**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №4**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Fənn:** “ Veb sistemləri və texnologiyaları ”

**Mövzu:** Kiber cinayətkarlıq

**Qrup:** 2441a

**Tələbə:** Abbasov Həsən

**Müəllim:** Heydərzadə Nübar

**BAKI 2024**

**Kompüter hücumları – kiberhücumlar**

**Kiberhücumlar** – rəqib (düşmən) dövlətlərin, habelə terrorçu qrupların əlində çox güclü silahdır.

Kompüter hücumları kompüter sistemlərinə və şəbəkələrinə qarşı yönələn, avadanlıqların fəaliyyətinin pozulması, əməliyyatlar üzərində nəzarətin dəyişdirlməsi və saxlanılan məlumatların korlanması məqsədlərini daşıyan hərəkətlər şəklində həyata keçirilə bilər. Kompüter hücumlarının müxtəlif üsulları kompüter sistemlərində və şəbəkələrində mövcud olan zəifliklərin istifadəsinə yönəlmiş olur və bu məqsədlə tətbiq olunan müxtəlif silahları özündə birləşdirir.

Hücum vasitələrinin tətbiqinin doğurduğu effektlərdən asılı olaraq kiberhücumlar bir neçə növə bölünür və fərqlənirlər. Lakin yüksək texnologiyalar inkişaf etdikcə bu növlər arasındakı fərqlərin azalması və tamamilə silinməsi ehtimal olunur.

**Fiziki hücum** – kompüterlərə, kompüter sistemlərinə və şəbəkələrinə qarşı ənənəvi silahların tətbiq edilməsini nəzərdə tutur. Fiziki hücumlar kompüter sistemlərini və şəbəkələrini sıradan çıxarır, onların etibarlılığını və məlumatlara giriş imkanlarını pozur. Belə hücumlar ənənəvi silahları tətbiq etmək, qızdırmaq, partlatmaq, fiziki məhv etmək, eləcə də elektrik xətlərinə və avadanlıqlara qeyri-qanuni fiziki girişi əldə etdikdən sonra onlar üzərində manipulyasiya etməklə həyata keçirilə bilər.

**Elektromaqnit hücumu** – silah qismində elektromaqnit enerjisinin gücündən istifadəni, kompüter sistemlərində gərginliyi həddən çox artırmaq üçün elektromaqnit impulslarının tətbiq edilməsini özündə ehtiva edir. Bu hücum daha çox düşmənin radioötürücülərinə rəqəm kodun birbaşa yerləşdirilməsi yolu ilə həyata keçirilir.

Kompüter sistemlərinə və ya şəbəkələrinə hücumlar (kiberhücumlar) – adətən ziyanverici proqramların tətbiqini özündə ehtiva edir. Belə proqramlardan sistemin proqram təminatında və konfiqurasiyasında, təşkilatın və ya istifadəçinin kompüter təhlükəsizliyinin təmin edilməsi sistemində mövcud olan zəif yerlərin istifadə edilməsi yolu ilə düşmənin kompüterlərinin və ya kompüter sistemlərinin yoluxdurlması üçün silah kimi istifadə oluna bilər.

Kompüter hücumları və ya kiberhücumlar nəticəsində məlumatların məxfiliyi, tamlığı, həqiqiliyi pozula bilər. Bu, adətən proqram təminatında məntiqi dəyişikliklər aparan, məlumatlara nəzarət edən və ya səhvlərə gətirib çıxaran ziyanverici proqramların istifadəsi yolu ilə həyata keçirilir.

Qeyd etmək lazımdır ki, elektromaqnit hücumlarının və ya kiberhücumların fiziki hücumlara nisbətən daha az ehtimal edilməsinə baxmayaraq həqiqətdə onlar daha təhlükəlidirlər. belə ki, yüksək texnologiyaların istifadəsi ilə dağıdıcılıq məqsədilə həyata keçirilən eletromaqnit hücumları və kiberhücumlar qabaqcadan gözlənilməyən nəticələrə gətirib çıxara və ya düşmən tərəfə nəzərə alınmamış üstünlüklər verə bilər.

