol ilə qeydiyyatdan keçmiş istifadəçilərin adı altında maskalanaraq sistemə daxil olma;
- istifadəçi səlahiyyətindən istifadə etməklə digər istifadəçilərin informasiya massivlərindən məlumatların oxunması;
- əməliyyat sisteminin və ya icazəsi olan istifadəçilərin sorğuları altında pərdələnmək yolu ilə sistemə daxilolma və məlumatların əldə edilməsi;
- icazəli sorğu yerinə yetirildikdən sonra yaddaş qurğusundan qalıq informasiyanın oxunması;
- informasiya daşıyıcılarında olan məlumatların köçürülməsi;
- proqram "tələlərinin" və qoyuluşların istifadə edilməsi;
- sistemə və ya proqramlara "troya atlar'ının daxil edilməsi;
- kompüter viruslarına bilmədən yoluxma və ya qəsdən yoluxdurma;
- icazə verilən əməliyyatlar kombinasiyasını tətbiq etmək yolu ilə qorunan məlumatların əldə keçirilməsi;

- proqramlaşdırma dillərində, əməliyyat sistemlərində və şəbəkə proqram təminatında olan boşluqların və çatışmazlıqların istifadə olunması;

- tətbiqi proqram təminatının, informasiya resurslarının və məlumatların qəsdən korlanması, sistemin parametrlərinin dəyişdirilməsi;

- texniki qurğularda və şəbəkə analizatorlarında baş verən nasazlıqlardan və sıradan çıxmalardan istifadə olunması.

Kənar şəxslərin sistemə müdaxiləsinin, sistemə təsir edən və ya edə biləcək hadisələrin və informasiyanımn sistemdən kənara sızmasınm bütün mümkün hallarını ümumi halda iki yerə bölmək olar:

- birbaşa müdaxilə;

- dolayı yolla müdaxilə.

Birbaşa müdaxilə zamanı ziyankar bilavasitə sistemin komponentlərinin yerləşdiyi yerə (binaya, otağa və s.) daxil olur. Birbaşa müdaxilə sistemin komponentlərində dəyişiklik etmədən və ya onları dəyişdirmək yolu ilə baş verə bilər. *Dolayı yolla müdaxilə* zamanı isə informasiyanın əldə edilməsi və ya sıradan çıxarılması üçün sistemin komponentlərinin yerləşdiyi yerə (otağa və ya binaya) girmək tələb olunmur.

§1.3. İnformasiya təhlükəsizliyinə olan təhdidlərin təsnifatı

Təhlükəsizliyin pozulması təhlükəsi (təhdidlər) dedikdə ayrı-ayrı şəxslərin və ya təşkilatların maraqlarına ziyan vurulmasına gətirib çıxaran, informasiyanın təsadüfən və ya düşünülmüş şəkildə (qəsdən) məhv edilməsi, icazəsiz açılması və dəyişdirilməsi təhlükəsini yaradan, şəbəkədə və ya kompüterlərdə saxlanılan, emal olunan və ötürülən, eləcə də qorunan informasiyaya qeyri-qanuni və icazəsiz girişin əldə olunması imkanlarını yaradan mümkün potensial hadisələr, hərəkətlər və təsirlər başa düşülür.

Kompüter şəbəkələrində mümkün potensial təhlükələri onların əmələgəlmə təbiətinə görə iki kateqoriyaya ayırmaq olar:

- təbii təhlükələr;
- süni təhlükələr.

Təbii təhlükələr - insanlardan asılı olmadan baş verən obyektiv fiziki proseslərin və ya təbiət hadisələrinin kompüter sistemlərinə və şəbəkələrinə, eləcə də onların elementlərinə təsiri nəticəsində yaranan təhlükələrdir. Təbii təhlükələri təbii fəlakətlər və təsadüfi amillər kimi iki qrupa bölmək olar.

Təbii fəlakətlərə yanğın, su basma, zəlzələ, ildırım, torpaq sürüşməsi və s. aid edilir. Bu təhlükələrin qarşısını almaq üçün kompüter sistemləri və

şəbəkələri, eləcə də onların yerləşdiyi bina və ya otaqlar layihələndirilən zaman bəzi məqamlar nəzərə alınmalıdır.

Belə ki, yanğın, su basma, zəlzələ və digər təbii hadisələr baş verdikdə kompüter texnikasının, telekommunikasiya qurğularının və digər informasiya daşıyıcılarının, eləcə də onlarda saxlanılan və emal olunan məlumatların təhlükəsizliyinin təmin edilməsi üçün binaların tikintisi zamanı müvafiq tədbirlər görülməlidir. Yanğından mühafizə sistemi qurularkən nəzərə alınmalıdır ki, yanğının söndürülməsi prosesində istifadə olunan su və digər vasitələr kompüter texnikasına, qurğu və avadanlıqlara ciddi xəsarət vurmasın.

Təsadüfi təhlükələr informasiya təhlükəsizliyinin pozulmasının daha tez-tez rast gəlinən formalarıdır. Bu növ təhlükələrə nümunə kimi gərginliyin gözlənilmədən (təsadüfən) qalxması və düşməsi, elektrik cərəyanının kəsilməsi, maqnit sahəsinin təsiri, birləşdirici kabellərin, qurğuların və sərinlətmə sisteminin sıradan çıxması və s. kimi hadisələri göstərmək olar.

Elektrik nasazlıqları yarandıqda ağır nəticələrin qarşısını almaq üçün texniki vəsaitlər, qurğular və avadanlıqlar elektrik xəttinə sabitləşdirici qurğular (stabilizatorlar) və ya gərginlik filtrləri, eləcə də fasiləsiz qidalanma mənbələri vasitəsilə qoşulur.

Avadanlıqlarda baş verən nasazlıqlar, kabellərin və kommunikasiya vasitələrinin sıradan çıxması ciddi informasiya itkisinə səbəb ola bilər. Maqnit sahəsinin maqnit informasiya daşıyıcılarına təsiri nəticəsində bu qurğularda saxlanılan informasiya təhlükəyə məruz qala və korlana bilər.

Sərinlətmə sisteminin işinin dayanması avadanlıqların və kompüter texnikasının texniki işləmə şərtlərinin təmin edilməməsinə, bu isə öz növbəsində onların düzgün fəaliyyətinin pozulmasına gətirib çıxara bilər.

Süni təhlükələr - kompüter sistemlərində və şəbəkələrində insanların fəaliyyəti və təsiri nəticəsində meydana çıxan təhlükələrdir. Yaranma səbəblərini və hərəkətlərin əsaslarını nəzərə alaraq süni təhlükələri iki yerə ayırırlar:

- *qəsdən törədilməyən (qərəzsiz və ya təsadüfən baş verən) təhlükələr* - kompüter sistemlərinin və şəbəkələrinin, eləcə də onların elementlərinin layihələndirilməsi, proqram-texniki təminatın işlənib hazırlanması prosesində, işçi personalın fəaliyyətində və s. səhlənkarlıq, səriştəsizlik və təcrübəsizlik səbəbindən buraxılan səhvlər nəticəsində yaranır. Belə təhlükələr informasiyanın sahibinə ziyan vurmaq məqsədi daşımır;

- *qəsdən törədilən (qərəzli) təhlükələr - i*nsanların (ziyankarların) bəd niyyətli (məkrli) fəaliyyəti nəticəsində yaranan təhlükələrdir.

