AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

İNFORMASİYA TƏHLÜKƏSİZLİYİ

(DƏRSLİK)

B A K I – 2 0 1 6

İNFORMASİYA TƏHLÜKƏSİZLİYİ

Redaktoru: i.e.d., prof., Balayev Rəsul Ənvər oğlu
Rəyçilər: i.e.d., prof,
i.e.d., prof.,
i.e.n., dosf., Musayev İsa Kərim oğlu
t.e.n., dos., Mənsimov Haqverdi İsgəndər oğlu
Dizayner: Əliyev Zaur Nəsrəddin oğlu

ƏLİZADƏ MƏTLƏB NURUŞ OĞLU
BAYRAMOV HAFİZ MƏHƏRRƏM OĞLU
MƏMMƏDOV ƏLÖVSƏT SULİDDİN OĞLU

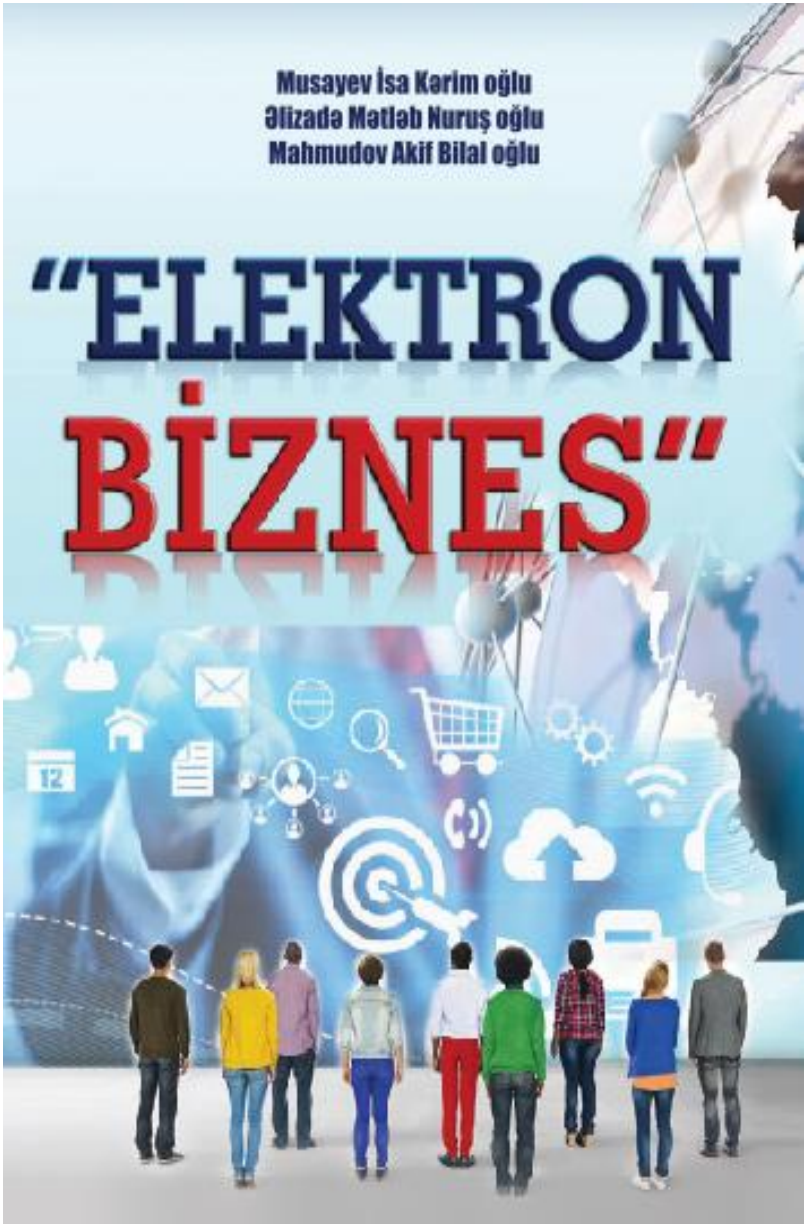
İNFORMASİYA TƏHLÜKƏSİZLİYİ, Dərslik, Bakı, "İQTİSAD UNİVERSİTETİ" nəşriyyatı, şəkilli, 2016 - 384 səh.

Dərslikdə informsiya təhlükəsizliyinin əsas anlayışları, kompüter sistemlərində və şəbəkələrində informasiya hədələri haqqında məlumat, onların təhlil edilməsi tutarlı səviyyədə verilir. Təhlükəsizlik siyasətinin baza anlayışları müəyyənləşdirilir. Kriptoqrafik üsullarla yanaşı kompüter informasiyasının müdafiə alqoritminə baxılır.

Korporativ şəbəkələrdə informasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma əsaslandırılır. Şəbəkələrarası verilənlərin mübadiləsinin müdafiə edilməsinin baza texnologiyası izah olunur. Antivirus müdafiə və onun üsullarına baxılır. Standartlardan istifadə etməklə informasiya təhlükəsizliyinin təmin edilməsi üçün istifadə olunan təşkilatı-qanunlar ətraflı izah olunur.

Dərslik tələbələr, bakalavr və magistr pilləsinin uyğun ixtisasında təhsil alanlar, müəllimlər və bu sahədə çalışan elmi işçilər üçün nəzərdə tutulmuşdur.

M Ü N D Ə R İ C A T


Musayev İsa Kərim oğlu
Əlizadə Mətləb Nuruş oğlu
Mahmudov Akif Bilal oğlu
"ELEKTRON
BİZNES"

İNFORMASİYA TƏHLÜKƏSİZLİYİ. GİRİŞ

ƏSAS ANLAYIŞLAR

İnformasiya təhlükəsizliyi dedikdə informasiyanın və informasiya mühitinin təsadüfi və ya düşünülmüş təbii və ya süni xarakterə malik təsirlərdən müdafiə vəziyyəti başa düşülür. Belə təsirlər informasiyaya və ya informasiya obyektlərinə, həmçinin informasiya istifadəçisinə və sahibinə yolverilməz ziyanlar vura bilir.

İnformasiyanın mühafizəsi – informasiya təhlükəsizliyinin təmin olunması üçün həyata keçirilən kompleks tədbirlərdir.

Bu baxımdan dərsliyin mahiyyəti nisbətən cavan, amma dinamik inkişaf edən informasiya texnologiyaları sahələrində istifadə olunan informasiyanın müdafiə olunma modelinin və üsullarının, həmçinin bu məqsədlə istifadə edilən vasitələrinin öyrənilməsi və tədqiq edilməsidir.

İndiki zamanda informasiyanın təhlükəsizliyi informasiyanın ən çox yayılmış üç əsas xüsusiyyətinə əsaslanır: konfidensiallıq, tamlıq və əlçatanlıq.

İnformasiyanın konfidensiallığı həddindən artıq məhdud dairədə olan insanlar ilə tanış olmağın mümkünlüyünü ifadə edir. Bu insanlar informasiya sahibləridirlər. Əgər informasiyanı bu şəxslərdən başqa icazəsi olmayan digər şəxslərdə istifadə edə bilirlərsə, onda informasiyanın konfidensiallığı itmiş olur.

Bəzi informasiya növləri üçün konfidensiallıq əsas atribut sayılır (məsələn, strateji tədqiqatlarla bağlı olan məlumatlar,

tibbi qeydlər, sığorta ilə bağlı yazılar, yeni istehsal olunacaq məhsul haqqında xüsusi məlumatlar və s.). Bəzi hallarda konkret şəxslər barədə olan məlumatlarda da konfidensiallığı saxlamaq lazımdır (məsələn, bankın müştərisi haqqında informasiyanı, kredit verənlər haqqında, vergi haqqında verilənləri, tibbi müəssisələrdə pasientlərin vəziyyəti haqqında məlumatları və buna bənzərləri).

İnformasiyanın tamlığı onun təhrif olunmamış şəkildə saxlanma bacarığını (qabiliyyətini) müəyyənləşdirir. Səlahiyyəti olmayan, qabaqcadan nəzərdə tutulmamış istifadəçi tərəfindən informasiyanın itirilməsi (operatorun səhvi və ya səlahiyyətsiz şəxsin qəsddən etdiyi hərəkət nəticəsində) onun tamlığının itirilməsinə səbəb olur. Tamlıq əsasən kritik infrastruktura malik obyektlərin müəyyən fuksiyanı yerinə yetirməsində yararlı olan maliyyə verilənləri üçün xüsusilə vacibdir (məsələn, enerji təminatında, hava yollarının idarə edilməsində və s.).

Pisniyyətli şəxsin İsveçrədə yerləşən nüvə fizikası laboratoriyasına gizli yolla daxil olaraq kompüter sisteminə daxil olması və **"π" *ədədində*** bir işarənin və ya vergülün yerinə dəyişməsi laboratoriyada həyata keçirilən eksperimentin mənasız aparılmasına, nəticədə milyonlarla paranın havaya sovrulmasına səbəb olacaqdır.

AŞIQLAMA: π ədədinin vergüldən sonra 1000 işarə dəqiqliklə hesablanması.

3,1415926535 8979323846 2643383279 5028841971 6939937510
5820974944 5923078164 0628620899 8628034825 3421170679
8214808651 3282306647 0938446095 5058223172 5359408128
4811174502 8410270193 8521105559 6446229489 5493038196
4428810975 6659334461 2847564823 3786783165 2712019091

4564856692 3460348610 4543266482 1339360726 0249141273
7245870066 0631558817 4881520920 9628292540 9171536436
7892590360 0113305305 4882046652 1384146951 9415116094
3305727036 5759591953 0921861173 8193261179 3105118548
0744623799 6274956735 1885752724 8912279381 8301194912
9833673362 4406566430 8602139494 6395224737 1907021798
6094370277 0539217176 2931767523 8467481846 7669405132
0005681271 4526356082 7785771342 7577896091 7363717872
1468440901 2249534301 4654958537 1050792279 6892589235
4201995611 2129021960 8640344181 5981362977 4771309960
5187072113 4999999837 2978049951 0597317328 1609631859
5024459455 3469083026 4252230825 3344685035 2619311881
7101000313 7838752886 5875332083 8142061717 7669147303
5982534904 2875546873 1159562863 8823537875 9375195778
1857780532 1712268066 1300192787 6611195909 2164201989

Hamıya məlum olan **π** ədədinin keçmiş adı *Ludolfov ədədidir*. π ədədi ilk dəfə İohan Lambert tərəfindən 1761-ci ildə sübut olunmuşdur. 1794-cü ildə Lejendr π ədədinin irrasional ədəd olduğunu sübut edir. 1882-ci ildə Münhen universitetinin professoru Feliks Kleyn ədədin ***transsendent ədəd*** olduğunu sübuta yetirir.

İlk dəfə ədədin yunan hərfi ilə işarə edilməsini ingiltərəli riyaziyyatçı Jons 1706-cı ildə təklif edir. Amma ədədin hamı tərəfindən qəbul olunması Leonard Eylerin apardığı elmi işlərlə bağlıdır (1737-ci il). Ədədin π kimi işarə olunması yunan hərflərindən yaranmış iki söz ilə bağılıdır: περιφέρεια — çevrə, kanar və περίμετρος — perimetr.

Ədədin keçdiyi tarixi yolu üç dövrə ayırırlar: qədim dövr (ədəd həndəsi baxımdan öyrənilir), klassik dövr (ədəd Avropada XVII əsrdə riyaziyyatın inkişafi ilə bağlı araşdırılır) və rəqəmsal kompüterlər dövrü (Con fon Neyman ENİAK

hesablama maşınında π ədədini 2037 ədəd dəqiqliklə hesablamış, buna 70 saat vaxt sərf etmişdi. Bu 1949-cu ilə təsadüf edir).

XX əsrin başlanğıcında hind riyaziyyatçısı Spinivasa Ramanudjan ədədin hesablamasına yararlı olan çoxlu düsturların olduğunu aşkar edir.

2005-ci ildə dünya rekordu, yəni vergüldən sonra 67 890 ədəd dəqiqliklə π -nin hesablanması çinli Lyu Çaoya məxsusdur. Çao buna 24 saat 4 dəqiqə vaxt sərf etmişdi. Vergüldən sonra 70 000 ədədin yadda saxlanılması 21 yaşlı hindistanlı tələbə Racvir Mina (Rajveer Merena) məxsusdur. Dünya rekordu 9 saaat 27 dəqiqə ərzində tələbə tərəfindən həyata keçirilmişdir (bu 2015-ci ilə təsadüf edir) və s.

1897-ci ildə Amerikanın İndiana ştatında ədədin 3,14 deyil 3,2 –yə bərabər olduğunu sübut edəcək qanun işıq üzü görür, amma bu məsələyə universitetin professoru Perdyu qarışdıqdan sonra qanun qüvvəsini itirir, ədədin qiymətinin əvvəlki kimi hesablanmasına qərara verilir.

Transsendent ədəd (latınca transcendere - keçmək, üstələmək) — cəbri olmayan, kompleks və ya həqiqi ədədlər, başqa sözlə, qüvvəti tam ədəd (və ya rasional ədədlər) olan polinomun (çoxhədlinin) kökü olmayan həqiqi ədədləri adlandırırlar.

İlk dəfə transsendent ədəd anlayışını elmə, 1844-cü ildə Liuvill Jozef (1809-1882) daxil etmişdir. Alim yaratdığı teoremində sübut etdi ki, cəbr ədədə, rasional kəsrlə yaxınlaşmaq mümkün deyil. 1873-cü ildə Ermit Şarl (1822-1901) natural loqarifmaların əsaslarında **e** ədədinin transsendentliyini sübut etdi.

Liuvill Jozef

Ermit Şarl

Karl Luis Ferdinand fon Lindeman

Aleksand Osipoviç Qelfond

İNFORMASİYA TƏHLÜKƏSİZLİYİ

1882-ci ildə Lindeman Ferdinand (1852-1939) "sıfır"dan fərqli cəbr göstəricisi ilə **e** ədədinin dərəcəsinin transsendentliyi haqqında teoremi sübut etdi, bununla da **π** ədədinin və dairə kvadraturası məsələsinin həll edilməzliyinin transsendentliyini sübut etdi.

1934-cü ildə A.O. Qelfond (1906-1968) sübut etdi ki, bütün bu tip ədədlər həqiqətən transsendentdir.

İnformasiyanın əlçatanlığı sistemdəki informasiya obyektinə müvafiq səlahiyyət sahibi olan istifadəçinin ona mənsub olan vaxt ərzində həmin obyektə maniəsiz daxil olma xüsusiyyətinin müəyyən edilməsidir. İnformasiyanın bloklanması və ya məhv edilməsi əlçatanlığın itməsinə gətirib çıxarır (məsələn, əməliyyatın düşünülmüş şəkildə və ya səhv olaraq yerinə yetirilməsi).

Əlçatanlıq informasiya sisteminin maliyyələşdirilməsinin əsas atributudur. Əlçatanlıq müştərilərə xidmətin göstərilməsinə istiqamətlənir (məsələn, sərnişinlərə dəmir yolu biletlərinin satılması, proqram təminatının yenilənməsinin həyata keçirilməsi və bu sahə ilə maraqlananlara çatdırılması və s.).

Əgər səlahiyyət verilmiş (təhkim edilmiş) istifadəçi müəyyən işləri yerinə yetirmək üçün informasiya sisteminə əlşatanlıqdan məhrumdursa, bu vəziyyət xidmətdən imtina kimi nəzərə alınır (məsələn, şəbəkə sistemindən istifadə edəçək şəxsin şəbəkədən istifadə etməsinə icazə verilmir).

Öndə göstərilənlərdən başqa daha iki xüsusiyyət informasiya təhlükəsizliyi üçün çox vacibdir. Bu xüsusiyyətlərə autentifikasiyanı və appelliyasiyanın verilməsini aid etmək olar.

Autentifikasiya məlumat sahibinin kimliyinin gerçəklənməsi imkanını müəyyən edir.

Apellyasiyanın verilməsi isə məlumat sahibinin həqiqətəndə başqası deyil, o şəxs olduğunu sübut etməyə imkan verir.

AÇIQLAMA: *Autentifikasiya* istifadəçi tərəfindən təqdim edilən identifikatorun əsl (həqiqi) olmasının yoxlanması prosesidir. Autentifikasiya (ingiliscə authentication) – real, həqiqi, müəllif anlamlarını verir.

Qədim zamanlardan insanlar qarşısında mürəkkəb bir məsələ dürürdü – vacib bir məlumatın dəqiqliyinə əmin olmaq. Bu məqsədlə müxtəlif formalı möhürlərdən, danişiq vaxtı deyilən parollardan istifadə edilirdi. Mexaniki qurğulardan istifadə etməklə autentifikasiya üsullarının yaranması bu problemi müəyyən qədər aradan qaldırdı (məsələn, müxtəlif qıfılların və açarların hazırlanması, yazıların müəyyən şriftlərlə kodlaşdırılaraq yazılması və s.). Autentifikasiya misal kimi yaşından asılı olmayaq bütün insanlar tərəfindən sevilə-sevilə oxunan "Əlibaba və qırx quldur" nağılını göstərmək olar. Quldurlar sadə bir sözdən ("Sim-Sim açıl") istifadə etməklə iri bir qayanı yerindən oynadırdılar.

Autentifikasiyanın müsbət nəticələrindən biri istifadəçinin müəlliflik huqunun tanınmasıdır. Yəni istifadəçiyə ona tapşırılmış müəyyən məsələlərin həll edilməsi üçün bu məsələlərin həllində istifadə olunacaq vəsait mənbəyindən istifadə hüququnun verilməsidir. Resursun vacibliyindən və ona yaxınlaşma (daxil olma) üsullarından asılı olaraq autentifikasiyanın müxtəlif üsulları istifadəçilərə təqdim edilir.

Rus dilində termin əsasən informasiya texnologiyalarında istifadə edilir. Bu baxımdan sistemin

təhlükəsizlik siyasətinin həyata keçirilməsi və inamın (etibarın) yerinə yetirilməsi bir tərəfli və ya qarşılıqlı ola bilir. Bütün bunlar kriptoqrafiyanın köməkliyi ilə yerinə yetirilir.

Autentifikasiyanı müəlliflik (subyektə müəyyən hüququn verilməsi) və identifikasiya (subyektin ona məxsus identifakatoru ilə tanınması) ilə qarışıq salmaq olmaz.

Autentifikasiyaya aşağıda verilənlərin həqiqiliyinin sübut edilməsi prosedurlarını aid etmək olar.

Məsələn:

- İstifadəçinin həmin şəxs olduğunun yoxlanması. Bunun üçün verilənlər bazasındakı parol ilə istifadəçinin parolu tutuşdurulur;
- Yola salınmış elektron məktubların həqiqiliyinin yoxlanması. Bunun üçün göndərənin ona məxsus açarı ilə məktubun rəqəmsal imzası tutuşdurulur;
- Faylların kontrol məbləğləri ilə müəllif tərəfindən təqdim edilmiş faylların məbləğləri tutuşdurulur.

İndiki zamanda şəbəkə texnologiyalarının sürətli inkişafı ilə əlaqədar olaraq avtomatlaşdırılmış autentifikasiyadan hər yerdə geniş şəkildə istifadə olunur.

Apellyasiya (appellatio - latınca müraciət etmə anlamını verir) qanuni qüvvəyə minməmiş aktın müəyyən prosessual qanunvericiliyə uyğun ali hakim tərəfindən yoxlanma prosedurasıdır.

Apellyasiya anlayışından Fransada istifadə edilmişdir və bu XIII əsrə təsadüf edir. Bu zamanlar apellyasiya haqsızlığa qarşı məhkəmə tərəfindən verilmiş şəxsi xarakterli hökm sayılırdı. 1667-ci ildə nəşr olunmuş qanun kitabında qeyd edilir ki, apellyasiya şəxsin məhkəməyə deyil, onun çıxardığı hökmə görə verilə bilər. 1579-cu ildə Henrix III belə bir fərman verir: karolun fərmanının əksinə verilmiş bütün

qanunlar dəyərsiz sayılmalıdır. XIX əsrdə Fransada iki məhkəmə qərarı qüvvəyə minir: kassasiya və apellyasiya.

Dərslikdə informasiyanın xüsusiyyətlərinin təbiəti, bu xüsusiyyətlərin əmələ gətirdiyi təhlükə (təhdid, qorxu, xətər) öyrənilir. Bununla yanaşı dərslikdə baş vermiş təhlükələrə qarşı həyata keçirilən tədbirlər və üsular araşdırılır.

İNFORMASİYA TƏHLÜKƏSİZLİYİNƏ YÖNƏLMİŞ TƏHLÜKƏLƏR

Təhlükə - istənilən bir şəxsin maraqlarına ziyan vura biləcək potensial baş verən hərəkət, hadisə, proses və ya təzahür hesab olunur.

Uyğun olaraq informasiya təhlükəsizliyinə yönəlmiş təhlükə dedikdə potensial baş verən hərəkətin, hadisənin, proses və ya təzahürin informasiyaya və ya avtomatlaşdırılmış informasiya sistemlərinin (AİS-nin) komponentinə təsiri başa düşülür. Yönəlmiş təhlükə birbaşa və ya bilavasitə informasiya münasibətlərində olan subyektlərin fəaliyyətinə ziyan vura bilir.

Hücum – təhlükənin realizə edilməsinə göstərilən cəhddir.

Pozma – təhlükənin realizə olunmasıdır.

Avtomatlaşdırılmış informasiya sistemlərinə təsir edəcək mümkün təhlükələrin təsnifatı, təhlili və müəyyən edilməsi həmin sistemlərin təhlükəsizliyinin təmin edilməsinin əsas aspektlərindən biri sayılır. Təhlükələrin siyahısı, onların realizə olunma ehtimalının qiymətləndirilməsi, həmçinin nizam-intizamı pozma modeli sistemin müdafiəsinə qoyulmuş tələblərin formalaşmasına və baş verə biləcək riskin təhlilinin araşdırılmasına imkan verir.

İnformasiya təhlükəsizliyinin təsnifatı bir neçə kriteriya əsasında yerinə yetirilə bilər:

1.*İnformasiya təhlükəsizliyinin aspekti baxımından*: təhlükənin konfidensiallığı, tamlığı və əlçatanlığı. Bura təhlükənin aufentifikasiyasını və apellyasiya verilməsini də əlavə etmək olar.

2.*Avtomatlaşdırılmış informasiya sistemlərinin təşkiledicilərinə təhlükənin vurduğu ziyan baxımından*: verilənlər, proqram təminatı, infrastrukturun dəstəklənməsi.

3.*Təhlükənin mənbəyinin yerləşməsi baxımından*: araşdırılan avtomatlaşdırılmış informasiya sisteminin daxilində və ya xaricində yerləşənlər. ***İnsayderlər*** tərəfindən həyata keçirilən təhlükələr daha qorxuludur.

4.*Əmələgəlmə təbiəti baxımından*: təbii (obyektiv) və sünii (subyektiv). *Təbii təhlükələr* - insandan asili olmayaraq AİS-nə və onun elementlərinə obyektiv fiziki proseslərin və təbii fəlakətlərin baş verməsi nəticəsində təsir göstərən təhlükələrdir. *Süni təhlükələr* – insanın fəaliyyəti nəticəsində baş vermiş təhlükələrdir. Belə təhlükələrə düşünülməmiş, məqsədsiz və təsadüfi təhlükələri, AİS-nin layihələndirilməsində baş vermiş səhvləri, proqram təminatında nəzərə alınmayan səhvləri, iş prosesi zamanı işçi personal tərəfindən buraxılmış səhvləri və nəhayət, bədəməlli şəxslərin məqsədyönlü həyata keçirdiyi təhlükələri və buna bənzərləri aid etmək olar.

AÇIQLAMA: *İnsayder* (ingiliscə insider) informasiya bazasına daxil olmaq imkanı olan, geniş kütlə tərəfindən o qədər də tanınmayan, müəyyən mütəxəssislər tərəfindən yaradılmış qrupun üzvlərindən biridir. Termin əsasən gizli saxlanan informasiya ilə bağlıdır, çünki qiymətli informasiyadan istifadə edə bilən şəxs ancaq bu qrupun

üzvü olmalıdır, yəni insayder olmalıdır. Bir çox hallarda insayderi müəssisədən kənarda çalışan mütəxəssis ilə müqayisə edirlər. Mütəxəssis müəssisədaxili və müəssisəxarici informasiyalara malik olduğu halda, insaydr şirkətdə "informasiyanı ilk eşidən" sayılır. ABŞ-da insayder şirkətin direktoru, şirkət aksioneri, şirkətin məsul qulluqçuları və nəhayət şirkətin aksiyasının 10%-dən çoxuna rəhbəhlik edənlər sayılırlar. İnsayder işə qəbul olunan zaman götürdüyü öhdəçilik ondan ibarətdir ki, o, şirkətin marağlarını öz maraqlarindan mütləq şəkildə üstün tutmalıdır. Şərti pozan insayder ciddi cəzalandırılır. Əgər insayder informasiyanın alqı-satqısı ilə məşğul olursa, o, aksionerlər qarşısında götürdüyü öhdəliklıləri pozmuş sayılır, işdən qovulur.

Müxtəlif ədəbiyyatlarda verilmiş təhlükələrin (insan tərəfindən törənilmiş - qərəzsiz, bilmərəkdən, diqqətsizlikdən və ya səhlənkarlıqdan, pislik fikrində olmadan) siyahısını nəzərdən keçirək:

1.Bilmərəkdən edilmiş hərəkətlər nətəcəsində sistemin hissələrlə və ya tam şəkildə işləməkdən imtina etməsinə, aparat hissəsinin dağıdılmasına, proqram təminatının zədələnməsinə, informasiya resurslarının xarab olmasına səbəb olur. Bu syahıya avadanlığın düşünülməmiş şəkildə dağıdılmasını, mühim informasiyanı özündə saxlayan faylların korlanmasını, istifadə olunan proqramların sistemdən kənarlaşdırılmasını və sairəni də əlavə etmək mümkündür;

2.Qurğuların və proqramın işləmə rejiminin dəyişdirilməsi və ya qanunsuz olaraq avadanlığın şəbəkədən ayrılması;

3.İnformasiya daşıyıcılarına düşünülmədən xətərin yetirilməsi;

4.Sərişdəsizlik (və ya təcrübəsizlik) üzündən sistemin işləmə qabiliyyətini korlayan proqramın işə salınması və ya informasiya daşıyıcılarının formatlanmasının həyata keçirilməsi, lazım olan verilənlərin ləğv edilməsi və s;

5.İş yerində istifadə olunan kompüterlərin resurslarından istifadə edərək qeyri-leqal və ədəbsiz proqramlardan istifadə edilməsinin və tətbiq edilməsinin (oyun, öyrədici, texnoloji və başqaları) məhdudlaşdırılması. Bunlar istifadə olunan kompüterlərin əlavə yüklənməsinə, operativ yaddaşın səmərəsiz istifadə edilməsinə, xarici yaddaş qurğusunun mənasız proqramlarla yüklənməsinə və s. gətirib çıxarır;

6.İstifadə olunan kompüterin viruslara yoluxmasına imkanın verilməsi;

7.Ehtiyatsız hərəkət nəticəsində konfidensial olan informasiyaların hamıya yayılması və bu tip informasiyaların hamı üçün əlçatan olması;

8.İstifadə olunan parolların, şifrələnmiş açarların, identifikasiya kartoçkalarının və başqalarının hamıya bildirilməsi nəticəsində informasiya atributlarının ötürülməsi, məxfiliyinin itirilməsi və istənilən şəxsin bu barədə məlumatlı olması;

9.Sistemin işləmə qabiliyyətinə və istifadə olunan informasiyaya təhlükə yaradan amillərin (məsələn, sistemin arxitekturasının layihələndirilməsi, verilənlərin texnologiya əsasında təhlili, tətbiqi proqramların yaradılması və s.) araşdırılması;

10.Sistem işləyərkən təşkilatı məhdudiyyətlərə qoyulmuş qanunlar əsasında əhəmiyyətin verilməməsi;

11.Müdafiə vasitələrindən yan keçməklə sistemə daxil olmaq (məsələn, sazlanmış əməliyyat sistemini xarici informasiya daşıyıcılarından istifadə etməklə sistemə yükləmək);

12.Təhlükəsizlik xidməti işçiləri tərəfindən müdafiə sisteminin qeyriqanuni şəbəkədən açılması, təcrübəsiz istifadə olunması, sazlanması və s. qarşısının alınması;

13.Abonentin (qurğunun) yanlış ünvanına verilənlərin göndərilməsi;

14.Düzgün olmayan informasiyanın daxil edilməsi;

15.Bilmərəkdən rabitə kanalına zədə vurulması.

Düşünülmüş şəkildə işin pozulmasının əsas yolları, sistemin işdən çıxarılması, sistemə daxil olma və icazəsiz informasiyadan istifadə etmə və s. aşağıdakı hallarda baş verir:

1.Sistemin fiziki dağıdılması (partlayış və yanğınlar törətməklə və s.) və ya kompüter sisteminin əsas təşkiledicilərinin sıradan çıxarılması (qurğular, əhəmiyyətli informasiya daşıyıcıları, əməkdaşlardan bəziləri və s.);

2.Hesablama sisteminin funksiya yerinə yetirməsini təmin edən altsistemlərin siradan çıxarılması və ya şəbəkədən ayrılması (elektrik qidalanması, soyuducu qurğular və hava dəyişmə qurğuları, rabitə xətləri və s.);

3.Sistemin işdən çıxarılmasına təsir edən faktorlar (qurğuların və proqramların iş rejiminin dəyişdirilməsi, əməkdaşların qəsdən işləməməsini və ya işlərini pozmaq yolu ilə işə mane olmaq, işçiləri nümayişə çağırmaq, sistemin işləməsinə maneçilik edəcək aktiv radiomaniənin yaradılmasına şərait yaratmaq və s.);

4.Təhlükəsizliyə cavabdehlik daşıyan əməkdaşlardan, həmçinin inzabati işçilər arasından könüllüləri seçmək;

5.Müəyyən işləri görmək üçün məsuliyyət daşıyan, müvəkkil seçilmiş istifadəçilərə hədə-qorxu gəlməklə və ya pulla ələ almaqla bəzi əməliyyatları yerinə yetirməyə cəlb etmək;

6.Xəlvəti qulaq asmaq üçün yararlı olan qurğulardan, uzaq məsafədən şəkil çəkməyə imkan verən fotoaparatlardan, video çəkilişlərdən və s. istifadə etmək;

7.Rabitə xəttində elektromaqnit, akustik və digər şüa buraxan qurğulardan, həmçinin aktiv şüalanma yaradan köməkçi texniki qurğulardan, informasiyanın təhlil olunmasında bilavasutə iştirak etməyən qurğulardan (telefon xəttindən, qida mənbəyindən, istilik sistemindən və buna bənzərlərdən) istifadə etmək;

8.Rabitə kanalı vasitəsilə ötürülən məlumatların əldə olunması, onların təhlili, avtorizasiya edilmiş istifadəçilərin sistemə daxil olmasının imitasiya edilməsinin təşkili;

9.İnformasiya daşıyıcılarının oğurlanması;

10.İnformasiya daşıyıcılarına yazılmış qiymətli informasiyanın icazəsiz surətinin alınması;

11.İstehsal tullantılarının (möhürü qopardılmış sənədlərin, əlyazmalarının, hesabdan silinmiş informasiya daşıyıcılarının və s.) oğurlanması;

12.***Operativ yaddaşda*** və ***xarici yaddaş*** qurğusunda saxlanılmış informasiyanın oxunması;

13.Əməliyyat sistemindən istifadə etməklə operativ yaddaşın müəyyən sahələrində qalmış informasiyanın oxunması, həmçinin asinxron rejimdə əməliyyat sisteminin çatışmazlıqlarından istifadə etməklə informasiyanın oxunması;

14.Parolların və digər məhdud istifadəyə malik ***rekvizitlərin*** qeyri-qanuni alınması (məsələn, istifadəçinin səhlənkarlığından istifadə etməklə, sistemin interfeysini imitasiya etməklə, sistemin interfeysini seçim etməklə, casus yönümlü işçiləri ələ almaqla və s.) və şirkətdə onlardan heç bir işçinin şübhələnməməsi üçün özlərini maskalaması;

15.Unikal fiziki xarakteristikaları olan istifadəçi terminallarından icazəsiz istifadə edilməsi (məsələn, şəbəkədəki işçi stansiyanın nömrəsindən, fiziki ünvandan, rabitə sistemindəki ünvandan, kodlama aparat bloklarından və s.);

16.Kriptoqrafiyadan istifadə etməklə şifrələnmiş informasiyanın açıqlanması;

17.Rabitə xəttinə qeyri-qanuni qoşulmaqla informasiyanı təhlil etməklə lazım olan "sətirlərarası" məlumatlardan bəhrələnmək və bu məqsədlə bu sahənin sahibinin adından istifadə etmək;

18.Şəbəkədən qanuni istifadə edən işçiyə mane olmaq üçün qeyri-qanuni yolla onu şəbəkədən fiziki şəkildə ayırmaqla lazım olan informasiyanı əldə etdikdən sonra həmin informasiyanı mənasız, yalanlardan ibarət olan informasiya ilə əvəz etmək.

Aparılmış tədqiqatlar göstərir ki, pisniyyətli işçilər öz əməllərini şirkət daxilində həyata keçirmək üçün öndə göztərilmiş yollardan ya birini seçir, ya da ki, onun üçün əlverişli olanlardan (bir neçəsindən) istifadə edirlər.

AÇIQLAMA: *Rekvizit* (latınca requisitum) sözü bizim dilimizə latın dilindən gəlmədir, "tələb edilən", "lazım olan" anlamını verir. Rekvizit sözü çoxmənalıdır və harada istifadə edilməsindən asılı olaraq mənasını dəyişir. Qədim zamanlarda rekvizit kəlməsi küçələrdə təşkil edilmiş tamaşaların gedişi zamanı aktyorlara lazım olan butafor əşyalarını (səhnə ləvazimatı hazırlayan usta butafor adlanır) işarə etmək üçün istifadə olunurdu. İndiki zamanda kino çəkilən meydançalarda istifadə edilən ləvazımatları da rekvizit adlandırırlar.

Köhnə sənəd qüvvəsini itirdikdə onun yerinə yeni

sənəd hazırlandıqda həyata keçirilən əməliyyatı rekvizit adlandırırlar.

AÇIQLAMA: *Opedrativ yaddaş* (ingiliscə Random Access Memory, RAM, ixtiyari əlçatanlıqlı yaddaş, Operativ Yaddaş Qurğusu, Operativka, kompüterin enerjidən asılı olan yaddaşı). İstifadəçi kompüterlə işləyən zaman yerinə yetirilən maşın əmrləri (proqramlar) operativ yaddaşda saxlanılır. Bununla yanaşı operativ yaddaşda prosessor tərəfindən təhlil edilmiş giriş, çıxış və aralıq verilənlərdə saxlanılır.

Ümumi halda operativ yaddaş əməliyyat sisteminin proqramlarından və verilənlərindən, istifadəçinin buraxılmış tətbiqi proqramlarından ibarətdir. Odur ki, operativ yaddaşın tutumu eyni zamanda əməliyyat sisteminin rəhbərliyi ilə kompüterin həll etdiyi məsələlərin sayından asılıdır.

OYQ ya ayrıca modul kimi hazırlanır, ya da ki, prosessor ilə bir kristalda yerləşdirilir.

1834-cü ildə Çarlz Bebbic analıtık maşının yaradılması ilə məşğul olurdu. Maşının əsas hissələrindən birini alim "anbar" (store) adlandırır. "Avbar"ın funksiyası aralıq nəticələri yadda saxlamaq idi. Ö dövrdə hazırlanan "anbar" mexaniki qurğudan ibarət idi. Dişli çarxların və vərdənənin (barabanın) fırlanması nəticəsində alınmış nəticə yadda saxlanılırdı.

Yaddaş qurğusunu aşağıdakı texniki elementlərdən istifadə edilməklə yaratmaq mümkündür:

Elektromaqnit relelər əsasında;

Akustik saxlama xəttindən istifadə etməklə;

Elektron-şüa borusundan istifadə etməklə;

Maqnit barabanlarından istifadə etməklə;

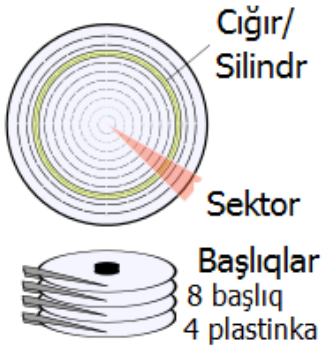
Maqnit nüvələrindən istifadə etməklə;
Mikrosxemlərdən istifadə etməklə və s.
İki növ operativ yaddaşdan istifadə olunur:
Statik (ARAM) – triggerlər yığımından istifadə etməklə;
Dinamik (DRAM) – kondensatorlar yığımından istifadə etməklə.

Operativ yaddaş qurğusu

1973-cü ildə IBM firması yeni texnologiya ilə 16 Kbayt informasiyanı saxlayan ilk sərt diski istehsala buraxır. Disk hər biri 30 sektora bölünən 30 silindrdən ibarət olduğundan, onun şərti işarəsi 30/30 kimi qəbul edilir. Bu işarə 30/30 kalibrinə malik, alman istehsalı olan Vinçester tipli məşhur avtomatik tüfəngə anoloji olduğu üçün ona "Vinçester" adı da verilir. O vaxtdan bəri sərt disklərin konfiqurasiyası xeyli dəyişmiş, tutumu, etibarlılığı və işləmə sürəti kəskin artmışdır. Lakin fərdi kompüterlərdə sərt diskin əvvəlki adı indi də istifadə edilməkdədir.

İlk sərt disklərin seriya şəkilində istehsalı 1979-cu ildə Seagate firması tərəfindən həyata keçirilmişdir. Beş düymlü ST-506 diskinin tutumu 6 Mbayta bərabər idi. 1979-cu ildə istehsal olunan sərt disk belə disklərin istehsalının təməlini

qoydu. Müasir vinçester yığıcıları bir ox üzərində quraşdırılmış maqnit disklər paketindən ibarətdir. Diskin hazırlanması üçün alüminium lövhədən, şüşə və keramikadan və onun üzərinə xüsusi texnologiya ilə yapışdırılmış (oturdulmuş) yüksək keyfiyyətli ferromaqnit qatdan istifadə olunur. Diskin üzərinə qat yapışdırılandan sonra onu firmada xüsusi texnologiya ilə emal edirlər. Emal olunmuş diskləri bir paketə yığıb otürücüyə quraşdırılmış oxa bərkidirlər (adətən bir paketdə 2-dən 12-yə qədər disk olur).



Xarici yaddaş qurğusunun işləmə sxemi

Vinçesterin ümumi görünüşü

Bir versiyaya görə diskə "vinçester" adını IBM firmasında layihə rəhbəri işləyən Kennet Hoton (ingiliscə Kenneth E. Haughton) vermişdir (bu 1973-cü ilə təsadüf edir). 1973-cü ildə sərt diskin 3340 modeli istehsal olunur.

Digər versiyaya görə diskin "Vinçester" adını alması Winchester Repeating Arms Company tərəfindən istehsal olunan tüfəng patronunun adı ilə bağlıdır. Amerikada istehsal olunan patron kiçik kalibirli tüfənglərdə istifadə edilirdi.

Avropada və ABŞ-da "Vinçester" adından geniş istifadə 1990-cı illərə təsadüf edir.

Xarici yaddaş qurğusunun daxili görünüşü

İNFORMASİYANIN AZALMA KANALLARI

Şirkətlər arasında şirkətin mənafeyini qoruyan danışıqların aparılması zamanı informasiyanın ötürülməsi və təhlil edilməsi üçün texniki vasitələrdən istifadə edilir və bu zaman istifadə olunan informasiyanın təhlükəsizlik qorxusu və informasiyanın kanallar vasitəsilə sızması halları yaranır.

Bunlar aşağıdakı hallarda mümkündür:

- İnformasiya xarakterli dəyərli danışıqların akustik qurğularla şüalandırılması;
- Nəzarət zonasından kanara çıxan, mikrofon effektinin hesabına informasiya xarakterli siqnalın akustik siqnaldan elektrik siqnalına çevrilməsi, naqillər və xəttlər böyunca yayılması (nəzarət zonası dedikdə ərazi, bina, binanın bir hissəsi nəzərdə tutulur və bu yerlərə nəzarətdən kanar, buraxılış vəsiqəsi olmayan şəxslərin və ya nəqliyyat vasitələrinin daxil olması başa düşülür);
- Titrəyişli akustik siqnalların mühafizə olunan sahələrə birbaşa təsir göstərməsi;
- Avtomatlaşdırılmış sistemlərdə istifadə edilən informasiyaya, həmçinin hamı tərəfindən istifadə olunan informasiya şəbəkələrinə qeyri-qanunu daxil olma və qeyri-qanuni münasibətin bəslənməsi;
- İnformasiyanın konfidensiallığını, tamlığını və əlçatanlığını, texniki vasitələrin iş qabiliyyətini, xüsusi tətbiq edilən proqram vasitələrinin, həmçinin informasiyanın müdafiə vasitələrinin işini pozmaq üçün informasiya sistemlərinin proqram və ya texniki vasitələrinə təsirin göstərilməsi;
- Konfidensial informasiyanı təhlil edən texniki vasitələr tərəfindən informasiya xarakterli siqnalın əlavə elektromaqnit şüalanması;
- Nəzarət zonasından kanara çıxan, texniki vasitələrin köməyilə elektrik qidalanma dövrəsində və rabitə xəttlərində təhlil olunan informasiya xarakterli siqnala çevrilməsi;
- Texniki vasitələrin tərkibinə daxil olan, müxtəlif qeneratorların işləməsi zamanı əmələ gələn (və ya texniki vasitələrin elementlərində yaranan parazit qenerasiyanın

nəticəsində əmələ gələn) informasiya xarakterli siqnalın modulyasıya olunması nəticəsində radioşüalanması;

- Texniki vasitələrin tətbiqi nəticəsində əmələ gələn radioşüalanma (və ya elektrik siqnalı), mühafizə edilən binalarda quraşdırılmış xüsusi elektron qurğular vasitəsilə danışıq informasiyasının tutulması, informasiya xarakterli siqnalın modulyasıya olunması;
- Texniki vasitələrin tətbiqi nəticəsində əmələ gələn radioşüalanmanın (və ya elektrik siqnalının) tutulması, rabitə kanalına qoşulmuş texniki vasitələrin köməyilə informasiyanın təhlil edilməsi;
- Telefon və radio danışıqlarına qulaq asılması;
- Kompüterin ekranında və digər əks etdirici qurğularda informasiyaya baxışın keçirilməsi, kağız üzərində olan və ya digər informasiya daşıycılarına yazılmış informasiyaya optik cihazların köməyilə nəzarətin həyata keçirilməsi;
- İnformasiya daşıyıcılarına və digər texniki qurğulara yazılmış informasiyanın oğurlanması;
- İnformasiyanın tutulması və ya texniki qurğulardan istifadə etməklə informasiyanın oxunulmasına maneçiliyin həyata keçirilməsi;
- Nəzarət zonasına yaxın nəqliyyat vasitələrindən istifadənin məhdudlaşdırılması;
- Şirkətlərə məxsus müştərək binalardan istifadə edilməsinin məqsədəuyğun olmaması;
- Şirkətin (müəssisənin) binalarına kanar şəxslərin daxil olması;
- Avtomatlaşdırılmış sistemlərdə, həmçinin avtomatlaşdırılmış texniki vasitələrdə istifadə olunan informasiyanın qeyri-qanuni yolla əldə edilməsi.

POZUCUNUN QEYRİFORMAL MODELİ

Pozucu – səhv olaraq qadağan olunmuş əməliyyatı yerinə yetirməyə cəhd edən, bilmərəkdən və ya düşünülmüş şəkildə, pis niyyətlə (və ya tamah məqsədi ilə) və yaxud həzz almaq üçün (özünü kiməsə göstərmək xatirinə) və s. bu hərəkətləri yerinə yetirmək üçün müxtəlif imkanlar axtaran, üsullar və vasitələrdən istifadə edən şəxsdir.

Bədəməl – düşünülmüş şəkildə tamah məqsədi ilə pozuculuq hərəkətlərini yerinə yetirən şəxsdir.

Avtomatlaşdırılmış informasiya sistemlərində informasiya təhlükəsizliyinin ehtimal olunan mənbəyini müəyyən etmək üçün və informasiyaya ediləcək hədələrin məsuliyyət dərəcəsini aydınlaşdırmaqdan ötrü *pozucunun qeyriformal modeli qurulur*. Model pozucunun potensial imkanlarını və nəyə qadir olduğunu, görəcəyi işin vaxtını və yerini, vuracağı (yetirəcəyi) ziyan üçün istifadə edəcəyi avadanlıqları və s. əks etdirir.

Pozucunun modeli özünə aşağıdakı fərziyyələri daxil edir:

1.*Pozucunun mənsub olduğu şəxslər*: Sistem istifadəçiləri, xidmətedici personallar, avtomatlaşdırılmış informasiya sistemlərinin yaradıcıları, təhlükəsizlik xidmətinin əməkdaşları, rəhbərlər – bunları şirkət daxili pozucular adlandırmaq olar; müştərilər, seyrçilər (görüşə gələnlər), rəqiblər, təsadüfi adamlar – bunları şirkətdən xaric pozucular adlandırmaq olar.

2.*Pozuculuq işlərini yerinə yetirdiyi anlara görə.* Əsas üç dəlil (səbəb, motiv) nəzərə alınır: *məsuliyyətsizlik*, *tamahkarlıq* və *özündənrazı*. Məsuliyyətsizlik olanda şəxsin pis niyyəti olmadan ehtiyatsızlıq və ya səriştəsizlik etməsi nəticəsində pozuculuq işləri həyata keçir. Şəxs (pozucu) özündənrazı olanda güya ki, avtomatlaşdırılmış idarəetmə sistemindən daha yaxşı müəyyən işləri özü həyata keçirəcək deyə sistemin işini

pozur və ya sistemə daxil olaraq özünü həmkarlarının gözü qarşısında "istifadəçi – sistemə qarşı çıxacaq" şəxs kimi göstərir. Tamahkarlıq halı ən qorxuludur, çünki şəxs məqsədyönlü sistemin işinə qarışır, məkrli və düşünülməmiş hərəkətlərə yol verir.

3.*Tutarlı səviyyədə olan pozucu*: avtomatlaşdırılmış informasiya sistemləri səviyyəsində istifadəçi, avtomatlaşdırılmış informasiya sistemləri səviyyəsində inzibatçı, informasiya təhlükəsizliyi sahəsində mütəxəssis səviyyəsində.

4.*Müəyyən üsullardan və avadanlıqlardan istifadə edə biləcək səviyyədə olan pozucunun imkanları:* cəsusluq üsullarından istifadə etməklə, ştat işçilərinin lazımı verilənlərə qeyri-qanuni yolla daxil olmaq imkanı əldə edilməsi, passiv avadanlıqlardan istifadə etməklə verilənlərin əldə olunması, aktiv avadanlıqlardan istifadə etməklə verilənlərin əldə edilməsi və modifikasiya olunması.

5.*Fəaliyyət vaxtına görə:* avtomatlaşdırılmış informasiya sistemlərinin ştat funksiyası yerinə yetirdiyi zaman ərzində, avtomatlaşdırılmış informasiya sistemlərinin boş dayanma vaxtına görə, istənilən vaxt ərzində.

6.*Fəaliyyət göstərmə yerinə görə:* təşkilatın nəzarətdə saxlanılan ərazisinə daxil olmadan, təşkilatın nəzarətdə saxlanılan ərazisinə daxil olmaqla, istifadəçinin iş yerinə görə, avtomatlaşdırılmış informasiya sistemlərinin baza verilənlərinə daxil olmaqla, avtomatlaşdırılmış informasiya sistemlərinin altsistemlərinə daxil olmaqla.

Pozucunun qeyriformal modeli avtomatlaşdırılmış informasiya sistemlərinin tətqid edilməsi əsasında qurulur. Bu zaman sahənin xüsusiyyəti və verilənlərin təhlil edilməsi üçün istifadə olunan texnologiya nəzərə alınmalıdır. Pozucunun mümkün konkret xarakteristikasının müəyyən olunması

müəyyən dərəcədə subyektiv prosesdir. Proses adətən özündə mümkün pozucuların simasını, yəni öndə göstərilən simalarını cəmləşdirir. Pozucunun qeyriformal modelinin qurulması informasiya təhlükəsizliyinin baş vermə səbəblərini aydınlaşdırmağa imkan verir. Bununla yanaşı modeldən istifadə etməklə pozulmanın cari növlərinin aradan qaldırılması üçün müdafiə sisteminin təkmilləşdirilməsini həyata keçirmək mümkün olur.

DÖVLƏT SƏVİYYƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

İnformasiya təhlükəsizliyi sahəsində hazırlanmış doktrina (elmi, fəlsəfi və ya siyasi nəzəriyyə) əsasında Rusiya Federasiyasının normativ-hüquqi aktı 9 sentyabr 2000-ci ildə prezidentin qərarı ilə təsdiq edilmişdir.

İnformasiya təhlükəsizliyi doktrinası özündə qoyulmuş məqsədə və məsələlərə rəsmi baxışı, Rusiya Federasiyasının informasiya təhlükəsizliyi təminatının və prinsiplərinin əsas istiqamətlərini birləşdirir. Bu baxış Rusiya Federasiyasının informasiya təhlükəsizliyi baxımından milli Konsepsiyasını informasiya sahəsində inkişaf etdirdi.

Konsepsiya aşağıdakıların həyata keçirilməsinə qulluq edir:

- Rusiay Federasiyasında informasiyanın təhlükəsizliyi sahəsində Dövlət siyasətinin formalaşmasının təmin edilməsi;
- Rusiya Federasiyasında informasiya təhlükəsizliyi sahəsində təşkilatı, elmi-texniki, metodiki, hüquqi baxımdan təkmilləşdirmə təkliflərinin hazırlanması;

- Rusiya Federasiyasında informasiya təhlükəsizliyi sahəsində məqsədli proqram təminatın hazırlanması.

Rusiya Federasiyasında informasiya təhlükəsizliyi sahəsində dövlətin, hökumətin və şəxsiyyətlərin maraqları toplumunu müəyyən edən, informasiya mühitində milli maraqlar baxımından təhlükəsizliyin təmin edən doktirinanın qəbulu həyata keçirilir.

Rusiya Federasiyasında informasiya təhlükəsizliyi sahəsində qəbul edilmiş doktirina aşağıdakıları özündə təzahür edir:

1.İnformasiya mühitində milli maraqlar və onların təmin edilməsi;

2.Dövlət siyasətinin bu sahədə dəstəklənməsi;

3.Müasir informasiya texnologiyalarının, dövlətdaxili sənayenin, telekommunikasiya vasitələrinin və rabitənin, hazırlanmış məhsulların dünya bazalarına çıxarılmasının və s. inkişaf etdirilməsı;

4.Rusiya sərhədləri daxilində informasiya təhlükəsizliyinin təmin edilməsi;

5.İnformasiya təhlikəsizliyinin təmin edilməsi üçün ümumi metodların hazırlanması;

6.İctimai həyatda, müxtəlif sahələrdə informasiya təhlükəsizliyinin xüsusiyyətlərini nəzərə almaqla bu sahənin təminatının həyata keçirilməsi;

7.Müxtəlif sahələrdə, məsələn, kredit-finans sistemlərində, dövlət statistika sahəsində, icra hakimiyyətlərində, iqtisdadiyyat sahəsində və s. informasiya təhlükəsizliyinin təmin edilməsi;

8.Beynəlxalq əməkdaşlıq sahəsində, informasiyanın toplanması, saxlanması, təhlili və müəyyən sahələrdə istifadə edilməsi sahəsində, intellektual kartlardan istifadə olunmaqla

ödəmənin həyata keçirilməsi sahələrində və başqa yerlərdə informasiya təhlükəsizliyinin həyata keçirilməsi və s.

MÜDAFİƏ OLUNAN AVTOMATLAŞDIRILMIŞ İNFORMASİYA SİSTEMLƏRİNİN QURULMA PRİNSİPLƏRİ

İNFORMASİYA TƏHLÜKƏSİZLİYİ SİSTEMLƏRİNİN MƏSƏLƏLƏRİ

İnformasiya təhlükəsizlinin hədələrə qarşı müqavimət göstərməsi məqsədilə müdafiə oluanan AİS-nin informasiya təhlükəsizliyi sisteminin təmin edilməsi üçün aşağıdakı məsələlər həll edilməlidir:

1.Avtomatlaşdırılmış informasiya sistemləri resurslarına istifadəçi əlçatanlığının idarə edilməsi.

2.Rabitə kanalı vasitəsilə ötürülən verilənlərin müdafiə edilməsi.

3.Sistemdə baş verənlərlə və sistemin təhlükəsizliyi ilə birbaşa əlaqəsi olan, sistemdə baş vermiş bütün hadisələr haqqında məlumatların, təhlillərin, informasiyanın yığılmasının və saxlanılmasının qeyd olunması.

4.Müdiriyyət tərəfindən sistem istifadəçisinin işinə nəzarətin yerinə yetirilməsi ilə yanaşı müdiriyyəti operativ şəkildə qeyri-qanuni sistemin resurslarına daxil olmaq istəyənlər barədə məlumatlandırmaq.

5.Potensial zərərli proqramların nəzarətsizlik üzündən sistemə tətbiq olunmasının qarşısını almaq məqsədilə qapalı mühitin yoxlanılmış proqram təminatı ilə təmin edilməsini

həyata keçirmək. Bununla yanaşı sistemə daxil ola biləcək kompüter virusları ilə mübarizə aparılmasını yerinə yetirmək.

6.Müdafiə sistemi resurslarının tamlığına nail olmaq üçün onları dəstəkləməklə yanaşı onlara nəzarəti həyata keçirmək.

Avtomatlaşdırılmış informasiya sistemlərində (AİS) daxili və xarici təhlükəsizliyi fərqləndirmək lazımdır. *Xarici təhlükəsizlik* sistemə təsir edə biləcək fəlakətlərlə (yanğın, zəlzələ və s.) və sistemə kənardan daxil olan bədniyyətlilərin əməlləri ilə bağlıdır. *Daxili təhlükəsizlik* sistemin qanuni istifadəçiləri və xidmətedici personalın fəaliyyətində etibarlı və əlverişli mexanizmlərin tətbiqi ilə əlaqədardır.

TƏHLÜKƏSİZLİK HƏDƏLƏRİNƏ QARŞI TƏDBİRLƏR

Kompüter təhlikəsizliyinin təmin olunmasına görə yerinə yetirilən tədbirlər aşağıdakı kimi bölünür: qanunvericiliyə (hüquqi) uyğun, inzibati (təşkilatı), proqram-texniki və prosedur.

Qanunvericiliyə uyğun müdafiə tədbirlərinə aiddir: fəaliyyət göstərən normativ-hüquqi aktlar, informasiya ilə rəftarın qaydaya (reqlamentə) salınması, informasiyanın təhlil və istifadə edilməsi üçün təhkim olunmuş iştirakçıların hüquqlarının qorunması və göstərilən tədbirlərin yerinə yetirilməsinə maneçilik edənlərin və qoyulmuş qaydaların (əsasəndə beynəlxalq) pozulmasına cəhd edənlərin məsuliyyətə cəlb edilməsi. Bu standartların içərisində ən çox seçiləni "Narıncı kitab"dır. Bununla yanaşı X.800 və "Common Criteria for IT Security Evaluation" (İnformasiya texnologiyaları təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri) satandartlarından da istifadə olunur.

"*Narıncı kitab*" ən böyük baza standartıdır. Standartda əsas anlayışlar, təhlükəsizlik servisi, informasiya sistemlərinin təsnifat üsulları və informasiya sistemlərinə təhlükəsizlik baxımından tələblər irəli sürülür.

X.800 təqdimatı əsasən şəbəkə konfiqurasiyasının müdafiə edilməsi suallarını özündə əks etdirir. Standart təhlükəsizliyin servislər toplusunun və istifadə mexanizminin inkişafı mərhələlərini təqdim edir.

"*İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri*" özündə 11 sinif, 66 ailə və 135 funksional təşkiledicini birləşdirir.

Siniflər aşağıdakı adları əks etdirirlər:

Birinci qrup təhlükəsizliyin elementar servisini müəyyən edir:

1.FAU – audit, təhlükəsizlik (servisə edilən tələblər, protokollaşdırma və audit);

2.FIA – identifikasiya və autentifikasiya;

3.FRU – resurslardan istifadə (imtinaya etibarlılığın təmin olunması);

İkinci qrup elementar bazaya əsaslanaraq servisin törəməsini müəyyən edir:

4.FCO – rabitə (göndərənin-qəbul edənin kommunikasiya təhlükəsizliyi);

5.FPR – qeyri-məcburi;

6.FDR – istifadəçiyə aid verilənlərin mühafizəsi;

7.FPT – qiymətləndirmə obyektinin təhlükəsizlik funksiyasının mühafizəsi;

Üçüncü qrup qiymətləndirmə obyektinin infrastrukturunu müəyyən edir:

8.FCS – kriptoqrafik dəstək (kriptoaçarların və kripto-əməliyyatların idarə edilməsinə xidmət edir);

9.FMT – təhlükəsizliyi idarə edir;

10.FTA - qiymətləndirmə obyektinə daxil ola bilir (istifadəçinin iş seansını idarə edir);

11.FTP – etibarlı marşrut/kanal;

Bunlardan başqa "İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri" özündə müasir texnologiyalardan istifadə etməklə hansı formada təhlükəsizliyin əldə olunması haqqında məlumatı əks etdirir. Bununla yanaşı "Ümumi kriterilər" müdafiə sistemini sertifikatlaşdırmağa da imkan verir.

2006-cı ilin payızında Rusiyada milli standart qəbul olundu, standart beynəlxalq ISO 17799 standartını dəstəkləyirdi.

İnzibatı müdafiə tədbirləri dedikdə AİS-nin müəyyən funksiyanı yerinə yetirmə proseslərinin reqlamentə uyğun qurulması, personalın fəaliyyəti, istifadəçinin sistemlə qarşılıqlı əlaqəsinin yaradılması, əhəmiyyətli dərəcədə təhlükəsizlik hədələrinin realizasiyasının ləğvi başa düşülür.

İnzibati müdafiə tədbirlərinə aşağıdakılar aiddir:

1.Sistem personalının hazırlığı və seçilməsi;

2.Buraxılış rejiminin və mühafizənin təşkili;

3.İnformasiya daşıyıcılarından istifadə edilməsi və lazımsız sənədlərin ləğv olunması, onların saxlanılması, hesaba alınmasının təşkili;

4.Daxilolmanı aradan götürməklə rekvizitlərin paylanması (parolun, şifrli açarın və s.);

Müdafiənin həyata keçirilməsində əsas rolu inzibati tədbirlər oynayır, bura informasiya təhlükəsizliyi sahəsində görülən işlərin proqramlarının formalaşdırılması və bu işlərin yerinə yetirilməsinin təmin edilməsidir. Formalaşdırılmış proqramların əsasını təhlükəsizliyin təmin olunma siyasəti təşkil

edir. Siyasətə idarəetmə prinsiplərinin toplumu, qanunlar, təhlükəsizlik sahəsində həyata keçirilən praktiki tədbirlərin prosedurları və s. daxildir. Bunları rəhbər tutmaqla təşkilat öz fəaliyyətini tutarlı səviyyədə yerinə yetirir.

Təhlükəsizlik siyasəti özündə aşağıdakıları müəyyənləşdirir:

- Hansı verilənləri və onları hansı dərəcədə müdafiə etmək;
- İnformasiya aspektində təşkilata kim və necə ziyan vurur;
- Hansı həddə kimi təhlükəsizliyin azaldılması mümkündür;
- Təhlükəsizliyin azaldılmasında hansı üsullardan istifadə olunur və azaldılma riski nə qədərdir.

Praktiki baxımdan təhlükəsizliyi üç səviyyədə həyata keçirmək mümkündür:

- Yuxarı;
- Orta;
- Aşağı.

Yuxarı səviyyəyə rəhbərlik tərəfindən ümumi xarakterli qəraralar aiddir.

Orta səviyyəyə təşkilatda istifadə edilən (ekspluatasiya edilən) müxtəlif sistemlərin informasiya təhlükəsizliyinə aid olan suallar aiddir.

Aşağı səviyyəyə konkret servislər və onların detalları (hissələri) aiddir. Bir çox hallarda aşağı səviyyədə təhlükəsizlik siyasətinə nail olmaq üçün bütün servislər öz səviyyərində realizə edilirlər.

Prosedur səviyyəsində həyata keçirilən tədbirlər avtomatlaşdırılmış informasiya sistemlərinin işlədiyi bütün dövr ərzində yerinə yetirilən ayrı-ayrı tədbirlər məcmusu kimi

götürülə bilər. Bu tip tədbirlər texniki avadanlıqlara deyil, insanlara yönəldilmişdir və aşağıdakı hissələrə bölünürlər:

- Personalın idarə edilməsi;
- Fiziki müdafiə;
- İş qabiliyyətinin saxlanılması;
- Təhlükəsizlik rejiminin pozulmasına reaksiyanın verilməsi;
- Planlaşdırılmış işlərin bərpa edilməsi.

Mühafizənin proqram-texniki təminatı xüsusi aparat vasitələrinin istifadə olunmasına və avtomatlaşdırılmış informasiya sistemlərinin tərkibinə daxil olan proqram təminatına əsaslanır.

Mühafizənin proqram-texniki təminatı müdafiə funksiyasını: şifrələməni, autentifikasiyanı, resurslara daxil olma məhdudiyyətini, məlumatların qeydiyyatını, virusların axtarılmasını və ləğv olunmasını və başqalarını yerinə yetirir. Bu barədə dərsliyin növbəti fəsillərində ətraflı məlumat veriləcək.

AVTOMATLAŞDIRILMIŞ İNFORMASİYA SİTEMLƏRİNİN MÜDAFİƏ SİSTEMİNİN QURULMASININ ƏSAS PRİNSİPLƏRİ

1.*Müdafiə mexanizminin sadəliyi*. Müdafiə vasitələrindən istifadə olunması istifadəçidən xüsusi hazırlıq tələb etməməli və ya istifadəçini əlavə zəhmətə qatmamalıdır. Onlar intiutiv başa düşülən və istifadəyə sadə olmalıdır.

2.*Sistemlik*. Sistemin yaradılması və onun istimara buraxılması zamanı bütün əlaqələri nəzərə almaq lazımdır. Bununla yanaşı təhlükəsizliyin təmin edilməsi üçün əhəmiyyətli sayılan qarşılıqlı fəaliyyət və zamana görə elementlərin

dəyişməsi, şərtlər və faktorlar da hesaba alınmalıdır. Digər tərəfdən avtomatlaşdırılmış informasiya sistemlərinin bütün zəif yerləri (hissələri) də nəzərə alınmalıdır ki, mümkün hücumların, yeni təhlükəsizlik hədələrinin yaranmasının səbəbləri və yaranma yerləri müəyyən edilsin.

3.*Komplektlik*. Müdafiə sisteminin tamlığının qurulması zamanı müxtəlif xüsusiyyətli vasitələrin istifadə edilməsi razılaşma əsasında olmalıdır, çünki bu vasitələr kanalların zəif birləşmə nöqtələrində yarana biləcək bütün mümkün hədələrin qarşısının alınmasına kömək edməlidirlər. Bu baxımdan eşalonlaşdırılmış müdafiə sisteminin qurulması məqsəduyğun hesab edilir, çünki belə yanaşma müxtəlif səviyyələrdə (xarici səviyyə - fiziki vasitələr, təşkilatı və hüquqi tədbirlər, əməliyyat sistemlərinin səviyyələri, tətbiqi səviyyə) kompleks təhlükəsizliyin təmin olunmasına zəmin yaradır.

4.*Arasıkəsilməzlik*. Avtomatlaşdırılmış informasiya sistemlərinin informasiya təhlükəsizliyinin təmin edilməsi üçün həyata keçirilən tədbirlər sistemin fəaliyyət göstərdiyi bütün dövr ərzində həyata keçməlidir, yəni layihələndirmədən başlamış istismara buraxılan anına kimi. Bu zaman ən yaxşı nəticə sistemin yaradılması ilə yanaşı onun avtomatlaşdırılmış informasiya sisteminin müdafiə edilmə məsələlərinin də parallel həyata keçirilməsi baş verir. Bununla yanaşı çalışılmalıdır ki, sistem işləyən zaman onun işində hədələr nəticəsində fasilələr (arakəsmələr) olmasın.

5.*Düşünülmüş kafilik*. İnformasiya təhlükəsizliyinin əsas prinsiplərinin birində belə bir anlam var: mütləq formada etibarlı müdafiə yaratmaq mümkün deyil. Belə alınır ki, istənilən pisfikirli insan müəyyən məbləğdə para xərcləməklə yaradılmış mürəkkəb mühafizə mexanizminin öhdəsindən gələ bilər. Müdafiə sistemi onda etibarlı sayılır ki, bədniyyətli insan

onu məhf etmək üçün xərclədiyi paranın məbləği sistem işləyərkən verəcəyi gəlirdən qat-qat yüksək olsun. Bəzən bu üsuldan da istifadə edilir: sistemin müdafiəsinə çəkilən xərc informasiyanın təhlükəsizliyinə çəkilən xərcdən artıq olmamalıdır.

6.*Uyuşqanlıq*. Sistemin mühafizəsi xarici şərtlərin dəyişməsinə adaptasiya (öyrəşmə) olunma imkanına malik olmalıdır.

7.*Müdafiə mexanizminin və alqoritmlərinin açıqlığı*. Sistem müdafiə üçün nəzərdə tutulmuş bütün işlərin pisniyyətli şəxsə məlum olacağını nəzərə almaqla onun həyata keçirə biləcəyi işlərin bütün detallarını araşdırıb öyrənməklə etibarlı müdafiəni təmin etməlidir.

TƏHLÜKƏSİZLİK MODELLƏRİ

TƏHLÜKƏSİZLİK MODELİNİN TƏYİNATI VƏ ANLAYIŞI

Sistemin formal şəkildə hazırlanmasında əsas rolu təhlükəsizlik modeli adlanan (daxilolmaların idarə edilməsi modeli, təhlükəsizliyin siyasi modeli) model oynayır. Modelin məqsədi cari sistemdə təhlükəsizlik baxımından qoyulmuş tələblərin ifadə edilməsidir. Model sistemə daxil olan informasiya axınını və informasiyaya əlçatanlığın idarə edilmə qanunlarını müəyyən edir.

Model sistemin xüsusiyyətlərini təhlil etməyə imkan verir. Öndə qeyd edildiyi kimi model formal olduğu üçün sistemin müxtəlif təhlükəsizlik xüsusiyyətlərini sübut etməyə şərait yaradır.

Təhlükəsizliyin təmin olunmasında istifadə olunan model bu xüsusiyyətlərə malik olmalıdır: *abstraktlıq*, *sadəlik* və *adekvatlıq*.

AÇIQLAMA: *Adekvatlıq* – analoji hallarda baş verən eyni hərəkətlərin (rəftarın, əməlin) yerinə yetirilməsidir.

İnformasiya təhlükəsizliyi modelində istifadə olunan əlçatanlığa müəyyən məhdudiyyətlər də qoyulur və bu məhdudiyyətlər Rusiya Federasiyası nəzdində fəaliyyət göstərən Dövlər Texniki Komissiyası tərəfindən hazırlanmış "İnformasiyaya qeyriqanuni əlçatanlığın müdafiə edilməsi" sənədidir.

Bura əsasən aşağıdakılar aiddir:

İnformasiyaya əlçatanlıq – informasiya ilə tanışlıq, onun təhlil olunması, əsasəndə surətinin alınması, informasiyanın modifikasiya və ya ləğv edilməsi;

Əlçatanlığın həcmi – avtomatlaşdırılmış sistemlərdə informasiya əlçatanlığın məhdudlaşdırılmasını müəyyənləşdirən informasiya resursları vahidi;

Əlçatanlığın subyekti – fəaliyyəti əlçatanlıq qanunları ilə tənzimlənən şəxs və ya proses;

Əlçatanlığın məhdudlaşdırılması qanunları – əlçatanlıq obyektlərinə subyektin daxil olmasını müəyyənləşdirən qanunlar toplumu.

DİSKRESİON ƏLÇATANLIQ MODELİ

Diskresion (öz mülahizəsinə görə hərəkət edən, istədiyi kimi hərəkət edən) model çərçivəsində subyektlərin (istifadəçi və ya əlavələr) obyektlərə (müxtəlif informasiya resursları – fayllara, əlavələrə, çıxış qurğularına və başqalarına) daxil olması nəzarətdə saxlanılır.

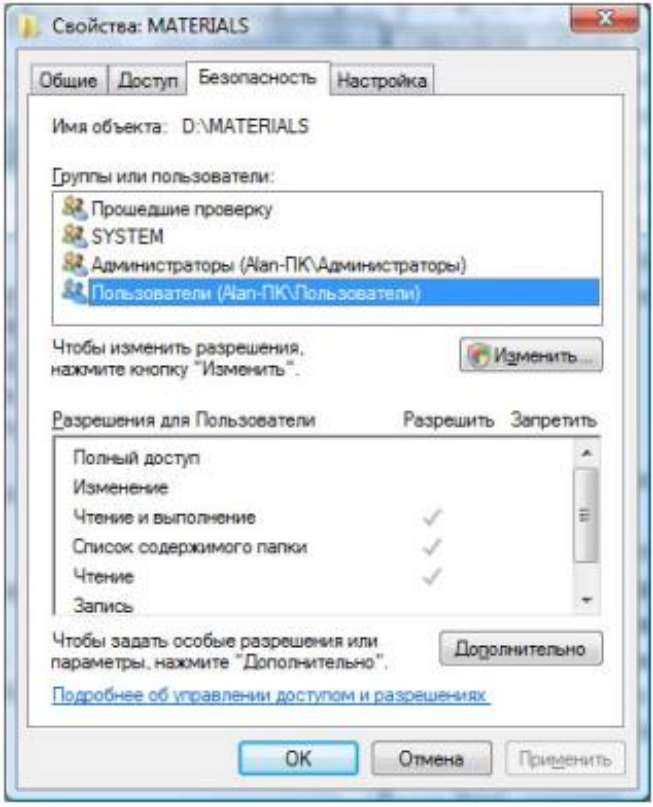
Hər bir obyektin özünə məxsus subyekt-sahibkarı vardır. Subyekt-sahibkar obyektə kimin daxil olma imkanının olmasını, həmçinin daxil olma imkanın genişləndirilməsi əməliyyatını müəyyən edir. Əlçatanlığın əsasını READ (Oxuma), WRITE (Yazma) və EXECUTE (yerinə yetirmə, ancaq proqram üçün) əməliyyatları təşkil edir. Deməli, diskresion modeldə hər bir subyekt-obyekt əlçatanlığı (daxil olma) üçün müxtəlif əlçatanlıq əməliyyatları toplumu təsis edilir.

Obyektə daxil olmanı sorğu etmək üçün sistem obyektə daxil ola biləcək subyekti siyahıdan axtarır, əgər subyekt

siyahıda varsa onda onun obyektə daxil olma yolu göstərilir. Əks halda əlçatanlıq nəzərə alınmır.

Klassik modellərdə əlçatanlıq "bağlı" hesab olunur. İndiki zamanda "açıq" sistemlərdən istifadə mümkündür, burada susma rejimində əlçatanlıq həyata keçirilir.

Belə model Windows və Linux əməliyyat sistemlərində yerinə yetirilir (şəkil 1.).



Şəkil 1. Windows Vista əməliyyat sistemində əlçatanlıq modeli

Diskresion modelin çatışmazlığı ondan ibarətdir ki, oxunmaq üçün nəzərdə tutulmuş subyekt bu əməliyyatı başqa subyektdə (obyektin sahibinin icazəsi olmadan) ötürə bilir. Deməli, informasiyanın ona daxil olmağa icazəsi olmayan subyekt tərəfindən əlçatan olmayacağına təminat yoxdur. Digər tərəfdən diskresion modeldə hər bir obyektə sahibkar müəyyən etmək mümkündür, yəni bir çox hallarda verilənlər ayrıca subyektlərə deyil, bütün sistemə məxsus olur.

BELLA-LAPADULA TƏHLÜKƏSİZLİK MODELİ

İndiki zamanda tanınmış təhlükəsizlik modellərindən biri – Bella-LaPadula modelidir (əlçatanlığın mandat idarəetmə modeli). Modeldə çoxlu sayda əlçatanlıq ilə bağlı olan anlamlar vardır, bunlara subyektin müəyyən edilməsi, obyektlər və əlçatanlıq əməliyyatları və bunların təsvir edilməsi üçün riyazi aparat aiddir. Model əsas iki təhlükəsizlik qaydaları ilə məşhurdur: birinci qayda oxumağa, ikinci qayda isə verilərlərin yazılmasına aiddir.

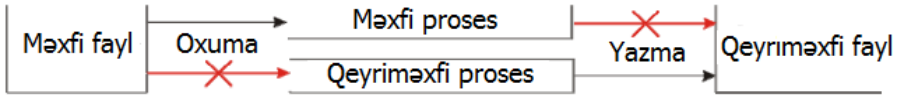
Nəzərə alaq ki, sistemdə iki verilən (fayl) mövcuddur: *məxfi* (*gizli*) və *qeyriməxfi* (*gizli olmayan*). Sistemdən istifadə edən istifadəçi də iki kateqoriyaya mənsubdur: gizli olmayan verilənlərə əlçatanlıq səviyyəsində (gizli olmayanlar) və gizli olan verilənlərə əlçatanlıq səviyyəsində (gizli olanlar).

1.Sadə təhlükəsizlik xüsusiyyətləri: qeyriməxfi istifadəçi gizli faylda olan verilənləri oxuya bilmir.

2.*-xüsusiyyəti: səviyyəli məxfi verilənlərə əlçatan (daxil ola bilən) istifadəçi qeyriməxfi verilənlərdən lazım olanlarını yaza bilmir. Qayda az da olsa ehtimallı, bir o qədər də lazımlıdır. Həqiqətəndə istifadəçi məxfi (gizli) faylın surətini alıb onu adi fayla köçürürsə (bu səhvən, bəzən də düşünülmüş ola

bilər), onda fayl bütün istifadəçilərə əlçatan olacaqdır. Bəzən sistemdə gizli fayllarla işləməyə məhdudiyyətlər də qoyulur (məsələn, bu faylın digər kompüterdə istifadə edilməsi üçün üzünü köçürmək olmaz, faylı elektron poçt ilə digər istifadəçiyə göndərmək qadağandır və s.). Təhlükəsizliyin ikinci qanunu təhlükəsizliyə təminat verir və nəzərə alınır ki, bu fayllar heç vaxt qeyriməxfi olmayacaqlar (yəni açıq fayllar olacaqlar), göstərilmiş məhdudiyyətlərdən kanarda qalmayacaqlar.

Beləliklə, məsələn, virus konfidensial verilənləri "oğurlaya" bilməz.



Şəkil 2. Bella-LaPadula təhlükəsizlik modeli

Baxılan qaydalar əsasən iki səviyyədən çox əlçatanlıq olduqda həyata keçirilir, məsələn, qeyriməxfi, konfidensial, məxfi və tamamilə məxfi verilənlər. Məxfi verilənlərə əlçatan istifadəçi qeyriməxfi, konfidensial və məxfi verilənləri oxuya bildiyi halda məxfi və tamamilə məxfi verilənlər yarada bilər.

Ümumi qanun belə səslənir: istifadəçi o sənədləri oxuya bilər ki, onların məxfiliyi onların əlçatanlığından artıq olmasın və ya istifadəçi öz əlçatanlığıdan aşağı olan sənədləri də yarada bilməz. Beləliklə, istifadəçi nəzəri olaraq sənəd yarada bilər, amma onları oxumağa icazəsi olmaya bilər (və ya icazəsi yoxdur).

Bella-LaPadula modeli kompüterlərdə istifadə olunan ilk modellərdən biridir və müəyyən dəyişikliklərə məruz qalmaqla hərbi sahələrdə də istifadə edilir. Model tamamilə riyazi

baxımdan formalaşdırılmışdır. Model əsas istiqamətini ***konfidensiallığa*** yönəltmişdir. Bəzi hallarda modeldən istifadə edən istifadəçi işlədiyi verilənlərdən istifadə edə bildiyi halda, onlar məxfi saxlanılır (istifadəçi onları görə bilmir).

AÇIQLAMA: *Konfidensial* (ingiliscə confidence – inam, etimad, etibar anlamını verir) – istənilən informasiyanın axmasının (hamıya bildirilməsinin) qarşısının alınmasıdır. Etimoloji baxımdan "Konfidensial" sözü latın dilindın gəlmədir – latınca confidentia – etibar deməkdir. Müasir rus dilində söz "yayılmaya ehtiyacı olmayan, gizli, vəkalətnamə" kimi səslənir (istifadə edilir). "Gizli" sözü fransızlardan gəlmədir (secret – sirr).

İnformasiya texnologiyalarının inkişafı ilə əlaqədar olaraq informasiyanın konfidensiallığı böyük əhəmiyyət kəsb edir. Müxtəlif ölkələrdə istifadəsindən asılı olaraq söz müxtəlif cür izah olunur.

Avropa Birliyi Ölkələrində informasiyanın konfidensiallığı bir neçə razılaşmalar və direktivlər vasitəsilə tənzim edilir. Bunlara misal olaraq EC 95/46/EC, 2002/58/EC, ETS 108, ETS 181, ETS 185, ETS 189 direktivlərini göstərmək olar.

Məsələn, "Kompüter informasiyası mühitində cinayətkarlıq haqqında" ***konvensiyada*** (ETS N 185) kompüter verilənlərinin və kompüter şəbəkələrinin, sistemlərinin konfidensiallığına qarşı yönəlmiş hərəkətlərin qarşısının alınması məsələlərinə baxılır.

QEYD: Konvensiya (latınca conventio – müqavilə, razılaşma anlamını verir) müxtəlif beynəlxalq müqavilələr deməkdir.

ƏLÇATANLIĞA NƏZARƏTİN ROL MODELİ (RBAC)

İdarəetmənin rol üsulu istifadəçinin informasiyaya əlçatanlığını onların sistemdəki aktivlik növünə (roluna) görə nəzarətdə saxlayır. *Rol* dedikdə fəaliyyətin növünün müəyyən edilməsi ilə bağlı fəaliyyətlər və öhdəliklər toplumu başa düşülür. Rola nümunə kimi: verilənlər bazasının administratorunu, meneceri, şöbə rəisini və s. göstərmək olar.

Rol üsulunda hər bir istifadəçi üçün deyil, hər bir rol üçün icazə verilən əlçatanlıq əməliyyatları hər bir obyekt ilə müqayisə olunur. Bununla yanaşı hər bir istifadəçinin yerinə yetirə biləcəyi rol ilə müqayisə edəcəyi rol tutuşdurulur. Bəzi sistemlərdə istifadəçi eyni zamanda bir neçə rolu yerinə yetirə bilər, bəzi sistemlərdə isə istifadəçinin bir və ya bir neçə rolu yerinə yetirməsi məhdudlaşdırılır (nəzərə almaq lazımdır ki, bu rollar bir-biri ilə ziddiyyət təşkil etmirlər).

RBAC modelinin formalaşdırılması üçün aşağıdakı razılaşmalardan istifadə olunur:

S = subyekt – insan və ya avtomatlaşdırılmış agent.

R = rol – işçi funksiya və ya ad, avtorizasiya səviyyəsində müəyyən edilir.

P = icazə - resursa təsdiq edilmiş daxil olma rejimi.

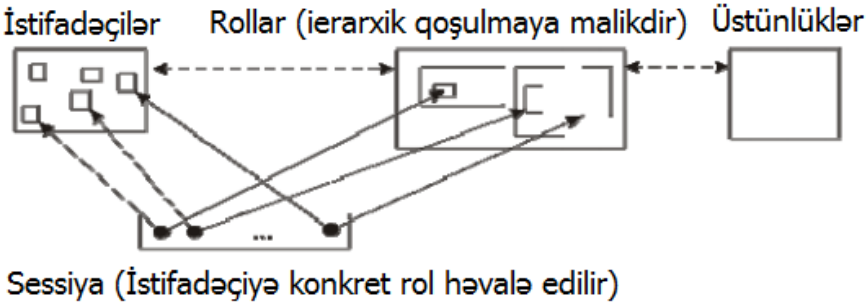
SE = sessiya – S, R və (və ya) P arasında uyğunluq.

SA = subyektin adı (Subject Assignment). $SA \subseteq S \times R.$ Bu zaman subyektlər rollarının əlaqəsinə və "çoxluğu çoxluğa doğru" münasibəti olan subyektlərə görə təyin edilirlər (bir subyektin bir neçə rolu və yaxud bir neçə subyektin bir rolu ola bilər) .

RH = icazənin təyinatı (Permission Assignment). $PA \subseteq P \times R$. Bu zaman icazə rolları "çoxluğu çoxluğa doğru" münasibətdə təyin edir.

RH = ierarxik rolların hissələrlə düzülməsi (Role Hierarchy). $PH \subseteq R \times R$.

Aşağıdakı şəkildə RBAC modelinin sxemi verilmişdir.



Şəkil 3. Əlçatanlığa nəzarətin rol modelinin sxemi (RBAC)

Rol modelinin əsas üstünlükləri:

1.*Administrasiyalaşmanın sadəliyi*. DAC modelindən fərqli olaraq bu modeldə hər bir "obyekt-istifadəçi" cütlüyü üçün icazənin qeyd edilməsinə tələbat yoxdur, çünki bunun yerinə "obyekt-rol" cütlüyü üçün icazə yazılır. İstifadəçinin cavabdeh obyektinin dəyişməsi zamanı sadəcə onun rolu dəyişir. Rolların iyerarxiyası (rol özünə məxsus üstünlüklərlə yanaşı digər rollardakı üstünlüklərə də varis ola bilər) administrasiyalaşma prosesini sadələşdirir.

2.*Az üstünlüklər prinsipi*. Rol modeli istifadəçiyə tələb edilən məsələlərin minimum yerinə yetirilməsi üçün sistemdəki rola uyğun qeydiyyatdan keçməyə imkan verir.

3.RBAC vahid sistem və ya əlavələr sərhəddində istifadəçi üstünlüklərini idarə etmək üçün geniş istifadə olunur. Sistem özünə: Microsoft Active Directory, SELLinux, FreeBSD, Solaris, SUBD Oracle, PostgreSQL 8.1, SAP R/3 və RBAC-da effektiv istifadə olunan çoxlu sayda sistemləri qoşur.

RBAC-ın köməyilə (əlçatanlıq ilə idarə edilən) diskrision və mandat sistemlərini idarə etmək mümkündür.

ƏLÇATANLIĞA HƏDD QOYMA SİSTEMLƏRİ

Əlçatanlığa hədd qoyma modelinin əlçatanlığa hədd qoyma sistemində (СРД - система разграничения доступа - əlçatanlığa hədd qoyma sistemi - ƏHS) konkret təcəssüm edilməsi, hesablama texnikası vasitələrində və ya avtomatlaşdırılmış sistemlərdə əlçatanlığa hədd qoyma qanunlarının həyata keçirilməsi cəmidir.

Hədd qoymanın çoxlu sayda sistemləri əlçatanlığın dispetçer konsepsiyasına əsaslanır. Konsepsiyanın əsasında əlçatanlıq dispetçeri anlamı – subyektlərin bütün obyektlərə müraciəti zamanı ortaq kimi iştirak edən abstrakt maşın anlamı dayanır. Əlçatanlıq dispetçeri müdafiə baza verilənlərindən istifadə edir. Bu verilənlərdə əlçatanlığın hədd qoyma qanunları saxlanılır və bu informasiyaya əsaslanaraq subyektin obyektə daxil olub-olmaması həll edilir.

Əlçatanlıq dispetçerinin əsasında aşağıdakı tələblər dayanır:

- Nəzarət edilən əməliyyatlara qoyulan tələblər əsasında bütün subyektlərin sistemdəki obytektlər uzərində yoxlanışı həyata keçirilir. Bu zaman dispetçerin yoxlama aparması qeyri mümkündür;

- Təcrid olunmaya qoyulan tələblər, yəni funksiyalama prosesinə təsir etmək məqsədi ilə dispetçerin əlçatanlıq subyektlərinin mümkün dəyişmələrindən müdafiə olunması;
- Düzgün funksiyalamanın formal yoxlanmasına qoyulan tələblər;
- Dispetçerin istifadə etdiyi resursların minimumlaşdırılması.

Verlənlərin müdafiə bazası əlçatanlığın matrisinə əsaslanaraq qurulur. *Əlçatanlıq matrisi* – sətirləri subyektlərə, sütunları obyektlərə, kəsişmə nöqtərələri isə subyektin obyektə əlçatanlığı qanunlarını əks etdirir. Matrisin əsas çatışmazlığı həddindən artıq böyük ölçüyə malik olması, administrasiyanın mürəkkəbliyi və sairədir. Əlçatanlıq matrisinin mürəkkəbliyini aradan götürmək üçün onun bəzi aşkar olmayan təqdimatlarını dəyişmək tələb olunur.

Onlardan bəzilərini nəzərdən keçirək:

1.*Əlçatanlığın idarə edilməsi siyahısı* (access control lists, ACL). "Sıfır" qiymətləri olan hər bir obyekt üçün subyektlərin siyahısı verilmişdir. Matris bütün "sıfır" qiymətlərini aradan götürür.

2.*Subyektlərin səlahiyyət siyahısı*. Burada hər bir subyekt üçün obyektlərin siyahısı verilmişdir. Belə təqdimat subyektin profili adlanır. Hər iki səlahiyyət oxşardır və eyni çatışmazlığa malikdir.

3.*Atribut sxemləri*. Prinsip subyektə və (və ya) obyektə müəyyən işarənin mənimsədilməsinə əsaslanır. Matrisin əlçatanlıq elementləri aydın şəkildə saxlanılmır, amma konkret subyekt-obyekt cütlüyü üçün əlçatanlığa cəhd göstəriləndə elementlər dinamik hesablanır. Bu zaman yaddaşa qənaət olunur. Əsas çatışmazlıq qoyulmuş tapşırığın mürəkkəbliyidir.

YOXLAMA TESTLƏRİ

1.Əlçatanlığın idarə edilməsinin hansı modeli Bella-LaPadula modelinə aiddir?

A.Distatsion əlçatanlıq modeli;
B.Mandan əlçatanlıq modeli;
C.Rol modeli.

2.AİS-nin (onun elementləri, proqram təminatındakı səhvlər, personalın fəaliyyətində yaranmış səhvlər və buna bənzərlər) layihələndirilməsi zamanı hədələr (təhlükələr) nəticəsində yaranmış səhvlər neçə adlanır?

3.Hansı müdafiə tədbirlərinə təhlükəsizlik siyasəti aiddir?
A.Administrativ;
B.Qanunvericilik;
C.Proqram-texniki;
D.Prosedur.

4.Təqdim edilən əlçatanlıq matrisindən hansı müəyyən fayla daxil olmağa icazəsi olan istifadəçini sadə şəkildə müəyyən etməyə imkan verir?

A.ACL;
B.Subyektlərə səlahiyyətli olan siyahı;
C.Atribut sxemləri.

5.Səlahiyyəti olmayan, onun sahibi tərəfindən dəyişilməsi nəzərə alınmayan informasiyanın xüsusiyyəti necə adlanır?

A.Tamlıq;
B.Apellyasiya olunan;
C.Əlçatanlıq;

D.Konfidensial;
E.Autentifikasiya.

6.AİS-nin mühafizə olunma sisteminin qurulması prinsipinə aşağıdakılardan hansl aiddir?
A.Aşkarlıq;
B.Müdafiə altsisteminin qarşılıqlı əvəz olunması;
C.Üstünlüyün minimumlaşdırılması;
D.Komplekslik;
E.Sadəlik.

7.Aşağıda verilmişlərdən hansının idarəetmə modeli vasitəsilə RBAC-a əlçatanlığı mümkündür?
A.Bir neçə rolu assosiasiya edən hər bir subyekt ilə (istifadəçi ilə);
B.İyerarxiyada qaydaya salınmış rollar ilə;
C.Bir neçə rola assosiasiya olunan hər bir subyektin əlşatanlığı ilə;
D.Hər bir "subyekt-obyekr" cütlüyü üçün mümkün qərarların toplumunun təyin edilməsi.

8.Daxilolma dispetçeri...
A. ...daxilolmanı məhdudlandıran qanunlar saxlanılan verilənlər bazasının mühafizəsi üçün istifadə edilir;
B. ... əlçatanlıq matrisini təqdim etmək üçün atribut sxemlərindən istifadə edilir;
C. ... subyektlərə və obyektlərə bütün müraciət hallarında ortaq kimi iştirak edir;
D.... sistem jurnalına daxil olmaq üçün edilmiş cəhdlər barədə informasiya fiksə edir.

9.Təxmini olaraq qeyriformal nizam-intizamı pozma modelinə hansıları qoşurlar?

A.Nizam-intizamı pozanın imkanlarını;

B.Nizsam-intizamı pozan müəyyən kateqoriya insanları;

C.Nizam-intizamı pozmağa alışanları;

D.Nizam-intizamı pozan tərəfindən edilmiş əvvəlki hücumu;

E.Nizam-intizamı pozanın bilik səviyyəsini.

10.Rusiya Federasiyasının infromasiya təhlükəsizliyi barədə olan doktrinası nələri təqdim edir?

A.İnformasiya təhlükəsizliyi mühitində qanunvericiliyi pozanların məsuliyyət daşıması haqqında normativ-hüquqi aktı;

B.İnformasiya təhlükəsizliyi sahəsində hüquqi münasibətin tənzimlənməsi haqqında federal qanunu;

C.Rusiya Federasiyasında mərhələlər və dövrlər ardıcıllığını təqdim edən informasiya təhlükəsizliyi sisteminin məqsədli inkişaf proqramını;

D.Rusiya Federasiyasında informasiya təhlükəsizliyini təmin edən məsələlərin, prinsiplərin, əsas istiqamətlərin və rəsmi baxışların toplumunu.

11.Təhlükəsizlik sahəsində təsdiq olunmuş iş proqramı informasiya təhlükəsizliyinin müdafiə olunma növünün hansı tələbinə aiddir?

A.Yuxarı səviyyənin təhlükəsizlik siyasəti;

B.Orta səviyyənin təhlükəsizlik siyasəti;

C.Aşağı səviyyənin təhlükəsizlik siyasəti;

D.İnfrastrukturu dəstəkləyən müdafiə.

12.Adları çəkilmiş hədələrdən hansı düşünülmüş sinfə aiddir?

A.Kompüterin viruslarla korlanması;

B.Yanğın nəticəsində sistemin fiziki dağılması;

C.Hesablama sisteminin funksional təmin edilmiş altsisteminin işdən çıxması və ya sistemin işdən imtina etməsi;

D.İnformasiyanın təhlükəsizliyinə və sistemin iş rejiminə təsir edən amillər (sistemin arxitekturasının layihələndirilməsi, verilənlərin təhlil olunma texnologiyası, tətbiqi proqramların yaradılması və s.);

E.Operativ yaddaşda və xarici yaddaş qurğusunda qalmış (müvəqqəti saxlanılmış) informasiyanın oxunması;

F.İnformasiyanın kriptomüdafiə şifrəsinin "sındırılması".

KRİPTOQRAFİYAYA GİRİŞ. SİMMETRİK ŞİFRƏLƏMƏ

KRİPTOQRAFİYANIN ƏSAS ANLAYIŞI

XX əsrin 70-ci illərinə kimi verilənlərin şifrələnməsi üsullarının yaradılması və öyrənilməsi ilə məşğul olan elm sahəsi və praktiki fəaliyyət *kriptoqrafiya* adlanırdı. İndiki zamanda elmin, texnikanın və praktiki fəaliyyətin bu sahəsi yaradıcılıq ilə əlaqəlidir, informasiyanın müdafiə sisteminin kriptoqrafik təhlilini və tətbiqini həyata keçirir.