**Kiberterrorçuluq cinayətlərinin xüsusiyyətləri**

Kiberterrorçuluq yalnız insanların və onlara məxsus olanəmlakın məhvinə, mühüm stateji və iqtisadi obyektlərin dağıdılmasına deyil, həmçinin maliyyə və kommunikasiya şəbəkələrinin və sistemlərinin işinin geniş miqyasda pozulmasına, iqtisadi infrastrukturunun dağıdılmasına və hakimiyyət strukturlarına öz iradələrinin qəbul etdirilməsinə yönəlmiş ola bilər.

Ümumiyyətlə, kiberterroçuluğa qarşı mübarizə spesifik xüsusiyyətlərə malik olan müvafiq hüquqi və texniki problemlər kimpleksinin meydana gəlməsi ilə müşayiət olunur. Bu əsasən aşağıdakılarla bağlı olur:

- Kiberterroçuluğa qarşı mübarizə sahəsində cinayət fəaliyyəti nizamlayan qanunvericilik aktlarının olmaması;

- İnformasiya– kommunikasiya sahəsində baş verən cinayətlərin qarşısının alınması, aşkar olunması və açılması üzrə ixtisaslaşan mütəxəssislərin, əməliyyat və istintaq aparatının olmaması;

- Kiberhücumlara müqavimət göstərə biləcək zəruri texniki bazanın olmaması;

- Xarici ölkələrin hüquq – mühafizə orqanları ilə etibarlı qarşılıqlı fəaliyyət mexanizmlərinin qurulmaması.

Kibercinayətləri qəsd obyektlərinə görə aşağıdakı qruplara bölürlər:

- Iqtisadi kompüter cinayətləri;

- Şəxsi hüquqlar və xüsusi sahənin toxunulmazlığı əleyhinə yönəlmiş kompüter cinayətləri;

- Ictimai və dövlət maraqları əleyhinə yönəlmiş kompüter cinayətləri.

Kompüterlərin və kompüter sistemlərinin istifadəsi xarakterinə görə kibercinayətləri aşağıdakı 3 növə ayırırlar:

- Kompüterlərin cinayətin aləti qismində istifadə edildiyi əməllər (informasiyanın oğurlanması, icazəsiz giriş, faylların və qurğuların məhv edilməsi və korlanması və s.);

- Kompüterlərin cinayətin silahı kimi istifadə edildiyi hərəkətlər (elektron oğurluq və s.);

- Kompüterlərin intellektual vasitələr rolunda iştirak etdiyi cinayətlər

Kibercinayətlərin aşağıdakı əsas növlərini qeyd etmək olar:

- Kompüter şəbəkələrinə daxil olmaq üçün parolların və kodların ələ keçirilməsi və onlardan istifadə edilməsi;

- Kredit kartlarının parollarının və ya kodlarının ələ keçirilməsi və istifadə edilməsi;

- Informasiyanın icazəsiz olaraq baxılması, surətinin çıxarılması, köçürülməsi və ya yayılması;

- Telekommunikasiya sistemlərinin və kompüter şəbəkələrinin, proqramların və texniki vəsaitlərin, məlumat bazalarının sıradan çıxarılmasına və ya onların işində dəyişikliklərin edilməsinə yönəlmiş xaker hücumları;

- Cinayətkar yolla qazanılmış maliyyə vəsaitlərinin köçürülməsi;

- Vergi ödəmədən maliyyə əməliyatlarının həyata keçirilməsi;

- Elektron poçtu vasitəsilə cinayətkar əlaqələrin yaradılması;

- Nüfuzdansalıcı məlumatların yayılması;

- Narkotiklərin istehlakının və satışının təşkili;

- Fərdi təyinatlı radioaktiv maddələrin oxşarlarının istehsalı və tətbiqi.

Kibercinayətlər aşağıdakı fərdi xüsusiyyətlərə malik olurlar:

- Kibercinayətlərin gizli şəkildə həyata keçirilməsi mümkündür;

- Kibercinayətlər üçün sərhəd yoxdur;

- Kompüter informasiyasını, habelə cinayətin izlərini sadə şəkildə məhv etmək və dəyişdirmək mümkündür;

- Kibercinayətlərin törədilməsi izləri texniki qurğuların yaddaşında, elektromaqnit sahəsində və kompüterlərin İnformasiyadaşıyıcılarında qala, maddi və əşya izləri arasında yer tuta bilər;

- “Virtual” izləri tamamilə silmək qeyri – mümkündür, bu izlərin surətini asanlıqla köçürmək olur;

- Kommunikasiya şəbəkələri operatorlarının serverlərində kibercinayətlərin izləri müəyyən zaman kəsiyində saxlanılır;

- Kompüter şəbəkələrində cinayətkar hərəkətlərə aidiyyəti olan kompüter informasiyasının və şəxslərin tanınması, aşkarlanması ənənəvi üsulların vasitəsilə həmişə mümkün olmur və bu məqsədlə xüsusi tədbirlərin həyata keçirilməsini tələb edir.