Kompüter sistemlərində və şəbəkələrində təsadüfən baş verən, yəni qəsdən törədilməyən təhlükələrə, əsasən, aşağıdakıları aid etmək olar:

- sistemin qismən və ya tam sıradan çıxmasına, aparat, proqram və informasiya resurslarının məhvinə (avadanlıqların korlanması, vacib məlumatları özündə saxlayan faylların və proqramların, o cümlədən sistem fayllarının pozulması və təhrif edilməsi və s.) gətirib çıxaran düşünülməmiş hərəkətlər;

- icazə olmadan avadanlıqların söndürülməsi və ya qurğu və proqramların iş rejimlərinin dəyişdirilməsi;

- informasiya daşıyıcılarının bilməyərəkdən xarab edilməsi;

- səriştəsiz istifadə səbəbindən sistemin iş qabiliyyətinin itməsinə (ilişməsinə) gətirib çıxaran texnoloji proqramların yüklənməsi və ya sistemdə bərpası mümkün olmayan dəyişikliklərin aparılması (informasiya daşıyıcılarının formatlaşdırılması və ya strukturunun dəyişdirilməsi, məlumatların və ya faylların pozulması və s.);

- sistem resurslarının izafi məsrəfinə (prosessorun yüklənməsinə, əməli yaddaşın və xarici informasiya daşıyıcılarında olan yaddaşın udulmasına) səbəb ola biləcək nəzərdə tutulmamış proqramların qeyri-leqal tətbiqi və icazəsiz istifadəsi;

- kompüter viruslarına yoluxma;
- məxfi məlumatın yayılmasına gətirib çıxaran və ya ümumi istifadəsinə imkan yaradan ehtiyatsız hərəkətlər;
- sistemin fəaliyyətinə və informasiyanın təhlükəsizliyinə təhdidlərin reallaşdırılmasına imkan verən arxitekturanın layihələndirilməsi, məlumatların emalı texnologiyalarının və tətbiqi proqramların işlənib hazırlanması;
- sistemdə işləyən zaman müəyyən edilmiş qaydalara və təşkilatlara məhdudiyyətlərə riayət olunmaması;
- mühafizə vasitələrindən yan keçməklə sistemə daxilolma (məsələn, disketlərdən digər əməliyyat sisteminin yüklənməsi yolu ilə sistemə daxilolma və s.);
- təhlükəsizlik vasitələrinin xidməti personal tərəfindən səriştəsiz istifadəsi, onların parametrlərinin dəyişdirilməsi və icazəsiz söndürülməsi;
- istifadəçinin (abonentin) və ya kompüterin ünvanının səhv göstərilməsi səbəbindən məlumatların başqa ünvana göndərilməsi;
- səhv məlumatların daxil edilməsi;
- bilməyərəkdən rabitə kanallarının sıradan çıxarılması və korlanması.

Göründüyü kimi, qəsdən törədilməyən təhlükələr, əsasən, informasiyanın emalına hazırlıq, eləcə də bilavasitə emal prosesində buraxılan səhvlər nəticəsində meydana çıxa bilər.

İnformasiya təhlükəsizliyinə qarşı yönəlmiş qəsdən törədilən təhlükələr informasiya resurslarına, onların saxlandığı, emal olunduğu, ötürüldüyü sistemlərə icazəsiz girişin əldə olunmasına yönəlmiş olur və iki qrupa bölünür:

- kompüter sistemlərinin və şəbəkələrinin, informasiya resurslarının, ayrı-ayrı kompüterlərin və digər avadanlıq və qurğularının qanuni istifadəçiləri

tərəfindən törədilən təhlükələr;

- istifadəçi olmayan kənar şəxslər tərəfindən həyata keçirilən təhlükələr.

Sistemin və onun komponentlərinin işinin pozulmasına, sıradan çıxmasma, sistemə və informasiyaya icazəsiz daxilolmaya, sistem və informasiya resurslarının əldə edilməsinə və ya təcrid olunmasına və s. səbəb olan, düşünülmüş şəkildə həyata keçirilən təhlükələrə, əsasən, aşağıdakıları aid etmək olar:

- sistemin fiziki məhv edilməsi (partlatma, yandırma və s.), onun bütün və ya bəzi daha vacib komponentlərinin (qurğuların, vacib sistem məlumatlarının daşıyıcılarının, xidməti personala daxil olan şəxslərin və s.) sıradan çıxarılması;

- kompüter şəbəkəsinin və sisteminin fəaliyyətini təmin edən alt sistemlərin (elektrik qidalanması, sərinləşdirici, hava dəyişən qurğular, rabitə və və s.) söndürülməsi və ya sıradan çıxarılması;
- sistemin fəaliyyətinin pozulmasına səbəb olan hərəkətlər (qurğuların və ya proqramların iş rejimlərinin dəyişdirilməsi, tətil, işçi personalın sabotajı, sistem qurğularının iş tezliklərinə uyğun güclü radiomaneələrin qoyulması və s.);
- sistemin işçi personalı arasına (o cümlədən təhlükəsizliyə məsul olan inzibatçılar qrupuna) agentlərin yeridilməsi;
- müəyyən səlahiyyətlərə malik olan personalın və ya istifadəçilərin cəlb edilməsi (maddi maraqlandırmaq, hədə-qorxu gəlmək və s. yolla);
- qulaqasma, uzaq məsafədən şəkil və video çəkmə qurğulaının və s. tətbiqi;
- qurğulardan və rabitə xətlərindən kənar elektromaqnit, akustik və digər şüalanmaların tutulması, eləcə də informasiya emalında bilavasitə iştirak etməyən texniki vasitələrin (telefon və elektrik xətlərinin, qızdırıcı qurğuların və s.) istifadəsi;

- rabitə kanalları vasitəsilə ötürülən məlumatların tutulması və mübadilə protokollarının, əlaqəyə girmə və istifadəçilərin avtorizə edilməsi

qaydalarının öyrənilməsi və gələcəkdə sistemə keçmək üçün istifadəsi;

- informasiya daşıyıcılarının (maqnit disklərinin və lentlərinin, CD

disklərin, mikrosxemlərin, əməli yaddaşların və bütövlükdə kompüterin)

və istehsal tullantılarının (çap vərəqlərinin, yazıların, istehsaldan çıxarılmış informasiya daşıyıcılarının və s.) oğurlanması;

- informasiya daşıyıcılarının məzmunlarının icazəsiz köçürülməsi;

- əməli yaddaşdan və xarici yaddaş qurğusundan qalıq informasiyanın oxunması;

- parolların və girişi məhdudlaşdıran digər rekvizitlərin qeyri- qanuni

yolla (agentlərin köməyi ilə, istifadəçilərin səhlənkarlığından istifadə etməklə, seçmə üsulu ilə, sistemin interfeysini imitasiya etməklə və s.) alınması və sonradan qeydiyyatdan keçmiş istifadəçinin adı altında maskalanma;

- istifadəçilərin unikal fiziki xassələrə (işçi stansiyanın şəbəkədə nömrəsi, fiziki ünvan, rabitə sistemində ünvan, kodlaşdırma üçün aparat bloku və s.) malik olan terminallarının icazəsiz istifadəsi;

- informasiyanın kriptoqrafik qorunması şifrlərinin açılması;

- xüsusi aparat vasitələrinin, proqram və aparat qoyuluşlarının,

eləcə də virusların (o cümlədən "troya atları"nın və "qurd"ların) tətbiqi, nəzərdə tutulmuş funksiyaların yerinə yetirilməsi üçün lazım olmayan lakin mühafizə sistemini keçmək, qeydiyyata düşmək, vacib məlumatları

tutulmuş funksiyaların yerinə yetirilməsi üçün lazım olmayan, lakin mühafizə

sistemini keçmək, qeydiyyata düşmək, vacib məlumatları ötürmək və ya sistemin fəaliyyətinin pozmaq məqsədilə sistem resurslarına gizli və qeyri-qanuni daxilolma imkanlarını reallaşdıran proqramlar; -

dezinformasiya aparmaq və yanlış məlumatları yaymaq məqsədilə qanuni istifadəçi sistemə daxil olduqdan sonra onun kompüterini şəbəkədən fiziki

ayırmaq və sonradan onun adı altında autentifikasiya proseduraşını uğurla keçmək (adlamaq) yolu ilə bilavasitə bu istifadəçini əvəz etmək üçün rabitə xətlərinə qeyri-qanuni qoşulma.