Kriptoqrafik sistem dedikdə kriptoqrafik vasitələrdən istifadə etməklə avtomatlaşdırılmış informasiya sistemlərində və ya şəbəkələrdə informasiyanın təhlükəsizliyinin təmin edilməsini həyata keçirən sistem nəzərdə tutulur. Bəzən bu məqsədlə altsistemin şifrələnməsi, istifadəçinin identifikasiyası, elektron rəqəmsal imza və başqalarından da istifadə olunur.

Kriptoqrafiya vasitələri dedikdə informasiyanın kriptoqrafik çevrilməsindən istifadə etməklə informasiya təhlükəsizliyinin təmin edilməsi üçün yararlı olan vəsaitlər və üsullar nəzərdə tutulur. Dar mənada isə kriptoqrafik vasitələr dedikdə kriptosistem funksiyasını yerinə yetirən ayrı-ayrı qurğular, sənədlər və proqramlar başa düşülür.

İnformasiyanın kriptoqrafik çevrilməsi dedikdə kriptoqrafik alqoritmlərin birindən istifadə etməklə informasiyanın çevrilməsi nəzərdə tutulur. *Kriptoqrafik alqoritmlərə* şifrələmə/deşifrələmə alqoritmləri, xeşləmə, formatlama və

elektron rəqəmsal imzaların yoxlanması, açarların paylanması və çoxlu sayda digər alqoritmlər daxildir. Adları çəkilən alqoritmlərin hər biri ehtimal olunan, nizam-intizamı pozan (düşmən, pisniyyətli və s.) şəxs tərəfindən müəyyən informasiya təhlükəsizliyinə qarşı yönəlmiş hədələrin aradan qaldırılmasına yardımçıdırlar.

Əksər kriptoqrafik alqoritmlər riyazı əsasa söykənərək qurulurlar.

Kriptoqrafiya kriptologiya elminin hissələrindən biridir. Kriptologiya elminin digər hissəsi kriptotəhlil (və ya kriptoanalız) ilə məşğul olur. XX əsrin 70-ci illərinə kimi elmin bu sahəsi şifrələmə üsullarının zəif və güclü tərəflərini, həmçinin şifrələrin sındırılması üsullarını öyrənirdi. İndiki zamanda kriptotəhlil kriptoqrafik sistemin müdafiəsi ilə məşğul olan elm sahəsidir. Sahə informasiya təhlükəsizliyinin pozulma üsullarının axtarılması ilə məşğul olur və cari sistemin informasiya təhlükəsizliyini təmin edir. Beləliklə, kriptotəhlil şifrələnmiş mətnin açarsız oxunma üsullarını, elektron rəqəmsal imzanın saxtalaşdırılma üsullarını və başqalarını öyrənir. Kriptoqrafiya və kriptoanaliz güclü elm sahələri olsada, bir-birinin əksinə yönəlmiş məqsədə qulluq edirlər. Sonuncu onilliklərdə bu elm sahələri fasiləsiz və intensiv inkişaf edir, nəticədə bir sahənin inkişafı digər sahənin inkişafına da səbəb olur.

ŞİFRƏLƏMƏ

Şifrləmə dedikdə açıq mətn adlanan **M** başlanğıc məlumatının şifrələnmiş mətn (və ya şifrmətn) adlanan **M'** formasına çevrilməsi başa düşülür. Nəzərə almaq lazımdır ki,

əks çevirməni həyata keçirmək üçün *açar* adlanan əlavə informasiyaya malik olmaq lazımdır.

Bəzi istifadəçilər şifrələməni kodlaşdırma ilə səhv salırlar. Əslində bu proseslər arasında hiss olunacaq dərəcədə fərq vardır. Kodlaşdırmada da başlanğıc məlumatın başqa bir formaya çevrilməsi prosesi yerinə yetirilir, amma bu çevrilmədə məqsəd informasiyanın əlverişli ötürülməsi və ya əlverişli təhlil edilməsidir. Məsələn, xüsusi hazırlanmış mətn ikilik kod ilə kodlanır (yəni hər bir simvol 1 və 0 –ların ardıcıllığı ilə əks olunur). Məqsəd bu informasiyanı Elektron Hesablama Maşınında rahat təhlil etmək, lazım gəldikdə yaddaşda saxlamaqdır, çünki elektrik impulsları ardıcıllığı ilə əks olunan informasiyanı kabel vasitəsilə ötürmək rahat və əlverişlidir.

Şifrələmənin məqsədi isə başqadır. Mətn ona görə şifrələnir ki, şifrəni açmaq üçün açara malik olmayan kənar şəxs (daha doğrusu pisniyyətli insan) şifrələnmiş mətni oxuya bilməsin (hətta mətn haqqında müəyyən məlumata malik olsa da belə).

Beləliklə, şifrələmə *informasiyanın konfidensiallığını* təmin edən alətdir.

Şifrələmə alqoritmi iki böyük qrupa bölünür:

1.Simmetrik (ənənəvi şifrələmə);

2.Açıq açarla şifrələmə.

SİMMETRİK ŞİFRƏLƏMƏ

Şifrələmənin simmetrik alqoritmində bir **K** açarından istifadə olunur. Açar məlumatı şifrələmək və sonrakı mərhələdə şifrədən çıxarmaq (deşifrə) üçün istifadə edilir. Deməli, məlumatı *göndərən* və *qəbul edən* həmin açara malik olmalıdır. Öndə söylənənləri sxem şəkilində belə yazmaq olar:

$$\mathbf{M'} = E(M, K)$$
$$\mathbf{M} = D(M', K)$$

Burada E – şifrələmə funksiyasıdır (encrypt), D - isə deşifrələmə funksiyasıdır (decrypt), hər iki funksiya bir yerdə K açarından istifadə edir.

Tarixə nəzər salsaq görərik ki, şifrələmə birinci yaranmışdır. Bununla yanaşı XX əsrin ortalarına kimi bu üsul şifrələmənin yeganə üsulu sayılırdı. Simmetrik alqoritm indiki zamanda geniş istifadə olunur.

Simmetrik alqoritm üç sinifə bölünür:

1. Dayaqlıq alqoritmi;

2.Başqasının yerinə qoyulma alqoritmi;

3.Həm dayaqlıq, həm də ki, başqasının yerinə qoyulma alqoritmi (EHM-da informasiyanın mühafizə edilməsi üçün müasir dövrdə hazırlanan bütün ***alqoritmlər*** praktiki olaraq bu sinifə aiddirlər).

AÇIQLAMA: *Alqoritm anlayışı* informatikanın mərkəzi anlayışıdır. Alqoritm sözü IX əsrdə yaşamış özbək riyaziyyatçısı əbu Abdulla Məhəmməd ibn Musa əl-Xörəzmin adı ilə bağlıdır.

Alimin yaşadığı Xörezm şəhəri Amu-Dərya çayı sahilində yerləşir. Alim öz əsərində hind riyaziyyatını ətraflı şərh etmişdi. Üç yüz il sonra (1120-ci ildə) alimin əsəri latın dilinə tərcümə edilir. Kitabı avropa alimləri "Alqoritmi de numero İndorum" ("Hind hesablamaları üçün alqoritm") adlandırırlar. Kitab uzun illər ilk dərslik kimi Avropanınn elm və tədris müəssisələrində geniş şəkildə istifadə olunur. Bu ərəfədə hind rəqəmlərindən ərəb ölkələrində də istifadə etməyə başlayırlar.

Məhəmməd əl-Xörezminin riyazı məsələləri tənliklərin

köməkliyi ilə həll etmək üçün yazdığı kitab təxminən 850-ci ildə çap olunmuşdu. Alim kitabı "Kitabi əl-Cəbr" adlandırmışdı. Kitab bu sahəni araşdıran elmin Cəbr adlandırılmasının təməlini qoyur.

Özbək riyaziyyatçısı əbu Abdulla Məhəmməd ibn Musa əl-Xörəzmi, yzdığı əsərdən bir parça

DAYAQLIQ ALQORİTMİ

Şifrələmənin dayaqlıq alqoritmi aşağıdakı prinsipə uyğun işləyir: başlanğıc məlumatın hər bir siqnalı (və ya simvollar ardıcıllığı) digər simvol ilə (və ya digər simvolların ardıcıllığı ilə) əvəz olunur (dəyişdirilir).

Konkret nümunələrə baxaq.

Sezar şifri.

Ən qədim və ən sadə dayaqlıq şifri Qay Yuliy Sezar tərəfindən istifadə edilən şifr sayılır. Burada başlanğıc məlumatın hər bir şifrələnən hərfi özündən üç mövqe sonra duran hərflə əvəz olunur.

М = криптография

-3

М' = нултхсеугчлз

К = ?

Şəkil 4. Yuliy Sezar şifrələnməsinə nümunə

Y.Sezar şifrinin xüsusiyyəti onun açarının olmamasıdır. 3 ədədi açar kimi istifadə edilə bilməz, çünki o məlumat göndərən tərəfindən seçilmir, sadəcə olaraq hərfin yerindən tərpədilməsi üçün istifadə edilir. Qeyd etmək lazımdır ki, Y.Sezarın rəhbərliyi dövründə göstərilən hal şifrin asanlığı sayılmırdı.

İndiki zamanda informasiyanın şifrələnməsi və deşifrələnməsi prosesi o qədər mürəkkəbləşdirilmişdir ki, lazım olan əməliyyatların əl ilə həyata keçirilməsi mümkün deyil. Bu məqsədlə proqram təminatından istifadə edilir və bu işlə məşğul olan şəxs lazım gəldikdə tamamilə şifrələmə alqoritmini bərpa edə bilir.

Kriptoqrafik proqram təminatı geniş kütlə üçün nəzərdə tutulmayanda bu qayda-qanun pozula bilər. Məsələn, elektron səsvermə sistemlərində, hökumət əlaqə xətlərində istifadə

olunan üsuldan imtina olunanda və s. nümunə kimi göstərilə bilər.

Təcrübə göstərir ki, bədniyyətli insanlar kriptoqrafik müdafiə sistemini sındırmaqla proqrama daxil ola bilir, istifadə olunan alqoritmləri təhlil edirlər.

Çoxəlifbali şifr (sadə dəyişməklə alinan şifr).

Dayaqlıq şifrələrindən geniş yayılmışıdır. Burada əlifbanın hər bir simvoluna digər əlifbanın bəzi simvolu uyğun gəlir. Şifrələmə zamanı açıq mətndəki hər bir simvol uyğun digər simvol ilə əvəzlənir.

Şifrə açar kimi hazırlanmış cədvəldən istifadə olunur. Başqa sözlə, şifrələnmiş mətnə açar əlifbada yeri dəyişdirilmiş simvollardır.

абвгдеёжзкйклмнопрстуфхчщьъэюя
К =йцукенгшщзхъэждлорпавыфячсмитьбюё
а = й
б = д
в = у
. . .
М = криптография
М' = ързоалкойызё

Şəkil 5. Hərflərin sadə üsulla dəyişməsinə nümunə

Göstərilən nümunədə aşarların sayı yerdəyişmədə iştirak edən hərflərin sayına, yəni 33-ə bərabərdir. Əgər milyon kompüter milyon mümkün açarların sayını yoxlasaydı, bütün variantların yoxlanmasına milyon il lazım gələcəkdi. Deməli, monəlifbalı şifrə seçim üsulu ilə açarın seçilməsinə imkan vermir, şifrənin sındırılması isə mümkün deyil.

Amma cari şifrə sadə şəkildə kriptoanalız aparmağa imkan verir. Kriptotəhlil hər bir simvolun hesablanması və həmin simvolun rast gəlinmə tezliyi ilə yerinə yetirilir. Kifayət qədər uzun məlumat (4 - 5 tərtibli cümlə) üçün bu informasiya kifayətdir, əlifbanın hərflərinin cədvələ uyğun təkrarlanması ilə onu tutuşdurmaq olar.

Məlumdur ki, bütün dillərdə istifadə olunan sözlərdə əlifba simvolların təkrarlanması mövcuddur, məsələn, rus dilində "О" hərfi daha tez-tez təkrarlanır, nəin ki, "Ф" hərfi. Bunu aşağıdakı cədvəldə aydın müşahidə etmək mümkündür.

Cədvəl 1. Rus dilində tez-tez təkrarlanan hərflər

Simvol	Ehtimal	Simvol	Ehtimal	Simvol	Ehtimal
probel	0,175	К	0,028	Ч	0,012
О	0,089	М	0,026	Й	0,010
Е	0,072	Д	0,025	Х	0,009
А	0,062	П	0,023	Ж	0,007
И	0,062	У	0,021	Ю	0,006
Н	0,053	Я	0,018	Ш	0,006
Т	0,053	Ы	0,016	Ц	0,004
С	0,045	З	0,016	Щ	0,003
Р	0,040	Ь	0,014	Э	0,003
В	0,038	Б	0,014	Ф	0,002
Л	0,03	Г	0,013		

İngilis dilində aparılmış araşdırmalar göstərir ki, ən çox *the* artikulundan istifadə edilir.

Beləliklə, monoəlifba şifrəsi aparılan kriptoanalizə zəif müqavimət göstərir. Bu baxımdan düşmənə məqsədyönlü açar axtarmaq lazım deyil, açar şifrəni araşdıran zaman özü-özünə bərpa olunacaq.

Öndə yazılanlardan aydın olur ki, Q.Y.Sezarın şifrəsi də monoəlifbalı idi.

Qronsfeld şifrəsi.

Yuliy Sezarın şifrəsinin modifikasiya olunmuş halını nəzərdən keçirək. Açar kimi fiksə olunmuş uzunluğa malik rəqəmlər ardıcıllığından istifadə edilir. Əgər açarın üzunluğu mətnin uzunluğundan qısadırsa, ardıcıllığın hər bir rəqəmi açıq mətnin bir simvolu ilə yazılır və bu halda açar dövrü olaraq təkrarlanır.

Nümunə kimi "информатика" sözünü "123" açarı ilə şifrələyək.

M = информатика

K = 123

M' = йпчгтлболгв

Şəkil 6. Qronsfeld şifrəsindən istifadə etməklə şifrələnmiş mətn

Cari şifr (Şifr Jül Vernin "Janqada" romanında oxuculara təqdim edilmişdi) *çoxəlifbalı şifrəyə* (və ya *mürəkkəb dəyişən şifrəyə*) aiddir. Çoxəlifbalı şifrədə açıq mətnin 1-ci simvolu çoxəlifbalı şifrənin köməyilə şifrələnir. Burada 1-ci simvolun açarı K_1, 2-ci simvolun açarı K_2 və s. n-ci simvolun açarı K_n, n+1 –ci simvolun açarı isə yenidən K_1 olacaqdır. n istifadə edilən əlifbaların (və ya sadə dəyişən şifrələrin) sayıdır. Öndə verilmiş nümunədə n=3.

Çoxəlifbalı şifrənin xüsusiyyətlərindən biri Qronsfeld şifrəsinin yaxşı formada nümayiş olunmasıdır. Qronsfeld şifrəsinin müəyyən çətışmazlıqları da vardır ki, onlarda Qronsfeld şifrəsinin modifikasiya edilməsi ilə aradan qaldırılmışdır, yəni açar kimi rəqəmlərdən deyil, hərflər

ardıcıllığından istifadə olunmasıdır. Açıq mətndəki hərflərin sıra nömrəsi onların altında yazılmış açarın hərfləri ilə üst-üstə yığılır və nəticədə şifrələnmiş mətnin hərflərinin sıra nömrəsi alınır.

M = информатика
васявасява **K = вася**

M' = ложнунтсллт

Şəkil 7. Modifikasiya olunmuş Qronsfeld şifri

Öndə araşdırılmış Sezar və Qronsfeld şifrələrinin "toplanma" mexanizmi (rəqəmlərlə və ya hərflərlə) başqa şriflərdə də istifadə olunur. Belə şifrələrin xüsusiyyəti ondan ibarətdir ki, şifrə açarın bərpa edilməsinə imkan verir (əgər açıq və şifrələnmiş mətn məlumdursa). Bu əks əlaqə əməliyyatı ilə, yəni "toplanma" – "çıxılma" ilə yerinə yetirilir.

Beləliklə, əgər pisniyyətli insan (düşmən) açıq mətnə malikdirsə və bu mətnə uyğun şifrəni bilirsə, onda o açara sahib ola bilər və açardan istifadə etməklə digər şifrələnmiş mətnlərin də şifrəsini açmağa cəhd göstərə bilər. Belə bir üsul *məlum açıq mətnlə yerinə yetirilən kriptoanaliz* adlanır. Təcrübə göstərir ki, Qronsfeld şifrəsi ilə şifrələnmiş mətn bu üsulun qarşısında acizdir.

Bəzən düşmənləri ən çox yayılmış üsulla aldadırlar, yəni qəsddən düşmənin açа biləcəyi şifrəyə uyğun mətni şifrələyir və kanal vasitəsilə ötürürlər. Bundan xəbərsiz pisniyyətli insan göndərilmiş mətni şifrədən azad edir və yalanlardan ibarət olan mətni məqsədi üçün istifadə edir. Nəticədə şifrədən azad olmuş mənasiz söz yığımına sahib olur. Belə şifrələmədən Böyük

Vətən Müharibəsində (1941-1945-ci illərdə) geniş istifadə edilirdi.

Çoxhərfli şifrələmə.

Dayaqlıq şifrələnməsində qeyd olundu ki, şifrələmə zamanı ilkin məlumatın hər bir simvolu deyil, simvollar qrupu şifrələnir. Nəzərə almaq lazımdır ki, bu zaman şifrələnəcək simvollar qrupu başqa bir qrupun simvolları ilə şifrələnir. Belə *şifrələnmə çoxhərfli şifrələmə* adlanır. Çoxhərfli şifrələməni aydınlaşdırmaq üçün Pleyfeyer şifrələnməsini araşdıraq. Şifrələmə zamanı şifrələmə vahidi kimi *biqrammadan* (hərf cütlüyü) istifadə edilir ki, burada da bir hərf cütlüyü digər hərf cütlüyü ilə əvəz olunur.

Şifrələmə ingilis əlifbası üçün nəzərdə tutulmuşdur. Açar kimi istifadə edilən kod cümləsi (ibarəsi) 5x5 kvadrat çərçivənin birinci hücrəsinə yazılır (təkrarlanan hərflər buraxılır). Sonra isə çərçivənin birinci hicrəsinə yazılmış hərflərdən başqa yerdə qalan bütün hərflər kvadratın çərçivəsinə əlifba sirası ilə yazılır (daha doğrusu çərçivə doldurulur). Nəzərə almaq lazımdır ki, I və J hərfləri eyni hərf kimi qəbul olunur.

Çərçivəni açar sözü olan MONARCHY sözü ilə dolduraq.

MONAR
CHY3D
EFCIK
LPOST
UVWXX

Şəkil 8. Pleyfeyer şifrələnməsi üçün kod çərçivəsi

İlkin mətn biqramma bölünür. Əgər açıq mətndə iki eyni hərf bir biqramm əmələ gətirirsə, onda onlar arasında X simvolu qoyulur (məsələn, BALLOON BALXLOON kimi şifrələnir).

Əgər biqramm bir sətirdən (sütundan) ibarətdirsə, onda dövrü yerdəyişməni nəzərə almaqla onlar birinci (aşağıdakı) qonşu sətir ilə yerlərini dəyişirlər. Nümunədə OR NM kimi, OP isə HV kimi şifrələnir.

Əgər biqrammın hərfləri müxtəlif sətirlərdə və sütunlarda yerləşirlərsə, onda hər bir hərf cütlüyü sətirin və sütunun kəsişdiyi hücrədə yerləşən ikinci hərf ilə əvəz olunur. Məsələn, BE CI kimi, OS isə AP kimi şifrələnir.

Deməli, INFORMATION sözü GAPHMORSFAAW kmi şifrələnəcək.

Carı şifrə ilkin mətnin statistik xüsusiyyətini saxlayır, yəni tezlik biqramm cədvəlini dil üçün qurmaq olur və bu zaman şifrələnmiş mətnin biqramm tezliyini təhlil etmək mümkün olur. Digər tərəfdən ingilis dilində 26 hərfin olduğunu nəzərə alsaq, onda biqramm $26^2 = 676$ olacaq. Bu baxımdan məsələ mürəkkəbləşir, şifrələnən mətnin həcminin artması nəticəsində çəkilən zəhmət uçuruma gedir.

Digər maraqlı çoxhərfli şifrələməyə nümunə kimi *Hill şifrini* göstərmək olar. Şifrə *m* əmsallı *m* xətti bərabərliklərdən ibarətdir. Şifrə açiq mətnin hər bir *m* hərfini şifrələnmiş *m* hərfi ilə əvəz edir. Məsələn, m=3 olduqda aşağıdakı bərabərlik sistemini əldə edirik (burada n - əlifbanın gücüdür).

$$C_1 = (k_{11}p_1+k_{12}p_2+k_{13}p_3) \bmod n$$
$$C_2 = (k_{21}p_1+k_{22}p_2+k_{23}p_3) \bmod n$$
$$C_3 = (k_{32}p_1+k_{32}p_2+k_{33}p_3) \bmod n$$

Şifrələmə açarı K əmsallı matrisa olacaqdır, amma şifrələməni vektorun tərtibi kimi təqdim etmək olar. Şifrələmə vektorunun tərtibi açıq mətnin hərflərinin ardıcıllıq nömrələrindən tərtib edilmişdir (birinci hərf 0 nömrəsinə malikdir). Onda K açar matrisası belə olacaqdır:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} k_{11} k_{12} k_{13} \\ k_{21} k_{22} k_{23} \\ k_{31} k_{32} k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

Şifrələnmiş mətni deşifrə etmək üçün matrisanı k əmsalına əks olan k^{-1} əmsalına vurmaq lazımdır.

Hill şifri ilkin məlumatın simvollar tezliyini yaxşı mühafizə etsədə (gizli saxlayır) məşhur açıq mətn kriptotəhlilinə zəif cavab verir. Sistem xəttidir, odur ki düşmənə şifrəni açmaq üçün m^3 cüt qədər "aşıq mətn – deşifrə olunmuş mətn" əməliyyatını həyata keçirmək lazımdır.

Cari şifrə üçün daha effektli kriptotəhlil üsulu *seçilmiş açıq mətnlə kriptotəhlil üsuludur*.

Birdəfəlik bloknot.

Qeyd etmək lazımdır ki, öndə baxılan bütün şifrələmə üsulları klassik alqoritmlərlə şifrələməyə aiddirlər və elm və texnikanın kompütersiz dövrlərində istifadə olunmuşdur. İstifadə olunan hər bir alqoritm müəyyən növ kriptotəhlil ilə bağlı olmuşdur.

İndiki zamanda yeni şifrələmə üsullarından istifadə olunur ki, onları "sındırmaq" həddindən artıq çətindir. Şifrə *Vernama şifrəsi* adlanır (bəzi ədəbiyyatlarda onu *birdəfəlik bloknot* da adlandırırlar).

Vernama şifrəsində açıq mətn onun ölçüsü ilə uyğun gələn *mütləq təsadüfi açarla* üst-üstə qoyulur. Sonra açar ləğv edilir (yəni digər mətnlərin şifrələnməsində istifadə olunmur). Şifrənin mütləq kriptodavamlığı Klod Şennon tərəfindən sübut olunmuşdur.

Təcrübədə birdəfəlik bloknotdan təsadüfi hallarda istifadə olunur (əsasən yüksək səviyyəli məlumatları şifrələyəndə ondan istifadə edilir). Digər tərəfdən bloknotun hazırlanması çox baha başa gəlir. Bununla yanaşı şifrə açarının şəxsə təqdim edilməsi şəxs ilə təkbə-tək görüş zamanı yerinə yetirilməlidir.

BAŞQASININ YERİNƏ QOYULMA ALQORİTMİ

Bu alqoritmdə açıq mətnin simvolları açarın müəyyən etdiyi simvollar ardıcıllığı ilə dəyişdirilir (başqasının yerinə qoyulur).

Bunu nümunədə aydınlaşdıraq. Açıq mətnin simvolları soldan sağa deyil, yuxarıdan aşağı başqasının yerinə qoyulur və nəzərə alınır ki, sütunun hündürlüyü məhduddur. Nəticə sətir kimi alınır.

M = в лесу родилась ёлочка

K = 27

влс оиаьёок
еурллс лча

M' = влс оиаьёок еурллс лча

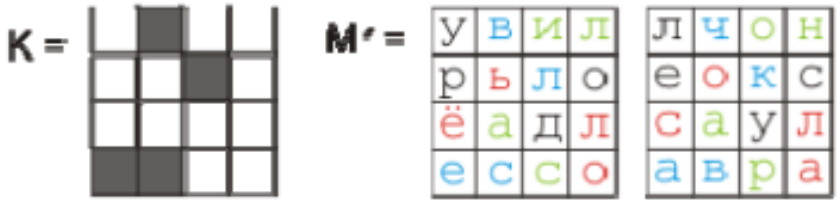
Şəkil 9. Başqasının yerinə qoyulma alqoritminə uyğun sadə şifrələnmə

Şifrə açarın seçilməsi ilə bağlıdır (açar kimi sütunun hündürlüyü iştirak edir) və istənilən halda açar məlumatın uzunluğundan çox ola bilməz.

Fleyberq çərçivəsinə başqa bir nümunədə baxaq. Şifrə açar kvadrat çərçivədir və çərçivənin yanları cüt sayda hücrələrdən ibarətdir. Hücrələrin dörddə biri (çərək) aşağıdakı prinsiplə kəsilir: əgər bəzi hücrə kəsilmişsə, onda həmin hücrə kəsilə bilməz, çünki o hücrə çərçivənin 90^0, 180^0 və 270^0 dönməsində hüdudu aşır.

Mətni şifrələmək üçün kəsiklə olan çərçivə cızıqlanmış kvadratın üzərinə qoyulur, sonra isə mətnin hərfləri kəsiklərə yazılır. Bütün kəsiklər dolduqdan sonra çərçivə 90^0 döndərilir. Çərçivənin dolma prinsipinə görə kəsiklər bu zaman dolmamış hücrələrin yerinə olacaqdır. Kəsiklərə mətnin davamı yazılır, yenidən çərçivə döndərilir və prosedur bir dəfə də təkrar olunur. Əgər mətn bir kvadrata yerləşməmişsə, onda eyni qayda ilə növbəti doldurulur. Sonuncu kvadratın boş qalmış hücrələri təsadüfi simvollar ilə doldurulur.

M = влесуродиласьёлочкавлесуонаросла



Şəkil 10. Fleyberq çərçivəsinin köməyilə şifrələmə

Fleyberq şifrəsi hamı tərəfindən (sözsüz ki uçaqlar nəzərdə tutulur) sevilə-sevilə oxunan mahnıdan istifadə

etməklə hazırlanmış açıq mətnin kriptotəhlilinə o qədər də tutarlı səviyyədə cavab verə bilmədi (nəzərə almaq lazımdır ki, ikilik əlifba üçün bu əlaqə müəyyən qədər azdır, amma təbii-dil əlifbaları üçün belə söyləmək düzgün deyil).

MÜASİR SİMMETRİK ŞİFRƏLƏMƏ ALQORİTMİ

Müasir simmetrik şifrələmə alqoritmi həm dayaqlıq, həm də ki, başqasının yerinə qoyulma üsulu ilə şifrələmədə istifadə olunur. Həqiqətdə isə (de-fakto) standart şifrələmə müxtəlif açarlar ilə şifrələmə raundlarından ibarətdir. İstifadə edilən açarlar ümumi açarın generasiya edilməsinə əsaslanır. İndiki zamanda istifadə olunan əksər alqoritmlər 1973-cü ildə yaradılmış Faystel şifrəsinin strukturuna bənzərdirlər.

Faystel şifrəsi Klod Şennonun praktiki şəkildə həyata keçirilən ideyalarına söykənərək hazırlanmışdır: etibarlı şifrələmə alqoritmi iki xüsusiyyəti təmin etməlidir: *diffuziyanı* və *koffuziyanı*.

Diffuziya – açıq mətnin hər bir biti şifrələnmiş mətnin hər bir bitinə təsir göstərməlidir. Diffuziyanın mənasi ondan ibarətdir ki, açıq mətnin statistik xarakteristikaları şifrələnmiş mətnin daxilində səpələnməlidir.

Koffuziya – açarlar və şifrələnmiş mətn arasında statistik əlaqənin olmamasıdır. Əgər bədniyyətli insan (düşmən) şifrələnmiş mətnin hansısa statistik xüsusiyyətini müəyyən edərsə, açar haqqında istənilən informasiyanı əldə etmək üçün əldə etdiyi məlumatlar onun bəd niyyətini həyata keçirməyə kifayət etməyəcəkdir.

Feystel şifrəsinin strukturunu araşdıraq.

Cari şifrə blok şifrələmə kateqoriyasına aiddir. Blok şifrələməsi çox da böyük olmayan, müəyyən uzunluğa malik

blokların şifrələnməsi üçün istifadə olunur. İxtiyari mətni şifrələmək üçün onu bloklara bölmək, sonra isə hər bir bloku ayrıca şifrələmək lazımdır. İstər Feystel şifrəsi, istərsə də bütün müasir alqoritmlər ikilik alqoritm ilə işləyirlər (burada açıq və şifrələnmiş mətn bitlər ardıcıllığı ilə təqdim edilir).

Qeyd etmək lazımdır ki, alqoritmlər Elektron Hesablama Maşınlarında şifrələmə əməliyyatlarını həyata keçirmək üçün istifadə olunurlar.

Şifrələmə alqoritminin girişinə açıq mətnin bloku verilir (blok 21 cüt uzunluğa və *K* açarına malikdir). Blok iki bərabər hissəyə bölünür – sağ R0 və sol L0. Sonra bu hissələr m raundlu təhlilə məruz qalırlar, sonra yenidən şifrələnmiş mətndə birləşirlər.

Hər bir i-ci raund K ümumi açarına əsaslanan generasiya olunmuş K_i altaçarından ibarətidr. K_i altaçarı bir para F_i çevirmə açarından asılı olan R_i blokuna tətbiq olunur. Nəticə ***XOR əməliyyatının*** ("VƏ YA" məntiqi əməliyyatı müstəsna olmaqla) köməyilə L_i bolku ilə üst-üstə yığılır (cəmlənir) və nəticədə R_{i+1} bloku alınır. R_i bloku dəyişmədən L_{i+1} blokunun yerinə götürülür.

Deşifrələmə əməliyyatı prinsipcə şifrələmə əməliyyatından fərqlənmir. Deşifrələmə əməliyyatında girişə deşifrə olunmuş mətn verilir, K_i açarı isə əks qaydada (ardıcıllıqla) hesablanır.

AÇIQLAMA: *XOR məntiq əməliyyatı* "VƏ YA" məntiqi əməliyyatının istisna edilməsi, əksi kimi qəbul edilir.

Faystel alqoritminin strukturundan istifadə edən müxtəlif alqoritmlər aşağıdakı paramterlərinə görə bir-birindən fərqlənirlər:

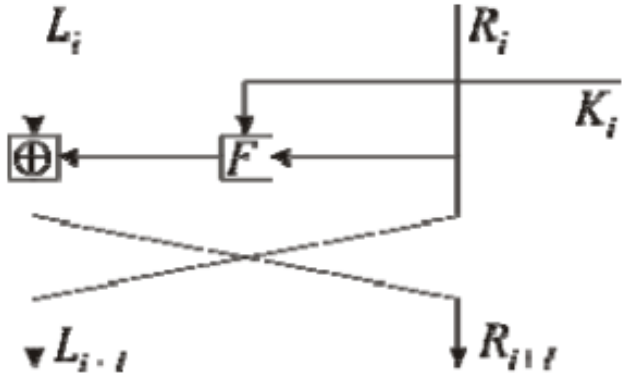
1.*Açarın uzunluğu*. Açarın uzunluğu alqoritmlə nəzərdə tutulmuşdan uzun olarsa, seçimi etmək də bir o qədər mürəkkəb olacaqdır. İndiki zamanda açarın uzunluğunun 1024 bitdən az olmaması nəzərdə tutulur.

2.*Blokun ölçüsü*. Blokun ölçüsü böyük olduqca, şifrələmə də bir o qədər etibarlı alınır, amma şifrələmə/deşifrələmə əməliyyatının yerinə yetirilmə sürəti bu halda aşağı düşür.

3.*Raundların təhlil olunma sayı*. Hər bir yeni təhlil olunma raundundan sonra şifrələmənin etibarlığı yüksəlir.

4. F raund funksiyası – funksiya mürəkkəbləşdikcə, şifrənin kriptotəhlili bir o qədər çətinləşir.

5. K_i aralıq açarının hesablanma alqoritmi.



Şəkil 11. Feystel şifrəsinin köməyilə i-ci raundun şifrələnmə sxemi

DES alqpritmi.

Uzun müddət ən məşhur simmetrik şifrələmə alqoritmi DES (Data Encrypting Standart) sayılırdı (alqoritm 1977-ci ildən istifadə edilməyə başlanmışdır). Alqoritm Faystel şifrəsinin

struktur bazasına söykənir. Alqoritm 64 bitlik bloka və 56 bitlik açara malikdir.

F raundun funksiyası səkkiz S-matris adlanan toplumdan bəhrələnir. Hər bir matris 4 sətirdən ibarətdir, hər bir sətir isə 0-dan 15-ə qədər rəqəmlərin (uyğun olaraq 16 sütundan) yerdəyişməsindən ibarətdir. Matrislər sərt verilmişdir. Hər bir matris 6 bitlik girişə malikdir və 4 bitlik nəticə verir. Girş kəmiyyətinin birinci və axırıncı biti matrisin sətirini, yerdə qalan dördü isə sütunlarını əks etdirir. Hesablamada ikilik say sistemindən istifadə olunur, sətirlərin və sütunların kəsişməsi çevrilmənin nəticəsi olacaqdır. Burada F çevrilməsi aşağıdakıları özündə əks etdirir:

1. 32 bitlik R_i bloku bəzi (bir para) 16 biti xüsusi cədvəlin köməyindən istifadə etməklə, təkrarlamaq yolu ilə 48 bitə kimi genişləndirilir.

2.Alınmış nəticə XOR əməliyyatının köməyilə 48 bitlik K_i altaçarından istifadə etməklə cəmlənir (üst-üstə yığılır).

3.Cəmlənmənin nəticəsi 8 altıbitlik bloka bölünür və onlardan hər biri uyğun S –matrisinin köməyilə yaradılır.

4.Nəticədə alınmış 32-bitlik blok dayaqlıq alqoritmində sərt verilmiş yerdəyişməyə məruz qalır.

AÇIQLAMA: S –matrisi DES alqoritminin ən şübhəli (ikimənalı) hissəsi sayılır. Alqoritmin yaradıcıları onun dolma prinsipini indiyə kimi agah etməyiblər. Sual olunur: nə üçün bu matris seçilmişdir və alqoritm "gizli gediş"lərə malikdirmi? Uzun illər boyu alqoritmin "sındırılması"na edilən cəhdlər səmərəsiz qalmışdır.

Uzun müddət ərzində ***DES*** ABŞ-ın federal standartı olmuşdur. Alqoritm lazımı formada "*sürətli axın effektini*"

nümayiş etdirir (açıq mətnin bir bitinin və ya açarının dəyişməsi şifrələnmiş mətnin çoxlu sayda bitlərinin dəyişməsinə səbəb olur) və uzun illər boyu şifrənin sındırılması cəhdinə qarşı mətanətlə dura bilmişdir. Digər tərəfdən uzunluğu 56 bit olan açar məhsuldarlığı böyük sürətlə artan EHM-lərin tələblərini tutarlı səviyyədə ödəmədiyi üçün 1997-ci ildə yeni alqoritmin yaradılması üçün müsabiqə elan olundu. Müsabiqənin şərti belə idi: yaradılacaq alqoritm ən azı 15-20 il müddətində kriptostandartlara lazımı səviyyədə qulluq göstərməlidir.

AES alqoritmi.

Müsabiqənin qalibi 2000-ci ildə müəyyən olundu – qalıb Belçika şifri RIJNDAEL elan olundu. Bir müddət sonra şifrə AES (Advanced Enecryption Standard) adlandırılır. Şifrə qeyristandart blok şifrəsidir və Feyştel şəbəkəsindən istifadə etmir. Hər bir giriş bloku ikiölçülü bayt massivi kimi təqdim edilir (blokun ölçüsündən asılı olaraq 4x4, 4x6 və ya 4x8 kimi müxtəlif şəkildə göstərilə bilər). Blokun ölçüsündən və açarın uzunluğundan asılı olaraq alqoritm 10-dan 14-ə kimi raundlardan ibarətdir və hər bir raundda bəzi dəyişikliklər həyata keçirilir (ya asılı olmayan sütunlar üzərində, ya asılı olmayan sətirlər üzərində, ya da ki, cədvəldə olan baytlar üzərində).

Öndə sadalanan şifrələrlə yanaşı indiki zamanda IDEA, Blowfish, RC5, CAST-128 simmetrik şifrələrindən də istifadə olunur.

AÇIQLAMA: *DES* (ingliscə sözündən yaranmadır) – simmetrik şifrələmə üçün alqoritmdir, IBM firması tərəfindən yaradılmışdır, 1977-ci ildə ABŞ hökuməti tərəfindən rəsmi standart kimi təsdiq olunmuşdur. DES üçün yararlı olan blokun tutumu 64 bitə bərabərdir. Alqoritmin əsasını 56 bit

uzunluğa malik 16 dövrlü (raundlu) və açarlı Feystel şəbəkəsi təşkil edir. Alqoritm xətti və qeyrixətti çevrilmələrin kombinasiyası üçün istifadə edilir. 1972-ci ildə ABŞ hökumətinin kompüter təhlükəsizliyinə olan ehtiyacı araşdırılır. Amerika "Milli Standartlar Bürosu" (indiki zamanda NIST adlanır) ümumi hökumət standartında qeyri-tənqidilik informasiyasının şifrələnməsini müəyyənləşdirir. Milli Standartlar Bürosu Milli Təhlükəsizlik Agentliyi (MTA) ilə apadığı məsləhətləşmə nəticəsində belə qərara gəlir ki, şifrin yaradılması üçün müsabiqə elan etsin. Müsabiqənin 15 may 1973-cü ildə başlaması nəzərdə tutulur. IBM firmasi müsabiqəyə "Lüsifer" adlı şifrəni təqdim edir. Müsabiqəyə təqdim olunan bütün şifrələrin heç biri müsabiqənin tələblərini ödəmir. 1973-1974-cü illərdə IBM firması H.Feystelin alqoritminə əsaslanaraq yeni şifrəni müsabiqəyə təqdim edir (şifrə yenə də "Lüsifer" adlandırılmışdı). Bu dəfə təqdim edilən şifrə juri tərəfindən qəbul edilir. 17 may 1975-ci ildə DES alqoritmi "Federal reyestr" tərəfindən nəşr edilir.

DES alqoritmini həddindən artıq uzun müddətə və böyük xərc tələb etməklə "sındırmaq" mümkün idi. Bunun nəticəsidir ki, DES alqoritmi nəhayət ki, 39 gün ərzində on minlərlə kompüterdən ibarət şəbəkənin köməyilə "sındırılır". İnternet şəbəkəsində şəxslərə məxsus gizli məlumatlar və informasiya təhlükəsizliyi ilə məşğul olan "EFF" ictimai təşkilatı bu problemi araşdırmaq üçün dəyəri 25 000 dollar olan kompüter yaradır və 1988-ci ildə DES üsulu ilə şifrələnmiş verilənləri üç gün ərzində 56 bitlik açardan istifadə etməklə şifrədən azad edə bilir. Superkompüter "EFF DES Cracker" adlandırılır. Sonrakı illərdə RSA Laboratory apardığı təcrübələrə əsaslanaraq daha güclü kodların da açılmasının mümkünlüyünü sübut edir. Aşağıda şifrənin açılmasını əks etdirən sxem verilmişdir.

BLOK ŞİFRƏLƏRİNİN FƏALİYYƏT REJİMİ

Şifrələmənin simmetrik alqoritmini iki kateqoriyaya bölmək olar: blok və arası kəsilməyən. *Arası kəsilməyən* alqoritmdə ilkin mətnin simvolları (baytlar və ya bitlər) ardıcıl şifrələnir. Buna klassik nümunə birdəfəlik bloknot və ya sadə dəyişmə şifrəsini göstərmək olar. Blok şifrələnmədə şifrələmə vahidi kimi blokdan (qeyd olunmuş bitlər ardıcıllığı) istifadə edilir ki, o da eyni uzunluqda olan şifrələnmiş mətn blokuna çevrilir.

Blok şifrələmənin müxtəlif sahələrdə optimal istifadə olunan əsas dörd iş rejimindən istifadə edilir.

1.*Elektron şifrələmə kitabı rejimi (ECB)*. Sadə və təbii üsuldur. Mətn bloklara bölünür və hər bir blok eyni açarla şifrələnir. Əsas çatışmazlığı ondan ibarətdir ki, eyni bloklar eyni şifrələndiyi üçün mühafizəni zəiflədir (böyük həcmli informasiya şifrələndikdə eyni hal baş verir).

2.*Şifrələnmiş blokların qoşulma rejimi (CBC)*. Aşıq mətnin hər bir bloku şifrələnmədən öncə XOR əməliyyatının köməyilə növbəti şifrələnmiş mətnin blokları ilə bir-birinə bağlanılır (qoşulur). Birinci blok öncədən məlum olan ***installyasiya***

olunmuş vektor ilə birləşir. Nəticədə açıq mətnin şifrələnmiş eyni blokları bir-birindən fərqlənirlər.

3.*Şifrələnmənin əks əlaqə rejimi (CFB)*. Burada əsas məqsəd blok şifrələnməsini (məsələn, 64 bitlik uzunluğa malik blok - DES) bir simvola görə şifrələnən (məsələn, ölçüsü j=8 bit – CBC) blokların qoşulma rejiminə çevirməkdir. İdeya ondan ibarətdir ki, ilkin olaraq 64 bitlik bufer installyasiya olunmuş, K açarı ilə şifrələnmiş vektorla doldurulur (göndərənə və qəbul edənə məlum olan). Alınmış nəticədən böyük (sol) j bit seçilir və açıq mətnin birinci simvolu ilə XOR əməliyyatının köməyilə birləşdirilir. Nəticədə ilk şifrələnmiş simvol alınır. Sonrakı mərhələdə buferdə yerləşən (installyasiya olunmuş, K açarı ilə şifrələnmiş vektor) j bit sola çəkilir, ən kiçik (sağ) j bit -ə şifrələnmiş simvol yazılır. Bununla da sistem növbəti simvolun şifrələnməsinə hazır olur.

4.*Çıxışa görə əks əlaqəli rejim (OFB)*. İş prinsipi öndəkinə eynidir. Burada, buferdəki kiçik j bit -in sürüşməsindən sonra yerinə şifrələnmiş simvol deyil, şifrələnmiş böyük j bit simvol yazılır. Belə rejim maniəyə davamlıdır, yəni mətnin şifrələnmiş bir simvolunun ötürülməsi zamanı yaranmış kəsilmə digər simvolların şifrələnməsinə təsir etmir.

AÇIQLAMA: *İnstallyasiya* (ingiliscə installation - hərfi mənası qurulma, quraşdırma, düzəldilmə, təsis edilmə deməkdir) – sonuncu kompüter istifadəçisinin kompüterinə proqram təminatının qurulma prosesidir. Əməliyyat sistemində olan xüsusi proqramla (menecer paketi) yerinə yetirilir (məsələn, RPM и APT в GNU/Linux, Windows Installer в Microsoft Windows).

SKREMBLERLƏR

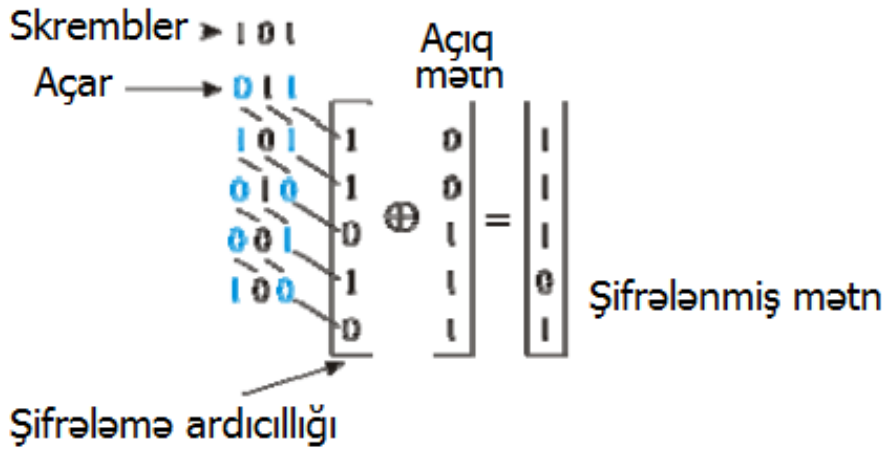
Geniş yayılmış axınlı alqoritm şifrələməsinin bir növü *skrembler* sayılır. *Skrembler* kəsilməz informasiya axınının bitlərlə şifrələnməsinə imkan verən alqoritmin proqram və ya aparat realizəsidir. Skrembler bitlər toplumudur və müəyyən alqoritmin hər bir addımında dəyişir. Hər bir yerinə yetirilən addımdan sonra onun çıxışında şifrələmə biti – 0 və 1 əmələ gəlir. Şifrələmə biti XOP əməliyyatı vasitəsilə informasiya axınının cari biti ilə üst-üstə düşür.

Sadə skremblerə nümunədə baxaq. Skrembler eyni uzunluğa malik iki bit ardıcıllığı ilə verilir, onlardan biri *açar* (başlanğıç ardıcıllıq), ikinci isə skrembler adlanır (əksər hallarda ardıcıllıq konkret aparat və proqram realizasiyası üçün fiksə olunur, amma açar isə adi simmetrik şifrələmə kimi seçilir). Açarın uzunluğu artdıqca (həmçinin skremblerin) alqoritm bir o qədər etibarlı olur.

Başlanğıc ardıcıllıq (açar) skrembler ilə toplanır və *maska* əmələ gətirir. Maskada ardıcıllığın ancaq o bitləri seçilir ki, onların pozisiyaları (mövqeləri) skremblerdəki vahidlərə uyğun gəlir. Sonrakı mərhələdə seçilmiş bitlər öz aralarında XOR əməliyyatı ilə toplanır. Yeni bit alınır və o açarın başlanğıcına (sol tərəfinə) yazılır. Axırıncı (sağdakı) bit isə açarın birinci bitinə çevrilir, ardıcıl simvolla kodlanır və atılır. Beləliklə, açarın sürüşməsi və bitlərdən birinin generasiyası baş verir. Generasiya olunan bit ilkin mətnin birinci biti ilə XOR əməliyyatı nəticəsində toplanır və şifrələnmiş mətnin birinci biti alınır. Bundan sonra dövr təkrarlanır.

Tutaq ki, 00111 məlumatını 011 açarlı 101 skrembleri ilə şifrələmək lazımdır. 2 modula uyğun cəm açarın birinci və üçüncü biti hesablanır: $1 \oplus 1 = 0$. Bu bit açarın yeni birinci biti

olacaqdır. Açarın sonuncu biti (1) şifrələmə ardıcıllığının bitinə çevriləcəkdir. Şifrələnmiş mətnin birinci bitini hesablayaq: $1 \oplus 0 = 1$. Sonra isə prosesi 101 açarı ilə təkrarlayaq. Məlumatın tam şəkildə şifrələnməsi 12 saylı şəkildə verilən kimidir.



Şəkil 12. 011 açarlı 101 skrembleri ilə 00111 ardıcıllığının skremblerlənməsi

Kriptoanalizin klassik məqsədi – açardan istifadə etmədən açıq mətndən şifrələnmiş mətn almaq (bəzən bunu açarın axtarılması da adlandırırlar).

Kriptotəhlinin ayrı-ayrı üsulları vardır ki, onlardan istifadə etməklə müasir şifrələri "sındırmaq" olur. Onlardan bəzilərinə nəzər salaq.

Statistik kriptoanaliz. Kriptotəhlil şifrələnmiş mətndə tez-tez rast gəlinən ayrı-ayrı simvolların (və ya simvollar qrupunun) sayılmasına əsaslanır. Əsasən simmetrik dayaqlıq alqoritminin sındırılması üçün istifadə olunur.

Differensial kriptitəhlil. Kriptotəhlil seçilmiş mətn ilə həyata keçirilir. Müasir simmetrik şifrələmə alqoritminin sıdırılmasında istifadə edilir, bu zaman mətn ardıcıl olaraq bir neçə çevrilmə ranudundan keçir. Üsul iki mətn arasında olan oxşarlığın dəyişilməsinin izlənməsinə əsaslanır.

Xətti kriptotəhlil. Simmetrik blok şifrələrinin sındıdılmasında istifadə olunur. Kriptotəhlilin əsasını xətti yaxınlaşma anlamı təşkil edir.

SİMMETRİK ALQORİTMLƏRİN PROBLEMLƏRİ

Bütün simmetrik alqoritmlər ümumi bir problemə malikdir, yəni məlumatı göndərən və qəbul edən eyni bir açardan istifadə etməlidir. Bununla yanaşı nəzərə alınır ki, onların etibarlı əlaqə kanalları yoxdur, əks halda məlumatı şifrələməyə ehtiyac olmazdı.

Yüz il bundan əvvəl bu problem sadə şəkildə həll edilirdi, məlumatı göndərən şəxs ilə qəbul edən şəxs üzbə-üz görüşərdilər. İndiki zamanda bu mümkün deyil. Bu baxımdan müxtəlif ölkələrdə yaşayan işgüzar tərəfdaşlar məlumatın konfidensiallığına çalışırlar.

İnternet-bankinq işgüzar insana mənzilindən və ya ofisindən kanara çıxmadan ona məxsus bank hesablarının idarə edilməsini, müştərilər ilə əməkdaşlığı yerinə yetirməyə və s. həyata keçirməyə imkan verir. Şifrələnmiş açarlardan istifadə edənlər şifrələri mütamadi dəyişir, bununla da şifrələmənin etibarlığını tutarlı səviyyədə artırırlar.

Deməli, simmetrik şifrələmə üçün *açarların dəyişilmə problemi* xarakterikdir. İndiki zamanda müəyyən sayda üsulların köməyilə bu problemi aradan qaldırmaq mümkündür.

Bununla yanaşı istifadəçinin çoxlu sayda açarları idarəetmə problemi də ortaya çıxır. Əgər n sayda insan məlumatı konfidensial şəkildə mübadilə edirsə, onda $O(n^3)$ açar lazım gələcəkdir (n-1 açar hər bir şəxsə). Əgər qrup bir açardan istifadə edəcəksə, onda informasiyanın kanara axması bir şəxsin əli ilə olar və bütün qrupun adına yazıla bilər.

Bu problemlər XX əsrdə yeni sinif şifrələmə alqoritmlərinin yaradılmasına səbəb oldu.

YOXLAMA TESTLƏRİ

1.Təsdiq edilmişlərdən hansının Pleyfeyr şlfrəsinə aid olduğu düzdür?

A.Pleyfeyer şifrəsi monoəlifbalı şifrəyə aiddir;

B.Pleyfeyr şifrəsi dayaqlıq şifrəsinə aiddir;

C.Pleyfeyr şifrəsində şifrələmə vahidi biqrammdır;

D.Pleyfeyr şifrəsini izafə açar üsulundan istifadə etməklə sındıranda onun zəif cəhətləri hansılardır.

2.Verilmiş 01010 məlumatını 011 açarlı 101 skrembleri ilə şifrələyin.

3.Monoəlifbalı şifrələmənin əsas zəif cəhəti nədən ibarətdir?

A.Çoxda böyük sayda olmayan açarlardan (izafə zəiflik) istifadə edilməsində;

B.Şifrələnən mətn açıq mətnin statistik xüsusiyyətlərini saxlayır;

C.Əgər iki mətn eyni açarla şifrələnərsə, onda şifrə avtomatik olaraq aşkara çıxır;

D.Bədniyyətli şəxs kifayət qədər açıq və şifrələnmiş nümunələrə malik olduqda açarı tapa bilər.

4.”КНИГА” sözünü 12 açarlı Qronsfeld şifrəsindən istifadə etməklə şifrələyin.

5.”КНИГА” sözünü Sezar şifrəsinin köməyilə şifrələyin.

6.Hill şifrəsini sındırmaq üçün kriptotəhlilin hansı üsulu daha effektivdir?

A.Seçilmiş mətn ilə təhlil;

B.Seçilmiş şifrələnmiş mətn ilə təhlil;

C.Seçilmiş açıq mətn ilə təhlil;

D.Məşhur açıq mətn ilə təhlil;

E.Ancaq şifrələnmiş mətn ilə.

7.Simmetrik şifrələmə nə anlamını verir?

A.İlkin məlumatın hər bir simvolunun (və ya simvollar ardıcıllığının) digər simvolu ilə (və ya simvollar ardıcıllığı ilə) əvəz edilən şifrələmə üsulu;

B.Eyni bir açar həm mətnin şifrələnməsində, həm də ki, deşifrələnməsində istifadə edilir;

C.Mətnin şifrələnməsində bir açar, deşifrələnməsində digər açar istifadə olunan şifrələmə üsulu;

D.Açardan istifadə olunduqda açıq mətnin simvolları ardıcıllığını dəyişən şifrələmə üsulu.

8.Adaları çəkilən hansı şifrə ən etibarlı sayıla bilər?

A.Pleyfeyer şifrəsi;

B.Hill şifrəsi;

C.Birdəfəlik bloknot;

D.Sezar şifrəsi;
E.Monoəlifbalı şifrə.

9.Müasir simmetrik alqoritmlərin xüsusiyyələrti necə adlanır: açıq mətnin hər bir biti şifrələnmiş mətnin hər bir bitinə necə təsir göstərir?

10.Simmetrik alqoritmlərdən istifadə zamanı yaranmış problem nə ilə əlaqədardır?
A.EHM-lərdə realizə olunmasının mürəkkəbliyi ilə;
B.EHM-lərin istifadəyə buraxıldığı andan istifadə edilən şifrələrin kriptotəhlil edilməsinin asanlığı ilə;
C.Açarların kiməsə verilməsi və açarların idarə edilməsi zamanı yaranan çətinliklər ilə;
D.Bu alqoritmlərin EHM-lərdə istifadə edilməsi zamanı çoxlu sayda hesablama resurslarının tələb olunması ilə.

11.İstifadə olunan mətn bloklara bölünəndə və bu bloklar eyni açarla şifrələnəndə blok şifrələrinin şifrələnmə rejimi necə adlanır?
A.Şifrələnmiş blokların bir-birinə bağlanması rejimi;
B.Əks əlaqə ilə şifrələnmə rejimi;
C.Çıxışa görə əks əlaqə rejimi;
D.Elektron şifrələmə kitabı rejimi.

AÇIQLAMA: *Kriptoqrafiya* (yunanca *gizli yazıram anlamını* verir) məxviliyin (informasiyanın kənar şəxs tərəfindən oxuna bilməməsi), tamlıq (informasiyanın hiss olunmayacaq qədər dəyişdirilə bilinməməsi), autentifikasiya (müəllifin və ya obyektin xüsusiyyətlərinin həqiqiliyinin

yoxlanması), həmçinin müəlliflikdən imtina edilməsinin mümkün olmaması anlamını verir.

İlk olaraq kriptoqrafiya informasiyanın şifrələnməsi üsullarını öyrənirdi. Ənənəvi olaraq kriptoqrafiya simmetrik kriptosistem əmələ gətirir, yəni bu sistemdən istifadə etməklə şifrələnmə və ya şifrədən azad olma bir açarın köməkliyi ilə həyata keçirilir. Bundan başqa müasir kriptoqrafiya özündə assimmetrik kriptosistemi və elektron rəqəmsal imza sistemini (ERİ), xeş-funksiyanı, açarlarla idarə etməni, gizli informasiyanın alınmasını, kvant kriptoqrafiyanı əks etdirir.

Kriptoqrafiya haqqında verilmiş qanun abonentlərin şantaj olunması və ya abonentin satın alınması, onun aldanılması, mənzilinin və ya avtomobilinin açarının oğurlanması, onun həyatını təhlükə altına alan hədələrin həyata keçirilməsi, müdafiə edilən verilənlər bazasından informasiya alarkən ona edilmiş təhlükə və s. hallar baş verdikdə subyektin müdafiəsi ilə məşğul olmur. Kriptoqrafiya qədim elm sahələrindən biridir, onun yaranma tarıxı bir neçə min illər əvvələ (təxminən 4 min il əvvələ) gedib çıxır.

Kriptoqrafiyadan istifadənin birinci dövründə (təxminən 3 min il əvvəl) şifrələnmə üçün monoəlifbadan (yazıda istifadə edilən hərflərin digər hərflər və ya simvolar ilə əvəz edilməsi) geniş istifadə olunurdu.

Kriptoqrafiyadan istifadənin ikinci dövründə (IX əsrdən başlayaraq Yaxın Şərqdə dövrünün görkəmli alimi abu Yusif Yaqub ibn İshaq əl-Kindi), XV əsrdən başlayaraq Avropada (Leon Battista Albert - XX əsrin sonlarına kimi) şifrələmə üçün çoxəlifbalıqdan geniş istifadə edilməyə başlanıldı.

Kriptoqrafiyadan istifadənin üçüncü dövründə (XX əsrin başlanğıcı və XX əsrin ortalarına kimi) şifrələmə

əməliyyatlarını yerinə yetirmək üçün elektromexaniki qurğulardan istifadə olundu. Bu məqsədlə qurğuları işlətmək üçün şifrələyici mütəxəssislər işə qəbul edilirdi. İnformasiyanın şifrələnməsi zamanı çoxəlifbaliq sisteminə daim mürəciət edilirdi.

Lorenz alman kriptomaşını, gizli məlumatların şifrələnməsi üçün İkinci Dünya Müharibəsində istifadə olunmuşdur

Gizli məlumatların şifrələnməsi üçün istifadə olunan kriptoqrafiya maşını

Kriptoqrafiya aləti

İnformasiyanın şifrələnməsinə nümunə kimi İkinci Dünya Müharibəsində istifadə edilən ENİQMA hesablama maşınından istifadəni göstərmək olar.

Kriptoqrafiyadan istifadənin dördüncü dövrü (XX əsrin ortalarından keçən əsrin 70-ci illərinə kimi) riyazi kriptoqrafiyaya keçid dövrü adlanır. Görkəmli alim K.Şennon əsərlərində informasiyanın ölçülməsi, verilənlərin ötürülməsi, entropiya, şifrələmə funksiyası kimi terminlərdən istifadə edir və bu terminləri sonralar elmə daxil edir. Şifrələnmiş informasiyanın müəyyənləşdirilməsi üçün "xətti differensial kriptoanaliz"dən istifadə olunmağa başlanılır. Bütün bunlara baxmayaraq 1975-ci ilə kimi kriptoqrafiyada "klassik" üsillardan istifadə olunurdu.

Kriptoqrafiyanın müasir dövrdə inkişafı (keçən əsrin 70-ci illərinin sonundan inkidiki zaman kimi) bu sahədə yeni istiqamətin – açıq açar prinsipli kriptoqrafiya - yaranmasına səbəb oldu. Müasir sahənin yaranması təkcə yeni texniki qurğulardan istifadə ilə deyil, həmçinin kriptoqrafiyadan fərdi şəxslərin istifadəsilə də bağlı oldu (əvvəlki dövrlərdə kriptoqrafiyadan ancaq dövlət səviyyəsində istifadə olunurdu). İnsanların şəxsi məqsədləri üçün kriptoqrafiyadan istifadə etməsi müxtəlif ölkələrdə müxtəlif cür qarşılanır, bəzi ölkələrdə buna qadağa qoyulsa da, bəzi ölkələrdə buna geniş imkanlar yaradılır.

Müasir kriptoqrafiya müxtəlif elmi istiqamətlər (riyaziyyat elminin informatika elmi ilə kəsişməsində) yaratmışdır. Bu barədə elmi jurnallarda mütamadi məqalələr çap edilir. Kriptoqrafiyadan istifadə müasir cəmiyyətin ayrılmaz bir hissəsinə çevrilmişdir. Ondan elektron kommersiyada, elektron sənəd dövriyyəsində, rəqəmsal imzada, telekommunikasiya sahəsində və digər sahələrdə

geniş istifadə olunur.

Müasir kriptoqrafiyada şifrələmənin açıq alqoritmindən istifadə edilir. İndiki zamanda sınaqdan çıxmış onlarla alqoritm istifadə edilir. Belə alqoritmlərə misal kimi aşağıdakıları göstərmək olar:

- Simmetrik DES, AES, DÜST 28 147-89, Camellia, Twofish, Blowfish, IDEA, RC4 və s.;
- Asimmetrik RSA və Elqamai (El-Qamal);
- Xeş-funksiya MD4, MD5, MD8, SHA-1, SHA-2, DÜST R 34.11-94 və s.

Bir çox ölkələrdə standart milli şifrələmədən istifadə olunur. 2001-ci ildə ABŞ-da AES (Rindael alqoritminə əsaslanan, açarın uzunluğu 128, 192 və 256 bit olan) standart simmetrik şifrələmədən istifadə edilir. Rusiya Federasiyasında DÜST 28 147-89 standartına üstünlük verilir.

Əbu Yusif Yaqub ibn İshaq əl-Kindi (elm aləmində əl-Kindi kimi məşhurdur) ərəb filosofu, riyaziyyatçı, musiqi nəzəriyyəçi, astronom kimi tanınır. İraqın Bəsrə şəhərində (bəzi məlumatlara görə Kufə şəhərində) anadan olmuşdur. Mühəmməd ibn Musa əl-Xorezmi tərəfindən Bağdadda təşkil olunmuş "Müdriklər evi"n-də keçirilən tədbirlərdə iştirak etmiş, orada elmi işlər ilə məşğul olmuşdur. Bağdada rəhbərlik edən əl-Mamunun (813-833-ci illər) və əl-Mutasimin (833-842-ci illər) əziz (istəkli) adamlarından biri olmuşdur. Sonrakı illərdə (əl-Mütavəkkilin rəhbərliyi dövründə) daim şəhərdən-şəhərə qovulmuş, təqib olunmuş, daim axtarışda olmuşdur. əl-Kindi metafizika elmində çoxlu sayda traktatların müəllifidir. Bununla yanaşı məntiq, etika, riyaziyyat, kriptoqrafiya, astrologiya, təbabət, metrologiya, optika, musiqi kimi elm sahələri ilə dərindən məşğul olmuş, bu elm sahələrinə dəyərli töhvələrini vermişdir. Alimi Qərbi

Avropada Alkindus kimi tanıyırlar.

əl-Kindi islam aləmində Aristotelin əsərlərinə müraciət edən ilk alimdir. Aristotelin əsərlərindən qaynaqlanan alim peripatetizmin (materializm ilə idealizm arasında tərəddüd edən qədim yunan filosofu Aristotelin nəzəriyyəsi) əsasını qoyur. Bu ərəfədə alim "Aristotel əsərlərinin xülasəsi", "Beş mahiyyət haqqında", "Yaranmanın və məhv olmanın əsas səbəbləri", "Əşyaların müəyyən edilməsi və təsvir edilməsi" əsərlərini yazır.

Aristotelin əsərlərini təhlil edən alim belə nəticəyə gəlir ki, "qədim (köhnə) heç bir zaman mövcud olmayan ola bilməz". Köhnənin var olması heç bir şeydən asılı deyil, əgər onun məhv olması üçün bir səbəb yoxdursa, o, məhv olmayacaq və dəyişməyəcək, çünki o cisim deyil. Alim kəmiyyətin keyfiyyətə keçməsində əvvəli olmayanları materiya adlandırır. Bununla yanaşı alim qeyd edir ki, əsası və atributu olmayan (fəlsəfədə substansiyanın ayrılmaz xüsusiyyəti, ayrılmaz cəhəti, məsələn, hərəkət materiyanın atributudur), səbəbsiz, əsli olmayan, vaxtından qabaq dəyişməyən, bütün bunları insan düşüncəsi anlaya bilməz, bunlar tədqiqat obyekti ola bilməz, deməli fəlsəfə mövzusuda ola bilməz, çünki fəlsəfə ancaq olanların təbiətini dərk edə bilir.

əl-Kindi "Hind cəbrinin tətbiqi", "Ədədlərin harmoniyası", "Rəqəmlər baxımından vahidlik", "Bərabəryanlı çoxbucaqlılar", "Dairənin iki nöqtəsini birləşdirən düz xəttin – xordanın təxmini hesablaması", "İzoperimetrik məsələlər haqqında", "Sonsuz ədədlərin və paralel xətlərin bölünməsi haqqında", "Kriptoqrafik məlumatların deşifrələnməsi haqqında", "Kürə daxilində qurulanlar haqqında", "Kürənin müstəvi üzərində layihələnməsi haqqında", "Günəş

saatlarının qurulması", "Yerdən Aya qədər olan məsafənin təyin edilməsi", "Səmada baş verənlər haqqında", "Planetlərin hərəkəti" və s. bu kimi sanballı əsərlərin müəllifidir.

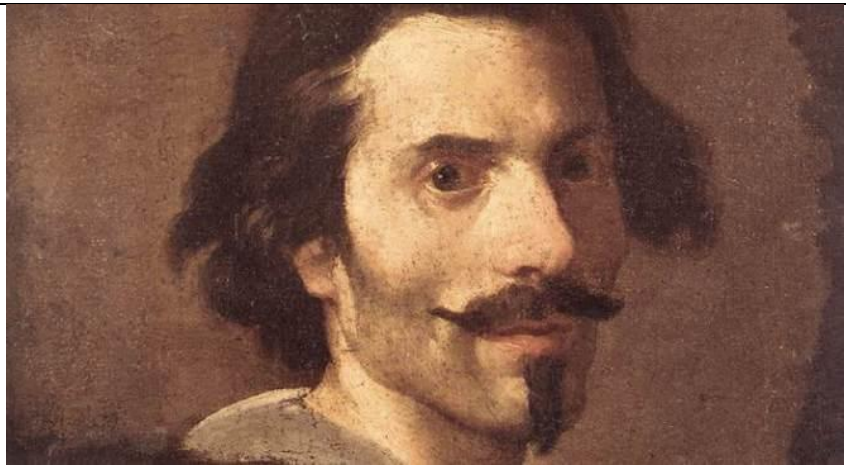
əl-Kindi harmoniya haqqında qədim əlyazmanı tərcümə etmiş və müsiqi səsləri arasında olan intervalın ədədlərlə bağlılığını göstərmişdir. O, ilk dəfə olaraq Şərqdə, ərəb hərflərindən istifadə etməklə müsiqini nota almışdır. Alim bu sahədə bir neçə elmi əsər yazmışdır. Bunlara "Melodiya və səs haqqında", "Melodiyanın tərtib edilmə təcrübəsi", "Ritm haqqında", "Musiqinin əsas bölmələri", "Musiqi mövzusunun bir neçə səs tərəfindən ardıcıl surətdə təkrar edilməsinin bölünməsi haqqında" və digər əsərləri göstərmək olar.

əl-Kindi Pifaqor ideyalarına əsaslanan musiqi nəzəriyyəsindən istifadə etməklə musiqi sənəti ilə makrokosmosda (kainatda, dünyada, aləmdə) və mikrokosmosda (kiçik kəmiyyətlər aləmində, atomlar aləmində) baş verən çoxlu sayda hadisələr arasında olan əlaqəni göstərmişdir.

Alim musiqi aləti udun simlərinin sayını (Ud musiqi alətində dörd sim vardır) su, torpaq, hava və od ilə, dünyanın dörd istiqaməti (şimal, cənub, şərq və qərb) ilə, ilin dörd fəsli (yaz, yay, payız və qış) ilə, bədəndəki mayenin (qan, soyuqqanlılıq, qara və sarı öd ifrazı) və başqaları ilə bağlılığını elmi surtədə əsaslandırmışdır. Bununla yanaşı musiqidə olan yeddi səsin (notun) Kainatda olan yeddi planetə, ud alətindəki oniki elementi isə (dörd sim, dörd burağac (aşıq) və dörd pərdə) 12 bürcə uyğunluğunu əsaslandırmışdır.

əl-Kindi "Şüalar haqqında", "Yandırıcı güzgülər haqqında", "Səmanın mavi rəngdə olmasının səbəbi",

"Qabarmanın və çəkilmənin səbəbləri", "Qarın, ildırımın, dolunun, tufanın, göy gurultusunun səbəbləri haqqında", "Yağış, leysan və külək haqqında", "Farmakologiya (dərmanların bədənə təsirindən bəhs edən elm) haqqında", "Ətirli və distilə edilənlərin kimyası haqqında" əsərlərin müəllifidir. Alim sonuncu əsərində 100-dən çox ətirli yağların, balzamların, ətirli suların və qiymətli dərmanların imitasiyasının reseptini vermişdir. Bunlarla yanaşı kitabda ətirlərin yaradılmasının 107 üsulu və resepti verilmiş, bu məqsədlə istifadə olunan çoxlu sayda avadanlıqların istifadə olunma qaydaları göstərilmişdir.

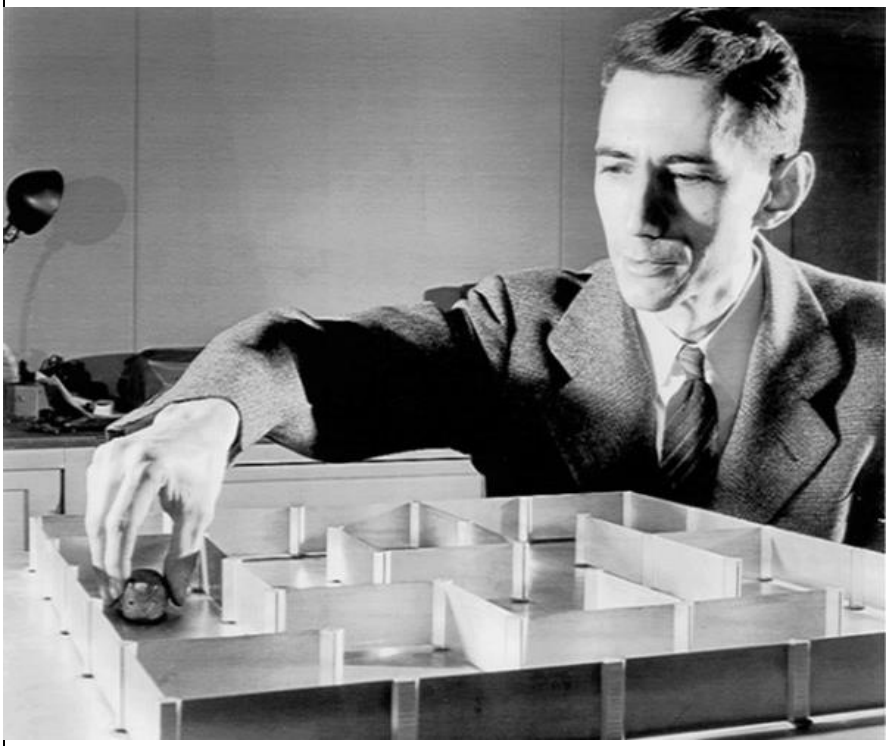


Leon Battista Alberti (italyanca Leone Battista Alberti: 1404-1472), italiyalı alim, humanist, yazıçı, yeni avropa memarlıq üslubunun təşəbbüskarlarından biri, intibah dövrü ilə bağlı mədəniyyətin aparıcı nəzəriyyəçilərindən biridir. L.B.Alberti ilk olaraq istiqbal (gələcək) ilə riyaziyyatın

əsaslarının əlaqəsi nəzəriyyəsini şərh etmişdir. Bununla yanaşı kriptoqrafiyanın inkişafı ilə bağlı 1466-cı ildə yazdığı "Rəqəmlər haqqında traktat" əsərində məlumatların şifrələnməsi üçün çox saylı əlifbadan istifadəni göstərmişdir.

L.B.Albert İtaliyadan Qeniyaya qovulmuş, tanınmış florensiyalı bir ailədə anadan olmuşdur. Universiteti bitirdikdən sonra kardinal Alberqatinin dəftərxanasında işləmiş, sonralar isə ömrünün axırına kimi Romada yaşamışdır. Leon Albertin çoxsahəli fəaliyyəti onu göstərir ki, alim İntibah dövründə hər bir sahə ilə maraqlanan bir alim olmuşdur. Bunun nəticəsidir ki, o, incəsənət, ədəbiyyat və arxitektura (memarlıq) sahələri ilə məşğul olmuş, bu sahələri dərindən araşdırmaqla bu sahələrə öz tövhələrini vermişdir. Alim etika və pedaqoqika problemləri ilə maraqlanmış, riyaziyyat və kriptoqrafiya ilə məşğul olmuşdur. L.Albertinin elmi araşdırmalarında mərkəzi yerlərdən birini təbiətdə baş verən qanunauyğunluqların harmoniyası tutur. Onun fikirincə insan elmi işlərlə məşğul olduğu zaman öz fikirlərinə qapanmamalı, əldə etdiyi nəticələri yaymalı və digərlərinində bu nəticələrdən müxtəlif sahələrdə istifadə etməsinə şərait yaratmalıdır. Görkəmli mütəfəkkir və istedadlı yazıçı L. Alberti kübar (aristokrat) və ortodoks (bir məsləkin sabit və ardıcıl tərəfdarı olan şəxs) bir insan kimi bütün bunların əleyhinə çıxaraq insanda elmi baxımdan baş verə biləcək hümanitar ardıcıllığı araşdırır və onun insan həyatına necə təsir etməsi yollarını elmi əsaslarla təklif edir. Onun fikirincə yaratdığın sənə aiddir, amma sən istər dini baxımdan, istərsə də insanı baxımdan bütün yaratdıqlarını hamının malı etməlisən. Alimin araşdırdığı və kitab şəkilində çap etdirdiyi elmi işlər indiki zamanda da müəyyən məsələlərin həllində istifadə olunur.

Klod Elvud Şennon 30 aprel 1916-cı ildə ABŞ-ın Miçiqan ştatında anadan olmuşdur, 24 fevral 2001-ci ildə ABŞ-ın Massaçusets ştatındakı Medford şəhərində dünyasını dəyişmişdir. K.E.Şennon amerikalı mühədis və riyaziyyatçıdır.



Alim informasiya nəzəriyyəsinin yaradıcısıdır, o, ehtimal nəzəriyyəsinə, avtomatlar nəzəriyyəsinə və idarəetmə sistemləri nəzəriyyəsinə böyük tövhələr vermişdir. K.Şennon

1948-ci ildə informasiyanın ölçülməsi üçün "bit" ölçü vahidindən istifadəni təklif etmişdir. 1932-ci ildə Miçiqan universitetinə daxil olduqdan sonra C.Bul ilə elmi işlərin aparılmasında iştirak etmişdir. Universiteti bitirdikdən sonra görkəmli alim Vannevar Buş ilə birgə elmi araşdırmalarda iştirak etmişdir. 1937-ci ildə maqistraturada oxuduğu zaman yazdığı "Rele və kommutatorların simvol təhlili" adlı elmi məqaləsi 1938-ci ildə "Amerika mühəndisləri institutu" jurnalında çap edildikdən sonra o, çap etdirdiyi elmi məqaləyə görə "Alfred Nobel" mükafatına layiq görülür.

Alimin apardığı elmi araşdırmalar XX əsrin ən vacib elmi işləri sayılır. K.E.Şennon 1940-cı ildə "Nəzəri genetika üçün cəbr" adlı doktorluq dissertasiyasını müdafiə edir. 1950-1956-cı illərdə alim məntiqi maşının yaradılması ilə məşğul olur. Onun hazırladığı məntiq maşını şaxmat oynaya bilirdi. 1950-ci ildə təqaütə çıxdıqdan sonra daim Bell laboratoriyası ilə elmi məsləhətləşmələri həyata keçirir. Klod Elvud Şennon dövrünün ən görkəmli alimlərindən biri sayılır.

AÇIQ AÇARLA ŞİFRƏLƏMƏ. ELEKTRON RƏQƏMSAL İMZA

AÇIQ AÇARLA ŞİFRƏLƏMƏ ALQORİTMİ

Açıq açarla şifrələmə alqoritmində hər bir istifadəçi bir cüt açara malikdir və bu açarlar bir-birilə bəzi asılılıqlarla bağlıdırlar. Açarlarda bu xüsusiyyətlər vardır: *bir açarla şifrələnən mətn, bir cüt açarla şifrələnən mətn*. Bir açarı *gizli (bağlı) açar* adlandırırlar. İstifadəşi özünə məxsus gizli açarı etbarlı bir yerdə gizlətməlidir və onu heç kimə etibar etməməlidir. İkinci açar *açıq açar* adlanır və istifadəçi bu açar barədə hamını məlumatlandırmalıdır.

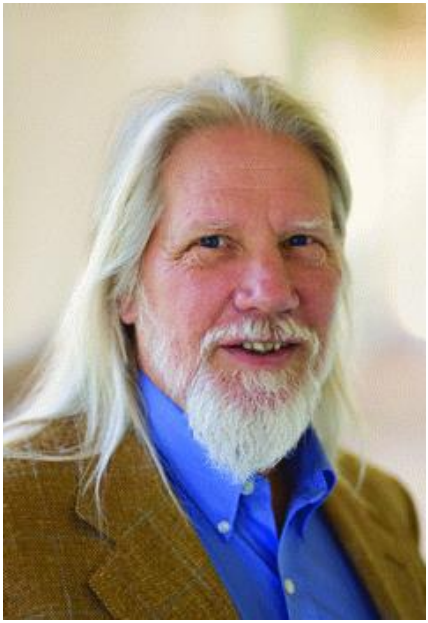
Əgər A istifadəçi B istifadəçiyə şifrələnmiş məlumat göndərmək istəyirsə, onda o həmin məlumatı B açarı ilə şifrələyir. Bundan sonra mətni heç kim (hətta A özü də) oxuya bilməz (B-dən başqa), çünki mətni şifrədən çıxarmaq üçün mütləq ikinci açar - gizli açar lazımdır.

Şifrələmə sxemi aşağıdakı kimidir:

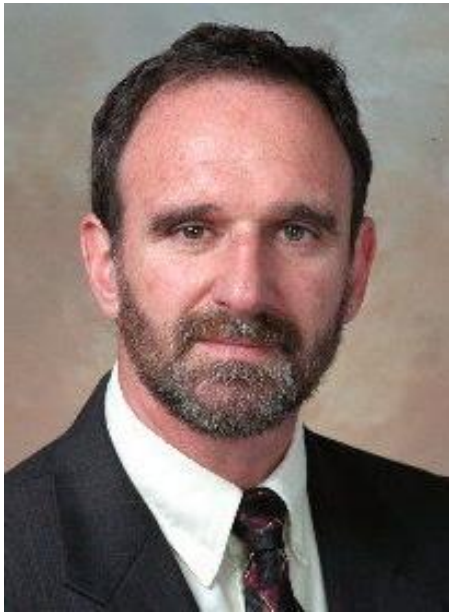
$$M' = E(M, K_{açıq})$$
$$M = D(M, K_{bağlı})$$

burada E – şifrələmə funksiyası (encrypt), D – deşifrələmə funklsiyası (decrypt), $K_{açıq}$ və $K_{bağlı}$ – uyğun olaraq məlumatı qəbul edənin açıq və bağlı (gizli) açarları.

Açıq açarla şifrələmə üsulu Diffi və Helmana məxsusdur (1976-cı il). Buna baxmayaraq onlar konkret alqoritm təklif edə bilmədilər, amma alqoritmin ödəyə biləcəyi prinsipləri və şərtləri formalaşdıra bildilər.



Uitfild Deffi



Martin Hellman

Bu şərtlərə aşağıdakılar aiddir:

1.Açarlar cütlüyünün (açıq və bağlı) generasiya prosesi hesablama çətinliyi yaratmamalıdır;

2.Mətnin şifrələnmə prosesi, yəni E (M, $K_{açıq}$) və deşifrələnmə prosesi D (M, $K_{bağlı}$) hesablama çətinlikləri yaratmamalıdır;

3.Düşmənin $K_{bağlı}$ açarı haqqında məlumatı olmamalıdır (əgər onda $K_{açıq}$ açarı haqqında məlumat olsada belə);

4.Düşmən **M'** şifrələnmiş mətnə və $K_{açıq}$ açara malik olsada belə, açıq **M** mətnini hesablama imkanı olmamalıdır.

Beləliklə, şifrələmə və deşifrələmə istənilən ardıcıllıqla yerinə yetirilsə də, belə etmək də mümkündür: mətni bağlı açarla şifrələməli, açıq açarla şifrədən çıxarmalı.

RSA alqoritmi.

RSA açıq açarla şifrələmə alqoritmlərindən biridir. Alqoritm 1977-ci ildə Rivest, Şamir və Adleman tərəfindən yaradılmışdır. Alqoritm 20 il ərzində ən populyar sayılmış və açıq açarla istifadə olunan alqoritmlər içərisində praktiki olaraq ən çox istifadə ediləni olmuşdur.

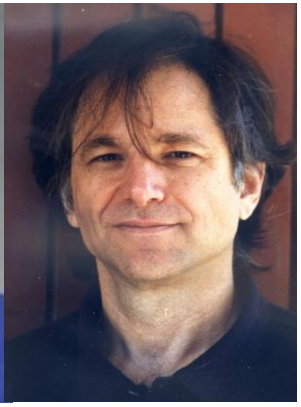
RSA ikilik mətnlərin şifrələnməsi üçün istifadə edilir. Açıq mətn bloklara bölünür və hər bir blok **M** ikilik ədədi kimi götürülür. Bu zaman M<n şərti ödənilməlidir (n=*pq*, burada *p* və *q* iki böyük təsadüfi sadə ədədlərdir).

Açıq və bağlı açarlar RSA alqoritmində bir-birilə əlaqəlidirlər, yəni bir açarın şifrələnməsi o biri açarın şifrədən çıxarılmasına səbəbdir.

Alqoritmin çatışmazlığı əməliyyatı aşağı sürətlə yerinə yetirməsidir. RSA alqoritmində şifrələmə və deşifrələmə əməliyyatları çox böyük tərtibli çox böyük ədədlərin qüvvətə yüksəldilməsi ilə yerinə yetirilir, bu isə öz növbəsində əməliyyatı yerinə yetirmək üçün həcmli resursların olmasını tələb edir.

Bu baxımdan təcrübədə ən çox iki alqoritmin kombinasiyasından istifadə olunur. Məlumat simmetrik alqotmin köməyilə şifrələnir (məsələn, AES), bu zaman hər dəfə təsadüfi açar generasiya olunur. Təsadüfi açar açıq açarla şifrələnir (məsələn, RSA alqoritmi ilə) və məlumat ilə birlikdə göndərilir. Belə hibrid sxem şifrələmə/deşifrələmə əməliyyatının sürətini təmin etməklə yanaşı onun etibarlığını da artırır.





Ronald Rivest *Adi Şamir* *Л. М. Адлеман*

Ronald Linn Rivest (ingiliscə Ronald Linn Rivest: 1947-ci ildə Skenektadi ştatının Hyu-York şəhərində anadan olmuşdur) kriptoqrafiya sahəsində amerika mütəxəssisidir. "Elektrotexnika və kompüter elmləri" fakultəsinin "Kompüter elmləri sahəsində Endri və Ernı Viterbi adına layiq görülmüş professor"udur. "Hesablama nəzəriyyəsi" laboratoriyasının üzvü və "Kritoqrafiya və informasiya təhlükəsizliyi" qrupunun lideridir.

Adi Şamir (6 iyul 1952-ci ildə Tel-Aviv şəhərində anadan olmuşdur) məşhur İsrail kriptotəhlilçisi, hesablama sistemləri nəzəriyyəsi sahəsində alim, Veysman adına institutda "İnformatika və tətbiqi riyaziyyat" sahəsində professor, Alan Türinq adına mükafatın laureatı.

Leonard Maks Adleman (ingiliscə Leonard Adleman-Eydelmen: 31 dekabr 1945-ci ildə anadan olmuşdur) kompüter elmləri sahəsində amerika alimi-nəzəriyyəçisi, Cənubi Kaliforniya Universitetinin kompüter elmləri və molekulyar biologiya üzrə professoru. RSA şifrələmə sisteminin və DNK-hesablamanın həmmüəllifidir.

***AÇIQLAMA**: RSA* (Rivest, Shamir və Adleman soyadlarının abbreviaturasıdır) - böyük tam ədədlərin faktorlaşdırılması məsələlərinin çətinliklə hesablanmasına əsaslanan açıq açarlı kriptoqrafik alqoritmdir. RSA şifrələmə və rəqəmsal yazılar üçün ilk kriptosistemidir. Alqoritm böyük sayda kriptoəlavələrdə istifadə olunur. 1976-cı ilin noyabr ayında Uitfild Diffi və Martin Hellman tərəfindən çap edilmiş "Kriptoqrafiyada yeni istiqamət" məqaləsi kriptoqrafik sistemlər barədə təsəvvürü alt-üst etdi və nəticədə yeni istiqamətin – açıq açarlı kriptoqrafiyanın əsası qoyuldu. Sonralar işlənib təkmilləşdirilmiş Diffi-Hellman alqoritmi müdafiə olunmayan kanaldan istifadə edən hər iki tərəfə ümumi gizli açar əldə etməyə imkan verdi. Amma yaradılmış yeni alqoritm autentifukasiya problemini həll edə bilmədi. Çap olunmuş məqaləni dərindən təhlil edən Massasuçest Texnologiya İnstitutunun alimləri Ronald Rivest, Adi Şamir və Leonard Maks Adleman belə nəticəyə gəldilər ki, U.Diffi və M.Hellman tərəfindən təklif olunan açıq açarlı kriptoqrafik sistemi araşdırmaq üçün mütləq riyazi funksiya tapılmalıdır. 40 yaxın variant araşdırıldıqdan sonra alimlər belə qərara gəldilər ki, araşdırma nəticəsində alınmış funksiyanı RSA adlandırsınlar.

1977-ci ildə "Scientific American" jurnalında Ronald Rivestin icazəsi ilə kriptosistemi aydınlaşdıran ilk məqalə çap edilir. Oxuculara şifrələnmiş alqoritmə malik olan, aşağıda verilmiş rəqəmlər çoxluğundan istifadə etməklə ingilis dilində olan bir cümlənin şifrəsini açmaq təklif olunur.

9686 1477 8829 7431
0816 3569 8962 1829
9613 1409 0575 9874

2982	3147	8013	9451
7546	2225	9991	6951
2514	6622	3919	5781
2206	4355	1245	2093
5708	8839	9055	5154

Ronald Rivestin elan edir ki, verilmiş kodu açmaq üçün 40 kvadrillion il lazımdır. Təxminən 15 il sonra, 1993-cü ilin sentyabr ayında tapmacanın həll olunmasına start verilir. Bir müddət sonra "başsındıran" tapılır. Tapmacada bu sözlər yazılmışdı: "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE"- "Sehirli söz - hər şeydən iyrənən quzuqapan, yırtıcı quş". Mükafata layiq görülən şəxs müəyyən məbləğdə olan pulu proqram təminatının yaradılması fonduna təmənnasız hədiyyə edir. 1982-ci ildə Ronald Rivest, Adi Şamir və Leonard Adleman RSA şirkətini yaradırlar. 1989-cu ildə DES simmetrik şifrəsi ilə birlikdə yaradılmış alqoritm İnternetdə də istifadə olunmağa başlanılır. 1990-cı ildə ABŞ-ın Müdafiə Nazirliyi hərbi işlərdə alqoritmdən istifadə edir. 1997-ci ildə, Hökumət Əlaqələri Mərkəzində işləyən ingilis riyaziyyatçısı Klifford Koks RSA oxşar olan kriptosistemi hazırlayır. Qeyd etmək lazımdır ki, İnternet sistemində RSA alqoritmindən geniş istifadə olunur. Aşağıdakı şəkildə simmetrik şifrələmə sxemi verilmişdir.

ELEKTRON RƏQƏMSAL İMZA

Qeyd edildi ki, çoxlu sayda açıq açarlı şifrələmə alqoritmləri bir-birini əvəz edə biləcək açarlar cütlüyü ilə işləyirlər, yəni bu açarlardan birinin şifrələdiyi mətni digər açar deşifrə etməyə imkan verəcəkdir.

Konfidensiallıq məqsədi ilə mətn məlumatı qəbul edənin açıq açarı ilə şifrələnir.

Məlumatın informasiyanı göndərənin baqlı (gizli) açarla şifrələndiyi halı nəzərdən keçirək. Bu halda həmin mətni kim istəsə şifrədən azad edə bilər, çünki bu halda açıq açar hamıya əlçatandır. Digər tərəfdən məlumatı alan əmin ola bilər ki, məlumatın həqiqi müəllifi məlumatı göndərəndir, yəni bağlı açarın sahibidir, çünki başqa bir şəxs bağlı açarı yarada bilməzdi.

Beləliklə, məlumatın həqiqiliyi (autentikliyi) yaranır. Hüquqi baxımdan məlumatın müəllifi ondan imtina edə bilməz (apellyasiya verə bilməz).

Bu ideya *elektron rəqəmsal imza* konsepsiyasının yaranmasına səbəb oldu.

Rəqəmsal imzalar.

Rəqəmsal imzalar informasiyanın həqiqiliyinə nəzarət etmək üçün elektron formada istifadə edilən güclü alətdir. Rəqəmsal imza elektron verilənlərin tamlığını təmin edir, verilənlərin aktuallığını müəyyən etməklə yanaşı müəlliflik hüququnu da təsdiqləyir. Rəqəmsal imza verilənlərin imzalanması üçün yaradılmış informasiya obyektidir və bu verilənlərin tamlığına və mötəbərliliyinə əmin olmağa imkan verir.

Elektron imza faylda baş verə biləcək xətaların qarşının alınması üçün təhlükəsizliyi müəyyənləşdirən elektron işarəsidir. Elektron işarə faylı yaradanı yoxlamağa və müəyyən etməyə imkan verir. Elektron işarə fayla rəqəmsal imza əlavə edildikdən sonra onda baş vermiş dəyişikliyi müəyyən edir.

Elektron imzanın müxtəlif növləri mövcuddur.

1.*Birləşdirilmiş elektron imza*. Birləşdirilmiş elektron imza yaradılan zaman elektron imzanın yeni faylı yaradılır və bu faylın daxilinə imzalanacaq faylın verilənləri yerləşdiriılir. Bu proses hazırlanmış sənədin konvertə (zərfə) qoyulduqdan sonra zərfin (konvertin) möhürlənməsinə bənzəyir. Sənədi konvertdən çıxaran zaman onun möhürləndiyinə əmin olmaq lazımdır. Birləşdirilmış elektron imzanın üstünlüyünə imzalanmış sənədin sonrakı mərhələdə istifadəsi zamanı *manipulyasiya* (yeni-latın dilində manus - əl, pellere – itələmək, vurmaq, hərəkətə gətirmək sözlərindən törəmədir) olunmasının sadəliyini aid etmək olar. Yəni həmin sənədin üzünü çıxarmaq, harasa göndərmək və s. əməliyyatları yerinə yetirmək olar.

2.*Ayrılmış elektron imza*. Ayrılmış imza yaradan zaman imza faylı ayrıca imzalanmış fayldan yaradılır, bu zaman imzalanmış fayl heç cür dəyişikliyə uğramır. İmzanı yoxlamaq üçün elektron imzalı fayldan istifadə etmək lazımdır. Ayrılmış elektron imzanın çatışmazlığı imzalanmış informasiyanın bir neşə fayl (imzalanmış fayl kimi və ya bir və ya bir neçə imzalı fayl şəkilində) şəkilində saxlanılmasıdır. Sonuncu vəziyyət imzanın qəbul edilməsini çətinləşdirir, çünki istənilən manipulyasiya əməliyyatında verilənlərin surətinin çəkilməsi və asılı olmayan faylların ötürülməsi tələb edilir.