Mütəxəssislər kiberterrorçuluğun həyata keçirilməsi üçün adətən 3 mərhələli modeldən istifadə olunduğunu qeyd edirlər:

- Birinci mərhələ - siyasi, iqtisadi və digər tələblər irəli sürülür, onların yerinə yetirilməyəcəyi təqdirdə ölkənin iqtisadi sisteminin iflic vəziyyətə salınacağı təhlükəsinin yaradılacağı bildirilir;

- Ikinci mərhələ - təhlükəni nümayiş etdirmək məqsədilə kifayət qədər böyük iqtisadi infrastruktura malik bir təşkilatın İnformasiyaresurslarına hücum həyata keçirilir və onun fəaliyyəti iflic vəziyyətinə gətirilir;

- Üçüncü mərhələ - gücün nümayiş etdirilməsinin effektinə əsaslanaraq, tələblər daha kəskin şəkildə təkrar etdirilir.

**Kiberterrorçuluğa qarşı mübarizə mexanizmləri**

İnformasiyanın toplanması, ötürülməsi və emalının müasir texniki vasitələrinin xarici cinayətkar təsirlərdən qorunmasının artırılması olduqca mürəkkəb məsələdir. Bu məqsədlə təhlükəsizliyin təmin edilməsinə kompleks yanaşmanın reallaşdırılması zəruridir.

Etibarlılıq və dözümlülük baxımından optimal informasiya sistemlərinin qurulması isə onların əsas effektivlik kriterisinə, yəni istifadəçinin rahatlığı, müştərilərin və tərəfdaşların informasiyaya operativ girişinin təmin edilməsi, emalın və ötürmənin asanlığı, məlumat bazasının məzmununa müraciətin sadəliyi prinsiplərinə ziddiyyət təşkil edir.

Bu baxımdan, kiberterrorçuluqla effektiv mübarizənin əsasını belə fəaliyyətin aşkar olunması, xəbərdar edilməsi və qarşısının alınması üzrə effektiv qarşılıqlı əlaqəli tədbirlər sisteminin yaradılması və həyata keçirilməsi təşkil edir.

Aydındır ki, yeni təhlükələrin meydana gəlməsi onların qarşısının alınması üçün yeni mübarizə üsullarının işlənib hazırlanması tələb olunur.

Cinayətkarlara qarşı mübarizə aparmaq, onların fəaliyyətini nəzarət altında saxlamaq və izləmək, habelə cinayətkar əməllərin həyata keçirilməsində onlara mane olmaq məqsədilə xüsusi xidmət orqanları və informasiya təhlükəsizliyinə cavabdeh təşkilatlar tərəfindən müxtəlif mexanizmlər və vasitələr reallaşdırılır. Məsələn, ABŞ xüsusi xidmətləri 2001-ci il 11 sentyabr hadisələrindən təxminən bir həftə əvvəl Usama Ben Ladenin elektron məktubunu aşkar etmiş, lakin bu məktub şifrləndiyindən onu vaxtında aça bilməmişdilər.

Bir çox inkişaf etmiş ölkələr tərəfindən müxtəlif kommunikasiya sistemlərindən informasiyanın çıxarılması və emalını təmin edən xüsusi sistemlər artıq çoxdan reallaşdırılaraq istismar olunur. Bu sahədə aparıcı ölkə olan ABŞ-da müxtəlif kommunikasiya sistemlərindən informasiyanın çıxarılması və emalı üçün xeyli sayda sistemlər işlənib hazırlanmışdır. Bu sistemlər arasında Eşelon və Carnivore (DCS1000) sistemləri çox geniş miqyasda yayılmışdır.

Eşelon sistemi hər şeyi əhatə edən radioelektron izləmə sistemidir. Bu sistemə bütün dünyanı əhatə edən çoxlu sayda izləmə stansiyaları və çox böyük geostasionar peyklər pleyadası daxildir. Bütün bunlar birlikdə, demək olar ki, dünyanın istənilən nöqtəsində adi və mobil telefonlardan edilmiş zəngləri, radio stansiyalarla aparılan danışıqları, eləcə də İnternetlə ötürülən elektron poçtunu tutmağa imkan verir.