§1.4. Kompüter virusları informasiya təhlükəsizliyinə təhdid kimi

Xüsusi şəkildə proqramlara daxil edilən, kompüterin digər proqramlarına, habelə rabitə kanalları və ya informasiya daşıyıcıları vasitəsilə kompüter sistemlərinin və ya şəbəkələrinin digər qovşaqlarına və kompüterlərinə yayılmaq qabiliyyətinə malik olan kompüter virusları son dövrlərdə informasiya təhlükəsizliyinə real təhlükə kimi meydana çıxmışdır.

Kompüter şəbəkələrində bir kompüterə düşmüş virusun qarşısı vaxtında alınmadıqda, o, nəzarətsiz olaraq həmin kompüterdən digərlərinə yayıla, böyük şəbəkələrdə isə bu problem "həqiqi epidemiya" xarakteri ala bilər.

Kompüter virusları - kompüterdə çoxalmaq, həmçinin rabitə kanalları, kompüter şəbəkələri və informasiya daşıyıcıları (CD və maqnit disklər və s.) vasitəsilə digər kompüterlərə və şəbəkələrə yayılmaq (ötürülmək) qabiliyyətinə malik olan ziyanverici proqramlardır.

Kompüter viruslan, bir qayda olaraq, ziyankar (məkrli niyyəti olan) proqramçılar tərəfindən hazırlanır və xüsusi şəkildə hər hansı proqramın tərkibinə yerləşdirilərək kompüterin yaddaşına daxil edilir. Belə proqramın yüklənməsi virusun işə düşməsinə səbəb olur. Bundan sonra, viruslar növündən asılı olaraq, kompüterin yaddaşına, yaddaşda olan informasiya resurslarına, yüklənmiş proqramlara və s. yayılır, müəyyən olunmuş vaxtda təyinatı üzrə xəbərdaredici və ziyan vurucu işləri yerinə yetirirlər.

Bəzən kompüter virusu yarandığı ilk anda fəaliyyət göstərmir. Kompüterin yaddaşında və ya proqramlarda "yaşayan" belə viruslar yalnız müəyyən olunmuş vaxtlarda işə düşür. Viruslar emal olunan bütün informasiyaları izləyir

və informasiya bir yerdən başqa yerə ötürüldükdə virus da onunla birlikdə yerini dəyişir.

Ümumiyyətlə, bioloji virusların canlı orqanizmlərə yoluxduğu kimi, kompüter virusları da kompüterlərə və kompüter proqramlarına yoluxur və onları "xəstələndirir". Kompüterin əməliyyat sistemi, tətbiqi proqramlar, dray-verlər, əməli yaddaşlar və s. kompüter viruslarına yoluxa bilər.

Virusların yayılmasmın ən asan yolu yoluxmuş fayllarm disketlər, CD disklər, kompüter şəbəkələri vasitəsilə köçürülməsidir. Belə ki, virusa yoluxmuş kompüterdə istifadə olunan disket və ya bu disketə yazılan yeni proqram
həmin virusa yoluxa bilər. Başqa sözlə, virus daşıyıcısı olan disketin tamamilə "sağlam" kompüterdə istifadəsi və ya bu kompüterə viruslu proqramın yüklənməsi həmin kompüteri də yoluxdurur.

Kompüter virusları proqram təminatında və yaddaş qurğularında yerləşməsi, kompüter sistemlərində və şəbəkələrində yayılması, fəallaşması üsullarına və vurduğu ziyanın xarakterinə görə fərqlənirlər.

Kompüter virusları yazılmış informasiyanın və proqramların təhrif olunması, korlanması və ya məhv edilməsi, istifadəçilərin sorğularına sistemin

reaksiya verməsi və proqramların yerinə yetirilməsi üçün tələb olunan vaxtın artması, kompüterin düzgün fəaliyyətinin pozulması, disk qurğularının sıradan çıxması və s. kimi ağır nəticələr verə bilər.

Viruslar bəzən xoşxassəli əlamətlərə də malik ola bilərlər. Məsələn, proqramların yerinə yetirilmə sürəti azala, ekranda simvollar və ya işıq saçan nöqtələr əmələ gələ bilər.

Bəzi viruslara inkişaf edən əlamətlər xas olur, belə ki, "xəstəlik" getdikcə kəskinləşir. Məsələn, aydın olmayan səbəblərdən proqramların həcmi əhəmiyyətli dərəcədə artır və maqnit diskləri dolur. Nəticədə, bu, faylların silinməsinə və proqram təminatının məhvinə gətirib çıxara bilər.

İnformasiya təhlükəsizliyi baxımından kompüter viruslarının müsbət cəhətini də qeyd etmək lazımdır. Belə ki, proqram təminatlarında virusların mövcud ola bilməsi faktı proqram oğurluğunun qarşısının alınmasında yaxşı mühafizəçi rolunu oynayır.

FƏSİL II. KİBERNETİK FƏZADA CİNAYƏTKARLIQ VƏ TERRORÇULUQ

§2.1. Kibernetik terrorçuluq: fantastika yoxsa reallıq

Məlum olduğu kimi, bir çox hallarda elmi ixtiralar, kəşflər və cəmiyyətdə baş verən mühüm hadisələr barədə ilkin məlumatlar, xəyalpərəst yazıçıların romanlarında və rejissorların ssenarilərində qabaqcadan bu və ya digər şəkildə əksini tapmış olur.

Kiberterrorçuluğun meydana gəlməsi də, analoji olaraq, müvafiq fantastik əsərlərin yazılması ilə müşayiət olunmuş, başqa sözlə, kiberterrorçuluq hadisələri baş verməmişdən xeyli əvvəl müvafiq hadisələrin təsviri fantastik əsərlərdə və filmlərdə öz əksini tapmışdır. Məsələn, Jül Vernin "Barsakın ekspedisiyasının qəribə əhvalatları" romanında əks olunan hadisələrlə Osama Ben Laden və onun terrorçu təşkilatı "Əl-Qaidə" ətrafında baş vermiş hadisələr arasmda sarsıdıcı oxşarlıq vardır.

Son 15-20 il ərzində bir çox kinofilmlərdə kiberterrorçuların hərəkətləri və əməlləri nəticəsində yüzlərlə insanın ölməsi, binaların partlaması, təyyarələrin düşməsi, qatarların aşması və s. nümayiş etdirilirdi. O zaman heç kəsin ağlına gəlməzdi ki, bu hadisələr nə vaxtsa günün dəhşətli reallığına çevriləcəkdir.

Təcrübə göstərir ki, kinolarda göstərilən hadisələr müəyyən müddətdən sonra həyatda real şəkildə baş verir. Deyilənləri sübut etmək üçün bir sıra məşhur Hollivud filmlərinin məzmunları və onların qabaqcadan xəbər verdikləri hadisələrin real həyatda baş verməsini nümayiş etdirən bəzi konkret nümunələr göstərmək olar.