3.*Verilənlərin daxilində elektron imza*. Belə şəkildə imzanın tətbiq edilməsi istifadə olunan əlavələrdən asılıdır (məsələn, elektron imza Microsoft Word və ya Acrobat Reader

sənədinin daxilində olarkən). Əgər elektron imza yaradılmış əlavədən kənardadırsa, onda verilənlərin müəyyən hissəsininn doğruluğunu yoxlamaq çətinlik yaradacaqdır.

Elektron imzadan müxtəlif sahələrdə istifadə etmək olar:

- Elektron imzadan elektron sənəddə məsulliyyət daşıyan imza kimi istifadə etmək olar (ya fərd şəxsən sənədi imzalayır, ya da ki, sənəd olan kağıza öz möhürünü vurur);
- Elektron imza proqramda, ya da ayrı modullarda istifadə edilir. Bu zaman kompüter istifadəçisi bu tip proqramları ya İnternetdən yükləyir, ya da ki, bu proqramları etibarlı və məlum mənbəədən alır.

Dəftərxana və ya müxtəlif şirkətlərin katibliyi ilə işgüzar yazışmaların aparılması zamanı elektron imza bəzən "zərf" rolunu oynayır, yəni bir tərəfdə göndərilən məktub elektron imza ilə "möhürlənir", digər tərəfdə isə alınmış məktub "açılır". Bu zaman hər iki halda verilənlərin toxunulmazlığı və həqiqiliyi öncədən yoxlanılır.

Elektron imza

Elektron imza məlumatı öhdəliklə əlaqələndirmək və ya məlumatın həqiqiliyini müəyyən etmək məqsədi ilə iştirakçı tərəfindən yerinə yetirilmiş və ya qəbul edilmiş, elektron vasitələrlə realizə olunmuş istənilən simvol və ya prosesdir. Elektron imzanın əsas funksiyası, adi imza kimi, müəllifin identifikasiyasıdır. Kağız sənəd dövriyyəsində olduğu kimi, elektron imzanın varlığı hələ sənədin həqiqiliyinə dəlalət etmir. Elektron imzalar ailəsinə rəqəm imzası texnologiyası, müəyyən biometrik verilənlər əsasında identifikasiyanı aparmağa imkan verən texnologiyalar (barmaq izləri, səsin tembri, göz tor damarlarının yerləşmə şəkli, əl imzası zamanı xətlərin

xronometrajı və başqa biometrik amillər), həmçinin əsasında müxtəlif ***smart-kartların*** və digər aparat açarlarının istifadəsi dayanan texnologiyalar aid edilir. Sadalanan bütün texnologiyalar (smart-kartlar istina olmaqla) - şəxsiyyəti identifikasiya etmə texnologiyalarıdır.

AÇIQLAMA: Daxilinə çip quraşdırılmış avtomatlardırılmış kart alman mühəndisi Helmut Qrettrup və onun həmkarı Yurgen Deslof tərəfindən 1968-ci ildə icad olunmuşdur. Karta patent isə1982-ci ildə verilmişdir. Kartlarin ilk kütləvi istifadəsi 1983-cü ildə Fransada, telefon danışıqları pulunun ödənilməsi üçün istifadə edilir. Fransız ixtiraçısı Ronald Morono 1974-cü ildə yaddaş kartına patent alır. 1977-ci ildə isə Bull şirkətinin əməkdaşı Mişel Uqon ilk dəfə olaraq daxilinə mikroprosessor yerləşdirilmiş smatr-kartı ixtira edir. 1978-ci ildə M.Uqon özüproqramlanan birçipli mikrokompüterə (СПОМ - самопрограммируемый одночипный микрокомпьютер) patent alır. Üç il sonra edilmiş ixtiraya əsaslanaraq qurulmuş CP8 çipi Motorola şirkəti tərəfindən istehsal olunur. Bu ərəfədə Honeywell Bull şirkəti smart-kartla bağlı mikroprosessorlara 1200-ə yaxın patentə sahib olur. Şirkət sonrakı illərdə şirkəti ilə əməkdaşlığa başlayır və yeni quruluşa malik smart-kartların istehsalını yerinə yetirir. Debet kartlı texnologiyanın kütləvi istehsalı 1992-ci ildə tamamlanır. Debet kartlı texnologiya istifadəyə çox asan idi, kart sahibi kartı terminala daxil etdikdən sonra ona məxsus PIN-kodu yığır və lazım olan əməliyyatı yerinə yetirirdi.

Smart-kart texnologiyasına əsaslanan elektron pul sistemi 1990-cı illərin ortasına kimi Avropada geniş istifadə edilir. Bununla yanaşı smart-kartdan Almaniyada (Geldkarte), Avstriyada (Quick), Belçikada (Proton), Fransada (Moneo),

Nidelandiyada (), İsveçrədə (Cash), Norveçdə (Mondex), İsveçdə (Cash), Finlyandiyada (Avant), Böyük Britaniyada (Mondex), Danimarkada (Danmønt) və Portuqaliyada (Portamoedas Multibanco) istifadə olunurdu.

Helmut Qrettrup (almanca Helmut Gröttrup; 1916 - 1981) alman mühəndis-raketçisi, idarəetmə sistemləri üzrə mütəxəssis, alman raket mütəxəsislərinin rəhbəri. Elektron çiplərinin köməyilə müştərilərə aid verilənlərin identifikasiya edilməsi sahəsinə öz tövhələrini vermişdir. Müasir informasiya texnologyalarında mütəxəssisin ideyalarından geniş istifadə olunur.

Smart-kartların geniş istifadəsi 1990-cı ilə təsadüf edir. Bu əsasən GSM mobil telefonlarında smart-kartın iş prinsipinə əsaslanan SIM-kartlardan istifadə ilə bağlı idi. 1993-cü ildə Beynəlxalq Ödəmə Sistemləri və Europay smart-kartdan kredit və debet hesablarının ödənilməsində istifadə olunması barədə müştərək işə başlayırlar. İlk EMV (Europay,

MasterCard, Visa) standartı 1994-cü ildə istehsal olunur. Texniki xarakteristikaları təkmilləşdərilmiş EMV 1998-ci ildən ustehsal olunmağa başlayır.

Rolan Moreno (fransızca Roland Moreno) kredit kartlarında və mobil telefonların SIM-kartında istifadə olunan elektron yaddaş kartının – smart-kartın ixtiraçısı.

Sənədlərin imza ilə müəlliflşdirilməsi çoxdan məlumdur. İstənilən sənəd yalnız onda müəllifin imzası (möhürü) olduqda hüquqi qüvvəyə minir. İstənilən imza sənədin müəllifinin kim

olduğunu dəqiq göstərir, sənədi imzalayanın sənəddə qeyd olunmuş məlumatla razı olması haqqında şəhadət verir, göndərənin başqa sənədi deyil, məhz göndərdiyi sənədi imzaladığını təsdiq edir, sənədin ilkin mətninin sonrakı dəyişiklik və təhriflərdən mühafizəsinə zəmanət verir.

Real elektron imza sistemlərinin fəaliyyəti hüquqi, təşkilati və proqram-texniki təminat tələb edir. Hüquqi təminatda elektron imzaya hüquqi qüvvə verən hüquqi aktların qəbul edilməsi aiddir. Təşkilati təminat istifadəçilərin müəyyən sertifikasiya mərkəzlərində qeydiyyatını, istifadəçi və sertifikasiya mərkəzi arasında bir-birinə verilmiş açıq açarlara görə cavabdehlik haqqında sənədlərin rəsmiləşdirilməsini əhatə edir. Proqram-texniki təminata elektron imzanın formalaşdırılmasını, yoxlanmasını, açarların generasiyasını və saxlanmasını, işlənmiş sənədləri və onların imzalarını saxlayan verilənlər bazasının saxlanmasını və s. təmin edən bütün proqram və aparat vasitələri daxildir.

Plastik kart ***bankomat*** və ***POS terminalları*** üçün əsas informasiya daşıyıcısı olduğu üçün həmişə saxtakarların, oğruların diqqət mərkəzindədir. Ona görə belə kartları buraxmazdan öncə təhlükəsizlik məsələləri dərindən işlənilməlidir.

AÇIQLAMA: *Bankomat* ingiliscə Automated teller machine sözündən yaranmadır, bəzən ATM, bəzən də bank avtomatı kimi oxunur. Bankomat proqram-texniki komnleks olub ödəmə kartından istifadə etməklə nağd pulun avtomatlaşdırılmış şəklildə alınması və verilməsi üçün istifadə edilir. Bununla yanaşı bankomatdan istifadə etməklə (ödəmə kartı ilə və ya onsuz) digər əməliyyatları da (məhsulun dəyərinin ödənilməsi, xidmətlərə görə pulun ödənilməsi,

uyğun əməliyyatların yerinə yetirilməsini təsdiqləyən sənədlərin tərtib olunması və s.) yerinə yetirmək mümkündür. Bankomatın prototipi 1939-cu ildə amerikalı alim Lüter Corc Cimçiyan tərəfindən icad olunmuşdur.

İlk hazırlanmış qurğu pulu tələbediciyə nağd şəkildə verirdi, amma alınmış pulun dəyərini ümumi hesabdan silə bilmirdi. İlk icad olunmuş qurğu ABŞ–da sınanılır. Lazımı nəticə əldə edilmədiyi üçün bank qurğudan istifadəni imtina edir. 30 ildən sonra alim yenidən qurğunu təkmilləşdirir və 1960-cı illərin axırlarında yenidən istifadəyə təklif edir. İlk bankomat 27 iyun 1967-ci ildə London şəhərinin şimal hissəsindəki Enfild rayonundakı bankların birində qurulur (bankomat Automated Teller Machine (ATM) adlandlrılmışdı). Qurğunun yaradıcısı şotlandıyalı Con Şepard-Barron idi. Qurğu De La Rue şirkətinin sifarişi əsasında yaradılmışdı. Şirkət dünyanın 150-dən çox ölkəsi üçün kağız pulun hazırlanmasında istifadə olunan qiymətli kağız istehsal edirdi. Con Şepard-Barronun hazırladığı qurğu pul tələb edən şəxsin hesabında nə qədər pulun olmasını yoxlaya bilmədiyi üçün bankirlərin rəğbətini qazana bilmir və ixtiraçı onu digər məqsəd üçün - şokalad satışı üçün təkmilləşdirir. 1966-cı ildə şotlandiyalı mühəndis Ceyms Qudfellou gizli 4 rəqəmli kod ilə mühafizə edilən koda patent alır (Patent bürosu koda "PIN-kod" adı altında identifikasiya nömrəsi verir). O dövrdən başlayaraq PIN-kod bank hesablarında geniş istifadə olunmağa başlanılır.

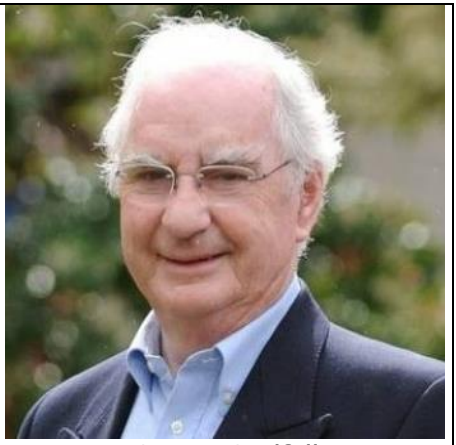
Bankomatların istifadəsi tədricən həyata keçirdi. 1971-ci ildə amerikanın 35 bankında bankomatlardan istifadə edilir. Amerikada bankomatların hər yerə quraşdırılması ilə məşğul olan Citibank bankıdır (bu hadisə 1972-ci ilə təsadüf edir).

İlk hazınlanmış bankomat

1972-ci ildə Böyük Britaniyada Lloyds bankı IBM şirkəti tərəfindən icad olunmuş Cash-Point adlı ilk on-layn bankomatlarını işə salır. Bankomatlar vauçerin yerinə maqnit zolaqlı plastik kartları qəbul edirdi. Telekommunikasiyanın sürətli inkişafı Amerikada, Vaşınqton ştatında, bir neçə yüz bankın Exchenge adı altında birləşməsinə səbəb olur. Bu ərəfədə (1972-1975-ci illər) istifadə olunan bankomatlar nəin ki, pulun verilməsini, həmçinin onun qəbulunuda həyata keçirə bilirdi.

Rusiyada ilk bankomat 1991-ci ildə istifadə olunmuşdur. Hesablamalar göstərir ki, 2011-ci ildə dünyada 2,4 milyon bankomatdan istifadə olunurdu. Təxmini hesablanmışdır ki, 2017-ci ildə bu rəqəm 3,4 milyona çatacaqdır.

Con Şepard-Barron



Ceyms Qudfellou

Nəşr edilmiş məqalərinin birində qeyd edilir ki, 2012-ci ildə Yaponiyanın The Ogaki Kyoritsu Bankında müştərinin övucunun şəkilini dəstəkləməklə işləyən bankomat istifadəyə verilmişdir.

AÇIQLAMA: *POS – terminal* (ingiliscə Point Of Sale sözündən yaranmadır və *satış nöqtəsi* anlamını verir) – plastik kartların köməyilə pulun ödənilməsindən ötrü yaradılmış elektron proqram-texniki qurğudur. Pos-terminal tərkibində çip olan kartları, maqnit zolaqlı və kontaktsız kartları, həmçinin kontaktsız toxunma prinsipi ilə işləyən kartları da qəbul edir. Bəzən Pos-terminal kimi xəzinədarın (kassirin) iş yerində quraşdırılmış proqram-aparat kompleksi də nəzərdə tutulur. POS-terminal istifadəçi ilə qarşılıqlı interfeysə malikdir. Bundan istifadə edən alıcı alacağı məhsul haqqında (onun qiyməti, istifadə müddəti, istehsal tarixi və s.) məlumat əldə edə bilir. POS-terminal müəyyən kassa proqramına uyğun satıla bilər.

Pos terminal

Elektron rəqəmsal imza əllə çəkilən imzanın elektron ekvivalentidir. Elektron rəqəmsal imza nəinki informasiya göndərənin əsilliyinin müəyyən olunmasına, həm də məlumatın tamlığının qorunmasına xidmət edir.

İnformasiya göndərənin əsilliyinin müəyyən olunması üçün, elektron rəqəmsal imzadan istifadə zamanı bağlı və açıq açarlar tətbiq olunur. Proses asimmetrik şifrələnməyə oxşayır, amma bu halda bağlı açar şifrələmək üçün, açıq açar isə şifrəni açmaq üçün istifadə olunur.

Elektron rəqəmsal imzanın tətbiq olunma alqoritmi bir sıra əməliyyatlardan ibarətdir.

İki qoşa açar yaradılır:

- 1.Açıq və bağlı;
- 2.Açıq açar bu işdə maraqlı olan tərəfə (sənədi qəbul edən, imzalanmış tərəf) ötürülür;

- 3.Göndərən informasiyanı bağlı açarın köməyilə şifrələyir və onu əlaqə kanalı vasitəsilə qəbul edənə ötürür;
- 4.Qəbul edən göndərilən informasiyanı açıq açarın köməyilə şifrədən azad edir.

Açıq açarla şifrələnmiş informasiyanın yalnız bağlı açarın köməyilə açılması elektron rəqəmsal imzanın məğzidir.

Nəzərə almaq lazımdır ki, elektron rəqəmsal imzaların əsasını xeş-funksiya təşkil edir.

Xeş-funksiya - yəni (H) funksiya məlumatın girişində (M) ixtiyari uzunluğu qəbul edir, amma çıxışda isə H(M) fiksə olunmuş uzunluğa malik qiymət alır. Bu M məlumatın *xeşi* və ya *profili* adlanır.

AÇIQLAMA: *Hashing* (bəzən *Xeşləmə* də adlandırılır) ixtiyarı uzunluğa malik olan giriş verilənlər massivinin müəyyən alqoritm ilə qeyd edilmiş uzunluqlu çıxış bitlər sətrinə çevrilməsidir. Belə çevrilməni həmçinin Xeş – funksiya və ya bağlama funksiyası da adlandırırlar. Funksiyanın nəticəsini Xeş, Xeş-kod, Xeş-cəm və ya əlaqə məlumatı (ingiliscə message digest) adlandırırlar. Müxtəlif xüsusiyyətə malik xeş alqoritmləri mövcuddur. 1953-cü ildə Donald Ervin Knut ilk dəfə sistem xeşləmə ideyasını təklif edir və bundan istifadəni IBM əməkdaşlarına məsləhət bilir. Sonrakı illərdə bu ideya ilə digər alimlər də məşğul olur və bu sahəyə öz tövhələrini verirlər.

Donald Ervin Knut (ingiliscə Donald Ervin Knuth) 10 yanvar 1938-ci ildə Viskonsin ştatının Miluoki şəhərində anadan olmuşdur, amerika alimidir, müxtəlif ölkələrdəki (o cümlədən Sankt-Peterburqdakı Dövlət Universitetinin) Universitetlərin, Stenford Universitetinin professorudur. Proqramlaşdırma sahəsində mühazirələr oxuyur (19 monoqrafiyanın, 160-dan çox elmi məqalənin, çoxlu sayda məşhur proqram texnologiyasının müəllifidir), yeni nəsil alimlərin yetişməsinə öz tövhələrini verir. Alim alqoritmin əsaslarına və hesablama riyaziyyatı üsullarına aid dünya şöhrətli, tanınmış seriya kitablar müəllifidir. D.E.Knut masaüstü TEX və METAFONT nəşriyyat sisteminin yaradıcısıdır.

Bunlarla yanaşı kriptoqrafiyada (əsasəndə elektron rəqəmsal imzada) aşağıdakı xüsusiyyətlərə malik olan funksiyalardan da istifadə olunur:

1.*Birtərəflilik*. İstənilən xeş üçün *h-ı* praktiki olaraq hesablamaq mümkün deyil və ya x elə seçmək lazımdır ki, H(X) = h bərabərliyi yerinə yetsin.

2.*Birinci üslub kolliziyaya görə dayanaqlıq*. İstənilən məlumat üçün *x-ı* praktiki olaraq hesablamaq mümkün deyil və ya başqa bir *y* məlumat seçmək lazımdır ki, H(x)=H(y).

3.*İkinci üslub kolliziyaya görə dayanaqlıq*. *x* və *y* müxtəlif məlumatları üçün elə cütlük seçmək lazımdır ki, praktiki olaraq hesablamaq mümkün olmasın və ya bunlar üçün H(x)=H(y).

Xeş funksiyanın dayanıqlıq kriptoqrafik xüsusiyyəti elektron rəqəmsal imzanın etbarlığını təmin etməlidir. Doğurdan da, orijinal məlumatın heç olmasa bir simvolu dəyişilərsə, onun xeş funksiyası (bu səbəbdən Elektron Rəqəmsal İmza da) dəyişəcəkdir, digər tərəfdən bu xeş funksiya ilə başqa bir məlumatı seçmək mümkün olmayacaqdır.

AÇIQLAMA: *Kolliziya* sözü latın dilindən gəlmədir (colloisio) və "toxunma", bəzəndə qüvvələrin, baxışların, maraqların, təçəbbüsün qarşıdurması kimi istifadə edilir. Bu zaman yaranan mübarizə həm fiziki, həm də ki, ideya səviyyəsində baş verə bilər. Odur ki, əksər hallarda kolliziya sözündən bədii ədəbiyyatda pesonajlar arasında yaranmış münaqişəni, həmçinin onların idealogiyasını əks etdirmək üçün istifadə olunur. Kolliziya termini müxtəlif sahələrdə də istifadə edilir. Sözə tikintidə, riyazı modelləşmədə, geologiya və hüquqda, sosioligiyada, mamalıqda və hətta informasiya texnologiyalarında da rast gəlmək mümkündür. Kolliziya sözü istifadə olunma əhəmiyyətinə görə çox qiymətlidir və digər sözlər ilə birləşərək müəyyən mənalar kəsb edir.

KRİPTOQRAFİYA PROTOKOLU

KRİPTOQRAFİYA PROTOKOLU ANLAYIŞI

Protokol dedikdə bəzi məsələlərin müştərək həll edilməsi üçün iki və daha çox tərəflər arasında qəbul olunan addımlar ardıcıllığı başa düşülür. Hər bir addım ciddi ardıcıllıqla yerinə yetirilməli və bir məsələnin həlli üçün atılacaq addım digər addım ilə əvəz olunmamalıdır.

Kriptoqrafik protokollar informasiya mübadiləsi zamanı müəyyən hərəkətlərin yerinə yetirilməsində istifadə olunur. Bu zaman pisniyyətli şəxs tərəfindən iştirakçıların qarşıya qoyduqları məqsəd pozula bilər (məsələn, konfidensiallıq, tamlıq və ya məlumatın təsdiqi düşmən tərəfindən zərbə altında qala bilər). Kriptoqrafik protokolun tərtib edilməsində əsas məsələ ondan ibarətdir ki, informasiya mübadiləsi zamanı iştirakçıların məqsədi həyata keçsin, amma düşmən isə öz məqsədinə çata bilməsin.

Kriptoqrafik protokol şifrələmədə, xeşləmədə, birtərəfli funksiyalarda, təsadüfi ədədlərin generasiyasında geniş istifadə edilir.

AUTENTİFİKASİYA PROTOKOLU

İstifadəçinin autentifikasiyası dedikdə bir tərəfin (yoxlayanın) autentifikasiya prosesindən istifadə etməklə digər tərəfin tam eyniliyinə (identiçliyinə) əmin olması başa düşülür.

***AÇIQLAMA**: İdentifikasiya* (latınca identifico) eyniləşdirmək, oxşatmaq deməkdir. Kriminal aləmdə həbs olunmuş şəxsin şəxsiyyətinin (və ya obyektin) söylənənlər ilə eyniləşdirilməsi prosesidir (Məsələn, şəxsin imzasının, əlinin izinin, səsinin yoxlanması). İdentifikasıya psixologiya və sosialogiya elmində də istifadə olunur. Bu sahədə identifikasıya şəxsin digər şəxs ilə emosional baxımdan oxşarlığının yoxlanması ilə həyata keçirilir. İdentifikasiyadan texnika aləmində, kimyada və s. sahələrdə də istifadə olunur.

Biznes lüğətində identifikasıyanın aşağıdakı açıqlanması verilir:

-Fiziki şəxsin məhkəmə prosesində oxşarlığının sübut edilməsi prosesidir;

-Obyektin bəzi etalonlar ilə müqayisə edilməsi prosesidir;

-Şəxsin imzası və digər atributları ilə şəxsiyyətinin sübut olunması prosesidir.

İndiki zamanda identifikasiyadan müxtəlif sahələrdə geniş istifadə edilir.

Autentifikasiya protokolu informasiyanı, özünü başqasının (başqa istifadəçinin) yerinə təqdim edən potensial pisniyyətli şəxsdən qorumalıdır.

Autentifikasiya protokolunu üç sinifə bölürlər:

1.Nəyi isə mənimsəməklə. Ən çox yayılmış variant parolu öyrənməkdir.

2.Nəyəsə malik olmaqla (Məsələn, maqnit kartları, smart-kartlar və s.).

3.Dəyişməz xarakteristikalara görə (səs, gözün toru, barmaqların izləri).

Cari kateqoriyada kriptoqrafik üsullardan istifadə olunmur.

Autentifikasiya protokolu təhlükəsizliyin təmini səviyyəsində aşağıdakı kimi təsnif olunur:

1.*Sadə autentifikasiya (parola əsaslanmaqla)*. Autentifikasiyanın ən sadə variantı ondan ibarətdir ki, sistem parolu açıq şəkildə, xüsusi fayl formasında yaddaşda saxlayır və istifadəçi sistemə daxil olanda sistem istifadəçiyə məxsus olan parol ilə yaddaşda saxlanılan parolu müqayisə edə bilir. Təhlükəsizlik baxımından belə yanaşma çox zəifdir, çünki parol ilə olan faylı bədniyyətli şəxs oğurlaya bilər. Odur ki, bunun qarşısını almaq üçün xüsusi faylda ancaq xeş parolu saxlamaq lazımdır. Belə olan halda istifadəçi ona məxsus olan faylı daxil etdikdə, sistem onun xeş parolunu hesablayır və yaddaşdakı fayl ilə müqayisə edir. Əgər düşmən (pisniyyətli şəxs) faylı oğurlamışsa, onda həmin faylda olan xeş əsl faylı bərpa etmək üçün kifayət etməyəcəkdir, nəticədə düşmənin cəhdi heçə enəcəkdir.

2.*Ciddi autentifikasiya (kriptoqrafik üsullara əsaslanmaqla)*. Autentifikasiyanın bu variantı ondan ibarətdir ki, istifadəçi bəzi bağlı açarları onların sahib olduqları əlamətə görə identifikasiya edir, amma açarın özü isə protokolun həyata keçirilməsi zamanı açılmır (gizli saxlanılır).

3.”Sıfır” səviyyəsində (daha doğrusu başlanğıc vəziyyətində) protokolların həqiqiliyini istifadəçilərə subut etməklə onlar barədə məlumatlar elan olunur.

Yazılanları nümunələrdə araşdıraq.

Təsadüfi ədədlər əsaslanan ciddi birtərəfli autentifikasiya. Hər iki tərəf onlara məlum olan K açarına ortaqdırlar və əməliyyatı həyata keçirmək üçün şifrələmənin simmetrik alqoritmini seçiblər.

1.B tərəfi (yoxlayan) *r* təsadüfi ədədlərini generasiya edir və generasiya olunmuşları A tərəfinə göndərir.

2.A tərəfi özünə alınmış *r* təsadüfi ədədlərini və öz adını qoşmaqla məlumat təşkil edir, onları K açarı ilə şifrələyir və B tərəfinə göndərir.

3.B tərəfi alınmış məlumatı şifrədən azad edir, alınmış A adı ilə r ədədinin bir-birinə uyğun olmasına əmin olur.

Əgər pisniyyətli insan şəbəkə ilə göndərilən məlumatı "tuta" bilərsə, o əldə etdiyi məlumatdan istifadə edə bilməyəcək, çünki K açarı açıq şəkildə şəbəkə ilə ötürülmədiyindən, özünü A və ya B kimi təqdim etmək istəyən pisniyyətli insan heç bir şeyə nail ola bilməyəcək. Səbəb odur ki, hər bir autentifikasiya seansı hər dəfə yeni təsadüfi ədədlərdən istifadə edir.

Təsadüfi ədədlər əsaslanan ciddi ikitərəfli autentifikasiya. İkitərəfli autentifikasiya dedikdə autentifikasiya seansı yerinə yetirilən zaman hər iki tərəfin doğurdanda bir-birinə dostluq münasibəti olduğu nəzərdə tutulur. İnformasiya mübadiləsi aşağıdakı sxem üzrə yerinə yetirilir:

B→A: təsadüfi r_1 ədədi.

A→B: r_1 –dən ibarət məlumat, B adı və r_2 təsadüfi ədədi K açarı ilə şifrələnmişdir.

B→A: r_1 və r_2 –dən ibarət məlimat K açarı ilə şifrələnmişdir.

Asimmetrik alqoritm əsasında autentifikasiya.

1.B tərəfi (yoxlayan) *r* təsadüfi ədədini seçir və B tərəfinə H(*r*), B, P_A (*r*, B) toplumunu göndərir.

Burada H – hər-hansısa xeş funksiyadır, P_A – asimmetrik şifrələmə alqoritmidir (şifrələmə bir-başa açıq A açarı vəsitəsilə həyata keçirilir).

2.A tərəfi $P_A(r, B)$ –ni şifrədən azad edir, əmin olur ki, *r*-in xeş funksiyası alınmış $H(r)$ kəmiyyəti ilə uyğundur və B tərəfinə *r* ədədini göndərir.

3.B tərəfi alınmış qiyməti yoxlayır və əgər bu qiymət *r* ilə uyğun gəlirsə, A-nın əsilliyinə əmin olur (A tərəfinin bağlı açarı bildiyi halında).

AÇARLARIN DƏYİŞİLMƏ PROTOKOLU

Açarların dəyişilmə protokolu dedikdə elə protokol başa düşülür ki, bu protokolun köməyilə hansısa gizli açar (gizli açardan istifadə etməklə sonralar simmetrik alqoritmin köməyilə şifrələmə yerinə yetirilə bilər) iki və ya daha çox tərəflər arasında bölünür, həm də nəzərə almaq lazımdır ki, düşmən göndərilə biləcək məlumatı "tuta" bilər, amma bu açarı əldə etməyə imkanı yoxdur.

Açarların dəyişilmə protokolunu üç növə ayırırlar:

- Açarların artıq generesiya olunmuş ötürmə protokolu;
- Ümumi açarın müştərək hazırlanma protokolu;
- Açarların öncədən paylanma sxemi.

Öncədən açarların paylanma sxemi iki alqoritmdən ibarətdir: *ilkin açarlı informasiyanın paylanması* və *açarın formalaşması*. Birinci alqoritmin köməyilə ilkin açarlı informasiyanın açıq hissəsi generasiya olunur, generasiya olunmuş hissə gizli həssədə və serverdə yerləşdirilir. İkinci alqoritm fəaliyyət göstərən açar üçün nəzərdə tutulmuşdur və bu açarın köməyilə abonentlər arasında hesablama həyata keçirilir.

Açarların öncədən paylanma sxemi dayanıqlı olmalıdır.

Açarların dəyişmə protokolları içərisində ən geniş yayılmışı Diffi-Hellman alqoritmidir. Alqoritm kanal vasitəsilə açarların dəyişilməsində etibarlı alqoritm sayılır.

ÖZÜNƏ XAS XÜSUSİYYƏTİ OLAN PROTOKOLLAR

Açarları dəyişmə protokolu və autentifikasiya protokolu ən çox kriptoqrafik protokollar sinifinə aiddirlər. Bununla yanaşı bəzi protokollar vardır ki, onlar başqa spesifik (özünə xas xüsusiyyəti olan) məsələləri həll etmək üçün yararlıdırlar. Bunlara aşağıdakıları aid etmək olar:

Səsvermə protokolu. Protokol seçkilərin aparılması zamanı istifadə edilir. Səsvermədə iştirak edən hər bir seçici anonim olaraq öz səsini verir. Bununla yanaşı səsvermədə iştirak edən şəxs iki dəfə bu prosesdə iştirak edə bilməz. Səsvermədə ancaq qeydiyyatdan keçmiş iştirakçı iştirak edir və həqiqətəndə onun səsverən şəxs olduğu ona məxsus olan sənəd vasitəsilə yoxlanılır.

Eyni zamanda imza atma protokolu. İştirakçıların əsas məqsədi ondan ibarətdir ki, onlar hər hansısa bir sənədi imzalayan zaman imzasına görə təminat ala bilsinlər. İştirakçılar imzalama mərasimi zamanı bir-birindən uzaq məsafədə ola bilərlər, odur ki, imzalama prosesi elektron rəqəmsal imza ilə də həyata keçirilə bilər.

Qrup şəkilində imzalama protokolu. Sənədin imzalanması bir qrup iştirakçı tərəfindən yerinə yetirilə bilər. İmzalanmış sənədi alan əks tərəf əmin olmalıdır ki, sənəd bir qrup iştirakçı tərəfindən imzalanmışdır, amma imzaların kimə məxsus olduğu onun üçün o qədər də maraqlı deyil. Əgər imzaların kimə məxsus olduğunu yoxlamaq tələb edilərsə, sözsüz ki, sənədi

imzalayanların imzaları ilə onların şəxsiyyəti araşdırılmaqla yoxlanılacaq.

Qrup şəkilində imzalamağın ən sadə forması inanılmış *arbitrdən* istifadədir. Arbitr çoxlu sayda açıq və bağlı açarları generasiya edir və bu açarları qrupun iştitakçılarına paylayır (məsələn, *m* ədəd açarı qrupun hər bir *n* üzvünə). Açıq açarların siyahısı çap edilir. Məlumatı imzalamaq üçün qrupun hər bir üzvü bağlı açarlardan istənilən birini seçir. Sənədin qrup üzvlərinin biri tərəfindən açıq açarla imzalandığını yoxlamaq üçün elektron rəqəmsal imza tərəfindən qrupa məxsus açıq açarlar toplumu yoxlanılır. Sonrakı mərhələdə isə imzaların imza sahiblərinə məxsusluğunu müəyyənləşdirməkdən ötrü *arbitrə* müraciət edilir (Arbitr latınca *arbiter* – hakim, ortaq anlamını verir).

Protokolun zəif cəhəti əsasən ondan ibarətdir ki, arbitrin nəyəsə aldanaraq qrup üzvlərinin imzalarını saxtalaşdırmasıdır.

Danılmaz imzalama. İmza adı rəqəmsal imzadan onunla fərqlənir ki, onun yoxlanılması üçün imzalayanın icazəsi mütləq olmalıdır.

Kor-koranə imzalama. Elektron rəqəmsal imzanın xüsusiyyətini özündə əks etdirsədə, ondan müəyyən qədər fərqlənir, yəni imzalayan şəxs imzaladığı sənədin məzmunu ilə tanış olmaqdan mərhumdur.

Sirrin bölünmə protokolu. Məlumat hissələrə parçalandıqdan sonra qrup üzvləri arasında paylanır, nəticədə qrupun istənilən üzvü onun payına düşən məlumatdan heç bir şey anlaya bilmir. Lazım gəldikdə qrup üzvləri bir yerə toplaşdıqdan sonra məlumatla tanış ola bilirlər.

Ən çox istifadə edilən protokol sirrın arbitrin iştirakı ilə bölünməsidir.

YOXLAMA TESTLƏRİ

1.Məlumatı imzalamaq üçün elektron rəqəmsal imzanın hansından istifadə edilir:

A.Göndərənin açıq açarından;

B.Qəbul edənin açıq açarından;

C.Göndərənin bağlı açarından;

D.Qəbul edənin bağlı açarından.

2.Təsadüfi ədədlərə əsaslanan ciddi ikitərəfli autentifikasiya protokolu üçün hansı təsdiqlər qanuna uyğundur?

A.Protokolun əsasını şifrələmənin simmetrik alqoritmi təşkil edir;

B.Yoxlayan B birinci addımında yoxlanılan A-ya təsadüfi ədədlər göndərir;

C.Yoxlanılan A-nın ikinci addımında yoxlayan B-yə şifrələnmiş məlumat göndərir. Məlumat birinci addımda təsadüfi ədələrdən, həmçinin yeni təsadüfi ədələrdən ibarətdir;

D.Protokol ancaq göndərilən iki məlumatı tələb edir.

3.Elektron rəqəmsaı imzanın köməyilə məlumatın imzalanması hansı ardıcıllıqla həyata keçirilir?

A.Xeş hesablanır, sonra isə xeş şifrələnir;

B.Öncə məlumat şifrələnir, sonra isə alınmış nəticə xeşlənir;

C.Məlumat imzalanan vaxtı şifrələnir, yoxlama zamanı isə xeş hesablanır;

D.İlkin məlumatın xeşi hesablanır, sonra isə şifrələnir.

4.Xətti generator bu parametrlərə məxsusdur: m=10, c=7, a=2, x_0=5. Bu generatorun köməyilə veriləcək ardıcıllığın ikinci üzvü necə olacaqdır?

5.H xeşləmə funksiyasının kolliziyanın birinci qaydasına görə xüsusiyyətləri nədən ibarətdir?

A.İstənilən H üçün praktiki olaraq hesablama aparmaq mümkün deyil və ya elə x seçmək lazımdır ki, H(x)=h olsun;

B.Praktiki olaraq hesablanma mümkün deyil və ya istənilən x və y cütlüyü üçün məlumatlar elə seçilməlidir ki, H(x)=H(y) olsun;

C.Giriş məlumatının uzunluğundan asılı olmayaraq xeşin uzunluğu fiksə olunmuş olmalıdır;

D.İstənilən məlumat üçün x praktiki olaraq mümkün olmamalıdır və ya başqa bir y məlumatını seçmək lazımdır ki, H(x)=H(y) olsun.

6.RSA alqoritminin korrektliyinin sübutu nəyə əsaslanır?

A.Eyler teoreminə;

B.Elliptik əyrilərin cəmi teoreminə;

C.Qalıqlar haqqında Çin teoreminə;

D.Evklid alqoritminin genişləndirilmiş formasına.

7.Psevdotəsadüfi (psevdo - mürəkkəb sözlərin əvvəlində yalançı, saxta mənasını ifadə edən hissəcik anlamını verir) ədədlər generatoru hansı xüsusiyyətlərə malik olmalıdır?

A.Determinə edilməmiş;

B.Qabaqcadan deyilənlərə əsaslanmayan;

C.Növbəti elementin öndəkindən asılı olmaması;

D.Elementlər ardıcıllığın bərabər paylanması;

E.Ardıcıllıq elementlərinin təkrarlanmaması (dövr ərzində).

8.Aşağıda verilmiş alqoritmlərdən hansı elektron rəqəmsal imza alqoritmidir?

A.DES;
B.QOST 34.10-2001;
C.QOST 34.11-94;
D.RSA

9. (15.2) cütlüyü RSA açıq açarına malikdir. 4 ədədini şifrələyin.

10.Elleptik əyri aşağıda verilənlərdən hansına aiddir?

A.$y^2= x^3+ax+b$ (mod p);
B.$y^3= x^2+ax+b$ (mod p);
C.$y= x^3+ax^2+b$ (mod p);
D.$x^3= y^2+ax+b$ (mod p).

11.Asimmetrik şifrələmə alqoritmindən istifadə etməklə məlumatı şifrələmək üçün lazımdır?

A.Göndərənin açıq açarı;
B.Qəbul edənin açıq açarı;
C.Göndərənin bağli açarı;
D.Qəbul edənin bağlı açarı.

12.Parola əsaslanaraq istifadəçini müəyyənləşdirən protokol protokolların hansı növünə aiddir?

A.Autentifikasiya protokoluna;
B.Açarların dəyişdirilmə protokoluna;
C.Eyni anda imzalama protokoluna;
D.Qrup şəkilində imzalama protokoluna;
E.Səs vermə protokoluna.

PAROLUN KÖMƏYİLƏ MÜDAFİƏ

AVTOMATLAŞDIRILMIŞ İNFORMASİYA SİSTEMLƏRİNİN (AİS) TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİNDƏ PAROLUN KÖMƏYİLƏ MÜDAFİƏNİN ROLU

Xarici müdaxilədən yaranan pozuntulardan informasiyanın mühafizə edilməsini (konfidensiallığını, tamlığını, autentikliyini və buna oxşarları) kriptoqrafik üsullar (əsasəndə şifrələmə) lazımı səviyyədə təmin edir. İnformasiya pozucuları rabitə kanalı ilə ötürülən informasiyanı əldə edə bilir və bəzi hallarda isə ötürülən məlumatı modifikasiya etməklə rabitə kanalında seans təşkil etməklə özünəməxsus informasiyanı həmin informasiyanın yerinə ötürürlər. Nəzərə almaq lazımdır ki, informasiya rabitə kanalı vasitəsilə ötürülən zaman öncədən kriptoqrafik çevrilməyə məruz qalır və kriptoqrafik protokola uyğun ötürülür. Kriptoqrafik protokol xüsusi olaraq informasiyanın ötürülməsinə maneçilik edən pozuculara qarşı nəzərdə tutulmuşdur və onun köməyilə pozucu tərəfindən həyata keçirilən təhlükələrin qarşısının alınmasında tutarlı səviyyədə rol oynayır. Ümumiyyətlə, informasiyanın təhlükəsizliyinin pozulması üçün informasiya pozucuları sistemdə dövr edən informasiya ilə qarşılıqlı əlaqənin yaranmasını həyata keçirməli, kriptoqtrafik alqoritm haqqında müəyyən məlumata malik olmalı və nəhayət, bunlardan

səmərəli istifadə etməyi bacarmalıdır. Bütün bunlar pozucunun qarşısında duran əsas problemlərdir.

Bəzən vəziyyət dəyişir, pozucu sistemə daxil olmaq üçün istifadəçinin səlahiyyətindən istifadə etməklə onu maraqlandıran verilənləri (məsələn, konfidensial faylların sürətini əldə edir, lazımlı verilənləri məhv edir və s.) əldə edir. Belə olan halda kriptoqrafik mühafizə öz əhəmiyyətini itirir.

Ümumiyyətlə avtomatlaşdırılmış informasiya sistemlərinin ən zəif nöqtəsi pisniyyətli insanların (düşmənlərin) onlara daxil olmasıdır. Bu baxımdan zəif nöqtə autentifikasiya protokolu vasitəsilə müdafiə edilir (məsələn, istifadəçinin həqiqiliyi daim yoxlanılır).

Öndə yazılanlardan belə nəticə çıxarmaq olar ki, istifadəçi üçün ən əlverişli autentifikasiya forması *paroldan istifadə etməklə müdafiədir*.

Beləliklə, bədniyyətli insan hər hansı bir yollasa sistemə daxil olmağa cəhd göstərsədə, ona məqsədinə çatmağa bir məsələ maneçilik edir – kompüterin klaviaturasında daxil edilən simvollar ardıcıllığı – parol.

Qeyd etmək lazımdır ki, bir neçə standart fəndlər vardır ki, pisniyyətli şəxs paroldan istifadə etməklə yaradılmış müdafiə sistemini "sındıra" bilir. Nəzərə almaq lazımdır ki, bunun qarşısını almaq üçün tutarlı səviyyədə əks təsir göstərən mexanizmlər işlənib hazırlanmışdır. İstifadəçi hazırlanmış mexanizmlərdən istifadə etməklə parolun təhlükəsizliyini düzgün formalaşdırmaqla yanaşı paroldan səmərəli və əlverişli istifadə edə bilər.

PAROLA HÜCUM ÜSULLARI. PAROLUN TƏHLÜKƏSİZLİYİNİN TƏMİNİ

Dərslikdə parolun müdafiə sistemindən düşmənin yan keçməsi və buna qarşı əks tədbirin görülmə üsullarına baxılır.

Tamamilə artıq (kobud güc tətbiq etmə üsulu – bruteforce).

Texniki baxımdan parola edilən ən sadə hücumdur. Burada əlçatan bütün kombinasiyaların, yəni birsimvollu parolların tamlığından söhbət gedir. Müasir hesablama texnikasının gücü informasiyanın təhlükəsizliyini təmin etmək üçün yararlı olan parolların uzunluğunu əlli-aıtmiş simvola qədər artırmağa imkan verir.

Bəzi sistemlər onlara edilən hücumu tamamilə artıq (izafi) formada həyata keçirməyə imkan vermir, amma səhv tərtib edilmiş, ardıcıl olaraq parola edilən hücum cəhdlərinə isə reaksiya verirlər. Məsələn, Windows əməliyyat sisteminə edilmiş üç uğursuz cəhd nəticəsində istifadəçi sistemə daxil olanda bir dəqiqəlik fasilə ilə üzləşir, amma telefonların sim-kartları və bankomatların kredit kartları isə tamamilə bloklanırlar ("qıfıl"lanırlar).

Çoxlu sayda sistemlər vardır ki, onlar sonsuz sayda edilən hücumlara reaksiya vermir, rahat işləyə bilirlər. Məsələn, parol ilə mühafizə edilən arxiv faylları (Win.Rar və ya Win.Zip, Microsoft Office sənədləri və s.) onlara olunan sonsuz hücumlara tutarlı səviyyədə cavab verə bilirlər (müxtəlif parollardan istifadə etməklə).

İndiki zamanda çoxlu sayda proqramlar vardır ki, onlar öndə göstərilən prosedurları avtomatik yerinə yetirirlər. Məsələn, Advanced RAR Password Recovery, Advanced PDF Password Recovery, Advanced Office XP Password Recovery və

s. Bununla yanaşı çoxlu sayda proqramlar xeş parolu əlçatan faylda saxlayırlar. Məsələn, müştəri elektron poçt ilə işləyən zaman istifadəçinin parolunu yaddaşda saxlaya bilir (bu zaman o, hamının istifadə edə biləcəyi kompüterdən istifadə edir).

Əməliyyat sisteminə daxil olmaqla xeş parolu olan faylı oğurlamaq üsulları da vardır. Oğru bu əməliyyatı yerinə yetirdikdən sonra əməliyyat sistemini yan keçməklə rahat şəraitdə parollar üzərində pisniyyətini həyata keçirmək üçün xüsusi proqramlardan bəhrələnməklə parolları "sındıra" bilir.

Parolun əsas xarkteristikası onun uzunluğudur, yəni simvollar sayıdır. *Müasir parol ən azı 12 simvoldan ibarət olmalıdır*.

Qeyd etmək lazımdır ki, parolun uzunluğuna 2 simvolun əlavə edilməsi onun etibarlığını 4000 dəfə, 4 simvolun əlavə edilməsi isə - 1.600.000.000 dəfə artırır. Onda belə alınır ki, əgər simvolların sayını 15 simvol qədər artırsaq, onda onun sındırılması üçün *Dünyanın yaşı qədər illər* lazımdır. Yaddan çıxarmaq lazım deyil ki, kompüterlərin hesablama gücü günü-gündən artır, deməli parolların etibarlığı da bu artıma uyğun çoxalır (məsələn, bir neçə il əvvəl uzunluğu 8 simvoldan ibarət parol təhlükəsiz sayılırdı).

MƏHDUD DİAPAZONDA İZAFİLİK

Məlumdur ki, bir çox istifadəçilər parol yaradan zaman müəyyən diapazonda yerləşən simvollardan istifadə edirlər. Məsələn, rus hərflərindən yaradılmış parolu və ya ancaq latın hərflərindən ibarət olan parolu və ya ədədlərdən ibarət olan parolu istifadəçi rahat yadda saxlaya bilir. Amma bədniyyətli insanın qarşısına qoyduğu məsələ, yəni yaradılmış parolu

sındırmaq inanılmaz dərəcədə onun üçün çətinləşir, buna baxmayaraq o öz pis əməlindən əl çəkmir, parolu sındırır.

Tutaq ki, n=70 –simvollar sayı, bundan istifadə etməklə parol yaratmaq lazımdır, amma 70 simvoldan 10-u ədəd, 30-u bir dilin hərfləri və 30-u isə başqa dilin hərfləridir. Nəzərə alaq ki, yaratdığımız parolun uzunluğu m=4 simvoldur.

Əgər parol təsadüfi yaradılırsa, onda mümkün kombinasiyalar sayı 70^4=24 010 000 olacaqdır. Hesab edək ki, düşmən belə düşünər ki, parol bir diapazona malik simvollardan ibarətdir (hətta hansı diapazon olduğu düşmənə məlum olmadıqda).

Belə parolların sayı $10^4+30^4+30^4$ = 10 000+810 000+810 000=163 000 olacaqdır. Əgər düşmən düzgün seçim etmişsə, onda kombinasiyaların sayı 147 dəfə azalmış olacaqdır. Əgər parolun uzunluğu və simvollar diapazonu artarsa, onda bu rəqəm də kəskin sürətdə artacaqdır.

Parolun avtomatik yaradılması proqramı (məsələn, Advanced Office XP Password Recovery) parolu seçim edən zaman simvolların hesablanmasına imkan verir.

Beləliklə, etibarlı *parol müxtəlif diapazonlardan* ibarət olmalıdır. Ümumiyyətlə, istifadəçiyə parol yaradan zaman rus və ya ingilis dilinin hərflərindən (böyük və kiçik hərflərindən), ərəb rəqəmlərindən, həmçinin digər simvollardan (durğu işarələri - nöqtə, vergül və i. a) istifadə etmək məsləhət bilinir.

LÜĞƏTƏ UYĞUN HÜCUM

Təsadüfi və mənasız yaradılmış parolu yadda saxlamaq çox çətindir. Bu baxımdan parolu yaddan çıxarmaq, qiymətli informasiyanı itirmək, bütün bunlar istifadəçi üçün real olmaqla yanaşı çox dəhşətli bir hadisədir. Bunu bədniyyətli insanın

sistemi "sındırması" ilə müqayisə etmək bir o qədər də düzgün deyil. Deməli, belə hadisələrdən yan keçmək üçün parolu sözlərdən yaratmaq məsləhətdir. Belə olan halda parolun düşmən tərəfindən sındırılması bayağı (çeynənmiş, köhnəlmiş) bir işə çevrilir.

Parol verilmiş fayldan proqram tərəfindən avtomatik yoxlanılır (lüğətə uyğun şəkildə). Nəzərə almaq lazımdır ki, müxtəlif dillərdə çoxlu sayda lüğətlər mövcuddur və proqram 200 000 sözdən ibarət lüğətdən yaradılmış parolu bir neçə saniyə ərzində yoxlayır. Belə olan halda pisniyyətli düşmənin bu sahədə pis niyyəti yerinə yetirməyi çətinləşir, bəzən həyata keçməyən olur.

Bir çox istifadəçi belə hesab edir ki, parolu yaradan zaman sadəcə olaraq əvvəcə rus əlifbasından, sonra isə ingilis əlifbasindan istifadə etmək lazımdır və yaxud da əksinə hərəkət etmək lazımdır. Belə olan parolun etibarlığını artırmaq mümkündür. Bəzən belə seçim xoşa gəlməyən hadisələrlə tamamlanır.

Deməli belə nəticəyə gəlmək olar ki, *etibarlı parol təbii dillərin sözlərindən yaradılmamalıdır*.

FƏRDİ LÜĞƏTƏ HÜCUM

Əgər hücum lüğətdən istifadə etməklə və çox da uzun olmayan, bir qrupa uyğun simvollardan yaradılmış parol üçün nəzərədə tutulmuşsa, bu pisniyyətli insanın arzusunun həyata keçməsinə köməklik edəcək, çünki pisniyyətli insan parolu sındırmaqda çətinlik çəkməyəcək. Buna səbəb istifadəçinin parolu yaradan zaman mənzilinin telefon nömrəsindən, mobil telefonun nömrəsindən, doğum günü ilə bağlı verilənlərdən,

adının, soyadının və atasının adının tərs yazılışından və s. istifadə etməsidir.

Bütün bunlardan yan keçmək üçün istifadəçi parolun avtomatik yaradılması üçün yararlı olan proqramdan bəhrələnməlidir, çünki proqram istifadəçinin seçdiyi lüğətə uyğun olan sözləri generasiya edir, bu da parolun etibarlı olmasına imkan yaradır.

Beləliklə, *etibarlı parol tamamilə mənasız sözlərdən yaradılmalıdır*.

ÜMUMİ ƏLÇATAN YERLƏRDƏ SAXLANILAN PAROLLARIN TOPLANMASI

Bir çox müəssisələrdə parol yaradıldıqdan sonra istifadəçilər arasında paylanılır. Bəzən belə parolları yadda saxlamaq çətin olur. Bundan çıxış yolu parolun yazılı şəkildə iş masasında (və buna uyğun yerlərdə) saxlanılmasından istifadə edilir. Bəzi hallarda parol kağız parçasına yazılaraq kompüterin ekranına yapışdırılır, cib dəftərcəsinə qeyd edilir və ya kağıza yazılmış şəkildə iş masasının gözə görünən yerinə qoyulur.

Araşdırmalar göstərir ki, istifadəçi bu məsələyə çox da ciddi yanaşmır. Adatən bu istifadəçinin təhlükəsizlik siyasətini lazımı səviyyədə başa düşə bilməməsi ilə, ona lazım olan verilənlərin və servislərin parolla müdafiə edilməsinin qiymətinin yüksək olması və s. faktorların düşməndən gizli saxlanılmasının vacibliyini anlaya bilməməsi ilə bir-başa əlaqəlidir. Bəzən istifadəçi müəssisəni özünə doğma saydığı üçün parolların gizli saxlanılmasını qiymətləndirə bilmir və bu sirrin agah olmasının ona və müəssisəyə vuracağı ziyanı qiymətləndirməkdə aciz qalır. Bütün sadalananlar pisniyyətli

insan üçün kifayətdir ki, o öz iyrənc məqsədini həyata keçirə bilsin.

Təcrübə göstərir ki, istifadəçi parolu müəssisə rəhbərliyindən alandan sonra onu ya kağız parçasına, ya da ki, cib dəftərçəsinə yazırsa, o bir müddət sonra parolu əzbər bildiyi üçün onları zibil qutusuna atır. Bu da düşmən üçün kifayət edici haldır.

Deməli belə bir qanun var: *parol hamı üçün əlçatan yerdə saxlanılmamalıdır*. İdeal variant – onu yadda saxlamalı və heç bir yerdə gizlətməməli. Əgər parol cib dəftərçəsindədirsə, dəftərçə nəzarətsiz qalmamalı, parolu sistemə daxil edəndə otaqda kənar şəxs olmamalı və nəhayət, istifadəçi bu işə məsuliyyətlə yanaşmalıdır.

SOSİAL İNJİRİNQ

Sosial injirinq – maşınlarla deyil, insanlarla manipulyasiya olunmadır. Burada əsas məqsəd istifadəçinin müdafiə edilən sistemə və ya müəssisəyə daxil olmasıdır. Əgər parolu para ilə almaq və ya oğurlamaq mümkün deyilsə, onda istifadəçini hansı yol ilə olursa olsun aldadıb (ələ almaqla) parolu ondan almaq lazımdır. Sosial injirinqin klassik taktikası ondan ibarətdir ki, bədniyyətli insan parolu soruşmağa səlahiyyəti olan hörmətli yoldaşın adından öz "qurban"ına zəng edir və ona lazım olan informasiyanı əldə edir. Məsələn, bədniyyətli şəxs sistem administratoru kimi özünü təqdim edir və istifadəçidən parolu ona söyləməyi xahiş edir (həmçinin digər qiymətli informasiyaları da soruşa bilər).

Pisniyyətli insan müxtəlif pis əməllərdən istifadə edə bilər. Məsələn, gecəyarısı istifadəçiyə zəng edib onu yuxudan etdiyi üçün dönə-dönə üzr istədikdən sonra güya ki, "istifadəçinin

işlədiyi müəssisənin bank hesabına küllü miqdarda para yatırtmaq istədiyini bildirir və bunu edə bilməməsinin səbəbini tutarlı səviyyədə aydınlaşdırır". Səbəb kimi kompüterinə virusun düşdüyünü bəhanə edən bədniyyətli insan istifadəçidən parol olan faylı soruşur və parolu əldə edərsə (bəzi hallarda əldə edə bilir) məqsədini həyata keçirir.

İstənilən halda qanunu başa düşmək lazımdır: kənar şəxsə parolu söyləmək qadağandır və bu heç bir halda bağışlanıla bilməz.

Qeyd etmək lazımdır ki, ancaq müstəsna hallarda, məsələn məhkəmə və ya hüquq mühafizə orqanları parolu tələb edərsə və buna məsuliyyət daşıyarlarsa, onda parolu sənədləşmə aparmaqla həmin təşkilatlara vermək olar. Bu halda da tam əmin olmaq lazımdır ki, parol təqdim edilən orqan işçiləri parolu almağa səlahiyyətlidirlər.

FİŞİNQ

Fişinq parolun təsadüfi İnternet istifadəçisi tərəfindən "aldadılıb alınması" prosedurudur. Adətən fişinq istifadəçini aldatmaqla ona məxsus olan paroloun "yalançı" saytlara yerləşdirilməsi ilə tamamlanır.

QEYD: *Fişinqdən* istifadə texnikası 1987-ci ildə ətraflı şəkildə nəşr olunan jurnalların birində verilmişdir. Termin isə ilk dəfə 2 yanvar 1996-cı ildə "Alit.online-service.America-Online" yeniliklər qrupunda istifadə edilmişdir. Bəzi mənbələrdə isə terminin daha əvvəllər xakerlərin nəşr etdikləri jurnallardan birində ("Xaker 2600" jurnalı nəzərdə tutulur) xatırlandığı barədə məlumat verilir.

Məsələn, bank hesabına daxil olmaq üçün parolun əldə olunmasından ötrü bankın saytını "yamsılayan" dizayn olunmuş sayt hazırlanır. Sözsüz ki, yalandan yaradılmış saytın ünvanı başqadır, amma bədniyyətli insan yalandan yaratdığı domenin adını elə şəkildə qurur ki, ad bankın domenindən bir simvol ilə fərqlənsin. Nəticədə istifadəçi səhv (mətbəə xətası) etməklə yalançı sayta daxil olur (bu zaman o səhv etdiyini anlamır). Bəzən də pisniyyətli insanlar bankın müştərisinə elektron poçt ilə məktub göndərir, mütəriyə guya ki, yardım etmək məqsədilə bank hesabını "təkrar yoxlamağı" məsləhət bilir, ya da ki, "yeni aksiyalar ilə tanış olun" deyə ona yardım etdiklərini başa salırlar. Beləliklə, müştəri aldadıcı manevrlərin "toruna" düşür.

Müştəri bədniyyətli insanın saytına daxil olan zaman ona təklif olunur ki, hesabına girmək üçün loqin və parolunu daxil etsin. Bu informasiya pisniyyətli insanın verilənlər bazasında saxlanılır, sonrakı mərhələdə isə əsl saytın əsas səhifəsinə göndərilir. İstifadəçi daxil etdiyi parolun "işləmədiyinin" şahidi olur və belə hesab edir ki, o səhvə yol vermişdir və ya sayt sadəcə olaraq "uşaq arabası kimi yırğalanır". Baş verən hadisəni başa düşə bilməyən istifadəçi yenidən parolu sistemə daxil edir və bununla da sistemə daxil olur. Beləliklə, müştərinin şübhəsinə son qoyulur, amma "axıntı" baş vermişdir, artıq gecdir.

Fişinqin digər növü onunla bağlıdır ki, əksər müştərilər eyni parolu müxtəlif məqsədlər üçün istifadə edirlər. Bundan düşmənlər müvəffəqiyyətlə istifadə edərək parola hücuma keçir və istədiklərinə nail olurlar.

Məsələn, bir neçə qrup istifadəçi üçün maraqlı olan sayt yaradılır. Əgər hücumun məqsədi konkret şəxsədirsə, onda bədniyyətli insan həmin şəxsin maraqlarını və nə ilə məşğul olduğunu araşdırır. Bununla da həmin sayt haqqında

informasiya potensial "qurban"lıq kimi hamıya xəbər formasinda çatdırılır (məsələn, reklam olunmaqla). İstifadəçi sayta daxil olan zaman özü üçün parol düşünməlidir. Sonrakı mərhələdə həmin parolun istifadəçinin digər resurslarına (elektron poçt, qeydiyyat zamanı göstərilən ünvan və s.) daxil olmaq üçün yararlı olduğunu müəyyənləşdirmək lazımdır.

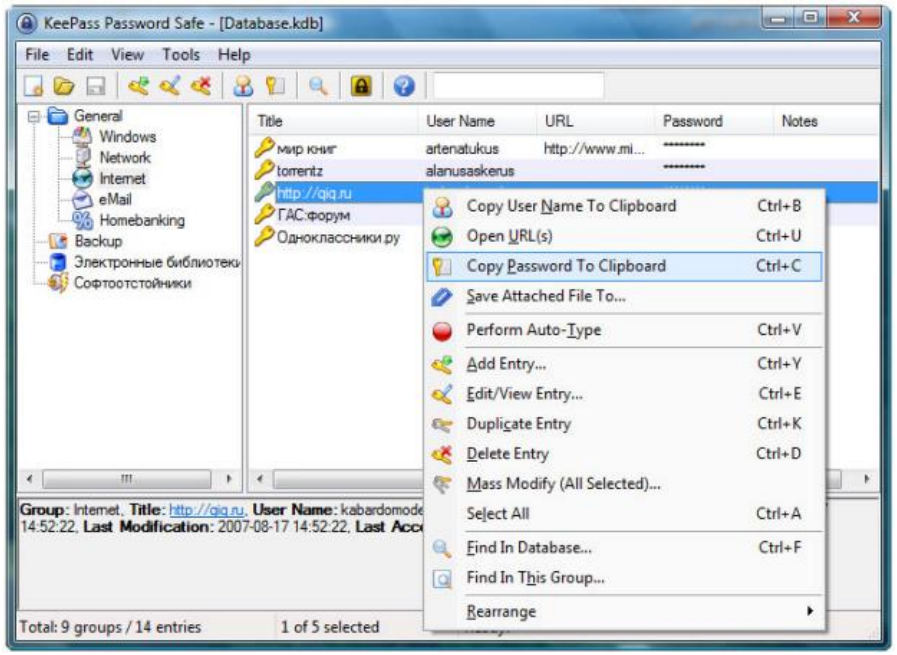
Fişinqdən gələn təhlükəyə qarşı dayanmaq üçün lazım olan parolu daxil etməzdən öncə saytın ünvanını diqqətlə yoxlamaq kifayətdir. Ünvanı brauzerin əlfəcinə (arasına) yerləşdirmək məsləhətdir və iş prosesində ancaq bu əlfəcindən istifadə etmək düzgündür. Bununla yanaşı işləyən zaman elektron məktublara istinad etmək qəti qadağandır.

Beləliklə, *müxtəlif parollardan istifadə etməklə müxtəlif servislərə daxil olmaq* məsləhətdir.

Öndə sadalanan bütün təqdimatlar kifayət qədər mürəkkəbdirlər. Bir neçə etibarlı parolu (uzun və mənasız) yadda saxlamaq o qədər də asan deyil. Amma parolun yaddan çıxma ehtimalı çoxdur. Bunları nəzərə alaraq istifadəçiyə bəzi vəsaitlər (üsullar) təklif edilir ki, o bunlardan istifadə etməklə yerinə yetirəcəyi əməliyyatları hiss olunacaq dərəcədə yüngülləşdirmiş olur. Bu vasitələrdən də önəmlisi parolların saxlanılması üçün proqramlardan istifadə olunmasıdır.

KeePass Portable proqramına nəzər salaq. Bu proqramda bütün parollar şifrələnmiş faylda saxlanılır. Fayla daxil olmaq üçün ağıllı (düşünülmüş) şəkildə yaradılmış paroldan istifadə etmək olar. Bu zaman proqram həmin parolu açıq şəkildə ekranda əks etdirmir. Resursa daxil olma parolunu daxil etmək üçün (məsələn, ya müəyyən saytdan, yaxud da elektron poçtdan) resursu siyahıdan seçməli və kontekst menyudan Copy Password To Clipboard əmrini aktivləşdirmək lazımdır (şəkil 13.). Parol mübadilə buferinə yerləşəcək. Daha doğrusu,

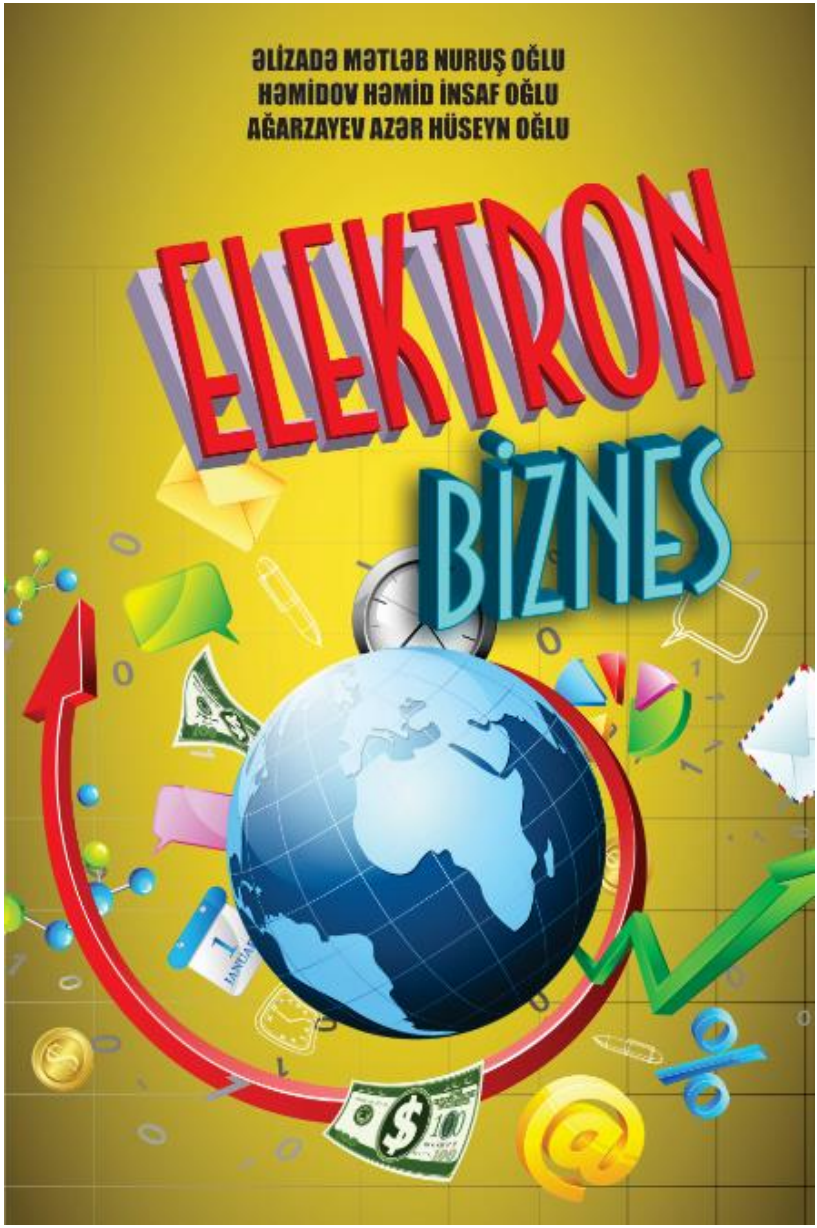
düşmən nə qədər diqqətli olsa da, parolu nə ekranda görəcək, nə də ki, onun klaviaturadan yığıldığının şahidi olacaq. Sonrakı mərhələdə dialoq pəncərəsinə keçid almaq üçün parolu mübadilə buferindən daxil olma sahəsinə gətirmək lazımdır (klaviatura üzərindəki Ctrl+V düymələri kombinasiyasını sıxmaqla və ya (Вставить контекстного меню-Kontekst menyunu daxil et) əmrini seçməklə). Parol o dəqiqə "ulduz" şəkilində əks olunacaq. Bir neçə saniyə ötdükdən sonra parol avtomatik olaraq mübadilə buferindən kənarlaşacaq.



Şəkil 13. KeePass Portable proqramının ekrana açılmış pəncərəsi

Proqram istifadəçiyə verilmiş uzunluqda olan təsadüfi parolu generasiya etməyə də imkan verir. Bununla yanaşı istifadəçi proqramın onun üçün yaratdığı parol haqqında məlumatsızda ola bilər (yəni parol avtomatık yaradıldığı üçün bu barədə istifadəçiyə məlumat verilmir).

KeePass Portable sistemə qoşulmağı istifadəçidən tələb etmir, çünki proqramı fləş qurğusunda gətirib kompüterə daxil etdikdən sonra onun işə salınması bilavasitə fləşsiz həyata keçirilir.


ƏLİZADƏ MƏTLƏB NURUŞ OĞLU
HƏMİDOV HƏMİD İNSAF OĞLU
AĞARZAYEV AZƏR HÜSEYN OĞLU
ELEKTRON
BİZNES

KOMPÜTER VİRUSLARI VƏ ONLARLA MÜBARİZƏ

İstifadəçi İnternetə qoşulan zaman İnternetdən fərdi kompüterə daxil olan ziyanverici viruslara qarşı həyata keçirilən müdafiə tədbirləri şəbəkələrarası ekranlaşdırıcı avadanlıqların köməkliyi ilə yerinə yetirilir. Belə avadanlıqlara nümunə olaraq şəbəkələrarası ekran proqramlarını göstərmək mümkündür. Hesablama texnikasında bu tip proqramları *brandmayer* və ya *Firewall* adlandırırlar.

Brandmayerlərin hansı funksiyanı yerinə yetirməsi onların necə sazlanmasından asılıdır. Adətən onlar digər kompüterlərin Sizin istifadə etdiyiniz fərdi kompüterin resurslarına daxil olma cəhdinin qarşısını alır və Sizin kompüterinizdə istifadə olunan proqramlara və İnternetə göndərilən informasiyaya nəzarət edirlər. Məsələn, troya adlanan viruslar İnternetdən və ya elektron poçtundan Sizin kompüterə daxil olub kompüterinizdə olan fayllar haqqında informasiya toplayaraq pisfikirli (bədəməlli) kompüter istifadəçisinə göndərir. Burada məqsəd müxtəlif ola bilir: heç bir fəaliyyətə ziyan vurmadan mümkün kommersiya təkliflərinin qiymətləndirilməsi üçün məlumatların toplanması naminə və ya ciddi sənaye casusluğu ilə məşğul olmaq üçün tutarlı səviyyədə əhəmiyyət kəsb edən informasiyaların əldə olunması xatirinə. Belə proqramlar Sizin kompüterə daxil etdiyiniz parolları izləməklə yanaşı digər məxfi (konfidensial) proqramları da nəzarətdə saxlaya bilir.

Brandmayerlərdən başqa İnternetlə bağlı təhlükələrin qarşısını almaqdan ötrü (casus proqramların axtarılması və

neytrallaşdırılması) *spyware* adlanan proqram təminatından da istifadə edilir.

Troya viruslarından başqa İnternetdən rəsmi şəkildə təqdim edilən proqram təminatı təşkilediciləri (komponentləri) bir çox hallarda proqram modullarına malik olurlar ki, onlarda Sizin istifadə etdiyiniz kompüter haqqında məlumat toplamaqla yanaşı Sizin icanəniz olmadan (Sizdən xəbərsiz) Sizə məxsus olan informasiyanı proqram istehsalçılarına göndərə bilirlər. Bir çox hallarda istehsalçı şirkətlər bu şəkildə informasiya toplanmasını və İnternet vasitəsi ilə onlara çatdırılmasını istifadəçinin işinə ziyan vurmayacağını sübut etməyə cəht göstərirlər və bu əməliyyatın hətta istifadəçiyə müəyyən qədər xeyir gətirəcəyini də sübut etmək istəyirlər. Nəzərə alınmalıdır ki, istənilən kompüter istifadəçisi ona məxsus olan informasiyanı gizli saxlamaqla yanaşı digər kompüter istifadəçisinə göndərməməyə də tam ixtiyarı vardır. Bu baxımdan da kompüter istifadəçisinin brandmayerdən istifadəsi məsləhətdir. Bununla o, fərdi kompüterini casus proqramlarından müdafiə etmiş olur.

Windows əməliyyat sisteminin bütün versiyalarında fərdi kompüterin viruslardan müdafiə edilməsi üçün sistemin proqram təşkilediciləri əlavə olunmuşdur. Onların arasında brandmayerlərə də rast gəlmək mümkündür (kompüterlərin susma rejimində brandmayer qoşulmuş vəziyyətdədir).

Bir çox hallarda istifadəçilər fərdi kompüterlərinin təhlükəsiz işləmələri üçün əlavə proqramlardan da istifadə edirlər, məsələn, kompüterə antivirus və ya anticəsus proqramlarının yüklənməsi məsəhətdir.

İstifadəçi nəzərə almalıdır ki, istehsal olunan bir çox antivirus proqramları bir-biri ilə uzlaşmır və bununda nəticəsində bir-birinə maneçilik edərək işləyirlər. Nəticədə hər

bir antivirus proqramı digərinə mane olur, virusun aşkarlanaraq aradan götürülməsində birinci olmaq istəyir.

Bu baxımdan da fərdi kompüter istifadəçisi istehsal olunan antiviruslardan birinə üstünlük verməli və seçdiyi antivirus proqramını fərdi kompüterinə yükləməlidir.

Bir çox hallarda fərdi kompüter istifadəçisinə dövrü olaraq digər antivirus proqramlarından (onlardan daim istifadə etməsələrdə) bəhrələnməyi məsləhət bilirlər. Məsələn, istifadəçi "Doktor Veb" şirkətinin rəsmi saytına daxil olaraq *Curelt!* adlanan antivirus proqramının pulsuz variantını kompüterinə yükləyər, ondan istifadə edə bilər.

Əksər antivirus və anticəsus proqramlarını fərdi kompüterə yükləmək tələb olunur. Onlar mütəmadi olaraq istifadəçinin fərdi kompüterini yoxlayır, istifadə zamanı açıq qalmış fayllara virusların daxil olmasına maneçilik göstərirlər. Bununla da Sizin kompüterinizin tutarlı səviyyədə təhlükəsiz iş rejimi təmin edilimiş olur.

AÇIQLAMA: Əksər istifadəçilər fərdi kompüterlərə düşən virusları bir-birindən fərqləndirə bilmir. Onlar ümumi halda bütün virusları ancaq ziyan vuran kompüter virusu kimi tanıyır. Bu sözsüz ki, düzgün fikir deyil. Nəzərə almaq lazımdır ki, viruslar müxtəlif ziyanverici proqram təminatıdır.

Virus nədir?

Kompüter virusu kompüterdəki fayla və ya proqrama bərkidilmiş (yapışdırılmış), bir kompüterdən digərinə keçməklə yayılan proqramdır. Viruslar kompüterə düşməklə onun işinə maneçilik edir, kompüterdə yerinə yetirilən əməliyyatları ləngidir, kompüterin əməliyyat sistemini tamamilə korlayır. Virusların yayılmasında əsas rolu kompüterlərdə istifadə edilən fləş qurğuları, bir istifadəçinin

digərinə məktub göndərdiyi zaman istifadə etdiyi e-mail, istifadəçilər arasında piratlıq (oğurluq) yolu ilə birindən digərinə ötrülən, çox istifadə edilən virus yoluxmuş proqramlar oynayır.

Soxulcan nədir?

Soxulcanları da müəyyən dərəcədə virus saymaq olar. Soxulcanlar kompüterdən kompüterə yayılırlar. Onların viruslardan əsas fərqi istifadəçinin köməkliyi (fəaliyyəti) olmadan kompüterlərdə səyahət etməsidir. Soxulcanın ən böyük qorxusu sistemdə özü-özünü modifikasiya etməsidir (kopiyalamasıdır). Soxulcan çoxalmaqla minlərlə kompüterə öz kopiyasını göndərə bilir.

Troya atı nədir?

Troya atı yalanlardan ibarətdir. İlk baxışda troya atı istifadəçiyə özünü lazımlı proqram kimi göstərir. Amma fərdi kompüteri işə salandan sonra hər şey alt-üst olur. Əməliyyat sistemi işə düşdükdən sonra troya atı faylları proqramdan kənarlaşdırmaqla onlarda olan informasiyaları məhv edir. Troya atının digər növü də mövcuddur, o, kompüterlərə düşərək istifadəçidə qıcıqlanma yatarmaqla onu əsəbləşdirir (istədiyi ölkənin himnini çalır, mənasız sözlər ilə istifadəçini əsəbləşdirir, hazırlanmış materialı müxtəlif rənglərlə rəngləyir və s.), kompüterdən heç bir faylı kənarlaşdırmır, sadəcə olaraq istifadəçinin işinə maneçilik edir. Viruslardan və soxulcanlardan fərqli olaraq troya atı faylları korlamaqla yayılmır, özü-özünü artırmır.

KOMPÜTER VİRUSLARININ TƏSNİFATI

Virusları daxili quruluşuna görə dağıdıcı (destruktiv) və dağıtmayan (qeyridestruktiv) kimi təsnif olunurlar. ***Destruktiv***

viruslar yerinə yetirdiyi funksiyaya görə aşağıdakı kimi təsnif olunurlar:

1.Verilənləri məhv edən (dağıdan) viruslar. Bu tip viruslara "Çernobıl" (1999-cu il) və "Klez.E" (2002-ci il) viruslarını nümunə kimi göstərmək olar.

2.Casus viruslar. Virusun daxili (özəyi) istifadəçi klaviatura üzərindəki istənilən düyməni sıxdıqda informasiyanı oğurlayır, verilənləri xüsusi fayla yazaraq virusun müəllifinə göndərir.

3.Virusa yoluxmuş kompüterdən əməliyyat meydanı (platsdarm) kimi istifadə edərək ***spamı*** və ya *paylaşdırılmış "DoS-hücumları"* müxtəlif yerlərə göndərir (kompüterə yoluxmuş bu tip virusları "Zombi-şəbəkə" adlandırırlar).

4.Kripto-viruslar. Sərt diskdə olan informasiyanı açıq açar alqoritmi ilə şifrələdikdən sonra istifadəçiyə təqdim edir.

Bu təsnifat ilə yanaşı virusları yayılma mexanizminə görə də təsnifatı vardır: fayl virusları, makroviruslar, yükləmə virusları və şəbəkə soxulcanları (bunlar haqqında ətraflı məlumat sönrakı bölmələrdə veriləcəkdir).

AÇIQLAMA: XIX əsrin sonlarında Western Union şirkəti özünəməxsus şəbəkə ilə təyin edilmiş ünvana teleqraf məlumatlarının dəfələrlə (dönə-dönə) göndərilməsinə razılıq verir. İlk kommersiya teleqramının göndərilməsi 1864-cü ilin may ayına təsadüf edir. Teleqram stomatoloji xidmətləri reklam etmək üçün Britaniya siyasətçiləri tərəfindən göndərilmişdi.

"Spam" kəlməsi ilk dəfə 1936-cı ildə yaranır. **SP**iced h**AM** sözü "daha tünd vetçina" (qaxac edilmiş donuz əti, donuz budu) kimi açıqlanır, söz Hormel Foods Corporation şirkətinin (Hormel Foods Corporation - Donuz ətindən hazırlanmış kolbasa farşı) ət konservlərini reklam etmək

üçün istifadə olunan əmtəə nişanı kimi istifadə olunurdu.

İkinci Dünya Müharibəsindən sonra həddindən artıq konserv ehtiyatı olan Hormel Foods Corporation şirkəti məhsullarını reklam etmək üçün hər bir küçəyə, döngəyə, binaya, kafeyə, restorana və s. yerlərə "SPAM" sözü olan reklamları yapışdırır. "SPAM" konservlərinin reklamı hətta radio ilə də translyasiya olunur. Hamının zəhləsini tökmüş "SPAM" sözü sonralar İngiltərədə məzhəkəçi-qrup tərəfindən yaradılan "Monti Paytonun uçan sirki" teleşousunda hazırlanan sketçdə (estrada üçün yazılmış kiçik məzhəkədə - pyesdə) geniş istifadə olunur.

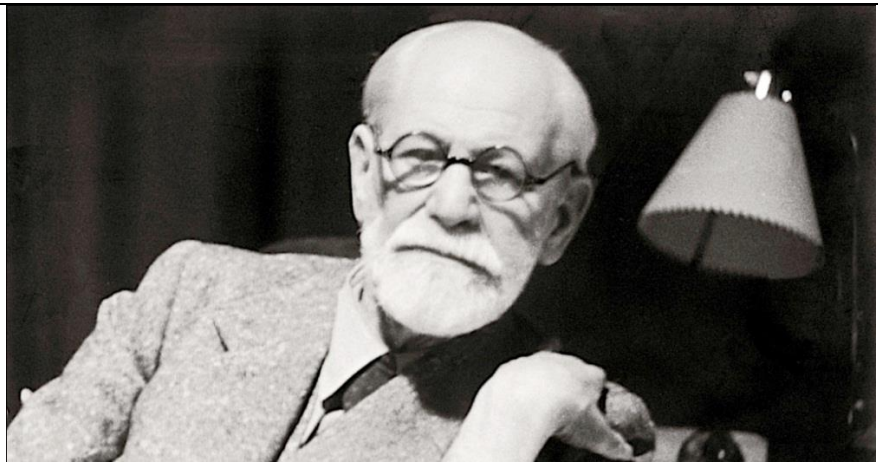
1986-cı ildə Usenet-in keçirdiyi konfransların birində Deyv Rodes hazırladığı maliyyə piramidasını reklam etmək üçün *eyni məlumatlar çoxluğundan* istifadə edir. Məqalənin başlığı belə səslənirdi: "Çoxlu pul qazan". Müəllif bunun yollarını da məqalədə göstərirdi. Bir qədər sonra müəllif hazırladığı testləri müxtəlif ünvanlara dəfələrlə göndərdiyi üçün hamını bezdirir. Testləri alanların yadına Hormel Foods Corporation şirkətinin konservlərə görə verdiyi reklamlar düşür və beləliklə, Deyv Rodesin testləri ilə sketç konservlərinin reklamlarını müqayisə etməyə başlayırlar.

Beləliklə, "Spam" yeni məna qazanır, termin kompüter texnologiyasında bezdirici reklamların göndərilməsində istifadə olunur, daha döğrusu bu əməliyyatı "Spam" adlandırırlar. Spam (ingiliscə "spam") – kommersiya xarakterli reklamların kütləvi şəkildə göndərilməsi və yaxud, kommersiya məlumatlarının və ya buna bənzər reklamların bu reklamları və məlumatları almaq istəməyən müəyyən insanlara dəfələrlə (bezdirməklə, cana gətirməklə) göndərilməsidir. Kompüter texnologoyalarında bezdirici məlumatları yayanları *spamer* adlandırırlar.

Deyv Rodes

Ümumi qəbul olunmuş "spam" termini rus dilində ilk dəfə elektron məktubların göndərilməsində istifadə olundu. Məlumatların ani dəyişdirilməsi sistemində (məsələn, ICQ) soruşulmayan məlumatları SPIM (ingiliscə *Spam over IM*) adlandırırlar. Dünya poçt trafikində 2006-cı ilin məlumatına görə spam 60%-dən 80%-ə kimi (2011-ci ilin məlumatı) təşkil edir.

AÇIQLAMA: *Destkruktivlik* (latincadan tərcümədə normal strukturun pozulması, dağıdılması anlamını verir) insanın özünə və başqalarına mənfi münasibəti və ona uyğun özünü aparmasıdır. Destruktivlik xüsusiyyəti insanlara məxsusdur, əsas fərq onların istifadə etdiyi əşyalardadır: insanlar destruktivliyin daşıyıcılarıdır. Bu fikirlər Ziqmund Freydə məxsusdur.



Ziqmund Freyd (1856-1939). Avstriya psixoanalitiki, psixiatr və nevroloqdur. Z.Freydin məşğul olduğu sahə psixologiyaya, təbabətə, sosiaslogiyaya, antropologiyaya, ədəbiyyata və incəsənətə hiss ediləcək dərəcədə təsir göstərmişdir.

KOMPÜTER VİRUSLARININ MEYDANA GƏLMƏSİNİN QISA TARİXİ

Heç kimə sirr deyil ki, hər bir müasir kompüterin ən böyük və qorxulu düşməni viruslardır. Virus üçün fərdi kompüterin hansı məqsədlə istifadə edilməsi, İnternetə və ya lokal şəbəkəyə qoşulub-qoşulmaması vacib deyildir. Bu gün müxtəlif ziyanverici proqramlar o qədər çoxdur ki, demək olar ki, hər bir kompüter təhlükə altındadır.

Kompüter virusu nədir? Əslində, bu ad altında bir-neçə növ ziyanverici proqramlar gizlənir ki, bunların da çoxdandır ki, hər birinin özünəməxsus kompüterə daxil olmaq metodikası

vardır. Bu günə 50 minə yaxın kompüter virusu məlumdur. Bu kiçik ziyanverici proqramlar aşağıdakı 3 qayda ilə yaşayırlar:

- Çoxalmaq;
- Gizlənmək;
- Pozmaq (xarab etmək).

Hələ viruslarla universal və etibarlı mübarizə vasitəsi yoxdur.

AÇIQLAMA: *Virus* ingilis sözüdür, tərcüməsi maniə, əngəl deməkdir. Rus dilli insanlar bu sözü düzgün tərcümə etməmiş, səhv olaraq virus kimi, yəni mikrob kimi istifadə etmişlər. Əslində söz *vayrus* kimi oxunmalıdır. Bu səhvi biz də qəbul etmişik və indiki zamanda da maniə və ya əngəl yerinə virus kəlməsindən istifadə edirik.

Dərslikdə müəyyən səviyyədə klassik kompüter virusları – "*parazitlər*" nəzərdən keçirilir. Ziyanverici proqramların bu növünün tarixi nə az-nə çox – 40 il əvvələ, keçən əsrin 60-cı illərinin sonuna gedib çıxır. Bu, o zaman idi ki, kompüterlə yalnız fantastik hekayələrin səhifələrində rastlaşmaq mümkün idi. O zaman ABŞ-ın iri tədqiqat mərkəzlərinə mənsub olan azsaylı kompüterlərdə ilk dəfə qeyri-adi davranışlı proqramlar aşkar edilmişdi. İnsanın bütün göstərişlərini yerinə-yetirən normal proqramlardan fərqli olaraq bunlar heç bir əmrə tabe olmurdular, kompüter daxilində anlaşılmaz işlərlə məşğul olaraq sistemin işini olduqca ləngidirdilər. Bu qeyri-adi proqramların yaxşı cəhəti o idi ki, bunlar heç nəyi pozmur və çoxalmırdılar. Lakin bu yaxşı cəhət uzun sürmədi...

İlk kompüterlərin, şəbəkələrin və şəbəkə protokollarının yaradıcıları gələcəyi görə bilsəydilər, çox güman ki, informasiyanın qorunması problemləri bu gün xeyli az olardı.

İlk vaxtlar kompüterlər binalardakı çoxlu sayda otaqları zəbt edən, bahalı, nəhəng texniki sistemlər olduğundan, onlardan yalnız iri dövlət müəssisələri və xüsusi şirkətlər istifadə edə bilirdilər. Müəyyən müddətdən sonra informasiya mübadiləsinə zərurət meydana çıxdı – ilk şəbəkələr yarandı. Lakin həmin vaxtlarda kompüterlər qapalı sistemlər idi və ağ xalatlı ciddi insanlar tərəfindən idarə edilirdi. Buna görə də o vaxtlar xuliqanlıq və ziyankarlıq barədə heç kim düşünməmişdi. Təəssüf ki, tarix kompüter ziyanvericilərinin yaradılması barədə olan çoxlu faktları üzə çıxarmır. Lakin buna baxmayaraq bəzi faktlar məlumdur. Özüçoxalan mexanizmlər (proqramlar) nəzəriyyəsinin əsasını qoyan fizika və piyaziyyat elmləri üzrə görkəmli elmi nəticələrə nail olmuş, dünya şöhrətli macar əsilli amerikalı alim Con fon Neyman (Yanoş Layoş Neyman) (1903-1957) olmuşdur. Con fon Neyman "Mürəkkəb avtomatlar nəzəriyyəsi və təşkili" mövzusunda mühazirələr seriyası oxuyurdu ki, bu mühazirələr də sonralar özütörəyən avtomatlar nəzəriyyəsinin təməlini təşkil etmişdi. Lakin bu, yalnız nəzəriyyə idi.

Həmin dövrdə bu nəzəriyyə tənqidə məruz qaldı və elmi ictimaiyyətin diqqətini cox da cəlb eləmədi. Con fon Neyman 1951-ci ildə belə mexanizmlərin yaradılması metodunu təklif etmişdi.

1957-ci ildə "Nature" jurnalında L.S.Penrouz, həyat yoldaşı, fizika üzrə Nobel mükafatı laureatı Rocer Penrouzla həmmüəllif olmaqla özüçoxalan mexaniki strukturlar haqqında ilk məqaləni çap etdirir. Bu məqalədə təmiz mexaniki konstruksiyalarla bahəm belə strukturlar üçün aktivləşmə, tutub saxlama və azad etmə imkanlarına malik olan ikiölçülü model də şərh edilir. Bu məqalədəki materiallara əsaslanmaqla F.J.Ştal IBM 650 elektron hesablama maşınında istifadə olunan

maşın dilində biokibernetik modeli proqramlaşdırır. Bu proqramda məxluq sıfıra bərabər olmayan sözlərlə qidalanmaqla hərəkət edir.

Məxluq müəyyən sayda simvolları "yeyəndən" sonra çoxalır. Bu zaman yeni əmələ gələn mexanizmlər mütasiya imkanına malik ola bilir. Kibernetik məxluq müəyyən müddət ərzində qidalanmayanda "ölürdü".

1961-ci ildə Bell Telephone Laborototies kompaniyasının (ABŞ) əməkdaşları V.A. Vısotski, X.D. Makilroy və Robert Morris "Darvin" adlandırılan qeyri-adi oyun yaradırlar. O vaxtlar hələ yüksək səviyyəli proqramlaşdırma dilləri yox idi. Oyun Assembler dilindən istifadə edilməklə yaradılmışdı. Bu oyunun mahiyyəti ondan ibarət idi ki, Assemler dilində yazılmış "orqanizmlər" adlandırılan bir neçə proqram komüterin yaddaşına yüklənirdi. Bir oyunçunun yaratdığı (daha dəqiq desək bir növə aid olan) orqanizmlər digər növə aid olan orqanizmləri məhv etməli və onların mövcud olduğu fəzanı zəbt etməli idi. Yaddaşı tamamilə zəbt edə bilən və ya daha cox xal toplaya bilən orqanizmlərlə oynayan oyunçu oyunun qalibi hesab edilirdi. Oyundakı prosesə "hakim" (əlavə proqram) nəzarət edirdi. Bu proqram həm də rəqiblərin mübarizə aparma qaydalarını müəyyən edirdi. Bu sadəcə eksperiment olsada və iştirakçıları təkcə prosesin özü maraqlandırsada məhz bu oyun proqramını ilk kompüter virusu adlandırmaq olardı.

İlk kompüter viruslarının yaradılması 1960-cı illərin sonlarına təsadüf edir. Ədəbiyyatda belə fikirlərə də rast gəlmək olar ki, əslində ilk viruslsr qəsdən zərərli proqramlar kimi yazılan proqramlar deyildi. Yəni təsadüf nəticəsində meydana gələn viruslar da olub. Bunu proqramlar yazılanda buraxılan səhvin nəticəsi hesab edənlər də var. Belə proqramlar ozü özünü köçürməklə kompüterin sərt diskini

korlayırdı (tuturdu). Belə fikirləşənlər də var ki, əksər hallarda viruslar tamamilə məqsədli şəkildə dağıdıcılıq məqsədi ilə yaradılmışdır.

1960-cı illərin sonu, 1970-ci illərin əvvəlində periodik olaraq maynfreymlərdə "dovşan" (The rabbit) adlandırılan proqramlar meydana çıxırdı. Bu proqramlar özlərini klonlaşdırıb sistem resurslarını zəbt edərək onların məhsuldarlığını aşağı salırdı.

Beləliklə, artıq keçən əsrin 70-ci illərində çoxalabilən ilk həqiqi viruslar meydana çıxdı. Belə ki, UNIVAC 1108 kompüteri Pervading Animal adlı virusa yoluxmuş, IBM 360/370 kompüteri isə Christmac tree adlı virusun hücumuna məruz qalmışdı.

1977-ci ildə ilk Apple fərdi kompüterlərinin istehsal olunması və infrastruktur şəbəkəsinin inkişafı ilə əlaqədar olaraq yeni viruslar əsrinin başlanğıcı qoyulur. İstifadə üçün faydalı proqram şəkilində kompüterə daxil olan ilk barbar-proqramı (barbar - mədəniyyət abidələrini dağıdan, məhv edən adam) kompüter işə düşən kimi istifadəçinin hazırladığı bütün məlumatları məhv edirdi.

Növbəti mərhələ - 1970-ci illərin əvvəlində BBN şirkətinin əməkdaşı Bob Tomas tərəfindən özü yerini dəyişən Creeper proqramı yaradıldi. Bu proqram RSEXEC altsistemi üçün nəzərdə tutulmuşdu və proqramların kompüterlər arasında özbaşına yerdəyişə bilməsi imkanını nümayiş etdirməkdən ötrü idi. Creeper proqramı ziyanverici deyildi və onun ilk nüsxəsi məhv edildi. Amma proqramın yaradılma ideyasına əsaslanaraq yaradılan yeni proqram bir kompüterdən digərinə keçə bilən virusun yaradılması üçün istifadə edildi. Bu zaman Reaper adlı daha bir proqram hazırlandı ki, bu da ilk antivirus proqramı idi. Reaper kompüterdən-kompüterə keçərək Creeper-in fəaliyyətdə olan nüsxəsini tapıb məhv edirdi.

1970-ci ildə daha bir əhəmiyyətli hadisə baş verdi. May ayında Venture jurnalında Qreqori Benfordun (Gregory Benford) fantastik "Üzü çapıqlı adam" hekayəsi çap edildi. Həmin hekayədə Virus və Vaccine adlı iki obraz var idi. Bu obrazlardan biri virus, digəri antivirus proqramının ilk təsvirləri idi. İki ildən sonra Devid Gerroldun "Xarli bir yaşında olanda" adlı fantastik romanında sistemi zəbt edən qurda bənzər proqram təsvir edilmişdi.