Təbii ki, bu nəhəng infrastrukturlar bir il ərzində yaranmamışdır. Belə ki, ilk peyklərin buraxılışı və yerüstü stansiyaların tikintisi hələ 80-ci illərdə həyata keçirilməyə başlanmışdı. Onlar Sovet İttifaqına qarşı mübarizə üçün nəzərdə tutulmuşdu, lakin Sovet İttifaqı dağıldıqdan sonra belə Eşelon layihəsi fəaliyyətini dayandırmadı, yalnız rəsmi olaraq onun təyinatı dəyişdirildi və cinayətkarlıqla, o cümlədən İnternetdə cinayətkarlığa qarşı mübarizəyə istiqamətləndirildi.

Eşelon sistemini işləyib hazırlamış ABŞ və Böyük Britaniyanın xüsusi xidmət orqanları və hərbi qurumları ilə yanaşı hazırda bu sistemin istismarında Avstraliyanın və Yeni Zelandiyanın xüsusi xidmət orqanları da iştirak edir. Sistemin özəyi çox güclü hesablama mərkəzindən ibarətdir. Bu mərkəzdən hər gün on milyonlarla elektron poçt məktubları, fakslar və digər məlumatlar keçir və onların məzmunlarından müvafiq nişanların (açar sözlərin) mövcudluğunu müəyyən etmək üçün emal olunur. Belə nişanlar qismində Usama Ben Laden, terrorçuluq, bakterioloji silah və s. götürülə bilər. Onları bəzən stopsiyahı adlandırırlar.

Məktubları və məlumatları ələkdən keçirən mürəkkəb emal alqoritmlərini keçdikdən sonra informasiya ştatda olan müvafiq mütəxəssislərdən birinin kompüterinə göndərilir. Həmin mütəxəssis bu informasiya ilə tanış olduqdan sonra müəyyən konkret qərar qəbul edir.

Göründüyü kimi, ilk baxışdan sistem alicənab məqsədlər– kiberterrorçuluq və mütəşəkkil cinayətkarlıqla mübarizə üçün nəzərdə tutulmuşdur. Lakin minlərlə istifadəçilər bu sistemdə özlərinin hüquqlarının pozulması təhlükəsini görürlər. Bu məqsədlə ictimaiyyət xüsusi etiraz aksiyaları keçirir, bu aksiyaların keçirildiyi həmin günlərdə etiraz edənlər bir-birlərinə stop-siyahıda olan sözlərin daxil olduğu çoxlu sayda məktublar göndərir və sistemi yanlış məktublarla həddən artıq yükləməyə çalışırlar. Hətta onlardan bəziləri kompüterləri yoluxduran və ünvanlar kitabında olan bütün ünvanlara Eşelon sisteminin stop-siyahısında olan sözlərin daxil olduğu məktublar göndərən xüsusi virus – İnternet-soxulcan yazmışdı. Ekspertlərin fikrincə bütün belə cəhdlər Eşelon sisteminə heç bir əhəmiyyətli ziyan vura bilməmişdir.

Eyni zamanda, yüksək vəzifəli Avropa məmurlarının son dövrlərdə bu sistemlərlə bağlı çıxışları ictimaiyyəti daha da qızışdırır və əhali arasında gərginlik yaradırdı. Belə ki, onların sözünə görə Eşelon sistemi çoxdan iqtisadi casusluq məqsədi ilə istifadə olunur. Sistemin belə fəaliyyəti nəticəsində milyardlarla dollar həcmində kontraktları Amerikanın xeyrinə itirirlər.

Bununla əlaqədar olaraq, Avropa İttifaqı növbəti iclaslarından birində bu məsələni müzakirəyə çıxarmış və özləri üçün Eşelon sisteminin analoqunun – TREVI sisteminin yaradılması üçün maliyyə vəsaitlərinin ayrılması barədə qərar qəbul etmişdi. Təbii ki, bu qərarda sistemin təyinatının adi cinayətkarlıqla və kibercinayətkarlıqla mübarizə olduğu göstərilmişdi.