Sandra Bullokun iştirakı ilə çəkilmiş "Şəbəkə" filmində hadisələr aşağıdakı kimi cərəyan edir. Kiberterrorçular qoruma (təhlükəsizliyin təmin edilməsi) proqramlarının adı altmda viruslar yayaraq, polisin, xəstəxanalarm, aero-portun kompüterləri üzərində nəzarəti ələ keçirirlər. Onlar bu sistemlərdə saxlanılan və emal olunan məlu-matlarla manipulyasiya edərək təyyarələrin uçuş istiqa-mətlərini, xəstələrin xəstəlik tarixçələrini dəyişdirir və

bu yolla xoşlarına gəlməyən insanların ölümünə nail olurlar.

Bir qədər sonra real həyatda da analoji hadisələr baş verir. Avstraliyada su hövzələrinin təmizlənməsi stan-siyalarının qurğularında baş verən hadisələr onların çıx-masına səbəb oldu. Belə ki, bu cinayətkarlar rezer-vuarlarda çirkliliyin səviyyəsinə nəzarət edən qurğuları (ötürücüləri) əvvəlcədən stansiyanm kompüterlərində qu-raşdırılmış xüsusi proqramlarm - "troya atlan" virusları-nın köməyi ilə uzaq məsafədən söndürmüşdülər. Bu kiberterror aksiyasının nəticəsində rezervuarlarda çirklənmənin səviyyəsi artaraq tez bir zamanda normadan qat-qat artıq olmuş, minlərlə kubmetr təmizlənməmiş çirkli su yaxınhqdakı su hövzələrinə axmış, nəticədə, ekspertlərin fıkrincə ətraf flora və faunaya qarşısınm ahnması çətin olan ciddi ziyan vurulmuşdu.

Bryus Villusun iştirakı ilə çəkilmiş "Möhkəm qoz-2" filmində hadisələr aşağıdakı süjet üzrə ekranlaşdırıl-mışdır. Məşhur narkotik ticarətçisinin azadhğa buraxıl-masına nail olan terrorçular qrupu aviauçuşlarm idarə olunmasını həyata keçirən təminatının kompüter sistemi üzərində nəzarəti uzaq məsafədən ələ keçirirlər. Öz imkanlarını nümayiş etdirmək məqsədlə onlar bir sərnişin təyyarəsinin uçuş istiqamətini dəyişdirərək onu məhv edirlər.2001-ci ilin 4 iyulunda Los-Ancelosda və 11 sentyab-rında Nyu-Yorkda real həyatda baş vermiş hadisələr gös-tərdi ki, bu filmin məzmunu artıq fantastika deyil.

2001-ci ilin iyulun 4-də Los-Ancelos aeroportunda olan tablolarda və terminallarda qəflətən Microsoft Windows əməliyyat sisteminin səhvi haqqmda məlumat peyda ol-muşdu. Bunu hətta aeroportda öz reyslərini gözləyən sərnişinlər də görə bilmişdilər.

Sonradan araşdırma nəticəsində məlum olmuşdur ki, bu aeroportda istifadə olunan kompüterlərin əksəriyyətində Microsoft Windows əməliyyat sistemi quraşdınlmışdır və aeroportun informasiya sistemi Windows vasitəsilə

idarə olunur. Windows sisteminin etibarh olmadığını sübut et-məyə isə ehtiyac yoxdur.

Kiberterrorçular məhz bu amil-dən istifadə edərək kompüterləri sırada çıxara bilmişdilər. Çox güman ki, bu hadisə həmin ilin 11 sentyabrma planlaşdırılan hadisə üçün sadəcə kəşfiyyat xarakteri daşıyırdı. 11 sentyabr hadisələri isə hammm gözü qarşısmda baş vermiş, hadisələrin gedişi və inkişafı telekanallar vasitə-silə bütün dünyaya nümayiş etdirilmişdi. Beynəlxalq tica-rət mərkəzinin göydələnləri əvvəlcə yamr, sonra isə bir-birinin ardmca çökürdülər. Pentaqonun bir qanadı dağı-dıhr və yamr, Ağ Evə doğru uçan təyyarə Pensilvaniya çöllərində partlayaraq yerə düşür. Həmin gün hadisələr aşağıdakı ardıcıllıqla baş vermişdir:

- ABŞ-ın şərq sahillərinin vaxtı ilə səhər saat 8:45 -American Airlines şirkətinin 1 1N°-H reysi ilə uçan Boinq-767 təyyarəsi' Beynəlxalq ticarət mərkəzinin şimal qülləsinə çırpılır;

- saat 9:03 - United Airlines şirkətinin 175N°-li reysi ilə uçan Boinq-767 təyyarəsi Beynəlxalq ticarət mərkəzinin cənub qülləsinə çırpılır;

- saat 9:45 - American Airlines şirkətinin 77N2-1İ reysi ilə uçan Boinq-767 təyyarəsi Pentaqonun binasına çırpıhr; ′,

- saat 10:48 - United Airlines şirkətinin 93N°-li reysi ilə uçan Boinq-767 təyyarəsi Pitsburqdan 120 km məsafədə düşür;

- saat 11:18 - American Airlines şirkəti uçuşda olan onlara məxsus iki təyyarə ilə əlaqənin itməsi barədə məlumat verir;
- saat 11:59 - United Airlines şirkəti uçuşda olan bu şirkətə məxsus iki təyyarəsi ilə əlaqəni itirməsi barədə məlumat yayır.

Burada məntiqi sual yaramr. Necə olur ki, iki böyük şirkətə məxsus olan iki təyyarə uçuş istiqamətini dəyişir, bu təyyarələrlə radioəlaqə kəsilir, onlar bir-birinin ardınca radarlarm ekranlarından itir, binalara çırpılır, lakin avia şirkətlər

bundan çox gec xəbər tuturlar, uçuşlarm idarə edilməsi mərkəzində heç kəs həyəcan siqnah qaldırmır?

Bunu bəzən aviadispetçerlərin həddən artıq yüklənməsi, həmin zaman səmada bir neçə yüz təyyarənin olması ilə izah edirdilər. Lakin burada nəzərə almaq lazımdır ki, ABŞ-ın səmasını "hava-hava" sinfindən olan ən güclü Phoenix raketlərinə malik Lomcat hərbi təyyarələri qoruyur, Nyu-York və Vaşinqton şəhərlərini ən güclün hava hücumundan müdafiə sistemi əhatə edir. İlk qəzadan sonra uçuş istiqamətini dəyişən istənilən təyyarənin üstünü həmin anda almaq iqtidarında olan bu sistemlər nə üçünsə öz funksiyalarını tələb olunan səviyyədə yerinə yetirə bilmirdi.

Araşdırmalar nəticəsində sonradan məlum oldu ki, həmin zaman terrorçular tərəfmdən ikiqat hücum həyata keçirilmişdir. Belə ki, bir qrup terrorçu təyyarələri oğur-layaraq onları Beynəlxalq ticarət mərkəzinə, Pentaqona və Ağ Evə istiqamətləndirdiyi vaxt digər terrorçular (kiber-terrorçular) qrupu isə kompüter şəbəkələri vasitəsilə mülki uçuşları idarə edən xidmətlərə kiberhücumlar təşkil etmiş və, beləliklə də, bu vəhşi cinayətləri həyata keçirməyə imkan yaratmışdır.