Rocer Penrouz

Qreqori Benford

"Qurd" termini ilk dəfə 1975-ci ildə Con Brannerin "Sarsıdıcı dalğada" adlı romanında istifadə olunmuşdu.

"Kompüter virusu" termini ilk dəfə 1973-cü ildə Westworld adlı fantastik filmdə istifadə edilmişdi. Bu sözbirləşməsi müasir adamların adət etdiyi mənada, yəni "kompüter sisteminə soxulan ziyanverici proqram" kimi işlədilmişdi.

Nəhayət, 1977-ci il aprelin 20-də kütləvi istifadə üçün kompüter istehsal edildi və bu hadisə özütörəyən proqramların

özünü reallaşdırması şəraitini əhəmiyyətli dərəcədə yaxşılaşdırdı.

1980-ci illərdə kompüterlər xeyli ucuzlaşdı və sayca çoxaldı. Bundan əlavə, bu maşınlar daha məhsuldar idi. Böyük həvəskar entuziastlar bu maşınları daha çox əldə etməyə başladılar. Nəticədə bu 10 illik kompüter dünyasında baş verən hadisələrlə olduqca zəngin oldu. Özütörəyən proqramlar və qurd-proqramlar yaratmaq sahəsində eksperimentlər aparıldı, nəticədə Elk Cloner və Virus adlı proqramlar meydana çıxdı ki, bunlar da ilk kompüter virusları hesab edilir.

Əgər əvvəllər eksperimental nüsxələr yeridildiyi kompüteri heç vaxt tərk etmirdisə, yeni proqramlar laboratoriyadan kənar kompüterlərdə, "azadlıqda" görünməyə başladılar.

1981-ci ildə 15 yaşlı məktəbli Riçard Skrenta Apple II fərdi kompüteri üçün ilk ***yükləmə virusunu*** hazırlayır. Virus çoxda böyük olmayan şeirdən ibarət idi və fərdi kompüter istifadəçisini salamlamaqla özünü biruzə verirdi.

Virus DOS əməliyyat sisteminə yoluxmaqla yayılırdı. Proqram virusa yoluxmamış disketə rast gələn kimi özünü həmin disketə köçürürdü.

Bu virusun təsirindən ilk zərər görənlər Riçardın dostları və tanışları, həmçinin onun riyaziyyat müəllimi olmuşdu.

QEYD: *Yükləmə virusları* verilənləri daşıyanlara yoluxdurur. Öncə disketlər və sərt disk virusa yoluxur. Yükləmə virusu özünü diskin "sıfırıncı" sektoruna yazır (bu sektora həmişə yükləmə proqramları yazılır). Növbəti mərhələdə proqram başqa yerə yazıldığı üçün yükləmə başlayanda virus özünü operativ yaddaşa yazmağa cəhd göstərir ki, sonralar sistem üzərində hökmranlıq edə bilsin. İndiki zamanda belə virusların hökmranlığı artıq sona

çatmışdır, çünki kompüterlərin disketlərdən yüklənməsindən demək olar ki, istifadə edilmir.

Belə viruslarla mübarizə aparmaq üçün daşınabilən qurğuları açanda ehtiyatlı olmaq lazımdır ki, qurğuda avtoişə salma işə düşə bilməsin. Məsələn, onları Total Commander buludundan istifadə etməklə, yaxud da, Windows bələdçisinin ünvan sətirindən istifadə etməklə işə salmaq lazımdır (Yarlıq üzərində mausun sol düyməsini iki dəfə sıxmamaq şərti ilə).

Riçard Skrenta

Aşağıda həmin virus nümunə kimi verilmişdir.

ELK CLONER:
THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER
IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM, TOO
SEND IN THE CLONER!

1980-ci illərdə artıq yüzlərlə dəyişilmiş fəal viruslar mövcud idi. Fərdi kompüterlərin meydana çıxması və yayılması ilə həqiqi epidemiya yarandı. Belə ki, artıq minlərlə virus var idi. Lakin "kompüter virusu" termini ilk dəfə 1984-cü ildə ABŞ-ın Lexay universitetində keçirilən informasiya təhlükəsizliyi üzrə konfransda həmin universitetin əməkdaşı F.Koen tərəfindən istifadə edilmişdir.

İlk "peşəkar" viruslar xeyli sadə idi və istifadəçidən gizlənmirdilər, öz dağıdıcı fəaliyyətlərini (faylların silinməsini, disklərin məntiqi quruluşunun dağıdılmasını) ekrana çıxardıqları gülməli şəkillərlə və "Kilimancaro dağlarının hündürlüyü neçə millimetrdir?" kimi mənasız suallarla və "Qeyri-düzgün cavab daxil edən kimi vinçesterdəki bütün verilənlər məhv ediləcəkdir!!!" kimi yersiz hədələyici zarafatlarla ört-basdır edirdilər. Belə virusların aşkar edilməsi asan həll edilən məsələ idi. Bu viruslar *.com və ya *.exe tipli fayllara qoşulduğundan, həmin faylların ölçülərini dəyişdirirdi. İlk antiviruslar bu cəhəti nəzərə alaraq yoluxmuş faylları təyin edirdi.

1984-cü ilin sentyabrında Fred Koenin ***fayl virusların*** müxtəlifliyinin tədqiq edilməsinə həsr edilmiş məqaləsi çap edilir. Bu virus problemləri ilə bağlı ilk akademik tədqiqat idi. Virus terminindən istifadəni təklif edən Koenin elmi rəhbəri Len Adleman olub. Amma "kompüter virusu" terminin müəllifinin Fred Koen olduğu qəbul edilmişdir. Fred Koen isə özünün

"Kompüter virusları ilə eksperimentlər" əsərində "kompüter virusu" terminin müəllifinin L.Adleman olduğunu göstərmişdir.

Fred Koen

Leonard Adleman

Apple II üçün digər viruslar A&M Texass universitetinin tələbəsi Coo Dellincer tərəfindən 1981-ci ildə yaradılmışdı. Bu virus həmin komüterdə istifadə edilən MS DOS 3.3. -ə hesablanmışdı. Bu virusun ikinci versiyası onun müəllifinin xəbəri olmadan digərlərinin də əlinə keçir və bütün universitetə yayılır. Virusda olan səhv o vaxtlar CONGO adı ilə məşhur olan populyar oyunun qrafikasını korlayırdı. Nəticədə cəmi bir neçə həftə ərzində həmin proqramın bütün (pirat) nüsxələri işləyə bilməyən vəziyyətə düşürdü. Müəllif vəziyyəti düzəltmək üçün əvvəlki virusun əvəz edilməsi üçün nəzərdə tutulan yeni, səhvi düzəldilmiş virusu dövriyyəyə buraxır. Virusun mövcudluğunu yaddaşda "(GEN 0000000 TAMU)" yoluxma sayğacının $B6E8

sürüşməsi və ya yoluxmuş diskin sıfırıncı sektorunun sonunda olmasına görə aşkar etmək olurdu.

QEYD: *Fayl virusları* kompüterdə fayldan istifadə etdikdə tətbiq edilir və özlərini ya faylın əvvəlinə, ya ortasına, ya da ki, axırına yazırlar. Deməli, istifadəçi faylı açanda viruslar da onunla birlikdə işə düşür. Qeyd etmək lazımdır ki, bir virusun kompüterə daxil olması kifayətdir ki, bir müddətdən sonra kompüterdəki bütün fayllar virusa yoluxmuş olsunlar.

Fayl virusları keçən əsrin 90-cı illərində geniş yayıldılar (əsasəndə disklərə yazılmış proqramlar əldən-ələ gəzəndə). İndiki zamanda onlar "modda" deyillər, onları akah etmək çox asanlaşıb.

Maraqlı cəhət odur ki, ilk viruslar piratlarla (quldurlarla) mübarizə məqsədi ilə yaradılmışdı. 1985-ci ildə 10 minlərlə kompüter Pakistanlı Əlvi qardaşları tərəfindən yaradılmış Brain virusuna yoluxmuşdu. Hiyləgər Əlvi qardaşları özlərinin proqram biznesini həyata keçirərək bilərəkdən öz proqram məhsullarını ziyanverici elementlə təchiz edib oğurluq nüsxələrdən istifadə edilməsinin qarşısını almağa çalışırdılar. Pakistan virusunun meydana çıxmasından keçən 10 il ərzində həmin virusun törəmələri bütün dünyaya yayıldı. Bu virusların təhlükəliliyi ondadır ki, istənilən proqramda (onun baş və icra faylında) mütləq şəkildə gizlənə bilir. Virusun kompüterə daxil olması və oradakı .com və .exe tipli faylları yoluxdurması üçün proqramı tək bir dəfə işə buraxmaq kifayətdir.

Əmcad Fərux Əlvi və Basit Fərux Əlvi qardaşları

1986-cı ildə IBM PC üçün ilk The Brain virusu yaradılır.

Kompüter viruslarının növbəti inkişaf mərhələsi 1987-ci ildən başladı. Bu dövrdə nisbətən ucuz IBM PC platformalı kompüterlər geniş yayılmağa başlamışdı. Bu da virusa yoluxan kompüterlərin sayının kəskin artmasına səbəb oldu. Məhz 1987-ci ildə üç böyük kompüter virusu epidemiyası baş verdi.

Əlvi qardaşlarının yaratdığı, birinci kompüter epidemiyasına səbəb olan Brain virusu 1987-ci ildə aşkar edilir.

McAfee-nin açıqlamasına görə təkcə ABŞ-da bu virusa (Brain virusu nəzərdə tutulur) 18 mindən çox kompüter yoluxmuşdu. Əslində bu proqram Əlvi qardaşlarının firmasından proqram təminatını oğurlayan yerli piratları cəzalandırmali idi. Proqramda onu yazan qardaşların adları, ünvanları və telefonları göstərilmişdi. Lakin heç kimin gözləmədiyi çox tez bir müddət ərzində The Brain virusu Pakistan sərhədlərini aşaraq bütün dünya üzrə yüzlərlə kompüterə yoluxdu. Brain virusu həm də ilk stels-virus hesab

edilir. Ona görə ki, yoluxmuş sektoru oxumağa cəhd edəndə proqram yoluxmuş sektorun orijinalını (yəni yoluxmamış variantını) təqdim edirdi.

İkinci epidemiya kompüterlərə ABŞ-ın Lexaysk universitetindən noyabr ayında yayılmağa başlamışdı. Həmin virus bir neçə gün ərzində universitetin hesablama mərkəzinin kitabxanasına aid olan yüzlərlə disketin və tələbələrin şəxsi disketlərinin məzmununu məhv etmişdi. Epidemiya müddəti ərzində dörd mindən çox kompüter bu virusa yoluxmuşdu.

1988-ci ilin may ayının 13-də eyni zamanda bir neçə universitetdə və firmada "Jerusalem" adlanan virus aşkar edildi. Həmin gün kompüterə yüklənən fayllar məhv edilmişdi. Bu, həqiqi epidemiyaya səbəb olan ilk MS-DOS viruslardan biri idi. Avropada, Amerikada və Yaxın Şərqdə kompüterlərin bu virusa yoluxması barədə xəbərlər yayıldı.

60 000 baytdan ibarət olan bu proqram UNİX Berkeley 4.3 əməliyyat sistemini zədələmək üçün yaradılmışdı. Virus yaradılanda əsas məqsəd bu proqramın gizli şəkildə ***ARPANET şəbəkəsi*** ilə əlaqəsi olan hesablama sisteminə daxil olub, ona zərər vermədən həmin sistemdə aşkar edilmədən qalması olmuşdu. Bu virusa informasiya sistemində mövcud olan parolları aşkar edən komponentlər daxil edilmişdi. Bu da həmin proqrama sistemin leqal istifadəçiləri kimi maskalanmağa imkan verirdi. Əslində isə proqramın əsas işi çoxalmaq və sürətləri göndərməkdən ibarət idi. Virus müəllifin fikirləşdiyi kimi tam təhlükəsiz və qizli qala bilmədi, çünki proqramın hazırlanma məhələsində bəzi səhvlərə yol verilmişdi və bu da virusun idarə edilməyən sürətlə özbaşına çoxalmasına səbəb olmuşdu.

AÇIQLAMA: 1958-ci ildə ABŞ prezidenti D.Eyzenxayerin təşəbbüsü ilə yeni dövlət strukturu, strukturun tərkibində isə gələcək problemlərin həlli üçün ARPA (Advanced Research Projects Agency) agentliyi yaradıldı. Agentlik qarşısında duran əsas məsələ müdafiə sahəsində yeni və perspektiv elmi layihələrlə bağlı məsələlərin həll edilməsi idi. Məqsəd bir idi – hərbi işlərdə Sovet dövləti Amerika Birləşmiş Ştatlarını ötüb keçməməli.

Buna səbəb dünyada ilk hesablama şəbəkəsinin 1956-1960-cı illərdə keçmiş sovetlər məkanında, Qazaxstanda akademik Lebedevin və Bursovun rəhbərliyi ilə yaradılması idi. Şəbəkəyə "Diana I" və "Diana II" adı verilmişdir.

Ö dövrdə əsas məsələ agentlik tərəfindən kompüterlər arasında verilənlərin mübadiləsini həyata keçirən elektron şəbəkənin yaradılması idi. Şəbəkə ARPANET adlandırıldı (Net –ingiliscə "şəbəkə" anlamını verir).

ARPANET şəbəkəsinin yaradılmasında istifadə edilən bütün təşkiledicilər sonralar tamamilə İNTERNET şəbəkəsində istifadə olundu.

İnternetin yaradıcısı kim olmuşdur sualına cavab vermək çətindir. Suala təxmini cavab belədir: şəbəkə bir nəfər tərəfindən deyil, çoxlu sayda alımlər və bu sahədə peşəkar olan şəxslər tərəfindən yaradılmışdır.

Bu barədə məlumata 2013-cü ildə texniki jurnalların birində çap edilmiş maqələdə rast gəlinir. Məqalədə şəbəkənin yaradılma təşəbbüskarının Cozef Liklayder (Joseph Carl Robnett Lieklider: 1915-1990) olduğu qeyd olunur.

Ümumiyyətlə, İnternetin yaradıcılarından birinin Pol Barana olduğunu (Paul Aleksandr Baran: 1926-2011) hesab etmək düzgündür. 1959-cu ildə "RAND Corporation"

şirkətində işləyərkən Pol Barana nüvə hücumlarından müdafiə olunmaq üçün şəbəkə sisteminin yaradılması ilə məşğul olur. Əsas məsələ şəbəkə vasitəsilə ötürüləcək məlumatların "paket"lər formasına salınaraq ötürülməsi və bu məqsədlə ötürülən informasiyanın həddindən artıq sıxlığa malik olması idi.

Bu ərəfədə informasiyanın kommunikasiya şəbəkələrində paketlər formasında ötürülməsi məsələsini ingilis fiziki Donald Devis də (Donald Watts Davies: 1924-2000) irəli sürür və maliyyə çatışmazlığı üzündən problem həllini tapa bilmir. Nəzərə almaq lazımdır ki, "RAND Corporation" şirkəti Amerikanın starteji mərkəzi olduğu üçün şirkətdə bu sahə ilə bağlı yerinə yetirilən işlər vaxtlı-vaxtında həyata keçirilidi, çünki şirkətin maliyyə təminatı lazımı səviyyədə yerinə yetirilirdi.

Çoxsaylı mütəxəssislər qrupu bu baxımdan da İnternetin yaradılmasını məhz həmin şirkətin adı ilə bağlayırlar. Digər tərəfdən də 1963-cü ildə vahid kompüter şəbəkəsinin yaradılması ideyası şirkətdə laboratoriya müdiri işləyən Cozef Liklayderə tapşırıldığı üçün bu məsələnin doğruluğunu müəyyən qədər təsdiq edir.

İdeyanın tamamilə həyata keçirilməsi ərəfəsində (1966-cı il) Cozef Liklayder şirkəti tərk edir və problemin həlli Bob Teylora (Robert William Taylor: 1932-) tapşırılır. B.Teylor tərəfindən yaradılan vahid kompüter şəbəkəsi 4 müxtəlif istiqamətdən məlumatları qəbul etməklə təhlil edirdi. Alınmış məlumatları təhlil etmək həddindən artıq çətinliyə gətirib çıxarırdı, çünki hər bir istiqamətdən gələn məlumat özünə uyğun terminalda təhlil olunurdu. Bu baxımdan da təşkilatçı müxtəlif istiqamətlərdən daxil olan informasiyaların bir terminala daxil edilməsini və həmin terminalda təhlil

edilməsini məsləhət görür, bu ideyanın həyata keçməsinə üstünlük verir və ideyanı həyata keçirir.

ARPANET şəbəkəsinin yaradılmasına 1966-cı ildən başlanılır. Tədqiqatlar Boston şəhərində yerləşən, Cozef Liklayderin rəhbərlik etdiyi BBN firmasına həvalə olunur. Layihənin yerinə yetirilməsində Kaliforniya ştatının üç universiteti və Yutı ştatının bir universiteti iştirak edir.

Bir-birindən 600 kilometr məsafədə yerləşən iki kompüter arasında ilk əlaqə seansı 1969-cu il, Oktyabr ayının 29-da, 21^{00}-da baş tutur. Bir terminaldan digər terminala ilk ötürülən informasiya "LOGİN" sözü olur.

Sonrakı illərdə şəbəkəyə daha 4 universitet qoşulur. Daha sonra şəbəkənin imkanlarından (1971-ci il) daha 15 universitet istifadə etməyə başlayır. 1973-cü ildə şəbəkəyə Böyük Britaniya və Norveç universitetləri də qoşulur.

Beləlikılə, şəbəkə ümumdünya statusu alır.

1990-cı ildə ARPANET şəbəkəsi öz işini dayandırır, çünki şəbəkə qarşısında qoyulmuş məsələ artıq öz həllini tapmışdı. Şəbəkənin işini onun bazası əsasında yaradılmış yeni şəbəkə - İNTERNET şəbəkəsi davam etdirir.

Cozef Liklayder

Pol Baran

Donald Devis

Bob Teylor

Morris soxulcanının törətdiyi bu insidentə (toqquşma, hadisə, anlaşılmazlıq, münaqişə) görə ən azı 9 milyon saatdan artıq vaxt itkisinə yol verilmişdi. Bu səbəbdən itirilmiş məsrəflərin ümumi məbləği 96 milyon dollar təşkil etmişdi. Əgər proqram əvvəlcədən dağıdıcılıq məqsədi üçün yaradılmış olsaydı zərərin məbləği daha çox ola bilərdi.

Morris soxulcanı 6200-dən çox kompüterə yoluxmuşdu. Bu virusun hücumu nəticəsində şəbəkələrin çoxu beş sutka müddətinə sıradan çıxmışdı. Şəbəkələr üçün kommunikasiya funksiyalarını yerinə yetirən, fayl-serverlər kimi istifadə edilən və eləcə də şəbəkə işinin digər təminat funksiyalarını yerinə yetirən kompüterlər də sıradan çıxmışdı.

Morris soxulcanı ilə mübarizədə fərdi kompüter istifadəçilərinin işi bir qədər asanlaşdı, çünki fərdi kompüterlərdə istifadə olunan platformaların əksəriyyəti və əməliyyat sistemləri ***unifikasiya*** edildi. Nəticədə Microsoft şirkətinin hazırladığı əməliyyat sistemi örtüyü altında işləyən Intel-birgəliyi olan kompüterlər bazarda üstünlük qazandı. Sonrakı hadisələr böyük sürətlə inkişaf etdi.

AÇIQLAMA: *Unifikasiya* (latınca *unus* – bir, *facio* – edirəm, birləşmə) bir-birinə oxşayan (həmahəng) sistemə və ya formaya salınma (gətirilmə) anlamını verir. Texnikada unifikasiya dedikdə müxtəlifliyin (çoxçeşidliliyin) idarə edilməsi (ingiliscə *variety control*, fransızca *gestion de la diversite*) başa düşülür. Texniki unifikasiyanın prinsipləri təkcə istehsalda deyil, fəaliyyətin digər sahələrində hazırlanaqcaq məmulatdan (məhsuldan), onun tərkib hissəsindən və hazırlanma prosesindən ilk növbədə gərəksiz (lazımsız, lüzumsuz) olan çoxçeşidliyi kanarlaşdırmaqdır.

1987-ci ilin son virus epidemiyası yeni il qabağı, dekabrın 30-da başladı. Bu virusu (proqramı) İsrailin Yerusəlim universitetində aşkar edilmiş virus çağırmışdı. Bu virus əhəmiyyətli fəsadlar törədə biməsə də o, qısa vaxt ərzində bütün düyaya yayıla bilmişdi.

Virusların yayıldığı ərəfədə qəzet və jurnallarda informasiya təhlükəsizliyinə həsr edilmiş materiallar nəşr edilsə də, virusları kompüter istifadəçiləri hələ də oyuncaq, eksperiment hesab edirdi. Təhlükə o zaman dərk edildi ki, həmin "oyuncaq" özünü ağıllı orqanizm kimi aparmağa, yəni qarşısına çıxan hər şeyi yoluxdurmağa başladı. Bu, 1988-ci il noyabrın 2-də baş verdi. Həmin gün Kornel universitetinin tələbəsi Robert Morris-oğul qurd-proqram yaradıb işə buraxdı. Morris qurdu "azadlıqda" artıb yayılan ilk şəbəkə qurdu idi. Bu, kompüterin bufer yaddaşını doldurub daşıran ilk qurd idi.

Robert Morris

Ziyanverici "qurd" təxminən saat yarım ərzində 6 minə yaxın kompüteri yoluxdurmuşdu. Bu hadisə cəmiyyəti şok (iflic) vəziyyətinə salmışdı, viruslar şəbəkə boyu yayılmaqda idi. Doğrudur, əvvəlki viruslar da şəbəkə boyu gəzirdi, lakin o vaxtadək hər 10 kompüterdən birini sıradan çıxarmaq heç bir virusa müyəssər olmamışdı. Təcili olaraq sistemlərin təhlükəsizliyi tələblərinə yenidən baxıldı və CERT (Computer Emergency Response Team – gözlənilməz kompüter situasiyalarına cavab əmri) kimi institutlar yaradıldı ki, bunlar da kompüterlərin təhlükəsizliyi ilə məşğul olmağa və virusların ləğv edilməsi üzrə təkliflər verməyə başladı.

1989-cu ildə DATACRIME virusları geniş yayılmağa başladı. Oktyabrin 12-dən etibarən bu viruslar fayl sistemini dağıtmağa başladılar. Bu müddətə kimi isə onlar sadəcə olaraq çoxalırdılar. Kompüter viruslarının bu versiyası 1989-cu ilin əvvəllərində Niderlandda, ABŞ-da və Yaponiyada daha geniş yayılmışdı və həmin ilin sentyabrında təkcə Niderlandda 100 mindən artıq kompüterə (FEHM-ə) yoluxmuşdu. Bu ölkədəki butün kompüterlərin təxminən 10%-ə qədərini təşkil edirdi. Hətta IBM firması da bu təhlükəyə reaksiya verdi və VIRSCAN adlı virus detektoru buraxdı. Bu detektor DATACRIME və digər viruslar üçün xarakterik olan sətirləri (siqnaturaları) tapa bilirdi. Siqnaturalar yığımı istifadəçi tərəfindən dəyişdirilə və ona əlavələr edilə bilərdi.

1989-cu ildə ilk "***troya atı***" AIDS virusu meydana gəldi. Virus sərt diskdə olan informasiyanı əlçatmaz edirdi və ekrana təkcə "Hansısa ünvana 189 dollarlıq çek göndərin" ifadəsi çıxırdı. Proqramın müəllifi çeki reallaşdıranda tutulur və şantaj maddəsi ilə cəzalandırılır.

QEYD: *Troya atı* ziyanverici proqram olasada (viruslardan fərqli olaraq) və özünüçoxaltmaq qabiliyyətinə malik deyil. Troya atı faydalı funksiya yerinə yetirən proqramların altında gizlənməklə özünü maskalayır. Beləliklə, virusunun yayılması bir-başa istifadəçi ilə bağlı olur, çünki o belə virusları İnternetdən istifadə edərkən öz kompüterinə "çəkmiş" olur. İstifadəçi İnternetə qoşulanda və ya sistem resurslarından istifadə edəndə "troya atı"nı işə salan kimi lazım olan səlahiyyətləri ona verir. Oxucunun nəzərinə çatdırmaq lazımdır ki, bu tip virusun geniş yayılmış özəyi texniki ədəbiyyatlarda *bekdor (backdoor)* adlanır və özək pisniyyətli istifadəçinin sistemə ziyanvermə məqsədlə istifadə etdiyi proqramdan ibarətdir (bəzi hallarda pisniyyətli istifadəçi sistemi tam nəzarətdə saxlaya da bilir).

1989-cu ildə həm də antivirus proqram təminatına əks təsir göstərən The Dark Averger adlı ilk virus yaradılır. Bu virus antivirus proqramının kompüteri yoxladığı müddət ərzində yeni faylları yoluxdururdu.

1990-cı il mayın 4-də Amerikanın "And içmə" məhkəməsi virusun müəllifi Morrisə 2 il azadlıqdan şərti məhrum etmə, 400 saat məcburi ictimai əmək və 10 min dollar məbləğində cərimə cəzası kəsdi.

1990-ci ilin əvvəlində Chameleon adlandırılan ilk polimorf virus meydana gəldi. Bu texnologiya tez bir zamanda stels-texnologiya (Stealin) və zirehləmə (Armored) ilə uzlaşdırılmaqla yeni viruslara antivirus paketlərə müqavimət göstərə bilmək imkanı yaradırdı. 1990-cı ilin ikinci yarısında Frodo və Whale adlı iki stels-virus yaradıldı. Bu virusların hər ikisində həddən artıq mürəkkəb olan stels alqoritmlərdən istifadə edilmişdi. 9 Kilobaytlıq Whale proqramında əlavə olaraq şifrələmənin bir

neçə səviyyəsi və düzəliş (otladka) əleyhinə fəndlər tətbiq edilmişdi.

AÇIQLAMA: *Stels-virus* (ingiliscə stealth virus – gözəgörünməyən virus) sistemdə öz varlığını tam və ya hissə-hissə gizlədir. Stels-virus əməliyyat sisteminə müraciət etdikdə, oxuma əməliyyatı yerinə yetirildikdə, əlavə informasiyanı yoluxmuş obyektlərdən oxuyanda (məsələn, yükləmə sektorlarından, fayl sistemi elementlərindən, yaddaşdan və buna bənzərlərdən) özünü biruzə verir.

Stels-aiqoritmlərin istifadə olunması viruslara imkan verir ki, onlar sistemdə özlərini tam və ya hissə-hissə gizlətsinlər. Ən çox stels-alqoritm yoluxmuş obyektlərdə "oxu/yaz" əmri yerinə yetirildikdə yayılır. Stels-virusu istənilən zaman müvəqqəti müalicə etmək olur və yaxud da ona imkan verirlər ki, o, özünü informasiyanın yoluxmamış hissəsi kimi aparsın.

1990-cı ildə Bolqarıstanda dünya üzrə ilk dəfə ixtisaslaşdırılmış (xüsusi) BBS (Bulletin Board System – elektron elanlar lövhəsi) yaradılır. Arzu edən hər kəs lövhədən yeni virus proqramını köçürə bilərdi. Elə həmin dövrdə virus yazmaq məsələlərinə həsr edilən Usenet konfransları fəaliyyət göstərməyə başlayır. Həmin il Mark Lüdviqin "Kompüter virusları haqqında kiçik qara kitab"ı çap edilir.

Kompüter viruslarının qarşısının alınması problemi iri kompaniyaların da diqqətini cəlb edir.

1991-ci ilin əvvəlində Tequila adlı yükləmə virusu kütləvi epidemiyaya səbəb oldu. 1991-ci ilin yayında ilk link-virus peyda oldu və peyda olan kimi də epidemiyaya səbəb oldu.

1991-ci ildə öz bədəninin şəklini dəyişə bilən ***polimorf*** viruslar meydana çıxdı. Windows 95 əməliyyat sistemi praktiki olaraq belə hücuma hazır olduğunu bildirdi və firma Windows 95 əməliyyat sisteminin beta-versiyasını 160 testediciyə payladı. Kompütredə istifadə olunan diskləri antivirusa yoxlayan firma əməkdaşı bütün disklərin Form adlanan yükləyici virusla yoluxduğunun şahidi oldu. Halbuki, prinsipcə yeni əməliyyat sisteminin (Windows 95-in) ilkin təqdimatına həsr edilmiş mərasimdə onun hər cür virusdan tamamilə qorunduğu bildirilmişdi. Bir-neçə aydan sonra bu fikir alt-üst oldu.

QEYD: *Polimorfizm* (yunanca πολυ - çoxlu + μορφή - forma, xarici görünüş) kompüter viruslarının skan-sətir (və ya evristika) vasitəsilə aşkarlanmasını çətinləşdirən texnikadır. Belə texnikadan istifadə edən virus polimorf adlanır.

Microsoft Word sənədlərini yoluxduran ilk ***makrovirus*** aşkar edildi. Bu, artıq sadəcə qeyri-adi şəkildə icra edilən fayl deyil, xüsusi ssenari idi. Bir ay ərzində "*Concept"* adlı makrovirus bütün Yer kürəsini dolaşaraq dünyada onlarla şirkətin mətn redaktorunu iflic etmişdi. Bugün Concept virusunun 100-ə yaxın modifikasiyası mövcuddur.

QEYD: *Makroviruslar* çoxalma mexanizminə görə *fayl* viruslarından fərqlənmirlər. Bunların əsas xüsusiyyəti icra edilən faylları deyil, müəyyən formatda olan populyar sənədləri yoluxdurmaqdır. Virusun təhlükəli olmasının digər cəhəti ondan ibarətdir ki, istifadəçi əksər hallarda onu virusa yoluxmuş sanədlərlə birlikdə alır və kompüterini virusa

yoluxdurur.

Makroviruslar bəzi proqramların imkanlarından (mətn, qrafik, cədvəl redaktorları, SUBD və s.) istifadə etməklə həmin proqramların yaratdığı sənədlərə daxil olur. Bu sənədləri *makroslar – prosedurlar* adlandırırlar.

Makroviruslar özlərini makrodildə yazılmış proqram kimi təqdim edir, müəyyən formatda olan sənədlərə yoluxur və sənədi açanda avtomatik işə düşürlər.

İndiki zamanda makroviruslar o qədər də populyar deyillər, çünki müasir makrodili dəstəkləyən proqramlar makrovirusun sənəddə olması barədə öncədən istifadəçini xəbardar edir. Digər tərəfdən makrovirusun işə düşməsinə imkan olarsa, bu zaman istifadəçidən təsadüfi hallarda proqramın sazlanmasını həyata keçirmək tələb edilir.

1992-ci ildə fərdi kompüterlər (PC) üçün ilk virus konstruktorları (VCL), hazır polimorf modullar (MtE, DAME və TPE) və şifrələmə modulları yaradıldı. Bu andan başlayaraq hər bir proqramçı öz virus proqramına rahatca şifrləmə funksiyası əlavə edə bilərdi. 1992-ci ilin sonunda Windows 3.1 üçün WinVer adlı ilk virus peyda oldu.

1993-cü ildə SatanBug virusu Vaşingtonda çoxsaylı kompüterlərə yoluxur. Virusun müəllifi 12 yaşlı oğlan idi.

1993-cü il daha çox virusların fayllara yoluxmaq, sistemə daxil olmaq və s. üçün qeyri-adi üsullardan istifadə etməsi ilə yadda qalıb.

Bunlara nümunə kimi:

- Intel 80386 prosessorunun qorunma (təhlükəsiz) rejimində işləyən PMBS virusunu;
- Kompanion virusların alqoritm diapazonunu xeyli genişləndirən Shadowgard və Carbuscle viruslarını;

- Yoluxduğu fayllarda öz kodunu gizlətmək üçün prinsipial yeni fəndlərdən istifadə edən Cruncher virusunu göstərmək olar.

Virus generatorlarının yeni versiyaları və yeni virus generatorları (PC_MPC və G2) yaradılır. Bu dövdrə məşhur virusların sayı minlərlə idi. Antivirus kompaniyaları polimorf viruslarla mübarizə üçün bir sıra səmərəli alqoritmlər hazırlaya bilsələr də çox vaxt yalançı təsirlənmə (işləmə) problemi ilə də üzləşirdilər. 1994-cü ilin əvvəlində Britaniyada iki mürəkkəb polimorf virus – SMFG.Pathogen və SMFG.Queeg peyda olur. Virusun müəllifi BBS stansiyaya yoluxmuş fayllar yerləşdirir. Bu da epidemiyaya və kütləvi informasiya vasitələrində çaxnaşmaya səbəb olur. Virusun müəllifi həbs edilir.

1994-cü ilin yanvarında obyekt modullara (OBJ-fayllara) yoluxan ilk virus – Shifer, həmin ilin yazında isə C və Pascal-da yazılmış ilkin proqram mətnlərinə yoluxan SrcVir viruslar ailəsi meydana çıxır. 1994-cü ilin iyununda OneHalf epidemiyası başlayır.

1995-ci ildə kifayət qədər mürəkkəb bir neçə virus – NightFall, Nostradamus, Nutcracker peyda oldu. İlk "ikicinsli" virus (RMNS və BAT-virus Winstart) yaradılır. ByWay və DieHard2 virusları geniş yayılır. Butün dünya üzrə kompüterlərin bu virusa yoluxması haqqında xəbərlər yayılir. 1995-ci ilin fevralında Windows 95-in beta-versiyası ilə insident yaşanır. Bütün disklər Form adlı MS-DOS virusa yoluxmuşdu.

1995-ci ildə Windows-un yeni rəsmi versiyası olan Windows 95 əməliyyat sistemi işıq üzü görur. Bu məsələyə həsr edilmiş mətbuat konfransında Bill Qeyts söyləmişdi ki, virus təhlükəsi artıq sona çatmışdır. Həqiqətən də Windows istehsal olunan zaman əməliyyat sistemi MS-DOS üçün mövcud olan viruslara çox davamlı idi. Lakin həmin ilin avqustunda Microsoft

Word üçün ilk Concept adlı virus peyda oldu və bu virus bir neçə həftə ərzində butün dünyaya yayıldı.

1995-ci ildə firma Microsoft Windows-95 əməliyyat sistemini disketlərdə istehsaldan buraxır. Artıq əməliyyat sistemi virusa yoluxmuş idi.

1996-cı ildə Tom Neff müxtəlif BBS-lər üzrə "Təhlükəli yükləmə proqramlarının siyahısı"nı yaymağa başlayır və bu siyahıya həmin dövr üçün məşhur olan vandal proqramların adları daxil edilir. Sonralar aşkar edilmiş troya proqramlarının və MS-DOS üçün "sındırılmış" (və ya adları dəyişdirilmiş) kommersiya proqram təminatının surətləri daxil edilmiş həmin siyahı qışa formada "çirkli sıra" («грязная дюжина») adı ilə geniş istifadə edilməyə başlanır.

1996-cı ilin iyununda OS2.AEP virusu yayılmağa başlayır. Bu OS/2 əməliyyat sisteminin EXE-fayllarını nəzakətlə yoluxduran ilk virus idi. Bu vaxta kimi ancaq OS/2 əməliyyat sistemi üçün təkcə kompanion-viruslara rast gəlinmişdi.

Belə güman edilir ki, Unix əməliyyat sistemləri ailəsi üçün ilk viruslar eksperimentlərin aparılması fonunda (gedişində) Fred Koen tərəfindən yazılıb. 1980-ci illərin sonunda virusların "Sh" dilində ilkin mətnləri çap edilir.

Linux əməliyyat sistemi üçün ilk virus (Bliss) 1996-cı ilin sentyabrinda aşkar edildi. 1996-cı ilin oktyabrında viruslara həsr edilmiş elektron jurnalda (VLAD) Staog virusunun ilkin mətni dərc edilir. 1995-ci ildə Mark Lüdviqin "The Giant Black Book of Computer Viruses" adlı kitabı dərc edilir və həmin kitabda FreeBSD üçün Snoopy virusunun ilkin mətni verilir. Snoopy və Bliss virusları C (Si) dilində yazılmışdı və praktik olaraq minimal dəyişdirmə ilə ixtiyari Unix əməliyyat sisteminə oxşar əməliyyat sistemlərinə keçə bilirdi.

1996-cı ilin yanvarında Windows 95 əməliyyat sistemi üçün Win95.Boza adlı ilk virus peyda oldu. Bir qədər sonra meydana çıxan Win95.Punch adlı rezident virusu Windows 95 əməliyyat sistemi istifadəçilərinin etibarını alt-üst etdi. Həmin ilin martında Windows 3.0/3.1 üçün yazılmış Win.Tentacle virusu ilə bağlı ilk epidemiya başlandı. Bu virus Fransanın bir-neçə idarəsinə məxsus kompüter şəbəkələrini yoluxdurdu. Buna qədər bütün Windows-viruslar yalnız virusu təsvir edən elektron jurnallarında və viruslarla maraqlananların kolleksiyalarında saxlanılırdı. Bu ərəfədə ancaq MS-DOS əməliyyat sistemi üçün yazılmış yükləyici və makroviruslar azad yayılmaqda davam edirdi. Həmin il Microsoft Excel elektron cədvəli onun üçün xüsusi olaraq yazılmış Laroux adlı makrovirusa tutulur.

1997-ci ildə FTP və mIRC-qurdlar kimi yeni virus növləri, 1998-ci ilin iyun ayında Win95.CIH virusu peyda oldu. Bu sonuncu virus ilk dəfə 1999-cu ilin aprel ayının 26-da aktivləşdi və sərt diskdəki (vinçesterdəki) informasiyanı məhv edib yerinə "zir-zibil" dolu informasiyanı yazdı. Bununla yanaşı Win95.CIH virusu fləş qurğusundakı açarın açıq vəziyyətində fləşə informasiyanın yazılmasına icazənin verilməsi zamanı Flash BIOS-u yenidən kompüterə təkrar yazır və ana platanı (lövhəni) sıradan çıxarırdı.

Win95.CIH virusu epidemiyası kompüter istifadəçiləri tərəfindən həm də "Çernobıl" adı ilə tanınır. Çünki o da o dövr üçün Çernobılda baş verən dağıdıcı hadisə kimi ən dağıdıcı virus olaraq tarixə düşmüşdü.

1997-ci ilin fevralında Mıcrosoft Office 97 üçün ilk makroviruslar meydana gəlir. İlk viruslar təkcə Word 6/7-nin yeni formatına təsir göstərsə də tezliklə Mıcrosoft Office 97-nin sənədlərinə də yönəlmiş olur. 1997-ci ilin martında MS Word

6/7-ni yoluxduran ShareFun makrovirusu geniş yayılır. Bu virus çoxalmaq üçün həm MS Word-ün standart imkanlarından istifadə edir, həm də öz surətlərini yaymaq, həmçinin İnternet vasitəsi ilə göndərmək üçün MS-Mail elektron poçtdan istifadə edir. Bu proqramı haqlı olaraq ilk mail-soxulcan hesab etmək olar. Həmin ilin iyun ayında Windows 95 əməliyyat sisteminin işinə maneçilik edən (əngəl törədən) özüşifrələnən virus yaradılır.

1997-ci ilin aprelində yayilmasından ötrü File Transfer Protocol (FTP) – dən istifadə edən ilk şəbəkə soxulcanı yaradıldı.

1997-ci ilin dekabrında isə şəbəkə viruslarının yeni forması olan mIRC soxulcanları meydana gəldi.

1998-ci ilin əvvəlində Win32.HLLP.DeTroie viruslar ailəsi epidemiya yaratdı. Bu viruslar yerinə yetirilən fayllara yoluxmaqla barabər öz "sahibinə" yoluxan kompüter haqqında informasiya da göndərirdi.

1998-ci ildə Kaliforniyalı iki yeniyetmə virus hazırlayır və bu virusla Pentaqonun 500-dən artıq kompüterini yoluxdurur.

1998-ci ilin fevralında Excel prposessorunda istifadə olunan düsturları yoluxduran virusun daha bir yeni forması – Excel4.Paix virusu aşkar edildi. 1998-ci ilin martında Microsoft Access üçün ilk AccessiV virusu, eləcə də MS Office: Access və Word kimi iki müxtəlif əlavəni yoluxduran Cross adlı ilk virus, onların ardınca isə öz kodunu bir Office-əlavədən digərinə keçirən daha bir neçə makrovirusu yaradılır.

1998-ci ilin fevral-mart aylarında ilk polimorf Win32-viruslarla (Win95.HPS və Win95.Marburq) insident qeyd edildi. 1998-ci ilin mayında RedTea.n epidemiyası başladı. Bu virus Windows-un EXE-fayllarına yoluxurdu və yoluxan faylları Eudora elektron poçtu ilə istifadəçilərə yayırdı.

1998-ci ilin avqustunda məsafədə yerləşən kompüterlərin və şəbəkələrin inzibatlaşdırılmasını gizlətmək üçün tətbiq edilən məşhur BackOrifice (Backdoor.BO) utiliti yaradıldı. Bunun ardınca bir neçə oxşar proqram: NetBus, Phase və digərləri yazıldı.

Avqust ayında həmçinin Java-nın yerinə yetirilən modullarını zədələyən Java.StangeBrew virusu peyda olur. Virus İnternet istifadəçiləri üçün heç bir təhlükə yaratmır. Bu səbədən müəyyən məsafədə yerləşən kompüterlərdə virusun çoxalması üçün zəruri olan funksiyalar fəaliyyət göstərə bilmir.

1998-ci ilin noyabrında VBScript.Rabbi virusu yayılmağa başladı. Ckript virusların İnternet-ekspansiyası (təcavüzü) VisualBasic skriptləri (VBS-faylları) yoluxduran üç virusla davam edirdi. Bu viruslar İnternet istifadəçisi Web-səhifələri yaradanda onlara qoşulurdu. Məntiqi nəticə kimi VBScript-viruslar HTML-virusun (HTML.Internal) yaranması demək idi.

1999-cu ildə Melissa hibrid virusu yayılır. Bu virus özündə makrovirusun imkanları ilə şəbəkə soxulcanının imkanlarını birləşdirirdi və çoxalmaq üçün Outlook ünvan kitabından istifadə edirdi. Virus yayılma sürətinə görə o dövrdə mövcud olan bütün rekordları aşmışdı.

1999-cu ildə Melisa virusu çox böyük sayda kompüterlərə yoluxur və istifadəçilərə 80 000 dollar məbləğində zərər vurur. Bu isə antivirus proqramlarına tələbatın kəskin artmasına səbəb olur.

ABŞ-ın hüquq-mühafizə orqanları Melissa virusunun müəlliflərini - 31 yaşlı proqramçı Nyu Cersi və Devid Smiti tapıb həbs edir. Həbs ediləndən bir müddət sonra Devit Smit Federal Təhqiqatlar Bürosu (FTB) ilə əməkdaşlıq etməyə başlayır və bunu nəzərə alan məhkəmə onu yumşaq cəzaya – 20 ay həbsdə qalmağa və $5000 cərimə edilməyə layiq görür. 1999-

cu ilin aprelində CIH ("Çernobıl") virusunun müəllifi tapılır. Bu Tayvan texnologiya universitetinin tələbəsi Çen İnxao idi. Yerli kompaniyalar tərəfindəın virusun təsirindən şikayət olmadığına görə əlində tutarlı məlumat olmayan polis onu həbs etməkdən vaz keçir.

1999-cu ildə CorelGala proqramı üçün ilk makro-virus aşkar edilir. Nəzərə almaq lazımdır ki, həmin ilin yay aylarında ZippedFiles İnternet-soxulcan epidemiyası tüğyan edirdi. Bu proqramın maraqlı cəhəti ondan ibarət idi ki, o "kobud və ya vəhşi" formada geniş yayılmış ilk sıxlaşdırılmış virus proqramı idi.

2000-ci ilin mayında Filippində buraxılmış *I love you* adlı qurd, bəzi hesablamalara görə, kompüter istifadəçilərinə 10 milyard dollardan artıq ziyan vurmuşdu. Növbəti qurd Code Red adlandırılmışdı. Bu, 14 saat ərzində İnternetə qoşulmuş 300 mindən artıq kompüteri yoluxdurmuşdu. Sonralar isə virus yaradıcıları tərəfindən digər dağıdıcı viruslar da yaradıldı. Bunlardan: Nimda (admiN sözünün tərs oxunuşu) və çoxvektorlu qurdu misal göstərmək mümkündür. Bu qurdlar eyni vaxtda müxtəlif üsullarla, o cümlədən, digər qurdların qoyub getdiyi "gizli yollarla" kompüterlərin daxilindəki elektron sxemlərində yayılırdı. O ərəfədə elektron poçtla yayılan MyDoom qurdu ən cəld yayılan qurd kimi məşhurlaşdı.

2001-ci ildə Hollandiyalı tələbələrdən biri Anna Kurnikova virusunu yaratdığı üçün həbs olunur və məhkəməyə müəyyən məbləğ cərimə ödəməklə 150 saatlıq islah işlərinə göndərilir. Məhkəmə virusun Niderland iqtisadiyyatına nə qədər ziyan vurduğunu hesablaya bilmir. Tələbənin mənzilində aparılan axtarış zamanı 7500-dən çox olan virus kolleksiyası aşkar edilir.

Melissa virusunu yaratdığına görə 2002-ci ildə proqramçı Devid Smitə məhkəmə 20 ay müddətinə həbs cəzası verir.

Həmin il ilk dəfə viris WWW-nin işini təmin edən 13 İnternet-serveri sıradan çıxarır.

Ümumi qəbul edilmiş təsnifata görə kompüter virusları 3 əsas tipə ayrılır. Ənənəvi virus – bu, kompüterə gizli düşüb çoxalan və müəyyən problemlər yaradan, məsələn, faylı məhv edən proqramdır. "I love you" adlı virus rekord nəticə göstərmiş, 2000-ci ildə 8 milyard dollarlıq ziyan vurmuşdu.

"***Qurdlar***" kompüterə şəbəkədən daxil olur. İstifadəçiyə yoluxmuş faylı elektron poçtla onun siyahısında olan bütün ünvanlara göndərməyə məcbur edir. Məsələn, 2003-cü ildə *Blaster* adlı qurd 1 milyondan artıq kompüteri yoluxdurmuşdu.

"Troya atı" bilavasitə özü kompüterə ziyan vurmur, lakin kompüterə daxil olan kimi ***xakerlərə*** imkan verir ki, başqalarının informasiyasına müdaxilə edə bilsinlər. QAZ xakerləri 2002-ci ildə "Troya atı" virusundan istifadə etməklə Microsoft şirkətinin məxfi proqramlarına müdaxilə imkanı əldə etmişdilər.

AÇIQLAMA: Lap əvvəllər *xaker* baltadan istifadə etməklə mebel düzəldən şəxsə deyirdilər. Xaker ingiliscə hacker - to hack sözündən törəmədir, *doğramaq*, *parça-parça etmək*, *didib tökmək* anlamını verir. Xaker sözü əsasən hesablama texnikası və proqramlaşdırma sahəsində geniş istifadə olunur.

Əvvəllər tərtib olunmuş proqramlarda buraxılmış səhvləri düzəldən şəxsləri *xaker* adlandırırdılar. Sonralar, XX əsrdən başlayaraq söz daha da məşhurlaşır və pis niyyətlə (qərəzli) tərtib olunmuş proqramlara daxil olmaqla onları korlayan "*kompüter oğru'larını* xaker adlandırırlar.

QEYD: *Qurdlar* və ya *Şəbəkə soxulcanları* müasir viruslar hesab olunur. Belə virusların məqsədi (daha doğrusu marağı) kompüterdə çoxlu sayda faylları yoluxdurmaqdan ibarət deyil. Onların əsas məqsədi İnternetə qoşulmuş kompüterlərə daxil olmaqdır. Bu zaman iki şərt yerinə yetirilməlidir:

1.Virus avtomatik işə düşməlidir (yaxşı olar ki, əməliyyat sistemi ilə birlikdə işə düşsün);

2.Viruisa yoluxmuş fayl istifadəçidən gizlənməlidir.

Avtomatik işə düşən, operativ yaddaşda daim müəyyən funksiya yerinə yetirən virus *rezident* adlanır. İnternetdə və ya lokal şəbəkədə öz surətlərini (kopiyalarını) yayan viruslar *Şəbəkə soxulcanları* adlanır. Əksər Şəbəkə soxulcanları rezident viruslardır.

İnternetdən istifadə etməklə yayılmış viruslar daha qorxuludurlar. Onlar qurbanları olan kompüterə iki mexanizm vasitəsilə daxil olurlar:

1.Standart kommunikasiya servisləri vasitəsilə;

2.Şəbəkə əlavələrində yaranmış "deşik" vasitəsilə, həmçinin Əməliyyat sisteminin özündən istifadə etməklə.

İstifadəçinin nəzərinə çatdırmaq kifayətdir ki, virusların hücumuna qarşı "dayanmaq" və onlarla müəyyən səviyyədə mübarizə aparmaq üçün kompüterdə vaxtlı-vaxtında yenilənmə aparmaq lazımdır.

Qurdlar və ya soxulcanlar Windows əməliyyat sisteminin sistem qovluqlarında özlərinə "yuva salırlar" və indiki zamanda o qədər virus vardır ki, istifadəçi demək olar ki, onların əksəriyyəti haqqında heç bir məlumatı yoxdur.

2003-cü ildə Slammer "soxulcanı" 10 dəqidə müddətində rekord sayda - 75 000-dən çox kompüterə yoluxmuşdu. Virus

Amerikanın Dövlət Departamentinin kompüterlərinə yoluxur və verilənlər bazasını zədələyirdi. Nəticədə ABŞ ***konsulluqları*** dünyada 9 saat müddətində viza verilməsi prosesini dayandırmalı olur.

AÇIQLAMA: *Konsul* – xarici ölkə ərazisində müəyyən dairədə (yəni ərazi sahəsində) öz ölkəsinin maraqlarını müdafiə edən diplomatdır. Konsul (latınca *consul*) başqa bir dövlətin ərazisində (torpağında) yerləşən konsulluq ərazisində daimi yaşama yeri olan, dövlət tərəfindən konsul funksiyasını yerinə yetirilməsi tapşırılan, konsul vəzifəsinə göndərən ölkənin və həmin ölkənin vətəndaşlarının hüquqi və iqtisadi maraqlarını müdafiə edən vəzifəli şəxsdir. Konsul funksiyasını yerinə yetirən şəxs olduğu dövlət ilə razılıq əsasında təmsil etdiyi dövlət tərəfindən xüsusi olaraq ayrılmış (və ya tutulmuş) konsulluq idarəsində işləyir (yaşayır).

Konsulluq idarəsinə rəhbərlik dörd sinifə bölünür: Baş konsul; Konsul; Vitse-konsul və konsulluğun agenti.

Destruktivlik imkanlarına görə virusları aşağıdakı kateqoriyalara bölmək olar:

- Zərərsiz viruslar;
- Təhlükəsiz viruslar;
- Təhlükəli viruslar;
- Çox təhlükəli viruslar.

Təhlükəsiz viruslar kompüterin işinə demək olar ki, təsir göstərmir. Bunlar təkcə özünün çoxalması hesabına diskdəki boş yaddaş sahəsinin həcmini azaldır. Təhlükəsiz virusların təsiri diskdə olan boş yaddaş sahəsinin qrafik, səs və digər effektlərlə azalması ilə məhdudlanır.

Təhlükəli viruslar kompüterin işində fəsadlara səbəb olur.

Çox təhlükəli virusların alqoritminə əvvəlcədən proqramların itməsinə, verilənlərin məhv edilməsinə, kompüterin işi üçün zəruri olan yaddaşın sistem oblastlarına yazılan informasiyanın pozulmasına, hətta kompüter əfsanələrindən birində deyildiyi kimi mexanizmlərin hərəkət edən hissələrinin (deyək ki, bəzi vinçester tiplərinin başlıqlarının) tez sıradan çıxmasına səbəb olan prosedurlar daxildir.

Kompüter viruslarının bəzi tiplərinə məxsusi adlar verilmişdir. Belə ki, icra edilən proqramlardakı qeyri-dəqiqlikdən və onların təkmilləşdirilməməsindən (məsələn, əsas proqramdan altproqrama giriş və altproqramdan əsas proqrama çıxış zamanı dəyişdirilən ünvanlar) istifadə edən viruslar "tələ" adlandırılır.

"Məntiqi bombalar" və ya "gec açılan bombalar" elə viruslara deyirlər ki, bunlar destruktiv təsirini həyata keçirmək üçün uzun müddət və cürbəcür hazırlıq işləri aparır, sonra müəyyən şərtlər kompleksi yerinə yetiriləndə (məsələn, işin müəyyən mərhələsi yerinə yetiriləndə, müəyyən edilmiş vaxt çatanda, proqrama müəyyən istifadəçi müraciət edəndə və s.) işə düşür. Belə viruslar ona görə daha təhlükəlidir ki, onlar uzum müddət dağıdıcı iş aparmalarına baxmayaraq praktik olaraq ozlərini büruzə vermirlər. Belə viruslar o vaxt aşkar edilir ki, əməliyyat sisteminin proqramlarının əksəriyyəti və ya hamısı demək olar ki, iş qabiliyyətini itirmiş olur. Beləliklə, kompüter iş qabiliyyətini tamamilə itirmiş olur.

Soxulcan-viruslar şəbəkə və ya periferiya qurğularının idarə olunmayan əməliyyatları yerinə yetirməsinə (məsələn, printerdə kağızın fasilsiz hərəkət etməsinə, əməliyyat sisteminin daim yenidən yüklənməsinə və s.) imkan yaradır.

"Troya atları" xüsusi təyinatlı proqram təminatı ilə yayılır və onların destruktiv fəaliyyəti kompüter istifadəçiləri üçün tamamilə gözlənilməz olur. Məsələn, belə virusa antivirus proqramının özü yoluxa bilir. "Tpoyalılar" ilk baxışda guya hansısa faydalı (kompüterdə yaddaşın bölüşdürülməsinin yalançı optimallaşdırılması, diskdə informasiyanın yalandan sıxılması və s. bu kimi) funksiyalar yerinə-yetirir. Əslində isə "Tpoyalılar" ya sistemi dağıdır (məsələn, kompüterin vinçesterini aşağı səviyyədə formatlaşdırır və ya informasiyanı çoxsaylı və operativ oxuyub/yazma əməliyyatlarını yerinə yetirməklə disk sürücüsünün (diskovodun) mexaniki sıradan çıxmasına şərait yaradır), ya da nəzarəti digərlərinin ixtiyarına verir.

Troya viruslarının növləri çox müxtəlifdir. Onların bəziləri ümumiyyətlə faydalı funksiya yerinə yetirmir, sadəcə olaraq kompüterin diskində gizli qalır və müxtəlif destruktiv funksiyalar yerinə yetirir. Bəziləri isə istifadəçilərdən qətiyyən gizlənmir və heç kimin şübhələnməyəcəyi manipulyasiyalar aparır. Birinci növ viruslara nümunə kimi Back Orifice adlı məşhur virusu göstərmək olar. Bu virus kompüter şəbəkəsində istifadəçiyə hiss etdirmədən onun kompüterinə nəzarəti demək olar ki, tamamilə istifadəçinin görə bilmədiyi "düşmənə" verir. İkinci tip virusa nümunə kimi saxta MS İnternet Explorer brauzer göstərilə bilər. Microsoft firmasının saytına qoşulanda verilənlərin kompüterdən Microsoftun serverinə ötürülməsinin aktivliyini olduqca çox artırır ki, bu da HTML sənədin (yəni, İnternet-də Veb-səhifənin) oxunması və ya kopiyasının çəkilməsi üçun sadə sorğunun həcmindən dəfələrlə artıq olur.

2003-2012-ci illər müəllif adı KuKu olan Win32.Sality epidemiyası ilə yadda qalıb. Bu polimorf virus bir neçə hissədən ibarətdir, şifrələmə və maskalama sistemindən istifadə edir.

Yerinə yetirilən faylların məzmununu dəyişdirir. Ona görə də belə faylları tam bərpa etmək olmur. Mürəkkəb rəftara və maskalama vasitələrinə malik olması ilə bağlı olaraq adi istifadəçi üçün bu virusun müalicə edilməsi demək olar ki, mümkün olmayan məsələdir. Virusa yoluxan kompüter dünyadakı ən iri bonet şəbəkələrindən biri hesab edilən Sality şəbəkəsinin hissəsinə çevrilmişdir.

Məlumat üçün qeyd edək ki, bonet nisbi-müstəqil (avtonom) proqram təminatı ilə idarə edilən və müəyyən sayda hostlardan (qovşaqlardan və ya lokal, yaxud da qlobal şəbəkəyə qoşulan ixtiyari kompüter və ya serverlərdən) ibarət olan kompüter şəbəkəsidir. Bonet anlayışı robot və net sözlərinin birləşməsindən yaranmışdır. Belə şəbəkələrdən bəd əməlçilər virusa yoluxmuş kompüterlərin resurslarından qeyri-leqal və ya bəyənilməyən (spam göndərmək, kompüterdəki parolları müəyyən edib öz sahibinə və ya digər məqsədlər üçün göndərmək və s. kimi) əməliyyatların yerinə yetirilməsi üçün istifadə edirlər.

Qeyd etmək yerinə düşər ki, Linux, Unıx və digər Unıx-ə oxşar əməliyyat sistemləri ümumiyyətlə kompüter viruslarından mühafizə edilmiş əməliyyat sistemləri hesab edilir. Linux üçün yazılmış virusların, troya proqramlarının və digər zərərli proqramların sayı təkcə 2005-ci ildə 422-dən 863-ə çatmışdı. Buna baxmayaraq rəsmi antivirus proqramlarının bəziləri çox az hallarda zərərli proqramları aşkar edə bilirdi.

MenuetOS üçün ilk virusu 2004-cü ildə RRLF virusmeykerlər qrupunun Second Part To Hell kimi məşhur olan üzvü yazır.

AROS üçün ilk virus 2007-ci ildə Doomriderz qrurunun Wargamer kimi məşhur olan iştirakçısı tərəfindən yazılır.

Klassik virusların "qızıl əsri" 10 ilə yaxın davam etmişdir. Bu gün onların sayı kəskin azalmışdır. Anatoli Kasperski laboratoriyasının (laboratoriya Moskva şəhərində yerləşir) məlumatına görə, klassik viruslar ümumi virusların cəmi bir-neçə faizini təşkil edir. Müasir antivirusların hər biri klassik virusla müvəffəqiyyətlə mübarizə apara bilir. Əməliyyat sisteminin özü də bu virusların hücumunu dəf etmək iqtidarındadır. Bu gün bəzi virus növlərinin, demək olar ki, kökü kəsilmişdir. Kökü kəsilən viruslardan biri sərt diskin yükləyici sektorunu zədələyən "*boot-virus"*udur.

AÇIQLAMA: Əgər hələ kompüterinizə antivirus yükləməmişsinizsə, onda kompüterinizdə virusun olduğuna əmin ola bilərsiniz. Odur ki, müvafiq saytın mühafizə sisteminə daxil olub münasib antivirusu pulsuz alın və fərdi kompüterinizə yükləyin.

İndiki zamanda virusların təsirindən bütün kommersiya təşkilatlarının illik itkiləri çox da böyük olmayan bir ölkənin büdcəsi ilə müqayisə edilən olub, hər il ikiqat artmaqdadır. Bəzi mütəxəssislərin narahatlığı təhlükəsizlik probleminin ciddiliyini göstərir.

MessgeLabs şirkətinin texnoloji departamentinin başçısı Aleks Şip göstərmişdi ki, 1999-cu ildə hər saatda 1, 2000-ci ildə hər 3 dəqiqədə 1, 2004-cü ildə isə bir-neçə saniyədə 1 yeni virus yaranmışdı (http://www.messaglabs.com). Sankt-Peterburqdakı İqor Anatolyeviç Danilovun antivirus laboratoriyasının (ООО «СалД») məlumatına görə, yalnız 2007-ci ilin mart ayında antivirus bazasına 7 mindən artıq yeni virus barədə yazı əlavə olunmuşdur.

Dr.Web şirkətinin rəhbəri İqor Anatolyeviç Danilov

Qreys Müller Hopper

Müasir virusların əksəriyyəti özündə bu keyfiyyətləri birləşdirir. Buna misal SoBig virusunu göstərmək olar. Virus 2003-cü ilin avqustunda elektron poçtla göndərilən məktubların təxminən 30%-ni yoluxdurmuşdu.

Aşağıda kompüter istifadəçiləri üçün maraqlı olan viruslarln yaranma xronologiyası verilir.

1945-ci il.

Terminin yaranması. ABŞ Hərbi Dəniz Donanmasının vitse-admiralı, hərbi-dəniz ştabının informasiya şöbəsinin rəhbəri Qreys Müller Hopper (Grace Murray Hopper) elektron-hesablayıcı maşının (müasir kompüterin prototipinin) nasaz işlədiyini aşkar edir.

Relelərdən birinə pərvanə (kəpənək) düşmüşdü. Bu problemi admiral "böcək" (bug) adlandırır (Admiral XIX əsrin sonlarında ABŞ və Böyük Britaniya fiziklərinin elektrik qurğularındakı ixtiyari nasazlıqları ifadə etmək üçün işlətdiyi "böcək" terminindən istifadə etmişdi). Admiral həm də ilk dəfə "böcəkdən xilas olmaq" (debugging) terminindən istifadə etmişdi.

Bu termin hal-hazırda kompüterdəki nasazlıqları aradan qaldırmaqla bağlı işləri ifadə edir.

1949-cu il.

Milliyyətcə macar olan amerika alimi Con fon Neyman (John von Naumann) özütörəyən proqramların yaradılmasının riyazi nəzəriyyəsini işləyib hazırladı. Bu, kompüter virusu yaratmaq üçün hazırlanan ilk nəzəriyyə idi (bu, o dövrdə elmi ictimaiyyətin ciddi marağına səbəb olmamışdı).

1950-ci il.

Bell şirkətinin tədqiqat bölməsinin riyaziyyatçı əməkdaşları oyun düzəltdilər. Bu oyun iki rəqibin kompüter sahəsini ələ keçirmək uğrunda mübarizəsini təsvir edirdi. Bu oyun virusların əcdadı oldu.

***1960*-cı illərin sonu.**

İlk virusların peyda olması. Bir sıra hallarda bunlar proqramlardakı səhvlərlə bağlı idi. Belə ki, bəzi proqramlar səhvən özünü nüsxələşdirib yaddaşı (vinçesteri) doldururdu. Nəticədə kompüterin məhsuldarlığı aşağı düşürdü. Lakin çox hallarda viruslar bilərəkdən pozuculuq üçün yaradılırdı. Çox güman ki, gerçək virusun ilk qurbanı əyləncə üçün yazılmış proqram idi ki, bunun da qurbanı Univac 1108 kompüteri olmuşdur. Bu virus Pervading Animal adlanırdı və hansı kompüterdə yaradılmışdısa, həmin kompüteri sıradan çıxarmışdı.

1975-ci il.

Telnet şəbəkəsi vasitəsilə tarixdə ilk şəbəkə virusu The Creeper yayıldı. Bu virusa qarşı ilk antivirus olan The Reeper yaradıldı.

1979-cu il.

Xerox şirkətinin tədqiqat mərkəzinin mühəndisləri ilk kompüter "qurdu" (worm) yaratdılar.

1981-ci il.

Elk Cloner virusu Apple kompüterlərini yoluxdurdu. Bu virus "oğurluq" kompüter oyunları ilə yayılmışdı.

1983-cü il.

Şimali Karolina Universitetinin alimi Fred Koen "kompüter virusu" terminini kompüter aləminə daxil etdi.

1984-cü il.

Amerika yazıçısı Vilyam Qibson ilk dəfə "hiperfəza" anlayışından istifadə etdi.

1986-cı il.

Artıq qeyd edildiyi kimi, IBM PC üçün yaradılan ilk virus The Brain olmuşdur. Bunu Pakistanlı iki qardaş yaratmşdı. Bunlar Brain virusunu öz firmalarının proqram təminatını yerli "quldurlardan" qorumaq və onları "cəzalandırmaq" məqsədi ilə yaratmışdılar. Lakin tez bir zamanda bu virus sərhədləri aşdı və yüzlərlə kompüteri yoluxdurdu. Kompüter ictimayyəti o zamanlar hadisələrin bu cür gedişini qarşılamağa hazır deyildi.

1987-ci il.

Virusların yaradılması və onlarla mübarizə aparılması barədə ilk kitab yazıldı. Bunu amerika proqramçısı Ralf Berger (Ralph Burger) yazmışdı. Kitab "Kompüter virusları. Yüksək texnologiyaların xəstəliyi" ("Computer Viruses. The Decease of High Technologies") adlanırdı. Kitab virus yaratmağa başlayanlar üçün "əlifba kitabı" kimi məsləhət görüldü.

1988-ci il.

23 yaşlı amerika proqramçısı ARPANET-i yoluxduran "qurd" yaratdı. İlk dəfə kütləvi yoluxma baş verdi – 6 min kompüter virusdan zərər gördü. İlk dəfə məhkəmə kompüter virusunun müəllifini mühakimə etdi. Müəllif 10 min dollar cərimə edildi və 3 il şərti iş aldı. Bu münaqişədən sonra

kompüter virusları haqqında ciddi yazıları digər qeyri-kompüter nəşriyyatları da yaymağa başladılar.

1989-cu il.

ARPANET rəsmi olaraq İNTERNET adlandırıldı. IBM PC üçün ilk antivirus proqram təminatı yaradıldı. AIDS adlı ilk "troya atı" meydana çıxdı. Bu virus vinçesterdəki bütün informasiyanı əlçatmaz edərək ekrana belə bir yazı çıxardı: "Aşağıda göstərilən ünvana 189 dollarlıq çek göndərin". Virusun müəllifi göndərilən pulu alan kimi həbs edildi.

Antivirus proqram təminatı ilə "döyüşə bilən" "Tünd Qisasçı" (The Dark Avenger) adlı ilk virus yaradıldı. Bu virus antivirus proqramı vinçesteri yoxladığı məqamda da yeni-yeni faylları yoluxdurmaqda davam edirdi.

Lawrence Berkeley Laboratory-nin əməkdaşı Kliff Stoll "Ququ quşunun yumurtası" (The Cuckoo's Egg) adlı kitab nəşr etdirdi. Həmin kitabda müəllif peyğəmbərcəsinə xəbər vermişdi ki, ümumdünya kompüter şəbəkəsi təkcə xeyirxah məqsədlərlə istifadə edilməyə də bilər. Belə ki, bu şəbəkə hərbçilər, cinayətkarlar və dələduzlar tərəfindən də fəal surətdə istifadə ediləcəkdir. K.Stoll hadisələrin bu məcraya yönəlməsinin qarşısının vaxtında alınması tədbirlərinin görülməsini təklif etmişdir.

1990-cı il.

Bu, PC Today adlı populyar kompüter jurnalı ilə bağlı məşhur münaqişə tarixidir. Çünki həmin jurnal öz abunəçilərinə virusa yoluxmuş disketlər yaymışdı.

1991-ci il.

Yalnız virus yaratmaq üçün yazılmış ilk VCS v1.0 adlı proqram işıq üzü görür.

1993-cü il.

SatanBug virusu ABŞ-ın paytaxtı Vaşinqtonda yüzlərlə kompüteri yoluxdurur. Hətta Ağ Evin kompüterləri virusa yoluxmuşdu. Federal Təhlükəsizlik Bürosu 12 yaşlı yeniyetmə müəllifi həbs edir.

Görkəmli şəxsiyyətlərin adları ilə bağlı olan, müəyyən tarixdə aktivləşən viruslar da peyda oldu. Bu tarix Mao Dze Dunun təvəllüd tarixi, Yeni il günü və i.a. ola bilərdi. Bu tip virus ilk dəfə The New York Times qəzetini hədəfə aldı və qəzetə böyük məbləğdə ziyan vurdu.

1994-cü il.

Böyük Britaniyada, ABŞ-da, Norveçdə bir-sıra virus müəllifləri həbs edildi.

1995-ci il.

Microsoft ***korporasiyası*** Windows-95-in beta-versiyasını virusa yoluxmuş disketlərdə dünyaya yaydı. Müəyyən proqramların proqram platformalarını dağıtmağa hesablanmış makroviruslar meydana çıxdı. Concept adlı makrovirus Microsoft Word proqramını zədələdi.

AÇIQLAMA: İlk *korporasiya* Qədim Romada yaradılmışdır. Respublika dövründə bir neçə korporasiya yaratmağa icazə verilir. Korporasiyanın yaradılmasına qoyulan tələb ondan ibarət idi ki, onun nizamnaməsi qanuna zidd olmasın. İmperiya yaradılan zaman isə yeni korporasiya yaratmaq həddindən artıq çətinləşir, çünki korporasiyanın yaradılması üçün mütləq senatın icazəsi olmalı idi. Korporasiyanın işini onun seçilmiş üzvü yerinə yetirə bilərdi. Əgər korporasiya ləğv edilirdisə, onda ona məxsus olanlar onun üzvləri arasında bərabər bölünürdü.

Dünyada yaradılmış ən qədim tarixə malik olan korporasiya İsveçrənin Falun şəhərindəki Stora

Kopparberget mis mədənidir. Korporasiya İsveç korolu Maqnus Erikssonun razılığı ilə 1347-ci ildə yaradılmışdı.

XVII əsrdə müstəmləkə ekspansiya dövründə (ekspansiya - genişlənmə, yayılma anlamını verir və imperialist dövlətlərin yeni torpaq, müstəmləkə və bazarlar əldə etmək məqsədilə öz siyasi və iqtisadi nüfuzunu başqa ölkələrə yaymaq üçün yeritdikləri təcavüzkar siyasət kimi qəbul edilir) çoxlu sayda Avropa ölkələri yaradılmış korporasiyalara müstəmləkə ölkələri ilə biznes əlaqəsi qurmağa şərait yaratdı. Bu şirkətlər müasir korporasiyaların yaradılmasına örnək oldular. Nümunə olaraq belə korporasiyalara Holsand Ost-Hindistan şirkətini və Qudzon zalifi şirkətini göstərmək olar.

Korporasiya (yeni latın dilində "corporatio" deməkdir, birləşmə anlamını verir) hüququ şəxsin yaratdığı şirkət və ya firma növlərindən biridir. Korporasiyanın üstünlüyü onun uyuşanlığı və məsrəfin azaldılması imkanlarının axtarılmasıdır.

1998-ci il.

Kaliforniyalı iki yeniyetmənin yazdığı virus Pentaqonun 500-dən artıq kompüterini sıradan çıxardı. Bu münaqişədən sonra ABŞ Müdafiə Nazirliyində belə bir nəticəyə gəldilər ki, kiberfəzadakı hücumlar ənənəvi döyüşdən heç də az təhlükəli deyildir. Hərbi analitiklər ilk dəfə "kompüterin qızğın silahlanması" terminindən istifadə etdilər.

1999-cu il.

İlk dəfə dünya miqyasında kompüter virusu epidemiyası baş verdi. Melissa adlı virus 10 minlərlə kompüteri yoluxduraraq ölkəyə 80 milyon dollar ziyan vurdu. Bu

münaqişədən sonra antivirus proqramlarına tələb kəskin şəkildə artdı.

2000-ci il.

Melissa virusunun rekordunu I Love You! virusu qırdı. Bu virus bir-neçə saat ərzində milyonlarla kompüteri yoluxdurdu. İstintaq aşkar etdi ki, bu virusu filippinli tələbə yazıb və heç bir cəza almayıb. Çünki Filippin qanunları bu cür əməllər üçün heç bir cəza nəzərdə tutmamışdı. Həmin il kompüter viruslarına qarşı beynəlxalq razılaşma imzalandı.

DOS-a edilmiş hücumlar nəticəsində onlarla populyar saytlar, o cümlədən, Yahoo, eBay, Amazon şəbəkədən vurulub-çıxarıldı, çünki İnternet-server elə böyük yüklənmələrə məruz qaldı ki, sonda server imtina edəsi oldu. Hücum mexanizmi belə idi: 10 minlərlə kompüter yoluxduruldu ki, bunun nəticəsində də hücuma məruz qalan saytlar şəbəkədən vurulub-çıxarılsın. İstintaq göstərdi ki, hücum Kaliforniya universitetinin tədris mərkəzində istifadə olunan kompüterlərdən həyata keçirilmişdir. Lakin ziyankarlar aşkar edilmədiyindən məsələ həll edilməmiş qaldı.

2001-ci il.

20 yaşlı hollandiyalı Yan De Wit Anna Kornikova adlı məşhur virus yaratdığına görə mühakimə edilərək 150 saatlıq islah işləri ilə məşğul olmağa məcbur edildi. Məhkəmə etiraf etdi ki, bu virusun Niderland iqtisadiyyatına vurduğu ziyanı dəqiq müəyyən etmək mümkün deyildir. De Vitdən 7,5 minlik virus kolleksiyası da müsadirə edildi. De Vit hakimə bildirdi ki, yazdığı proqramın virus olduğundan və belə bir ziyan vura biləcəyindən xəbəri olmamışdır.

2002-ci il.

İlk dəfə virus müəllifi həbsxanaya düşdü. Melissa virusunun müəllifi 33 yaşlı proqramçı Devid Smit 20 aylıq həbs cəzası aldı.

İlk dəfə virus Ümumdünya Şəbəkəsinin fəaliyyətini təmin edən 13 İnternet-server qovşağını yoluxdurdu. Analitiklər təsdiq edirlər ki, yaxşı təşkil edilmiş və həyata keçirilmiş kompüter hücumu bir həftəyə İnterneti məhv edə bilər.

2003-cü il.

Yayılma sürəti rekordunu Slammer adlı "qurd" qırdı. Belə ki, 10 dəqiqə ərzində 75 min kompüter virusdan "xəstələnmişdi". Virus ABŞ-ın Dövlət Departamentinin kompüterlərini zədələyərək verilənlər bazasını dağıtmışdı. ABŞ konsulluğu bu səbəbdən bütün dünyaya viza verilişini 9 saat dayandırmaq məcburiyyətində qalmışdı.

İlk dəfə virus müəllifi Avropada həbsxanaya salındı. Bu, 22 yaşlı Saymon Vellor idi. Böyük Britaniya məhkəməsi onu Gokar, Redesi və Admirer viruslarını yaratdığına görə 2 il həbs cəzası ilə cəzalandırmışdı. Bu viruslar 42 ölkənin 27 min kompüterini yoluxdurmuşdu.

Beləliklə, kompüter viruslarının inkişafı tarixi daha çox qızğın silahlanmanı yada salır. Əvvəlcə ziyanverici proqram, sonra isə ondan müdafiə proqramı əmələ gəlir. Bu spiralvari inkişaf nəticəsində viruslar sadə proqramlardan mürəkkəb komplekslərə - öz pozucu fəaliyyətlərini gizlədə bilən, kriptoqrafik və şəbəkə texnologiyalarından istifadə edərək gözəgörünməz ziyankarlara çevrilirlər.

Paralel olaraq antivirus vasitələri də inkişaf etdi.

İlk antiviruslar primitiv utilitlər olub, fayllarda olan məlum siqnatura (göstəriş, təlimat) üzrə axtarış aparıb faylı həmin siqnaturadan təmizləyirdi. İndiki antiviruslar isə müxtəlif

proqramlardan tərtib edilmiş, müxtəlif aşkarlama və ləğvetmə üsullarından istifadə edən mürəkkəb komplekslərdir.

POLİMORFİZM – VİRUSLARIN MUTASİYASI

İlk polimorfik virus – "Chameleon" keçən əsrin 90-cı illərinin əvvəllərində meydana çıxmışdır. Lakin polimorfik virus problemi yalnız 1991-ci ilin aprelində ciddi şəkil aldı. Bu, "Tequila" adlı polimorfik virusun dünyanı bürüyən epidemiyası ilə bağlı idi. 1994-cü ildə Rusiya "Phantom1" adlı polimorfik virus epidemiyası ilə üzləşdi.

Özünü şifrələyən polimorfik viruslar ideyasının populyarlaşması polimorfik kod generatorunun meydana çıxması tarixi ilə - 1992-ci ilin əvvəlində məşhur "Dedicated" virusunun peyda olması ilə bağlı idi. Sözügedən virus MtE adlı ilk polimorfik generatorda yerləşdirilmişdi. Çox keçmədi ki, həmin polimorfik generator obyekt modula (OBJ-fayla) çevrildi. Beləliklə, adi virusun OBJ-fayla keçirilməsi ilə polimorfik-***mutant*** almağa imkan yarandı.

1993-cü il polimorfik virusların kütləvi istehsalı ili oldu. Nəticədə: Bootache, CivilWar (dörd versiyada), Crusher, Dudley, Fly, Freddy, Ginger, Grog, Haifa, Mochtezuma (iki versiyada), MVF, Necros, Nukehard, PcFly (üç versiyada), Predator, Satanbug, Sandra, Shoker, Todor, Tremor, Trigger, Uruguay (səkkiz versiyada) və s. virusları yarandı.

Polimorfik viruslarla yanaşı, polimorfik generatorlar da inkişaf etdirilir və təkmilləşdirilirdi. 1993-cü ildə artıq 7 polimorfik kod generatoru mövcud idi: MTE 0.90 (Mutation Engine), TPE-nin (Trident Polymorphic Engine) 4 müxtəlif

versiyası, NED (Nuke Encryption Device), DAME (Dark Angel's Multiple Encryptor).

AÇIQLAMA: *Mutasiya* (latınca *mutatio – dəyişmə* sözündən yaranmadır) xarici və daxili mühitdə baş verənlər nəticəsində gen növünün yaranmasıdır. Termin Xuqo de Friz tərəfindən təklif edilmişdir. Mutasiya baş verən proses mutageniz adlanır.

Xuqo de Friz

Xuqo de Friz (niderlandca Hugo fe Vries – 1848-1935) Hollandiya botaniki və genetikidir, Rusiya Elmlər Akademiyasının xarici müxbir üzvi (1924), SSRİ Elmlər Akademiyasının fəxri üzvi (1932) seçilmişdir. Alim ilk dəfə olaraq dəyişkənlik və təkamül haqqında elmi fikirlər söyləmiş, ilk dəfə olaraq mutasiya prosesini sistem şəkilində araşdırmışdır.

O vaxtdan bəri hər il bir-neçə polimorfik generator yaradılır.

1992-ci il, iyulun 5-də IBM PC üçün ilk virus kodu konstruktoru – VCL (Virus Creation Laboratory) yarandı. Bu da virus istehsalının avtomatlaşdırılması demək idi. Bu konsrtuktor 10-15 dəqiqə ərzində 30-40 müxtəlif virus istehsal etmək iqtidarında idi.

TƏHLÜKƏSİZLİYƏ QARŞI VİRUS HƏDƏLƏRİNİN TİPLƏRİ

Antivirus təhlükəsizliyinə qarşı virus hədələrinin əsas növləri ziyankar proqram təminatlarının müxtəlif tipləri ilə reallaşdırılır. Ziyankar proqram təminatı dedikdə, kompüter virusları və "troya atı", adware, spyware və s. tipli proqramlar nəzərdə tutulur.

Virus – kompüter mühitində sərbəst surətdə yayıla bilən xüsusi hazırlanmış proqram kodudur. Hal-hazırda virusların aşağıdakı tipləri fərqləndirilir: fayl virusları, yükləyici viruslar, "şəbəkə qurdları", bədənsiz viruslar və həmçinin kombinə edilmiş viruslar. Bu virus tiplərinin hər biri daşıyıcı növünə və yayılma (yoluxma) metoduna görə bir-birindən fərqlənir.

"Troya atı" tipli proqram da ziyankar proqram kodu olsa da viruslardan fərqli olaraq sərbəst surətdə yayıla bilmir. Bu proqram kodu sistemin ştatda olan proqram təminatı altında gizlənərək məsafədən icazəsiz müdaxilə imkanı yarada bilir. Yəni "troya atı" hansı kompüterə qurulursa, həmin kompüterdəki istənilən informasiyanı oğurlamaq imkanı yaradır.

Spyware tipli ziyankar proqram təminatı istifadəçinin gördüyü iş barədə informasiya toplamaq üçün nəzərdə tutulmuşdur. Belə informasiyaya nümunə olaraq istifadəçinin müraciət etdiyi İnternet saytlarının siyahısı, onun işçi stansiyasında qurulmuş proqramların siyahısı, elektron poçtla

ötürülən məlumatların məzmunu və s. göstərilə bilər. Toplanan informasiya spyware proqramları ilə əvvəlcədən təyin edilmiş ünvana ötürülür.

Beləliklə, spyware proqram təminatı potensial olaraq məxfi informasiyanın sızması kanalı kimi işləyir.

Adware proqram təminatı istifadəçilərin işçi stansiyalarında reklamların görünməsini təmin etmək üçün nəzərdə tutulmuşdur. Bu proqram təminatı bilavasitə ziyankar olmasa da, spyware proqram təminatının ziyankar əməllər törətməsi üçün şərait yarada bilir.

Bir qayda olaraq, virus hədələri öz həyat tsiklinin (dövrünün) 4 mərhələsinin birində ola bilir.

Birinci mərhələ sistemin zəif yerinin təyin edilməsidir. Zəif yer həm təşkilati-hüquqi, həm də proqram-aparat təminatı ilə bağlı ola biləndir.

İkinci mərhələ sistemin zəif yerindən virus hücumu üçün istifadə edilməsidir. Bu mərhələdə virus ***host****lardan* birini yoluxdurur.

Üçüncü mərhələ virusun işə başlamasıdır. Bu mərhələdə hədəf kompüter arzuolunmaz davranışlara başlayır.

Dördüncü mərhələ virusun kompüter mühitində yayılmasıdır. Bu mərhələdə növbəti kompüterin zəif yeri təyin edilir və yuxarıdakı mərhələlər növbəti kompüterdə həyata keçirilir.

AÇIQLAMA: *Hostinq* (ingiliscə hosting) informasiyanı daim şəbəkəyə qoşulmuş serverdə (adətən İnternetdə) yerləşdirmək üçün nəzərdə tutlan xidmətlərin təqdim olunma resurslarıdır. Adətən hostinq sayta göstərilən xidmət paketinə daxil olur və serverdə yerləşmiş sayt fayllarına minimum xidmət göstərir.

Host maşınlar

MÖVCUD YANAŞMALARIN NÖQSANLARI

Hal-hazırda bir çox şirkətlərdə elə təsəvvür vardır ki, mövcud antivirus vasitələri virus təhlükəsinə qarşı etibarlı müdafiə qurmağa imkan verir. Halbuki belə düşünmək yanlışdır. Çünki antivirus vasitələrin əksəriyyəti ***siqnatura*** metodlarına əsaslandığından yeni virusu tanıya bilmir. Çox hallarda təşkilatlarda antivirus vasitələri ilə işləmək qaydalarını reqlamentləşdirən normativ-metodiki sənədlər mövcud olmur. Antivirus vasitələri sistemin zəif yerlərini təyin etməyi və

aradan qaldırmağı bacarmırlar. Antivirus vasitələri virus hücumu nəticələrini aradan qaldırmaq üçün funksional imkanlara malik deyildirlər.

AÇIQLAMA: *Siqnatura* (latınca signatura – işarə etmə, qeyd etmə, nişanlama, göstərilmə, işarə edilmə və s. anlamlarını verir). Funksiyanın suqnaturası proqramlaşdırmada funksiyanın müəyyən xarakteristikasının hissəsidir. Siqnatur hücum kompüter virusunun xarakteristik xüsusiyyətidir.

Ziyanverici koda qarşı müdafiə məsələsinə digər geniş yayılmış yanaşma növü yalnız bir antivirus istehsalçısının məhsullarına etibar etməkdir. Əgər hər hansı səbəbdən həmin antivirus istehsalçısı yeni virus istehsalından geri qalarsa, külli miqdarda kompüter müdafiəsiz qala bilər. Antivirus istehsal edən şirkətlərin yeni virusa reaksiya müddəti fərqli olduğundan, daha cəld istehsalçıya müraciət edilməsi motivasiyasının mövcudluğu bu sahədə güclü rəqabət mühiti yaratmaqla situasiyanın daim dəyişməsinə səbəb olur.

Bütün bu deyilənlər virus hücumlarından qorunmaq üçün kompleks yanaşma tələb olunduğunu ön plana keçirir.

Virus hücumundan kompleks müdafiənin təşkilati, hüquqi, kadr, texniki, texnoloji, proqram və s. tərəfləri vardır.

Təşkilati aspekt virus hücumuna qarşı sistemin zəif yerini aşkarlayıb ləğv etməlidir. Bu, virus hücumunun mümkün olması ehtimalını aradan qaldırır.

Antivirus təhlükəsizliyinin təmin edilməsində normativ-metodiki, texnoloji və kadr təminatları mühüm rol oynayır.

Normativ-metodiki təminat nəzərdə tutmalıdır ki, virus hücumlarından müdafiə sahəsində balanslaşdırılmış hüquqi

baza yaradılsın. Bunun üçün şirkətdaxili normativ sənədlər kompleksi işlənib hazırlanmalıdır.

Kadr təminatı çərçivəsində şirkət virus hücumlarına qarşı lazımi tədbir görə bilən əməkdaşlardan istifadə etməli və mövcud əməkdaşları bu sahədə biliklərdirməlidir.

Texnoloji təminat, viruslardan müdafiə üzrə nəzərdə tutulan bütün digər tədbirlərlə yanaşı, əsas diqqəti səbəkə ekranlaşdırmasına yönəltməlidir. Bu, istifadəçilərin işçi stansiyalarını şəbəkə viruslarının hücumundan qorumaq üçün potensial təhlükəli paketlərin filtrlənməsi (süzgəclənməsi) yolu ilə əldə edilir.

Endi Hopkins

Ci Vonq

İlk antivirus proqramları CHK4BOMB və BOMBSQAD 1984-cü ilin qışında yaradılmışdır. Onları amerikalı proqramçı Endi

Hopkins (Andy Hopkins) yazmışdı. Kompüterdəki informasiyanı virus hücumlarından müdafiə edə biləcək ıik antivirus proqramı 1985-ci ildə meydana çıxmışdır. DRPROTECT adlanan proqram proqramçı Ci Vonqun (Gee Wong) böyük zəhməti bahasına əmələ gəlmişdi. Yaradılmış proqram kompüterdə BIOS-dan keçərək yerinə yetirilən bütün əməliyyatları (informasiyanın yazılmasını, formatlama əməliyyatlarını) bloklama qabiyyətinə malik idi. İş prosesində belə əməliyyat əmələ gəldikdə proqram sistemin yenidən yüklənməsini tələb edirdi.

İlk antivirus utilitlər 1984-cü ilə yaradıldı.

ANTİVİRUS PROQRAMLARININ YARADILMASI VƏ İNKİŞAFI

Kompüter viruslarından qorunmanın əsas yolları aşağıdakılardan ibarətdir:

- Virusun kompüterə daxil olmasına yol verməmək;
- Əgər virus kompüterə daxil olubsa, vurus hücumuna yol verməmək;
- Əgər virus hücumu baş veribsə, hücumun nəticələrini aradan qaldırmağa cəhd etmək.

Kompüter viruslarından qorunmanın təmin edilməsinin üç metodu mövcuddur:

- Proqram metodları;
- Aparat metodları;
- Təşklati metodlar.

İnformasiyanın qorunması üçün istifadə edilən əsas vasitə qiymətli məlumatların ehtiyat köçürülməsidir (surətinin alınmasıdır). Kompüterin bərpa edilməsi ehtiyat daşıyıcıda saxlanan verilənlərin köçürülməsi ilə başa çatır. İnformasiyanın

qorunmasının proqram metodu deyəndə antivirus proqramlarından istifadə edilməsi nəzərdə tutulur.

1974-cü ildə ARPANET şəbəkəsinin kommersiya variantı olan Telnet şəbəkəsi yaradılır. Bu şəbəkə yaradılandan sonra kompüter virusları tarixində ilk dəfə 1975-ci ildə The Creeper adlanan şəbəkə virusu yayılmağa başlayır. Virusun müəllifi BBN (Bolt Beranek and Newman) kompaniyasının əməkdaşı Bob Tomas olmuşdur. Proqram yerini serverlər arasında müstəqil dəyişə bilirdi. Kompüterə daxil olandan sonra ekrana "I'M THE CREEPER... CATCH ME IF YOU CAN" ("Mən Kriperəm...bacarsan məni tut") məlumatı çap edilirdi. Mahiyyət etibarilə bu proqram virus deyildi. Ona görə ki, nə destruktiv, nə də casus xarakterli əməliyyatlar yerinə yetirilmirdi.

1975-ci ili antivirus proqramlarının yaradılması tarixi kimi də xarakterizə etmək olar. Belə ki, həmin ildə BBN kompaniyasının digər əməkdaşı Rem Tomlinson The Creeper virusunun təsirini aradan qaldırmaq üçün nəzərdə tutulan The Reepet adlanan xüsusi antivirus proqramı yazır. Proqram virusu tapan kimi onun fəaliyyətini dayandırırdı.

Həmin vaxtdan etibarən kompüter virusları və antivirus vasitələri arasında belə demək caizsə, silahlı qarşıdurma və ya yarış davam edir.

1980-cı ilin fevralında Dortmund universitetinin tələbəsi Yurgen Kraus "Özüçoxalan proqramlar" mövzusunda diplom işi yazır.

Bu diplom işində nəzəri mülahizələrlə bahəm ciddi özüçoxalan proqramların mətni də verilmişdi. Əslində bu proqramlar Siemens kompüterlər üçün virus proqramlar deyildi.

Yurgen Kraus

AÇIQLAMA: Bəzi texniki ədəbiyyatlarda ilk kompüter viruslarının yaradılmasını səhv olaraq 1970-ci illərə, hətta 1960-cı illərə aid edirlər.

Belə yazılarda adətən Animal, Creeper, Cookie Monstr və Xerox worm kimi proqramlar virus proqramları kimi təqdim edilir.

Fərdi kompüterlər üçün ilk məşhur viruslar Virus 1,2,3 və Elk Cloner proqramları hesab edilir. Bu virusların hər ikisi funksionallığına görə çox oxşar idi və bir-birindən aslı olmadan kiçik vaxt fərqi ilə 1981-ci ildə yaradılmışdı.

1977-ci ildə ilk Apple Fərdi Elektron Hesablama Maşınının və şəbəkə strukturunun yaradılması ilə kompüter virusları tarixinin yeni dövrü başlanır. Bu dövrdə troya vandal proqramları da yaradılır. Belə proqramlar öz destruktiv fəaliyyətini müəyyən qədər vaxt keçəndən sonra və ya müəyyən şərtlər ödənəndə yerinə yetirirdi.

1987-ci ildə amerikalı proqramçı Ralf Berger viruslarla mübarizə metodları haqqında kitab yazır. Bu kompüter virusları tarixində mühüm mərhələ oldu. 1990-cı illərin ortalarından başlayaraq kompüter virusları əleyhinə mübarizə getdikcə güclənir. ABŞ və İngiltərə kimi ölkələrdə kompüter virusları yazan və onları yayanlara qarşı bir sıra səs-küylü məhkəmə prosesləri aparılır. Təqsirləndirilənlər cərimələnir və cərimələrin məbləği getdikcə artırılır. Antivirus proqram təminatı daim təkmilləşdirilir, virusların yayılmasının və dağıdıcı fəaliyyətinin qarşısının alınmasında onların rolu xeyli gücləndirilmiş olur.

Antivirusdan söhbət gedirsə bu sahədə ən görkəmli simalardan birinin Yevgeniy Kasperski olduğu şübhəsizdir.

1989-cu ildə məxfi dövlət Elmi Tədqiqat İnstitutunun əməkdaşı olan Y.Kasperskinin kompüterinə Cascade virusu düşür. Kacperski virusu aradan qaldırmaq üçün həyatında birinci dəfə antivirus proqramı yazır. Bu iş ona çox maraqlı gəlir və o bu problemlə ciddi məşğul olmağa başlayır. O bir sıra iri kontraktlardan xeyli vəsait qazanır və gəlirinin çox hissəsini biznesin inkişafına xərcləyir.

