AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

SUMQAYIT DÖVLƏT UNİVERSİTETİ

K.Ə.Allahverdiyeva

Kompüter sistemlərinin təhlükəsizliyi

(məşğələ materialları)

060631 - Kompüter mühəndisliyi bakalavr ixtisası üçün

SUMQAYIT - 2020

"Təsdiq edirəm"
"İnformasiya və KT" kafedrasının müdiri
_____ dos. Mənsurov Q.M.
"_____"_____ 2020-ci il

Mühəndislik fakültəsi, Bakalavr təhsili pilləsi, qrup-612, kurs II
050631-Kompüter mühəndisliyi ixtisası,
Kompüter sistemlərinin təhlükəsizliyi (İPF-B10, 4 kredit) fənni üzrə
Təqvim-tematik plan (məşğələ, 15 saat)

№	Tədris olunacaq mövzular	Tarix	Saat
1	***2***	***3***	***4***
1.	Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi.	24.02.2020	*2*
2.	Ziyanverici proqramlar. Kompüter virusları.	09.03.2020	*2*
3.	İnformasiyanın qorunmasının aparat və proqram vasitələri.	23.03.2020	*2*
4.	Sadə şifrləmə üsulları. Sezar şifrləməsi.	06.04.2020	*2*
5.	Sadə şifrləmə üsulları. Yerdəyişmə üsulu.	20.04.2020	*2*
6.	Sadə şifrləmə üsulları. Kardonanın sehirli kvadratı.	04.05.2020	*2*
7.	Sadə şifrləmə üsulları. İkiqat biqram cədvəli.	18.05.2020	*2*
8.	Sadə şifrləmə üsulları. Qoşa şifr.	.05.2020	*1*

Ədəbiyyat

1. Qasımov V.A. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin Nəşriyyat-Poliqrafiya Mərkəzi. 2009, 340 s.
2. Əlizadə M. N., Bayramov H.M., Məmmədov Ə. S. İnformasiya Təhlükəsizliyi, Dərslik, Bakı, "Iqtisad Universiteti" nəşriyyatı, 2016, 384 səh.
3. Laboratoriya işinə aid təlimatlar.

Fənn müəllimi: **b/m.K.Ə.Allahverdiyeva**

1. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi

İnformasiya təhlükəsizliyinin təmin olunması problemi kompleks yanaşma tələb edir. Onun həlli üçün tədbirləri aşağıdakı səviyyələrə bölmək olar:

- qanunvericilik tədbirləri;
- inzibati tədbirlər;
- təşkilati tədbirlər;
- proqram-texniki tədbirlər.

Qanunvericilik tədbirləri müvafiq qanunları, normativ aktları, standartları və s. əhatə edir. Təəssüflə qeyd etmək lazımdır ki, qanunvericilik bazası bütün ölkələrdə praktikanın tələblərindən geri qalır. Qanunvericilik səviyyəsinin funksiyalarına aid etmək olar:

- İnformasiya təhlükəsizliyinin pozucularına qarşı neqativ münasibət yaratmaq və onu dəstəkləmək;
- İnformasiya təhlükəsizliyi probleminin vacibliyini hər zaman qeyd etmək;
- resursları tədqiqatların ən mühüm istiqamətlərində cəmləşdirmək;
- təhsil fəaliyyətini koordinasiya etmək.

Qanunvericilik səviyyəsində hüquqi aktlar və standartlar xüsusi diqqətə layiqdir. Standartların arasında «Narıncı kitab», X.800 tövsiyələri, ISO 15408 («Ümumi meyarlar»), ISO 17799 standartları daha geniş yayılıb.

İnzibati tədbirlərin əsas məqsədi təşkilatda informasiya təhlükəsizliyi sahəsində tədbirlər proqramını formalaşdırmaq və onun yerinə yetirilməsini zəruri resurslar ayırmaqla və işlərin vəziyyətinə nəzarət etməklə yerinə yetirilməsini təmin etməkdir. Tədbirlər proqramının əsasını təşkilatın öz informasiya aktivlərinin mühafizəsinə yanaşmasını əks etdirən informasiya təhlükəsizliyi siyasəti təşkil edir.