Bu istiqamətdə FTB, MKİ və İnterpolun istintaq və təhqiqat qrupları tərəfindən istifadə olunan "i2" sistemini xüsusi qeyd etmək olar. Böyük Britaniyanın eyni adlı şirkətinin proqram məhsulu inkişaf etmiş ölkələrin milli hüquq mühafizə orqanları tərəfindən standart kimi qəbul edilmişdir.

“i2" sisteminin əsasını belə ideya təşkil edir ki, cinayət əməlləri müəyyən hərəkətlər ardıcıllığının köməyi ilə həyata keçirilir və hər bir konkret hərəkət müəyyən iz buraxır. Məhz "i2" sistemi belə izləri axtarmaq və öyrənmək məqsədilə yaradılmışdır. O, müxtəlif məlumat bazalarını (telefon danışıqlarını, təyyarədə uçan şəxslər haqqında məlumatları, avtomobili olanların siyahılarını, şübhəli bilinən şəxslər haqqında fərdi məlumatları, İnternet şəbəkəsinin bu və ya digər abonentinin hərəkətləri barədə informasiyanı və s.) özündə birləşdirir, mütəxəssislərə bu informasiya massivində olan məlumatların mümkün kombinasiyalarını tədqiq etməyə və müvafiq nəticələr çıxarmağa imkan verir.

Bu proqram kompüter informasiyası sahəsində cinayətkarların və terrorçuların tutulması üçün istifadə olunur. "I love you" virusunun filippinli müəllifi Onela de Quzman məhz bu proqramın köməyi ilə aşkar olunmuş və tutulmuşdur. Hazırda "i2" sistemi bir nömrəli terrorçu Usama Ben Ladenin tutulması üçün istifadə olunur.

Kibercinayətkarlığa qarşı mübarizə sahəsində Rusiya xeyli geri qalır. Rusiya hüquq mühafizə orqanları kompüter cinayətləri ilə mübarizədə əsasən İnternetdə qulaqasma qurğularının quraşdırılması və tətbiqinə ümid edirlər. Bu qurğuların köməyi ilə elektron poçtu ilə ötürülən məlumatlara baxmaq, istifadəçilərin İnternet səhifələrinə müraciətlərini izləmək mümkündür.

Məhz bu məqsədlə Rusiyada yaradılmış SORM (Materialların təhqiqatının asanlaşdırılması sistemi) sistemi əsasən vergilərin ödənilməsindən yayınanları və digər pozucuları aşkar etmək üçün nəzərdə tutulmuşdur. Lakin onun tətbiqinin əleyhdarları belə fikirdədirlər ki, bu sistem hamının danışıqlarına qulaq asılmasını və informasiya mübadiləsinə nəzarəti həyata keçirəcək və, beləliklə də, qanuna riayət edən vətəndaşların hüquqlarını pozacaqdır.

Təbii ki, kibermüharibə başlayarsa, bütün bu kimi sistemlər çox tez zamanda hərbi məqsədlər üçün istifadəyə istiqamətləndiriləcək və onun əsas silahı olacaqdır. Çox güman ki, bu məqamlar həmin sistemlərin konstruksiyasında nəzərdə tutulmuşdur.

**Kibercinayətlərin gizlədilməsi üsulları**

Kibercinayətkarlar öz əməllərini gizlətmək və fəaliyyətlərinin izlənməsini çətinləşdirmək məqsədilə müxtəlif sıra üsul və mexanizmlərdən istifadə edirlər. Daha çox istifadə olunan bəzi belə üsul və mexanizmlər barədə məlumatlar bunlardır:

- Parolların istifadəsi. Cinayətkarlar öz məlumatlarını ötürərkən onların parollarla bağlanması ən geniş yayılmış üsullardan biridir.

- Məlumatların şifrlənməsi. bir çox kompüter cinayətkarları müxtəlif formatlı məlumatları şəbəkə vasitəsilə ötürərkən onları şifrləyirlər. Bu yolla onlar məlumatlarının hüquq mühafizə və xüsusi xidmət orqanlarının, eləcə də rəqib tərəfin əlinə keçməsinin və ya onlar tərəfindən başa düşülməsinin qarşısını almağa çalışırlar.

- Mürəkkəb şifrləmə. Adətən məşhur xakerlər və təhlükəli cinayətkarlar öz məlumatlarını adi şifrləmə üsulları ilə deyil, xüsusi şifrləmə standartlarının köməyi ilə sifrləyirlər. belə şifrkodları açmaq üçün güclü kompüterlər, böyük vaxt və maliyyə vəsaitləri tələb olunur.