Təhqiqat prosesində xüsusi xidmətlər tez bir zamanda aşkar etdilər ki, bu əməliyyatm həyata keçirilməsində, həmçinin, onun təmin edilməsində və ona yardım göstəril-məsində dünyanın tamamilə müxtəlif ölkələrində yerləşən onlarla insan iştirak etmişdir.

Məhz buna görə də, hələ faciənin baş verdiyi ilk günlərdə ABŞ-ın Federal Təhqiqat Bürosu (FTB) digər ölkələrin xüsusi xidmət orqanları ilə birgə həyata keçirdiyi fəaliyyət nəticəsində Floridada, Almaniyada və Böyük Britaniyada bir sıra terrorçuları (kiberterrorçuları) tutub saxlamışdı.

Stiven Siqalın iştirakı ilə ekranlaşdırılmış "Osadada-2" filminin ssenarisi aşağıdakı kimidir. Ərəb milyarderləri tərəfindən maliyyələşdirilən manyak-kompüterçi məxfı hərbi təyinath peyk üzərində idarəetməni ələ keçirmiş və ABŞ

hökumətini Vaşinqtonu məhv edəcəyi ilə şantaj edə-rək fantastik dərəcədə böyük məbləğ istəmişdir. İnsanlar arasında vahimə yaratmaq məqsədiiə filmdə terrorçular kimyəvi silah istehsal edən zavodu partladırlar.

Bir qədər sonra real həyatda baş vermiş hadisələr, demək olar ki, filmin ssenarisini təkrarlayırdı. Böyük Britaniyadakı vəziyyət barədə Reuter agentliyi vasitəsilə daxil olmuş səhih məlumatlar sadəcə inanılmaz idi. Naməlum xakerlər (kiberterrorçular) qrupu Böyük Britaniyanın peyk rabitələrindən biri üzərində nəzarəti ələ keçirmişdilər.

§2.2. Kompüter cinayətkarlığı və kibernetik terrorçuluq sahəsində əsas anlayışlar

Son zamanlar terrorçuluğun ən müasir növlərindən birinə çevrilmiş kibernetik terrorçuluğun beynəlxalq aləm-də yayılması böyük narahatçılığa səbəb olmuşdur. Kiber-netik terrorçuluğu bəzən «informasiya terrorçuluğu» və ya «kompüter terrorçuluğu» adlandırırlar.

Lakin mütəxəssislər hesab edirlər ki, «kompüter terrorçuluğu» adı kiber-netik terrorçuluğun mahiyyətini süni olaraq məhdudlaş-dırır, çünki bu halda söhbət cinayətin özündən deyil, onun törədilmə vasitəsindən gedə bilər.

«İnformasiya terror-çuluğu» adı da kibernetik terrorçuluğun xüsusiyyətlərini tam əhatə etmir. Belə ki, bu növ terrorçuluq yalnız kompüter şəbəkəsi ilə deyil, eyni zamanda poçt, teleqraf, radio, televiziya və s. vasitəsilə də həyata keçirilə bilər.

Bu baxımdan, «kibernetik terrorçuluq» anlayışının istifadəsi daha məqsədəuyğundur, çünki bu termin terrorçuların kibernetik məkanda fəaliyyət göstərmələrinin və onlar tərəfindən qlobal informasiya şəbəkələrinin imkan-larından istifadə olunmasının mahiyyətini özündə tam əks etdirir. Burada, sadəlik naminə, bəzən «kibernetik» sözü-nü «kiber» sözü ilə əvəz edərək «kibernetik terrorçuluq» termini əvəzinə «kiberterrorçuluq» terminindən istifadə edirlər.

Müharibələr bəşəriyyətin yaranışının başlanğıcından onu təqib edən hadisələrdir. Tarix boyu müharibələrin mahiyyəti dəyişməsə də, onlann aparılması formaları dəyişir. Hər bir əhəmiyyətli kəşf tez bir zamanda hərbi məqsədlər üçün öz tətbiqini tapır. İnternet də bu qəbildən müharibə məqsədləri üçün istifadə olunmağa başlamışdır.

80-ci illərin sonlarında Amerika Təhlükəsizlik və Kəşfiyyat İnstitutunun böyük elmi işçisi Berri Kollin virtual fəzada terrorçuluq fəaliyyətini ifadə etmək üçün ilk dəfə "kibernetik terrorçuluq" terminini istifadə etmişdir. O zaman bu termin praktiki əhəmiyyət kəsb etmirdi və yalnız gələcək üçün proqnoz verməkdən ötrü istifadə olunurdu.

Berri Kollinin özü isə kiberterrorçuluqdan yalnız XXI əsrin ilk onilliyində danışmağın real olduğunu qeyd etmişdir. Lakin real vəziyyətlə əlaqədar olaraq, FTB-nin xüsusi agenti Mark Pollit 1996-cı ildə kiberterrorçuluq termininin tərifini təklif etmişdir.

Yuxarıda qeyd olunduğu kimi, kiberterrorçuluq və kibermüharibə nə jurnalistlərin, nə də informasiya təhlü-kəsizliyi ilə məşğul olan şirkətlərin uydurması deyil, bu gün dünyada mövcud olan real vəziyyətdir. Kiberterror-çuluq hadisələri artıq real olaraq baş vermişdir və verməkdədir, kibermüharibənin isə yaxın illərdə həyata keçirilməsi üçün əlverişli zəmin yaranmışdır.

Ümumiyyətlə, kiberterrorçuluq dedikdə, kompüterdə emal olunan informasiyaya, kompüter sisteminə və şəbə-kəsinə düşünülmüş, siyasi motivlərə əsaslanmış hücum başa düşülür. Əgər belə hərəkətlər ictimai təhlükəsizliyin pozulması, əhalinin qorxudulması, hərbi konfliktlərin, təxribatlarının törədilməsi məqsədilə həyata keçirilmiş olarsa, onda bu hücum insanların həyatı və sağlamhğı və ya digər ağır fəsadların baş verməsi üçün daha böyük təhlükə yaradır.

Kiberterrorçuluq cinayətkar niyyətlərin əldə olunması məqsədilə əhalinin, hakimiyyət orqanlarının qorxudulması kimi qəbul edilir. Bu, müəyyən siyasi və ya digər məq-sədlərin əldə olunması, şəxslərin, təşkilatların və ya haki-miyyət strukturlarının müəyyən hərəkətlərə məcbur edil-məsi, kiberterrorçunun şəxsiyyətinə və terrorçu təşkilata diqqətin yönəldilməsi məqsədilə əhalinin təhlükəyə məruz qoyulması, daimi qorxu vəziyyətində saxlanması şəklində özünü göstərə bilər.

Qeyd olunanlar nəzərə alınmaqla müasir dövrdə kiberterrorçuluğa verilmiş aşağıdakı tərifləri xüsusi qeyd etmək olar.

Kiberterrorçuluq - ölkənin həyati vacib (mühüm) informasiya infrastrukturlarına maksimal dərəcədə ziyanın vurulması ilə müşayiət olunan planlaşdırılmış kompüter hücumlarıdır.

Kiberterrorçuluq - hər hansı məsələ ilə bağlı dövlət, təşkilat və ya fiziki şəxs tərəfindən qərarın qəbul olunmasına təsir etmək məqsədi ilə asayişin pozulması, cəmiy-yətin qorxudulması və əsarət altında saxlamlması üçün kompüter sistemlərinin dağıdılması və kibernetik məkanın sabitliyinin pozulmasıdır.