Y.Kaspersknin kompaniyası 1997-ci ilin iyun ayından fəaliyyət göstərir. Antivirus sahəsində Y.Kasperski dünyanın aparıcı ekspertlərindən biridir. Onun yaratmış olduğu "Kasperskinin Laboratoriyası" mərkəzi ofisi Mockvada yerləşən beynəlxalq kompaniyalar qrupudur. Kompaniyanın İngiltərə, Çin, Fransa, ABŞ, Almaniya, Rumıniya, Yaponiya, Cənubi

Koreya, Niderland, Polşa, Birləşmiş Ərəb Əmirlikləri və Kanadada nümayəndəlikləri var. Kampaniya özünün partnyorlar (tərəfdaşlar) şəbəkəsində dünyanın 60-dan çox ölkəsində yerləşən 500-dən çox kompaniyanı birləşdirir.

"Kasperskinin Laboratoriyası" kompüter viruslarından, spamlardan və xaker hücumlarından müdafiə sistemlərinin yaradılması üzrə ixtisaslaşmışdır. Bu kompaniya İnternetlə yayılan təhlükələrdən informasiyanın müdafiə edilməsi üçün tətbiq edilən proqram təminatının satışından əldə edilən gəlirin həcminə görə dünya üzrə beş aparıcı kompaniyadan biridir. Kompaniya genişlənir və inkişaf edir. Bu laboratoriyanın təkcə Moskva ofisində çalışan əməkdaşlarının sayı 1500-dən, əməkdaşlarının ümumi sayı isə 2500-dən çoxdur.

Kasperskinin laboratoriyası həm adi, həm də ixtiyari miqyasa malik olan korporativ şəbəkələrdə informasiyanın təhlükəsizliyini təmin edən proqram təminatı hazırlayır. Kompaniyanın məhsullarından Windows, Linux, Mac və s. kimi populyar əməliyyat sistemlərində də istifadə edilir. Kasperskinin antivirus proqramının nüvəsindən Microsoft (ABŞ), Cheek Point Softwre Texnologies (İsrail, ABŞ), Juniper (ABŞ), Nokia İCG (ABŞ), F-Secure (Finlandiya), Aladdin (İsrail), Subari (ABŞ), Deerfield (ABŞ), Alt-N (ABŞ), Microworld (Hindistan), BorderWare (Kanada) və s. kompaniyalar öz məhsullarının hazırlanmasında istifadə edirlər. "Kasperskinin Laboratoriyası" kompaniyasının məhsulları Microsoft, IBM, Intel, Cisco Systems, Red Hat, Citrix Systems, Novell və s. kimi dünyanın aparıcı aparat və proqram təminatı istehsalçılarının sertifikatlarını almışdır.

1990-ci illərin əvvəllərinə kimi antivirus proqramları virus kodunun nümunələrindən (onlarla siqnaturadan) ibarət olurdu. 1992-ci ildə polimorf kod generatoru MtE meydana gələndən

sonra istənilən proqramçı daim dəyişən kodla polimorf virus yarada bilirdi. Belə vəziyyətdə kod emulyatorundan istifadə etmək zərurəti yaranmışdı. Sistem polimorf virusun şifrələnən hissəsini açıb virusun daimi hissəsini müəyyən etməli idi. Emulyatora malik ilk antivirus proqramını da (AVP) Yevgeniy Kasperskiy yaradır. Həmin dövrdə kod emulyatorlarından başqa kriptotəhlil, statistik təhlil, ***evristik*** təhlil və davranış blokiratorları kimi virusdan müdafiə sistemləri yaradılır.

AÇIQLAMA: *Evristika* (qədim yunan sözü εὑρίσκω – "axtarıram", "açıram" deməkdir) insan təfəkkürü ilə dərk edilməyən yaradıcılığı öyrənən elm sahəsidir. Evristika psixologiya, fiziologiya, kibernetika və digər elm sahələri ilə əlaqəlidir, amma elm sahəsi kimi hələlik tam şəkildə formalaşmamışdır. Qədim Yunanstanda evristika dedikdı Sokrat tərəfindən həyata keçirilən tədris sistemi başa düşülürdü. Evristika anlayışından yunan riyaziyyatçısı Pappanın "Məsələni həll etmə bacarığı" əsərində istifadə edilmişdir (bizim eradan əvvəl 300 - ci il).

Evristik metodların intensiv axtarışı və yaradılması XX əsrin ikinci yarısına təsadüf edir. Sonrakı illərdə elm sahəsindən mühəndislər və digər yaradıcı işçilər, həmçinin psixologoya və beynin fiziologiyası sahələrində də istifadə olunmuşdur.

1998-ci ildə iki amerikalı yeniyetmənin yaratdıqları virus ABŞ müdafiə nazirliyinin 500-dən çox kompüterinə yoluxandan və nəticədə nazirliyin işi praktik olaraq iflic vəziyyətinə düşəndən sonra dövlət də, cəmiyyət də başa düşməyə başladı ki, kompüter viruslarının törədə biləcəyi təhlükə kütləvi qırğın silahlarının törətdiyi təhlükədən az olmaya bilər.

Bundan sonra əvvəlcə Pentaqon, onun ardınca isə bütün iri korporasiyalar keyfiyyətli və etibarlı antivirus proqram təminatına sifarişləri artırırlar.

Bu da daha keyfiyyətli antivirus proqram təminatı vasitələrinin yaradılmasını stimullaşdırırdı.

Bu cür vəziyyət dolayı yolla müxtəlif sahələrdə, o cümlədən şəbəkələrdə informasiya təhlükəsizliyi sisteminin inkişafında müsbət rol oynadı. Yəni insanlar anlamağa başladılar ki, təhlükə təkcə viruslardan yaranmır.

Windows əməliyyat sistemi yaranandan və İnternetdən istifadə genişlənəndən sonra kompüter virusları ilə mübarizə daha da kəskin şəkil alır. Hazırda dünyada antivirus proqram təminatının işlənib hazırlanması ilə 60-a qədər kompaniya məşğul olur.

Microsoft Securiti Essentials pulsuz antivirusdur. Bu antivirus öz imkanlarına görə pullu antiviruslardan geri qalmır. Hal-hazırda demək olar ki, kompüter istifadəçilərinin hamısı daim virus bazaları ilə yenilənən antivirus vasitələrindən istifadə etmək məcburiyyətindədir.

Dr.Web antiviruslar ailəsi poçt və şəbəkə soxulcanlarından, putkitlərdən (aşkar və ləğv edilməsi daha mürəkkəb olan viruslardan), fayl viruslarından, troya proqramlarından, stels-viruslardan, polimorf viruslardan, cansız (cisimsiz) viruslardan, makroviruslardan, MS Office sənədləri yoluxduran viruslardan, casus proqram təminatından, parol oğurlayan proqramlardan, klaviatura casuslarından, pullu zəng proqramlarından, reklam proqram təminatından, potensial təhlükəli proqram təminatından, xaker utilitlərindən və s. mudafiə üçün nəzərdə tutulmuşdur.

Antivirus ESETNOD32. 1988-ci ildə Çexoslovakiya televiziyası ilə "Şəhər kənarında xəstəxana" adlı maraqlı serial

göstərirdilər. İlk kompüter virusları da diskin kənarinda yerləşən boot-sektora hücum edirdilər. Antivirusun adındakı NOD abbreviaturası da bundan götürülmüşdür. NOD (Nemocnica na Okraji Disku və ya Disk kənarında xəstəxana). Antivirus NOD32 32 və 64 mərtəbəli Windows əməliyyat sistemlərini himayə edir. Bu antivirus sistemi asinxron yoxlaya bilir. Antivirus makrovirusu tapmaq üçün MS Word və Excel faylların daxili quruluşunu təhlil edir. NTFS fayl sistemini himayə edir.

Yevqeniy Valentinoviç Kasperskiy

Con MakAfi

1989-cu ildə Con MakAfi ABŞ-da öz antivirus kompaniyasını yaradır. Bir neçə aylıq gərgin işdən sonra McAfee VirusScan antivirus proqramı yaradılır. Kompaniya antivirusu istifadəçilərə pulsuz verirdi. Ona görə də bu kompaniya əvvəlcə Kaliforniya

ştatında, sonra da bütün ölkədə istifadəçilərin çox böyük məhəbbətini qazandı.

Panda kompaniyasının əsası 1990-cı ildə Mikel Urizarbarren tərəfindən İspaniyanın Bilbao şəhərində qoyulmuşdur.

Panda Security antivirus proqramı minimal resurslardan istifadə etməklə virusdan səmərəli mudafiənin həyata keçirilməsini təmin edə bilir. Panda firmasının məhsulları məişət və korporativ kompüter istifadəçilərin informasiya təhlükəsizliyini təmin edir. Bu kompaniyanın dünyanın 200-dən çox olkəsində müştəriləri, 50-dən çox olkəsində isə ofisləri var.

Antivirus Panda faktiki iki moduldan ibarətdir – Panda Ultrafast və Panda SmartClean2. Birinci modul - süni intellektin bəzi texnologiyalarından və mexanizmlərindən istifadə etməklə virusları tapır və zərərsizləşdirir. İkinci modul isə virusun törətdiyi nəticələri aradan qaldırır.

AVAST kompaniyasının əsası 1991-ci ildə Çexoslovakiyada qoyulmuşdur. Kompaniyanın baş ofisi Praqada yerləşir.

Avast! antivirus proqramı Windows, Lınux, Mac OS əməliyyat sistemləri, həmçinin Palm, Android və Windows CE platformalı kompüterlərdə (cibdə gəzdirilən fərdi kompüterlərdə) isifadə edilə bilir. Evdə - yəni məişətdə istifadə etmək üçün antivirusun Free-pulsuz; Pro, Internet Security və Premier kimi pullu, həmçinin qeyri-kommersiya məqsədi ilə istifadə edilən variantları buraxılır. Anivirusun orta və böyük biznes üçün Endpoint Protection, Endpoint Protection Plus, Endpoint Protection Suite və Endpoint Protection Suite Plus kimi versiyaları mövcuddur. Antivirusun serverlər üçün File Server Security və Email Server Security kimi versiyaları vardır. Avast antivirus proqramı ICSA Labs (təhlükəsizlik məhsullarının o cümlədən antivirusların tədqiqi, sınaqdan keçirilməsi və

sertifikatlaşdırılması ilə məşğul olan) beynəlxalq assosiasiyanın sertifikatını almışdır.

Proqramın adı "avast" ingiliscə "anti-virus advansed set" – "qabağa çəkilmiş antivirus yığımı" mənasını verən ifadənin qısaldılmış formasıdır. Nədənsə ingilis dilində dayan! mənasını verən avast sözünün də olmasına uzun muddət fikir verən olmayıb.

Avast! Free ən populyar pulsuz antivirus hesab edilir. Dünya üzrə avast! antivirus istifadəçilərinin sayı təxminən 200 milyona çatır. 1995-ci ildən başlayaraq Avast firması təkcə antivirus məhsulları yaratmaqla məşğuldur.

2010-cu ilə kimi bu firma ALWIL Software adlanırdı. 2010-cu ildə bu firmanın adını dəyişdirib AVAST Software qoydular. Bu firma 1988-ci ildə işə yeni başlayanda onun əməkdaşlarının sayı 5-6 nəfərdən ibarət olub. İndi bu firmada yüzlərlə mütəxəssis çalışır.

Beləlikə, son olaraq qeyd etmək lazımdır ki, hər bir kompüter istifadəçisi viruslardan daim müdafiə olunmalı və bu məqsəd uğrunda daim mübarizə aparmaq üçün mütləq istifadə etdiyi fərdi kompüterinə tanıdığı antivirus proqramını yükləməlidir. Yerinə yetirilən bu əməliyyat həm onun kompüterdən istifadəsini sadələşdirər, həm də ki, ona məxsus olan kompüterdən uzun müddət səmərəli istifadə etməsinə imkan verər.

VİRUSLA MÜBARİZƏ

Virusla mübarizə aparmaq üçün xüsusi proqram təminatından – *antivirusdan* istifadə edilir.

İndiki zamanda antivirusların müxtəlif növlərinə rast gəlmək mümkündür və onlar aşağıdakı funksiyaları yerinə yetirirlər:

- *Proqramlar-detektorlar* operativ yaddaşda və fayllarda virus üçün xarakterik olan kodların (siqnaturların) axtarışını həyata keçirirlər. Virus tapıldıqda uyğun məlumatı bildirirlər;
- *Proqramlar-doktorlar* və ya faqi. Bunlar da virusa yoluxmuş faylları axtarıb tapır və onları "müalicə" edirlər, yəni faylı əvvəlki vəziyyətinə qaytarırlar. Faqların arasında yarımfaqlardan da istifadə olunur. Yarımfaqlar və yaxud proqramlar-doktorların təyinatı ondan ibarətdir ki, onlar böyük sayda virusları tapmaqla yanaşı onları məhv də edirlər;
- *Revizorlar* (və ya *müfəttişlər*) obyektin yoluxmamışdan qabaqkı vəziyyətini yadda saxlayır və mütamadi olaraq cari vəziyyəti başlanğıc vəziyyətlə müqayisə edirlər;
- *Proqramlar-süzgəclər* və ya rezidentlər (yaxud da daim işləyənlər) kompüter işləyən zaman onda baş vermiş şübhəli fəaliyyəti (viruslara xarakterik olan fəaliyyəti) aşkar etmək üçündür.
- *Vaksinlər* rezident proqramlardır, faylların virusa yoluxmasının qarşısını alırlar.

Müasir antivirus proqramları çoxfunksiyalı proqram kompleksidir, əsas vəzifələri virusu tapmaq, müalicə etmək (yəni kanarlaşdırmaq), həmçinin onun kompüterə daxil olmasına maneçilik etməkdir.

Müasir antivirus proqramları iki rejimdə işləyir.

Monitor rejimində antivirus daim işləyir, sistemin fayla müraciətini izləyir, prosesə daxil olmaqla bu faylların yoluxma predmetini yoxlayır. Deməli, virusun fayla düşməsi üçün etdiyi

birinci cəhd antivirus tərəfindən bloklanır (qıfıllanır) və bu barədə xəbərdarlıq olunur. Kompüter monitor rejimində işləyəndə kompüterin işində ləngimə baş verir, çünki hesablama resurslarının bir hissəsi işlərini antivirusa həsr edirlər, bununla yanaşı fayla və bəzi obyektlərə istənilən müraciət skanerləmə proseduru ilə həyata keçirilir. Digər tərəfdən əgər kompüterdə yoluxmuş fayllar varsa və o fayllar aktivlik göstərmirsə, onda onlara müraciət baş vermir, onlar nəzərdən kanarda qalırlar.

Skaner rejimində antivirus proqramı verilmiş sahədə (müəyyən kataloqda, sərt diskin bölmələrində və ya informasiya saxlayan bütün qurğularda) bütün faylları yoxlayır və yoluxmanı kanarlaşdırır (və ya skanerin sazlanmasından asılı olaraq onlar barədə məlumat verir). Verilənlərin kompüterdə yoxlanılması müəyyən qədər vaxt aparır (bəzən bir neçə saat). Bununla yanaşı bəzi hallarda virus sistemə skanerə əməliyyatı tamamlandıqdan sonra da düşə bilər.

Sistemin etibarlı müdafiə edilməsi üçün hər iki rejimdən istifadəni məsləhət bilirlər. Monitor rejimində antivirus proqramının daim işləməsi nəzərə alınmaqla yoxlamanı mütamadi olaraq həftədə bir dəfə (bütün verilənləri yoxlamaqla), skaner rejimində isə yoxlamanı axşamlar həyata keçirməyi məsləhət bilirlər.

Antivirusun öz "qurbanları"nı necə aşkar etməsi üsullarına baxaq.

Siqnatura əsaslanan aşkaretmə. Əgər antivirus sistemə virusun soxulmasını aşkar edirsə, onda antivurus faylı (və ya şəbəkədən gələn paketi) nəzərdən keçirir, sonra isə məşhur hücumların və ya virusların adları olan siqnatur lüğətə müraciət edir. Seçim edildikdən sonra antivirus fəaliyyətə başlayır.

Siqnaturun yaradılması əl ilə, bir neçə faylın korporativ araşdırmalar yolu ilə yerinə yetirilir. Siqnaturun avtomatik generasiya edilməsi (adətən polimorf viruslar olan mühitdə) hələlik tutarlı səviyyədə nəticə verməmişdir.

Hər bir müasir antivirus proqramı geniş (bir neçə yüz minlərlə) mütamadi yenilənən siqnatur bazasına malikdir. Yoluxmanın siqnaturlar vasitəsilə müəyyən edilməsi ona əsaslanır ki, yeni virus (hələlik siqnaturu bazada olmayan) çox asanlıqla antivirus müdafiəsini yarıb keçə bilər. Odur ki, siqnaturu yaradanda və onu istifadəçiyə təqdim edəndə bu 11-dən 97 saata kimi vaxt aparır (istehsalçıdan asılı olarq).

Nəzəri olaraq hesablanmışdır ki, virus İnternetə elə hücum təşkil edər ki, onu 30 saniyədən az müddət ərzində zəbt edər.

Proqramın özünü şübhəli aparmasının aşkar edilməsi üsulu. Antivirus proqramı bütün işləyən proqramların özünü necə aparmasını izləyir və virusa xarakter olan halların (məsələn, verilənlərin exe-fayla yazılmasını) aşkarlanmasına cəhd göstərir. Təcrübə göstərir ki, bu üsul bəzi hallarda baş vermiş hadisəyə reaksiya verə bilmir (yalana uyur), nəticədə istifadəçi edilən xəbardarlığa reaksiya vermir.

Üsulun müxtəlif növləri vardır.

*Proqramın **emulyasiya** olunması*, yəni proqram işə salınmazdan öncə antivirus onun özünü aparmasını (şübhəli halları izləmək məqsədi ilə) imitasiya etməyə çalışır.

AÇIQLAMA: *Emulyasiya* (ingiliscə emulation) hesablama texnikasında proqramlar, aparat vasitələri və ya onların birləşməsi (ahəngi, uyğunluğu) kompleksidir və bir hesablama sistemi (qonaq) funksiyasının digərinə (birincidən fərqli, hesablama sisteminə - hosta) kopiyalanması (və ya emulyasiyası) üçün nəzərdə tutulmuşdur (burada əsas

məsələ emulyasiya olunmuş sistemin özünü qonaq sistem kimi aparmasının vacibliyidir).

"*Ağ siyahı"* üsulu. Öncədən təhlükəsiz kod kimi administrator tərəfindən qeyd olunan kompüter kodları kombinasiyasının qabağı alınır (təhlükə yaratmayanlar nəzərə alınmır).

Evristik skanerə üsulu. Üsul siqnatura və evristikaya əsaslanır. Üsulun əsas məqsədi siqnaturdan istifadə etməklə skanerləmə bacarığını artırmaq və modifikasiya edilmiş virus versiyalarını aydınlaşdırmaqdır. Modifikasiya edilmiş virus versiyalarını aydınlaşdıranda siqnaturun naməlum proqram cismi ilə uyğunluğu ən azı 100% olması nəzərə alınmalıdır.

Texnologiya müasir proqramlarda istifadə olunur. İstifadə zamanı çox ehtiyatlı olmaq tələb edilir, çünki yalançı işləmələrin sayının çoxalma ehtimalı vardır.


İNTELLEKTUAL
SİSTEMLƏR VƏ
TEXNOLOGİYALAR

ŞƏBƏKƏNİN MÜDAFİƏ VASİTƏLƏRİ

Əgər müəssisənin və ya fərdi kompüterin lokal şəbəkəsinin İnternetə çıxışı varsa, onda izolə edilmiş şəbəkəyə və kompüterə nisbətdə təhlükəsizıik hədələri onlarla dəfə artmış olacaqdır. Şəbəkə vasitəsilə informasiyanın ötürülməsi və ya şəbəkədən informasiyanın alınması zamanı şəbəkə virusları, sistemə kanardan daxil olma cəhdləri (parolu oğurlamaqla, proqram təminatına pis məqsədlə daxil olma və s.) verilənlərin tutulması və ya dəyişdirilməsi – bütün bunlar ən çox rast gəlinən hədələrdəndir.

Şəbəkə hücumlarının xüsusiyyətini nəzərə almaqla istifadə edilən informasiyanın müdafiə edilməsi üçün müəyyən sayda vəsaitlər, üsullar (metodlar) və müdafiə texnologiyaları mövcuddur.

ŞƏBƏKƏLƏRARASI EKRANLAR

Şəbəkələrarası ekran (*brandmayer, fayrvol*) dedikdə, onlardan keçən şəbəkə paketlərinin verilmiş qanunlara uyğun müxtəlif səviyyələrdə ***OSI modelinin*** süzgəclənməsi (filtrlənməsi) prosesini və bütün bunlara nəzarətin yerinə yetirilməsini təmin edən aparat və/və ya proqram təminatı kompleksi başa düşülür.

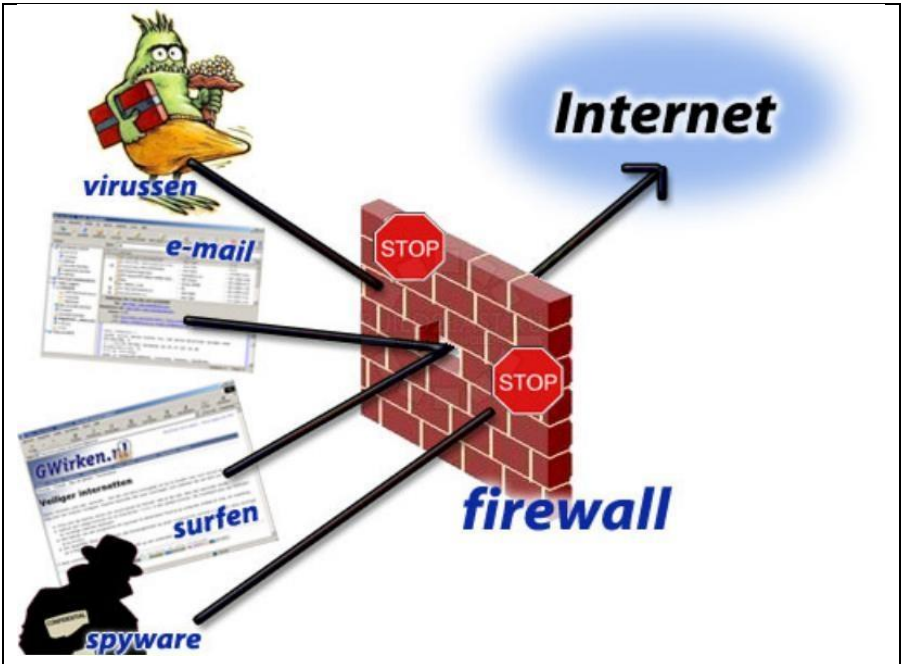
AÇIQLAMA: *OSI şəbəkə modeli* (Open Systems İnterconnection Basic Reference Model – Açıq sistemlərin

qarşılıqlı etalon baza modeli) dedikdə şəbəkə profokollarının yaradılması və kommunukasiyası üçün istifadə edilən abstrakt şəbəkə modeli qəbul edilir. OSI şəbəkəyə səviyyəli yanaşmanı təqdim edir. Hər bir səviyyə qarşılıqlı prosesə özünəməxsus xidmət göstərir. Belə struktur sayəsində şəbəkə avadanlıqları və proqram təminatı daha təbii və şəffaf olur. İndiki zamanda ən çox istifadə olunan TCP/IP protokollar ailəsidir. Nəzərə almaq lazımdır ki, TCP/IP protokollar ailəsinin yaradılması OSI ilə bağlı olmamışdır.

Şəbəkələrarası ekran qoşulduğu şəbəkədə bir neçə interfeysə malikdir. İstifadə edilən qanunlar bir şəbəkədən digər şəbəkəyə trafikin hansı şəkildə ötürülməsini müəyyənləşdirir. Əgər qanunda trafikin buraxılması nəzərə alınmamışsa, onda şəbəkələrarası ekran paketləri ya ləğv edir, ya da ki, qəbul etmir.

Şəbəkələrarası ekran bəzən şəbəkədə *proxy-server* kimi iştirak edir. Proxy-server – bu proqram və ya şəbəkə düyünüdür, müəssisənin daxili şəbəkəsi və xarici şəbəkəsi arasında ortaq rolunu yerinə yetirir (məsələn, İnternet). Proxy-server müəssisənin kompüterlərinin daxili ünvanlarını gizli saxlayır. Yerinə yetirilən funksiya *şəbəkə ünvanlarının translyasiyası* (NAT – Network Address Translation) adlanır. Əgər daxili şəbəkənin hər hansısa düyünü informasiyanı kanara ötürmək istəyərsə, onda o həmin informasiyanı proxy-serverə göndərir (proxy-server eyni zamanda şəbəkələrarası ekran rolunu oynayır). Şəbəkələrarası ekran süzgəcləmə siyasətinə uyğun göndərilən (ötürülən) informasiya paketlərini yoxladıqdan sonra yeni birləşməni başlayır və paketləri öz adından şəbəkəyə ötürür. Bütün bu əməliyyatların nəticəsində şəbəkə ünvanlamasının daxili sxemi gizli saxlanılır və pisniyyətli

insan tərəfindən onun təhlil edilməsi çətinləşir (əgər düşmən əməliyyatlar arasında əlaqəni araşdırmaq fikirindədirsə).



Windows əməliyyat sistemində fayrvoldan (və ya brandmayerdən) istifadə edilməsi

Şəbəkələrarası ekran müxtəlif kateqoriyalara uyğun təsnif olunur:

1.Nəzarət olunan verilənlər axınının əhatə edilməsindən asılı olaraq.

- *Ənənəvi şəbəkələrarası ekran* – ***şlüzə*** quraşdırılmış (serverə ötürülən şəbəkələrarası trafik) proqramdır və ya bir-birinə birləşmiş şəbəkələrarası daxil olan və

göndərilən verilənlər axınını nəzarətdə saxlayan aparat həllidir. Belə brandmayerin əsas vəzifəsi müəsisənin daxili şəbəkəsinə icazəsiz daxil olmanın qarşısını almaqdır.

- *Fərdi şəbəkələrarası ekran* – istifadəçinin kompüterinə yazılmış proqramdır və ondan istifadə olunmasında əsas məqsəd qeyriqanunu yolla ancaq bu kompüterə daxil olmaların qarşısının alınmasıdır.

2.OSI modelinin səviyyəsindən asılı olaraq əlçatanlığa nəzarət həyata keçirilir.

- *Şəbəkə səviyyəsində işləyənlər* – süzgəcləmə əməliyyatı göndərənin ünvanlarına və qəbul edənin paketlərinə (OSI modelinin transport səviyyəsində portların nömrələri, administrator tərəfindən verilmiş statik qanunlar) əsaslanmaqla baş verir;
- *Seans səviyyəsində işləyənlər* - əlavələrarası seans işlənilir və TCP/IP xüsusiyyətlərini pozan paketlər şəbəkəyə buraxılmır (belə paketlər tez-tez pisniyyətli məqsədlər üçün istifadə edilir, onlardan istifadə etməklə resursların kopiyası alınır, TCP/IP protokolundan düzgün istifadə etmədikdə pisniyyətli insanlar "sındırma"dan istifadə edir, birləşmələrin qırılması və informasiyanın yubanaraq göndərilməsi və buna bənzərlər baş verir);
- *Əlavələr səviyyəsində işləyənlər* – göndərilən paketlərin daxilində əlavə verilənlərə əsaslanmaqla süzgəcləmə əməliyyatı həyata keçirilir, sazlamalara və informasiya siyasətinə söykənməklə xoşagəlməyən və qorxulu informasiyanın ötürülməsi bloklanır (qıfıllanır).

3.Aktiv birləşmələrin izlənməsindən asılı olaraq aşağıdakılar yerinə yetirilir:

- *Stateless (sadə süzgəcləmə)* – cari birləşmələr izlənilmir (məsələn, ***TCP/IP protokolu***), amma verilənlər axını statik qanunlara ciddi əməl olunmaqla süzgəclənir;
- Stateful (***kontekst*** nəzərə alınmaqla süzgəcləmə) – cari birləşmələr izlənilir və o paketlər şəbəkəyə buraxılır ki, onlar uyğun protokolları və əlavələri müəyyən məntiqə və alqoritmə əsaslanmaqla təmin etsinlər.

Tətbiqi proqramlar kimi realizə edilən porulyar brandmayerləri nəzərədən keçirək.

1.*Outpost Firewall Pro*. Fərdi brandmayerdir, aşağıdakı funksiyalara malikdir:

- Verilənlərə qeyriqanunu daxil olmaların qarçısını alır;
- Şəbəkədə müdafiə edilən sistemin gizlədilməsi (sistem pisniyyətli "dağıdıcı" şəxs üçün "gözəgörünməz" olur);
- Daxil olan poçt məlumatlarının təhlili və baş verə biləcək potensial təhlükələrin bloklanması;
- Sistemın şəbəkə aktivliyinin təhlili və monitorinqi;
- "Qadağa" qoyulmuş saytlara daxil olmaların (əlçatanlığın) bloklanması (əsasəndə uşaqlar və şöbədə işləyən bəzi əməkdaşlar üçün nəzərdə tutulur).

2.*ZoneAlarm Pro*. Funksional sazlamalara uyuşanlıq (çeviklik) göstərən güclü brandmayerin imkanlarına aşağıdakılar daxildir:

- Şəbəkədə istifadə olunan hər bir proqram üçün qanunun yerinə yetirilməsinə imkan verən süzgəc əlavəsi;
- Rəqəmsal imzanın dəstəklənməsi;
- Hadisələrin ətraflı *loq-faylı* və onun təhlili üçün vasitələr (nəticədə mətn və qrafik təhlili istifadəçiyə təqdim edir);
- Cookies sazlanan nəzarəti;

- Daxil olma əlavəsinin İnternetə ötürülməsinin bloklanmasını avtomatik və ya əl ilə yerinə yetirən ani mexanizm;
- Elektron poçt ilə İnternetə yerləşdirilmişin avtomatik yoxlanılması.

AÇIQLAMA: *Kontekst* (latınca *contextus* – "birləşmə", "əlaqə" anlamlarını verir) mətnin yazılı və ya şifahi formada olan tamamlanmış hissəsidir. Kontekst ümumi mənada mətnə daxil olan ayrı-ayrı sözlərin, cümlələrin və i.a. müəyyənləşdirilməsinə imkan verir.

İnternetə qoşulmaq istəyən təşkilat xüsusi kompüterdən istifadə edir ki, buna ***şlüz*** deyilir. Şlüz, məlumatların lazımi ötürmə marşrutlarını seçməklə bərabər, şəbəkənin ayrı-ayrı hissələrində nasazlıqlar baş verən halda məlumatların ötürülmə marşrutlarını təshih (korrektə) etmək üçün daha böyük şəbəkəyə qoşulan altşəbəkələrin parametrləri haqqında məlumata malik olmalıdır. Burada yerləşdirilmiş proqram təminatı vasitəsilə şlüzdən keçən bütün məlumatlar işlənir. Hər bir şlüzün öz İnternet protokol ünvanı olur.

1973-cü ildə DARPA-nın İnformasiya Departamentinin direktoru Robert Elliot (Bob) Kan və amerika alimi Vinton Qrey Serf Pentaqonun Elmi Tədqiqatları İdarəsi (Defense Advanced Research Projects Agency) DARPA-da işləyərkən informasiyanın paketlər vasitəsi ilə uzaq məsafələrə ötürülməsi üçün protokol kəşf edirlər və onu sonralar TCP/IP protokolu adlandırırlar.

İnternet şlüz

Loq-fayl (Log-file) – mətn faylıdır, sayta aid olan bütün sorğuları, həmçinin bu sorğular ilə bağlı olan səhvləri də qeydiyyatdan keçirir.

Robert Elliot (Bob) Kan

Vinton Qrey Serf

XÜSUSİ VİRTUAL ŞƏBƏKƏ (VPN)

Xüsusi virtual şəbəkə (VPN) dedikdə başqa bir şəbəkənin üzərində yaradılmış (qurulumş) məntiqi şəbəkə (əsasəndə İnternet) başa düşülür. Şəbəkənin düyünləri arasından ötürülən bütün verilənlər şifrələnir, bu səbəbdən fiziki verilənlər təhlükəsiz protokollar vasitəsilə aşıq şəbəkə ilə ötürülür, mahiyyət etibarı ilə isə VPN ilə əlaqəsi olmayan bağlı informasiya mübadiləsi kanalı funksiyasını həyata keçirir.

Şifrələmədən istifadə etməklə müdafiə olunan iki düyün arasındakı kanaldan ***trafikin*** ötürülməsi *tunel* adlanır.

VPN iki əsas sinfə bölünür:

1.*Müdafiə olunan*. Bu ən çox yayılmış variantdır. Bu variantdan istifadə etməklə etibarsız şəbəkəni (məsələn, İnternet şəbəkəsi) etibarlı və müdafiə olunan altşəbəkəyə çevirmək olur. VPN -ə nümunə kimi IPSec, OpenVPN və PPTP (nöqtədən nöqtəyə tunel kimi istifadə olunan protokol) şəbəkələrini göstərmək mümkündür.

2.*Etibarlı*. Virtual altşəbəkənin yaradılması üçün istifadə olunur. Altşəbəkə müdafiə olunan və etibarlı başqa bir şəbəkənin əsasında yaradılır. Altşəbəkədə təhlükəsizliyin təmin edilməsi məsələsi əsas sayılmır. Etibarlı VPN şəbəkəsinə MPLS və L2TP protokollarını nümunə kimi göstərmək olar.

AÇIQLAMA: İngilis sözü "*traffic*" tərcümə olunduqda "hərəkət", "transport", "daşınma" və "ticarət" anlamlarını verir. İnternet-trafik müəyyən vaxt anında İnternetdən ötürülən verilənlərin tutumudur. Daxil olan və yola salınan trafilklərdən istifadə olunur. Daxil olan trafik istifadəçinin İnternetdən qəbul etdiyi, xaric olan isə istifadəçinin ötürdüyü (yola saldığı) verilənlərin tutumu başa düşülür. Trafik

bitlərlə, baytlarla və s. ilə ölçülür.

Texniki məsələlərin həll edilmə arxitekturasına görə VPN aşağıdakı siniflərə bölünür:

1.*Korporativ daxili*. Bu sinif müəssisə daxili bölmələr arasında qarşılıqlı münasibətin müdafiə olunmasını və korporativ əlaqələri olan birliklərin müəssisənin daxilində yaradılmış qruplar ilə əlaqəsini təmin edir (bura seçilərək ayrılmış rabitə xətlərini də əlavə etmək lazımdır).

2.*Uzaqlaşdırılmış əlçatanlığı olan VPN*. Bu sinif korporativ informasiya resurslarına malik olan şirkətin uzaq məsafədə olan əməkdaşlarının və ya mobil telefonla əlaqələr yaradan işçilərinın (şirkətdən çox-çox uzaqda işləyənlər nəzərdə tutulur) informasiya əlaqələri yaratması zamanı müdafiənin yaradılmasını təmin etmək üçün nəzərdə tutulmuşdur.

3.*Korporativarası VPN* (extranet VPN). Bu sinif bir şirkətin şəbəkəsindən digər şirkətin şəbəkəsinə daxil olan zaman müdafiənin təmin olunması üçün nəzərdə tutulmuşdur (məsələn, tərəfdaşlar, müştərilər və s.).

Texniki realizə olunma üsuluna görə VPN aşağıdakı kimi təsnif edilir:

- Marşrutlaşdırıcılara əsaslanmaqla (qrafikanın şifrələnməsi məsələsi marşrutlaşdırıcıların köməyilə yerinə yetirilir və lokal şəbəkədən alınan informasiya onlardan keçir);
- Şəbəkələrarası ekrana əsaslanmaqla;
- Proqram təminatına əsaslanmaqla;
- Xüsusi hazırlanmış aparat vasitələrinə əsaslanmaqla.

IPSec protokolları toplumunu nəzərdən keçirək. Toplum IP protokoluna uyğun ötürülən verilənlərin müdafiə edilməsi üçün müəyyən edilmişdir. IPSec protokolu IP paketlərinin

əslliyini və şifrələnməsini təsdiq etməyə imkan verir. Protokol İnternetdən istifadə etməklə açarların dəyişdirilməsi əməliyyatının müdafiə olunmasını təmin edir.

IPSec protokolları OSI şəbəkə modeli səviyyəsində işləyir. Onları iki sinifə bölürlər:

- Verilənlər axınının ötürülməsinin müdafiəsinə cavabdeh olan protokollar (ESP, AH);
- Açarlarla mübadilə protokolları (IKE).

Verilənlər axınının ötürülməsinin müdafiəsinə cavabdeh olan protokollar iki rejimdə işləyirlər:

- Daşıma (transport) rejimi;
- Tinel rejimi.

Daşıma rejimində IP-paketinin informasiya hissəsi şifrələnir (və ya imzalanır), amma başlıqlara toxunulmur (bu baxımdan marşrutlama proseduru dəyişmir).

Tunel rejimində IP-paketi tamamilə şifrələnir. Şifrələnmiş paketi şəbəkə ilə ötürmək üçün paket dikər IP-paketinə yerləşdirilir. Nəzərə çatdırmaq lazımdır ki, bu rejim xüsusi virtual şəbəkənin təşkil edilməsində istifadə olunur.

IPSec-tunelləmə rejimi aşağıdakı kimi işləyir:

1.Adi IP-paketi yola salan IPSec-qurğusuna yönəldilir (şəbəkəarası ekran və ya marşrutlaşdırıcı) və orada şifrələndikdən sonra lokal şəbəkənin sonuncu sisteminə göndərilir.

2.Yola salan IPSec-qurğusu qəbul edən qurğunu autentifikasiya edir.

3.İki "IPSec-qurğusu" öz aralarında istifadə edəcəkləri şifrə və alqoritm autentifikasiyası barədə "razılığa" gəlirlər.

4.Yola salan IPSec-qurğusu informasiyalı IP-paketini şifrələyir və onu digər AH (başlıqlar ilə autentifikasiya olunmuş) paketinə yerləşdirir.

5.Paket TCP/IP protokoluna uyğun olaraq şəbəkə ilə göndərilir.

6.Göndəriləni qəbul edən IPSec-qurğusu IP-paketini oxuyur, onun əslliyini (həqiqiliyini) yoxlayır və şifrələnmişləri şifrədən azad edir.

7.Qəbul edən qurğu başlanğıc paketi təyin edilmiş punkta göndərir.

ZORLA MÜDAXİLƏNİ AŞKARLAYAN SİSTEMLƏR (IDS)

Zorla müdaxiləni aşkarlayan sistemlər - (Intrusion Detection System – IDS) – kompüter sistemlərinə qeyriqanuni yolla (müəlliflik hüquqi olmadan) daxil olma faktlarını aşkarlamaq üşün istifadə olunan, həmçinin sistemə icazəsiz daxil olaraq onu idarə edənlərə qarşı (əsasəndə İnternetdən istifadə etməklə) mübarizə aparan proqram və ya aparat vasitələridir.

Zorla müdaxiləni aşkarlayan sistemlər şəbəkənin və ya sistemlərin təhlükəsizliyinin pozulması zamanı zərərverici aktivliyin bəzi tiplərini aşkarlamaq üçün istifadə edilir. Bunlara nümunə kimi servislərin üstünlüyünün müəyyən edilməsini, vacib sayılan fayllara müəlliflik hüquqi olmayanların daxil olmasını, zəif quruluşa malik servislərə qarşı şəbəkə hücumlarını, həmçinin ziyanverici proqramların (məsələn, viruslar, troya atları və s.) fəaliyyətinə dəstək verən proqram təminatını göstərmək olar.

Zorla müdaxiləni aşkarlayan sistemlər aşağıdakı komponentlərdən (təşkiledicilərdən) ibarətdir:

1.*Sensor altsistem* müdafiə edilən sistemin fəaliyyətinə toxunan hadisələri izləyir.

2.*Təhlilin altsistemi* bu hadisələrin içərisindən elələrini müəyyən edir ki, onlar ya təhlükəsizliyi pozurlar, ya da ki, sistem üçün təhlükə mənbəyinə çevrilirlər.

Zorla müdaxiləni aşkarlayan passiv sistemlərdə belə hadisələri aşkar edəndə hadisə haqqında informasiya saxlanca yerləşdirilir, sonra isə təhlükə haqqında siqnal müəyyən kanal ilə sistem administratoruna istiqamətləndirilir.

Zorla müdaxiləni aşkarlayan aktiv sistemlərdə (zorla müdaxiləni aradan qaldıran sistemlər) eyni cavab tədbirləri həyata keçirilir (məsələn, birləşmə "qırılır" və ya bədniyyətli insandan trafikin təhlükəsizliyini təmin etmək üçün şəbəkəarası ekran avtomatik sazlanır).

3.*Saxlanc* sensor altsistemin verilənlərinin saxlanmasını və toplanmasını, həmçinin onların təhlil edilməsi nəticəsində alınmış məlumatları saxlamaq üçündür.

4.***İdarəetmə konsolu*** zorla müdaxiləni aşkarlayan sistemlərin sazlanması üçün istifadə edilir. Bununla yanaşı idarəetmə konsolu müdafiə olunan sistemin vəziyyətini, altsistemdə aşkarlanmış qarşıdurmanın təhlilini həyata keçirir.

> ***AÇIQLAMA***: *Kompüter konsolu* (ingiliscə console – idarəetmə pultu) kompüter ilə insan-operator arasında qarşlıqlı əlaqəni təmin edən qurğular toplumudur (bura giriş-çıxış qurğuları da əlavə edilməlidir).

Müasir zorla müdaxiləni aşkarlayan sistemlərin bəzi növlərini araşdıraq.

1.*Şəbəkə seqmentini müdafiə edən sistemlər*. Heç bir əlavənin işləmədiyi xüsusi serverdə qurularaq işləyir (sistem əsasən edilən hücumlardan etibarlı qorunur, bununla yanaşı serverə edilən hücumlara "görünməyəndir"). Şəbəkəni müdafiə

etmək üçün bir neçə belə server şəbəkəyə qoşulur və onlar şəbəkə trafikini müxtəlif şəbəkə seqmentlərində təhlil edirlər. Beləliklə, bir neçə əlverişli yerləşdirilmiş sistem böyük şəbəkəyə nəzarət edə bilir.

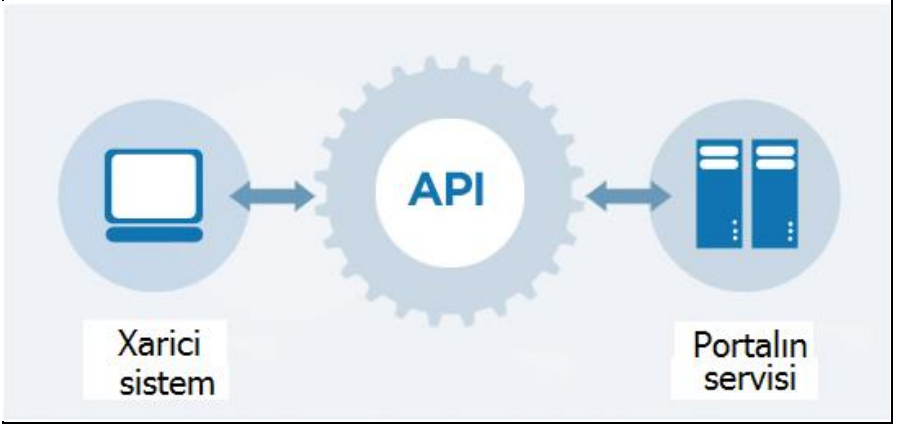
Belə sistemlərin çatışmazlıqları şəbəkənin ancaq böyük yük altında işlədiyi momentdə ona edilən hücumu tanıması (müəyyən etməsi) və sistemə edilən hücumun ziyankarlıq dərəcəsini təhlil edə bilməməsidir.

2.*Ayrıca serveri müdafiə edən sistemlər*. Burada konkret serverdə baş verən proseslər haqqında informasiya toplanılır və təhlil edilir. Təhlil nəticəsində vurulacaq ziyanın hansı pisniyyətli istifadəçi tərəfindən yerinə yetiriləcəyi müəyyən edilir. Bəzən sistemdə bir neçə qrup server idarə olunur, mərkəzləşdirilmiş şəkildə hesablamalar aparılır və mümkün hücumlar araşdırılır. Ondəki sistemdən fərqli olaraq bu sistem şifrələnmiş verilənlər ilə də işləyə bilir. Nəzərə almaq lazımdır ki, bu sinifə aid olan sistem ancaq "öz" serverindən paketləri qəbul etdiyi üçün bütün şəbəkədə baş vermiş situasiyalara (vəziyyətlərə) nəzarət edə bilmir, nəticədə effektivlik aşağı düşmüş olur.

3.*Əlavələri müdafiə edən sistem*. Ayrı-ayrı əlavələr hüdudunda yaranan hadisələrə nəzarət edir. Əlavələr haqqında məlumata malik olmaq, sistem jurnalının köməyilə onu təhlil etmək və birbaşa ***API*** ilə əlaqələndirmək, bütün bunlar istifadəçinin fəaliyyətinə nəzarəti həyata keçirməyə imkan verir.

AÇIQLAMA: *Proqram əlavəsi interfeysi* (ingiliscə Application Programming Interface, *API)* – proqramçının proqram təşkiledicilərinin funksionallığına (proqramlar, modullar, kitabxanalar) əlçatanlıq üçün istifadə etdiyi üsullar (funksiyalar) toplusudur. API funksionallığı "təmiz görkəmdə" təsvir edən əsas mücərrəd fikirdir. Əgər proqram

(modul, klitabxana) "qara qutu" kimi təsvir edilirsə, onda API – çoxlu sayda "dəstəklər"dir ("əltutanlardır") və onlardan istifadə etməklə istifadəçi qara qutuya əlçatanlıq edə bilir, qutunu firlada və ya silkələyə bilir. Proqram vasitələri bir-birilə API vasitəsilə əlaqə saxlayırlar. Bu zaman adi təşkiledicilər ierarxiyanı yaradırlar – yüksək səviyyəli təşkiledicilər API-dən aşağı səviyyəli təşkiledici kimi istifadə edirlər, daha doğrusu API daha aşağı səviyyəli təşkiledicilərdən istifadə edir. İnternet vasitəsilə verilənlərin ötürmə protokolu API prinsipinə uyğun qurulur. İnternetin standart protokolu (OSI şəbəkə modulu) 7 səviyyəni dəstəkləyir. Hər bir səviyyə verilənlərin ötürülməsinin öndəkinin funksionallığından istifadə edir və bu da öz növbəsində növbəti səviyyənin tələb edilən funksionallığına imkan verir. Qeyd etmək lazımdır ki, protokol anlamının API anlamı ilə yaxınlığı vardır.



Antivirus proqramlarında olduğu kimi sistemə olunan hədələrin aşkar edilməsini iki yanaşmadan araşdırırlar:

1.*Siqnaturaya əsaslanan yanaşma*. Bu yanaşmada məşhur hücumları təsvir edən unikal hadisələr toplumuna uyğun fəaliyyət aydınlaşdırılır. Üsul effektivdir və kommersiya proqramlarında istifadə edilən əsas üsullardan sayılır. Amma nəzərə almaq lazımdır ki, zorla müdaxiləni aşkarlayan sistemlər yeni yaranan hücumlarla, həmçinin ənənəvi videohücumlarla tutarlı səviyyədə mübarizə apara bilmirlər.

2.*Anomaliyaya əsaslanan yanaşma*. Bu yanaşmada hücumu aşkar etməklə yanaşı serverə və ya şəbəkəyə edilən qeyriadi hücumlarda identifikasiya olunur. Yanaşma istifadəçiyə öncədən planlaşdırılmamış (həmçinin proqramlaşdırılmamış) hücumların qarşısını almağa imkan verir.

YOXLAMA TESTLƏRİ

1.Makroviruslar hansı yolla sistemə daxil olurlar?

A.Elektron poçt vasitəsilə;

B.Yoluxmuş fayllarla birlikdə istənilən üsuldan istifadə etməklə;

C.Pisniyyətli insan virusu sistemə əl ilə daxil etdikdə;

D.Şəbəkə proqramlarında yaranmış səhvlər zamanı İnternetdən istifadə edəndə;

E.Gəzdirilə bilən yaddaşlardan istifadə edəndə.

2.Fərdi lüğətə hücumlar edilən zaman istifadə olunan parol hansı tələbləri ödəməlidir?

A.Parolu yaradan zaman şəxsi verilənlərdən istifadə edilməməlidir;

B.Parolun uzunluğu 12 və ya daha çox simvoldan ibarət olmalıdır;

C.Parolu hər "yoldan keçənə" açmaq (göstərmək) olmaz;
D.Müxtəliv servislər müxtəlif parollar ilə müdafiə edilməlidir;
E.Parol müxtəlif əlifbanın müxtəlif simvollarından, reqistrlərdən, rəqəmlərdən, işarələrdən, durğu işarələrindən və s. yaradılmalıdır.

3.Hücumu aşkar edən, anomaliyaya əsaslanan yanaşma ilə işləyən sistemin hansı çatışmazlıqları vardır?
A.Yalançı (uydurma) işləmələrin yüksək faizlə olması;
B.Bütün şəbəkəyə nəzarəti həyata keçirmək imkanının olmaması;
C.Hücumların daxil olmasını təhlil etmək qabiliyyətinin olmaması;
D.Şəbəkənin həddindən artıq yüklənməsi nəticəsində yerinə yetirəcəyi işin çətinliklə həyata keçirməsi.
E.Quraşdırıldığı serverin işləmə effektivliyinin azalmasına görə.

4. ... – kanaldan keçən şifrələnmiş informasiyaya görə müdafiə edilən, iki düyün arasındakı kanal necə adlanır?

5.Əməliyyat sisteminin işə düşməsi üçün start veriləndə yaranan virus (həmçinin operativ yaddaşda daima fəaliyyət göstərən virus) necə adlanır?
A.Rezident viruslar;
B.Stels-viruslar;
C.Makroviruslar;
D.Polimorf virusları;
E.Troya atları.

6.Cari birləşməni izləyən, məntiq və alqoritmin işini təmin edən uyğun əlavələr və protokollardan istifadə etməklə işləyən şəbəkələrarası ekran hansı sinifə məxsusdur?

A.Şəbəkə səviyyəsində işləyənlər sinifinə;
B.Seans səviyyəsində işləyənlər sinifinə;
C.Əlavələr səviyyəsində işləyənlər sinifinə;
D.Stateless;
E.Stateful.

7.Rezident kimi işləyən və faylları yoluxduran virus necə adlanır?

A.Detektorlar;
B.Faqilər;
C.Revizorlar (və ya müfəttişlər);
D.Vaksinlər;
E.Süzgəclər.

8.Verilənlərin daşıyıcılarını yoluxduran viruslar hansılardır?

A.Fayl virusları;
B.Yükləmə virusları;
C.Makroviruslar;
D.Şəbəkə soxulcanları;
E.Troya atları.

9.VPN -ə əsaslanaraq etbarsız şəbəkədən etibarlı və müdafiə olunan altşəbəkənin yaradılması necə adlanır?

A.Daxili korporativ;
B.Müdafiə olunan;
C.Uzaqlaşdırılmış əlçatanlıqlı;
D.Məxfi;
E.Korporativ arası.

10.Fişinqə qarşı əks təsir göstərə bilən parol hansı tələbləri ödəməlidir?

A.Parol istənilən təbii dildəki istənilən sözlərdən yaradılmamalıdır;

B.Parolun uzunluğu 12 və daha çox simvoldan ibarət olmalıdır;

C.Parolu heç kimə göstərmək olmaz;

D.Müxtəlif servislər müxtəlif parollar ilə müdafiə olunmalıdır;

E.Parola müxtəlif əlifbanın müxtəlif simvolları və registrləri, ədədlər, durğu işarələri və s. əlavə edilməlidir.

11.VPN nədir?

A.Zorla girməni müəyyən edən sistem;

B.Mübadilə açarı protokolu;

C.Şəbəkə ünvanlarının translyasiyası;

D.Şəbəkənin virtual hissəsi;

E.Ötürülən axının müdafiə edilmə protokolu.

12.Evristik skanerə üsulu ilə virusun müəyyən edilməsində əsas çatışmazlıq nədən ibarətdir?

A.Yalançı işə düşmənin hiss edilmə ehtimalı;

B.Antivirusun həddindən artıq ağır işləməsi;

C.Yeni virusların müəyyən edilməsinin imkansızlığı;

D.Antivirusun ağır zəhmət bahasına əmələ gələn əl ilə sazlanmasına tələbatın olması.

ŞƏBƏKƏLƏRİN İNFORMASİYA TƏHLÜKƏSİZLİYİ PROBLEMLƏRİ

Kompüter şəbəkələrini avtonom (müstəqil işləyən) kompüterlərdən ayıran əsas xüsusiyyətlər onlarda informasiya mübadiləsinin şəbəkə düyünləri arasında baş verməsi və verilənlərin xətlər vasitəsilə ötürülməsi məsələlərinin həlli ilə bağlıdır.

Kompüterlərin kompüter şəbəkələrində birləşməsi istifadəçiyə kompüter sistemlərindən effektiv istifadə etməsinə imkan verir. Bu zaman effektivliyin artırılması kompüter şəbəkələri arasında informasiya mübadiləsinin həyata keçirilməsi hesabına, həmçinin hər bir kompüterdə şəbəkənin ümumi resurslarından istifadə imkanının olmasına görə baş verir (informasiya resursları dedikdə informasiya, xarici yaddaş qurğusu, proqram əlavələri, xarici qurğular və s. nəzərdə tutulur).

Korporativ şəbəkənin əsas əlamətlərindən biri müəssisə filiallarının ayrı-ayrı lokal şəbəkələrinin qlobal şəbəkə daxilində birləşməsi və müəssisənin mərkəzi lokal şəbəkədən uzaqda yerləşmiş əməkdaşlarının istifadə etdiyi kompüterlərin birləşdirilərək istifadə edilməsidir. Son illərdə kompüterlərin naqilsiz əlaqə xətlərindən istifadəsi geniş füsət almışdır (nümunə kimi WLAN – Wireless Local Area Network naqilsiz lokal şəbəkəni göstərmək olar).

ŞƏBƏKƏ İNFORMASİYA MÜBADİLƏSİNƏ GİRİŞ

İnformasiya texnologiyalarının çox sürətli inkişafı İnternet qlobal şəbəkəsinində sürətli inkişafına səbəb oldu. Kompüter şəbəkələrinin inkişafı standart aparat təminatı prinsiplərinə ciddi nəzarət edilməsi və proqram təminatının düzgün seçilməsi ilə bağlıdır. Müasir anlamda İnternetin yaranma tarixi TCP/IP kommunikasiya protokollarının 1983-cü ildən başlayaraq standartlaşdırılması ilə bir-başa əlaqəli olmaqla yanaşı Ümumdünya Hörümçək Torunun yaranmasına da təkan verdi (əsasını qoydu). İnternet kompüter şəbəkələrinin bir-biri ilə qarşılıqlı əlaqəsinin yaradılması kompüterlər arasında informasiya mübadiləsinin ümumi razılıq prinsipinə uyğun tətbiqi ilə bağlıdır.

İNTERNET ŞƏBƏKƏDƏN İSTİFADƏ

İnternet qlobal şəbəkəsinin inkişafı daha ücuz və daha əlçatan korporativ qlobal şəbəkələrinin qurulmasına (seçilmiş kanallar ilə müqayisə etdikdə) və İnternetdən informasiyanin nəql edilməsi üçün istifadə edilməsinə əhəmiyyətli dərəcə də yardımçı oldu. İnternet şəbəkəsi istifadəçiyə müxtəlif kommunikasiya metodları təklif edir, informasiyanın təhlil edilməsi üçün əlçatan üsullardan istifadəyə şərait yaradır və nəhayət belə tədbirlərin həyata keçirilməsi nəticəsində çoxlu sayda şirkətlərin həm informasiya mübadiləsində, həm də ki, onların iqtisadi baxımdan inkişaf etməsilə yanaşı lazımlı səviyyədə informasiya sistemlərindən istifadə etmələrinə geniş imkanlar yaradır.

İnternetin korporativ şəbəkələrə yeni anlamda təsir göstərməsi yeni şəbəkələrin – İntranet (İntranet, İntraşəbəkə)

yaranmasına gətirib çıxarır. Bu zaman İnternetə məxsus olan informasiyanın təhlili və nəql olunması korporativ şəbəkəyə də aid olunur.

İnternet şəbəkə korporativ şəbəkənin qurulmasına müəyyən imkanlar təqdim edir, bunları qeyd edək.

İnternetin üçuz və əlçatan kommunikasiya kanalı. XXI əsrin əvvəlində dünyada İnternetin və şəbəkələrin kollektiv formada güclü inkişafı nəticəsində informasiyanın müxtəlif istiqamətlərdə yayılmasına və istifadəçilər üçün informasiyaya əlçatanlığın təmin edilməsi həyata keçirildi. İstifadəçilər ücüz və əlçatan kommunikasiya kanalı olan İnternetdən səmərəli istifadə etməyə başladılar. Digər tərəfdən istifadə olunan avadanlıqlardan iqtisadi baxımdan əlverişli istifadə olunması istifadəçiyə bu kanallardan istifadə etməklə informasiyanın ötürülməsi ilə yanaşı idarə edilməsinə də imkan yaratdı.

Universallıq. İnternetin yaradılmasında əsas məqsəd uzaq məsafədə yerləşən istifadəçilər arasında informasiya əlaqəsinin yaradılması olmuşdur. İnternet-texnologiyaların inkişafı populyar istifadəçi şəbəkəsinin (World Wide Web – WWW) yaranmasına gətirib çıxardı ki, bununda nəticəsində istifadəçi bir-başa olaraq qlobal qulluq növündən bəhrələnə bildi. Texnologiyadan istifadə edən istifadəçiyə WWW-brauzerdən istifadə etməklə qlobal şəbəkəyə qoşularaq ona lazım olan informasiyaya baxış keçirməyə imkan yarandı. İnformasiyaya baxış utilitləri və informasiya serverləri arasında informasiya mübadiləsi interfeyslərinin standartlaşdırılması ilə eyni interfeysli müxtəlif platformalardan istifadəni təşkil etdi.

Müxtəlif xarakterli informasiyaya və İnternet qulluqlarına əlçatanlıq. Müxtəlif növ abonentlər üçün verilənlərin tranzit ötürülməsinə görə nəzərdə tutulmuş nəql xidmətlərindən başqa İnternet şəbəkəsi geniş çeşidli, yüksək

səviyyəli İnternet-servislərin çatdırılmasını təmin edir. Bura: ümumdünya hörümçək toru World Wide Web; DNS domen adları servisi; FTP fayl arxivlərinə daxil olma; elektron poçt (e-mail); telekonfrans (Usenet); ICQ, IRC mübadilə servisi; Telnet servisi; İnternetdə informasiya axtarışı aiddir.

Bu xidmətləri təqdim edən kompüterlər *serverlər*, bu xidmətlərdən bəhrələnən kompüterlər isə *müştərilər* adlanır. Bu terminlər kompüter-serverlərdə və kompüter-müştərilərdə istifadə olunan proqram təminatına da aiddir. İnternet şəbəkəsi istifadəçini böyük həcmdə və müxtəlif xarakterdə informasiya ilə təmin edir ki, bu da şəbəkəyə qoşulmuş *host-düyünlər* vasitəsilə yerinə yetirilir. Host dedikdə kompüter və ya kompüterlər qrupu nəzərdə tutulur. Host İnternet ilə bir başa şəbəkə birləşməsinə malikdir və istifadəçiyə şəbəkənin bütün imkanlarından istifadə etməyə şərait yaradır. Bu kompüterlərdən əksəriyyəti server rolunu icra edir və istənilən istifadəçiyə İnternetə çıxış verməklə yanaşı elektron resurslara – verilənlərə, əlavələrə və xidmətlərə də çıxış imkanı verir. Şirkətlər özlərinə məxsus şəbəkəni bu resurslarla birləşdirməklə effektiv informasiya axınından və kommunukasiyadan səmərəli bəhrələnə bilər. Göstərilən xidmətlərdən yararlanan şirkətlər bu xidmətlərin üstünlüklərindən istifadə etməklə çəkilən xərcləri minimuma endirməklə yanaşı effektivliyin yüksəlməsinə də nail ola bilərlər.

İstifadədə sadəlik. İnternet-texnologiyadan istifadə etmək üçün personalın xüsusi olaraq öyrədilməsi tələb edilmir.

Lokal şəbəkələrin qlobal şəbəkəyə birləşdirilməsi üçün xüsusi kompüterlərdən (marşrutlaşdırıcılardan və şlüzlərdən) istifadə olunur. Onların köməyilə lokal şəbəkə şəbəkələrarası rabitə kanalına birləşdirilir. Marşrutlaşdırıcılar və şlüzlər lokal şəbəkəni fiziki olaraq bir-biri ilə birləşdirir. Bu zaman xüsusi

hazırlanmış proqram təminatından istifadə olunur ki, onun da köməyilə verilənlər bir şəbəkədən digərinə ötürülür. Qlobal şəbəkə mürəkkəb şaxələnmiş struktura və bolluca (çoxlu miqdarda) əlaqələrə malikdir. Marşrutlaşdırıcılar və şlüzlər qlobal şəbəkələrdə verilənlərin ötürülməsi zamanı optimal axtarışı təmin edir və bununda nəticəsində məlumatlar axınının maksimal sürəti əldə olunur. Lokal şəbəkələr arasında yüksək sürətli rabitə kanalı optik-lifli kabellərdən və ya peyk rabitə kanalından istifadə edilməsi nəticəsində əldə olunur. Bəzi hallarda şəbəkələr arasında əlaqəni yaratmaq üçün misdən hazırlanmış telefon xətlərindən istifadə edilir.

İnternet şəbəkə texnologiyasından istifadə etməklə korporativ kompüter şəbəkələrinin qurulması üçün ən əvvəl TCP/IP protokolundan istifadə edilməlidir. Bu verilənlərin nəql edilməsinə və Veb-texnologiyadan istifadəyə imkanlar yaradır.

ISO/OSI MODELİ VƏ TCP/IP PROTOKOLAR YIĞIMI

Kompüter şəbəkələrini yaradan zaman əsas məsələ elektriki və mexaniki xarakteristikaya malik olan avadanlıqların müştərək (bir yerdə) işləməsinin təmin edilməsi, kodlaşdırma və verilənlərin formatlanması sisteminin informasiya təminatının (proqramlar və verilənlər nəzərdə tutulur) uyuşanlığıdır. Bu məsələlərin həll edilməsi standartlaşdırma sahəsinə aiddir. Kompüter şəbəkələrində standartlaşdırmanın metodoloji əsasları qarşılıqlı əlaqəsi olan şəbəkə avadanlıqların yaradılmasına çoxsəviyyəli yanaşmadır. Belə yanaşmanın əsasını 1980-cı ildə Ümumdünya Standartlar Təşkilatı (ISO – International Standards Organization) tərəfindən hazırlanmış və təklif olunmuş texniki təkliflər təşkil edir. Bu baxımdan ISO

tərəfindən *açıq sistemlərin standarta əsaslanan qarşılıqlı əlaqə modeli* (OSI – Open Systems Interconnection) işlənib hazırlandı. ISO/OSI modeli kompüter şəbəkələrinin inkişafında əsas rol oynadı.

OSI modeli müxtəlif səviyyəli sistemlərin aralarındakı fərqləri müəyyən etməklə yanaşı həmin sistemlərin hansı funksiyaları yerinə yetirmələrini də müəyyənləşdirir. Vasitələrin qarşılıqlı əlaqə modeli OSI yeddi səviyyəyə bölünür:

- Tətbiqi (Application);
- Təqdimatlı (Presentation);
- Sesiyalı (Session);
- Nəqli (Transport);
- Şəbəkə (Network);
- Kanallı (Data Link);
- Fiziki (Physical).

Modelin ən yuxarı səviyyəsi Tətbiqi (Application) səviyyədir. Bu səviyyədə istifadəçi əlavələr ilə qarşılıqlı münasibətdə olur. Modelin ən aşağı səviyyəsi isə Fiziki (Physical) səviyyədir. Bu səviyyədə isə qurğular arasında siqnal mübadiləsi həyata keçirilir.

Rabitə kanalı vasitəsilə verilənlərin mübadiləsi verilənlərin yuxarı səviyyədən aşağı səviyyəyə sürüşdürülməsi ilə yerinə yetirilir. Sonrakı mərhələdə verilənlərin rabitə kanalı vasitəsilə nəql edilməsi əməliyyatı və nəhayət, müştərinin kompüterində verilənlərin əks əlaqə ilə sürüşdürülməsi, yəni aşağı səviyyədən yuxarı səviyyəyə ötürülməsi yerinə yetirilir.

Kompüter şəbəkəsinin hər bir səviyyəsində müəyyən uyğunluğu təmin etmək üçün *xüsusi standart protokollardan* istifadə edilir. Protokollar məlumatların formatlanması və ardıcıllığını formallaşdıran qanunlardan (qaydalardan) ibarətdir. Protokolların köməyilə bir səviyyədə və müxtəlif şəbəkə

düyünlərində yerləşən şəbəkə komponentləri arasında mübadilə həyata keçirilir.

Şəbəkədə düyünlərin qarşılıqlı əlaqəsini təmin edən ierarxik təşkil olunmuş protokollar toplusu *kommunikasiya protokolları yığımı (steki)* adlanır. Texniki ədəbiyyatlarda ISO/OSI modelinin ISO/OSI protokollar yığımından dəqiq fərqlənməsi göstərilir. ISO/OSI modeli açıq sistemlərin konseptual sxemidir, ISO/OSI protokollar yığımı isə ISO/OSI modeli ilə müəyyən edilən, yeddi səviyyənin qarşılıqlı əlaqəsində iştirak edən protokolların konkret təsnif olunmasının yerinə yetirilməsidir.

Kommunikasiya protokolları həm proqram, həm də aparat baxımından tətbiq edilə bilərlər. Aşağı səviyyə protokolları adətən proqram və aparat vasitələrinin kombinasiyası kimi, yuxarı səviyyə protokolları isə proqram vasitələri kimi tətbiq edilir.

Şəbəkənin bir düyünündə yerləşən qonşu səviyyələrin icra olunan protokollar modulu, dəqiq qanunlara əsaslanmaqla məlumatların standart formatlanmasının köməyilə bir-biri ilə qarşılıqlı əlaqədə olmalıdırlar. Bu qaydaları (qanunları) *səviyyələrarası interfeys* adlandırırlar. Səviyyələrarası interfeys cari səviyyə ilə qonşu səviyyənin servislər toplumunu müəyyən edir.

Ümumiyyətlə, protokol və interfeys yaxın anlamlar sayılır, amma ənənəvi baxımdan isə şəbəkədə onlara fəaliyyətin müxtəlif sahələri aid olunur. Protokollar müxtəlif şəbəkələrdə qarşılıqlı əlaqənin eyni səviyyədəki modulunu, interfeys isə bir düyündə qonşu səviyyələrdə qarşılıqlı əlaqə qanunlarını müəyyənləşdirir.

TCP/IP (Transmission Control Protocol/İnternet Protocol) protokollar yığımı (steki) qlobal şəbəkə üçün yaradılmış

kommunikasiya protokolları yığımının standartıdır. TCP/IP standartı Request for Comment (RFC) adlanan nəşr olunmuş sənədlər seriyasidir. RFC sənədləri İnternet şəbəkəsinin daxili işini təsvir edir. Bəzi RFC-lər şəbəkə servislərini və ya protokollarını (onlardan istifadə olunmanı ümumiləşdirməklə) onların realizə edilməsini təsvir edirlər.

TCP/IP steki bir-biri ilə qarşılıqlı mübadilədə olan protokol toplumunu birləşdirir. Toplumdan ən vacib olan protokol IP protokoludur. Protokol İnternetdə çoxlu sayda aralıq şəbəkələrdə, şlüzlərdə və marşrutlaşdırıcılarda, marşruta uyğun verilənlər blokunun bir kompüterdən digər kompüterə ötürülməsində istifadə edilən marşrutların (və ya marşrutun) axtarılmasına məsuliyyət daşıyır. Bunlarla yanaşı TCP protokolu məlumatların etibarlı, səhvsiz və müəyyən qanunla ötürülməsini də təmin edir.

TCP/IP yığımının inkişafına ABŞ-da, Berkli ştatındakı Kaliforniya universitetinin böyük köməkliyi olmuşdur. Universitet protokolların yeni pulsuz və hamı tərəfindən əlçatan versiyasını (onlara məxsus olan versiyasını) istifadəyə buraxır. İstehsal olunan əməliyyat sisteminin populyarlığı IP, TCP və digər protokollar yığımının da populyar olmasına gətirib çıxardı. İndiki zamanda protokollar yığımı İnternet şəbəkəsində istifadə olunan kompüterlər arasında rabitə əlaqəsinin yaradılmasına yardımçıdır. Bununla yanaşı protokollar yığımından korporativ steklərdə də istifadə edilir. Kompüter şəbəkələrinin yaradılmasında TCP/IP protokollar steki ən çox yayılmış protokolar ailəsi hesab olunur.

TCP/IP stekinin geniş yayılması aşağıda səbəblərlə izah olunur:

- Daha tamamlanmış standartdır və çoxillik tarixçəsi olan şəbəkə protokollarının populyar stekidir;

- Əksər böyük şəbəkələr onlara məxsus olan trafiklərin əsas hissələrini TCP/IP protokolu vasitəsilə ötürürlər;
- Bütün müasir əməliyyat sistemləri TCP/IP stekini dəstəkləyir.

Bunlarla yanaşı TCP/IP:

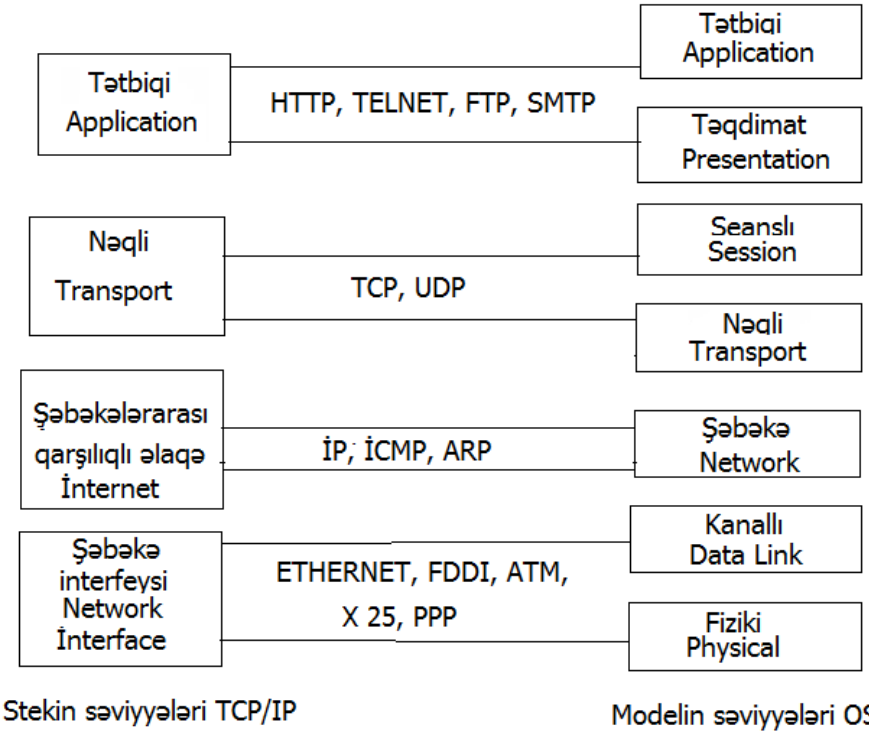
- İnternet şəbəkəsinə daxil olmağa imkan verən üsuldur;
- Həm nəqli altsistemi səviyyəsində, həm də ki, tətbiqi servislər səviyyəsində müxtəlif xüsusiyyətli sistemlərin birləşməsinə imkan verən çevik texnologiyadır;
- İntranetin (korporativ şəbəkə, WWW texnologiyası, İnternetin nəql olunma texnologiyası) yaradılması üçün əsasdır;
- Müştəri-server əlavəsi üçün platformalar arası miqyaslaşdırılmış dayanıqlı mühitdir.

TCP/IP PROTOKOLLAR YİĞİMİNİN STRUKTURU VƏ FUNKSİYALARI

Çoxsəviyyəli struktura malik olan TCP/IP yığımı açıq sistemlərin qarşılıqlı əlaqə modeli OSI –nin meydana gəlməsindən əvvəl yaradılmışdır. TCP/IP protokollar yığımının strukturu 14 saylı şəkildə verilmişdir. TCP/IP protokollar yığımı dörd səviyyədən ibarətdir: Tətbiqi (Application), nəqli (Transport), qarşılıqlı şəbəkəarası səviyyə (İnternet) və şəbəkə interfeysləri səviyyəsi (Network). Müqayisə üçün 14 saylı şəkildə OSI modelinin yeddi səviyyəsi də verilmişdir. Nəzərə almaq lazımdır ki, TCP/IP yığımının səviyyəsi ilə OSI modeli səviyyəsi arasındakı uyğunluq şərtidir.

Tətbiqi səviyyəyə (Application) çoxlu sayda protokollar və servislər daxildir. Bunlara populyar olan FTP fayllarının

surətinin alınması protokolu, Telnet terminalının emulyasiya protokolu, İnternet şəbəkəsində istifadə edilən elektron poçt SMPT poçt protokolu, uzaqlaşdırılmış informasiyaya daxil olmağa imkan verən hipermətn servisi, WWW başqaları daxildir.



Şəkil 14. TCP/IP protokollar yığımının səviyyələri

Adları çəkilən protokollardan bəzilərini qeyd edək.

FTP faylların göndərilmə protokolu (File Transfer Protocol) fayla uzaqdan əlçatanlığı yerinə yetirir. Etibarlı ötürməni təmin etmək üçün FTP protokolu birləşmənin quraşdırılması üçün

əlverişli olan TCP nəql protokolundan istifadə edir. Faylların göndərilməsi üşün FTP protokolu istifadəçiyə digər xidməti də təqdim edir. Məsələn, istifadəçiyə uzada yerləşmiş maşınla interaktiv işləmə imkanı yaradılır. Bununla yanaşı istifadəçi hesablama maşınının kataloqunda olanları çapa da göndərə bilər. Bu sadalananlarla yanaşı FTP protokolu istifadəçinin autentifikasiyanı da həyata keçirir. Öncədən fayla əlçatanlıq əldə etmək üçün protokola uyğun olaraq istifadəçi ona məxsus parolu və öz adını xəbər verməlidir. FTP-arxivinin ictimai kataloqlarından istifadə etmək üçün İnternet autentifikasiya parolunu tələb etmir, onu öncədən müəyyən edilmiş *Anonymous* istifadəçi adindan istifadə etmək kifayətidr.

Telnet protokolu proseslərarası baytlar axınının ötürülməsini, həmçinin proseslərarası və terminallararası ötürməni təmin edir. Bəzi hallarda protokoldan uzaqda yerləşdirilmiş kompüter terminalının emulyasiyası üçün də istifadə edirlər. Telnet servisindən bəhrələnən istifadəçi faktiki olaraq uzaqda yerləşmiş kompüterləri lokal şəbəkə istifadəçiləri kimi idarə edə bilir. Bu əməliyyatı lazımı səviyyədə həyata keçirmək üçün yaxşı müdafiənin olması vacibdir.

Telnet serverləri iş zamanı istifadəçidən minimum parola uyğun autentifikasiyanı tələb edir, bəzi hallarda isə müdafiə vasitəsi kimi Kerberos sistemindən bəhrələnir.

SNMP (Simple Network Management Protocol) protokolu şəbəkənin idarə edilməsində istifadə olunur. Öncə protokol uzaqlaşdırılmış nəzarət və İnternet marşrutlaşdırıcılarını idarə etmək üçün hazırlanmışdı. Protokolun populyarlığı artdıqca ondan müxtəlif kommunikasiya avadanlıqlarının (konsentratorlar, körpülər, şəbəkə adapterləri və başqaları) idarə edilməsi üçün istifadə olunmağa başlanıldı. SNMP standartında şəbəkə tərəfindən idarə edilə bilən informasiya

verilənləri bazasının təsnifatı müəyyən olunmuşdur. MIB (Management İnformation Base) təsnifatı verilənlər bazası kimi məşhurdur. MIB o verilənlərin elementlərini müəyyən edir ki, onları idarə edici qurğular yaddaşlarında saxlayırlar və onlar üzərində əməliyyatların aparılması istifadəçi üçün əlçatandır.

Nəql səviyyəsində (Transport) TCP/IP stekində (həm də əsas səviyyə adlanır) TCP protokolu və UDP protokolu fəaliyyət göstərir.

Ötürməni idarə edən TCP protokolu (Transport Control Protocol) sonuncu iki düyün arasında etbarlı informasiya mübadiləsi məsələsini həll edir. Protokolu bir çox hallarda "quraşdırılmış birləşmə" protokolu da adlandırırlar. Belə adlandırılmaya əsas səbəb odur ki, protokolun köməyilə əlaqə yaradan iki düyün bir-birinin arasında "müqavilə bağlayırlar" ki, verilənlər axınını öz aralarında dəyişəcək və dəyişdikləri verilənlər axınlarını idarə edəcəklər. TCP protokoluna uyğun olaraq göndərilən verilənlər çox da böyük olmayan paketlərə uyğun "kəsilir", sonra hər bir paket elə bir şəkildə markalanır ki, həmin paketlər istifadəçinin kompüterinə daxil olduqda (markalanmaya uyğun) istifadəçi tərəfindən lazımi səviyyədə istifadə oluna bilsin.

UDP istifadəçisinin deytaqram protokolu (User Datagram Protocol) tətbiqi paketlərin deytaqram üsulu ilə ötürülməsini təmin edir, yəni düyündən düyünə ötürülən informasiya bloku (paketi) təhlil edilir və asılı olmayan informasiya vahidi (deytaqram) kimi yayılır. Bu zaman UDP protokolu şəbəkə protokolu və çoxsaylı tətbiqi proseslər arasında birləşdirici həlqə funksiyasını yerinə yetirir. UDP protokolunun üstün cəhətlərindən əsası onun əlavələri ayırma "bacarığı"nın olması və informasiyanı əlavədən əlavəyə çatdırma imkanının olmasıdır.

Şəbəkəarası qarşılıqlı əlaqə səviyyəsi (İnternet) birləşməni qurmadan paketlərin komutasiya konsepsiyasını həyat keçirir. Bu səviyyənin əsas protokolu IP ünvan protokolu hesab olunur. Protokol əvvəlcə həm lokal, həm də ki, qlobal birləşdirilmiş çoxlu sayda lokal şəbəkələrdən ibarət olan şəbəkənin tərkibində paketlərin ötürülməsi üçün layihə edilmişdi.

IP protokolunun məqsədi ondan ibarətdir ki, İnternet şəbəkəsinin hər bir istifadəçisi özünəməxsus unikal ünvana (IP ünvan) malik olsun. Bunsuz TCP - paketlərinin dəqiq işçi yerinə çatdırılması barədə söz söyləmək olmaz. Ünvan çox sadə şəkildə (dörd bayt ilə) göstərilir: məsələn, 185.47.39.14.

IP ünvanın strukturu elə şəkildə qurulmuşdur ki, hər hansı TCP-paketi keçən hər bir kompüter göstərilən dörd rəqəm ilə paketin hansı yaxın "qonşu"ya göndərilməsini müəyyən edir, yəni paket göndərilən ünvanın informasiya alıcısına ən "yaxın" olmasını müəyyənləşdirir. Nəticədə TCP-paketlərinin müəyyən sayda ünvanlara göndərilməsi yerinə yetirilir.

Nəzərə almaq lazımdır ki, "yaxınlıq" dedikdə coğrafi yaxınlıq nəzərdə tutulmur. Burada rabitə kanalının buraxma qabiliyyəti və əlaqə şərtləri hesaba alınır. Məsələn, müxtəlif qitədə yerləşən iki fərdi kompüter bir-biri ilə peyk əlaqəsi yaratdığına görə onları bir-birinə yaxın birləşmiş sayırlar, nəin ki, telefon xəttilə bir-biri ilə əlaqə saxlayan, iki qonşu şəhərdə yerləşən kompüterlər.

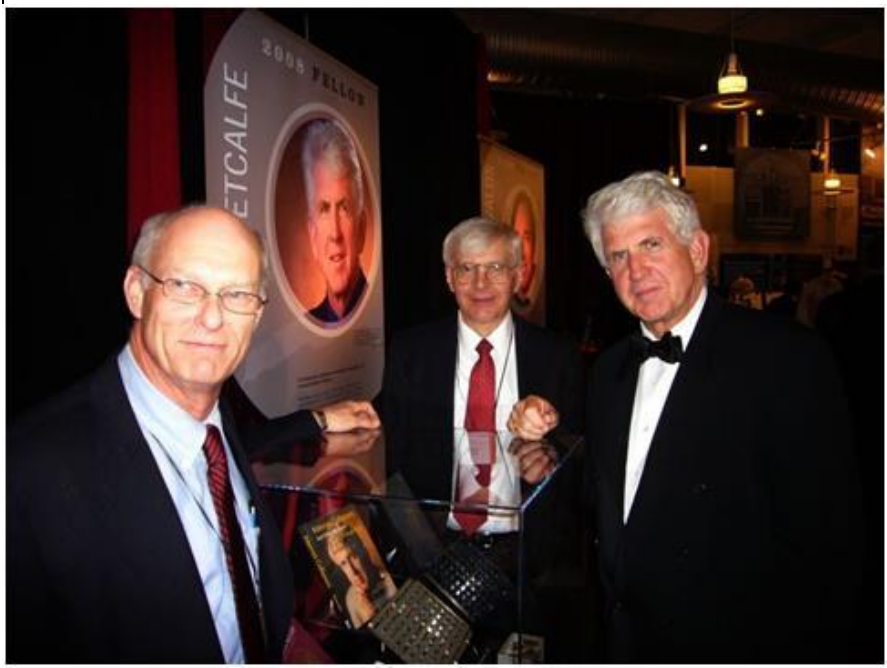
Qeyd etmək lazımdır ki, hansı kompüterlər bir-birinə "yaxın"dır, hansılar uzaq məsafədə yerləşirlər, bu sualların hamısı marşrutlaşdırıcılar vasitəsilə həll olunur. Marşrutlaşdırıcı rolunu şəbəkənin düyün serverində qoşulmuş xüsusi kompüter, ya da ki, xüsusi hazırlanmış proqram oynaya bilər.

Şəbəkə interfeysi səviyyəsi (Network) OSI modelinin fiziki və kanal səviyyəsinə uyğundur. TCP/IP protokollarında bu səviyyə nəzərə alınmır, amma səviyyənin bütün populyar fiziki və kanal standartlarını dəstəkləyir: lokal şəbəkələr üçün - ***Ethernet***, ***Token Ring***, ***FDDI***, ***Fast Ethernet***; qlobal şəbəkələr üçün – ***PPP*** və ***SLIP*** "nöqtə-nöqtə" birləşmə protokolu, X.25 kommutasiya paketləri protokolu olan sahə şəbəkəsi, frame relay. Kanal səviyyəsində nəql üçün ***ATM*** texnologiyasını müəyyən edən təsnifat işlənib hazırlanmışdır.

AÇIQLAMA: *Ethernet texnologiyası* şəbəkə düyünlərinin ümumi şinə paralel qoşulması şəraitində işləyir. Marker azad olan kimi şəbəkənin növbəti ötürməyə hazır olduğunu xəbər verir. Rəsmi olaraq *Ethernet şəbəkəsinin* yaranma tarixi 22 may 1973-cü il hesab edilir. Palo-Alto şəhərində yerləşən Xerox firmasının Elmi-tədqiqat mərkəzinin əməkdaşları B.Metkalf və D.Boqqs sayılan jurnalların birində eksperimental şəbəkə haqqında məqalə çap etdirirlər və həmin şəbəkənin Enhernet adlandırıldığı barədə oxuculara məlumat verirlər.

Ethernet (ether – efir, network – şəbəkə, dövrə sözbirləşməsindən yaranmadır). Kompüter şəbəkələrində verilənlərin paket formasında ötürülməsi texnologiyasıdır. Şəbəkə koaksial kabellə qurulmuşdu və verilənlərin kabel vasitəsi ilə ötürülməsi 2,94 Mbit/saniyə təşkil edirdi. 1979-cu ildə Digital, Intel və Xerox şirkətləri lokal şəbəkə vasitəsi ilə informasiyanın 10 Meqabit/saniyə ötürülməsinə imkan verəcək texnologiyanın hazırlanması üçün DIX konsersiumunu yaradırlar. 1980-cı ildə Ethernet layihəsi üzərində tədqiqatları həyata keçirmək üçün elmi işçilərdən qrup yaradılır. Həmin qrup 1983-cü ildə Ethernet 802.3 və

Ethernet 10Base5 standartlarını təsdiq edir. İnformasiyanın etibarlı (səmərəli, əlverişli) şəkildə ötürülməsi üçün koaksial kabeldən, şəbəkənin düyünlərində isə transiverlərdən istifadə olunması nəzərdə tutulur. Ethernetin yaradılmasında növbəti addım 1990-cı ildə 10Base-T standartının yaradılması olur. Standartda informasiyanın ötürülmə mühiti kimi bir cüt ekranlaşmamış kabelin burulmasından (Unshielded Twisted Pair – UTP) istifadə olunurdu. Standartın arxitekturası "ulduz" topologiyasina əsaslanırdı. Topologiyada hər bir işçi stansiya toplanmış (konsentrasiyalı) məzkəz ilə əlaqə saxlayırdı.



Devid Boqqs, Ron Kreyn və Bob Metkalf

Tokren Ring texnologiyası əvvəlcə IBM kompaniyası tərəfindən 1970-ci ildə işlənib hazırlanmışdır. 1985-ci ildə IEEE 802 komitəsi bu texnologiya əsasında IEEE 802.5 standartını qəbul edir. Araşdırmalar göstərir ki, son vaxtlar IBM şirkətinin məhsulları Ethernet ailəsini texnologiyasına aid olan məhsullar üzərində hakim vəziyyət tutmuşdur (buna texniki dildə dominasiya deyirlər). Nəzərə almaq lazımdır ki, IBM şirkəti uzun müddət ərzində lokal şəbəkələrin qurulmasında Token Ring texnologiyasından bəhrələnmişdir.

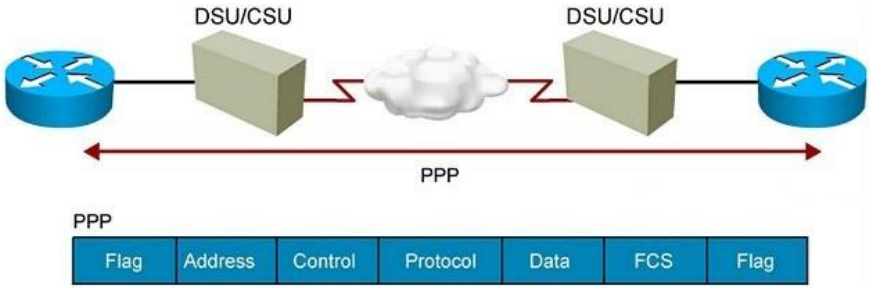
FDDI (ingiliscə Fiber Distributed Data Interface – Verilənlərin ötürülməsi üçün yararlı olan lifli-optik inyterfeys) – 200 kilometr məsafədə verilənlərin standart ötürülməsi üçün istifadə olunan lokal şəbəkədir. Standart Token Ring protokoluna əsaslanır. FDDI verilənlərin ötürülməsində böyük əraziyə malik olmaqla yanaşı bir neçə minlərlə istifadəçini də dəstəkləməyə qadirdir. Standart keçən əsrin 80-cı illərində Amerikanın Milli Standartlar İnstitutu (ANSI) tərəfindən yaradılmışdır. Nəzərə almaq lazımdır ki, FDDI –nin indiki zamanda geniş yayılması nəticəsində (Ethernet və ya TokenRing ilə müqayisə etdikdə) özünə müəyyən sayda ardıcıllar toplaya bilmişdir, bu səbəbdən də FDDI interfeysə çəkilən xərclərin azalmasına nail olmuşdur. FDDI əksər hallarda lokal şəbəkəyə daxil olan sürətli kompüterlərin bir-birilə birləşməsi vasitəsi kimi istifadə edilir.

Fast Ethernet (FE) – Ethernet texnologiyasına əsaslanaraq kompüter şəbəkələrində verilənlər toplumunun standart ötürülməsinə verilən addır. Burada verilənlər 100 Mbit/saniyə sürətlə ötürülür. Bəzi hallarda texnologiyanı 100BASE-X kimi işarə edirlər (X – realizə variantını göstərir, məsələn, 100BASE-TX, 100BASE-FX və s.). 1992-ci ildə bəzi

istehsalçılar (məsələn, 3COM, SynOptics və başqaları) yeni spesifikasiya yaratmaq üçün Fast Ethernet Alliance birliyi yaradırlar. Birlik 1992-1993-cü illərdə IEEE institutu ilə birləşərək yeni spesifikasiyanın hazırlanmasına başlayır və bu məqsədlə Hewlett-Packard AT&T şirkətlərini müştərək işləməyə dəfət edir. Çəkilən birgə zəhmətin nəticəsində 26 oktyabr 1995-ci ildə IEEE 802.3u standartı qəbul edilir.

PPP (ingiliscə Point-to-Point Protokol) – OSI şəbəkə modelini dəstəkləyən kanal səviyyəsində ikinöqtəli protokolu (Data Link) adətən şəbəkənin iki düyünü arasında birbaşa əlaqənin yaradılması üçün istifadə edilir. Protokol birləşmənin autentifikasiyasını, şifrələnməsini və verilənlərin sıxılmasını təmin edir. Çoxlu sayda fiziki şəbəkələrdə: sıfır-modem kabellərində, telefon xətlərində, mobil (cellular-sotovıy) rabitə xətlərində və buna bənzərlərdə istifadə olunur. PPP protokolunun müxtəlif növləri (məsələn, PPPoE, PPPoA və s.) müxtəlif rabitə kanallarında istifadə edilir.

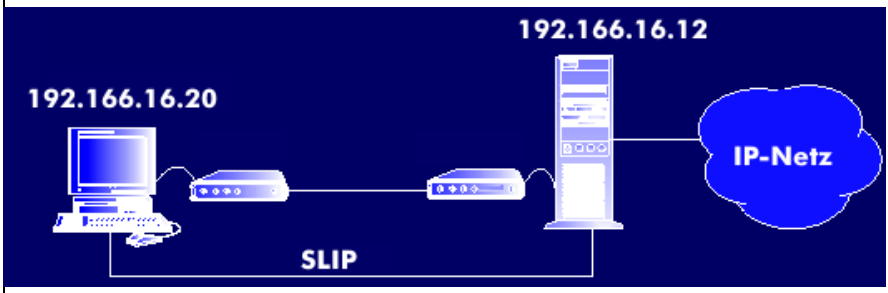
PPP özündə çoxlu sayda protokollar ailəsini birləşdirir: rabitə xəttini idarə edən protokol (LCP), şəbəkəni idarə edən protokol (NCP), autentifikasiya protokolu (PAP, CHAP), MLPPP çoxkanallı protokolu.



PPP protokolu

SLIP (Serial Line İnternet Protocol) – OSI etalon şəbəkə modelinin kanal səviyyəsində mənəvi qocalmış şəbəkə protokoludur. Protokoldan TCP/IP steki şəbəkələrinə əlçatanlıq üçün istifadə edirlər. Protokol kommutasiya olunan

birləşmələrdə ardıcıl portların köməyilə müştəri-server birləşməsini "nöqtə-nöqtə" növündən istifadə etməklə həyata keçirir. SLIP keçən əsrin 80-cı illərində 3COM şirkəti tərəfindən yaradılmışdır. 1984-cü ildən başlayaraq Rik Adamsın (Rick Adams) təşəbbüsü və iştirakı ilə geniş yayılmışdır. R.Adamsın zəhməti nəticəsində protokol İnternetə qoşulmada istifadə edilmişdir (ardıcıl COM portlarından istifadə etməklə). Sadə olduğu üçün indiki zamanda mikrokontrollerdə istifadə olunur.