- Elektron poçtunun (e-mail) şifrlənməsi. xakerlər elektron poçtu vasitəsilə də məlumat göndərərkən onları şifrləyirlər. Xakerlərin əksəriyyəti elektron poçtunun şifrlənməsi üçün PGP şifrləmə proqramından istifadə edirlər. bu proqramı İnternetdən pulsuz əldə etmək olur. Cinayətkarlar mətnlərlə yanaşı, onları maraqlandıran yerlərin xəritələrini, fotoşəkillərini və digər müxtəlif detallarını elektron poçtu ilə göndərən zaman onları şifrləyirlər.

- Faylların sıxılması. Məlumatları, o cümlədən faylları ötürərkən onları əvvəl xüsusi proqramlar vasitəsilə sıxıb sonra şifrlədikdə effekt daha böyük olur və belə şifrkodun açılması xeyli çətinləşir. Onlara sıxılma prosesi zamanı parol da qoymaq mümkündür.

- Steqanoqrafiya. Bu mexanizm məxfi məlumatların varlığının gizlədilməsi prinsipinə əsaslanır. Belə məlumatlar faylların adını, parolu və ya diskdə yazıldığı yeri bilməyən istənilən şəxs üçün görünməz olur.

- Məlumatların başqa yerdə saxlanması. Kompüterlərdə təhlükəsizlik tədbirləri kifayət qədər etibarlı olmadıqda xakerlər öz məlumatlarını başqa yerdə olan kompüterlərdə saxlaya bilərlər. bu zaman məlumatların başqa kompüterlərdə gizlədilməsindən, adətən həmin kompüterlərin sahiblərinin xəbəri olmur.

- Anonim elektron poçtu. Anonim poçt xidməti göndərən şəxs haqqında heç bir İnformasiyaolmadan məlumatı ünvana çatdırır. Belə ki, bu zaman məlumatı alan tərəf göndərənin kimliyi və məlumatın mənbəyi haqqında heç bir bilgi əldə edə bilmir. Bu texnologiya anonim poçt vasitəçisi adlanan xüsusi poçt xidmətinin köməyilə həyata keçirilir.

- Açıq formların istifadəsi. cinayətkarlar şifrləmə mexanizmlərini istifadə etməklə açıq forumlarda sərbəst şəkildə ünsiyyətə girə bilərlər. 1997-ci ildə cinayətkarlar məhz açıq forum texnologiyasından, daha doğrusu America Online Net Girl Board xidmətindən istifadə etməklə Microsoft şirkətinin Bill Qeytsi ölümlə hədələmişdilər.

- Internetdə söhbət və görüş texnologiyasından istifadə. Cinayətkarlar interaktiv danışıq və ya yazışma vasitəsilə ünsiyyətin qurulmasını İnternetin söhbət (chat) rejiminin köməyilə həyata keçirə bilərlər. onlar burada əvvəlcədən xüsusi kodlaşdırılmış formada, yəni şərtilikləri istifadə etməklə ünsiyyətdə olurlar.

- Kompüter müdaxiləsi və dolaşdırma. Xakerlər hər hansı sistemə soxula və ondan digər kompüterə daxil olmaq üçün aralıq vasitə kimi istifadə edə bilərlər. bu yolla müvafiq kompüterə daxil olan xakerlər öz məlumatlarını digər kompüterə ötürür, beləliklə, izi itirməyə çalışır ki, onu izləmək çətin olsun. Bu texnologiyanı dolaşdırma adlandırırlar.

- Yoxlamama imkanın olmaması. Bir çox təşkilatlar sonradan hadisələrin baş verəcəyi təqdirdə izləməni təmin etmək məqsədilə sistemə giriş parollarını avtomatik yoxlayan proqramları reallaşdırır və tətbiq edirlər. belə olduqda cinayətkarlar başqa proqramları (Root Kit və ya Zap proqramlarını) istifadə etməklə bu proqramın yoxlamanı həyata keçirən hissəsini sıradan çıxarır və ya onların fəaliyyətinə aid olan yazıları pozurlar.