Kiberterrorçuluq - siyasi, tamahkarhq və ya digər bəd niyyətləri həyata keçirmək məqsədilə hərb, tibb, bank, maliyyə və s. sahələrdə kompüter şəbəkələrinə və sistem-lərinə, informasiya ötürülməsi vasitələrinə və onların idarə edilməsi mərkəzlərinə edilən hücumlar, eləcə də ictimai tarazlığı pozmaq, əhalini qorxutmaq, hakimiyyət orqanları tərəfindən qərarlarm qəbuluna təsir etmək üçün kompüter texnologiyalarmın istifadəsi və ya istifadəsinin ehtimal olunması təhlükələrinin reallaşdırılmasıdır.

Kiberterrorçuluq - ictimai təhlükəsizliyi pozmaq, əha-lini qorxutmaq və ya hərbi münaqişəyə təhrik etmək məq-sədilə insanların həyat və sağlamhğına xətər yetirilməsinə, eləcə də daha ağır nəticələrin meydana gəlməsinə səbəb ola biləcək təhlükələr yaratmaq üçün kompüterdə emal olunan informasiya resurslarına, kompüter sistemlərinə və şəbəkələrinə düşünülmüş hücumlar və törədilmiş digər cinayətlərdir.

Kiberterrorçuluqla bağlı daha bir neçə termini qeyd etmək lazımdır.

Kiberterrorçu - kiberterrorçuluğu həyata keçirən və ya bu işdə iştirak edən şəxs, yəni xüsusi təyinath xakerdir.

Öz məqsədlərinə çatmaq üçün partlayıcı maddələr və atıcı silahlardan istifadə edən adi terrorçudan fərqli olaraq, kiberterrorçu kompüter sistemlərinə icazəsiz soxulmaq və informasiya resurslarına uzaq məsafədən hücumlar təşkil etmək üçün müasir informasiya texnologiyalannı, kompüter sistemlərini və şəbəkələrini, xüsusi proqram təminatını istifadə edir.

İlk növbədə onlara "məntiqi bombalar", "troya atları", sniffer proqramlan və digər növ informasiya silahları ad-lanan, informasiyanm çıxarılmasını, dəyişdirilməsini və ya məhv edilməsini həyata keçirən kompüter, o cümlədən

şəbəkə proqram qoyuluşlarını aid etmək olar.

Ümumiyyətlə, terrorçuların İnternetdə fəaliyyətini üç kateqoriyaya bölmək olar: "aktivlik", "xakerlik" və "kiber-terrorçuluq".

"Aktivlik" - öz ideyalarınm təbliğ olunması, qazanc əldə edilməsi və qrupa yeni üzvlərin cəlb olunması məqsə-dilə kiberfəzanın terrorçular tərəfindən qanuni istifadəsini nəzərdə tutur.

"Xakerlik" - ayrı-ayrı kompüterlərin, kompüter sistem-lərinin və şəbəkələrinin, eləcə də İnternet saytlarımn sıradan çıxarılması, məxfı məlumatların əldə edil-məsi, vəsaitlərin oğurlan-ması və digər məqsədlərlə həyata keçirilən xaker hücumlarıdır.

Xaker termini digər şəxslərin kompüterlərinə, sistemlərinə və məlumat-larına qeyri-qanuni giriş əldə edən və ya buna cəhd göstərən şəxsləri göstərmək üçün istifadə olunur.

Xaker - kompüter sahəsində öz bilik, bacarıq və imkanlarını qorunan informa-siya resurslarina icazəsiz giriş əldə etmək üçün istifadə edən yüksəkixtisaslı mütəxəssisdir.

Xaker - informasiya texnologiyaları sahəsində müxtəlif növ qeyri-qanuni hərəkətlər törədən (başqasmın kompü-terlərinə, kompüter sistemlərinə və şəbəkələrinə icazəsiz soxulan və ondan informasiyam əldə edən, proqram məh-sullanndan qoruma mexanizmlərini qeyri-qanuni çıxaran və onları köçürən, kompüter viruslarım yaradan və yayan) şəxslərdir.

Qeyd etmək lazımdır ki, ilkin olaraq xaker sözü kompüter elmlərində görkəmli və radikal proqramçıları (adətən, Berkli, Stendford və ya Massaçusets universitetlərində) assosiasiya edirdi.

Yüksək texnologiyalar üzrə lüğətdə xakerlər, əsasən, kompüterlər üzrə müəyyən bilikləri olan və kompüter proqramlarını yaratmağı bacaran, adətən, bu qabiliyyətini assembler və ya aşağı səviyyəli dillərdə tətbiq edən şəxslər kimi xarakterizə olunur.

Xaker, həmçinin, maneələri adlamaq və sistemdə mü-əyyən edilmiş hədləri aşmaq üçün xüsusi yollar axtarıb tapan yüksək ixtisash proqramçı kimi də qəbul edilirdi.

Bu termin dörd ardıcıl nəslin dövründə aşağıdakı kimi dörd müxtəlif mənalarda işlədilmişdir:

- *birinci nəsil* (1960-cı illər) bu termini qabiliyyətli, məharətli proqramçüarı göstərmək üçün istifadə et-mişdir;

- *ikinci nəsil* (1970-ci illər) bu termini kompüter (elektron hesablayıcı maşmlan) təkamülçülərini, yəni kompüter texnologiyalarını inkişaf etdirənlər mütəxəssisləri göstərmək üçün istifadə etmişdir;

- *üçüncü nəsil* (1980-ci illər) bu termini kommersiya əhəmiyyətli oyun proqramlarını və müəlliflik hü-quqlarını sındıran şəxsləri (proqramçılan) göstərmək üçün istifadə etmişdir;

- *dördüncü nəsil* (1990-cı illərdən bu günədək) bu termini kompüter sahəsində (o cümlədən kiberfəza-da) fəaliyyət göstərən cinayətkarları, yəni kiberci-nayətkarları göstərmək üçün istifadə etmişdir və edir.

Xakerləri bir neçə kateqoriyaya bölmək olar:

- *piratlar* - müəyyən qədər texniki təcrübəsi olan, fəa-liyyəti sistemə soxula bilmək qabiliyyətini sübut və nümayiş etdirməklə məhdudlaşan qeyri-peşəkarlar qrupu.

- *"brauzerlər"* (browser - baxan sözündən) - orta sə-viyyəli texniki qabiliyyəti olan, başqa şəxslərin kom-püterlərinə, sistemlərinə və informasiya resurslarına qeyri-qanuni giriş əldə etməyi bacaran mütəxəssislər qrupu. Onlar müəlliflik hüquqlannı adlayıb keçə bilir, lakin, bir qayda olaraq, resurslara ziyan vur-murlar.

- *"krekerlər"* - ən yüksək texniki imkanlara malik olan oğrular və kibercinayətkarlar. Onlar daha təhlükəli qrup olaraq çox böyük zərər vurur,

fayllarm köçürül-məsindən tutmuş proqramların və sistemlərin korlan-masına qədər müxtəlif hərəkətləri həyata keçirə və əməlləri törədə bilərlər.
Xakerlər təhlükəsizlik sistemlərini onlann yolunda ma-neə və əngəl kimi deyil, bir çağınş kimi qəbul edirlər.

IBM şirkətinin qlobal təhlükəsizliyin təhlili ilə məşğul olan laboratoriyasmın məlumatlarına əsasən dünyada xa-kerlərin ümumi sayı təxminən yüz minlərlə ölçülür. Bu xakerlərin 90%-i birinci qrupa (piratlara), 9%-i ikinci qrupa (brauzerlərə), 1%-ə qədəri isə daha təhlükəli olub üçüncü qrupa (krekerlərə) aid edilir.