SLIP protokolu

ATM (ingiliscə asynchronous transfer mode – verilənlərin asinxron ötürülməsi üsulu) – paketlərin multipleksiya edilməsi və kommutasiya oluması üçün istifadə olunan yüksək məhsuldarlığa malik şəbəkə texnologiyasıdır.

ATM texnologiyasının əsası bir-birindən asılı olmayan iki alim tərəfindən: Fransada Franca Telecom şirkətinin əməkdaşı Jan-Piyerre Koudruse, Amerika da isə Bell Labs laboratoriyasının əməkdaşı Sandi Fraser tərəfindən yaradılmışdır. Hər iki alim elə bir arxitektura yaratmaq istəyirdilər ki, ondan istifadə etməklə verilənlərin nəql olunması şəbəkədə yüksək sürətlə (səs sürətinə yaxın) effektif ötürülsün.

Jan-Piyerre Koudruse

Sandi Fraser

1988-ci ildə Jeneva şəhərində ITU –nun (Telefon və teleqraf sahəsində Beynəlxalq Məsləhət Komitəsi) toplantısında ATM yuvalarının uzunluğu 53 bayt seçilir (Amerika mütəxəssiləri 64, Avropa mütəxəssisləri isə 32 bayt təklif edirdilər). 1990-cı ildə ATM-in bünövrə təqdimatları qəbul olunur. Qəbul edilmiş qərar vaxtı ilə Jan-Piyerre

Koudruse və Sandi Fraser tərəfindən təklif edilmiş qərarları yamsılayırdı, daha doğrusu onlara çox oxşayırdı. 1990-cı ildən başlayaraq ATM texnologiyası daha da inkişaf etməyə başlayır.

TCP/IP protokollarından istifadə etməklə verilənlər kanal vasitəsilə açıq şəkildə ötürülür, odur ki, təhlükəsizlik (informasiyanın ümumiyyətlə İnternetdə ötürülməsi nəzərdə tutulur) baxımından istifadəçi nəzərə almalıdır ki, əgər lazım olan tədbirlər həyata keçirilməzsə, məlumatlar göndərilən nöqtədən verilənlərin ötürülmə yollarında yerləşən istənilən məlumatı qəbul edən düyün nöqtəyə kimi bədniyyətli insanlar bu məlumatların surətini alaraq öz məqsədləri üçün istədikləri kimi istifadə edə bilərlər. Nəticədə verilənlər ya təhrif olunar, ya da ki, məhv edilər.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNƏ EDİLƏN HƏDƏLƏRİN TƏHLİLİ

Eynicinsli olmayan şəbəkə mühitində kommunikasiyanın təşkil edilməsi üçün TCP/IP protokollar yığımından istifadə edilir. Protokollar yığımı müxtəlif növ kompüterlər arsında uyğunluğu həyata keçirir. Uyğunluq TCP/IP protokollar yığımının əsas üstünlüyüdür, odur ki, əksər kompüter şəbəkələri bu protokolları dəstəkləyirlər. Digər tərəfdən protokollar yığımı istifadəşiyə İnternetin resurslarından bəhrələnməyə imkan yaradır.

TCP/IP öz populyarlığına görə şəbəkələrarası əlaqədə de-fakto standartı hesab oluna bilər. Bununla yanaşı TCP/IP protokollar yığımının geniş yayılması onun bəzi zəif cəhətlərinin də üzə çıxmasına səbəb oldu. TCP/IP –nin yaradıcıları onun

müdafiə edilməsinə səbəb görmədilər. Odur ki, TCP/IP –nin əvvəlki verisyalarında təhlükəsizlik məsələlərinin həll olunmasına tələb olmadığı üçün onun realizə edilməsi zamanı müəyyən bağlılıq ortaya çıxdı.

IP ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİLİK PROBLEMİ

İnternet-texnologiyalarının populyarlığı şəxsi məlumatların, dövlət sirrlərinin, korporativ resursların və s. agah edilməsinə gətirib çıxardı. Xakerlər və digər pisniyyətli şəxslər şəbəkədə olan informasiya resurslarına müdaxilə etməklə onları daim qorxu altında saxlayırlar. Belə hücumlar günü-gündən artmaqla yanaşı həyata keçirilmə imkanlarına görə də o qədər də mürəkkəb olmur, rahat tətbiq edilir. Buna iki səbəb imkan yaradır.

Birincisi, İnternetə daxil olanların sayının günü-gündən artması, milyonlarla kompüterlərin şəbəkəyə qoşulması, informasiya mübadiləsinin fasiləsiz olaraq yerinə yetirilməsi və s. bu kimi faktorlar xakerlərə imkan verir ki, qlobal miqyasda öz əməllərini həyata keçirsinlər, onları maraqlandıran sualları araşdırmaqla informasiya mübadiləsində iştirak etsinlər.

İkincisi, istifadəçilərin yaradıcılıq işlərində geniş istifadə olunan əməliyyat sistemlərinin sadəliyi və geniş yayılmasıdır. Bu faktor pisniyyətli insanın (xakerin) lazımi səviyyədə bilik sahibi olmasını tələb etmir, çünki əvvəllər xakerdən proqramlaşdırmanı və əməliyyat sistemlərini tutarlı səviyyədə bilmək tələb olunurdusa, indiki zamanda ona ancaq lazım olan saytın IP-ünvanını bilmək kifayət edir. Sadəcə olaraq mausun sol düyməsini sıxmaq və ziyanverici əməlləri hayata keçirmək – xakerin arzusunun həyata keçməsinə kifayətdir.

İNFORMASİYA TƏHLÜKƏSİZLİYİ

Korporativ kompüter şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsi problemi lokal işçi stansiyalarina, lokal şəbəkələrə, korporativ şəbəkələrə edilən hücumlarla bağlıdır, çünki adları çəkilən şəbəkələrdən istifadəçilərin istifadə etdiyi ümumi şəbəkələrə çıxışlar vardır.

Şəbəkə hücumları çox müxtəlif xarakterlidir. Bəzən sistemə edilən hücum mürəkkəb olur, bəzən hücum operator tərəfindən yerinə yetirilir, bəzən də hücumun hansı mənbəədən edildiyi məlum olmur və s. Bu baxımdan hücum edənin məqsədi aşağıdakı kimi təsnifləndirilir:

- Ötürülən informasiyanın konfidensiallığının pozulması;
- Ötürülən informasiyanın tamlığının və etibarlılığının pozulması;
- Bütün sistemin və ya sistemin ayrı-ayrı hissələrinin işləmə qabiliyyətinin pozulması.

Paylanmış sistemlər ən əvvəl uzaqdan edilən hücumlara məruz qalır, çünki paylanmış sistemlərin təşkiledičiləri verilənlərin ötürülməsi üçün açıq kanallardan istifadə edir. Pisniyyətli şəxs ötürülən informasiyaya passiv təsir göstərsədə, bir çox hallarda informasiya ötürən trafiki modifikasiya etməklə kanala və informasiyaya aktiv maneçilik də edir. Trafikə olunan aktiv təsir qeyd olunan olsada, passiv təsir praktiki olaraq müşahidəyə tabe olmur. Açıq kanaldan ötürülən informasiya, həmçinin istifadəçinin istifadə etdiyi informasiya, əsasəndə xidməti informasiya daim hücum obyektinə çevrilir.

Edilən hücumların araşdırılması və müəyyən edilməsi ağlagəlməz nəticələr törətdiyi üçün birinci yerdə onların təyin edilməsi və onlara qarşı mübarizənin aparılması durur.

Lokal şəbəkənin təhlükəsizliyi şəbəkələrarası təhlükəsizlikdən fərqlənir. Bu baxımdan əhəmiyyətinə görə birinci yerdə *qeyd edilmiş istifadəçilərin pozuntuları* durur,

çünki lokal şəbəkədə verilənlərin ötürülmə kanalları nəzarətdə olan sahələrdə yerləşir və sanksiyalanmamış (icazəsiz) qoşulmalardan kanardırlar.

Təcrübədə IP-şəbəkələri verilənlərin kanallar vasitəsilə mübadiləsi zamanı icazəsiz hücumlarla müxtəlif növ üsullarla bağlılığı mövcuddur. Kompüter və şəbəkə texnologiyalarının inkişafı (məsələn Java-əlavələrinin yaranması, AcyiveX elementlərindən istifadə və s.) nətəcəsində IP-şəbəkəsinə olunan hücumların növü daim çoxalmaqdadır.

Ən çox aşağıdakı hücumlar geniş yayılmışdır:

Qulaqasma (sniffing). Əsasən kompüter şəbəkələrində verilənlər müdafiə edilməmiş formatda ötürülür (məsələn, açıq mətn şəkilində), bu da bədniyyətli insana verilənlərin ötürüldüyü xəttə daxil olaraq trafikə qulaq asmağa və yaxud da verilənləri yoxlamağa imkan verir. Kompüter şəbəkələrində informasiyaya qulaq asmaq üçün *snifferdən* istifadə edilir. *Sniffer paketləri* dedikdə müəyyən domen ilə ötürülən, bütün şəbəkə paketlərini özündə cəmləşdirən tətbiqi proqramlar nəzərdə tutulur.

AÇIQLAMA: *Sniffer* – NIC (Şəbəkə İnterfeys Xəritəsi) rəhbərliyi ilə qurulan proqramdır. Bəzən snifferi Ethetnet xəritə də (kompüterlərin lokal şəbəkəyə fiziki qoşulması üçün lazım olan aparat vasitələrinin lazımlı hissələrindən biri) adlandırırlar. Məlumdur ki, informasiya şəbəkədə paketlərlərlə ötürülür, sniffer aralıq kompüterə qurulur və ötürülən paketlər ondan keçir. Sniffer son məqsədə çatmayan paketləri tutub saxlamaq imkanına malikdir. Sniffer şəbəkə analizatoru kimi məşhurdur. Onlar arasında real fərq yoxdur, amma Təhlükəsizlik və Federal Dövlət şirkəti ikincə addan istifadəyə üstünlük verir, çünki ikinci ad

daha qorxulu, zəhmli səslənir.

İndiki zamanda snifferlər şəbəkədə qanuna əsaslanaraq işləyirlər. Onlardan nasazlıqların diaqnostikasında və trafiklərin təhlil olunmasında istifadə edilir. Digər tərəfdən bəzi şəbəkə əlavələri verilənləri mətn formatında ötürdükləri üçün (məsələn, Telnet, SMTP, POP3 və i.a.) snifferdən bəhrələnən istifadəçi ancaq faydalı informasiya haqqında məlumat əldə edə bilir, bəzi hallarda isə, hətta konfidensial (məxfi) informasiya barədə də lazımı məlumatları ala bilir (məsələn, istifadəçinin adını, parolunu).

Şifrələnməmiş formada parolun kanal vasitəsilə ötürülən zaman "tutulması" kanala "qulaqasma" yolu ilə baş verir və qulaqasmanın növlərindən biri hesab olunur. Ədəbiyyatlarda bu prosesi *password sniffing* adlandırırlar. Parolun və adın tutulması hər zaman eyni loqindən istifadə edən istifadəçi üçün çox təhlükəlidir. Bir çox istifadəçilər isə bütün resurslara daxil olmaq üçün bir paroldan və əlavədən istifadə edirlər. Əgər əlavə müştəri/server rejimində işləyirsə və autentifikasiyalı sənədlər şəbəkə ilə mətn formasinda göndərilirsə, böyük ehtimalla digər korporativ və ya xarici resurslardan istifadə etmək olar.

Sniffinq paketlərindən gələn təhlükəni (hücumu) birdəfəlik audentifikasiya parolundan istifadə etməklə, aparat və ya proqram təminatının həyata keçirilməsi yolu ilə, həmçinin snifferi müəyyən edən kriptoqrafik müdafiə üsullarından istifadə etməklə aradan qaldırmaq olar.

Verilənlərin dəyişdirilməsi. Sizin məlumatları oxumaq imkanı əldə edən bədniyyətli insan, belə bir addım ata bilər – verilənləri dəyişmək. Ümumiyyətlə, paketə daxil olan verilənlər istənilən halda, yəni pisniyyətli insanın verilənləri göndərən

istifadəçi, hətta məlumatı qəbul edən istifadəçi barədə məlumatı olmadıqda belə dəyişmək imkanı vardır. Digər tərəfdən Sizin verilənlərin ciddi məxfi saxlanmasına ehtiyac duyulmasa da belə, bütün hallarda Siz verilənlərin ötürülmə kanallarında dəyişikliyə məruz qalmasını istəməzsiniz.

Şəbəkə trafikinin təhlili. Hücum əsasən rabitə kanallarına qulaqasmaq məqsədi güdür. Bununla yanaşı hücum zamanı ötürülən verilənlərin və xidməti informasiyanın təhlili, onların arxitekturasının və topologiyasının öyrənilməsi, quruluşunun araşdırılması, istifadəçiyə aid olan informasiyaların əldə edilməsi (məsələn, istifadəçi parolu, kredit kartın nömrəsi və i.a.) və s. proseslər qulaqasmaya məruz qalır. Belə hücumlara FTP və ya Telnet protokolları da meyllidir. Bunların xüsusiyyəti ondan ibarətdir ki, istifadəçinin adı və parolu açıq şəkildə, protokol çərçivəsində ötürülür.

İnanılmış subyektin əvəz edilməsi. Kompüterin IP-ünvanı şəbəkənin əsas hissəsini və əməliyyat sistemini istifadə edir, bununla da ünvançının həmin şəxs olduğu (lazım olan şəxs) müəyyən olunur. Bəzi hallada IP-ünvanı ötürücünün digər ünvanı iilə əvəz olunur. Ünvana olunan bu növ hücum *ünvanın falsifikasiya olunması* adlanır (*IP-spoofing*).

IP-spufinq bəzi hallarda özünü elə göstərir ki, bundan istifadə edən pisniyyətli insan istər şirkət daxilində olsun, istərsə də şirkətdən kanarda, güya o, qanuni istifadəçidir. Pisniyyətli insan bundan istifadə etməklə IP-ünvandan bəhrələnir. Pisniyyətli insan xüsusi proqramlardan da istifadə edə bilər. Bu proqramlar IP-paketlərini elə şəkildə formalaşdırır ki, onlar korporativ şəbəkənin daxili ünvanları kimi özlərini biruzə verirlər.

IP-spufinq hücumu bəzi hallarda digər hücumlar üçün dayaq nöqtəsinə çevrilir. Buna klassik nümunə kimi "xidmətdən

imtina" hücumunu (DoS) göstərmək olar, hücum xakerin şəxsiyyətini gizlətməklə başqasının ünvanından başlayır.

Spufinqin təhlükəsini (hədəsini) onu ləğv etmədən azaltmaq mümkündür, bunun üçün xarici şəbəkəyə əlçatanlığı düzgün sazlamaqla yanaşı spufinqin digər şəbəkədən istifadəçi şəbəkəsinə daxil olmasına maneçilik etmək kifayətdir. Digər yol istifadəçinin autentifikasiya üsulundan istifadə etməklə IP-spufinqinin qarşısının alınması, birdəfəlik parollardan və ya kriptoqrafiya metodlarından istifadə edilməsidir.

Vasitəçilik. Hücum aktiv qulaqasma ilə yanaşı ötürülən informasiyanın aralıq düyünlərdə tutulması və idarə edilməsi ilə bağlıdır. Kompüterlər aşağı şəbəkə səviyyələrində qarşılıqlı informasiya mübadiləsində olarkən çox vaxt hansı verilənlərin dəyişdirilməsinə ehtiyacın olduğunu müəyyən edə bilmirlər.

Şifrələnməmiş açarlardan istifadə etməklə vasitəçilik (*man-in-the-middie* hücumu – *insan-harada* hücumu). Hücumu təşkil edən bədniyyətli insana şəbəkə ilə ötürülən paketlərə əlçatanlıq olmalıdır. ISP provayderi vasitəsilə istənilən başqa şəbəkəyə ötürülən bütün paketlərə belə əlçatanlığı provayderin əməkdaşı əldə edə bilər. Bu tip hücumdan tez-tez paketlərin snufferləri, nəql protokolları və marşrutlaşdırıcıların protokolları istifadə edirlər.

man-in-the-middie hücumu informasiyanı oğurlamaq, cari sessiyanı "tutmaq" və şəxsi şəbəkə resurslarına daxil olmaq, trafiki təhlil etmək, şəbəkə haqqında və ondan istifadə edən istifadəçi haqqında informasiya almaq, DoS növlü hücumu həyata keçirmək, verilən məlumatların təhrif edilməsini həyata keçirmək və qeyriqanuni informasiyanı şəbəkəyə daxil etmək üçün istifadə olunur.

man-in-the-middie hücumuna qarşı effektiv mübarizə kriptoqrafiyadan istifadə etməkdir. Bu növ hücumlara qarşı

mübarizə aparmaq üçün *aşıq açarlarla idarə olunan infrastruktur* (*PKI – Public Key İnfrastructure*) üsulundan bəhrələnmək olar.

Seansın tutulması (session hijacking). Qanuni istifadəçi (məsələn, poçt serveri) tərəfindən başlanğıc prosedur bədniyyətli insan tərəfindən yeni hosta dəyişdirilir, başlanğıc serverə isə əlaqənin qırılması barədə əmr verilir. Nəticədə qanuni istifadəçinin "həmsöhbət"i hiss edilmədən dəyişdirilir.

Şəbəkəyə daxil olan pisniyyətli insan şəbəkəyə hücum etməklə aşağıdakılara nail olur:

- Korrektə edilməmiş (təshih edilməmiş) verilənləri şəbəkə xidmətindən istifadə edib göndərməklə şəbəkədə qəzalı vəziyyət yaratmaqla yanaşı şəbəkənin düzgün işləməməsinə nail olmaq;
- Bütün trafiki və ya kompüteri lazımsız informasiya ilə doldurmaq, yenidən yükləməni həyata keçirməklə sistemin dayanmasına nail olmaq;
- Trafiki bloklamaqla şəbəkə resurslarına istifadəçinin daxil olmasının qarşısını almaq.

Xidmət edilməsinə imtina (Denial of Service, DoS). Bu hücum digərlərindən fərqlənir: birincisi, hücum şəbəkəyə daxil olmağı, ikincisi, şəbəkədən hər-hansı məlumatı almağı qarşısına məqsəd qoymayıb. DoS hücumu şəbəkəni adi istifadəçi üçün əlçatmaz edir. Həqiqətdə isə istifadəçi şəbəkənin resurslarından istifadə etməklə yanaşı şəbəkəyə qoşulmuş kompüterlərdən bəhrələməkdən də məhrumdur.

Edilən əksər DoS hücumlar sistemin arxitekturasının zəifliyindən istifadə edir. Bəzi server əlavələrindən istifadə hallarında (məsələn, Veb-server və ya FTP-server) isə DoS hücumları adi istifadəçiləri şəbəkənin xidmətindən istifadə

etməkdən məhrum edir, şəbəkəni məşğul vəziyyətində saxlayır, və nəhayət şəbəkə düyünlərinin işləməsinə maneçilik edir.

DoS hücumları adətən İnternet protokollarından bəhrələnir (məsələn, ICMP (İnternet Control Message Protocol) və TCP protokolları).

DoS hücumlarının qarşısının alınması çox çətindir, çünki bunun üçün provayderin fəaliyyəti koordinasiya (uzlaşdırılma, əlaqələndirilmə) olunmalıdır.

Əgər bu növ hücum eyni vaxtda çoxlu sayda qurğulara edilirsə, onda edilən paylanmış hücum xidmətdən imtina (DDoS – distributed DoS) adlanır. DoS hücumunun realizə edilməsinin sadəliyi və onun vurduğu ziyan ona qarşı daha diqqətli olmağı tələb edir.

Parol hücumları. Hücumun məqsədi parola və istifadəçinin qanuni loginina sahib olmaqdır. Bədniyyətli insanlar belə hücumları yerinə yetirmək üçün aşağıdakı üsullardan istifadə edirlər:

- IP-ünvanın dəyişdirilməsi (IP-spufinq);
- Qulaqasma (snifinq);
- Sadə normadan artıq alınmış.

IP-spufinq və snifinq paketləri haqqında öndəki bölmələrdə qeyd olundu. Bu üsullar bədniyyətli insanlara parola və istifadəçi loginina malik olmağa imkan yaradır. Bu zaman əsas məsələ kanal vasitəsilə ötürülən informasiyanın açıq mətnlə ötürülməsi və ötürülən zaman müdafiə oluna bilməməsidir.

Xakerlər bir çox hallarda parolu və logini əldə etmək üçün dəfələrlə təşəbbüs göstərirlər. Həyata keçirilən bu üsul *tam artıqlaması ilə hücum* (*brute force attack*) adlanır. Hücumda ümumi istifadə resurslarına (məsələn, serverə) daxil olmaq üçün hazırlanmış xüsusi proqramdan istifadə edilir. Əgər

pisniyyətli insan parolu "sındıra" bilirsə, onda resurslara daxil olma imkanı əldə edir.

Parol hücumlarından müdafiə olunmaq asandır, bunun üçün ilk növbədə mətn parollarından istifadə etmək məsləhət deyil. Birdəfəlik parollardan və kriptoqrafik auytentifikasiyadan istifadə olunması praktiki olaraq hədələri heçə endirə bilər. Təəsüflər olsun ki, nə bütün əlavələr, hostlar və qurğular autentifikasiyanın təklif edilən üsullarını dəstəkləmirlər.

İstifadəçi adi parol yaradan zaman çalışmalıdır ki, parolu sındırmaq çətin olsun. Parolun uzunluğu minimum 8 simvol olmalıdır. Parol klaviaturanın yuxarı reqistr simvollarından, rəqəmlərdən və xüsusi işarələrdən (məsələn, #, $, %, və i.a.) yığılmalıdır.

Açarın tapılması. Kriptoqrafik açar müdafiə ediləcək informasiyanın kod və ya ədəd ilə qorunmasıdır. Digər tərəfdən açarın bilinməsi böyük xərc tələb edir. Açarın məlum olması üçün xüsusi proqramlar işlənib hazırlanmışdır.

Əgər açara hücum olunarsa, açar *etibardan düşmüş* hesab olunur. Hücuma keçən şəxs etibardan düşmüş açardan istifadə etməklə göndərilən və qəbul edilən informasiyaya əlçatan olur. Belə açar pisniyyətli insana kodlanmış informasiyanı koddan azad etməyə və dəyişməyə imkan verir.

Əlavələr səviyyəsində hücum bir neçə üsulla yerinə yetirilir. Bunlardan ən çox yayılmışı FTP, HTTP və Veb-server proqram təminatlarıdır.

Əlavələr səviyyəsində hücumun əsas problemi ondan ibarətdir ki, burada əsasən şəbəkələrarası ekran keçidindən keçən portlardan istifadə edilir. Bu hücum barədə məlumatlar yayın orqanlarında ətraflı nəşr olunur. Buna əsas səbəb administratorlara korreksiya modulunun (patç) köməyilə problemi həll edə bilməsinə imkanın verilməsidir. Əfsuslar olsun

ki, əksər xakerlər də bu barədə məlumatlıdırlar və pis məqsədlə bunlardan istifadə edirlər.

Edilən hücumu əlavələr səviyyəsindən istifadə etməklə tamamilə ləğv etmək mümkün deyil. Xakerlər də İnternetdəki saytlarda istifadə olunan tətbiqi proqramların zəif yerləri haqqında məlumatları verir və bundan da lazım olduqda istifadə edirlər.

Edilən hücumların qarşısını almaq və onların vurduğu ziyanı müəyyən qədər azaltmaq üçün aşağıdakı tədbirləri görmək lazımdır:

- Xüsusi analitik əlavələrdən istifadə etməklə əməliyyat sistemlərinin və şəbəkənin log-fayllarını təhlil etmək;
- CERT verilənlərindən istifadə etməklə tətbiqi proqramın zəif yerini nəzarətdə saxlamaq;
- Əməliyyat sisteminin ən sonuncu versiyasından, əlavələrin və korreksiya modulunun axırıncı versiyalarından istifadə etmək;
- Hücumu müəyyənləşdirən IDS (Intrusion Detection Systems) sistemindən istifadə etmək.

Şəbəkə kəşfiyyatı. Bu əlavələrdən və əlçatan verilənlərdən istifadə etməklə şəbəkə haqqında informasiyanın toplanmasıdır, çünki hücuma hazırlaşan xaker həmişə çalışır ki, hücum edəcəyi şəbəkə haqqında çoxlu sayda informasiyaya malik olsun.

Şəbəkə kəşfiyyatı DNS sorğu, exo-testləmə (ping sweep) və portların skanerə edilməsi formasinda yerinə yetirilir.

DNS sorğusu domenin sahibinin kim olması, domenə hansı ünvanın mənimsənilməsi (verilməsi) haqqında informasiyadır.

Ünvanların exo-testlənməsi hansı hostun verilmiş mühitdə real işləməsini görməyə imkan verir. Hostların siyahısını alan

xaker edilən xidmətlərin tam siyahısını tərtib etmək və bu xidmətləri dəstəkləyən hostlar haqqında məlumat almaq üçün portların skanerlənməsini həyata keçirir. Nəticədə "sındırılması" lazım olan informasiya əldə edilir.

Şəbəkə və host səviyyəsində IDS sistemi adətən şəbəkə kəşfiyyatı məsələsinin öhdəsindən yaxşı gəlir. Bu səbəbdəndə sistem istifadəçiyə ediləcək hücuma lazımı səviyyədə hazırlaşmağa imkan verir və bu barədə provayderi (ISP) məlumatlandırır.

Etibardan sui-istifadə. Fəaliyyətin bu növünü sözün əsl mənasında hücum saymaq düzgün deyil. Növ sadəcə olaraq şəbəkədə yaranmış etibardan qərəzli istifadə edilməsi ilə bağlıdır. Buna tipik nümunə kimi korporativ şəbəkənin periferiya hissəsində baş verən hadisələrdən sui-istifadə olunmasını göstərmək olar. Şəbəkənin bu seqmentində DNS, SMTP və HTTP serverləri yerləşir. Bu serverlər bir seqmentdə yerləşdikləri üçün onlardan birinin "sındırılması" digərlərinin də "sındırılması"na gətirib çıxarır, çünki serverlər digər sistemdə olan, onlara uyğun serverlərə etibar edirlər.

Etibardan sui-istifadə riskini etibar üzərində sərt nəzarət qoymaqla azaltmaq mümkündür. Sistemdən kanarda olan serverlər etibardan mütləq formada istifadə etməməlidirlər. Serverlərin bir-birinə olan etibarı həm IP-ünvanına, həm də ki, digər parametrlərə görə müəyyən protokollar və autentifikasiya ilə məhdudlaşmalıdır.

HƏDƏLƏR VƏ NAQİLLİ KORPORATİV ŞƏBƏKƏLƏRİN ƏLAQƏLƏNDİRİLMƏSİ

Başlanğıc mərhələdə şəbəkə texnologiyalarının inkişafına viruslardan və digər kompüter hücumlarından o qədərdə ziyan

dəymirdi, çünki dünya iqtisadiyyatının inkişafı informasiya texnologiyalarından o qədər də asılı deyildi. İndiki zamanda biznesin elektron vasitələrindən asılılığı, informasiya mübadiləsi və elektron qurğularına edilən hücumlar və onların vurduğu ziyanlar milyon dollarla ölçülür, dünya iqtisadiyyatına vurulan ziyanlar isə onlarla milyard dollara bərabər olur.

Korporativ şəbəkələrdə təhlil edilən informasiya bir-biri ilə əlaqəlidir və buna aşağıdakılar səbəbdir:

- Kompüterdə təhlil olunan, ötürülən və onun yaddaşda saxlanılan informasiyanın həcminin artması;
- Əhəmiyyətinə və konfidensiallığına görə müxtəlif informasiyanın verilənlər bazasında toplanması;
- Verilənlər bazasında saxlanılan informasiyanın müəyyən istifadəçilər tərəfindən istifadə edilməsinə imkanın olması;
- Hesablama texnikası resurslarından müəyyən dairə istifadəçilərin istifadəsi;
- Uzaqlaşdırılmış işçi yerlərinin sayının çoxalması;
- Qlobal İnternet şəbəkəsindən və müxtəlif rabitə kanallarından geniş formada istifadə olunması;
- Kompüter istifadəçiləri arasında informasiya mübadiləsinin avtomatlaşdırılması.

Ən çox yayılmış hədələrin təhlili göstərir ki, müasir naqilli korporativ şəbəkə pisniyyətli insanın zorla şəbəkəyə daxil olmasından tutmuş virusların kompüterə və şəbəkəyə daxil olmasına qədər olan müxtəlif hədələrə məruz qalır (Bu zaman hədənin də mənbəyinin dəyişməsi nəzərə alınmalıdır). Təhlilin nəticəsi ən böyük təhlükənin insan amili olduğunu sübut edir.

Qeyd etmək lazımdır ki, təhlükə mənbəyi informasiya sisteminin daxilində, həm də ki, xaricində ola bilər. Belə yanaşma düzgündür. Odur ki, təhlükə mənbəyi haqqında çoxlu

məlumatın əldə olunması təhlükəyə qarşı effektiv avadanlıqların hazırlanmasına və şəbəkənin belə avadanlıqlar ilə təmin edilməsinə zərurət yaradır.

Ən təhlükəli və ən tez-tez vurulan ziyan istifadəçilərin, operatorların, sistem administratorlarının və informasiya sistemləri qulluqçularının düşünmədən etdiyi səhvlərdir. Bəzən belə səhvlər bir-başa ziyanla (məsələn, verilənləri daxil edəndə, proqramda səhv olduqda, sistemin qəflətən dayanması hallarında, sistemin dağılması nəticəsində və s.) tamamlanır. Bundan istifadə edən bədniyyətli insan öz məqsədlərini həyata keçirir.

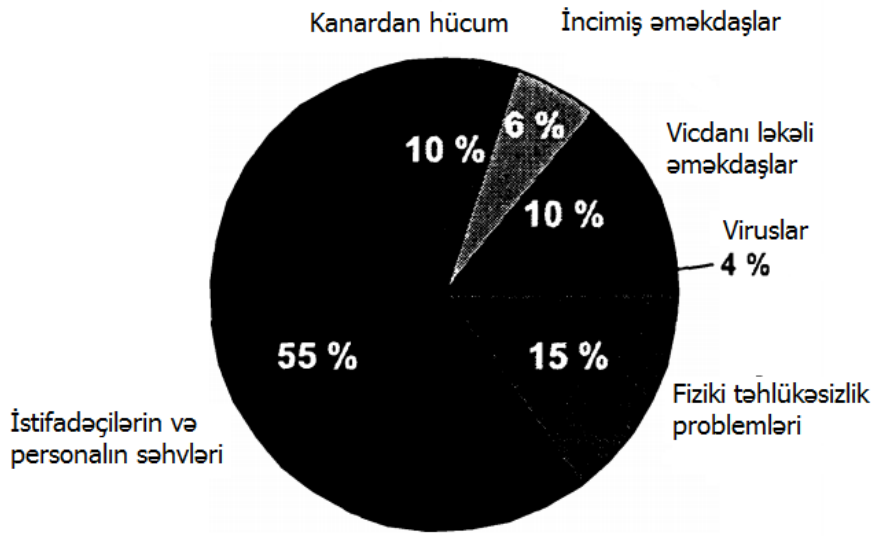
Amerikanın Milli Standartlar və Texnologiyalar İnstitutunun məlumatına görə (NIST) baş verən hadisələrin 55% informasiya sistemlərinin təhlükəsizliyinin pozulması ilə bağlıdır. Qlobal miqyasda bu faktor aktualdır. Qeyd edilir ki, ziyan mənbəyi kimi təşkilatlarda işləyən istifadəçilər, qlobal şəbəkə istifadəçiləri və s. ola bilir.

15 saylı şəkildə informasiya sistemləri kanallarında baş verən təhlükəsizliyin pozulması diaqramı verilmişdir.

Vurulan ziyanın ölçüsünə görə ikinci yerdə oğurluq və saxtakarlıq durur. Əksər araşdırmalarda günahkarlar təşkilatın ştatda olan əməkdaşlarının olduğu müəyyən olunur, çünki onlar iş rejimi və müdafiə tədbirləri ilə tanışdırlar. Güclü informasiya kanalına malik qlobal şəbəkələrdə də lazımi şəkildə həyata keçirilən işlərə (və tədbirlərə) nəzarətin olmaması üzüdən qlobal şəbəkələr əlavə ziyanlar mənbəyinə çevrilir, şəbəkənin fəaliyyətinə müəyyən qədər ziyan vurur.

Bəzən müəssisədə işləyən əməkdaş müəssisədə ona qarşı yönəlmiş xoşagəlməz hadisələrdən inciyir, müəssisənin fəaliyyəti barədə yaxın yoldaşına məlumatlar verir (və ya çatdırır), bütün bu hadisələr müəssisənin iş rejiminə, onun

effektivliyinə böyük ziyan vurur. Odur ki, əməkdaş işdən azad olunan zaman onun qiymətli informasiyaya əlçatanlığı tamamilə ləğv edilməlidir.



Şəkil 15. Təhlükəsizliyin pozulma mənbələri

Təhlükəsizliyin pozulmasına xarici kommunikasiya avadanlıqlarının da təsiri vardır, onların vurduğu ziyan 10% təşkil edir. Bu rəqəmin o qədər də böyük olmamasına baxmayaraq Amerikanın İnformasiya Sistemlərinin Müdafiəsi Agentliyinin apardığı testlərə istinad etməklə demək olar ki, istifadə olunan kompüterlərin 88%-i informasiya təhlükəsizliyi baxımından zəif yerlərə (hissələrə) malikdirlər. Bununla yanaşı təşkilatın informasiya strukturuna uzaqdan əlçatanlığın da baş verməsini daim nəzərdə saxlamaq, bu mənbəədən gələn zərbələr də araşdırılmalıdır.

Təhlükəsizlik siyasətini qurmazdan öncə həyata keçiriləcək riskləri (təşkilatın kompüter mühiti, uyğun fəaliyyətin qəbulu və s.) qiymətləndirmək lazımdır. Həmçinin nəzərə almaq lazımdır ki, təşkilatın bu məsələlərə (nəzarətin təşkili, təhlükəsizlik hədələrinin aradan qaldırılması və s.) ayırdığı paralar gözlənilən həddi aşıb keçməməlidir.

Aparılmış statistik hesablamalar təşkilatın personalına və rəhbərliyinə əsas gücü (və diqqəti) hara (sistemlərin və korporativ şəbəkələrin təhlükəsizlik hədələrinin effektiv azaldılmasına) yönəltməyə aydınlıq gətirir. Bununla yanaşı fiziki təhlükələrə və əməkdaşların buraxdığı səhvlərdən yaranan təhlükələrə qarşı da mübarizə aparılmalıdır. Rəhbərlik şəbəkə təhlükəsizliyinə diqqəti artırmaqla yanaşı korporativ şəbəkəyə və sistemə xaricdən, həmçinin daxildən edilən hücumlara qarşı mübarizə aparmalı, onların qarşısının alınmasında bütün imkanlardan istifadə etməldir. Bütün bunların həll edilməsinə yönəldilmiş cəhdlər təhlükəsizlik problemləridir.

HƏDƏLƏR VƏ NAQİLSİZ KORPORATİV ŞƏBƏKƏLƏRİN ƏLAQƏLƏNDİRİLMƏSİ

Naqilsiz şəbəkə qurulan zaman əsas məsələ həmin şəbəkənin təhlükəsizlik problemi ilə bağlıdır. Əgər adi şəbəkələrdə informasiya naqillər vasitəsilə ötürülürsə, burada radiodalğalar naqilisiz xətlərlə ötürülür və uyğun avadanlıqlardan istifadə etməklə onları asanlıqla tutmaq mümkündür. Naqilsiz şəbəkənin fəaliyyət prinsipi belə şəbəkələrin çoxlu sayda hücumlara və şəbəkəyə daxilolmalara məruz qalmasına səbəb olur.

Naqilsiz lokal WLAN (Wireless Local Area Network) şəbəkə avadanlığı şəbəkəyə və işçi stansiyalara abonentin naqilsiz qoşulmasına imkan verir.

AÇIQLAMA: Naqilsiz lokal şəbəkə (ingiliscə Wireless Local Area Network; Wireless LAN; WLAN) – naqilsiz texnologiyaya əsaslanaraq qurulmuş lokal şəbəkədir. Şəbəkədə verilənlərin ötürülməsi radioefir vasitəsilə həyata keçirilir. Şəbəkədə qurğuların bir-birilə əlaqəsi kabel birləşmədən istifadə etmədən yerinə yetirilir. İndiki zamanda ən geniş yayılmış naqilsiz birləşmə Wi-Fi əlaqəsidir. Naqilsiz birləşmə texnologiyası telekommunikasiya mühitində innovasiya məsələlərini həll etmək üçün dünyada ən populyar və geniş tətbiq olunan sayılır.

İndiki zamanda Böyük Britaniyada, Finlandiyada, Norveçdə, ABŞ-da və digər inkişaf etmiş ölkələrdə WLAN şəbəkəsinin yaradılması böyük sürətlə həyata keçirilir. Abonentlərin işgüzar səfərlərində onlara WLAN-rouminq xidməti təklif edilir. Bu zaman İnternet-resurslardan istifadə və korporativ şəbəkələrə əlçatanlığı abonentin ofisini tərk etmədən həyata keçirdiyi əlaqələr ilə eynilik təşkil edir.

Əlçatanlıq AP nöqtəsi (*Access Point*) konsentrator (bir yerə toplama, yığma) rolunu oynayır, abonentlər arasında, həm də öz aralarında əlaqəni təmin edir, körpü funksiyasını yerinə yetirir, İnternet və lokal şəbəkə ilə kabel rabitəsini yerinə yetirir. Hər bir əlçatan nöqtə bir neçə abonentə xidmət edə bilir. Bir neçə yaxın yerləşmiş əlçatanlıq nöqtəsi ***Wi-Fi*** əlçatanlıq zonası əmələ gətirir. Bu zona naqilsiz adapterlər ilə təmin olunur ki, onlarında köməyilə şəbəkəyə əlçatanlıq mümkündür. Belə zonalar insanların toplandığı yerlərdə:

aeroportlarda, tələbə şəhərciklərində, kitabxanalarda, mağazalarda, biznes-mərkəzlərdə və s. yerlərdə yaradılır.

AÇIQLAMA: *Wi-Fi* (Wireless Fidelity – ingiliscədən tərcümədə "naqilsiz keyfiyyət" anlamını verir) adı ilə dünyada məşhur olan lokal naqilsiz şəbəkənin yaradılma texnologiyasına 1980-cı illərin sonunda başlanılmışdır. Wi-Fi naqılsız şəbəkəsi IEEE 802.11 standartı bazasına əsaslanaraq hazırlanmış Wi-Fi Alliance satış markasıdır.

Wi-Fi lokal naqilsiz şəbəkə 1991-ci ildə Niderlandiyanın Niveqeyn şəhərində NCR Corporation/AT&T tərəfindən yaradılmışdır. Hazırlanmış şəbəkə ilk dəfə kassa aparatları sisteminə qulluq üçün nəzərdə tutulmuşdu. Wi-Fi şəbəkəsinin yaradıcısı Vik Heyz (Vic Hayes) rəhbərlik etdiyi qrupun köməkliyi ilə IEEE 802.11b, IEEE 802.11a və IEEE 802.11g standartlarının hazırlanmasında fəal iştirak etmişdir.

IEEE 802.11n standartı 11 sentyabr 2009-cu ildə təsdiq edildi. Standartdan istifadə etməklə verilənlərin ötürülmə sürəti əvvəlki standartlarla müqayisədə (maksimal sürət 54 Mbit/saniyəyə bərabər idi) dörd dəfə artırıldı. 2011-

2013-cü illərdə yeni standart yaradıldı və həmin standartın (IEEE 802.11ac standartı nəzərdə tutulur) tam qəbulu 2014-cü ilə planlaşdırıldı. Yeni standartda informasiyanın ötürülmə sürəti Qiqabit/saniyələrlə ölçülməsi nəzərdə tutuldu.

Wi-Fi lokal naqilsiz şəbəkədə fiziki mühit kimi radiotezlikli və ya infraqırmızı diapozona malik mühiddən istifadə edilir.

Əlçatanlıq nöqtəsinin servislərinin toplama identifikatoru – SSID (Service Set Identifier) vardır. SSID 32 bitlik sətirdir, naqilsiz şəbəkədə ad kimi istifadə olunur, onun köməyilə şəbəkənin bütün düyünləri assosiasiya olunur. SSID identifikatoru işçi stansiyanın şəbəkəyə qoşulması üçün yararlıdır.

İşçi stansiyaları əlçatanlıq nöqtərləri ilə birləşdirmək üçün hər iki sistem eyni SSID-yə malik olmalıdır. Əgər işçi stansiya lazım olan SSID-yə malik deyilsə, onda o, əlçatanlıq nöqtəsi ilə birləşə bilmir, şəbəkəyə qoşulmaq imkanından məhrum olur.

Naqilli və naqilsiz şəbəkələrin bir-birindən əsas fərqi naqilsiz şəbəkənin sonuncu nöqtələri arasında nəzarət edilməyən sahələrin olmasıdır. Bu fərq hücum edənə (bədniyyətli insana) imkan verir ki, bilavasitə naqilsiz struktura yaxın yerləşən sahələrə ardıcıl hücumlar etsin (belə hücumları naqilli şəbəkələr mühitində yerinə yetirmək mümkün deyil).

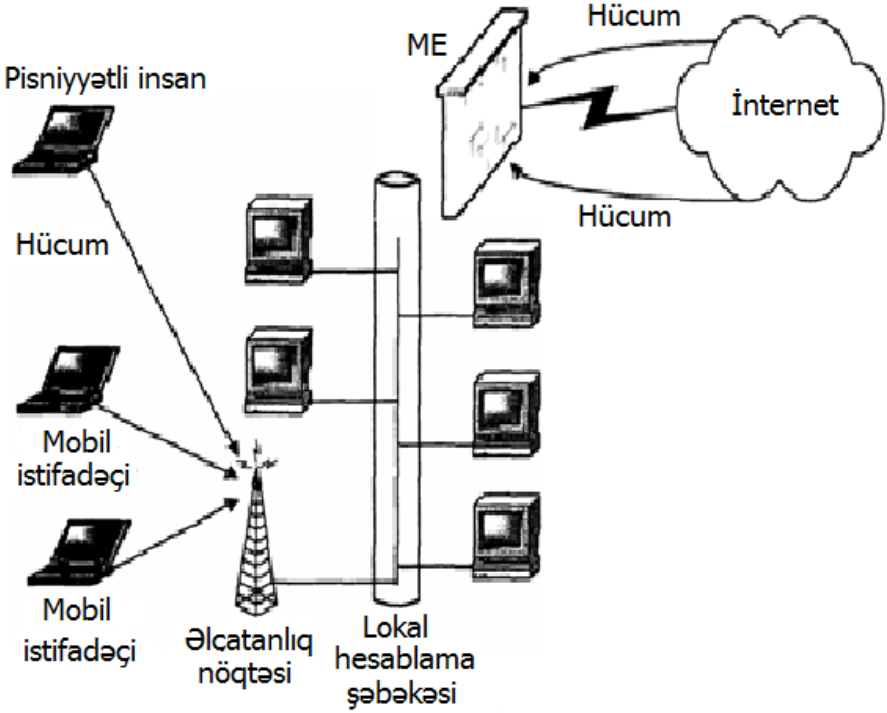
Lokal naqilsiz şəbəkədən istifadə edəndə təhlükəsizlik hücumları hiss ediləcək dərəcədə çoxalır (şəkil 16.).

Aşağıda naqilsiz şəbəkə təhlükələri və onlar arasında əsas əlaqələr verilmişdir.

Radiomayak radio verilişi. Radiomayak geniş veriliş diapazonuna malikdir və naqilsiz rabitə barədə ətraf yerlərə məlumatlar göndərir. Geniş diapazona malik siqnallar naqilsiz

əlçatanlıq informasiya nöqtələrindən ibarətdir və özünə SSID birləşdirməklə mövcud olan sahədə naqilsiz düyünləri qeyd etməyə dəvət edir.

Susma rejimində olan istənilən işçi stansiya SSID ala bilər və özünə uyğun şəbəkəni əlavə edə bilər. Radiomayakın verilişləri naqilsiz şəbəkənin "anadangəlmə patalogiyası"ndan ibarətdir. Bir çox modellər verilişlərdən SSID-ə aid olanları ayırmağa imkan verir. Nəticədə naqilsiz şəbəkədə qulaqasmalar çətinləşir.



Şəkil 16. Lokal naqilsiz şəbəkəyə edilən hücumlar

WLAN-nın aşkar edilməsi. Naqilsiz şəbəkə WLAN-nın aşkar edilməsi üçün, məsələn, NetStumber utuliti ilə Qlobal mövqeli GPS sistemi peyk naviqatorunun (naviqasiya mütəxəssisinin) birgə fəaliyyətindən istifadə edilir. Utilitin mövcud parametrləri WLAN şəbəkəsində SSID ilə ldentifikasiya olunur. Portativ kompüterdə xarici antennadan istifadə edən zaman müəyyən şəhərin yanından keçəndə və ya şəhərdə gəzinti təşkil edəndə WLAN şəbəkəsini aşkar etmək mümkündür. WLAN şəbəkəsinin aşkar olunmasının ən etibarlı metodu istifadəçinin offis binasında fərdi kompüteri əllərində saxlamaqla (daha doğrusu gəzdirməklə) axtarış etməsidir.

Xəlvətcə qulaq asma. Xəlvətcə qulaq asmaqla şəbəkədən informasiya toplanılır və toplanmış informasiyadan istifadə etməklə şəbəkəyə hücum həyata keçirilir. Məlumatı ələ keçirən şəxs onlardan istifadə etməklə şəbəkə resurslarına əlçatanlıq edə bilər. Naqilsiz şəbəkə xarakterinə görə ondan müəyyən məsafədə yerləşən kompüterin fiziki şəbəkəsi ilə əlaqə yarad bilər (əgər kompüter bilavasitə şəbəkəyə daxildirsə). Məsələn, naqilsiz şəbəkəyə binada yaradılmışsa, onda binadan çox da uzaq məsafədə olmayan (və yaxud da binanın yanında maşında oturmuş insan) insan şəbəkəyə qoşula bilər. Beləliklə, passiv şəkildə xəlvətcə qulaq asmaqla mübarizə aparmaq praktiki olaraq mümkün deyil.

Şəbəkəyə daxil olmaq üçün yaradılmış yalanşı nöqtə. Peşəkar pisniyyətli şəxs şəbəkə resurslarını imitasiya etməklə şəbəkədə yalançı nöqtə yarada bilər. Bundan xəbərsiz abonentlər yalançı nöqtəyə müraciət etməklə onlara məxsus əhəmiyyətli rekvizitləri söyləyə bilərlər (məsələn, autentifikasiya edilmiş informasiyanı). Belə hücum bədniyyətli insanın şəbəkəyə daxil olmaq üçün yararlı olan həqiqi nöqtəni "boğduqdan" sonra onun tərəfindən yerinə yetirilir.

Xidmətdən imtina. Şəbəkəni tam iflic vəziyyətinə salmaq üçün DoS növlü hücumdan (Denial of Service) – xidmətdən imtina hücumundan istifadə olunur. Xidmətin məqsədi istifadəşinin şəbəkə resurslarına daxil olmasına maneçilik etməkdir. Naqilsiz sistemlər belə hücumlara həssasdırlar. Naqilsiz şəbəkədə fiziki səviyyə dedikdə əlçatanlıq nöqtəsi ətrafında abstrakt mühit başa düşülür. Pisniyyətli insan ona məxsus olan avadanlığı işə salmaqla bütün işçi spekteri maneələrlə və qeyrileqal trafiklərlə doldurub işə tam maneçilik edə bilər. Bu məsələnin həll edilməsi pisniyyətli insan üçün heç bir çətinlik törətmir.

Beləliklə, fiziki səviyyədə DoS hücumun həyata keçirilməsini sübuta yetirmək mümkün deyil.

"***İnsan ortada***" ***növlü hücum***. Bu növ hücumu naqilsiz şəbəkələrdə həyata keçirmək naqilli şəbəkələrdə həyata keçirməkdən daha asandır, çünki naqilli şəbəkədə ona müəyyən əlçatanlığın müəyyən növünün realizə olunması tələb olunur. Adətən bu növ hücumdan rabitə əlaqəsinin tamlığını və konfidensiallığını dağıtmaq üçün istifadə edilir. MITM hücumu digər hücumlara nisbətdə daha mürəkkəbdir. Belə hücumları yerinə yetirmək etmək üçün şəbəkə haqqında ətraflı informasiyanın olması vacibdir. Pisniyyətli insanlar adətən şəbəkə resurslarından birinin identifikasiyasını dəyişirlər. Pisniyyətli insan qulaqasma və qeyrileqal yolla verilənlər axınını əldə etməklə verilənlərin məzmununu dəyişir, digər hostu imitasiya etmək üçün MAC-ünvanı digəri ilə əvəz edir və s.

İnternetə anonim yolla daxil olmaq. Müdafiə olunmayan naqilsiz lokal hesablama şəbəkəsi xakerlərə imkan verir ki, İnternetə anonim yolla hücum etsinlər. Xakerlər müdafiə edilməyən lokal hesablama şəbəkəsindən istifadə etməklə İnternetə çıxış əldə edə bilir və bu zaman heç bir iz

qoymurlar. Müdafiə olunmayan lokal hesablama şəbəkəsi olan təşkilatlar formal olaraq xakerlər tərəfindən hücum mənbəyinə çevrilirlər.

Qeyd etmək lazımdır ki, öndə yazılan hücumlar xakerlər tərəfindən istifadə edilən hücumların bir qismidir.

ŞƏBƏKƏNİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏ ÜSULLARI

Kompüter sistemlərinin və şəbəkələrinin təhlükəsizliyinin təmin edilməsi probleminə iki yanaşma mövcuddur: "fraqmentlərlə" və "kompleks".

"*Fraqmentlərlə*" yanaşma verilmiş şərtlər daxilində dəqiq müəyyən edilmiş hücumlara qarşı dayanma hallarına yönəldilmişdir. Nümunə kimi əlçatanlıq ilə idarə edilən avadanlıqları, şifrələmənin avtonom vasitələrini, xüsusi hazırlanmış antivirus proqramlarını və i. a. göstərmək olar.

Belə yanaşmanın üstünlüyü konkret hücuma qarşı yüksək yaradıcılıqdır. Yanaşmanın çatışmazlığı isə müdafiə olunacaq birləşmiş informsiya təhlili mühitinin olmamasıdır. İnformasiyanın müdafiəsini təmin edən fraqmentlərlə müdafiə tədbirləri konkret kompüter sistemləri və şəbəkələri obyektlərinin mühafizə edilməsini təmin edir. Hətta çoxda böyük olmayan hədənin videodəyişikliyi müdafiənin effektivliyinin itməsinə səbəb olur.

Kompleks yanaşma kompüter sistemləri və şəbəkələrində informasiya təhlili mühitinin mühafizə edilməsinin yaradılması üçün nəzərdə tutlmuşdur. Yanaşma hədələrə qarşı çıxmaq üçün müxtəlif tədbirlər kompleksindən ibarətdir. İnformasiya təhlili mühitinin müdafiə edilməsinin təşkili kompüter sistemlərinin və şəbəkələrinin təhkükəsizlik səviyyəsinin lazımi səviyyədə olmasına təminat verir. Bu da kompleks yanaşmanın üstünlüklərindən sayılır. Kompleks yanaşmanın çatışmazlığına bunları aid etmək olar: kompüter sistemləri və şəbəkələri istifadəçisinin məhdud imkanının olması; müdafiə mühitinin sazlanmalara qarşı həssas olması; idarəetmənin mürəkkəbliyi və s.

Kompüter sistemlərinin və şəbəkələrinin müdafiə edilməsinə kompleks yanaşmadan böyük təşkilatlar, bəzən də kiçik təşkilatlar istifadə edir. Əsas məqsəd mühüm əhəmiyyətə malik xüsusi (əlahiddə) informasiyanın təhlil olunması və buna məsul yanaşmaların lazımi səviyyədə yerinə yetirilməsidir. Böyük müəssisələrdə informasiya təhlükəsizliyinin pozulması böyük həcmdə həm müəssisəsə, həm də ki, müştəriyə ziyan vurur. Odur ki, belə müəssisələr təhlükəsizlik təminatına xüsusi fikir yönəldir, kompleks tədbirlər həyayta keçirirlər. Kompleks yanaşmanı əksər dövlət və böyük həcmli kommersiya təşkilatları və müəssisələri dəstəkləyir. Belə yanaşma özünü hazırlanmış müxtəlif standartlarda əks etdirir.

Təhlükəsizliyin təmin edilməsi probleminə kompleks yanaşma kompüter sistemləri və şəbəkələri üçün hazırlanmış təhlükəsizlik siyasətinə əsaslanır. Təhlükəsizlik siyasəti kompüter sistemləri və şəbəkələrinin müdafiə mühitinin effektiv istifadə edilməsinə şərait yaradır. Təhlükəsizlik siyasəti sistemin ozünü müxtəlif vəziyyətlərdə necə aparmasından asılı olmayaraq informasiyanın təhlil edilməsində mümkün olacaq

bütün xüsusiyyətləri əhatə edir. Nəzərə almaq lazımdır ki, sistemin təhlükəsizliyi effektiv nəticə verən siyasət olmadan yaradıla bilməz.

Subyektlərin informasiya baxımından müdafiə maraqlarını müxtəlif səviyyələrdə birləşdirmək zəruridir:

- Qanunvericilik (standartlar, qanunlar, normativ aktlar və buna bənzərlər);
- Administrativ-təşkilatı (ümumi xarakterli fəaliyyət, təşkilatın rəhbərliyi tərəfindən qəbul edilənlər, insanlarla bağlı olan konkret təklükəsizlik tədbirləri);
- Proqram-texniki tədbirlər.

Qanunvericilik səviyyəsində tədbirlər informasiyanın təhlükəsizliyi üçün çox vacibdir. Bura informasiya təhlükəsizliyinə qarşı neqativ halları yaradanlara və nizam-intizamı pozanlara qarşı cəmiyyətdə həyata keçirilən və hamı tərəfindən dəstəklənən kompleks tədbirlər daxildir.

İnformasiya təhlükəsizliyi – bu fəaliyyətin yeni növüdür, burada təkcə qadağa qoymaq və ya cəzalandırmaq, həmçinin öyrətmək, başa salmaq, kömək etmək və sair bu kimi tədbirlərin həyata keçirilməsi əsas sayılır. Cəmiyyət problemi başa düşməli, onun aradan qaldırılması üçün yerinə yetiriləcək tədbirləri dəstəkləməlidir. Dövlət belə tədbirləri optimal şəkildə həyata keçirir. Burada çoxlu məbləğdə maddi yatırımların yerinə yetirilməsi deyil, əsas məsələ intellektual səviyyənin yüksəldilməsidir.

Administrativ-təşkilatı səviyyədə tədbirlər. Təşkilatın rəhbərliyi təhlükəsizlik rejimini dəstəkləməli və bunun həyata keçirilməsi üçün lazımi resurslar ayırmalıdır. Administrativ-təşkilatı səviyyədə tədbirlərin əsası təhlükəsizlik siyasəti və təşkilatı tədbirlər kompleksidir. Kompleksə insanlar tərəfindən

həyata keçirilən təhlükəsizlik tədbirləri daxildir. Təşkilatı tədbirləri aşağıdakı kimi təsnifləndirirlər:

- Personalla (fərdlə) idarəetmə;
- Fiziki müdafiə;
- İş qabiliyyətinin saxlanması;
- Təhlükəsizlik rejiminə reaksiya verilməsi;
- Bərpa işlərinin planlaşdırılması.

Hər bir müəssisə təsnifatı yerinə yetirmək üçün müəyyən tədbirlər tolumunu həyata keçirməlidir.

Proqram-texniki səviyyədə vasitələr və tədbirlər. İnformasiya təhlükəsizliyi rejiminin dəstəklənməsi üçün proqram-texniki səviyyə tədbirləri əsasdır, çünki kompüter sistemlərinə edilən hücumlar (avadanlığın işləməkdən imtina etməsi, proqram təminatında olan səhvlər, istifadəçilərin və rəhbərliyin müəyyən işləri yerinə yetirərkən sapmalara yol vermələr və i.a.) əsasən onlardan edilir. Müasir informasiya şəbəkələri çərçivəsində sistem aşağıda verilmiş təhlükəsizlik mexanizmlərinə əlçatan olmalıdır:

- İstifadəçilərin həqiqiliyinin yoxlanması və identifikasiya edilməsi;
- Daxil olmaların idarə edilməsi;
- Ptorokollaşdırma və audit;
- Kriptoqrafiya;
- Ekranlaşdırma;
- Yüksək səviyyədə əlçatanlığın təmin edilməsi.

Standartların qəbul edilməsinə zərurətin olması. Şirkətlərin informasiya sistemləri müxtəlif istehsalçıların istehsalı olan proqram və aparat vasitələrindən qurulur. Araşdırmalar göstərir ki, indiki zamana kimi heç bir istehsalçı-şirkət istifadəçiləri onlara lazım olanların tam siyahısına uyğun avadanlıq və proqram təmintı ilə təmin etsin. Müxtəlif

xüsusiyyətli informasiya sistemlərində informasiyanı etibarlı müdafiə etmək üçün yüksək ixtisaslı mütəxəssislərin olması vacibdir. Onlar informasiya sistemlərinin hər bir komponentinin (təşkiledicisinin) təhlükəsizliyinə cavabdeh olmalı, informasiya sistemlərini düzgün sazlamalı, sistemdə baş verən dəyişiklikləri daim izləməli, istifadəçinin işinə nəzarət etməli və s. işləri tutarlı səviyyədə icra etməlidirlər. Aydındır ki, informasiya sistemləri nə qədər müxtəlif xüsusiyyətlərə malik olsalar, o qədər də onların təhlükəsizliyini təmin etmək mürəkkəbdir. Korporativ şəbəkələrinin və müdafiə qurğuları sistemlərinin çoxluğu, şəbəkədaxili ekranlar, şlüzlər və VPN-lər, həmçinin korporativ verilənlərə istifadəçilərin maraqlarinin artmasi və həmin verilənlərə istifadəçilərin daxilolmalarının çoxalmasl, tərəfdaşlar və sifarişçilərin sayının artması və s. mürəkkəb müdafiə sisteminin yaradılmasını zəruri edir.

Təhlükəsizliyin təşkilatı baxımdan həll edilməsi müdafiəni bütün səviyyələrdə təmin etməlidir. Odur ki, vahid standartlar toplumunun yaradılması həm istehsalçılar üçün, həm də ki, istehlakçılar üçün sözsüz ki, vacibdir.

İnformasiya təhlükəsizliyinin təmin olunması sahəsində tətbiq olunan standartlar daimi bünövrə yaradır, kriteriyaların müəyyən edilməsində əsas rol oynayırlar. Standartlar müxtəlif istehsalçıların istehsal etdikləri məhsullar arasında uyğunluğun əldə olunmasında və bu məhsullardan informasiya sistemlərində istifadəsi zamanı təhlükəsizliyin lazımi səviyyədə qorunmasında bünövrə sayılırlar.

Təhlükəsizliyin təmin edilməsi probleminə kompleks yanaşma, qanunvericilik, inzibatı-təşkilatı və proqram-texniki tədbirlər, sənaye, milli və beynəlxalq standartlar – bütün bunlar korporativ şəbəkələrin müdafiə sisteminin təməlidir.

ŞƏBƏKƏLƏRDƏ İNFORMASİYANIN MÜDAFİƏ PROBLEMİNİN HƏLLİ YOLLARI

İnternet şəbəkəsindən istifadə edən zaman informasiya təhlükəsizliyi probleminin həlli yollarının axtarılması üçün asılı olmayan konsersium ISTF (İnternet Security Task Force) yaradıldı. ISTF ictimai təşkilatdır, informasiya təhlükəsizliyi vasitələrinin, elektron biznes və İnternet-infrastrukturları provayderlərinin tədarükçi şirkətlərinin ekspertlərindən və nümayəndələrindən yaradılmışdır. Konsersuimun məqsədi İnternetdə işləyərkən təhlükəsizliyin təmin edilməsi üçün texniki, təşkilatı və əməliyyat xarakterli əsasnamələrin hazırlanmasıdır.

ISTF konsersiumu informasiya təhlükəsizliyini 12 sahəyə bölmüşdür və ilk növbədə əsas diqqəti elektron biznesə yönəltməyi məsləhət bilir. Elektron biznesdə əsas məsələ onun iş qabiliyyətinin təmin edilməsidir. Bununla yanaşı siyahıya aşağıdakılar da əlavə edilmişdir:

- Autentifikasiya (identifikasiya edilmiş informasiyanın obyektiv təsdiq edilmə mexanizmi);
- Fərdi informasiya malik olma hüququ (məxfi informasiyanın təmin edilməsi);
- Təhlükəsizlik hadisələrinin müəyyən edilməsi (Security Events);
- Korporativ perimetrin müdafiəsi;
- Edilən hücumların müəyyən edilməsi;
- Əlçatanlığa nəzarət;
- İnzibatçılıq;
- Baş vermiş hadisələrə reaksiyanın verilməsi (İncident Response).

ISTF -nin təqdimatları fəaliyyətdə olan və ya yeni fəaliyyətə başlayan elektron biznes və elektron kommersiya şirkətləri üçün nəzərdə tutulmuşdur. Bu təlimatların şirkətlərə tətbiqi onu göstərir ki, elektron biznes sistemində informasiyanın müdafiəsi kompleks şəkildə olmalıdır.

Hücumlardan kompleks müdafiə və təminat iqtisadi baxımdan əlverişlidir. Odur ki, elektron biznes üçün kommunikasiya resurslarından istifadə etmək üçün aşağıdakılar vacibdir:

- Elektron biznes sistemlərində təhlükəsizlik hədələrinin təhlil edilməsi;
- İnformasiya təhlükəsizliyi siyasətinin işlənib hazırlanması;
- Konfidensiallığı, tamlığı və ötürülən informasiyanın əslliyini qorumaqla kanal vasitəsilə informasiyanın ötürülməsinin müdafiə olunmasının təşkil edilməsi;
- İnternetə və kanarda olan şəbəkələrə açıq şəkildə qoşulmaq və bu şəbəkələrdən istifadə edənlər üçün təhlükəsizliyin təmin olunmasına imkanın yaradılması;
- Ən çox kommersiya məqsədi ilə istifadə edilən informasiya sistemlərinin müdəfiəsinin təmin edilməsi;
- Kommersiya məqsədli informasiya sistemlərində verilənlərin ötürülməsi üçün yararlı olan kanallarda müdafiənin yaradılması;
- Korporativ şəbəkələrin informasiya resurslarından istifadə etməklə personala müdafiə şəraitinin yaradılması;
- Şəbəkə vasitələrinin mərkəzləşdirilmiş şəkildə etibarlı idarə edilməsinin müdafiəsinin təşkil olunması.

ISTF təqdimatlarına əsasən elektron biznes sahəsində informasiya sistemlərinin təhlükəsizliyinin yaradılmasında birinci

və əsas mərhələ əlçatanlıq mexanizminin idarə edilməsi, onlardan istifadənin təşkili, onlara daxil olma imkanının yaradılması, təhlükəsiz kommunikasiya mexanizmi, virtual VPN şəbəkəsinın müdafiəsi və sairədir.

Mərkəzləşdirilmiş formada idarə edilən informasiya sistemlərinin təhlükəsizliyini əldə etmək üçün bütün informasiya müdafiə sisteminin idarə olunmasını və inteqrasiyasını yerinə yetirmək lazımdır.

Növbəti mərhələ nəzarət vasitələrinə istifadəçi əlçatanlığının ümumi strukturunun sistemə inteqrasiya edilməsi və sistemə birdəfəlik daxil olmaya (Single Sign On) ixtiyarın verilməsidir.

Əgər söhbət verilənlərin konfidensiallığından gedirsə, əslinə baxanda, antivirus müdafiəsi, audit vasitələri və hücumun müəyyən edilməsi təhlükəsizlik sisteminin inteqrasiya tamlığının yaradılmasını tamamlayır. Belə olan halda elektron-rəqəmsal imzanın və verilənlərin kriptoqrafik müdafiə olunması üçün avadanlıqların varlığı tələb edilir.

Elektron biznes üçün təhlükəsizlik sistemlərinin əsas funksional təşkiledicilərinin realizə olunması üçün müxtəlif üsullar və informasiyanın müdafiə vasitələrindən istifadə edilir. Bunlara aşağıdakılar aiddir:

- Müdafiə olunan kommunikasiya protokolu;
- Kriptoqrafiya vasitələri;
- Autentifikasiya və vəkalət vermə (ixtiyar vermə) mexanizmi;
- Şəbəkənin işçi yerlərinə daxil olmalara və ümumi istifadə şəbəkələrinə əlçatanlığın nəzarət vasitələri;
- Antivirus kompleksləri;
- Audit və hücumun aşkara çıxarılma proqramları;

- Istifadəçilərin sistemə daxil olmasının mərkəzləşdirilmiş şəkildə idarə edilməsi üçün vasitələrin varlığı;
- IP-şəbəkələrində, aşıq formada verilənlər paketinin və istənilən məlumat əlavələrin təhlükəsiz dəyişdirilməsi.

Korporativ sistemin bütün səviyyələrində kompleks müdafiə vasitələrinin tətbiq edilməsi informasiya təhlükəsizliyi sisteminin etibarlı və effektiv qurulmasına imkan verir.

TƏHLÜKƏSİZLİK SİYASƏTİ

Təhlükəsizliyin təşkil olunma siyasəti dedikdə informasiyanın müdafiəsinə yönəldilmiş və onunla birlikdə resursların assosiasiya olunmasının idarəetmə qərarlarının sənədləşdirilməsinin toplumu başa düşülür. Təhlükəsizlik siyasəti vasitələrdən ibarətdir və onların köməyilə kompüter informasiya sisteminin təşkil olunması fəaliyyəti həyata keçirilir. Ümumiyyətlə, təhlükəsizlik siyasəti kompüter mühitində istifadə edilir və təşkilatın spesifik tələbatını əks etdirir.

Adətən kompüter informasiya sistemləri (KİS) dedikdə müxtəlif xüsusiyyətli mürəkkəb kompleks başa düşülür və ya aparat və proqram təminatının arabir öz aralarında lazımi səviyyədə işləmələrinin uyuşa bilməməsi qəbul edilir. Bura kompüterlər, əməliyyat sistemləri, şəbəkə vasitələri, verilənlər bazalarını idarəetmə sistemləri, müxtəlif əlavələr aiddir. Bütün bu komponentlər (təşkiledicilər) özünəməxsus müdafiə vasitələrinə malikdir və bunların bir-biri ilə razılaşdırılması mütləqdir. Bu baxımdan da korporativ sistemlərin təhlükəsizliyinin təmin olunması təhlükəsizlik siyasətinin effektiv həyata keçirilməsində mühüm rol oynayır.

TƏHLÜKƏSİZLİK SİYASƏTİNİN ƏSAS ANLAYIŞLARI

Təhlükəsizlik siyasəti rəhbərliyin faydalı saydığı və seçdiyi informasiya təhlükəsizliyi sahəsində idarəetmə strategiyasını,

resursların miqdarını və onlara yanaşmanın ölçüsünü müəyyən edir.

Təhlükəsizlik siyasəti müəssisənin informasiya sistemi üçün real sayılan cəsarətin (və ya cürətin) təhlil edilməsinə əsaslanaraq qurulur. Belə olan halda cürət təhlil edilir, müdafiə strategiyası müəyyən olunur, informasiya təhlükəsizliyini təmin edən proqram tərtib edilir - bütün bunlar təhlükəsizlik siyasətidir. Tərtib olunan prioqrama uyğun olaraq resurslar ayrılır, bu resurslara məsul şəxslər seçilir, proqramın yerinə yetirilmə ardıcıllığı müəyyən edilir və s.

Müəssisənin təhlükəsizlik siyasəti müxtəsər struktura malik olmaqla yanaşı yüksək səviyyəli siyasətı dəstəkləməlidir. Yüksək səviyyəli siyasət daim nəzərdən keçirilməli və müəssisənin cari tələblərini ödəməklə yanaşı bu tələblərin ödənilməsinə təminat da verməlidir. Siyasət sənədi elə tərtib edilməlidir ki, konkret texnologiyadan asılı olmasın və bu sənədin tez-tez dəyişilməsinə ehtiyac duyulmasın.

Təhlükəsizlik siyasəti ilə tanış olmaq üçün bəzi müəssisənin hipotetiklik (fərziyyəyə əsaslanma) lokal şəbəkəsini nümunə kimi araşdırraq.

Təhlükəsizlik siyasəti adətən sənəd formasında tərtib olunur, bura problemin izahı, tətbiq olunma sahələri, müəssisənin tutduğu mövqe, rəhbərlikdə vəzifələrin bölüşdürülməsi və s. bölmələr daxil edilir.

Problemin izahı. Lokal şəbəkə çərçivəsində dövr edən informasiya kritik vacib sayılmalıdır. Lokal şəbəkə istifadəçiyə imkan verir ki, təhlükəsizliyi artıran hədələri proqramlardan və verilənlərdən müştərək istifadə etməklə minimuma endirsin. Odur ki, şəbəkəyə qoşulan hər bir kompüter istifadəçisi daha güclü müdafiəyə ehtiyac duyur. Bütün bunlar sənəd formasinda

informasiya təhlükəsizliyinin müəssisə daxilində yüksək səviyyədə həyata keçirilməsinə yardımçıdır.

İstifadə sahələri. Müəssisənin lokal şəbəkəsinə daxil olan bütün aparat, proqram və informasiya resursları cari siyasətin istifadə sahəsi hesab edilir. Siyasət şəbəkədə çalışan işçilərə, istifadəçilərə, subpodratçılara, tədarükçülərə və digərlərinə yönəldilmişdir.

Müəssisənin mövqeyi. Əsas məqsəd verilənlərin tamlığının, əlçatanlığının və konfidensiallığının, həmçinin aktuallığının və dolğunluğunun təmin edilməsidir. Məqsədə aşağıdakıları aid edirlər:

- Normativ sənədlərə uyğun olaraq təhlükəsizlik səviyyəsinin təmin edilməsi;
- Müdafiə tədbirlərinin seçilməsində məqsədəuyğun iqtisadiyyata əməl edilməsi (müdafiə xərcləri informasiya təhlükəsizliyinin pozulmasından yaranan zərəri keçməməlidir);
- Lokal şəbəkənin hər bir funksional sahəsində təhlükəsizliyin təmin edilməsi;
- İnformasiya və resurslardan istifadə edən istifadəçinin bütün fəaliyyətinin təhtəlhesabı (hesabat verməli olması) təmin olunmalı;
- Qeyd olunan informasiyanın təhlilinin təmin edilməsi;
- Təhlükəsizlik rejiminin düşünülmüş formada dəstəklənməsi üçün istifadəçiyə kifayət qədər informasiyanın təqdim olunması;
- Qəzadan sonra bərpa planının işlənib hazırlanması və şəbəkənin fasiləsiz iş rejiminin təmin edilməsi məqsədi ilə funksional sahələrdə kritik vəziyyətlərin nəzərə alınması;

- Təhlükəsizliyin uyğun qanunlarına və ümumtəşkilat siyasətinə əməl olunması.

Vəzifələrin və rolların bölünməsi. Öndə qeyd edilmiş məqsədin həyata keçirilməsi sözsüz ki, vəzifə sahiblərinin və şəbəkə istifadəçilərinin öhdəsinə düşür.

Bölmə rəhbərləri təhlükəsizlik siyasətinin vəziyyəti barədə məlumatları istifadəçiyə çatdırmaqla yanaşı onların bir-biri ilə əlaqə yaratmalarına da cavbabdehlik daşıyırlar.

Lokal şəbəkə administratorları şəbəkənin fasiləsiz işləməsini təmin etməklə bərabər təhlükəsizlik siyasətinin həyata keçirilməsi üçün lazım olan texniki tədbirlərin realizə edilməsinə cavabdehdirlər. Administratorların borcudur:

- Lokal şəbəkə avadanlıqlarının müdafiəsini təmin etsinlər və digər şəbəkələr ilə interfeys yaratsınlar;
- Operativ və effektiv şəkildə baş verənlərə, yavaş-yavaş azalan hədələrə reaksiya versinlər və servis administratorlarını müdafiənin pozulması barədə məlimatlandırsınlar;
- Şübhəli halları müəyyən etsinlər və gündəlik informasiyanı qeyd etməklə yanaşı fayl serverində baş verənləri təhlil etsinlər;
- Öz vəzifələrindən sui-istifadə etməsinlər;
- Zərərli proqram təminatından lokal şəbəkəni qorusunlar və zərərli kodu müəyyənləşdirməklə onu ləğv etsinlər;
- Fayl serverində saxlamaq şərti ilə informasiyanın surətini həmişə əldə etsinlər;
- Şəbəkədə aparat-proqram dəyişikliklərini həmişə izləsinlər;
- Şəbəkə resurslarına əlçatanlıq üçün identifikasiya və autentifikasiya prosedurlarının yerinə yetirilməsinə

təminat versinlər və istifadəçini qeydiyyat formasını doldurmaq üçün parol ilə təmin etsinlər;
- Lokal şəbəkənin etibarlı işləməsini həmişə yoxlasınlar və digər istifadəçilərin məlumatları əldə etmələrinə imkan verməsinlər.

Servis administratorları konkret serverlərə cavabdehdirlər. Onlar təhlükəsizlik siyasətini rəhbər tutmaqla müdafiənin təşkil edilməsinə məsuliyyət daşıyırlar. Onlar borçludur:
- Xidmət edilən obyektlərə istifadəçilərin daxil olmasını idarə etməyə;
- Operativ və effektiv şəkildə baş verənlərə, yavaş-yavaş azalan hədələrə reaksiya verməyə, hədələrin qarşısının alınmasına kömək etməyə, qayda pozucularını müəyyən etməklə onları cəzalandırmağa;
- Serverlərdə təhlil olunan informasiyanın surətini həmişə əldə etməyə;
- Qeydiyyatdan keçdikdən sonra istifadəşiyə parol verməklə yanaşı serverə daxil olma adını verməyə;
- Serverə aid olan informasiyanı gündəlik yoxlamağa və servisə ziyanverici proqram təminatının daxil olmasına maneçilik göstərməyə;
- Servisin etibarlı müdafdiə edilməsini mütəmadi yoxlamağa və qeyriqanuni istifadəçilərə servisdən istifadəyə üstünlük verməməli.

İstifadəçilər təhlükəsizlik siyasətinə uyğun olaraq lokal şəbəkə ilə işləyir, təhlükəsizlik aspektinin ayrı-ayrı hissələrinə cavabdeh olan, əmrlər verən şəxslərin verdiyi əmrlərə tabe olur, rəhbərliyi şübhəli vəziyyətlər haqqında daim məlumatlandırırlar. İstifadəçilər aşağıdakıları yerinə yetirməlidirlər:

- Qanunları bilməli və onları yerinə yetirməli, cari təşkilatda qəbul edilmiş təhlükəsizlik siyasətini qəbul etməli, konfidensiallığı təmin etmək üçün müdafiə mexanizmindən tutarlı səviyyədə istifadə etməli və istifadə etdikləri informasiyanın tamlığına məsuliyyət daşımalıdırlar;
- Faylların müdafiə mexanizmindən istifadə etməli və fayllardan lazımi şəkildə istifadə etməlidirlər;
- Keyfiyyətli paroldan bəhrələnməli, parolu tez-tez dəyişməli, parolu kağıza yazmamalı, digər şəxslərə parolu deməməlidirlər;
- Təhlükəsizliyin pozulması halları baş verdikdə, həmçinin digər şübhəli vəziyyət hiss etdikdə rəhbərliyi məlumatlandırmalıdırlar;
- Əgər lokal şəbəkə və ya servisdə zəiflik hiss olunarsa, ondan istifadə etməməli, özünə məxsus olmayan fayllardan istifadə etməməli və nəhayət, işlədiyi zaman ərzində başqalarının işləməsinə maneçilik etməməlidirlər;
- Başqasının adından istifadə etməklə iş görməməli, informasiyanın autentifikasiya və korrekt identifikasiya olması barədə məlumat verməlidirlər;
- Lazımlı informasiyanın ehtiyat üçün surətini almalı, həmişə informasiyanı sərt diskdə saxlamalıdırlar;
- Ziyanverici proqram təminatının iş prinsipini bilməli, onun sistemə daxil olma yollarını araşdırmalı, yayılmasına imkan verməməli, ziyanverici kod sistemə daxil olduqda təcili xəbardarlıq etməli, ziyanverici kodu tapmağa və ləğv etməyə çalışmalıdırlar;
- Fövqaladə hallarda özlərini necə aparmağı bacarmalı, baş vermiş qəzanı aradan götürməyi bacarmalıdırlar.

Sanksiya (bir müqavilə və ya qanunun yerinə yetirilməsini təmin edən şərt). Təhlükəsizlik siyasətinin pozulması lokal şəbəkəyə və onda dövr edən informasiyaya bağışlanmaz təsir edir. Odur ki, təhlükəsizliyin işçi personal tərəfindən pozulması operativ şəkildə rəhbərlik tərəfindən baxılmalıdır, lazım olan tədbirlər görülməli, əgər tələb olunarsa, işçi tutuğu vəzifədən azad edilməlidir.

Əlavə informasiya. Müəyyən qrup istifadəçi üçün əlavə sənədlərlə tanış olmağa ehtiyac yaranır. Bu sənədlərə təhlükəsizlik prosedurlarına və siyasətinə aid sənədlər, həmçinin rəhbərlik tərəfindən verilmiş xüsisi əmrlər və göstərişlər aiddir. Belə sənədlərin yaradılmasına əsasən böyük müəssisələrdə ehtiyac duyulur. Kiçik ölçülü müəssisələrdə müəyyən təhlükəsizlik siyasətini dəstəkləyən sənədlərin hazırlanmasına tələb yaranır. Bu baxımdan belə sənədlər qısa şəkildə tərtib edilir və həcmi bir-iki səhifədən artıq olmur.

İNFORMASİYA TƏHLİKƏSİZLİYİNİN TƏMİN EDİLMƏSİNDƏ İDARƏ ETMƏ TƏDBİRLƏRİ

İdarəetmə səviyyəsində həyata keçirilən tədbirlərin əsas məqsədi informasiya təhlükəsizliyi sahəsində görülən işlərin proqramının formalaşması və onların yerinə yetirilməsi üçün lazım olan resursların ayrılması, həmçinin görülən işlərin vəziyyətinə nəzarətin həyata keçirilməsidir. Proqramın əsasını çoxsəviyyəli təhlükəsizlik siyasətı təşkil edir. Təhlükəsizlik siyasəti informasiya aktivlərinin və resursların müdafiə edilməsinin təşkilinə kompleks yanaşmanı əks etdirir.

Təcrübə nöqteyi-nəzərindən təhlükəsizlik siyasətini üç səviyyəyə bölmək olar (bu barədə əvvəlki bölmələrdə qısa məlumat verilmişdi):

Yuxarı səviyyə. Təhlükəsizlik siyasətinin bu səviyyəsi müəssisəyə aid olan məsələlərin tam şəkildə həll edilməsinə toxunur. Məsələnin bu şəkildə həll edilməsi ümumi xarakter daşıyır və bu qərarlar qayda-qanuna görə müəssisənin rəhbərliyindən asılıdır.

Qərarlar özlərinə aşağıdakı elementləri aid edirlər:

- Müəssisənin informasiya təhlükəsizliyi sahəsində müəyyən məqsədə çatması üçün görəcəyi işlərin formalaşdırılması, bu məqsəd naminə ümumi istiqamətin müəyyənləşdirilməsi;
- İnformasiya təhlükəsizliyinin təmin edilməsi proqramına kompleks yanaşma və ya proqramın formalaşdırılması, proqramın yerinə yetirilməsində (inkişaf baxımından) məsul şəxslərin müəyyən edilməsi;
- Qanunların və qaydaların yerinə yetirilməsi üçün material bazasının yaradılması;
- İdarəedicilik qərarlarının həlli baxımından proqram təminatının yerinə yetirilmə məsələsinin dürüst ifadə edilməsi.

Yuxarı səviyyənin təhlükəsizlik siyasəti informasiya təhlükəsizıliyi siyasətinin tamlığını, əlçatanlığını və konfidensiallığını dürüst ifadə edir. Əgər müəssisə kritik (tənqidi yanaşılmış) vacib verilənlərin dəstəklənməsinə cavabdehlik daşıyırsa, birinci planda həmin verilənlərin tamlığı dayanır. Satış ilə məşğul olan təşkilat üçün göstərilən xidmətin qiyməti və xidmət barədə informasiyanın aktuallığı vacibdir. Bununla yanaşı satış təşkilatını maraqlandıran məsələlərdən biri potensial alıcıların maksimal sayıdır. Qayda-qanun ilə işləyən təşkilat birinci növbədə informasiyanın konfidensiallığı barədə düşünməlidir, daha döğrusu qeyriqanuni əlçatanlığın müdafiə edilməsinə çalışmalıdır.

Yuxarı səviyyənin təhlükəsizlik siyasəti öz təsir dairəsini dəqiq müəyyənləşdirməlidir. Yuxarı səviyyəyə ancaq müəssisənin bütün kompüter sistemi deyil, həm də əməkdaşların evdə istifadə etdikləri kompüterlərin də qoşulması mümkündür. Bunun üçün yuxarı səviyyə siyasəti onların istifadə edilməsinin bəzi aspektlərini nizama salmalıdır. Bəzən elə bir vəziyyət yaranır ki, yuxarı səviyyənin təhlükəsizlik siyasəti dairəsinə ancaq daha mühüm sistemlər qoşulurlar.

Yuxarı səviyyənin təhlükəsizlik siyasətində təhlükəsizlik proqramlarını işləyib hazırlayan məsul şəxslərin vəzifələri müəyyən edilməlidir, çünki bu şəxslər həmin proqramları həyaya keçirirlər.

Yuxarı səviyyənin təhlükəsizlik siyasəti qanunaitaətli və intizama riayət edən üç aspekt ilə əlaqəlidir. Birincisi, müəssisə mövcud qanuna əməl etməldir. İkincisi, təhlükəsizlik proqramını işləyib hazırlayan məsul şəxsin fəaliyyəti nəzarətdə saxlanılmalıdır. Üçüncüsü, müəssisədə təltif etmə (və ya cəzalandırma) üsulundan istifadə etməklə personalın lazımi səviyyədə tapşırığı yerinə yetirmə intizamına riayət etməsi təmin edilməlidir.

Orta səviyyə. Bu səviyyədə müəssisə tərəfindən istismar olunan müxtəlif sistemlər üçün əsas sayılan təhlükəsizlik siyasəti informasiya təhlükəsizliyi ilə bağlı ayrı-ayrı aspektləri müəyyən edir.

Orta səviyyənin təhlükəsizlik siyasəti informasiya təhlükəsizliyinin hər bir aspekt üçün aşağıdakı momentləri müəyyən etməldir:

- *Aspektin izahı* – müəssisənin mövqeyi bəzən kifayət qədər ümumi şəkildə formalaşır, çünki müəssisə cari aspektdə bu məqsədlərin yerinə yetirilməsində maraqlıdır;

- *Tətbiq sahələri* – təhlükəsizlik siyasətinin harada, nə vaxt, necə, kimə və nəyə münasibətdə tətbiq ediməsinin təsnifləşdirilməsini yerinə yetirmək;
- *Vəzifələr və rollar* – tərib olunmuş sənəd təhlükəsizlik siyasətinin həyata keçirilməsinə cavabdeh olan məsul şəxs haqqında informasiya daşımalıdır;
- *Qadağa* – təhlükəsizlik siyasəti qadağan olunmuş fəaliyyət haqqında ümumi formada izahata malik olmaqla yanaşı onu pozan haqqında cəzalari da göstərməlidir;
- *Əlaqə nöqtəsi* – müəyyən hadisələr baş verdikdə hara müraciət olunması aydınlaşdırılmalı, göstərilən yardım və əlavə informasiya izah edilməlidir. Adətən "əlaqə nöqtəsi" kimi məsul şəxs cavabdehdir.

Aşağı səviyyə təhlükəsizlik siyasəti konkret servisə əsaslanır. Səviyyə özündə iki aspekti birləşdirir – məqsəd və ona çatmaq üçün qanunları. Odur ki, onları realizasiya ilə bağlı suallardan ayırmaq çətindir. Öndə araşdırılan səviyyələrdən fəqli olaraq aşağı səviyyəli siyasət təvsilatı ilə baxılmalıdır, yəni səviyyə aşağıdakı suallara cavab verməldir:

- Servis tərəfindən dəstəklənən obyektlərə daxil olmağa kimin hüquqi vardır;
- Hansı şəraitdə verilənləri modifikasiya etmək (şəkilini dəyişmək) və oxumaq olar;
- Uzaqdan servisə daxil olma necə təşkil olunmuşdur.

Aşağı səviyyənin təhlükəsizlik siyasəti tamlıq, əlçatanlıq və konfidensiallıq baxımından irəli gəlir və bu siyasət onların yerinə yetirilməsinə maneçilik etməməlidir. Ümumi halda servis bunlar arasında əlaqə yaratmalı və onlarsız fəaliyyət göstərməməlidir.

Məqsəddən aydın olur ki, təhlükəsizlik qanunlarına kim və hansı şəaitdə əməl etməlidir. Qanunlar nə qədər diqqətlə hissə-hissə araşdırılarsa, bir o qədər də onların proqram-texniki baxımından yerinə yetirilməsini dəstəkləmək mümkündür. Adətən formal da olsa, obyektlərə əlçatanlıq qanunları təqdim olunur.

MÜƏSSİSƏNİN TƏHLÜKƏSİZLİK SİYASƏTİNİN STRUKTURU

Əksər təşkilatlar üçün təhlükəsizlik siyasəti sözün əsl mənasında vacibdir. Siyasət müəssisənin təhlükəsizliyə münasibətini müəyyən edir və özünəməxsus aktivlərin və resursların qorunmasının təşkilinə imkan yaradır. Təhlükəsizlik siyasəti ilə bağlı təhlükəsizlik vasitələrin və prosedurların müəyyən edilməsi, onların yerinə yetirdikləri rollar və müəssisədə işləyən əməkdaşların məsuliyyəti (təhlükəsizliyə əməl etmə baxımından) müəyyən edilir.

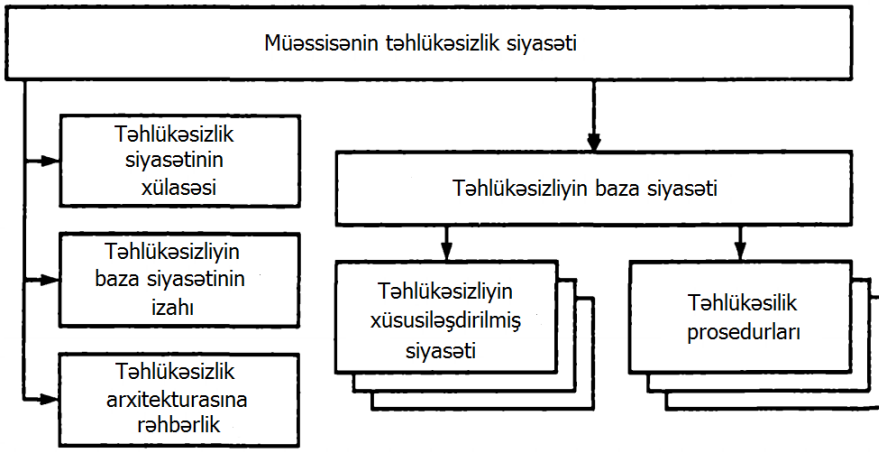
Adətən müəssisədə təhlükəsizlik siyasəti aşağıdakıları yerinə yetirməlidir:

- Baza təhlükəsizlik siyasətini;
- Xüsusiləşdirlmiş təhlükəsizlik siyasətini;
- Təhlükəsizlik prosedurlarını.

Müəssisənin təhlükəsizlik siyasətinin müddəaları aşağıdakı sənədlərdə əks olunur:

- *Təhlükəsizlik siyasətinin xülasəsi* – təhlükəsizlik siyasətinin məqsədini və strukturunu açıqlayır, kimin nəyə cavab verməsini müəyyənləşdirir, edilmiş dəyişikləri vaxt çərçivəsində müəyyən edir. Müəssisənin miqyasından asılı olaraq təhlükəsizlik siyasəti az və ya çox bölmələrdən ibarət ola bilər;

- *Təhlükəsizlik baza siyasətinin izahı* – qadağa qoyulmuş və icazə verilmiş fəaliyyətin müəyyən edilməsi, həmçinin təhlükəsizlik arxitekturasının həyata keçirilmə çərçivəsində idarəetmə vasitələrinin varlığı;
- *Təhlükəsizliyin arxitekturası baxımından rəhbərlik* – şəbəkənin təşkil ediməsində istifadə olunan təhlükəsizlik mexanizmi arxitekturasının tərkib hissəsinin həyata keçirilməsinin izahı (şəkil 17).



Şəkil 17. Müəssisənin təhlükəsizlik siyasətinin strukturu

Qeyd etmək lazımdır ki, təhlükəsizlik siyasətinin əsas komponenti baza təhlükəsizlik siyasəti hesab edilir.

TƏHLÜKƏSİZLİYİN BAZA SİYASƏTİ

Təhlikəsizliyin baza siyasəti müəssisənin informasiyanı neçə təhlil etməsini, informasiyaya kimin əlçatan olmasını, buna necə nail olmağı müəyyənləşdirir.

Get-gedə azalan təhlikəsizliyin baza siyasəti təhlükəsizlik sisteminin yaradılması üçün yararlı olan işlərin bütünlükdə deyil, daim və ardıcıl yerinə yetirilməsinə imkan verir. Baza siyasəti təhlükəsizlik siyasəti ilə istənilən vaxt bütünlükdə tanış olmağa və müəssisədə təhlükəsizliyin cari vəziyyətini araşdırmağa şərait yaradır.

Təhlükəsizlik siyasətinin tərkibi və strukturu şirkətin məqsədindən və həcmindən asılıdır. Adətən müəssisənin baza siyasətini müəssisəyə xüsusi hazırlığı olan siyasətçilər dəstəsini dəvət etməklə və təhlükəsizlik tədbirlərini həyata keçirməklə yerinə yetirirlər.

XÜSUSİLƏŞDİRİLMİŞ TƏHLÜKƏSİZLİK SİYASƏTİ

Hal-hazırda onlarla xüsusiləşdirilmiş siyasət mövcuddur və onlardan istər kiçik ölçülü, istərsə də böyük ölçülü müəssisələr istifadə edə bilərlər. Bəzi siyasətlər hər bir müəssisə tərəfindən istifadə edilə bilər, bəziləri isə müəyyən xüsusiyyətə malik müəssisələr üçün nəzərdə tutulmuşdur.

Xüsusiləşdirlmiş təhlükəsizlik siyasətinin xüsusiyyətlərini nəzərə almaqla təhlükəsizliyi iki qrupu bölmək olar:

- Müəyyən sayda istifadəçinin marağına toxunan siyasət;
- Konkret texnika sahəsi ilə bağlı olan siyasət.

Müəyyən sayda istifadəçinin maraqlarına toxunan xüsusiləşdirilmiş siyasətə aşağıdakılar aiddir:

- Əlçatanlıq siyasətindən istifadə edilməsi;
- Uzaqda yerləşmiş şəbəkə ehtiyatlarına əlçatanlıq siyasəti;
- İnformasiyanın müdafiə siyasəti;
- Parolun müdafiə siyasəti və s.