**Müxtəlif sahələrdə olan kibernetik cinayətlər**

İnkişaf etmiş ölkələrdə maliyyə və bank sistemlərinin informasiya-texniki təminatı ilə məşğul olan strukturlar, praktiki olaraq, onlara qeyri-məhdud dərəcədə təsir göstərmək imkanlarına malik olurlar. Belə ki, maliyyə vəsaitlərinin real idarə edilməsi üçün həmin texniki təşkilatlar tərəfindən xidmət göstərilən məlumat banklarına, kompüter şəbəkələrinə və telekommunikasiya sistemlərinə daxil olmaq lazım gəlir. İnformasiya texnologiyalarının beynəlxalq xarakteri ona gətirib çıxarmışdır ki, kompüter şəbəkələri vasitəsilə həyata keçirilən informasiya axınlarına giriş əldə edə bilən şəxslər, təşkilatlar və ölkələr real olaraq müxtəlif ölkələrdə vəziyyətə təsir etmək iqtidarında olurlar. Məsələn, ABŞ-ın xarici borcu bir neçə trilyon təşkil etməsinə baxmayaraq, bu, ölkənin rəhbərliyini çox da narahat etmir. Məsələ ondan ibarətdir ki, dünyanın bütün banklarının 60%-nin fəaliyyətini təmin edən informasiya bankları ABŞ-da yerləşir. Bu isə müasir dövrdə real kapitaldır.

İsveçrə bankları dünyada maliyyə sahəsində liderliyə malikdirlər, lakin bu ölkənin banklarının 80%-nin informasiya xidməti ABŞ-da həyata keçirilir. Məhz bu kibernetik terrorçuluq cinayətləri amil ABŞ-ın bu sahədə üstünlük əldə etməsinə imkan verir. Ona görə də kompüterlər, kompüter sistemləri və şəbəkələri çox şeylər vəd edən cinayətkarlıq silahına çevrilmişdir. İnkişaf etmiş ölkələrdə, praktiki olaraq, bütün pul əməliyyatları kompüter sistemləri və şəbəkələri vasitəsilə həyata keçirilir. Active Media Research şirkətinin məlumatlarına görə, ABŞ-da 2000-ci ildə elektron kommersiyanın ümumi həcmi 2 trilyon ABŞ dolları təşkil etmişdir.

Qərb ölkələrində iqtisadiyyat sahəsində kibercinayətkarlıq hadisələri nəticəsində dəyən ziyanın məbləği orta hesabla 450 mindən 1 milyardadək ABŞ dolları təşkil etmişdir. Müxtəlif ölkələrdə məhz bu səbəbə görə firmaların illik itkiləri artıq milyardlarla (ABŞ ~ 100 milyard, Böyük Britaniya ~ 4,45 milyard, Qərbi Avropa ölkələri ~ 39 milyard) ABŞ dolları ilə ölçülür. Çirkli pulların leqallaşdırılması («yuyulması»), kompüter proqramları üzərində olan intellektual mülkiyyət hüquqlarının pozulması, kommersiya və ya sənaye casusluğu, elektron ödəniş kartlarının mənimsənilməsi ilə bağlı cinayətlər xüsusilə diqqəti cəlb edir.

Ekspert qiymətləndirmələri göstərir ki, beynəlxalq səviyyədə elektron ödəniş kartları ilə bağlı cinayətlər bey-nəlxalq bank sistemlərinə kart hesabları üzrə əməliy-yatların 10%-dək həcmində zərər vurur. Belə ki, Master kart beynəlxalq elektron ödəniş sistemində 703000 ABŞ dolları, VİSA kart elektron ödəniş sistemində isə 1,2 milyard ABŞ dolları məbləğində zərərlə nəticələnən belə fırıldaqlar qeydə alınmışdır.

Kredit kartlarının saxtalaşdırılması, kompüterlərin köməyi ilə pulların oğurlanması ABŞ, İtaliya və bir sıra digər ölkələrdə həqiqi fəlakət xarakteri almışdır. Şirkətlər, ələlxüsus, banklar əmanətçilərin, aksiyaçıların, tərəfdaşların yanında etibarlarının itirilməsindən qorxaraq kompüter oğurluğu faktlarını mümkün qədər gizlətməyə çalışırlar. Ona görə də itkilərin miqyasının statistik qiymətləndirilməsi barədə rəsmi məlumat, demək olar ki, yox dərəcəsindədir. Ekspertlərin fikrincə, ABŞ-da kompüterlərin köməyi ilə banklardan silahlı qarətlərə nisbətən 4 dəfə çox oğurluq həyata keçirilir. Son on il ərzində belə oğurluqlar nəticəsində itkilərin həcmi 20 dəfədən çox artmış və onların ümumi məbləği onlarla trilyon dollar miqdarında müəyyən edilir. Ümumiyyətlə, belə cinayətlərin açılması 15%-dən çox deyildir.