Kibercinayət - ictimai təhlükəsizliyin pozulması, əha-linin qorxudulması və ya hakimiyyət orqanları tərəfmdən cinayətkarlara sərfəli olan qərarların qəbuluna təsir edil-məsi, özlərinin maddi və digər maraqlarının qanunsuz yolla təmin olunması məqsədi ilə telekommunikasiya sistemlərinin, kompüter şəbəkələrinin və onlann kom-ponentlərinin sıradan çıxarılması, şəbəkə mühitində fəa-liyyət göstərən kompüter proqramlarımn işinə, kompüter məlumatlarına icazəsiz (qanunsuz) müdaxilə etməklə və digər yollarla dövlətin xüsusilə vacib infrastruktur seq-mentlərinin işinin pozulmasına, insanların tələf olmasına, əhəmiyyətli maddi ziyanının vurulmasına səbəb olan və ya digər ciddi ictimai təhlükələr yaradan əməllərdir.

BMT ekspertlərinin mülahizələrinə əsasən, kibercinayət termini kompüter sistemlərinin və şəbəkələrinin köməyi ilə, eləcə də kompüter sistemləri və şəbəkələri çərçivə-sində və ya onlara qarşı törədilə biləcək istənilən cinayəti özündə ehtiva edir. Prinsip etibarı ilə kibercinayət elektron mühitdə baş verən, törədilən istənilən cinayəti əhatə edir.

İnformasiya cinayəti - informasiya sahəsində şəxsiy-yətin, təşkilatların, cəmiyyətin və ya dövlətin qanunla müəyyən edilmiş hüquqlarmı pozan və onlara mənəvi və ya maddi ziyan vuran hüquqazidd hərəkətlərdir.

Kompüter sabotajı - kompüter informasiyasının və ya proqramının qəsdən (düşünülmüş şəkildə) məhv edilməsi, blokirovkası, yararsız hala

sahnması, kompüter avadanlıq-larının sıradan çıxarılması, kompüter sisteminin, şəbəkə-sinin və ya informasiya daşıyıcısının dağıdılmasıdır.

Statistik məlumatlar göstərir ki, 2001-ci ildə kompüter sistemlərinə 5700000 müdaxilə hadisələri qeydə alınmış və onlardan 12%-i ziyanın vurulması ilə nəticələnmişdir. Bu müdaxilələr nəticəsində dəyən ziyanm miqdarı oğur-lanmış proqram təminatma görə 5,5 milyard dollar və telefon kredit kartlarmın oğurlanmasına görə bir milyard dollar təşkil etmişdir.

Adətən, baş vermiş təhlükəsizliyin pozulması hadisələrinin 80%-i siste-min daxili xakerləri tərə-fından törədilmiş, onlann yalmz 20%-i xarici xaker-lərin payına düşür.

Kibertəhlükə və ya *kibermüdaxilə* - kompüterlərə, onlar tərəfindən idarə olunan sistemlərə və ya şəbəkələrə icazəsiz müdaxilə (soxulma) cəhdləridir. Belə icazəsiz hərəkətlərin əsasmda risk, kəskin hislər və ya maraq xatirinə sistemə sadəcə müdaxilə, qisas almaq, infor-masiyanı oğurlamaq, qarışıqhq salmaq, pul tələb etmək və ya oğurlamaq, eləcə də kompüterlərin, kompüter sistem-lərinin və şəbəkələrinin qəsdən sıradan çıxarılması və ya həddən artıq böyük infrastrukturlara (məsələn, su və ya enerji təchizatı sistemlərinə) ziyanın vurulması üçün sistemə daxil olmaq kimi müxtəlif məqsədlər dura bilər.

Kibermüharibə adi müharibələrdən istifadə edilən silah-ların növünə, təsir dairəsinə və nəticələrinə görə fərqlənir. Belə ki, kibermüharibələr adi müharibələr kimi eyni prinsip və üsullarla aparılsa belə onların miqyası qat-qat geniş ola bilər.

İnformasiya müharibəsi - informasiya üstünlüyü əldə etmək məqsədilə rəqibin informasiya resurslarma, infor-masiyaya əsaslanmış proseslərinə və informasiya sistem-lərinə ziyan vurmaq və eyni zamanda, özünə məxsus olan informasiya resurslarını, informasiyaya əsaslanmış proses-ləri və informasiya sistemlərini qorumaq yolu ilə həyata keçirilən əməliyyatlardır.

İnformasiya müharibəsi - maddi, hərbi, siyasi və ya ideoloji sahələrdə müəyyən üstünlük əldə etmək üçün sistemlərin bir-birinə açıq və ya gizli şəkildə

məqsədyönlü informasiya təsirləridir. Bu baxımdan dövlət səviyyəsində həyata keçirilən hərbi tədqiqatlar barədə məlumatlar çox məxfi saxlanıhr. Lakin bir fakt dəqiq məlumdur ki, dünyada superdövlət iddiasında olan dövlətlər (Çin, ABŞ, Rusiya) fəal surətdə *kibersilahlanma* ilə məşğuldurlar.

İnformasiya silahı - bütövlükdə informasiya infra-strukturunun və onun ayrı-ayrı elementlərinin funksiya-larının və ya xidmətlərinin müvəqqəti və ya tamamilə sıradan çıxarılması üçün tətbiq olunan xüsusi (fiziki, informasiya, proqram, radioelektron və s.) üsul və vasitələr toplusudur. Başqa sözlə, informasiya silahı informasiya müharibəsi zamanı düşmənə informasiya təsirini həyata keçirməyə imkan verən üsul və vasitələr kimi başa düşülür. O, dövlətin və ya onun silahh qüvvə-lərinin informasiya sahəsinin obyektlərini, eləcə də onların qorunmasını sarsıdan, dağıdan, blokirovka və məhv edən vasitələrin (qurğuların) və texnologiyaların tətbiqinə əsas-lanan dağıdıcı təsirlərə malik xüsusi silahlardır.

Kibermüharibənin olub-olmayacağı, onun nədən ibarət olacağı, bəşəriyyətin ondan necə ziyan çəkəcəyi barədə dəqiq fıkir söyləmək çətindir. Əlbəttə, arzu olunur ki, kibermüharibə elə fantastika olaraq qalsın. Lakin infor-masiya texnologiyalarının inkişaf tendensiyası göstərir ki, bu yalnız fantastik filmlərdə və əsərlərdə əksini tapmış təhlükə deyil, o, həmçinin, artıq real həyatda da mövcud olan təhlükədir.

Kompüter texnologiyaları günbəgün daha geniş şəkildə bizim həyatımıza daxil olur, daha çox kompüterlər və kompüter şəbəkələri İnternetə qoşulur. Bununla da cəmiy-yət kompüterlərdən və kompüter sistemlərindən daha çox asıh olur. Ona görə də ayrı-ayrı siyasət və dövlət xadim-lərində kibermüharibənin aparılması vasitələrinə müraciət etmək arzusu yarana bilər.

Bəzən cəmiyyətdə elə fıkirlərə rast gəlinir ki, guya informasiya texnologiyalarının yüksək inkişaf etmədiyi, istehsal sahələrində və ya

idarəetmədə kompüter texni-kasının və kompüter şəbəkələrinin geniş tətbiq olunmadığı ölkələrdə, o cümlədən Azərbaycan Respublikasında kiber-müharibə təhlükəsi mövcud deyil. Əlbəttə, Azərbaycanda digər inkişaf etmiş ölkələrdə olduğu kimi, həyat fəa-liyyətinin bütün sahələrində kompüter texnologiyalarının tətbiqi arzu olunan səviyyədə deyil.