Konkret texniki sahə ilə bağlı olan xüsusiləşdırılmış siyasətə daxildir:

- Şəbəkələrarası ekranların quruluşunun siyasəti;
- Kriptoaçarların şifrələnməsi və idarəedilməsi siyasəti;
- Virtual müdafiə olunan VPN şəbəkə təhlükəsizliyi siyasəti;
- Naqilsiz şəbəkə ilə təchiz edilmişlərin siyasəti və başqaları.

Xüsusiləşdirilmiş siyasətlərdən bəzilərini aydınlaşdıraq.

Əlçatanlıq ilə istifadə olunan siyasət. Siyasətin məqsədi kompüter avadanlıqlarından və şirkətlərin servislərindən təhlükəsiz istifadə edilməsi üçün standart normaların müəyyən edilməsi, həmçinin əməkdaşların onlara məxsus informasiyanı qoruması və korporativ resursların təhlükəsizliyini təmin etməsidir. Kompüter avadanlıqlarından və servislərdən düzgün istifadə etmədikdə şirkət müəyyən risklər (virusların hücumu, şəbəkə sisteminin və servisin etibardan düşməsi və s.) ilə qarşılaşır.

Şirkətin əməkdaşları, məsləhətçilər, müvəqqəti işə qəbul edilmiş qulluqçular və şirkətin digər işçiləri, həmçinin başqa müəssisələrin əməkdaşları əlçatanlıq siyasətindən istifadə edirlər. Əlçatanlıq siyasəti sonuncu istifadəçi üçün nəzərdə tutulmuşdur və ona hansı hərəkəti edib-etməməsinə göstəriş verir.

İstifadənin əlçatanlıq siyasəti aşağıdakıları müəyyən edir:

- İstifadəçinin istənilən informasiyanı onun kompüterində saxlandıqdan sonra müdafiə etməsi üçün məsuliyyət daşıması;
- İstifadəçiyə adi olmayan faylların, amma onlardan istifadə etməsinə icazəsi olduğu üçün oxumasına, surətinin almasına səlahiyyətinin olması;
- Veb-əlçatanlıq və elektron poçtdan istifadəyə icazə imkanının verilməsi.

Təhsil və dövlət müəssisələri üçün əlçatanlıq siyasəti sadəcə olaraq məcburidir.

Əlçatanlıq siyasəti üçün xüsusi format yoxdur. Əlçatanlıq siyasəti yüksək ixtisaslı peşəkarlar tərəfindən servisə uyğun işlənib hazırlanmışdır.

Uzaqlaşdırılmış əlçatanlıq siyasəti. Siyasətin məqsədi şirkətin şəbəkəsi ilə istənilən host arasında təhlükəsiz əlaqənin standart normalara uyğun yaradılmasıdır. Standart normalar şirkətin gördüyü işlər zamanı ona vurulacaq ziyanı minimuma endirmək üçündür. Ziyana şirkətin intellektual mülkiyyəti, şirkətin imicinin təhrif olunması, şirkətin daxilində baş verə biləcək çəkişmələr və s. aiddir.

Siyasət bütün əməkdaşlara, mal göndərənə (tədarükçiyə), şirkətin agentlərinə, şirkətdə istifadə olunan kompüterlərə və ya işçi stansiyalara aiddir.

Uzaqlaşdırılmış əlçatanlıq siyasəti aşağıdakıları yerinə yetirməlidir:

- Daxili şəbəkə ilə uzaqlaşdırılmış şəbəkənin birləşmə üsulunu müəyyən etməklə yanaşı qeyd etmək;
- Əhəmiyyətli olan iri şirkətdə şəbəkənin necə paylanmasını təyin etmək;
- Daxili resurslara əlçatanlıq üsulunun imkan daxilində paylanmasını təmin etmək.

Uzaqlaşdırılmış əlçatanlıq siyasəti müəyyən etməlidir:

- Uzaqlaşdırılmış obyekt üçün hansı üsul icazə verilir;
- Uzaqlaşdırımış obyektin qəbul edəcəyi verilənlərin məhdudlaşdırılması;
- Kim uzaqlaşdırılmış obyektə malik ola bilər.

Müdafiə olunan obyekt ciddi şəkildə nəzarətdə saxlanılmalıdır. Nəzərə almaq lazımdır ki, yoxlamadan keçmiş insanlar informasiyaya malik ola bilərlər. Şirkətin əməkdaşları özlərinə məxsus logini və parolu heç kimə verə bilməzlər (hətta ailə üzvlərinə də). Uzaqlaşdırılmış obyektin idarə edilməsi sadə olmalı və istifadə zamanı səhv yaranmamalıdır.

Əlçatanlığa nəzarəti birdəfəlik parol ilə yerinə yetirmək məsləhətdir. Bununla yanaşı istifadə edilən bütün avadanlıqlara müasir antivirus proqramı yüklənməlidir. Bu tələbat şirkətin fərdi kompüterlərinə də aiddir.

Şirkətin istənilən əməkdaşı hazırki siyasəti pozduqda rəhbərlik tərəfindən cəzalandırılmalıdır (işdən azad edilə də bilər).

TƏHLÜKƏSİZLİK PROSEDURLARI

Təhlükəsizlik proseduru təhlükəsizlik siyasətinə lazımlı və əsas əlavə kimi hesab edilir. Təhlükəsizlik siyasəti nəyin müdafiə edilməsini və müdafiə qanunlarından hansıların əsas olmasını müəyyən edir. Təhlükəsizlik prosedurları resursları (siyasəti yerinə yetirən mexanizmi, daha doğrusu təhlükəsizlik siyasətini necə həyata keçirməyi) necə müdafiə etməyi müəyyən edir.

Əslində təhlükəsizlik prosedurları operativ məsələləri addım ba addım necə həll etmək üçün təlimatdır. Prosedurun

bir həssəsi siyasəti real fəaliyyətə çevirmək üçün alətdir. Məsələn, parolların formalaşdırılması siyasəti parolların qurulması qanunlarıdır, bura parolu necə müdafi etmək, onu tez-tez necə dəyişmək və s. aiddir. Parolların idarə edilməsi proseduru yeni parolun yaranmasını izah edir, bununla yanaşı kritik vəziyyətdə parolu dəyişən zaman ona təminat da verir.

Təhlükəsizlik ilə bağlı olan bir çox prosedurlar istənilən bölmədə standart vəsaitlər olmalıdır. Məsələn, ehtiyyat üçün surəti alınmış material və sistemdən kanar onun müdafiə olunmaqla yaddaşda saxlanılması, loginin və istifadəçi parolunun arxivləşdirilməsi, istifadəçi işdən azad olduqda ona məxsus parolun ləğv edilməsi və s. halları nümunə kimi göstərmək olar.

Aşağıda hər bir təşkilat üçün əsas sayılan təhlükəsizlik prosedurları verilmişdir.

Baş vermiş hadisələrə reaksiya verən prosedurlar bir çox müəssisələr üçün əsas təhlükəsizlik vasitələri sayılır. Müəssisə onun şəbəkəsinə kanardan müdaxilə edildikdə və ya bədbəxt hadisə baş verdikdə ciddi ziyana düşmüş olur.

Belə prosedurları bəzən *hadisələrin təhlili proseduru* və ya *baş vermiş hadisəyə reaksiya verən prosedur* adlandırırlar. Təcrübə göstərir ki, baş vermiş qayda-qanun pozuntularına cavab vermək mümkün deyil, amma bəzi pozuntular vardır ki, onlar baş verməmiş qarşısını almaq vacibdir. Məsələn, şəbəkə portlarının skanerə edilməsi, "xidmətdən imtina" hücumunun vaxtında yoluna qoyulması, hostun nüfuzdan salınması, qeyriqanuni əlçatanlıqla mübarizə və s. nümunə göstərilə bilər.

Prosedur aşağıdakıları müəyyən edir:

- Reaksiya vermə komandası üzvlərinin vəzifələri;
- Hansı informasiyanı qeyd etmək və izləmək;

- Normadan kanarlaşan tədqiqatların təhlili və qəflətən edilən hücumların araşdırılması;
- Kimi və nə vaxt xəbərdar etmək;
- Kim informasiyanı kanara yaya bilər və bunun üçün nə etməlidir;
- Yerinə yetiriləcək təhlillərə kim rəhbərlik etməlidir və burada kimlərin iştirakı vacibdir.

Reaksiya vermə komandasına şirkətin vəzifəli şəxsləri, marketinq meneceri (mətbuat ilə əlqə qurmaq üçün), sistem və şəbəkə inzibatçıları və qanun keşiyində dayanan orqanların nümayəndələri daxil olmalıdır. Prosedur bunların hansı ardıcıllıqla çağırılmasını müəyyən etməlidir.

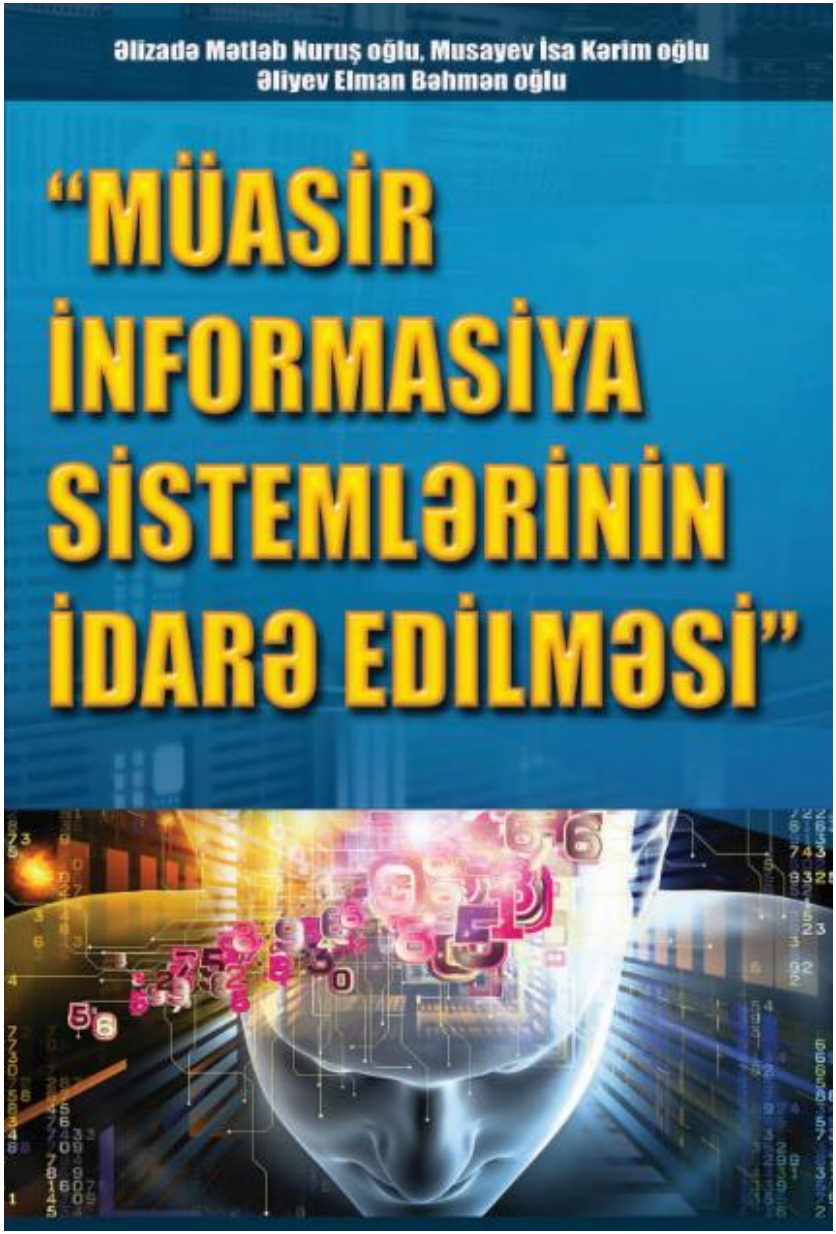
Xarici görünüşü idarəetmə prosedurları adətən ya korporativ səviyyədə, ya da ki, bölmələr səviyyəsində müəyyən edilir. Prosedura müəssisədə sənədləşmə prosesində və bütün səviyyələrdə qəbul edilmiş konfiqurasiyanın (xarici görünüşün) dəyişməsinə ehtiyac duyulduqda həyata keçirilir. Prinsipcə yaradılmış mərkəzi qrup xarici görünüşün dəyişməsi ilə bağlı sualları nəzərdən keçirməli və lazım olan qərarı qəbul etməldir.

Xarici görünüşü idarəetmə proseduru aşağıdakıları müəyyən edir:

- Proqram və aparat təminatının konfiqurasiyasının dəyişməsinə kim cavabdehdir;
- Yeni proqram və aparat təminatını kim testdən keçirməli və instalizasiya etməlidir;
- Proqram və aparat təminatının sənədləşdirilməsində dəyişiklik necə yerinə yetirilməlidir;
- Proqram və aparat təminatının dəyişdirlməsi barədə kim məlumatlı olmalıdır.

Xarici görünüşü idarəetmə proseduru vacibdir, çünki edilmiş dəyişikliklər auditin imkanlarını müəyyən edir; istifadə

edilən sistemin sənədləşdirilməsinə imkan verir; edilmiş dəyişikliyin elə şəkildə yerinə yetirilməsinə şərait yaradır ki, dəyişiklik digərlərinə maneçilik törətməsin.


Əlizadə Mətləb Nuruş oğlu, Musayev İsa Kərim oğlu
Əliyev Elman Bəhmən oğlu
"MÜASİR İNFORMASİYA SİSTEMLƏRİNİN İDARƏ EDİLMƏSİ"

İNFORMASİYA TƏHLÜKƏSİZLİYİ STANDARTLARI

İnformasiya təhlükəsizliyi problemləri ilə o vaxt məşğul olmağa balanıldı ki, kompüter istifadəçisi üçün qiymətli olan verilənləri təhlil etməkdən ötrü təhlükəsizlik bir alətə çevrildi. Kompüter şəbəkələrinin imkişafı və elektron xidmətlərə müraciətlərin artması nəticəsində informasiya təhlükəsizliyi mühitində yaranan problemlər ciddi şəkildə kəskinləşdi. Yaranmış problemlərin həll edilməsi həm ixtiraçılar üçün, həm də ki, informasiya texnologiyaları istifadəçiləri üçün aktuallığa cevrildi.

İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ STANDARTLARIN ROLU

İnformasiya təhlükəsizliyi standartlarında əsas məsələ informasiya texnologiyaları məhsullarının təsnif edilməsində ekspertlər, istehsalçılar və istehlakçılar arasında qarşılıqlı əlaqənin yaradılmasinin əsasini qoymaqdir. Hər bir qrupun informasiya təhlükəsizliyi probleminə öz maraqları və özünəməxsus baxışları vardır.

İstehlakçılar onların ehtiyaclarına cavab verən və onların problemlərini həll edən məhsulu əsaslı şəkildə seçmək üçün müəyyən metodikaya maraqlıdırlar. Bunun üçün onlara təhlükəsizliyi qiymətləndirən qiymət şkalasının varlığı vacibdir. İstehlakçı öz tələblərini istehsalçının qarşısında formalaşdırmaq üçün müəyyən alətə də möhtacdır. Bu zaman istehlakçını sonuncu məhsulun hansı üsullarla hazırlanması və ya

gələcəkdə hansı uğurlar qazanacağı deyil, ancaq onun hansı xüsusiyyətləri və xarakteristikaları əks etdirəcəyi maraqlandırır. Əfsuslar olsun ki, bir çox istehlakçılar başa düşmürlər ki, təhlükəsizlik tələbləri ilə funksional tələblər mütləq şəkildə bir-birinə ziddir (iş şəraitinin əlverişli olması, sürətlə fəaliyyət göstərməsi və i.a.), bu ziddiyyət onlar arasındakı uyğunluğun birliyinə məhdudiyyət qoyur, geniş yayılmış və müdafiə olunmayan tətbiqi proqram vasitələrindən imtina etməyə məcbur edir.

İstehsalçılar öz məhsullarının müqayisə edilməsi üçün standartlara, onların xüsusyyətlərini obyektiv qiymətləndirmək üçün sertifikatlaşdırma prosedurları mexanizminə, təhlükəsizliyin təmin edilməsi üçün müəyyən standartlar toplumuna ehtiyac düyürlar. Bunlardan istifadə edən istehsalçılar sifarişçinin konkret məhsula fantaziyasını məhdudlaşdırır, onu bu topluma aid olan tələbləri seçməyə məcbur edir. İstehsalçı baxımından təhlükəsizlik tələbləri maksimal konkret olmaqla yanaşı, bu və ya digər vəsaitələrin, mexanizmlərin, alqoritmlərin və i.a. tətbiqinin nizama salınmasına da zəruri olmalıdır. Bunlardan əlavə, tələblər informasiyanın mövcud olan təhlil olunma paradiqmasına (sözlərin hallara salınması və ya dəyişməsi formalarını göstərən cədvəl), hesablama sistemlərinin arxitekturasına və informasiya məhsullarının yaradılma texnologiyasına əks olmamalıdır. Belə yanaşmanı hakim mövqe tutan kimi (əsas yer tutan, üstünlük təşkil edən) saymaq düzgün deyil, çünki belə yanaşma istifadəçinin ehtiyacını nəzərə almasada, onun tələblərini mövcud sistemlərin və texnologiyaların istifadəsi baxımından müdafiə edilməsinə cəhd göstərir.

Təsnifat üzrə ekspertlər və sertifikatlaşdırma üzrə mütəxəssislər standarta bir alət kimi baxırlar. Alət onlara

informasiya texnologiyaları məhsulları ilə təmin olunmaqla təhlükəsizlik səviyyəsini qiymətləndirməyə imkan verir. Təsnifat üzrə ekspertlər ikili vəziyyətdə dururlar: bir tərəfədən onlar istehsalçılar kimi baş sındırmadan, konkret məhsula tətbiq olunan dəqiq və sadə kriteriyalara maraqlıdırlar, digər tərəfdən isə onlar istifadəçilərə məhsulun onların ehtiyaclarını ödədiyinə əsaslandırılmış cavab vermədirlər.

Beləliklə, informasiyanın təhlükəsizliyi standartı qarşısında sadə məsələ durmur. Standart üç baxış nöqtəsini nəzərə almaqla bütün tərəflərin effektiv münasibət mexanizmini yaratmalıdır, çünki tərəflərdən birinin tələblərinin məhdudlaşdırılması onlar qarşısında qoyulmuş ümumi məsələnin həll edilməsinə, yəni informasiya təhlilini müdafiə etmə sisteminin yaradılmasına imkan verməyəcəkdir.

Belə standartlara ehtiyac çoxdan yaranmışdır və bu istiqamətdə müəyyən inkişafla bağlı nəticədə əldə olunmuşdur (bütün bunlar 1990-cı illərdə hazırlanmış sənədlərdə öz əksini tapır). İlk və müəyyən qədər tanınmış sənəd "Narıncı kitab" sayılır (kitabın üzlüyü narıncı rəngdədir). "Kompüter sistemlərinin təhlükəsizlik kriteriləri" adlanan sənəd Amerika Birləşmiş Ştatlarının Müdafiə Nazirliyinə aiddir. Sənəddə 4 təhlükəsizlik səviyyəsi – D, C, B və A müəyyən olunmuşdur. D səviyyəsindən A səviyyəsinə keçidə sərt tələblər irəli sürülür. C və B səviyyələri siniflərə (C1, C2, B1, B2, B3) bölünür. Sistemin sertifikatlaşdırma proseduru nəticəsində müəyyən sinifə aid edilməsi üşün, onun müdafiə edilməsi müəyyən tələbləri ödəməlidir. İnformasiya təhlükəsizliyi standartına digər əsas sənədlər: "Rusiya Dövlət Komissiyasının rəhbər sənədi", "İnformasiya texnologiyaları təhlükəsizliyinin Avropa kriteriləri", "ABŞ informasiya texnologiyaları təhlükəsizliyinin federal

kriteriləri", "Kompüter sistemləri təhlükəsizliyinin Kanada kriterilər" və s. sənədləridir.

Son illərdə müxtəlif ölkələrdə standartların yeni nəsli yaranmışdır. Onlar şirkətlərin informasiya təhlükəsizliyi ilə bağlı sualların praktiki olaraq həll edilməsinə həsr edilmişdir. Bu sənədlərə nümunə kimi informasiya təhlükəsizliyinin idarə edilməsinə aid beynəlxalq satandartları (ISO 15408, ISO 17799 və başqaları) göstərmək olar. İstehsalçılara bu sənədlərdəki əsas məsələləri təhlil etmək, onların qoyduğu tələbləri və kriteriləri araşdırmaq, onların praktikada istifadəsinin effektivliyini müəyyən etmək və s. tutarlı səviyyədə öyrənmək məsləhətdir.

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN BEYNƏLXALQ STANDARTI

Beynəlxalq və milli standartlara uyğun olaraq informasiya təhlükəsizliyinin təmin edilməsi istənilən şirkətdə aşağıdakıları nəzərdə tutur:

- Kompüter sistemlərində informasiya təhlükəsizliyinin təmin edilməsinin məqsədi;
- İnformasiya təhlükəsizliyini idarəetmə sisteminin effektivliyinin yaradılması;
- Qoyulmuş məqsədlərə uyğun informasiya təhlükəsizliyinin qiymətləndirilməsi üçün ətraflı hazırlanmış keyfiyyət və kəmiyyət göstəriciləri cəminin hesablanması;
- İnformasiya təhlükəsizliyinin təmin edilməsi üçün alətlərin tətbiq edilməsi və onun cari vəziyyətinin qiymətləndirilməsi;

- İnformasiya aktivlərinin müdafiə edilməsini obyektiv qiymətləndirməyə imkan verən təhlükəsizliyi idarəetmə üsulundan istifadə və şirkətin informasiya təhlükəsizliyinin idarə olunması.

İnformasiyanın müdafə olunması sahəsində daha çox məşhur olan beynəlxalq satandartları gözdən keçirək.

ISO/IEC 17799:2002 (BS 7799:2000) STANDARTLARI

Beynəlxalq ISO/IEC 17799:2002 (BS 7799:2000) standartı "İnformasiya təhlükəsizliyi - İnformasiya texnologiyalarının idarə edilməsi" ("Information technology – Information security management") informasiyanın müdafiə edilməsi sahəsində tanınmış məşhur standartdır. Standart İngiltərə standartı BS 7799-1:1995 "İnformasiya təhlükəsizliyinin idarə edilməsinə praktiki tövsiyyə" ("Information security management – Part 1:Code of practice for information security management") standartının birinci hissəsini əsas tutaraq yardılmışdır və kompüter informasiya sistemlərinin informasiya təhlükəsizliyi standartlarının yeni nəsilinə aiddir.

Standartın cari (növbəti) ISO/IEC 17799:2000 (BS 7788-1:2000) versiyası müəssisələrin və təşkilatların informasiya təhlükəsizliyinin təmin edilməsinin aşağıdakı aktual suallarını əhatə edir:

- İnformasiya təhlükəsizliyinin təmin edilməsinin zəruriliyi;
- İnformasiya təhlükəsizliyinin müəyyən edilməsi və əsas anlayışları;
- Şirkətlərin informasiya təhlükəsizliyi siyasəti;
- Müəssisələrdə informasiya təhlükəsizliyinin təşkil edilməsi;

- Korporativ informasiya resurslarının (vəsaitlərinin) idarə edilməsi və təsnifatı;
- İnformasiya təhlükəsizliyi və kadr menecmenti;
- Fiziki təhlükəsizlik;
- Korporativ informasiya sistemləri təhlükəsizliyinə inzibatçılığın edilməsi;
- Əlçatanlığın idarə edilməsi;
- Korporativ informasiya sistemlərinin yaradılması, istismarı və müşayiət edilməsi baxımından təhlükəsizlik tələblərin qoyulması;
- Şirkətin informasiya təhlükəsizliyi baxımından biznes-proseslərinin idarə edilməsi;
- Şirkətin informasiya təhlükəsizliyi daxili auditi.

Standartın ikinci hissəsi BS 7799-2:2000 "İnformasiya təhlükəsizliyinin idarə edilməsinin təsnifatı" ("İnformation security management – Part 2: Specification for information security management systems") korporativ informasiya təhlükəsizliyinin idarə etmə sisteminin funksional imkanlarını cari standartın birinci hissəsinin tələblərinə uyğun onların yoxlanması baxımından müəyyən edir. Bu standartın əsasnaməsinə uyğun olaraq korporativ informasiya sistemindəki audit proseduru da normaya salınır.

İnformasiya təhlükəsizliyinin idarə edilməsinə verilən əlavə tövsiyələri İngiltərə standartlar institutu (BSI – British Standards Institution) tətəfindən 1995-2003-cü illərdə hazırlanmış təlimatlarda tapmaq mümkündür (məsələn, "İnformasiya təhlükəsizliyinin idarəetmə problemlərinə giriş", "BS 7799 standartının tələblərinə uyğun sertifikatlaşdırma imkanları" və s.

2002-ci ildə ISO 17799 (BS 7799) standartı yenidən işlənildi və standarta yeni əlavələr edildi. Mütəxəssislərin

fikirincə standarta olunmuş əlavələr şirkətin informasiya müdafiə mədəniyyətini yüksəltməklə yanaşı bu sahədə aparıcı dövlət və kommersiya strukturuna daxil olan müəssisələrin də fəaliyyətində müsbət nəticələr verəcəkdir.

BSI ALMAN STANDARTI

ISO 177999 standartından fərqli olaraq "Baza səviyyəsində müdafiə üçün informasiya texnologiyalarının müdafiə olunmasına rəhbərlik" alman standartı şirkətin informasiya təhlükəsizliyinin idarə edilməsində şəxsi sualların müfəssəl baxılmasına həsr olunmuşdur.

BSI alman standartında aşağıdakılar təqdim olunur:

- İnformasiya təhlükəsizliyinin idarə edilməsinin ümumi metodikası (informasiya təhlükəsizliyi sahəsində menecmentin təşkil edilməsi, idarəçiliyin həyata keçirilməsi metodologiyası);
- Müasir informasiya texnologiyalarının təşkiledicilərinin təsvir edilməsi;
- İnformasiya təhlükəsizliyi rejimininin təşkil edilməsinin əsas təşkiledicilərinin (komponentlərinin) təsvir edilməsi (verilənlərin texniki və təşkilatı səviyyədə müdafiəsi, fövqəladə hallarda fəaliyyətin planlaşdırılması, biznesin kəsilməz fəaliyyətinin dəstəklənməsi);
- Obyektlərin informatlaşdırılma xarakteristikaları (binalar, otaqlar, kabel şəbəkələri, nəzarət zonaları);
- Şirkətlərin əsas informasiya aktivlərinin xarakteristikaları (aparat və proqram təminatı, DOS ailəsinə daxil olan əməliyyat sistemlərinin rəhbərliyi altında işləyən işçi stansiyalar və serverlər, Windows və UNIX);

- Müxtəlif şəbəkə texnologiyasına əsaslanan kompüter şəbəkələrinin xarakteristikaları (məsələn, Novell NetWare şəbəkəsi, UNIX və Windows şəbəkələri);
- Təchiz edən aparıcı şirkətlərin telekommunikasiya avadanlıqlarının passiv və aktiv xarakteristikaları (məsələn, Cisco Systems);
- Nəzarət tədbirlərinin və təhlükəsizlik hədələrinin ətraflı kataloqu (hər bir kataloqda 600 –dən çox ad vardır).

Şirkətin informasiya aktivlərində verilmiş müdafiə sualları müəyyən ssenariyə əsaslanaraq baxılır: şirkətin informasiya aktivinin ümumi təsvir olunması – mümkün hədələr və təhlükəsizliyin zəif yerləri – mümkün tədbirlər və nəzarət və müdafiə vasitələri.

ISO 15408 "İNFORMASİYA TEXNOLOGİYALARI TƏHLÜKƏSİZLİYİNİN ÜMUMİ KRİTERİLƏRİ" BEYNƏLXALQ STANDARTI

Standartlaşdırmanın əsas nəticələrindən biri sayılan müdafiə olunan informasiya kompleksinin sistemləşdirilmiş xarakteristikaları və tələbatları sahəsi beynəlxalq və milli informasiya təhlükəsizliyi standartıdır. Standart yüzdən çox müxtəlif xarakterli və məzmunlu sənədləri özündə cəmləşdirir. Bu sistemin daxilində əsas yerlərdən birini ISO 15408 standartı tutur. Standart "Common Criteria" adı ilə məşhurdur.

1990-cı ildə standartlaşdırma üzrə Beynəlxalq təşkilatı (ISO) ümumi istifadə edilən informasiya texnologiyalarının qiymətləndirilməsi üçün yararlı olan beynəlxalq standart kriteriyanın hazırlanmasına başladı. Standartın hazırlanmasında aşağıdakı təşkilatlar iştirak edirdilər: Milli standartlar və texnologiyalar institutu və milli təhlükəsizlik agentliyi (ABŞ),

Kommunikasiya təhlükəsizliyi dövlət idarəsi (Kanada), İnformasiya təhlükəsizliyi agentliyi (Almaniya), Milli kommunikasiya təhlükəsizliyi agentliyi (Hollandiya), İnformasiya texnologiyalarının sertifikatlaşdırılması və təhlükəsizliyi proqramının yerinə yetirilməsi orqanı (İngiltərə), Sistemlərin təhlükəsizliyinin təmin edilməsi mərkəzi (Fransa).

On illər boyu dünyanın tanınmış mütəxəssisləri tərəfindən hazırlanmış sənədlər dəfələrlə redaktə edildi. İlk iki versiya 1998-ci ilin yanvar və may aylarında çap olundu. Standartın 2.1 versiyası 8 iyun 1999-cu ildə təsdiq edildi. Versiya həmin ildə Standartlaşdırma üzrə beynəlxalq təşkilatın (ISO) beynəlxalq informasiya təhlükəsizliyi standartı ISO/IEC 15408 kimi iştirakı ilə "İnformasiya texnologiyaları təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri" və ya "Commen Criteria" adı altında təsdiqləndi.

"Ümumi kriterilər" "Narıncı kitab"dan istifadə zamanı əldə olunmuş təcrübəyə əsaslanır, avropa və kanada kriterilərini ümumiləşdirir, ABŞ federal kriteriləri konsepsiyasının real strukturunu ifadə edirdi.

"Ümumi kriterilər"də informasiya texnologiyaları təhlükəsizliyi tələbləri geniş şəkildə təsnif olunur, onların qruplar üzrə strukturu müəyyənləşdirilməklə istifadə prinsipləri də təqdim edilirdi. "Ümumi kriterilər"in əsas məziyyətləri (yaxşı cəhətləri) – təhlükəsizliyə tələblərin tamlığı və onların sistemləşdirilməsi, istifadə olunmasında uyuşanlığı və gələcəkdə inkişaf etməsi üçün aşkarlığı idi.

Dünya miqyasında tanınmış istehsalçılar "Ümumi kriterilər"dən bəhrələnərək sifarişçilərə kriterilərin tələblərini tam şəkildə ödəyən vəsaitləri göndərməyə başladılar.

"Ümumi kriterilər"i üç qrup mütəxəssisin (informasiya texnologiyaları məhsullarının istehsalçıları və istehlakçıları,

həmçinin onların təhlükəsizlik səviyyəsini qiymətləndirən ekspertlər) tələblərini ödəmək üçün yaradılmışdı.

"Ümumi kriterilər"də informasiya təhlükəsizliyi məsələsinə bir neçə yanaşmada baxılır.

Birincisi, informasiyanın tamlığı və konfidensiallığı toplumu və informasiya texnologiyaları məhsullarının təhlil edilməsi baxımından, həmçinin hesablama sistemləri resurslarına əlçatanlıq baxımından yanaşılır.

İkincisi, avadanlıqların hədələrə tab gətirməsi, təhlükəsizlik siyasətinin həyata keçirilməsi və istismar mühitində avadanlıqların düzgün istismar edilməsi baxımımndan yanaşılır.

Beləliklə, "Ümumi kriterilər" konsepsiyasına layihələndirmə prosesinin bütün aspektləri, müəyyən təhlükəsizlik hədələri üçün nəzərədə tutulmuş informasiya texnologiyaları məhsullarının istismarı və istehsalı daxil edilir.

İnformasiya texnologiyaları istehlakçıları təhlükəsizlik hədələrinin varlığına həmişə qayğı ilə yanaşırlar, çünki belə hədələr təhlil olunan informasiyanın müəyyən riskə məruz qalmasına səbəb olur. Belə hədələrə qarşı mübarizə aparmaq üçün müdafiə vasitələrindən istifadə etmək məsləhətdir, müdafiə vasitələrinin sertifikatlaşdırılması onların hədələrə və risklərə adekvatlığını artırır.

"Ümumi kriterilər"i istehsalın, informasiya texnologiyaları vasitələrinin istismarının və təsnifatlaşdırılmasının təhlilində, həmçinin bütün mərhələlərdə qanuniləşdirirlər (nizama salırlar). "Ümumi kriterilər" istehsalçılara və istehlakçılara yerinə yetirdiklər həcmli işlərə aid normativ sənədlərin tərtib edilməsi üçün yararlı olan yaradıcılıq prosesi konsepsiyasını və təsnifatlaşdırmanın təhlilini təklif edir.

"Ümumi kriterilər"ə informasiya təhlükəsizliyi baxımından qoyulan tələbləri hər şeydən xəbardar ensiklopediya adlandırılar. Odur ki, informasiya texnologiyalarında yaranmış təhlükəsizlik problemlərinin həll edilməsində "Ümumi kriterilər"dən məlumat kitabçası kimi istifadə etmək çox əlverişlidir.

ISO 15408 standartı informasiya texnologiyalarının standartlaşdırılmasını dövlətlərarası səviyyəyə qaldırdı. Nəticədə vahid informasiya təhlükəsizliyi məkanının real perspektiv planının yaradılması meydana gəldi. Bununlada informasiya sistemlərinin milli baxımdan inteqrasiyasının qlobal miqyasda həyata keçirilməsi və informasiya texnologiyalarının yeni tətbiq sahələrinin yaradılmasına şərait yaradıldı.

Qəbul olunmuş informasiya təhlükəsizliyinin baza standartı (ISO 15408) sözsüz ki, bütün inkişaf etmiş ölkələrin yaradıcıları üçün çox vacib bir sənəddir.

NAQİLSİZ ŞƏBƏKƏLƏR ÜÇÜN STANDARTLAR

IEEE 802.11. standartı. 1990-cı ildə IEEE 802 komitəsi 802.11 işçi qrupunu formalaşdırdı və qrupa naqilsiz lokal şəbəkə üçün standartın hazırlanmasını tapşırdı. Standartın yaradılması 7 il vaxt apardı. 1997-ci ildə naqılsız standartın ilk spesifikasiyası IEEE 802.11 ratifikasiya (ratifikasiya - dövlətlər arasında bağlanan müqavilənin, paktın və s. ali hökumət orqanı tərəfindən təsdiq edilməsi) olundu. Standart 2,4 Qhers tezlik zolağında 1Mb/saniyə sürətlə (bəzəndə 2Mb/saniyə sürətlə) verilənlərin ötürülməsini təmin edirdi (Tezlik zolağı dünyanın əksər ölkələri üçün lisenziyalı sayılmır).

AÇIQLAMA: IEEE (Institute of Electrical and Electronics Engineers) elektronika və elektrotexnika sahəsində mühəndislər institutudur. IEEE peşəkar səviyyədə özünəməxsus standartlar hazırlayan mütəxəssislər birliyidir, 1884-cü ildə təsis edilmişdir. IEEE –nin üzvləri ***ANSI*** və ***ISO*** cəmiyyətləridir. IEEE-nin (IEEE http://www.ieee.org) tərkibində 150 ölkədən 410000 insan vardır. IEEE institutu hər il bütün ölkələrdə 600 elmi tədbirin keçirilməsinə, dünyada çap olunan texniki ədəbiyyatın 33%-nin çap olunmasına (elektrotexnika, radioelektronika və kompüter sahələrinə aid), maarifləndici proqramların hazırlanmasına, 900–dən çox standartın hazırlanmasına və dəstəklənməsinə himayədarlıq edir. IEEE tələbələrin və aspirantların elmi işlər ilə məşğul olmasına böyük diqqət yetirir. Bunun üçün xüsusi proqramların hazırlanmasına da rəvac verir. IEEE 39 ictimai birlikdən (Societies) və seksiyadan (Sections) ibarətdir, bunlara elmi qruplar və tələbə bölmələri daxildir. IEEE –yə kollektiv və fərdi formada üzv olmaq mümkündür. Üzv olmaq üçün heç bir maliyyə xərci tələb edilmir. Əksinə, IEEE-nin üzvü peşəkar səviyyəli görüşlərdə, xaricə ezam olunduqda, simpozium və konfranslarda iştirakda IEEE-dən maliyyə dəstəyi alır. Üzvlərə onları maraqlandıran jurnallar və qəzetlər pulsuz təqdim olunur. IEEE-nin üzvləri The Institute qəzetinə və Spectrum jurnalına güzəştlə abunə yazıla bilərlər. IEEE hər il müsabiqələr keçirir, qalibləri pul və ya medalla təltif edir və s.

Amerika Milli Sdtandartlar İnstitutu (ingiliscə ***A****merican* ***n****ational* ***s****tandards* ***i****nstitute, ANSI*) – amerika sənaye və işgüzar qruplar birliyidir, ticarət və kommunikasiya standartları hazırlayır. ISO və IEC təşkilatlarına daxildir, ABŞ-

ın maraqlarına xidmət edir.

19 oktyabr 1918-ci ildə "Amerika mühəndislər standartları komitəsi" (AESC) yaradılır. 1928-ci ildə komitənin adını dəyişərək "Amerika standartlar assosiasiyası" (ASA) qoyurlar. 1966-cı ildə yenidənqurma nəticəsində komitə "ABŞ standartlar institutu" adlandırılır. Komitəyə ANSI adı 1969-cu ildə verilmişdir. Komitənin üzvləri amerika şirkətləri, beynəlxalq təşkilatlar, şəxsi insanlar və hökumətə xidmə təşkilatlarıdır.

Beynəlxalq standartlar təşkilatı (International Organization for Standardizion, ISO) beynəlxalq təşkilatdır və standartların hazırlanması ilə məşğul olur. 1946-cı ildə yaradılmışdır. 1947-ci ildən isə faktiki olaraq işə başlamışdır.

IEEE 802.11 standartı baza standartı sayılır və WLAN (Wireless Local Area Network) naqilsiz lokal şəbəkənin təşkil edilməsi üçün lazım olan protokolları müəyyən edir. Bu protokollar içərisində əsas sayılan MAC (Medium Accsess Control – Kanal səviyyəsinin aşağı yarımsəviyyəsi) mühitinə əlçatan idarə etmə protokolu və fiziki mühitdə siqnalların ötürülməsi üçün yararlı olan PHY protokoludur (fiziki mühit dedikdə radiodalğalardan və infraqırmızı şüalanmadan istifadə edilməsi nəzərdə tutulur).

IEEE 802.11 standartının əsasını mobil (cellular-sotovıy) rabitə xətlərinin arxitekturası təşkil edir, həm də nəzərə almaq lazımdır ki, şəbəkə ya bir, ya da ki, bir neçə yuvalardan ibarət ola bilər. Bu yuvalardan hər biri *AP (Access Point) əlçatanlıq nöqtəsi* adlanan baza stansiyası tərəfindən idarə edilir. Bu əlçatanlıq nöqtəsinin təsir dairəsində olan istifadəçinin işçi stansiyaları əlçatanlıq nöqtəsi ilə birlikdə *BSS (Basic Service*

Set) baza xidmət zonası yaradır. Şəbəkə öz aralarında *bölüşdürücü sistemləri* ilə əlaqə yaradır. İnfrastruktur bölüşdürücü sistemləri ilə birləşərək *genişləndirilmiş xidmət zonasını* əmələ gətirir.

Standart əlçatanlıq nöqtəsi olmayan şəbəkənin yaradılmasına da imkan verir, bu zaman əlçatanlıq nöqtəsinin funksiyasını işçi stansiyalar yerinə yetirirlər.

WLAN (Wireless Local Area Network) naqilsiz lokal şəbəkənin müdafiə edilməsi üçün IEEE 802.11 standartında WEP (Wired Equivalent Privacy) alqoritmi nəzərə alınmışdır. Alqoritm şəbəkədə qeyriqanuni əlçatanlığa qarşı müqavimət göstərməklə yanaşı informasiyanın tutulması üçün şifrələmə əməliyatını da yerinə yetirir (Qeyriqanuni əlçatanlıq - НСД несанкционированного доступа).

IEEE 802.11 standartının müəyyən çatışmazlıqları da vardır – açar ilə idarə edilmənin olmaması, ümumi statik açardan istifadə edilməsi, açarın kiçik mərtəbələr sayından istifadə edilərək düzəldilməsi, ***RC4*** alqoritmindən istifadənin mürəkkəbliyi və s.

IEEE 802.11 standartının yaradıcıları göstərilən çatışmazlıqları (və buna bənzərləri) aradan gptürmək üçün standartın digər versiyalarını da işləyib hazırladılar.

AÇIQLAMA: RCA (ingiliscə *Rivest cipher 4* və ya *Ron's code*), həmçinin APC4 və ya ARCFOUR (alleged RC4) kimi məşhurdur. RC4 axınlı şifrdir, kompüter şəbəkələrində informasiyanın müdafiə sistemlərində geniş istifadə olunur (məsələn, SSL və TLS protokolarında, WEP və WPA naqilsiz şəbəkələrdə təhlükəsizliyin təmin edilmə alqoritmlərində). RC4 axınlı şifri 1987-ci ildə "RSA Security" şirkətinin əməkdaşı Ronald Rivest tərəfindən yaradılmışdır. Yeddi il

ərzində şifrə kommersiya sirri kimi gizli saxlanılır. 1994-cü ilin sentyabr ayında əldə olunmuş razılığa əsasən alqoritmin dəqiq izahı verilir. Bir az sonra RC4 usenet "sci.crypt" yeniliklər qrupunda nəşr olunur və oradan da İnternet şəbəkəsinin çoxlu sayda saytlarına daxil olur.

IEEE 802.11b standartında (1999-cu il) tezlik zolağı və ötürmə tezliyi artırılmış, spekterin bölüşdürülməsi üçün bir-başa ardıcıllıq metodundan istifadə edilmişdi. Bununla yanaşı verilənlərin maniə tərəfindən təhrif olunmasının qarşısı hiss ediləcək dərəcədə alınmış, yüksək dayanıqlıq əldə edilmişdir.

IEEE 802.11a standartında tezlik zolağı və ötürmə tezliyi 5 dəfə artırılmaqla yanaşı digər yeniliklərdə əlavə edilmişdi. Nəticədə yararlı siqnalın eyni zamanda bir neçə tezlik diapazonunda paralel ötürülməsi həyata keçirilmiş, kanalın buraxma qabiliyyəti yüksəldilmiş, siqnalın keyfiyyəti artırılmışdı. Standartın çatışmazlığı böyük güc tələb etməsi və kiçik təsir dairəsinə (100 metrə yaxın) malik olmasıdır.

IEEE 802.11g standartında verilənlərin ötürülmə tezliyi 54 Mbit/saniyəyə çatdırılmışdır, aşağı güc tələb edir, təsir dairəsi artırılmış (300 metrə kimi) və kanalın ötürmə zolağı genişləndirilmişdir.

IEEE 802.11i standartında naqilsiz şəbəkənin təhlükəsizliyi təmin edilmişdir. Standart 2004-cü ildə ratifikasiya edilmişdir. Standart Wi-Fi şəbəkələrində də istifadə edilə bilər. Standart autentufikasiya prosesində üç iştirakçının olmasını təklif edir: AS (Authentication Server) autentifikasiya serveri, AP (Access Point) əlçatanlıq nöqtəsi və STA (Station) işçi stansiya. Standartda şifrələmə prosesində AP və STA iştirak edir. Standart ilə işləməkdən ötrü müxtəlif açarlardan (məsələn, MK (Master Key) – Ustad-açar, PMK (Paiwise Master

Key) – cüt Ustad-açar, müvəqqəti və qrup şəkilində olan açarlardan və s.) istifadə edilir. Açarlar geniş verilişli şəbəkə trafikini müdafiə etmək üçün qulluq edirlər.

IEEE 802.11i standartının işini beş fazaya bölurlər.

Birinci faza – aşkarlama. Bu fazada STA işçi stansiyası AP əlçatanlıq nöqtəsini aşkar edir.

İkinci faza – autentifikasiya. Bu fazada STA autentifikasiyası ilə AS serveri qarşılıqlı fəaliyyət göstərir.

Üçüncü faza – AS serveri PMK açarını AP əlçatanlıq nöqtəsinə yönəldir.

Dördüncü faza – 802.1x açarının idarə edilməsi. Bu fazada PTK açarının generasiyası, bağlılığı və yoxlanması (verifikasiyası) baş verir.

Beşinci faza – verilənlərin ötürülməsi və şifrələnməsi. Bu fazada şifrələnmə üçün PTK –dan istifadə edilir.

İNTERNETDƏ İNFORMASİYA TƏHLÜKƏSİLİYİ STANDARTI

Birləşmiş Millətlər Təşkilatının məlumatına görə kompüter cinayətkarlığı beynəlxalq səviyyədə bir problemə çevrilmişdir. Bu baxımdan İnternet şəbəkəsində və qarışıq İntranet şəbəkələrində problem öz həllini tapmalıdır.

İnternetin bu sahədə əsas xidməti hamını bu texnologiyaya başqa çür baxmağa məcbur etdi. Birincisi, İnternet açıq standartların tətbiq edilməsini genişləndirdi, istifadəçilərin ondan lazımı səviyyədə istifadə etmələri ilə yanaşı ona olan marağı da artırdı. İkincisi, İnternet dünyada demək olar ki, yeganə şəbəkədir ki, istənilən şəxs ona qoşula bilər. Və nəhayət, İnternet dünya bazarında yeni texnologiyalar və yeni məhsullar deməkdir və bunlardan hamı bəhrələnə bilər.

İnternetdə müəyyən komitələr vardır ki, onların köməyilə standartlaşma prosesindən istifadə etməklə müəyyən texnologiyalara yiyələnmək olar. Bu komitələr əsasən mühəndislər qrupundan yaradılır. Məsələn, IETF (İnternet Engineering Task Force) qrupu standartlaşma üzrə bir neçə protokolu ((TCP/IP verilənlərin ötürülmə protokolu, elektron poçt üçün istifadə edilən SMTP (Simple Mail Transport Protocol) və POP (Post Office Protokol) protokolları, şəbəkənin idarə edilməsi SNMP (Simple Network Management Protocol) protokolu)) işləyib hazırlamışdır.

İnternetdə verilənlərin təhlükəsiz ötürülmə protokollarından SSL, SET və IPSec geniş istifadə olunmaqla yanaşı həm də ki, populyarlıq qazanmışdır. Protokollar yaxın zamanlarda istifadəyə verilmişdir.

SSL protokolu (Secure Socket Layer) şəbəkə ilə şifrələnmiş verilənlərin təhlükəsiz ötürülməsi üçün populyar şəbəkə protokoludur. Protokol verilənlərin tamlığına nəzarət edir, birləşmələrin müdafiə edilməsinə imkan verir və müxtəlif məsələlərin həll edilməsində yardımçıdır. Protokol kriptoqrafiyadan istifadə etməklə servislər arası verilənlərin ötürülməsinin müdafiəsini təmin edir.

AÇIQLAMA: *SSL* (ingiliscə *Secure Sockets Layer* – Müdafiə Edilən Soketlər) protokolu ilk olaraq Netscape Communications şirkəti tərəfindən yaradılmışdır. Şirkət SSL-in birinci versiyası haqqında heç vaxt informasiya verməmişdir, bunu sirr kimi saxlayır. İkinci versiya 1995-ci ilin fevral ayında istehsala buraxılır. İkinci versiyada çoxlu sayda təhlükəsizlik baxımından çatışmazlıqlar mövcud idi. Bu səbəbdən şirkət protokolun üçüncü versiyasının hazırlanması ilə məşğul olur və 1966-cı ildə yeni versiyanı istehsal edir.

Üçüncü versiya TLS 1.0 protokolunun yaradılmasına səbəb oldu. TLS 1.0 protokolu İnternet Engineering Task Force (IETF) üçün standarta çevrilmişdir və digər təşkilatlar İnternet şəbəkəsində kommersiya məqsədi ilə SSL protokolundan istifadə etməyə lisenziyalıdırlar.

Soket (ingiliscə socket – dərinləşmə, yuva, sökmə anlamlarını verir) prosessorlar arasında verilənlərin mübadiləsini təmin edən proqram interfeysinin adıdır. Prosessorlar belə mübadiləni ya bir Elektron Hesablama Maşınında, ya da ki, bir-birilə şəbəkə ilə əlaqə yaratmış müxtəlif EHM-lərdə yerinə yetirə bilirlər. Soket – sonuncu nöqtəni birləşdirən abstrakt obyektdir. Müştəri və server soketləri mövcuddur. Müştəri soketini kobud şəkildə telefon şəbəkəsindəki telefon aparatı ilə, server soketlərini isə kommutatorlarla müqayisə etmək olar. Müştəri qoşulmalarını (məsələn, brauzer) ancaq müştəri soketləri, server qoşmalarını isə (məsələn, brauzerin sorğu göndərdiyi Veb-server) həm müştəri soketləri, həm də ki, server soketləri həyata keçirirlər.

Sistem administratorundakı selenqlərdə soket IP-ünvan kombinasiyasını və portun nömrəsini (məsələn, http://10.10.10.10.80.) göstərir.

Soketin interfeysi ilk dəfə BSD Unix-də zahir olmuşdur. Soketin proqran interfeysi POSIX. 1 standartında yazılmışdır və bütün əməliyyat sistemləri tərəfindən dəstəklənir.

SET protokolu (Security Electronics Transaction) İnternet şəbəkəsində elektron ***tranzaksiyaların*** təhlükəsiz perspektiv standartıdır, İnternetdən istifadə etməklə elektron

ticarətin təşkil edilməsinə yardımçıdır. SET protokolu X.509 standartına uyğun rəqəmsal sertifikatdan istifadəyə əsaslanır.

Protokol MasterCard və Visa şitkətləri tərəfindən yaradılmışdır (prosesdə IBM, GlobeSet və digər tərəfdaşlarda iştirak etmişlər).

AÇIQLAMA: *Tranzaksiya* bir hesabdan digər hesaba pul vəsaitlərinin köçürülməsi üçün bank əməliyyatıdır.

SET İnternetdə təhlükəsiz ödəmələrin yerinə yetirilməsinə və plastik kartlardan istifadəyə imkan verir. Əksət hallarda protokolu İnternetdən istifadə etməklə *standart texnologiya* və ya *plastik kartlardan istifadə etməklə təhlükəsiz ödəmələri yerinə yetirən protokol* adlandırırlar. Protokol kriptoqrafiyadan (əsasəndə rəqəmsal sertifikatlardan) istifadə etməklə istehlakçı ilə satıcılar arasında bütün ticarət əlaqələrinin yaradılmasına köməklik edir.

SET protokolunun köməyilə informasiyanın əlçatanlığı, tamlığı, konfidensiallığı və hüquqi əhəmiyyəti tam şəkildə həll olunur.

SET-in əsas üstünlüyü rəqəmsal sertifikatdan istifadə edilməsidir (digərlərinə nəzərən). SET bank ilə satıcılar arasında cari sistemə inteqrasiya olunan əlaqə yarada bilir.

IPSec protokolu. IPSec protokolunun spesifikasiyası TCP/IP protokolunun cari versiyası ilə münasibətdə əlavə kimi sayıla bilər (burada IP v.6 standartından istifadə edilir). Protokol IP Security IETF işçi qrupu tərəfindən işlənib hazırlanmışdır. İndiki zamanda protokol özünə 3 alqoritmi – RFC-standartını təmsil edən müstəqil baza spesifikasiyanını birləşdirir. Protokol IP şəbəkə səviyyəsində standart rəqəmsal trafik üsulunu dəstəkləyir. Protokolun köməyilə ikitərəfli

şifrələmə üsundan istifadə etməklə informasiyanın müdafiə olunmasını həyata keçirmək mümkündür. Bundan istifadə edən təşkilatlar İnternetdə özlərinə məxsus xüsusi virtual şəbəkə yaratmışlar.

PKI açıq açarı ilə idarə olunan infrastrukturu (Public Key İnfrastructure) kriptoqrafik açıq açar prinsipinə əsaslanaraq elektron sənəd dövriyyəsini kriptioqrafik müdafiə edən strukturdur. Struktur beynəlxalq X.509 standartına əsaslanır və sənəd dövriyyəsində bütün iştirakçılara məxsus sənədlərin elektron formada dəyişdirilməsini yerinə yetirir.

ƏMƏLİYYAT SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN TƏMİNİ

ƏMƏLİYYAT SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ PROBLEMLƏRİ

Əksər informasiyanın proqram müdafiə vasitələrinin çoxu tətbiqi proqramlardır. Onların yerinə yetirilməsi üçün mütləq Əməliyyat sistemindən (ƏS) dəstək lazımdır. Əməliyyat sistemlərinə məxsus olan funksiyaların yerinə yetirilməsinin əhatə dairəsi *etibarlı hesablama bazası* (EHB) adlanır. Etibarlı hesablama bazası informasiya təhlükəsizliyini təmin edən elementlər toplumundan ibarətdir. Bura proqramlar, şəbəkə avadanlıqları, vəsaitlərin fiziki müdafiəsi və təşkilatı prosedurlar daxildir. Əmələ gələn piramidanın əsas müdafiəsi əməliyyat sistemidir.

ƏMƏLİYYAT SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNƏ HƏDƏLƏR

Əməliyyat sisteminin effektiv və etibarlı müdafiəsinin təşkili mümkün hədələrin və onların təhlükəsizliyinin öncədən təhlili olmadan mümkün deyil. Əməliyyat sistemlərinin hədələrdən təhlükəsizliyi sistemin istimar şərtlərindən, hansı informasiyanın yaddaşda saxlanılmasından, hansı

informasiyanın sistemdə təhlil edilməsindən və buna bənzərlərdən hiss ediləcək dərəcədə asılıdır. Məsələn, əgər əməliyyat sistemi müəssisədə elektron sənəd dövriyyəsi üçün istifadə edilirsə, onda ən təhlükəli hədə qeyriqanuni əlçatanlığın fayllara vurduğu ziyandır. Əgər əməliyyat sistemi İnternet-xidmətin provayder platformasinda istifadə edilirsə, onda ən qorxulu hücumlar əməliyyat sisteminin şəbəkə proqram təminatına edilən hücumlardır.

Əməliyyat sistemlərinin hədələrdən təhlükəsizliyini onların istifadə edilmə baxımından təsnifləşdirmək olar.

1.Hücumun məqsədinə görə:

- İnformasiyanın qeyriqanuni oxunmasına görə;
- İnformasiyanın qeyriqanuni dəyişdirilməsinə görə;
- İnformasiyanın qeyriqanuni məhv edilməsinə görə;
- Əməliyyat sisteminin tam və ya hissə-hissə dağılmasına görə.

2.*Əməliyyat sisteminə təsir prinsipinə görə*:

- İnformasiyanın əldə edilməsi üçün məşhur (leqal) kanallardan istifadə edilməsi, məsələn, faylların qeyriqanuni oxunmasına hədələr və s.;
- İnformasiyanın əldə edilməsi üçün gizli kanalların istifadə olunması, məsələn, bədniyyətli insanın əməliyyat sisteminin sənədləşdirilməmiş imkanlarından istifadə etmək üçün hədələrdən istifadə etməsi;
- Proqram əlavələrinin köməyilə informasiyanın əldə edilməsi üçün yeni kanalların yaradılması.

3.*Bədniyyətli insan tərəfindən müdafiənin pis vəziyyətə salınması növünə görə*:

- Uyğun olmayan təhlükəsizlik siyasəti, o cümlədən sistem inzibatçısının səhvləri;

- Əməliyyat sisteminin səhvi və proqram təminatı imkanlarının sənədləşdirilməməsi, o cümlədən sistemin müdafiəsini yan keçməyə imkan verən, təsadüfən və ya düşünülmüş şəkildə qurulan "xidməti giriş" (onu çox vaxt "*lyuk – anbar ağzı"* da adlandırırlar);
- Əvvəllər istifadə olunan proqram əlavələri.

4. *Əməliyyat sisteminə etdiyi təsirin xarakterinə görə*:

- Aktiv təsir – pisniyyətli insanın sistemə qeyriqanuni təsir göstərməsi;
- Passiv təsir – sistemdə baş verən proseslərin qeyriqanuni şəkildə pisniyyətli insan tərəfindən müşahidə edilməsi.

Əməliyyat sisteminin təhlükəsizlik hədələrini onların əlamətlərinə görə təsnif edirlər. Bunlara: pisniyyətli insan tərəfindən edilən təsirin üsulu, istifadə edilən hücum vasitələri, hücum obyektləri, hücuma məruz qalan obyektə edilən təsirin üsulları, hücum edilən obyektdə istifadə edilən əməliyyat sisteminin hücum zamanı vəziyyəti aiddir.

Əməliyyat sistemi aşağıdakı hücumlara məruz qala bilər:

- *Fayl sisteminin skanerə edilməsi*. Bədniyyətli insan kompüterin fayl sisteminə nəzər salır və bütün faylları ardıcıl oxumağa (və ya surətini almağa) cəhd göstərir. Gec və ya tez inzibatçının heç olmasa bir səhvi aşkar olunur. Nəticədə pisniyyətli insan ona qadağa qoyulmuş informasiyaya əlçatanlıq edir;
- *Parolun seçilməsi*. Parolun seçilməsində bir neçə üsuldan istifadə edilir:
  - Ümumi izafə (izafə - normadan artıq alınmış (götürülmüş) şey anlamını verir);

- Statistikada rast gəlinən simvolların optimallaşdırılması və ya lüğətdan istifadə etməklə ümumi izafə;
- İstifadəçini tanımaqla parolun seçilməsi (onun adı, soyadı, doğum günü, telefon nömrəsi və s.);

- *Açar informasiyanın oğurlanması*. Pisniyyətli insan istifadəçi tərəfindən yığılmış parola baxa bilər və yaxud da, istifadəçının klaviatura üzərində əlinin hərəkətini izləməklə onun yığdığı parolu bərpa edə bilər. Bununla yanaşı açar informasiya (smart-kart, Touch Memory və başqaları) pisniyyətli insan tərəfindən sadəcə oğurlana bilər;
- *"Zibil qutu"suna atılmışın toplanması*. Bir çox əməliyyat sistemlərində istifadəçi tərəfindən ləğv edilmiş informasiya fiziki olaraq ləğv olunmur, sadacə olaraq "Zibil qutusu" adlanan qutuya atılır. Bədniyyətli insan atılmış informasiyanı bərpa edir, ona baxış keçirir və ona lazım olan hissələrin (ola bilsin tam faylın) surətini alır;
- *Səlahiyyətini aşma*. Bədniyyətli insan əməliyyat sistemində proqram təminatındakı səhvdən və təhlükəsizlik siyasətindən istifadə etməklə özü üçün səlahiyyət əldə edir. Adətən belə hallar proqramı işə salarkən başqa istifadəçinin adından istifadə etdikdə baş verir;
- *Proqrama qoşulma*. Əməliyyat sistemlərində istifadə olunan proqrama qoşulma digər proqrama qoşulmalar sinifindən fərqlənmir;
- *Proqrama acgözlük*. Bu proqram kompüterin bəzi resurslarını ələ keçirə bilir, nəticədə digər proqramlar ya yerinə yetirilə bilmirlər, ya da ki, ağır sürətlə yerinə

yetirilirlər. Acgöz proqramın işə salınması məhvə gətirib çıxarır.

ƏMƏLİYYAT SİSTEMİNİN MÜDAFİƏ OLUNMA ANLAYIŞI

Əməliyyat sistemi o vaxt müdafiə olunan sayılır ki, o kanardan edilən müxtəlif sinif hücumları dəff edə biləcək vasitələrdən istifadə edə bilsin. Müdafiə olunan əməliyyat sistemi mütləq şəkildə istifadəçinin onun resurslarına əlçatanlıq etməsinə məhdudiyyət qoyan vasitələrə malik olmalıdır. Bununla yanaşı əməliyyat sistemində istifadəçinin həqiqiliyini yoxlaya biləcək vəsaitdə olmalıdır. Əməliyyat sistemi təsadüfi təsirlərə və ya onun işini pozacaq (işdən çıxara biləcək) hallara da hazır olmalıdır.

Bəzən elə olur ki, əməliyyat sistemi bütün baş verə biləcək hədələrdən deyil, onlardan bəzilərindən müdafiə olunur. Belə olan halda əməliyyat sistemi *qismən müdafiə olunan* əməliyyat sistemi adlandırılır.

ƏMƏLİYYAT SİSTEMİNİN MÜDAFİƏ OLUNMASINA YANAŞMA

Əməliyyat sisteminin müdafiə edilməsinə iki əsas yanaşma mövcuddur – *fraqmentlərlə* və *kompleks*. Fraqmentlərlə yanaşmada əvvəlcə bir hədədən müdafiəni həyata keçirirlər, sonra növbəti hədəni və s. Fraqmentlərlə yanaşmaya nümunə kimi müdafiə edilməyən Windows 98 əməliyyat sistemini göstərmək olar, çünki, əməliyyat sisteminə

antivirus proqramı quraşdırılır, şifrələmə sistemindən istifadə edilir, istifadəçinin fəaliyyəti qeydiyyat sistemində nəzərədə saxlanılır və s.

Fraqmentlərlə yanaşmada əməliyyat sisteminin altsisteminin müdafiə edilməsi dedikdə müxtəlif istehsalçılardan alınan dağınıq proqram məhsulları nəzərədə tutulur. Bu proqram vasitələri bir-birindən asılı olmadaq işləyirlər (iş zamanı onların birliyini təmin etmək praktiki olaraq mümkün deyil). Bununla yanaşı belə altsistemin müdafiə edilməsinin ayrı-ayrı elementləri bir-biri ilə kobudcasına (qeyrikorrekt) işlədiyinə görə ümumilikdə sistemin etibarlığı sərt şəkildə aşağı düşür.

Kompleks yanaşmada müdafiə funksiyası əməliyyat sistemi layihələndirilmə mərhələsində olanda ona daxil edilir və onun ayrılmaz hissəsinə çevrilir. Kompleks yanaşmaya əsaslanaraq yaradılmış altsistemin müdafiə olunmasının ayri-ayri elementləri müxtəlif məsələlərin həll edilməsində və informasiyanın müdafiə edilməsində bir-birilə qarşılıqlı əlaqədə olduğu üçün ayrı-ayrı elementlər arasında praktiki olaraq münaqişənin yaranması mümklün deyil. Kompleks yanaşma əsasında qurulmuş altsistemin müdafiəsi bəzən elə qurulur ki, sistemdə qarşısı alınmaz pozuntular baş verdikdə əməliyyat sisteminin əsas elementlərində yaranan bu hallar (pozuntular) əməliyyat sisteminin müvəffəqiyyətsizliyinə gətirib çıxarır, nəticədə pisniyyətli insan sistemin müdafiə olunma funksiyasını pozmağa imkan tapa bilmir. Nəzərə almaq lazımdır ki, fraqmentlərlə yanaşmada altsistemin bu şəkildə müdafiə edilməsi mümkün deyil.

Qeyd etmək lazımdır ki, kompleks yanaşmaya əsaslanaraq qurulmuş əməliyyat sistemi altsisteminin müdafiəsi elə şəkildə layihələndirilir ki, onun ayrı-ayrı elementlərini dəyişmək

mümkün olsun. Belə olan halda münasib proqram modulunu digər modul ilə dəyişmək mümkün olur.

MÜDAFİƏNİN İNZİBATI TƏDBİRLƏRİ

Əməliyyat sisteminin müdafiəsinin proqram-aparat vasitələri mütləq inzibatı tədbirlər ilə tamamlanmalıdır. İnzibatçı tərəfindən daim ixtisaslaşdırılmış dəstək yerinə yetirilməsə ən etibarlı proqram-aparat müdafiəsi belə nəticəsiz alına bilər.

Aşağıda əsas inzibatı tədbirlər verimişdir:

1.*Əməliyyat sisteminin daim işlək olmasına nəzarətin korrektliyi* xüsusilə onun altsisteminin müdafiəsi ilə bağlıdır. Belə nəzarəti təşkil etmək əlverişlidir. Bu əsasən o zaman baş verir ki, əməliyyat sistemi əsas hadisələrin (event logging) xüsusi jurnalda avtomatik olaraq qeyd olunmasını dəstəkləyir.

2. *Adekvat (tam uyğun) təhlükəsizlik siyasətinin təşkili və dəstəklənməsi*. Əməliyyat sisteminin təhlükəsizlik siyasəti daim korrektə edilməlidir, çünki bədniyyətli insan əməliyyat sisteminə ziyan vura bilər, onun quruluşunu dəyişər, tətbiqi proqramların qurulmasına və ya sistemdən kanarlaşdırılmasına maneçilik edə bilər.

3.*İstifadəçinin əməliyyat sistemindən istifadəsinin təlimatlandırılması* əməliyyat sisteminin işlədiyi zaman ərzində təhlükəsizlik tədbirlərinə riayət edilməsinə və bu tədbirlərin həyata keçirilməsinə nəzarətin yerinə yetirilməsinə imkan verir.

4.*Mütamadi olaraq ehtiyat surətlərin və əməliyyat sistemi verilənlərinin yaradılması və təzələnməsi*.

5.*Əməliyyat sisteminin, verilənlərin təhlükəsizlik siyasətinin və quruluşunun dəyişməsinə daim nəzarət*. Belə dəyşiklikləri qeyrielektrik informasiya daşıyıcılarında saxlamaq məsləhətdir, çünki bədniyyətli insanın əməliyyat sisteminin

müdafiəsini dağıdaraq sistemə daxil olması və özünü maskalayaraq qeyriqanuni fəaliyyət göstərməsi mümkün olmaz.

Ədəbiyyatlarda konkret əməliyyat sistemi üçün digər inzibatı tədbirlərin həyata keçirilməsi haqqında qeydlər vardır.

ADEKVAT TƏHLÜKƏSİZLİK SİYASƏTİ

Adekvat təhlükəsizlik siyasətinin seçilməsi və dəstəklənməsi əməliyyat sistemi inzibatçısının əsas vacib məsələlərindən biri sayılır. Əgər əməliyyat sistemində qəbul olunmuş təhlükəsizlik siyasəti adekvat deyilsə, bu pisniyyətli insanın sistemin resurslarına qeyriqanuni əlçatanlığına imkan verəcək və əməliyyat sisteminin etibarlı işləməsinə şərait yaradacaq.

Məlumdur ki, əməliyyat sıstemi nə qədər yaxşı müdafiə olunarsa, istifadəçinin və inzibatçının onunla işləməsi bir o qədər çətin olacaqdır. Bu aşağıdakı faktorlar ilə bağlıdır:

- İstifadəçinin bəzi əməllərinin qərəzli olduğunu müdafiə sistemi həmişə müəyyən edə bilmir. Sistem nə qədər çox müdafiə olunarsa, istifadəçinin leqal fəaliyyəti bir o qədər yüksək olacaqdır;
- İstənilən sistemdə informasiyanın müdafiə funksiyası nəzərə alınmışsa, inzibatçıdan adekvat təhlükəsizlik siyasətinin dəstəklənməsinə istiqamətlənmiş müəyyən fədakarlıq tələb edilir. Əməliyyat sistemində müdafiə funksiyası nə qədər yüksək olarsa, müdafiənin dəstəklənməsi üçün bir o qədər vaxt və vəsait tələb olunur;
- Əməliyyat sistemi müdafiəsinin altsistemi, həmçinin istənilən başqa bir proqram paketi kompüterin aparat vasitələrinin resurslarını sərf edir. Əməliyyat sisteminin

müdafiə funksiyası nə qədər mürəkkəb qurularsa, kompüterin resursları da bir o qədər çox olacaqdır (məsələn, prosessor vaxtı, operativ yaddaş və s.). Bu resurslar müdafiə altsisteminin dəstəklənməsinə sərf edilir və kompüterin tətbiqi proqramına bir o qədər az resurs payı düşür;

- Təhlükəsizlik siyasətinin həddidən artıq dəstəklənməsi əməliyyat sisteminin işləməsinə neqativ təsir edə bilər. Siyasətə həddindən artiq sərt yanaşma çətin aşkarlanan səhvlərə səbəb ola bilir və əməliyyat sisteminin işini dayandırmasına, nəticədə məhv olmasına gətirib çıxarır;

Təhlükəsizlik siyasətinin optimal adekvatlığı dedikdə bədniyyətli insana nəin ki, qeyriqanuni fəaliyyətini həyata keçirməyə imkanın verilməməsi, həmçinin öndə yazılanlarda neqativ effektin baş verməsinə gətirib çıxarmaması prosesi başa düşülür.

Adekvat siyasət nəin ki, əməliyyat sisteminin arxitekturası ilə müəyyən edilir, həm də ki, onun quruluşu, ona quraşdırılmış tətbiqi proqramlar və i.a. ilə müəyyən edilir. Əməliyyat sisteminin adekvat təhlükəsizlik siyasətinin formalaşmasını və dəstəklənməsini iki mərhələyə bölürlər.

1.*Hücumların təhlili*. Əməliyyat sisteminin administratoru əməliyyat sisteminin cari nüsxəsində mümkün təhlükəsizlik hədələrinə (hücumlarına) baxış keçirir. Mümkün hədələrin içərisindən ən çox təhlükəli olanları seçilir və onlardan müdafiə üçün maksimum vəsait ayrılır.

2.*Təhlükəsizlik siyasətinə tələbin formalaşdırılması*. Bu və ya digər hədələrdən müdafiə olunmaq üçün hansı üsullardan və vəsaitlərdən istifadə edilməsini administrator (inzibatçı) müəyyən edir. Məsələn, əməliyyat sisteminin bəzi obyektlərinin qeyriqanuni əlçatanlıqdan müdafiə olunması üçün müxtəlif

üsullardan – kriptoqrafik vasitələrdən, əlçatanlıqla mübarizə apara bilən bəzi vasitələrin kombinasiyalarından və s. istifadə olunur.

3. *Təhlükəsizlik siyasətinin formal müəyyən edilməsi.* İnzibatçı öndəki mərhələdə formalaşdırılmış tələblərin konkret olaraq necə yerinə yetirilməsini müəyyən edir. Əməliyyat sisteminin quruluşuna, həmçinin əlavə müdafiə paketlərinə olan tələblər formalaşdırılır. Formalaşdırma əməliyyatı ancaq belə paketlərin qurulmasına ehtiyac duyulduqda həyata keçirilir. Yerinə yetirilmiş mərhələnin nəticəsi əməliyyat sisteminin konfiqurasiyasının qurulmasını açıq şəkildə əks etdirən siyahısının tərtib edilməsi və hansı vəziyyətdə hansı sazlamanın qurulması üçün əlavə müdafiə paketlərindən istifadə edilməsi ilə bağlıdır.

4. *Təhlükəsilik siyasətinin həyata keçirilməsi*. Bu mərhələnin məqsədi öndəki mərhələdə formal olaraq müəyyən edilmiş əməliyyat sisteminin konfiqurasiyasının və əlavə müdafiə paketlərinin təhlükəsizlik siyasətinə uyğun həyata keçirilməsidir.

5. *Təhlükəsizlik siyasətinin korreksiya olunması və dəstəklənməsi*. Bu mərhələdə inzibatçının qarşısında duran əsas məsələ təhlükəsizlik siyasətinə nəzarəti yerinə yetirmək və lazım gəldikdə müəyyən dəyişiklikləri həyata keçirməkdir.

Qeyd etmək lazımdır ki, əməliyyat sisteminin müdafiə edilməsi üçün xüsusi olaraq hazırlanmış standart hələlik yoxdur. Əməliyyat sisteminin müdafiə edilməsini qiymətləndirmək üçün ümumilikdə kompüter sistemi üçün işlənib hazırlanmış standartdan istifadə edilir.

Adətən əməliyyat sisteminin sertifikatlaşdırılması adekvat təhlükəsizlik siyasəti üçün tələblərin tərtib edilməsi ilə müşahidə olunur. Adekvat təhlükəsizlik siyasətini müəyyən

edən zaman əməliyyat sisteminin administratoru ilk növbədə əməliyyat sisteminin konkret hədələrdən müdafiə edilməsinə əsaslanmalıdır.

ƏMƏLİYYAT SİSTEMİNİN MÜDAFİƏ OLUNMA ALTSİSTEMİNİN ARXİTEKTURASI

ƏMƏLİYYAT SİSTEMİNİN MÜDAFİƏ OLUNMA ALTSİSTEMİNİN ƏSAS FUNKSİYALARI

Əməliyyat sisteminin müdafiə altsistemi əsasən aşağıdakı funksiyaları yerinə yetirir.

1.*İdentifikasiya və autentufikasiya*. Heç bir istifadəçi özünü identifikasiya etməmiş əməliyyat sistemi ilə işə başlaya bilməz. İstifadəçi işə başlayan zaman sistemə autentifikasiya olunmuş informasiyanı təqdim etməlidir. Bununla yanaşı istifadəçi sistemə onun varlığını (yəni bu doğurdan da həmin istifadəçidir) təsdiq edəcək informasiyanı da təqdim etməlidir.

2.*Məhdudlaşdırılmış əlçatanlıq*. Hər bir istifadəçinin əməliyyat sisteminin o obyektlərinə əlçatanlığı olur ki, ona cari təhlükəsizlik siyasəti həmin obyektlərə əlçatanlığa icazə verir.

3.*Audit*. Əməliyyat sistemi sistemin təhlükəsizliyini dəstəkləyən potensial qorxulu xüsusi hadisələr jurnalına reaksiya verir.

4.*Təhlükəsizlik siyasətinin idarə edilməsi*. Təhlükəsizlik siyasəti daim adekvat vəziyyətdə saxlanılmalıdır, yəni əməliyyat sisteminin işləməsi şərtlərinin dəyişməsinə çevik reaksiya verməlidir. Təhlükəsizlik siyasətinin idarə edilməsi sistem administratoru (inzibatçı) tərəfindən həyata keçirilir, administrator bunun üçün uyğun əməliyyat sisteminə qurulmuş vəsaitlərdən istifadə edir.

5.*Kriptoqrfaik funksiyalar*. İnformasiyanın müdafiə olunmasını kriptoqrafik vəsaitlərdən istifadə etmədən təsəvvür etmək mümkün deyil. Əməliyyat sistemlərində şifrələmə istifadəçinin parollarını və sistemin təhlükəsizliyini, həmçinin qorxulu olan digər verilənləri rabitə kanalları vasitəsilə ötürülməsi və saxlanması zamanı istifadə olunur.

6.*Şəbəkə funksiyaları*. Müasir əməliyyat sistemləri lokal və ya qlobal kompüter şəbəkələrin tərkibində izolə edilməmiş işləyirlər. Bir şəbəkəyə daxil olan kompüterlərin əməliyyat sistemləri müxtəlif məsələlərin həll edilməsində bir-birinin arasında qarşılıqlı əlaqədə olurlar (o cümlədən, o məsələlərin həllində ki, onlar birbaşa informasiyanın müdafiəsi ilə əlaqəlidirlər).

Müdafiənin altsistemi adətən vahid proqram moduluna malik deyil. Bu baxımdan sadalanmış müdafiə altsisteminin funksiyası bir və ya bir neçə proqram modulu ilə həll olunur. Bəzi funksiyalar bilavasitə əməliyyat sisteminin nüvəsinə quraşdırılırlar (yapışdırılırlar). Odur ki, modullar arasında dəqiq interfeys olmalıdır və bu interfeysdən ümumi məsələlərin həll edilməsində (modulların qarşılıqlı əlaqəsi yaranan zaman) istifadə edilir.

Belə əməliyyat sisteminə Windows əməliyyat sistemini nümunə göstərmək olar. Burada müdafiənin altsistemi əməliyyat sisteminin ümumi arxitekturasında dəqiq seçilir (ayrılır). Amma UNIX əməliyyat sistemində müdafiə funksiyası praktiki olaraq əməliyyat sisteminin bütün elementlərinə paylanmışdır.

Qeyd etmək lazımdır ki, istənilən əməliyyat sistemi standart müdafiəni təmin edirsə, onda həmin əməliyyat sistemi öndə sadalanan funksiyaları yerinə yetirməlidir. Adətən

əməliyyat sisteminin müdafiə altsistemi proqram modulunun əlavə genişlənməsinə sazlanmış olur.

ƏLÇATANLIQ SUBYEKTLƏRİNİN İDENTİFİKASİYASI, AUTENTİFİKASİYASI VƏ AVTORİZASİYASI

Müdafiə olunan əməliyyat sistemində istənilən istifadəçi (əlçatanlıq subyekti) sistem ilə işə başlamazdan əvvəl identifikasiyadan (eyniləşdirmədən), autentifikasiyadan (mötəbərlikdən) və avtorizasiyadan (vəkalət vermədən) keçməlidir. *Əlçatanlıq subyekti* (və ya sadəcə olaraq *subyekt*) dedikdə əməliyyat sisteminin elementləri üzərində əməliyyatların yerinə yetirilməsinə təşəbbüs göstərən istənilən varlıq nəzərdə tutulur. Bir çox hallarda istifadəçi əlçatanlıq subyekti hesab olunur.

Əlçatanlığın identifikasiya subyekti dedikdə subyektin özü haqqında (adı, hesab nömrəsi, və s.) identifikasiya edilmiş informasiyanın varlığını məlimat verməklə bildirir, yəni özünü identifikasiya edir.

Bəzən subyektin doğurdan da həmin şəxs olduğunu sübut etmək tələb olunur, bu autentifikasiya prosesidir. Prosesin məqsədi kanar şəxsin sistemə daxil olmasının qarşısının alınmasıdır.

Subyektin autentifikasiya olunması dedikdə subyekt əməliyyat sisteminə identifikasiya olunmuş informasiya ilə autentifikasiya olunuş informasiyanı da təqdim etməsi başa düşülür.

Subyektin avtorizasiya olunması dedikdə əlçatanlığın baş verməsi, identifikasiya və autentifikasiya prosedurlarının əlverişli şəkildə yerinə yetirilməsi başa düşülür. Subyektin

avtorizasiya olunmasında əməliyyat sistemi subyektin sistemdə iş başlaması üçün lazım olan fəaliyyəti yerinə yetirilir. Məsələn, UNIX əməliyyat sistemi istifadəçinin işləməsinə yardımçı olacaq əməliyyat buludunu yaradır. Windows əməliyyat sistemində istifadəçinin avtorizasiyası əlçatanlıq markerinin yaradılmasına şərait yaradır və s. Subyektin avtorizasiya proseduru əməliyyat sisteminin müdafiə altsisteminə bir-başa bağlı deyil. Avtorizasiya prosedurunda texniki məsələlər həll edilir. Bu məsələlər sistemdə subyektin identifikasiya və autenyifikasiya prosedurları ilə əlçatanlıq baxımından əlaqəlidirlər.

Əməliyyat sisteminin təhlükəsizliyinin təmin edilməsi baxımından identifikasiya və autentifikasiya prosedurları son dərəcə məsuliyyətli hesab olunurlar. Doğurdanda, əgər pisniyyətli insan sistemə başqa bir istifadəçinin adından istifadə etməklə daxil olubsa, bu zaman o istifadəçinin daxil ola bildiyi bütün obyektlərə asanlıqla daxil ola bilir. Belə olan halda auditin altsistemi əməliyyat sisteminin təhlükəsizliyi üçün potensial təhlükəli olan baş vermiş hadisələr barədə məlumatı generasiya edirsə, onda auditin jurnalında istifadəçinin adından istifadə edən və sistemdə işləyən bədniyyətli insanın adı deyil, istifadəçinin adı yazılmış olacaqdır.

ƏMƏLİYYAT SİSTEMLƏRİ OBYEKTİNƏ ƏLÇATANLIĞIN MƏHDUDLAŞDIRILMASI

Əməliyyat sistemləri obyektlərinə əlçatanlığın məhdudlaşdırılma prosesinin əsas anlayışı obyektə və subyektə əlçatanlıq üsulu, həmçinin obyektə əlçatanlıqdır.

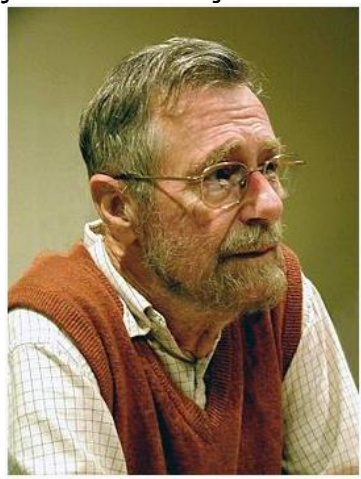
Əlçatanlıq obyekti (sadəcə olaraq obyekt) əməliyyat sisteminin istənilən obyekti hesab edilə bilər. Bunlara istifadəçilərin və digər subyektlərin əlçatanlığı ola bilsin ki, heç

bir şeyə əsaslanmadan məhdudlaşdırılsın. Əməliyyat sisteminə daxil olma imkanı təkcə əməliyyat sisteminin arxitekturası ilə deyil, cari təhlükəsizlik siyasəti ilə də müəyyən olunur. Daxilolma obyektləri kimi avadanlıq resursları (məsələn, prosessor, yaddaşın seqmentləri, disklər və yaddaş lentləri), proqram resursları (məsələn, fayllar, proqramlar, ***semaforlar***), və nəhayət, nə varsa, onlara daxil olma həmişə nəzarətdədir. Hər bir obyekt özünəməxsus unikal ada malikdir, bu adlar sistemdəki digər obyektlərdəki adlardan fərqlənirlər və onlardan hər biri yaxşı müəyyən edilmiş və əhəmiyyəti olan əməliyyatlara daxil ola bilir.

Obyektə əlçatanlıq metodu obyekt üçün müəyyən olunmuş əməliyyat adlanır. Əməliyyatın növü obyektdən asılıdır. Məsələn, prosessor əmr yerinə yetirir, yaddaş seqmentləri yazılır və oxuna bilir, maqnit disk hesablayıcıları ancaq oxuya bilir, fayllar üçün "oxumaq" və "əlavə etmək" (faylın sonuna informasiya əlavə etmək nəzərdə tutulur) üçün əlçatanlıq metodu müəyyən edilir və s.

Subyektə əlçatanlıq obyekt üzərində əməliyyatı yerinə yetirməyə imkanı olan (obyektə bir neçə əlçatanlıq üsulu ilə müraciət edə bilən), təşəbbüs göstərə bilən istənilən varlıq nəzərdə tutulur (adlanır). Bir çox hallarda obyektlər çoxluğuna əlçatanlıq ilə subyektlər çoxluğuna əlçatanlığın kəsişmədiyini qeyd edirlər. Bəzi hallarda əlçatanlıq subyektinə sistemdə yerinə yetirilən prosesləri aid edirlər. Amma əlçatanlıq subyekti kimi istifadəçinin adını hesab etmək məntiqə uyğundur (o adı ki, proses həyata keçirilir). Əlçatanlıq subyekti kimi kompüterdə işləyən fiziki istifadəçi deyil, əməliyyat sistemində yerinə yetirilən prosesin "məntiqi" istifadəçisinin adı götürülür.

AŞIQLAMA: *Semafor* (ingiliscə semaphore) kodun verilmiş sahəsinə daxil ola biləcək axınların sayını məhdudlaşdıran obyektdir. Termin ilk dəfə Edsqer Deykstr tərəfindən istifadə olunmuşdur. Semaforlar bölünmüş yaddaşdan keçən verilənlərin ötürülməsinin müdafiə edilməsi və sinxronlaşdırılması üçün istifadə olunur. Bununla yanaşı semaforlardan proseslərin və axınların yerinə yetirdikləri işlərin sinxronlaşdırılması üçün də istifadə edirlər.



Edsqer Vibe Deykstr (niderlandca Edsger Wybe Dijkstra, 1930-cu ilin may ayında Niderlandın Rotterdam şəhərində anadan olmuşdur, 2002-ci ilin avqust ayında Hyuenen şəhərində dünyasını dəyişmişdir), Niderland alimidir, elmi əsərləri "İnformatika və informasiya texnologiyaları" sahələrinin inkişafına təsir göstərmişdir. E.Deykstr struktur proqramlaşdırmanın konsepsiyasını hazırlayanlardan biridir, formal ***verifikasiya*** və paylanmış hesablamaların araşdırıcılarından biri hesab edilir. A.Türinq adına mükafata layiq görülmüşdür (1972).

Verifikasiya (latınca *verus – həqiqi*, *facere – etmək*) – istənilən nəzəri yolla alınmış verilənlərin təcrübi (empirik) yolla alınmışlarla müqayisə edilməsidir, yoxlanmasıdır, sinanmasıdır, əsaslandırılmasıdır və s. üsullarıdır. Verifikasiya verilənlərin əslliyinin təsdiq olunması aktı və ya prosesidir. İnternetdə verifikasiyadan bu və ya digər

saytda qeydiyyat yazıları sahibinin şəxsiliyini təsdiq etmək üçün istifadə edirlər.

Beləliklə, *obyekt əlçatandır* - nəyə görə əlçatanlıq yerinə yetirilir, *subyekt əlçatandır* – kimə görə əlçatanlıq yerinə yetirilir, *üsul (metod) əlçatandır* – necə əlçatanlıq yerinə yetirilir kimi qəbul olunmalıdır.

Obyekt üçün *sahib* müəyyən oluna bilər. Sahib – cari obyektin kimə məxsus olduğunu müəyyən edən, obyektdə olan informasiyanın konfidensiallığına cavabdehlik daşıyan, obyektə əlçatlıq və obyektin tamlığına görə məsuliyyət daşıyan subyekt qəbul olunur.

Adətən obyektin sahibi avtomatik olaraq cari obyekti yaradanı subyekt kimi təyin edir, sonrakı mərhələlərdə isə obyektin sahibi obyektə əlçatanlıq üsuluna uyğun olaraq dəyişə bilər. Amma sahib qanuna görə başqa subyektlərin cari obyektə daxil olmalarına konkret məhdudiyyətin qoyulmasına cavabdehlik daşıyır.

Obyektə əlçatanlıq hüquqi (ixtiyarı) obyektə daxil olmaq üçün yerinə yetirilən bir para və ya qrup halında olan üsullar adlanır. Məsələn, əgər istifadəçinin faylı oxumağa imkanı varsa, onda onun bu faylı oxumağa da ixtiyarı vardır.

Subyektlərin obyektlərə əlçatanlığın məhdudlaşdırılması qanunlar toplumundan ibarətdir, toplum hər bir üçlük (subyekt – obyekt – üsul) üçün cari subyektin cari obyektə cari üsulla daxil olmasına imkan verilməsini müəyyənləşdirir.

Subyekt obyektə daxil olmaq üçün məhdudlaşdırılmış qanunları nəzərə almırsa, onda əlçatanlığı *superistifadəçi* adlandırırlar.

Əlçatanlığın məhdudlaşdırılması qanunları. Fəaliyyətdə olan əməliyyat sistemində qanunlar sistem

administratoru tərəfindən cari təhlükəsizlik siyasətini müəyyən edən zaman müəyyin edilir. Bu qanunlara nəzarət əməliyyat sistemində müdafiənin altsisteminin bir hissəsi olan *istinad monitoru* tərəfindən yerinə yetirilir.

Əlçatanlığın məhdudlaşdırılması qanunları aşağıdakı tələbləri yerinə yetirməlidir:

1.Əməliyyat sisteminə quraşdırılmış, təşkilat tərəfindən qəbul edilmiş, qanunlara analoji olaraq uyğun olan qanunları dəstəkləməlidir, yəni qoyulmuş qanunlara əsasən istifadəçi qeyriqanuni informasiyaya əlçatanlıq edirsə, onda istifadəçiyə bu əlçatanlıq qadağan olunmalıdır.

2.Əməliyyat sisteminin normal işləməsinə maneçilik edən, qeyriqanuni yerinə yetirilən, dağıdıcı təsir göstərən subyektlərin əməliyyat sisteminə daxil olmasına yol verilməməlidir.

3.Hər bir obyektin sahibi olmalıdır. Heç kimin obyekti olmayan obyektin (sahibsiz obyektin) varlığı icazə verilən deyil.

4.Heç bir subyektin müraciət edə bilməyəcəyi və yaxud, heç bir qanuna riayət edə bilməyən obyektin olmasına icazə verilmir.

5.Məxfi informasiyanın axmasına icazə verilməməlidir.

Əlçatanlığın iki əsas modeli mövcuddur:

- Seçməklə (diskression);
- Müvəkkil (mandatlı).

Seçməklə olan modeldə subyekt və ya subyektlər qrupu üzərində konkret əməliyyatın aparılmasına ya icazə verilir, ya da ki, icazə verilmir. Əksər əməliyyat sistemləri seçməklə üsulundan bəhrələnirlər.

Müvəkkil üsulunda bütün obyektlər məxfilik səviyyəsindədirlər, amma subyektlər isə informasiyaya əlçatanlıq səviyyəsinə uyğun ierarxiya əmələ gətirirlər. Bəzən

model təhlükəsizliyin çoxsəviyyəli modeli adlandırılır. Model məxfiliyin saxlanması üçün yararlıdır.

ƏLÇATANLIĞIN SEÇMƏKLƏ MƏHDUDLAŞDIRILMASI

Əlçatanlığın seçməklə məhdudlaşdırılması sistemi qanuna uyğun olaraq aşağıdakı kimi formalaşdırılır:

- Əməliyyat sistemi obyektinin sahibi vardır;
- Obyektin sahibi digər subyektlərin ixtiyarı olaraq daxil olmasını məhdudlaşdırır;
- Hər üçlük üçün (subyekt-obyekt-üsul) əlçatanlığın müəyyən edilməsi eynidir;
- Heç olmasa bir imtiyazlı (üstün) istifadəçi (administrator) vardır ki, o istənilən üsulla istənilən obyekta müraciət etmə imkanına malikdir.

İmtiyazlı istifadəçi obyektə əlçatanlığın məhdudlaşdırılmasına əhəmiyyət verməyə bilməz. Məsələn, Windows NT əməliyyat sistemində administrator kanar obyektə (başqa subyektə məxsus olan obyektə) müraciət etmək üçün əvvəlcə bu obyektin sahibi olduğunu elan etməlidir (administratorun istənilən obyektə sahiblik çıxma üstünlüyündən istifadə etməsi ilə), sonra özünə lazım olan üstünlüklərdən istifadə etməklə həmin obyektə müraciət edə bilər. Həyata keçirilən sonuncu tələb potensial daxil olmaq imkanından məhrum olan obyektlərə aid deyildir.

Obyektlərə daxil olma imkanı olan subyektlər əlçatanlığın seçməklə məhdudlaşdırılmasından istifadə etməklə yeni anlayışdan - əlçatanlıq matrisi və təhlükəsizlik domeni anlayışından istifadə edir. Əlçatanlıq matrisinin sətirlərində əlçatanlığın subyektləri, sütunlarında - əlçatanlığın obyektləri,

hücrələrində isə - əməliyyatlar sadalanır. Bu sadalananları subyekt obyekt üzərində yerinə yetirə bilər.

Təhlükəsizlik domeni (protection domain) əməliyyat sisteminin hər bir obyekti üzərində yerinə yetirilə bilən obyektlər toplumunu və əməliyyatların növünü müəyyən edir.

Əməliyyat sistemində işləyən konkret obyektlər arasında əlaqə aşağıdakı şəkildə təşkil edilmişdir:

- Hər bir istifadəçi domen ola bilər. Belə olan halda əlçatanlıq təmin olunan obyektlər toplusu istifadəçinin identifikasiyasından asılıdır;
- Hər bir proses domen ola bilər. Belə olan halda əlçatanlıq obyektlərinin toplusunu prosesin identifikasiyası müəyyən edir;
- Hər bir prosedura domen ola bilər. Belə ola halda əlçatan obyektlər toplusu prosedurun daxilində müəyyən edilən lokal dəyişənlərlə müəyyən edilir. Qeyd etmək lazımdır ki, prosedurun yerinə yetirilməsi domenin dəyişməsinə səbəb olur.