Kompüter cinayətkarlığı ilə mübarizə məsələləri sa-həsində Mərkəzi və Şərqi Avropa ölkələrinin hüquq mühafizə orqanları ilə əməkdaşlıq üzrə İnterpolun işçi qrupunun 28-30 avqust 2000-ci ildə keçirilən altıncı iclasında qeyd olunmuşdur ki, kibercinayətlər nəticəsində əldə olunan mənfəət həcminə görə narkotik alveri və qeyrileqal silah satışı yolu ilə əldə olunan mənfəətdən sonra üçüncü yeri tutur.

Avropa Şurasının ekspertləri tərəfindən qeyd olunmuşdur ki, xakerlərin yalnız kredit kartları vasitəsilə həyata keçirdikləri fırıldaqlar nəticəsində Avropa Birliyi ölkələrinə hər il təxminən 400 milyon, kompüter virusları vasitəsilə təxminən 12 milyard, mülkiyyət hüquqlarının pozulması nəticəsində isə 250 milyard ABŞ dolları həcmində ziyan vurulur.

ABŞ-da informasiya sistemlərinin müdafiəsi üzrə agentlik (DİSA) tərəfindən keçirilən eksperiment çərçivəsində 1995-ci ildə yüksək ixtisaslı «elektron piratlar» qrupu qısa müddət ərzində Pentaqonun kompüter sisteminə daxil olmuş və ABŞ Müdafiə Nazirliyinin 8900 kompüterindən 88%-ni öz nəzarəti altına almışdır.

Pentaqonun təhlükəsizlik şöbəsi hər bazar günü ABŞ Müdafiə Nazirliyinin informasiya qovşaqlarına 60-dan artıq xaker hücumlarını qeydə alır.

1995-ci ildə ABŞ-ın Hesablama Palatası Müdafiə Nazirliyi, həmçinin onun sifarişlərini yerinə yetirən təşkilatlar tərəfindən nazirliyin informasiya resurslarına xarici İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq şirkətlərin buraxılmasının qadağan olunması məsələsini ciddi şəkildə qaldırmışdır.

Məhz həmin il Almaniyadan olan xaker Hərbi Hava Qüvvələrinin Nyu-Yorkdakı kompüter bazasına (bu bazada hansı bombanın nə vaxt və hara atılacağı barədə informasiya saxlanılırdı) daxil olmuşdu. Sonra həmin xaker bu kompüter vasitəsilə Çili, Kolumbiya, Latviya və Koreyadakı digər kompüterlərə qoşularaq Pentaqonun kompüter şəbəkələrindən nüvə silahı haqqında 29 sənədi, o cümlədən nüvə, kimyəvi və bakterioloji silahlardan müdafiənin ordu planını oğurlaya bilmişdi.

Reuter agentliyinin məlumlarına görə 2001-ci ildə Fələstin tərəfdarı olan minlərlə istifadəçi öz kompüterlərindən eyni zamanda məqsədyönlü şəkildə hücumlar həyata keçirməklə İsrailin Müdafiə Nazirliyinin saytının fəaliyyətində problemlər yaratmış, nəticədə trafik olduqca yüklənmiş və bu saytlara giriş, demək olar ki, bağlanmışdır. Bunun cavabında İsrail xakerləri «Hizbullah» müsəlman qruplaşmasının saytını uzun müddətə sıradan çıxarmışdılar.

Əl-Qaidənin kompüter texnologiyaları üzrə yüksək ixtisaslı mütəxəssislərə və «Promis» kompüter proqramına malik olması barədə informasiya artıq o zaman bəlli idi. «Promis» proqramı Amerikanın xüsusi xidmət orqanlarının fəaliyyətini izləmək, ABŞ-ın strateji obyektləri haqqında məxfi məlumatları əldə etmək, eləcə də heç bir problem olmadan cinayətkarlara «çirkli pulları yumaq» imkanlarını yaradırdı.

1992-ci ildə Litvadakı İqnalin AES-in kompüterinə «troya atının» yeridilməsi nəticəsində Çernobıl qəzasına bənzər qəzanın baş verməsi təhlükəsi yaranmışdı.