Lakin, nəzərə alınmalıdır ki, bir çox mühüm strateji vacib sahələrdə artıq kompüter şəbəkələri yaradılmış, bu şəbəkələr vasitəsilə informasiyanın toplanması və mübadiləsi artıq həyata keçirilməyə başlamışdır. Məsələn, bank, maliyyə, vergi, gömrük, respublikaya giriş-çıxışa nəzarət, nəqliyyat (metro, hava, qatar, avtomobil, su və s.), energetika, rabitə, radio, teeleviziya, seçki sahələrində artıq belə sistemlər mövcuddur.

Əgər bu siyahıya ırespublikada elektron sənəd dövriyyəsinə keçid və yeni Elektron-Azərbaycan platformasınm yaradılması istiqamətlttində aparılan işləri, Azərbaycanda yüksək texnologiyah arm tətbiqi ilə həyata keçirilən beynəlxalq layihələr (məsələn, Bakı-Tbilisi-Ceyhan neft kəməri) və s. əlavə esdilərsə, onda mövcud (və ya yetiş-məkdə olan) təhlükəniin miqyasını təsəvvür etmək olar.

Kibermüharibələrim aparılması mexanizmləri və ya üsulları barədə konkret məlumat vermək çox çətindir, lakin məlumatların sarxlanılması və ötürülməsinin mövcud üsullarının təhlilinə əsäslanan mütəxəssislərin yekdil rəyinə əsasən birmənaıh şəkildə aşağıdakı xaker üsullannın tətbiqi mümkün hesab edilir:

- *DoS (Denial of Service) hücumlar* - kompüter və informasiya sisttemləri tərəfindən xidmətin göstə-rilməsindən imtrina edilməsi effektini yaradan hücumlar.

- *Məntiqi bombalcar* - uzaq məsafədən idarə olunan, vaxta görə işə cdüşən və ya komanda idarə olunan proqram vasitələ«ri (kibermüharibənin ən güclü silah-lanndan biridir).

- *Radio və elektrotiexniki maneələrin* istifadəsi.

- *Virus* hücumları.

§2.3. Kompüter hücumları – kiberhücumlar

Yuxarıda qeyd edilənlərdən aydın olur ki, *kiberhücumlar* rəqib (düşmən) dövlətlərin, habelə terrorçu qruplarm əlində çox güclü silahdır.

Pentaqonun yüksək vəzifəli şəxslərinin fıkrinə görə, gələcəkdə düşmənlər informasiya-kommunikasiya texno-logiyaları vasitəsilə ABŞ-ın hərbi qüvvələrini iflic edə bilərlər. Bu onunla izah olunur ki, ABŞ-ın hərbi qüvvələrinin saxlanılması və fəaliyyəti əhəmiyyətli dərəcədə "mülki" texnoloji vasitələrin (kommunikasiya sistemlə-rinin, elektron qurğuların, proqram təminatının və s.) köməyi ilə həyata keçirilir. Gələcək konfliktlər mülki və hərbi məqsədlər arasında sərhədlərin silinməsi ilə xarak-terizə oluna bilər.

Beləliklə, çox böyük ehtimalla ABŞ-ın mühüm infra-strukturlarınm fəaliyyətini təmin edən kompüterlərin də daxil olduğu mülki sistemlər düşmənlər, o cümlədən ki-berterrorçular tərəfmdən zəif qorunan hədəflər kimi baxıla və onların hücumlarına məruz qala bilər.

Eyni zamanda, bəzi mütəxəssislər hesab edirlər ki, kompüter hücumları, o cümlədən kiberhücumlar vacib infrastrukturlar üçün o qədər də böyük təhlükə yarada bilməz, lakin digər qrup mütəxəssislər iddia edirlər ki, kiberhücumlar ölkənin milli təhlükəsizliyi üçün real təhlükədir.

İnternet şəbəkəsi, onun web, chat və e-mail kimi xidmətləri terrorçular tərəfindən əlaqələrin qurulması, eləcə də gələcək niyyətlərinin həyata keçirilməsi məqsədilə getdikcə daha çox istifadə olunur. Bu yolla mühüm infrastrukturlarda tətbiq olunan informasiya texnologiya-larmda mümkün zəif yerlərin olması barədə biliklər terrorçu qruplar tərəfindən daim toplanır və gələcəkdə digər məqsədlər üçün istifadə olunur.

Kompüter hücumları kompüter sistemlərinə və şəbəkələrinə qarşı yönələn, avadanlıqların fəaliyyətinin pozul-ması, əməliyyatlar üzərində nəzarətin dəyişdirilməsi və saxlanılan məlumatların korlanması məqsədlərini daşıyan hərəkətlər şəklində həyata keçirilə bilər. Kompüter hücumlarının müxtəlif üsulları kompüter sistemlərində və şəbəkələrində mövcud olan zəifliklərin istifadəsinə yönəl-miş olur və bu məqsədlə tətbiq olunan müxtəlif silahları (onların bir çoxu istənilən anda terrorçu qrupların əlinə keçə bilər) özündə birləşdirir.

Məsələn, qorxu dəhşətini nümayiş etdirmək məqsədilə terrorçuların da çətinlik çəkmədən istifadə edə biləcəyi lokal təxribat mexanizmini misal göstərmək olar. Tutaq ki, hər hansı "təşkilat" bir mütəxəssisi işə götürür və aşağı-dakı işləri həyata keçirməyi ona tapşırır:

- rəqib şirkətin əsas 10-15 telefon xətlərinin nömrə-lərini aydınlaşdırmaq;
- 10-15 ədəd yeni mobil telefon almaq;
- bu mobil telefonları avtomatik zəng etmə rejiminə quraşdırmaq;
- bir neçə gün müddətində fasiləsiz zənglərlə rəqib şirkətin telefon xətlərinin giriş trafikini tam məşğul etmək.

NƏTİCƏ

Hazırladığım bu kurs işimi fəsillərə ayırmışam.

FƏSİL I – də Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyinin əsasları, informasiya təhlükəsizliyi problemi və onu xarakterizə edən amillər, kompüter sistemlərində və şəbəkələrində informasiyanın sızması yolları, informasiya təhlükəsizliyinə olan təhdidlərin təsnifatı, kompüter virusları informasiya təhlükəsizliyinə təhdid kimi mövzular haqda məlumat vermişəm.

FƏSİL II – də Kibernetik fəzada cinayətkarlıq və terrorçuluq, kibernetik terrorçuluq: fantastika yoxsa reallıq, kompüter cinayətkarlığı və kibernetik terrorçuluq sahəsində əsas anlayışlar, kompüter hücumları – kiberhücumlar bu kimi mövzular haqda ətraflı məlumat vermişəm.

ƏDƏBİYYAT

1. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm imza texnologiyası. Bakı. Elm. 2003. – 132 s.
2. Голубев В. Кибертерроризм – понятие, терминология, противодействие. http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism/.
3. Голубев В. Кибертерроризм – угроза национальной безопасности. http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism/.
4. Медведовский И.Д., Семянов П.В., Леонов Д.Г. Атака на Интернет. – М.: ДМК, 2000. – 336с.
5. Михеев И.Р. Терроризм: понятие, ответственность, предупреждение. http://www.crime.vl.ru/docs/stats/stat_62.htm.