Əlçatanlığın seçməklə məhdudlaşdırılmasının üsyünlüyü cevikliyidir (uyuşanlığıdır). Çatışmazlığı mərkəzləşdirilmiş nəzarətin mürəkkəb olması və idarəetmənin səpələnməsidir.

Əlçatanlığın seçməklə məhdudlaşdırılmasında müdafiənin altsistemi tərəfindən əməliyyat sisteminin müdafiə olunmasının təşkili bəzi hallarda kifayətedici olmur. Məsələn, ABŞ-da dövlət əhəmiyyətli informasiyanın (əgər informasiya əlçatanlığın seçməklə məhdudlaşdırılmasını dəstəkləyirsə) kompüter sistemlərində saxlanılması qadağan olunmuşdur.

Əlçatanlığın seçməklə məhdudlaşdırılmasının genişləndirilmiş modeli izolə edilmiş (qapanmış) proqram mühiti sayılır.

İzolə edilmiş proqram mühitində subyektin obyektə daxil olma hüquqi təkcə subyektin üstünlüyü və hüquqi ilə deyil, subyektin obyektə müraciət etmə prosesi ilə müəyyən olunur. Məsələn, *doc.* genişlənməsi olan fayllara müraciət Word, Word Viewer və WPview proqramlarına müraciət etməklə həyata keçirilə bilər.

İzolə edilmiş proqram mühitində əməliyyat sistemi dağıdıcı proqramın təsirlərindən müdafiə olunmaq üçün (bura proqram əlavələri ilə birlikdə kompüter viruslarını da əlavə etmək lazımdır) müdafiə qabiliyyətini artırır. Bununla yanaşı cari modeldən istifadə etməklə sistemdə saxlanılan verilənlərin tamlığı da müdafiə edilir.

ƏLÇATANLIĞIN MÜVƏKKİL MƏHDUDLAŞDIRILMASININ İNFORMASİYA AXININA NƏZARƏTİ

Müvəkkil və ya mandatlı, əlçatanlığın məhdudlaşdırılması (mandatory access control) adətən əlçatanlığın seçilmiş məhdudlaşdırılması toplumuna tətbiq edilir. Dərslikdə belə bir modelə baxış keçirilir. Əlçatanlığın məhdudlaşdırılması qaydaları cari modeldə aşağıdakı kimi formalaşır:

1.Əməliyyat sisteminin istənilən obyekti üçün sahib vardır.

2.Obyektin sahibi istənilən məhdudiyyət ilə istənilən obyektin cari obyektə daxil olmasını yerinə yetirə bilər.

3.Hər bir dördlük üçün (subyekt-obyekt-üsul-proses) əlçatanlıq hər bir anda mütləq formada mümkündür. Prosesin zamana görə vəziyyətinin dəyişməsi əlçatanlığın da dəyişməsinə səbəb olur. Bununla yanaşı hər bir an üçün əlçatanlıq mütləqdir. Prosesin hüquqi zamana görə obyektə daxil olması dəyişdiyindən onun açıq obyekt üzərində həyata

keçirilməsi, yəni oxunması və yazılması əməliyyatları yoxlanılmalıdır.

4.Heç olmasa üstünlüyə malik istifadəçi (administrator) vardır ki, istənilən obyekti ləğv edə bilsin.

5.Obyektlər çoxluğundan səlahiyyətli obyekt seçilir. Hər bir obyekt məxfi qrifə malikdir. Obyektlərin məxfi qrifinin sayı artdıqca, obyekt bir o qədər məxfi sayılır. Əgər məxfi qrif sıfır qiymətə maliksə, onda obyekt məxfi sayılmır. Belə olan halda məxfi olmayan obyektə istifadəçi istənilən anda müraciət edə bilər.

6.Əlçatanlığın hər bir subyekti buraxma səvyyəsinə malikdir. Buraxma səviyyəsinin rəqəmlərlə qiyməti nə qədər yuxarı olarsa, bir o qədər də (yəni böyük səviyyəyə) subyekt buraxma səviyyəsinə malik olur. Buraxma səviyyəsinin "sıfır" qiymətində subyektin buraxma səviyyəsi yoxdur. Adətən subyektin "sıfır"dan fərqli qiymətləri istifadəçi-subyekt tərəfindən müəyyən edilir.

7.Subyektin obyektə əlçatanlığına qadağa qoyulması əlçatanlıq matrisinin vəziyyətindən asılı olmamalıdır.

8.Əməliyyat sistemində hər bir prosesin *konfidensiallıq (məxfilik) səviyyəsi* vardır. Məxfilik səviyyəsi obyektlərin gizli qriflərinin maksimumuna bərabərdir. Konfidensiallıq səviyyəsi faktiki olaraq informasiyanın gizli qrifini əks etdirir. Gizli qrif operativ yaddaşda saxlanılır.

9.Əlçatanlıq matrisinin vəziyyətindən asılı olmadan obyektdən obyektdə daxil olmağa qadağa qoyulmalıdır.

10.Obyektin gizli qrifini azaltmaq (zəiflətmək) üçün subyekt xüsusi üstünlüyə malik olmalıdır.

Göstərilən modeldən istifadə olunması zamanı ən çox əməliyyat sisteminin məhsuldarlığı mənəvi əzab çəkir. Bununla yanaşı model istifadəçiyə müəyyən əlverişsizlikdə yaradır: əgər

prosesin konfidensiallıq səviyyəsi "sıfır"dan yuxarıdırsa, onda yaddaşda olan bütün informasiya faktiki olaraq gizli hesab olunur və gizli olmayan obyektə yazıla bilmir.

Qeyd etmək lazımdır ki, əməliyyat sistemi istifadəçisi cari modeldən istifadə edirsə, onda bu modeli nəzərə almaqla hazırlanmış proqram təminatından istifadə etməlidir. Əks təqdirdə istifadəçi ciddi problemlərlə üzləşəcəkdir.

Nəzərə almaq lazımdır ki, araşdırılan hər bir modelin müəyyən üstün və çatışmayan cəhətləri vardır.

AUDİT

Əməliyyat sisteminə *audit* prosedurunun tətbiqi əməliyyat sistemi üçün təhlükə sayılan hadisələrin *audit jurnalında* və ya *təhlükəsizlik jurnalında* qeyd edilməsi ilə əlaqəlidir. Audit jurnalını oxumağa hüquqi olan sistem istifadəçisi *auditor* adlanır.

Auditin funksiyasına aşağıdakılar daxildir:

- Müdafiə sisteminin əsas məqsədi sistemə ediləcək hücumu aşkar etməkdir, çünki məsələnin həll edilməsi sistemə daxil olmadan (zorla girmədən) əmələ gəlmiş ziyanı minimuma endirir və zorla daxil olma üsulları haqqında informasiya toplamağa imkan verir;
- Əməliyyat sisteminin müdafiə altsistemi bəzən təsadüfi səhvləri qəsd ilə edilmiş hərəkətlərdən fərqləndirə bilmir. Belə olan halda administrator audit jurnalına baxış keçirir, istifadəçi tərəfindən parolun düzgün daxil olunmamasını müəyyən edir, səhvin leqal istifadəçi tərəfindən və yaxud da, bədniyyətli insan tərəfindən yerinə yetirildiyini müəyyənləşdirir. Əgər istifadəçi parolu

20-30 dəfə tapmağa cəhd göstərmişsə, onda bu açıq-aşkar parolun seçilməsinə edilən cəhddir;

- Əməliyyat sistemi inzibatçısı təkcə sistemin cari vəziyyəti haqqlnda deyil, əvvəllərdə necə işləməsi barədə informasiya əldə etməldir. İstifadəçiyə belə imkanı audit jurnalı təqdim edir;
- Əgər administrator əməliyyat sisteminə bədniyyətli insan tərəfindən tutarlı səviyyədə hücumun edildiyini, hücumun necə yerinə yetirildiyini və hansı vəziyyətdə icra olunduğunu müəyyən etmişsə, nəzərə almaq lazımdır ki, bütün bunlar audit jurnalında qeyd olunmuşdur.

Əməliyyat sistemi üçün təhlükə törədə biləcək hadisələrə aşağıdakıları aid etmək olar:

- Sistemə giriş və ya çıxışın olması;
- Fayllar üzərində yerinə yetirilmiş əməliyyatlar (faylın açılması, bağlanması, adının dəyişdirilməsi, ləğv edilməsi);
- Uzaqlaşdırılmış sistemə müraciətin edilməsi;
- Təhlükəsizlik atributlarının dəyişdirilməsi (əlçatanlıq rejimi, istifadəçinin sədaqətlilik səviyyəsi və s.).

Əgər audit jurnalında bütün hadisələr qeyd olunarsa, onda jurnalda informasiyanın həcmi sürətlə artacaq, nəticədə istifadəçi hadisələri təhlil etməkdə çətinlik çəkəcək. Odur ki, lazım olanların qeyd olunması bütün hallarda əlverişlidir.

Auditə qoyulan tələbat. Əməliyyat sisteminin audit altsistemi aşağıdakı tələbləri ödəməlidir:

- Audit jurnalına əlavələr etməyə ancaq əməliyyat sisteminin imkanı vardır;
- Audit jurnalına olunmuş qeydləri heç bir subyekt (əməliyyat sistemi də daxil olmaqla) ləğv edə bilməz;

- Audit jurnalına baxış keçirməyə ancaq müəyyən üstünlüyü olan istifadəçi edə bilər;
- Audir jurnalını ancaq istifadəçi-auditor "təmizləyə" bilər;
- Audit jurnalı dolduqda əməliyyat sistemi qəza halında işi tamamlayır ("zavizanie – asılılıq" baş veirir). Sistem yenidən yükləndikdən sonra onunla ancaq auditor işləyə bilər. Bu zaman audit jurnalı "təmizlənir" və əməliyyat sistemi adi iş rejiminə keçir.

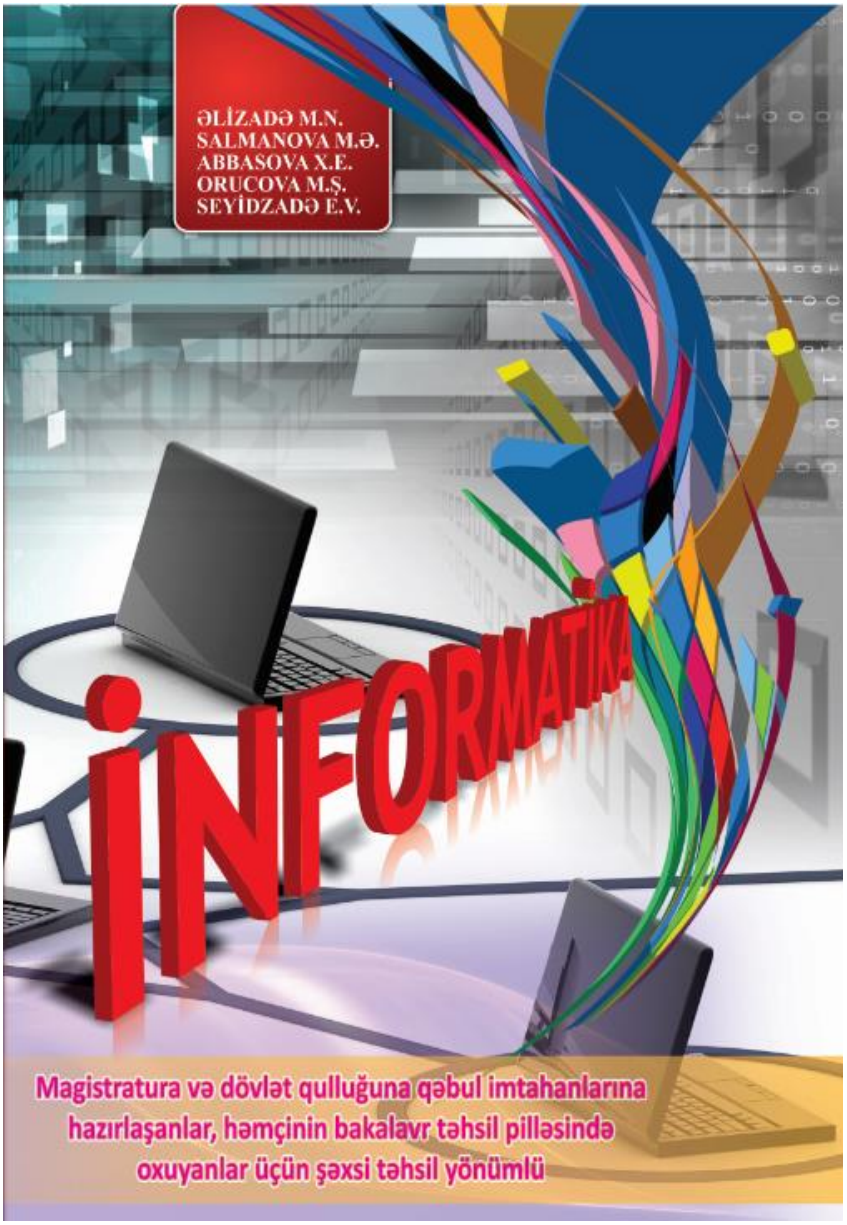
Audit jurnalına əlçatanlığın məhdudlaşdırılması üçün xüsusi müdafiə vasitələrindən istifadə olunmalıdır.

Asudit siyasəti – qaydalar toplumudur, audit jurnalında hansı hadisənin qeyd olunmasını müəyyən edir. Əməliyyat sisteminin etibarlı müdafiə edilməsi üşün audit jurnalında aşağıdakı hadisələrin qeyd edilməsi vacibdir:

- Sistemdən istifadəçinin giriş/çıxış cəhdləri;
- İstifadəçilərin siyahısının dəyişdirilməsinə cəhdin göstərilməsi;
- Təhlükəsizlik siyasətinin dəyişdirilməsinə cəhd (o cümlədən audt siyasətinin dəyişdirilməsinə edilən cəhd).

Hadisələrin seçilərək audit jurnalında qeyd olunması auditorun boynundadır. Hadisələri seçən zaman audit jurnalın tez bir zaman ərzində dolacağını nəzərdə tutmalıdır, buna qarşı lazımı tədbirlər görməlidir. Audit siyasəti əməliyyat sistemində baş vermiş dəyişikliklərə operativ reaksiya verməlidir.

Bəzi əməliyyat sistemlərində audit siyasəti audit jurnalında baş vermiş hadisələrin qeydiyyatı ilə bərabər auditorları həmin hadisələr haqqında interaktiv xəbərdar da edir.


ƏLİZADƏ M.N.
SALMANOVA M.Ə.
ABBASOVA X.E.
ORUCOVA M.Ş.
SEYİDZADƏ E.V.
İNFORMATİKA
Magistratura və dövlət qulluğuna qəbul imtahanlarına
hazırlaşanlar, həmçinin bakalavr təhsil pilləsində
oxuyanlar üçün şəxsi təhsil yönümlü

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ VASİTƏLƏRİLƏ İDARƏETMƏ ÜSULLARI

Korporativ şəbəkələrin idarəetmə sistemlərinin əsas komponenti (təşkiledicisi) informasiyanın təhlükəsizliyi sistemidir. Sistem aşağıdakıları yerinə yetirməlidir:

- Şəbəkə təhlükəsizliyi vasitələrinə mərkəzləşdirilmiş və operativ idarəetmə təsiri göstərmək;
- Operativ qərarlar qəbul etmək üçün informasiya təhlükəsizliyinin vəziyyəti haqqında obyektiv informasiya əldə etməyə imkan verən mütamata audit və monitorinq keçirmək.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ VASİTƏLƏRİLƏ İDARƏETMƏ MƏSƏLƏLƏRİ

Müəssisə miqyasında şəbəkə təhlükəsizliyi vasitələrilə idarəetmənin əsas məsələlərini formalaşdıraq. Müəssisə miqyasında paylanmış şəbəkədə informasiyanın müdafiə vasitələrinin idarə edilməsi sistemi funksional şəkildə aşağıdakı məsələləri həll etməlidir:

- *Təhlükəsizliyin qlobal siyasətinin* (TQS) idarə edilməsi. Müəssisə şəbəkəsi çərçivəsizdə təhlükəsizliyin qlobal siyasətinin (TQS) idarə edilməsi, bəzi vasitələrin *lokal təhlükəsizlik siyasətinin* (LTS) formalaşdırılması və informasiyanın müdafiəsi ilə bağlı olan bütün vasitələrin lokal təhlükəsizlik siyasətinə qədər çatdırılması;
- Əlçatanlıq obyektlərinin və subyektlərinin quruluşunun idarə edilməsi. Bura heyətlə, versiyalarla, vasitələrin

təşkilediciləri ilə, proqram təminatının müdafiəsi ilə idarə etmə, həmçinin təhlükəsizliyin təmin edilməsi məhsullarında aşkar edilmiş deşiklərin bağlanması üçün xidmət göstərən patçlar (***patch***) ilə idarə etmə daxildir;

- Paylanmış tətbiqi sistemlərdə müdafiə servisinin, həmçinin müdafiə olunan əlavələrin və onların resurslarının təqdim edilməsi. Bu qrupa daxil olan əlavələr əvvəlcə tətbiqi sistem tərəfindən müdafiə servisi vasitəsilə idarə edilmənin təmin olunması interfeysini (API) təmin etməlidir;
- Kriptovasitələrin idarə edilməsi, xüsusilə də - açarlarla idarə etmə (açar infrastrukturu). Açar infrastrukturu infrastruktur xidmətin tərkibində işləməlidir (müəyyən funksiyanı yerinə yetirməlidir);
- Hadisələrin protokollaşdırılması. Protokollaşma müxtəlif qurğularda loqun aşkar olunmasının sazlanmasını, loqun ətraflı işlənmə səviyyəsinin idarə edilməsini, hadisələrin tərkibinin idarə edilməsini və s. yerinə yetirir;
- İnformasiya sistemlərinin təhlükəsizlik auditi. Təhlükəsizlik auditi informasiya sistemlərinin cari müdafiə vəziyyətinin obyektiv qiymətləndirilməsi, loqun təhlili (loqun təhlili dedikdə auditin təhlükəsizliyi başa düşülür), nizam-intizamı pozanların axtarılması, sistemdə yaranmış "deşik"lərin tapılması və s. funksiyaların ***loq*** tərəfindən idarə edilməsi ilə həll olunur;
- Sistemin təhlükəsizlik monitorinqi. Monitorinq qurğularda baş verən potensial hücumların, qurğuların aktivliyi və ***kontekst*** təhlükəsizliyi ilə bağlı baş verən hadisələri, real zamanda alınmış informasiyanı təmin edir;
- Xüsusi müdafiə olunan əlavələrin işləməsinin təmin edilməsi, əməliyyat üzərində nəzarətin yerinə yetirilməsi,

yerinə yetirilən tədbirlər (məsələn, açarın və parolun dəyişdirilməsi, qurğuların müdafiə edilməsi, smart-kartların buraxılışı və s.) reqlamentinin dəstəklənməsi;

- Layihə qrupunun işləməsinin təmin olunması, qrup tərəfindən müəssisənin şəbəkəsində müdafiə nöqtələrinin müəyyən edilməsi. Bura:
  - İstifadə edilən müdafiə vasitələrinin qeyd olunması;
  - Müdafiə vasitələrinin modul tərkibinə nəzarət;
  - Müdafiə vasitələrinin vəziyyətinə nəzarət və s. daxildir.

AÇIQLAMA: *Paçt* və ya *yamaq* (ingiliscə *patch* – *yamaq* anlamını verir) kompüter fayllarında müəyyən olunmuş dəyişikliklərin avtomatik yerinə yetirilməsi üçün nəzərdə tutulmuş informasiyadır. Bir çox hallarda patçın yerinə yetirilməsini "yamaq vurma"da adlandırırlar. Bəzi mənbələrdə patçı və ya yeniləməni (update) proqram təminatında və ya onun işləməsində baş vermiş dəyişikliklərin və ya problemlərin aradan qaldırılması üçün istifadə edilən proqram vasitələri kimi təqdim edirlər. Patçın ölçüsü bir neçə Kbaytdan yüzlərlə Mbayta qədər ola bilər. Patçın ölçüsünün artması yerinə yetirilən çoxlu sayda dəyişikliklər ilə bağlıdır. Bu baxımdan "paçt" və ya "yamaq" sözü çoxda böyük olmayan dəyişikliklərdə istifadə edilir, amma proqramın yenilənməsində və ya dəyişilməsində "service pack" və ya "software updates" sözündən istifadə düzgündür.

Vaxtı ilə kompüterlərə proqramı yükləyən zaman perfokartdan və ya kağız lentlərindən istifadə edilirdi. Odur ki, proqram yaradıcıları patçı perfokart kimi yayırdılar, yəni

perforasiya olunmuş perfokartda dəyişiklik etmək üçün yer ayırırdılar, daha doğrusu perfokartın üzərinə - ayrılmış yerə yeni proqram olan kağızı yapışdırırdılar – yamaq vururdular. Bu baxımdan da o vaxtlar perfokartda və ya perfolentdə ayrılmış yeri "patç" – "yamaq" adlandırmaq məsləhət bilinmişdi. Sonralar maqnit lentlərin, disketlərin istehsalı başlanılır, patç istifadəçiyə zərflərin içərisində göndərilir. İndiki zamanda İnternetdən istifadə edilən zaman kompüter proqramları və onların istifadəçiləri patçı sayt istehsalçılarının saytlarından "çəkirlər".

Loq (ingiliscə loq) – hadisələr jurnalı, gündəlik, protokol anlamını verir. *Loqlar* (Loq Files – Loq faylları) – saytların qiymətləndirilməsi və təhlili üçün istifadə edilən, serverin işləməsi barədə sistem informasiyanı özündə saxlayan fayllardır. Loqlar proqramın və ya istifadəçinin nə etdiyi barədə ətraflı protokoldır.

Kontekst (latınca *contextus* – "birləşmə", "əlaqə" anlamlarını verir) mətnin yazılı və ya şifahi formada olan tamamlanmış hissəsidir. Kontekst ümumi mənada mətnə daxil olan ayrı-ayrı sözlərin, cümlələrin və i.a. müəyyənləşdirilməsinə imkan verir.

Şəbəkədə informasiya vasitələrinin idarəetmə sisteminin müəyyən problemləri yaranır ki, onlarında həll edilməsinə iki yanaşma tətbiq edilir. Birinci yanaşma şəbəkə vasitələrinin və ya sistemlə idarəetmənin (müdafiə vasitələrinin idarəedilmə mexanizmi ilə birlikdə) inteqrasiyası ilə, ikinci yanaşma isə təhlükəsizliyin idarəetmə məsələlərinin həll edilməsi üçün istifadə edilən vasitələrin istifadəsi ilə əlaqəlidir.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ VASİTƏLƏRİLƏ İDARƏETMƏ ARXİTEKTURASI

Müəssisənin resurslarının informasiya təhlükəsizliyinin təmin edilməsi üçün informasiya müdafiə vasitələrini adətən bilavasitə korporativ şəbəkələrdə yerləşdirirlər. Şəbəkələrarası ekran korporativ resurslara əlçatanlığa nəzarətlə yanaşı kanardan pisniyyətli insanın etdiyi hücumların da qarşısını alır, virtual xüsusi şəbəkə şlüzləri (VPN) isə açıq qlobal şəbəkədən (İnternet nəzərdə tutulur) informasiyanın ötürülməsi zamanı konfidensiallığı təmin edir. İndiki zamanda etibarlı eşelonlaşdırılmış müdafiə sistemi yatartmaq üçün zorla girmələri (soxulmaları) aşkar etmə sistemindən (IDS – Intrusion Detection Systems), informasiyanın məzmununa əlçatanlığa nəzarət vasitələrindən, antivirus sistemlərindən və s. istifadə olunur.

Əksər korporativ informasiya sistemləri (KİS) müxtəlif istehsalçılar tərəfindən istehsal olunan proqram və aparat vasitələrinə əsaslanaraq qurulmuşdur. Vasitələrin hər biri mükəmməl və xüsusi quruluşa uyğun hazırlanmışdır və istifadəçi ilə əlçatan resurslar arasında qarşılıqlı əlaqəni əks etdirirlər. ***Heterogen*** korporativ informasiya sistemlərində etibarlı informasiya müdafiəsini təmin etmək üçün korporativ informasiya sistemlərinin təhlükəsiz idarəetmə sistemini yaratmaq lazımdır. Yaradılmış sistem korporativ informasiya sisteminin hər bir təşkiledicisini düzgün sazlamaqla yanaşı təhlükəsizliyinidə təmin etməlidir. Bunun üçün sistemdə baş verən dəyişikliklər izlənməli, yaranmış yarıq (zədə, dəlik, deşik) "tutulmalı", istifadəçinin işinə nəzarət olunmalıdır. Nəzərə almaq lazımdır ki, informasiya sistemi nə qədər müxtəlif olarsa,

onun təhlükəsizliyinin idarə edilməsi bir o qədər də mürəkkəb olcaqdır.

AÇIQLAMA: *Heterogen* (yunanca ἕτερος -başqa + γένω –cins) – müxtəlif cinsli, yabanşı, tərkibdə eyni olmayan hissələrin varlığı, nəyinsə tərkibində olmaq və s.

ƏSAS ANLAYIŞLAR

Aparıcı şəbəkə təhlükəsizliyi vasitələri istehsalçı-müəssisələrin təcrübəsi göstərir ki, şirkət paylanmış korporativ informasiya sistemlərinin təhlükəsizlik siyasətini əlverişli həyata keçirə bilər. Bunun üçün təhlükəsizliyin idarə edilməsi mərkəzləşdirilmiş olmalı, istifadə edilən əməliyyat sistemlərindən və tətbiqi sistemlərdən asılı olmamalıdır. Bununla yanaşı korporativ informasiya sistemlərində hadisələrin qeydiyyat sistemi (məsələn, qeyriqanuni əlçatanlıq, istifadəçinin üstünlüyünün dəyişməsi və i.a.) vahid olmalıdır, çünki bundan istifadə edən administrator (inzibatçı) korporativ informasiya sistemlərində baş verən dəyişikliyi tam təsvir edə bilməlidir.

Təhlükəsizliyin idarə edilməsi ilə bağlı müəyyən məsələləri həll etmək üçün vahid üfqi infrastruktur növlü X.500 kataloqun istifadəsi məsləhət bilinir. Məsələn, şəbəkə əlçatanlığı siyasəti istifadəçinin identifikasiyasını bilməyi tələb edir. Bu informasiya dəgər əlavələrdə də istifadə edilə bilər, məsələn, kadrların uçotu sistemində, əlavələrə birdəfəlik daxil olmalarda (Single Sign-On) və i.a. Eyni verilənlərin təkrarlanması sinxronlaşdırmaya gətirib çıxarır, yerinə yetirilən işlərin çətinləşməsinə və çaşğınlığın yaranmasına səbəb olur. Bütün bunlardan yan keçmək üçün *vahid üfqi infrastrukturdan* istifadə edilir.

Müxtəlif istifadəçi altsistemlərində istifadə olunan, müxtəlif OSI/ISO səviyyələrində işləyən üfqi sruktura aşağıdakılar aid etmək olar:

- *Açıq açarlarla idarəetmə infrastrukturu PKI*. İdarəetmə üçün əsas sayılan, amma geniş yayılmamış maraqlı faktı qeyd etmək lazımdır. İndiki zamanda əsasən "şəxsiyyəti göstərən vəsiqə" adlanan rəqəmsal sertifikatdan istifadə edilir (identity certificates), amma haradasa istifadə olunan və inkişafda olan "üfqi fərman" əlçatanlığı çevik idarə edən rəqəmsal sertifikat tətbiq edilir (credential certificatec);
- *Kataloqlar*. Məsələn, əlçatanlıqla idarə edilən sistemlər üçün lazımlı olan istifadəçi identifikatoru və istifadəçi haqqında başqa məlumatlar. Qeyd etmək lazımdır ki, kataloqlar verilənləri saxlamaq üçün istifadə olunmaqla yanaşı onlara əlçatanlıq siyasəti, sertifikatlar, əlçatanlıq siyahıları və başqaları da yerləşdirilir;
- *Autentifikasiya sistemləri*. Bunlara RADIUS, TACACS, TACACS+ serverləri aiddir;
- *Monitorinq və audit hadisələrinin protokollaşdırılması sistemləri*. Qeyd etmək lazımdır ki, bu sistemlər çox vaxt vertikal olmurlar, onlar əksər hallarda konkret altsistemin marağına uyğun olaraq avtonom işləyir və ixtisaslaşdırılırlar.

Təhlükəsizliyin qlobal idarə etmə konsepsiyası şirkətin heterogen şəbəkə təhlükəsizliyinin idarə edilməsinin effektiv ierarxik sistemini qurmağa imkan verir. Şəbəkə TrustWorks Systems şirkəti tərəfindən yaradılmışdır.

Mərkəzləşdirilimiş korporativ informasiya sistemləri təhlükəsizliyinin idarə edilməsinin təşkili aşağıdakı prinsiplərə əsaslanır:

- Korporativ şəbəkənin təhlükəsizliyinin idarə edilməsi təhlükəsizliyin qlobal siyasəti (TQS) səviyyəsində həyata keçirilməlidir. Bura korporativ şəbəkə obyektləri arasında qarşılıqlı təsirin təhlükəsizlik baxımından dəstəklənməsi qanunları, korporativ şəbəkələr ilə xarici obyektlər arasında əlaqənin təhlükəsizliyi daxildir;
- Şirkətin biznes-prosesi təhlükəsizliyin qlobal siyasətinə uyğun olmalıdır. Bunun üçün obyektlərin təhlükəsizliyi və tələb olunan təhlükəsizlik şirkətin quruluşuna və biznesinə uyğun təşkil olunmalıdır;
- Ayrı-ayrı müdafiə vasitələri üçün lokal təhlükəsizlik siyasəti (LTS) formalaşdırılmalıdır. LTS-in translyasiyası təhlükəsizliyin qlobal siyasəti qaydalarına və müdafiə olunan şəbəkənin topologiyasına uyğun avtomatik yerinə yetirilməlidir.

Mərkəzləşdirilimiş korporativ informasiya sistemləri təhlükəsizliyinin idarə edilməsinin metodologiyası müasir təhlükəsizlik texnologiyasını ətraflı əks etdirdiyi üçün bu metodologiyanı və onun bəzi aspektlərini ətraflı nəzərdən keçirək.

TƏHLÜKƏSİZLİYİN İDARƏEDİLMƏSİNİN QLOBAL KONSEPSİYASI

Mərkəzləşdirilimiş korporativ informasiya sistemləri təhlükəsizliyinin idarə edilməsinin əsasında təhlükəsizliyin idarə ediməsinin qlobal konsepsiyasi GSM (Global Security Management) dayanır. Təhlükəsizliyin idarə edilməsinin qlobal konsepsiyasi kompleks idarəetmə sisteminin və müəssisənin informasiya resurslarının müdafiəsinin qurulmasını aşağıdakı xüsusiyyətlərə uyğun həyata keçirilməsinə imkan verir:

- Müəssisənin təhlükəsizlik siyasəti bazasında bütün mövcud vasitələrin müdafiəsinin idarə edilməsini, tamlığın təmin edilməsini, müəssisənin bütün resurslarının müdafiə olunması üçün bir-birinə zidd olmayan qaydalar toplumunun tamlığını (təhlükəsizlik siyasəti obyektlərini) və müxtəlif istehsalçıların təqdim etdiyi təhlükəsizlik vasitələrinin müdafiə siyasətinin razılaşdırılma ilə yerinə yetirilməsini;
- Müəssisənin vahid kataloqdan istifadə etməklə bütün informasiya resurslarının müəyyən edilməsini, resursların qeyd olunmasını şəxsi vasitələrin köməyilə, həmçinin digər müəssisələrin kataloqlarından (o cümlədən LDAP protokolları da daxil olmaqla) birbaşa istifadə etməklə aktuallaşdırılmasını;
- Təhlükəsizlik siyasətini (Policy-based) əsas tutmaqla informasiyanın müdafiə vasitələrinin lokal idarə edilməsinin mərkəzləşdirilməsini;
- LAS autentifikasiya (istehlakçının seçiminə uyğun) mühitində əlavə lokal vasitələrdən istifadə imkanından bəhrələnib PKCS#11 ***token****indən* istifadə etməklə müəssisənin siyasətinə uyğun obyektlərin ciddi autentifikasiya edilməsini və PKI aşıq açarlarının infrastrukturunu;
- Müəssisənin kataloqda (və ya kataloqun bir hissəsində) qeyd olunmuş müəyyən resurslarına əlçatanlıq imkanının genişlədirilməsi, müəssisə resurslarına əlçatanlıq qaydalarının seçilməsinin idarə edilməsini, təhlükəsizlik siyasəti elementlərinin dolayı yolla müəyyən edilməsinə əlçatanlıq qaydalarının (credentials) təyin edilməsini;
- Auditin, təhlükəsiliyin monitoringinin, həyacan siqnalının təhtəlhesablığının təmin edilməsini;

- Ümumi idarəetmə sistemlərinin təhlükəsizlik sistemlərinin infrastrukturundan (PKI, LAS, IDS) istifadə etməklə inteqrasiyasını.

AÇIQLAMA: Elektron təhlükəsizlik sualları indiki zamanda dünyada əsas məsələlərdən biri kimi diqqət mərkəzindədir. İndiyə kimi onun həll edilməsi üçün çoxlu sayda üsullar təklif olunmuşdur. *Token* bunlardan biridir. Token dedikdə istifadəçinin informasiya təhlükəsizliyini təmin edən qurğu başa düşülür. Qurğu öz sahibinin identifikasiyasını həyata keçirməklə yanaşı ona müdafiə edilən, uzaqda yerləşdirilmiş əlçatanlıqlı müxtəlif informasiya növlərindən istifadə etməsinə imkan verir. Token parolun yerinə istifadə oluna bilər. Adətən onlar çoxda böyük ölçüyə malik deyillər, rahat çibdə gəzdirilə bilirlər. Müasir tokenlər kriptoqrafik açarların (məsələn, elektron imzaların, biometrik verilənlərin) saxlanılmasına imkan verir. Tokenlərin xarici görünüşü müxtəlif ola bilir: bəzilərində ancaq ekran, bəzilərində miniatür klaviatura, bəzilərində xırda düymələr və s. vardır. Tokenlər RFID funksiyası ilə, USB yuvaları və interfeys ilə təhciz olunurlar. Onları müxtəlif şirkətlər: məsələn, "E Token" və "Ru Token" və s. istehsal edir. Tokenlərin istifadəsində iki problem mövcuddur: istifadəçi onları ya itirir, ya da ki, oğurladır. Bu problemin həlli onların asılqanlarla istehsal olunmasında qismində olsa aradan qaldırılmışdır.

Müxtəlif görüntülü tokenlər

Hazırkı idarəetmə konsepsiyası çərçivəsində təhlükəsizlik siyasətinə söykənən idarəetmə - PBM (Policy based management) – idarəetmə qaydaları toplusunu realizasiya olunması ilə müəyyən olunur. Bu da öz növbəsində müəssisənin bütün biznes-obyektlərini əhatə etməklə bir-birinə zidd olmayan idarəetmə qaydalarının formalaşdırılmasına təminat verir.

PBM prinsiplərini rəhbər tutaraq müəssisənin təhlükəsizliyinin idarəedilməsi təhlükəsizliyin idarəediməsinin qlobal konsepsiyasina (GSM) əsaslanan idarəetmə sisteminə yönəldilmişdir və aşağıdakı tələbləri ödəməlidir:

- Müəssisənin təhlükəsizlik siyasəti özündə məntiqi və semantik əlaqəni əks etdirir, bu əlaqə verilənlərin vahid strukturu ilə təhlil və redaktə edilir;
- Müəssisənin təhlükəsizlik siyasəti müdafiənin bütün səviyyələri konteksində müəssisənin informasiya resurslarının təhlükəsizlik siyasətinə və şəbəkə təhlükəsizlik siyasətinə tam yanaşmada müəyyən olunur;

- İnzibatı resursların və müəssisənin təhlükəsizlik siyasətinin sadələşdirilməsi üçün siyasətin parametrlər sayı minimumlaşdırılmalıdır.

Siyasətin parametrlər sayının minimumlaşdırılması üçün aşağıdakı yanaşmalardan istifadə olunur:

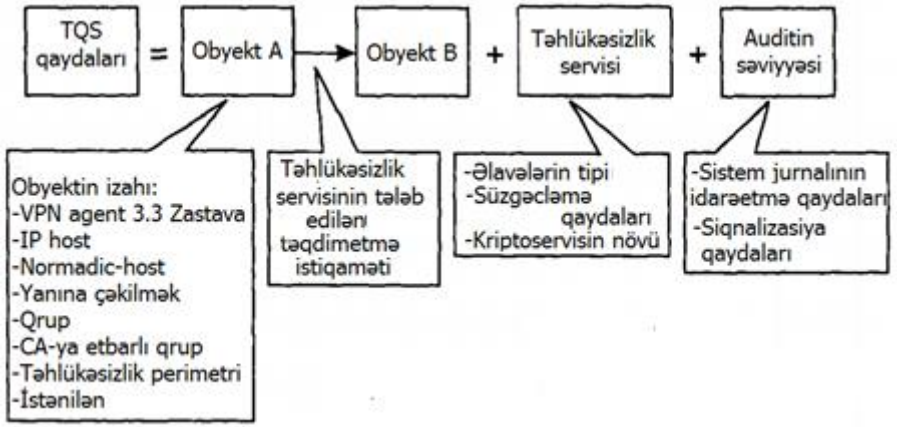
- Təhlükəsizlik obyektlərinin qrup şəkilində müəyyən edilməsi;
- Dolayı yolla müəyyən etmə (məsələn, bütün vəkalətvermə (mandat vermə - credential) atributların müəyyən edilməsi);
- Əlçatanlığın vəkalət verməklə idarə edilməsi.

Təhlükəsizliyin idarə ediməsinin qlobal konsepsiyasi təhlükəsizlik siyasətinin müxtəlif təhlil mexanizmini təmin edir.

TƏHLÜKƏSİZLİYİN QLOBAL VƏ LOKAL SİYASƏTİ

Korporativ şəbəkə təhlükəsizliyinin qlobal siyasəti sonlu sayda təhlükəsizlik qaydaları təqdim edir (security rules) (şəkil 18.). Qaydalar korporativ şəbəkə obyektlərinin informasiya təhlükəsizliyi konteksində qarşılıqlı əlaqələri əks etdirir. Bura daxildir:

- Təhlükəsizlik servisinin birləşməsi üçün lazım olanlar (məsələn, təhlil etmə qaydaları, trafikin müdafiəsi və süzgəclənməsi);
- Təhlükəsizlik servisi istiqamətinin təqdim olunması;
- Obyektlərin aitentifikasiya qaydaları;
- Açarların dəyişmə qaydaları;
- Sistem jurnalına təhlükəsizlik hadisələrinin nəticələrinin yazılma qaydaları;
- Baş vermiş təhlükə bildirən hadisələrin siqnalızasiya qaydaları və s.



Şəkil 18. Qlobal təhlükəsizlik siyasəti qaydalarının strukturu

Qeyd etmək lazımdır ki, təhlükəsizliyin qlobal siyasəti obyektləri ayrıca işçi stansiyalar və altsistemlər ola bilər, çünki özünə şirkətin bütün bölmələrinin strukturunu birləşdirən obyektlər qrupu (məsələn, marketinq şöbəsi və ya maliyyə departamenti) və ya ayrıca şirkətlər (məsələn, holdinqə daxil olanlar) bura daxildirlər. Ayrıca obyekt üçün təhlükəsizlik siyasəti avtomatik olaraq bütün obyektlər üçün təkrarlanır.

Paylanmış korporativ sistemlər üçün biznes-obyektlərin müdafiə məsələlərini qaydalar terminləri ilə formalaşdırmaq olar, çünki şəbəkə əlaqələrini Subj subyekti ilə Obj obyekti arasında informasiya ötürülməsi kimi təsvir etmək mümkündür. Bu əlaqələr SecSrv müdafiə servisinin və P parametrinin köməyilə sazlanır. Nəticədə müəssisənin təhlükəsizlik qlobal siyasəti qaydalar toplusu kimi təqdim olunur:

(Subj, Obj, SecSrv (P)).

Nəzərə almaq lazımdır ki, Obj obyekti üçün qaydalar olmadığı halda, bu o deməkdir ki, cari Obj üçün istənilən əlçatanlığa qadağa qoyulmuşdur.

Sadəlik üçün müəssisənin təhlükəsizlik məqsədini müəyyən edən zaman iki növ obyekt – Subj və Obj - nəzərdən keçirilir. İstifadəçi (U) və resurs (R) kimi qeyd olunur.

Resurs R ola bilsin ki, məlumatlı (IR) və ya şəbəkəli (NR) olsun.

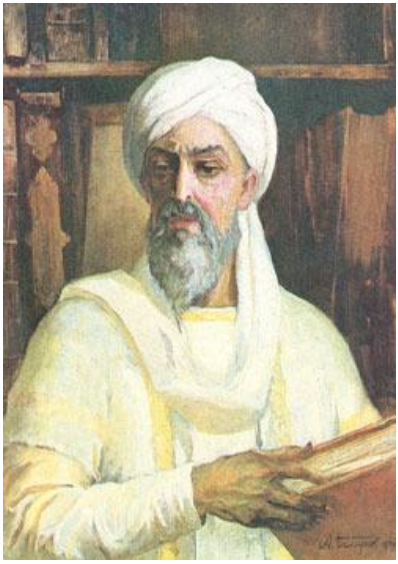
İstifadəşi və resurs aqressiyanın istənilən formasında çıxış edə bilər və sistemdə bunlar – qruplar, domenlər, rollar, departamentlər, kataloqların bölmələri – tərəfindən dəstəklənir.

Korporativ sistemin istənilən müdafiə olunan obyektə görə əlçatanlığı üçün *susmaya görə siyasət* özündə qadağa qoyulmuş qaydanı (qanunı) birləşdirir: *aşıq şəkildə icazə verilməyən nə varsa – qadağandır*. Belə qayda müəssisənin şəbəkəsində istifadə olunan informasiyanın tam şəkildə müdafiəsini və təhlükəsizlikdə yaranmış "deşik"lərdəki ***aprior*** çatışmazlığı da təmin edir.

AÇIQLAMA: Qədim Yunan flosofu Platonun "Xatırlama haqqında təlim" əsərində *aprior* haqqında məlumatlar verilir. Aprior insana miras qalmış və ona məxsus olan bilikdir. "Aprior" termininin yaranması Aristotelin fəlsəfəsi ilə əlaqəlidir. Aristotel sonuncudan alınan təsdiq ilə ondan əvvəlkindən alınan təsdiq arasında fərqin olduğunu sübut etmişdir. Sonrakı illərdə bu fərqi Şərqin görkəmıli alimlərindən olan, orta əsr ərəb flisofları İbn Ruşt və İbn Sina da araşdırmışdır.

Latin dilində termindən orta əsr sxolastikasında (sxolastika - orta əsrin dini ehkamlara əsaslanan son dərəcə mücərrəd idealist fəlsəfəsi, həyat ilə heç bir əlaqəsi olmayan,

təcrübədə yoxlanıla bilməyən, mücərrəd mühakimələrə əsaslanan görüş) istəfadə olunmuşdur. Aristotelin baxışlarına əsaslanan Avropa sxolastikləri aprioru cisimlərin dərk edilməsi adlandırmışlar.



Abu Əli Hüseyn ibn Abdulla ibn əl-Həsən ibn Əli ibn Sina

Abdul-Valid Məhəmməd ibn Əhməd əl-Kurtubi (ibn Ruşt kimi məşhurdur)

Aprior (latınca a priori – hərfi mənada "öndə gedəndən" anlamını verir) – təcrübəyə qədər və ondan asılı olmayan bilikdir (aprior bilik, biliyin aprioru). Fəlsəfi termin Kantın dərketmə və məntiq ilə bağlı əsərlərində özünə layiqli yer tutmuşdur. Terminin uzun keçid yolu olmuşdur və öz dövrünə uyğun olaraq müxtəlif mənalar daşımışdır.

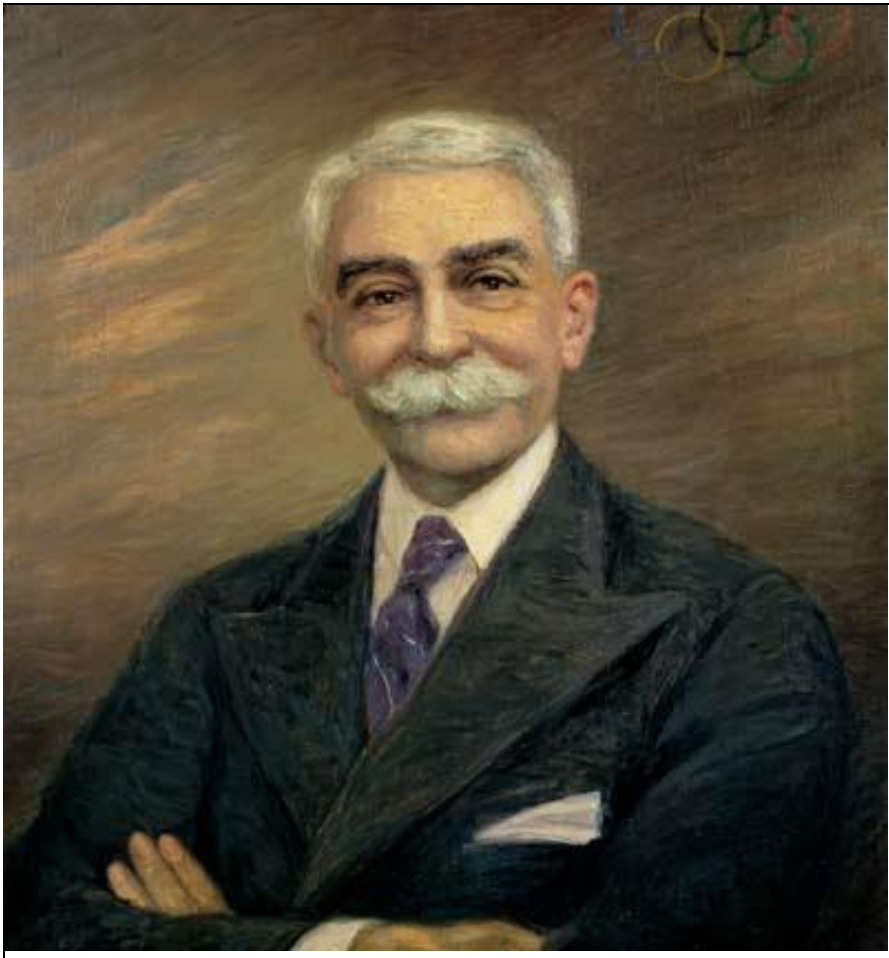
Şəbəkədə qurğuların qarşılıqlı əlaqəsini təmin etməkdən ötrü onlar üçün *start konfiqurasiyası* (xarici görünüşü) "yaradırlar" və ümumi halda rabitə kanalından istifadə etməməklə "çatdırılar". Start konfiqurasiyası qurğuların mərkəzi idarəedilməsini sazlamaq üçün lazım olan qaydalardır - *qurğuların start təhlükəsizlik siyasətidir*.

Qlobal təhlükəsizlik siyasəti şəbəkədə qarşılıqlı əlaqə kimi, həm də ki, sistemin özünü idarəetməsi və nəzarət funksiyası kimi yayıla bilər.

Qlobal təhlükəsizlik siyasəti şəbəkə miqyasında təhlükəsizlik siyasətinin tam şəkildə *məntiqi* və ***semantik*** izahıdır. Bununda əsasında ayrı-ayrı qurğuların təhlükəsizlik siyasəti qurula bilər.

AÇIQLAMA: ***Semantika*** yunanca *qeyd etmə*, *göstərmə*, *işarə etmə* anlamını verir və məna baxımından danışıq dilinin ölçülməsinin qiymətini öyrənir. Bu məqsədlə ləvazımat kimi semantik təhlildən istifadə edilir. XIX əsrin sonu, XX əsrin əvəllərində semantikanı bir çox hallarda semasiologiya (yunanca *işarə*, *göstəriş*) adlandırırdılar. Semantika ilə məşğul olan alimləri də indiki zamanda semasioloqlar adlandırırlar. Əksər sinif dil vahidlərinin qiymətlərini (məsələn, "hərəkət feillərinin semantikası") semantika ilə işarələyirlər.

Semantik problemlər uzaq keçmişdə fəlsəfi mənada araşdırılırdı. Termin fransız dilşunası (linqvisti) Mişel Breal (1832-1915) tərəfindən elmə daxil edilmişdir. 1910-1920-ci illərdə semantika məsələlərinin öyrənilməsi bir çox mütəxəssisləri özünə cəlb etmişdir.



Mişel Breal (fransizca Michel Bréal) fransiz linqvisti və tarixçisi, ictimai xadim, əlyazmalar Akademiyasının üzvü.

Lokal təhlükəsizlik siyasəti. İnformasiya təhlükəsizlik servisini realizə edən istənilən müdafiə vasitələri üçün lokal təhlükəsizlik siyasəti tərəfindən müəyyən işlər yerinə

yetirilməlidir. Bura autentifikasiya qaydalarını korrekt realizə olunması üçün sazlamaların dəqiq izahı, əlçatanlığın idarə edilməsi, trafiklərin müdafiəsi və s. daxildir.

Lokal təhlükəsizlik siyasəti informasiyanın müdafiə vasitələrini tələb edən, informasiya xidmətlərinin təmin olunması üçün istifadə edilən, cari qurğunun birləşdirilməsinə icazə verən qaydaların tam toplusundan ibarətdir.

Şəbəkədə qlobal təhlükəsizlik siyasəti ilə realizə olunan qaydalar (və ya qanunlar) ilə lokal təhlükəsizlik siyasəti tərəfindən konkret qurğulara realizə olunan qaydalar arsında fərqlər vardır. Bu əsasən onunla bağlıdır ki, qlobal təhlükəsizlik siyasəti şəbəkə hüdudlarında olan obyektlər və subyektlər arasında ixtiyarı şəkildə paylansada, lokal təhlükəsizlik siyasəti (lokal təhlükəsizlik siyasəti obyektləri və subyektləri daxil olmaqla) ancaq bir şəbəkə qurğusunun mühiti hüdudunda mümkündür.

TƏHLÜKƏSİZLİK VASİTƏLƏRİLƏ İDARƏETMƏ SİSTEMLƏRİNİN İŞLƏMƏSİ

TrustWorks təhlükəsizlik vasitələri idarəetmə sistemlərinin struktur elementlərinə təhlükəsizlik agenti (Trusted Agent), idarəetmə mərkəzi (Trusted GSM Server) və idarəetmə konsulu (Trusted GSM Console) daxildir.

Təhlükəsizlik vasitələrinin əsas təyinatı. Bura aşağıdakılar aiddir:

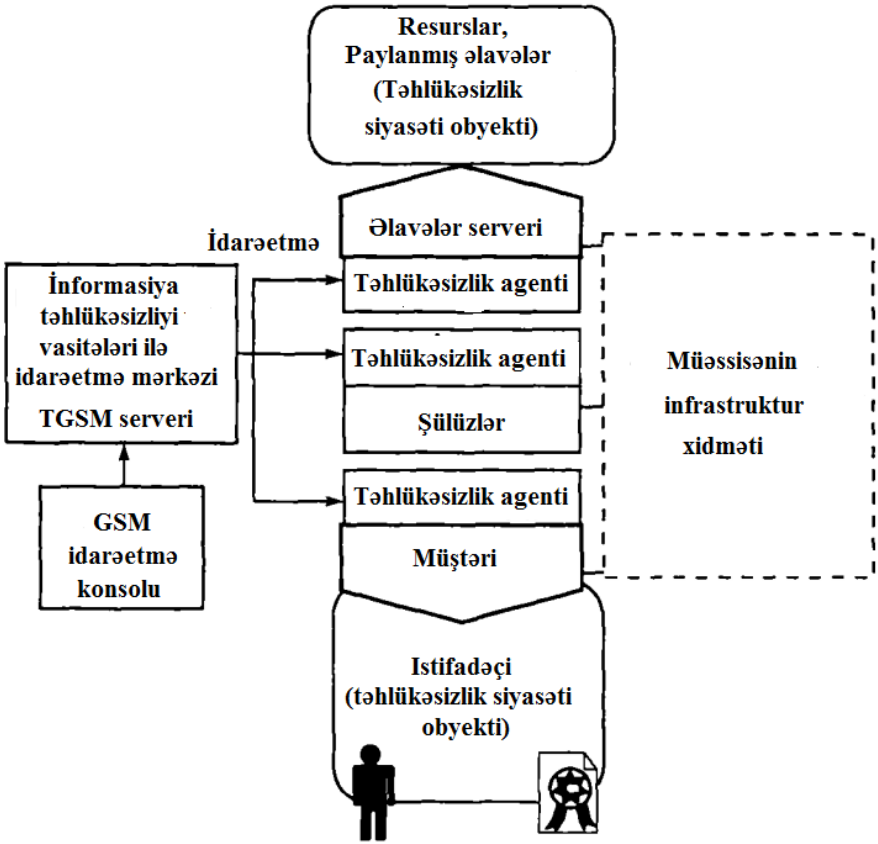
1.Təhlükəsizlik agenti (Trusted Agent) istifadəçinin fərdi kompüterinə quraşdırılır, fərdi müdafiə üçün nəzərdə tutulmuşdur, kliyent-server kimi iştirak edir.

2.Əlavələr serverinə quraşdırılmış təhlükəsizlik agenti paylanmış əlavələrin server təşkiledicilərinin müdafiəsinin təmin olunması üçün müəyyən olunmuşdur.

3.Şlüz kompüterinə quraşdırılmış təhlükəsizlik agenti müəssisələr daxilində və ya müəssisələr arasında şəbəkə seqmentinin aydınlaşdırılmasını təmin edir.

İdarəetmə mərkəzi (Trusted GSM Server) şəbəkə miqyasında qlobal təhlükəsizlik siyasətinin saxlanılmasını (saxlanc qurğulari nəzərdə tutulur) və izahını təmin edir. Bununla yanaşı idarəetmə mərkəzi qlobal siyasətin translyasiyasını, müdafiə qurğularının lokal təhlükəsizlik siyasətini, müdafiə qurğularının yüklənməsini və sistemin bütün agentlərinin vəziyyətinə nəzarət edir. Müəssisədə GSM sistemində təhlükəsizlik siyasətinin idarəedilməsi sxeminin təşkil olunması üçün bir qədər (təxminən 65 535 ədəd) GSM serveri tələb olunur.

İdarəetmə konsulu (Trusted GSM Console) sistem administratoru üçün iş yerinin təşkil edilməsinə xidmət edir. Hər bir GSM serverində bir neçə konsul quraşdırıla bilər, bunlarında hər biri sistemin GSM administratoruna uyğun sazlanırlar.



Şəkil 19. İnformasiya təhlükəsizliyi vasitələrinin idarəetmə sisteminin ümumi struktur sxemi

Lokal təhlükəsizlik agenti (*Trusted Agent*) sonuncu qurğuda (müştəridə, serverdə, şlüzdə) yerləşən və aşağıdakı fuksiyaları yerinə yetirən proqramdan ibarətdir:

- Obyektlərin təhlükəsizlik siyasəti autentifikasiyanı, müxtəlif autentifikasiya serverlərinin inteqrasiyasını;

- Sistemdən istifadə edən istifadəçinin (istifadəçinin verilənlərinə uyğun) müəyyən edilməsini;
- Əlçatanlığa nəzarətin və təhlükəsizlik vasitələrinin idarə edilməsinin mərkəzləşdirilməsinin təmin edilməsini;
- Resursların idarə edilməsini, tətbiqi səviyyədə resurslara əlçatanlığın idarə edilməsinin dəstəklənməsini;
- Trafikin süzgəclənməsini;
- Monitoringin, həyacanlı siqnalların, hadisələrin protokollaşdırılmasını.

Bu funksiyalarla yanaşı Lokal təhlükəsizlik agentinin (Trusted Agent) əlavə funksiyaları da yerinə yetirməsi vacibdir:

- Kriptoservisin çatdırılması (multiple concurrent pluggable modules);
- Single-Sing-On perimetrinin idarə edilməsi (istifadəçinin autentifikasiyasının altməsələsi kimi nəzərdə tutulur);
- Müdafiə olunan əlavələrin servisi;
- Trafikin sıxılması (IPcomp, pluggable module);
- Şəbəkə resurslarının ehtiyatda saxlanılmasının idarə edilməsi (QoS);
- Şəbəkədə antivirus müdafiə agentinin lokal funksiyası.

Lokal agentin mərkəzi elementi lokal təhlükəsizlik siyasəti prosessorudur (LSP prosessor). Prosessor lokal təhlükəsizlik siyasətini interpretasiya etməklə yanaşı ayrı-ayrı təşkiledicilər arasında paylanmanı idarə edir.

Resursların müdafiəsi. Bura aşağıdakılar daxildir:

1. *Əlçatanlığın autentifikasiyası və avtorizasiyası*. Yerinə yetirdiyi funksiyalara görə müxtəlif autentifikasiyalardan istifadə olunur, bunların da hər biri özündə autentifikasiya növlərini və obyektlərin identifikasiya üsullarını (mexanizmini) birləşdirir.

Autentifikasiya növlərinin seçilməsi üçün müxtəlif imkanlardan: məsələn, GSM mühitinə daxil olan istifadəçi autentifikasiyasından və ya lokal əməliyyat sistemindən, şəbəkəyə (şəbəkə seqmentinə) daxil ola bilən istifadəçinin autentifikasiyasından, obyektlərin qarşılıqlı şəbəkə autentifikasiyasından (əlavə-əlavə) istifadə olunur. İdentifikasiya üsullarını seçmək üçün növbəti variantlar: token (smart-kart), parol, "xarici" autentifikasiya.

2.*Şəbəkənin qarşılıqlı əlaqəsində əlçatanlığa nəzarət*. Lokal əməliyyat sistemində müdafiə olunan şəbəkənin inisializasiyasında və ya lokal təhlükəsizlik agentinin (Trusted Agent) birləşmə uclarında (və/və ya aralıq şlüzlərdə) xarici birləşmənin qurulmasına sorğunun alınması üçün təhlükəsizliyin lokal siyasətinə müraciət olunmalıdır, edilən müraciət bu birləşmənin yerinə yetirilməsinə icazənin verilməsini yoxlayır. Əgər birləşmə dağıdılmışsa, onda verilən birləşməni müdafiə servisi təmin olunur.

3.Tətbiqi obyektlər səviyyəsində əlçatanlığa nəzarət. GSM –də müdafiə olunmayan paylanmış əlavələr, daxili obyektlərin əlçatanlıq səviyyəsində verilmiş əlavələrdə məhdudlaşma qaydaları servisi tərəfindən təmin edilir. Obyektlər səviyyəsində nəzarət *proxy* mexanizmindən istifadə edilməsi hesabına həyata keçirilir. Proxy hər bir tətbiqi protokol üçün hazırlanır. HTTP protokolu əvvəlcədən müəyyən edilmiş hesab olunur.

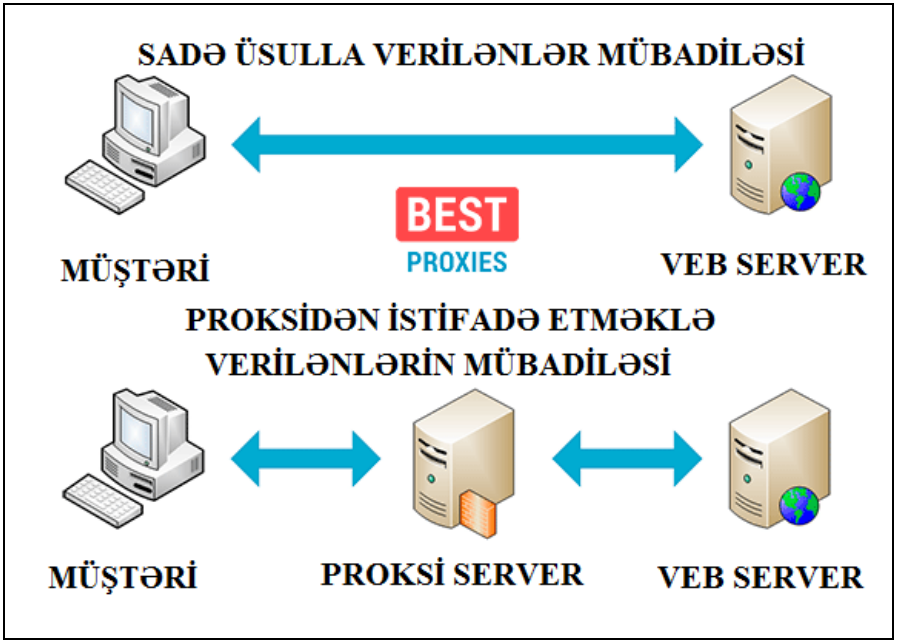
Proxy (proksi) agent əlavələrə və sistemdəki müştəri yerlərinə nəzarəti yerinə yetirən təhlükəsizlik şlüzünə qurula bilər.

AÇIQLAMA: ***SNMP*** modelinin əsasında ***MIB*** verilənlər bazası ilə agentin eyni zamanda mövcud olma prinsipi dayanır. Prinsip şəbəkənin uzaqlaşdırılmış nöqtəsi tərəfindən idarə edilməklə yanaşı nəzarətdə də saxlanılır. Proksi-agent dolayı yol ilə qurğuya əlçatanlığa icazə verməklə bu modeli müəyyən qədər inkişaf etdirir. İdarəetmə stansiyası proksi ilə onda əlaqə yaradır ki, əlçatanlıq lazımdır və ya informasiyanın dəyişməsinə tələbat vardır. Proksi-agent qurğu ilə informasiya mübadiləsini ayrıca birləşmənin köməyilə həyata keçirir.

Proksi (ingiliscə *proxy – kiminsə adından fəaliyyət göstərən*) aralıq tranzit Veb-serverdir, brauzer ilə sonuncu Veb-server arasında ortaq rolunu oynayır. Proksi-server xüsusi İnternet-serverdir, lokal İnternet şəbəkədə daxil olan və çıxan trafikləri idarə edir. Proksi-server faylların və ya məlumatların şəbəkədə təhlükəsiz ötürülməsini müəyyən edir.

SNMP (ingiliscə Simple Network Management Protokol - şəbəkə idarəetmənin sadə protokolu) IP şəbəkələrində TCP/UDP arxitekturasına əsaslanaraq qurğuların idarə edilməsi üçün standart İnternet-protokoludur.

MIB (Management Information Base – idarəedilən informasiya bazası) – virtual verilənlər bazasıdır, rabitə xətlərində obyektlərin idarə olunması üçün istifadə edilir. Bir çox hallarda bu anlamı Simple Network Management Protokol anlamı ilə əlaqələndirirlər.



Müdafiə vasitələri ilə idarəetmə. TrustWorks həllinin əsas elementi mərkəzləşdirmədir. Mərkəzləşdirmə müəssisə miqyasında informasiya təhlükəsizliyi və şəbəkə vasitələrinin idarəetmə sistemi (policy based) siyasətinə əsaslanır. Sistem istehlakçının aşağıdakı keyfiyyət xarakteristikalarını təmin edir:

- İdarəetmə sisteminin yüksək səviyyədə müdafiəsinin təşkili (müəssisənin daxili şəbəkəsinin idarə edilməsinin müdafiə perimetrinin seçilmə yolu ilə);
- İnformasiya təhlükəsizliyi idarəetmə sisteminin genişləndirilməsi;
- İdarəetmə sisteminin və onun açar elementlərinin yüksək səviyyədə etibarlı işləməsi;
- Ümumi korporativ şəbəkə və informasiya idarəetmə sistemlərinin inteqrasiyası;

- Müəssisə miqyasında (enterprise level policy based management) təhlükəsizlik siyasətinin diaqnostikası və monitorinqi, formalaşması, sadəliyi, erqonomikliyi, infrastrukturu və s. keyfiyyət xarakteristikaları.

İdarəetmə xüsusi proqram təminatı administratoru – idarəetmə konsulu (Trusted GSM Console) tətəfindən yerinə yetirilir. Proqram təminatı sisteminə quraşdırılmış Trusted GSM Console sayı və funksiyası müəssisənin təşkilatı strukturundan asılı olaraq baş administrator tərəfindən müəyyən edilir. Trusted GSM Console –də hər bir işçi yerinin müəyyən edilməsi üçün sistemin idarəetmə funksiyasından istifadə olunur.

GSM idarəetmə funksiyası. Obyektlərin idarə edilməsi növündən asılı olaraq GSM funksiyasını üç kateqoriyaya bölürlər.

1.İnformasiya kataloqları ilə idarəetmə.

2.Əlçatanlıq hüquqi və istifadəçinin idarə edilməsilə.

3.Qlobal təhlükəsizlik siyasəti qaydalarına əsaslanmaqla idarə olunma.

Autentifikasiya sisteminin hər bir administratoru nəzərə alınmış qaydalara əsasən Trusted GSM Console sistemindən istifadə etməklə işləyir. Administratorların istənilən fəaliyyəti nəzarət altındadır (və ya cüt-cüt nəzarətdədir).

TƏHLÜKƏSİZLİYİN AUDİTİ VƏ MONİTORİNGİ

Təşkilatlarda istifadə olunan kompüterin sayı bir neçə onlarla (hətta yüzlərlə) kompüteri keçmişdir. Bütün kompüterlər müxtəlif proqram təminatlarının rəhbərliyi altında işləyirlər. Burada əsas məsələ kompüterlərin müxtəlif müdafiə sistemləri ilə müdafiə olunmasıdır. Şəbəkə infrastrukturunun mürəkkəbliyi, verilənlərin və əlavələrin müxtəlifliyi ona səbəb

olur ki, adminidtratorun nəzarət dairəsindən kanarda işləyən informasiya sistemlərinin təhlükəsizliyi zərbə altında qala bilər. Odur ki, informasiya sistemlərinin təhlükəsizliyinin mütəmadi olaraq yoxlanması üçün audit və monitoringə müraciət tələb olunur.

İnformasiya sisteminin təhlükəsizliyi auditi.

Təhlükəsizliyin auditi anlayışı. Audit müəssisənin ayrı-ayrı sahələrinin işləməsinin müstəqil ***ekspertizini*** özündə əks etdirir. Auditin təkbinə daxil olanlardan biri müəssisənin informasiya sisteminin təhlükəsizlik auditidir.

İndiki zamanda informasiya sisteminin təhlükəsizlik auditi sürətlə artmışdır. Bu təşkilatın informasiyadan və informasiya sistemindən asılılığının artması ilə əlaqədardır. İnformasiya sistemi ilə asılılıq bir tərəfdən informsiya sistemlərinin elementlərinin mürəkkəbliyinin yüksəlməsi ilə, digər tərəfdən isə verilənlərin ötürülməsinin və saxlanmasının yeni texnologiyalarının tətbiqi və proqram təminatı həcminin artması ilə bağlıdır. Müəssisələrdə məlumatların və tranzaksiyaların açıq qlobal şəbəkələr vasitəsilə ötürülməsindən aktiv istifadə edilməsi nəticəsində informasiya sistemlərinə olunan hədələrin (hücumların) spektri də genişlənmişdir.

AÇIQLAMA: *Ekspert* (latınca *expertus* sözündən törəmədir, bacarıqlı anlamını verir) dedikdə müəyyən bir problemin həll edilməsi üçün dəvət edilən və ya pulla tutulan mütəxəssis nəzərdə tutulur. Ekspert araşdırılan və ya həll edilən məsələlərin bu sahəyə aid olmayan şəxslər tərəfindən verdikləri rəyə daha düzgün və ixtisaslı fikir söyləmək üçün müəyyən məbləğ pul ilə dəvət olunur. Ekspertlər

mütəxəssislərin, ustaların, hətta yaradıcıların işlərinə müdaxilə edir, bu barədə öz fikirlərini söyləyirlər. Ekspertləri elmi baxımdan texniki və təsərrüfat sahələrini araşdıran mütəxəssislərə ayırırlar.

İnformasiya sistemlərinin təhlükəsizlik auditi təşkilat rəhbərlərinə və əməkdaşlarına aşağıdakı suallara cavab almağa imkan verir:

- Biznesin inkişafı baxımından mövcud informasiya sistemlərindən optimal necə istifadə etməli;
- Təhlükəsizlik sualları və əlçatanlığa nəzarət necə həll edilir;
- Vahid idarəetmə sistemini və monitoringi necə qurmalı;
- Avadanlıqların və proqram təminatının modelləşməsini nə vaxt və necə həyata keçirməli;
- Müəssisənin informasiya sistemlərində konfidensial informasiyanı yerləşdirən zaman riski necə minimuma endirmək, həmçinin yaranacaq problemin həll edilməsi üçün hansı yolların axtarımasını yerinə yetirmək.

Öndə verilmiş suallara (həmçinin ona yaxın olanlara) birmənalı və ətraflı cavab o dəqiqə vermək mümkün deyil. Deməli, ətraflı və əsaslandırılmış cavablar almaq üçün yaranmış problemlər arasında qarşılıqlı əlaqələr tutarlı səviyyədə araşdırılmalıdır. Auditin aparılması informasiya sistemlərinin təhlükəsizliyi ilə bağlı sualları qiymətləndirməyə, risklərin təhlilinə şərait yaradır. Bunlardan istifadə etməklə müəssisənin biznes-proseslərini idarə etməyə və yaranacaq problemləri öncədən müəyyənləşdirməyə, informasiya resurslarının təhlükəsizliyinin təmin edilməsi ilə bağlı suallara cavabların tapılmasına və onların korrekt və əsaslı həll edilməsinə imkan yaranır.

İnformasiya sistemlərinin təhlükəsizlik auditinin aparılmasında məqsəd aşağıdakılardan ibarətdir:

- İnformasiya sistemlərinin müdafiə olunması səviyyəsinin qiymətləndirilməsi;
- İnformasiya sistemlərinin müdafiə sisteminin məhdud yerlərinin lokallaşdırılması;
- İnformasiya sistemləri resurslarına münasibətdə təhlükəsizlik hücumlarının yaranma imkanları ilə bağlı olan risklərin təhlili;
- İnformasiya sistemlərinin mövcud təhlükəsizlik mexanizminin effektivliyini artırmaq üçün yeni tövsiyələrin işlənməsi və həyata keçirilməsi;
- İnformasiya təhlükəsizliyi sahəsində mövcud olan standartlardan istifadə edilməsi.

Bununla yanaşı auditə aid olan əlavə sualların cavabları da müəssisə daxilində araşdırılmalı və lazımı tədbirlər yerinə yetirilməlidir.

İnformasiya sistemlərində təhlükəsizlik auditinin tətbiq edilməsi. Təhlükəsizlik auditinin tətbiqi ardıcıl mərhələlərlə yerinə yetirilir:

- Audit prosedurlarının yaradılması (***inisializasiya*** olunması);
- Auditlə bağlı informasiyanın toplanması;
- Auditlə bağlı verilənlərin analızı;
- Tövsiyyələrin işlənib hazırlanması;
- Audit hesabatlarının aparılması.

AÇIQLAMA*: İnisializasiya* (ingiliscə initialization – inisializasiya olunma, yaradılma, aktivləşdirmə, işə hazırlıq, parametrlərin təyin olunması anlamlarını verir). İnisializasiya dedikdə proqramların və qurğuların istıfadə edilməsi üçün

hazırlıq vəziyyətinə gətirilməsi başa düşülür. Termin proqram və aparat vasitələri üçün istifadə edilir. İnisializasiya fəaliyyəti obyektin (proqramlar, qurğular nəzərdə tutulur) parametrlərinin müəyyən edilməsinə və onlarla işin təşkili qaydalarına yönəldilir.

Audit hesabatı auditin aparılmasının əsas nəticəsidir. Hesabat auditin aparılmasında məqsədin izahından, informasiya sistemlərinin xarakteristikalarının öyrənilməsindən, cari auditin verilənlərinin təhlilindən, baş verə biləcək çatışmazlıqların aradan götürülməsindən və müdafiə sisteminin təkmilləşdirilməsindən ibarətdir.

Sisteminin təhlükəsizliyi monitoringi.

İnformasiya sistemlərinin təhlükəsizlik monitoringinin funksiyası edilmiş hücumların təhlilini və onların avadanlıqlardan istifadə etməklə aşkar olunmasını yerinə yetirir. Müdafiəni yerinə yetirən avadanlıqlar işçi stansiyalarda və serverlərdə əməliyyat sistemi elementlərinin və verilənlər bazasının müdafiə olunmasını icra edirlər. Avadanlıqlar şəbəkənin topologiyasını araşdırır, şəbəkədə düzgün yerinə yetirilməyən birləşmələri və həmin birləşmələrin müdafiəsini təmin edir və nəhayət şəbəkələrarası ekranların sazlanmasını təhlil edirlər.

Təhlükəsizliyin idarə eilməsi sisteminin funksiyasına şəbəkədə baş vermiş nasazlıqların administratorun təkliflərinə əsaslanmaqla aradan götürülməsi daxildir.

Şəbəkədə təhlikəsizliyin idarə edilməsinin adaptiv modelindən istifadə olunması sistemdə bütün hücumların nəzarət altında saxlanılmasına, onlara vaxtında reaksiya

verilməsinə, hücumlar arasında yaranmış əlaqələrin kanarlaşdırılmasına, onların yaranması ilə bağlı sualların təhlil olunmasına imkan verir.

Ə D Ə B İ Y Y A T

Əilizadə M.N., Seyidzadə E.V., Salmanova M.Ə. İnformatika (Mövzular, suallar və testlər), Dərs vəsaiti, Bakı 2012,

Abbasov Ə.M., Əlizadə M.N., Seyidzadə E.V.,Musayev İ.K. İnformatika və kompüterləşmənin əsasları, Dərslik, Yeni işlənmiş nəşri, RS "Poliqal" nəşriyyatı, 2012, 932 səh.

Rüstəmov Ə.M. İnformatika, Bakı 2012, səh. 522.

Rüstəmov Ə.M. İnformatika – izahlı terminlər lüğəti (Azərbaycanca, rusca və ingiliscə izahlı lüğət), Bakı 2011, 568 səh.

Kərimov S.Q., Həbibullayev S.B., İbrahimzadə T.İ. İnformatika, Dərslik, Bakı 2011, 534 səh.

Qurbanov İ.Ə., Qurbanov A.İ., Asadullayev R.A. İnformatika, Bakı 2012, 420 səh.

Fərziyev T. İnformatika (maqistraturaya hazırlaşanlar üçün vəsait), Bakı 2012, 322 səh.

Абдикеев Н.М. Интеллектуальные информационные системы. М.: КОС- ИНФ, Рос. экон. акад. - 2003.-188 с.

Абрамов А. В., Панасенко С. П., Петренко С. А. VPN-решения для российских компаний // Конфидент. 2001. № 1.

Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. 39с.

Агеев А.С. Компьютерные вирусы и безопасность информации// Зарубежная радиоэлектроника.1989. N 12.

Астахов А. М. Аудит безопасности информационных

систем. Конфидент. 2003. № 2.

Ахметов К. Безопасность в Windows XP // Безопасность. 2001. № 12.

Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. — М.: Гелиос АРВ, 2002. — 240 с.

Базовый стандарт организации беспроводных локальных сетей IEEE 802.11. 1999.

Банковское дело : Справ. пособие/ М.Ю. Бабичев, Ю.А. Бабичева, О.В.Трохова, и др.; Под ред. Ю.А. Бабичевой. М.: Экономика, 1993. 397 с.

Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с.

Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М.:Юридическая литература, 1991. 160 с.

Безопасность информационных технологий. Выпуск 1.М.:Госкомитет РФ по высшему образованию, МИФИ. 1994. 100 с.

Беляев А. В. Методы и средства защиты информации, 2000.

Бияшев О.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации//Зарубежная радиоэлектроника. 1989. N 12.

Бытко Ю.И., Бытко С.Ю. Уголовное право России. Части Общая и Особенная. Учебник. — Саратов: Изд-во «Научная книга», 2005.

Борисова Е. А. Проверка судебных актов по гражданским делам. М.: Городец, 2005.

Буш Г. Я. Стратегии эврилогии. — Рига: Общество

«Знание» ЛатвССР, 1986. — 64 с.

Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. / Под ред. Б.П. Смагоринского. М.: 1996.

Вильям Столлингс. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001.

Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России,- М.: ГТК РФ, 1992. 29с.

Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. - Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.

Гайкович В., Першин А. Безопасность электронных банковских систем. М.: Единая Европа, 1994.

Гайкович В.Ю., Першин А.Ю. Безопасность электронных банковских систем. М.:Единая Европа, 1994. 363 с.

Галатенко В. А. Информационная безопасность — грани практического подхода. Конференция «Корпоративные Информа ционные Системы». М., 1999.

Галатенко В. А. Информационная безопасность / / Открытые системы. 1996. № 1.

Галатенко В. А. Информационная безопасность в Intranet // LAN. 1996. № 7.

Галатенко В. А., И. Трифоленков. Введение в безопасность Интернет // LAN. 1996. № 6.

Галицкий А. В., РябкоС.Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез

решений М.: ДМК Пресс, 2004.

Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М: Энергоатомиздат, 1994. 400 с. и 176 с.

Герасименко В.А. Проблемы защиты данных в системах их обработки// Зарубежная радиоэлектроника. 1989. N 12.

Герасименко В.А., Размахнин М.К., Родионов В.В. Технические средства защиты информации//Зарубежная радиоэлектроника. 1989. N 12.

Голубев В.В., Дубров П.А., Павлов Г.А. Компьютерные преступления и защита информации в вычислительных системах //Вычислительная техника и ее применение. М.:Знание, 1990, N 9, С.3-26.

Грегори Р. Эндрюс. Основы многопоточного, параллельного и распределённого программирования. — Вильямс, 2003.

Грушо А.А.,Тимонина Е.Е. Теоретические основы защиты информа- ции. М.:Яхтсмен, 1996. - 192с.

Грязное Е. С., Панасенко С. П. Безопасность локальных сетей // Мир и безопасность. 2003. № 2.

Давыдовский А.И., Максимов В.А. Введение в защиту информации//Интеркомпьютер.1990. N 1.С.17-20.

Дал У., Дейкстра Э., Хоор К. Структурное программирование = Structured Programming. — 1-е изд. — М.: Мир, 1975. — 247 с.

Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. – М.: Изд.центр «Академия», 2005. – 144 с.

Дейкстра Э. Дисциплина программирования = A discipline of programming. -1-е изд.М.:Мир, 1978. — 275 с.

Дейтел Г. Введение в операционные системы: В 2-х т. Т.2. Пер. с англ. М.: Мир, 1987. 398 с.

Диффи У Первые десять лет криптографии с открытым ключом // ТИИЭР. Т. 76. 1988. № 5.

Дружинин Г.В.,Сергеева И.В. Качество информации.М.:Радио и связь, 1990. 172 с.

Дшхунян В. Л.у Шанъгин В. Ф. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. М.: АСТ: НТ Пресс, 2004.

Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 335 с.

Жумадилова М.Б. Теоретические основы криптографии. Актау: Актау - Принт, 2012.

Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. -264 с : ил.

Защита информации в персональных ЭВМ/Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. М.:Радио и связь, МП "Веста", 1992. 192 с.

Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.:Горячая линия - Телеком, 2000. - 452с.

Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2001.

Зима В. М., Молдовян А. А., Молдовян Н. А. Компьютерные сети и защита передаваемой информации. СПб.: Изд. СПбГУ, 1998.

Иванов П. IPSec: защита сетевого уровня / / Сети. 2000. № 2.

Карасик И. Программные и аппаратные средства защиты информации для персональных компьютеров //Компьютер-пресс.1992. N 3. С.37-46. 16. Касперский Е. "Дыры" в MS DOS и программы защиты информации// Компьютер-пресс. 1991. N 10. С.6-14.

Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 1998.

Кляйн Д. Как защититься от "взломщика". Обзор методов парольной защиты и набор рекомендаций по ее улучшению //Программирование, 1991, N 3, С.59-63.

Кондаков Н. И. Логический словарь-справочник. — 2-е изд. — М.: Наука, 1975. — 674 с.

Конхейм А. Г. Основы криптографии. М.: Радио и связь, 1987.

Концепция создания системы платежей крупных сумм. Рабочие ма- териалы // Департамент информатизации ЦБ РФ, 1994. 29. Г.Дж. Симмонс. Защита информации. ТИИЭР, т.76 N5, май 1988г.

Коротыгин С. Развитие технологии беспроводных сетей: стандарт IEEE 802.11.

Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.

Костров Д. Системы обнаружения атак // BYTE Россия. 2002. № 8.

Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. — М.: ИНФРА-М-НОРМА, 1997.

Кузнецов С. Защита файлов в операционной системе UNIX.

Латыпов Н.Н., Ёлкин С.В., Гаврилов

Д.А. Инженерная эвристика / под.ред. А.А. Вассермана. — М.: Астрель, 2012. — 320 с.

Латыпов Н.Н., Ёлкин С.В., Гаврилов Д.А. Самоучитель игры на извилинах / под.ред. А.А. Вассермана. — М.: АСТ, 2012. — 320 с.

Лукацкий А. Безопасность беспроводных сетей / / Технологии и средства связи. 2005. № 1.

Лукацкий А. Обнаружение атак. СПб.: БХВ-Петербург, 2003.

Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. М., 1998.

Максим М., Полино Д. Безопасность беспроводных сетей / Пер. с англ. А. В Семенова. М.: ДМК Пресс, 2004.

Мамаев М., Петренко С. Технологии защиты информации Интернета. Спец. справ. СПб.: Питер, 2002.

Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с.

Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.

Мельников В. В. Защита информации в компьютерных системах. М.:Финансы и статистика, 1997.

Моисеенков И.Э. Американская классификация и принципы оценивания безопасности компьютерных систем//Компьютер-пресс. 1992. N2, N 3. С.47-54.

Моисеенков И.Э. Основы безопасности компьютерных систем//Компьютерпресс.-1991. N10. С.19-24, N11. С.7-21, N12.

Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. СПб.: «Лань», 2000.

Монин С. Защита информации и беспроводные сети / / Ком пьютерПресс. 2005. № 4.

Мюллер С. Модернизация и ремонт ПК = Upgrading and Repairing PCs / Скотт Мюллер. — 17-е изд. — М.: Вильямс, 2007. — С. 653—700.

Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза. Часть 1 / Под ред. В.Н.Черкасова — Саратов: СЮИ МВД России, 2003.

Нечаев В. И. Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999.

Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004. — 432 с.

Олифер В. Г. Защита информации при работе в Интернет // Connect. 2002. № 11.

Олифер В. Г., Олифер Н. А. Новые технологии и оборудование IP-сетей. СПб.: БХВ-Петербург, 2000.

Олифер Н. А. Дифференцированная защита трафика средствами IPSec / / LAN. 2001. № 4.

Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004.

Основы криптозащиты АСУ. Под ред. Б. П. Козлова. М.: МО, 1996.

Панасенко С. П. Вновь об ЭЦП: стандарт X.509 / / Системы безопасности, связи и телекоммуникаций. 2003. № 3.

Панасенко С. П., Батура В. П. Основы криптографии для экономистов: учеб. пособие / под ред. Г. Гагариной. М.: Финансы и статистика, 2005.

Панасенко С. П., Петренко С. А. Криптографические методы защиты информации для российских корпоративных сис тем // Конфидент. 2001. № 5.

Петренко С. А. Построение эффективной системы антивирусной защиты // Конфидент. 2002. № 3.

Петренко С. А. Реорганизация корпоративных систем безопасности // Конфидент. 2002. № 2.

Петров А. А. Компьютерная безопасность: криптографические методы защиты. М.: ДМК Пресс, 2000.

Петров В.Н. Информационные системы. СПб: Питер, 2003. 687с.

Петрова С.С. Криминология: Учеб. Пособие. — М.: Издательство РИОР, 2005.

Пойа Д.Н. Как решать задачу. — М.: Учпедгиз, 1961. — 206 с.

Пойа Д.Н. Математика и правдоподобные рассуждения. — М.: ИЛ, 1957. — 535 с.

Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. — М.: ЮИ МВД РФ, 2003.

Программно-аппаратные средства обеспечения информаци онной безопасности. Защита программ и данных: учеб. пособие для вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. М.: Радио и связь, 1999.

Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю. Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.

Проскурин В. Г., Крутов С. В., Мацкевич И. В. Программно-аппаратные средства обеспечения

информационной безопасности. Защита в операционных системах: учеб. пособие для вузов. М.: Радио и связь, 2000.

Пушкин В.Н. Эвристика - наука о творческом мышлении. — М.: Политиздат, 1967. — 272 с.

Родин Г. Некоторые соображения о защите программ//Компьютер - пресс. 1991. N 10.- С.15-18.

Романец Ю. В., Тимофеев П. А., В. Ф. Шаньгин. Защита информации в компьютерных системах и сетях. 2-е изд. М.: Радио и связь, 2001.

Российское законодательство X-XX веков. В 9 т. Т. 2: Законодательство периода образования и укрепления Русского централизованного государства / Под общ. ред. О. И. Чистякова; Отв. ред. тома А. Д. Горский; Рец. В. И. Корецкий. - М.: Юридическая литература, 1985.

Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. — 2-е изд. — М.: Горячая линия — Телеком, 2013. — 229 с.

Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004.

Сарбуков А.у ГрушоА. Аутентификация в компьютерных системах // Системы безопасности. 2003. N° 5(53).

Семейство стандартов IEEE 802.11. http://www.wireless.ru/ wireless/wrl_base80211

Симонов С. В. Методология анализа рисков в информационных системах // Конфидент. 2001. № 1.

Скородумов Б. Безопасность союза интеллектуальных карточек и персональных компьютеров // Мир карточек. 2002. № 5—6.

Скородумов Б. И. Стандарты для безопасности электронной коммерции в сети Интернет, http://www.stcarb.comcor.ru

Скотт Мюллер. Глава 6. Оперативная память // Модернизация и ремонт ПК = Upgrading and Repairing PCs. — 17-е изд. — М.: Вильямс, 2007. — С. 499—572

Смирнова С.А. Судебная экспертиза на рубеже XXI века. Состояние, развитие, проблемы. 2-е издание, переработанное и дополненное. — СПб.: Питер, 2004 10.

Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002.

Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. БХВ- Петербург. 2002.-496 с.

Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России, М.:ГТК РФ, 1992. 25с.

Теоретические основы компьютерной безопасности: Учеб. пособие для 11 вузов / П.Н. Девянин, О.О.Михальский, Д.И.Правиков и др.- М.:Радио и Связь, 2000. - 192с.

Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. М.:Яхтсмен, 1996. - 302с

Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России, М.:ГТК РФ, 1992. 13с.

Трифаленков И., Зайцева Н. Функциональная безопасность корпоративных систем // Открытые

системы. 2002. № 7—8.

Трофимова М.С. История развития апелляции в гражданском процессе России: прошлое, настоящее, будущее. // История государства и права. 2010. N 5. С. 2-5. Нечаев В. И. Элементы криптографии (Основы теории защиты информации). — М.: Высшая школа, 1999. 109 с.

Уголовное право. Особенная часть: Учебник / Под ред. проф Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Изд-во Эксмо, 2004.

Удалов В.И., Спринцис Я.П. Безопасность в среде взаимодействия открытых систем//Автоматика и вычислительная техника.1990.N3, С.3-11.

Умер Эдсгер Вайб Дейкстра (8 августа 2002). Проверено 27 сентября 2013.

Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1996.

Филиппов М Вопросы обеспечения безопасности корпоративных беспроводных сетей // Технологии и средства связи. 2003. № 2.

Фойницкий И. Я. Курс уголовного судопроизводства. Т. II (издание 3-е, пересмотренное и дополненное). Спб.: Сенатская типография, 1910. С. 507.

Фролов А.у Фролов Г. Защита от компьютерных вирусов // BYTE Россия. 2002. № 9.

Фролов А.у Фролов Г. Что нужно знать о компьютерных вирусах // BYTE Россия. 2002. № 8.

Хоффман Л. Современные методы защиты информации. М.:Сов.радио, 1980. – 264с.

Четкое О. Особенности применения двухфакторной аутентификации // Информационная безопасность. 2005.

№ 3.

Чмора А.Л. Современная прикладная криптография. М.: Гелиос АРВ, 2001.

Шагурин И., Бродин В., Калинин Л., Толстов Ю., Петров С., Исенин И., Эйдельман С., Ванюлин В. Средства проектирования и отладки систем управления на базе МК фирмы Motorola.

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011.

Шаньгин В.Ф. Защита информации в компьютерных системах и сетях М.: ДМК Пресс, 2012. — 592 с.

Шеннон К. Э. Теория связи в секретных системах // Шеннон К. Э. Работы по теории информации и кибернетике. М.: Иностр. лит., 1963.

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.

Шрамко В. Н. Аппаратно-программные средства контроля доступа // PCWeek/RE. 2003. № 9.

Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации // PCWeek/RE. 2004. № 12.

Шрамко В. Я. Комбинированные системы идентификации и аутентификации / / PCWeek/RE. 2004. № 45.

Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В.- 2001- 352 с.

Щербаков А.Ю. Современная компьютерная

безопасность. Москва • Книжный мир • 2009

Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.

Advanced Encryption Standard (AES) Development Effort. February 2001

CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department of Defense System Evaluation Criteria in Specific Environments.

Daemen J., Rijmen V. AES Proposal: Rijndael. Document version 2. September 1999

Datapro Reports on Information Security, vol.1-3, 1990-1993.

Dierks T., Allen C. RFC 2246: The TLS Protocol Version 1.0. January 1999

DoD 5200.28-STD. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC) 1985.

Dusse S., Hoffman P., Ramsdell B. etc. RFC 2311: S/MIME Version 2 Message Specification. March 1998

Evaluation Levels Manual, Department of Trade and Industry, Computer Security Branch, Kingsgate House, 66-74, V22.

FIPS Publication 197. Announcing the Advanced Encryption Standard (AES). November, 2001

Gladny H.M.- In: Performance of Computer Installation, Berke, 1978, Proceedings, p.151-200.

Hodges J. RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification. September 2002 / J. Hodges, R. Morgan

Housley R.y Ford W,Polk W. etc. RFC 2459: Internet X.509 Public Key Infrastructure. January 1999

Interoperability Specification for ICCs and Personal

Computer Systems. Part 8. Recommendations for ICC Security and Privacy Devices. Revision 1.0. PC/SC Workgroup, 1997.

ISO/IEC 14443-1 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics International Standard. 2000.

ISO/IEC 14443-2 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 2: Radio frequency power and signal interface International Standard. 2001.

Kent S., Atkinson R. RFC 2401: Security Architecture for IP. November 1998.

Menezes A. /., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1999. 82. Schneier B. Applied Cryptography. John Wiley & Sons, 1996.

Orman H. RFC 2412: The OAKLEY Key Determination Protocol. November 1998

Paulauskas N. Computer System Attack Classification / N. Paulauskas, E. Garšva // Electronics and Electrical Engineering. – 2006. – № 2(66). – P. 84–87.


AZƏRBAYCAN • DÖVLƏT • İQTİSAD • UNİVERSİTETİ
1930


AZƏRBAYCAN • DÖVLƏT • İQTİSAD • UNİVERSİTETİ
1930

İNFORMASİYA TƏHLÜKƏSİZLİYİ

Nəşriyyatın müdiri: Kamil Hüseynov
Baş redaktor: İsmət Səfərov
Redaktor: Rəhilə Cabrayılova
Korrektor: Südabə Manafova
Kompüter operatoru: Təranə Baxşəliyeva

ƏLİZADƏ M,N, BAYRAMOV H,M, MƏMMƏDOV Ə,S.

DƏRSLİK

Çapa imzalanmışdır 00.00.2016. Kağız formatı60x84 1/16. Həcmi 24,75 ç.v. Sifariş 00. Sayı: 300.

"İQTİSAD UNİVERSİTETİ" NƏŞRİYYATI.
AZ 1001, Bakı, İstiqlaliyyət küçəsi, 6

İNFORMASİYA TƏHLÜKƏSİZLİYİ