İnformasiya təhlükəsizliyi siyasəti - təşkilatda məxfi verilənlərin və informasiya proseslərinin mühafizəsi üzrə qabaqlayıcı tədbirlər kompleksidir. İnformasiya təhlükəsizliyi siyasətinin işlənməsinin əsas istiqamətləri aşağıdakılardır:

1. Hansı verilənləri və hansı ciddiyyətlə mühafizə etmək lazım olduğunu müəyyənləşdirmək;
2. Müəssisəyə informasiya aspektində kimin və nə həcmdə ziyan vura biləcəyini müəyyənləşdirmək;
3. Risklərin hesablanması və onların qəbuledilən səviyyəyədək azaldılması sxeminin müəyyən edilməsi;
4. Planlaşdırılan bütün texniki və inzibati tədbirlərin təsviri;
5. Baxılan proqramın iqtisadi qiymətinin hesablanması;
6. Müəssisənin rəhbərliyi tərəfindən təsdiq olunma və sənədləşdirmə;
7. Həyata keçirilmə.

Təşkilati tədbirlər informasiya mühafizəsinin səmərəli vasitələrindən biri olmaqla yanaşı, qurulan bütün mühafizə sistemlərinin əsasını təşkil edir. Təşkilati tədbirlər aşağıdakı mövzuları əhatə edir:

- şəxsi heyətin idarəolunması;
- fiziki mühafizə;
- sistemin iş qabiliyyətinin saxlanması;
- təhlükəsizlik rejiminin pozulmasına reaksiya;
- bərpa işlərinin planlaşdırılması.

Biz aşağıdakı proqram–texniki tədbirləri nəzərdən keçirəcəyik: identifikasiya və autentikasiya, icazələrin idarəolunması, protokollaşdırma və audit, kriptoqrafiya, ekranlaşdırma. İdentifikasiya və autentikasiya. İdentifikasiya (ingilis dilində identification) istifadəçiyə (və ya müəyyən istifadəçinin adından fəaliyyət göstərən prosesə) özünü adlandırmağa (öz adını bildirməyə) imkan verir.

Autentikasiya (ingilis dilində authentication) vasitəsi ilə ikinci tərəf əmin olur ki, subyekt doğrudan da özünü qələmə verdiyi şəxsdir. Autentikasiya sözünün sinonimi kimi çox vaxt “həqiqiliyin yoxlanması” işlədilir. Subyekt aşağıdakı mənbələrdən ən azı birini təqdim etməklə özünün həqiqiliyini təsdiq edə bilər:

- bildiyi nəyi isə (parolu, şəxsi identifikasiya nömrəsi, kriptoqrafik açar);
- sahib olduğu nəyi isə (şəxsi kart və ya digər təyinatlı analoji qurğu);

- özünün tərkib hissəsi olan nəyi isə (səs, barmaq izləri və s., yəni özünün biometrik xarakteristikalarını).

Autentikasiyanın ən geniş yayılmış növü paroldur. Daxil edilmiş parol və istifadəçi üçün əvvəlcədən verilmiş parol müqayisə edilir. Onlar üst-üstə düşdükdə istifadəçinin həqiqiliyi təsdiqlənmiş sayılır.

Parolların ən başlıca nöqsanı onların elektron ələ keçirilməsidir. Praktik olaraq yeganə çıxış yolu rabitə xətləri ilə ötürülməzdən əvvəl parolların kriptoqrafik şifrələnməsidir. Aşağıdakı tədbirlər parol mühafizəsinin etibarını artırmağa xeyli imkan verir:

- texniki məhdudiyyətlər qoyulması (parol çox qısa olmamalıdır, parolda hərf, rəqəm, durğu işarələri olmalıdır və s.)
- parolun fəaliyyət müddətinin idarə olunması, onların vaxtaşırı dəyişdirilməsi;
- parollar faylına icazənin məhdudlaşdırılması;
- sistemə uğursuz daxilolma cəhdlərinin məhdudlaşdırılması;
- istifadəçilərin təlimatlandırılması;
- parol generasiya edən proqramların istifadəsi.

Sadalanan tədbirləri həmişə, hətta parolla yanaşı digər autentikasiya metodları istifadə olunduğu halda da tətbiq etmək məqsədə uyğundur. Biometrik xarakteristikalara nəzarət qurğuları mürəkkəb və bahadırlar, buna görə də yalnız təhlükəsizliyə yüksək tələblər olan təşkilatlarda istifadə olunurlar.

İcazələrin idarə edilməsi. İcazələrin idarə edilməsi subyektlərin (istifadəçi və proseslərin) obyektlər (informasiya və digər kompyuter resursları) üzərində yetinə yetirə biləcəyi əməliyyatları müəyyən etməyə və onlara nəzarət etməyə imkan verir. İcazələrin məntiqi idarə edilməsi (icazələrin fiziki idarə edilməsindən fərqli olaraq) proqram vasitələri ilə realizə olunur. Məsələnin formal qoyuluşuna baxaq. Subyektlər məcmusu və obyektlər toplusu var. İcazələrin məntiqi idarəolunması hər bir (subyekt, obyekt) cütü üçün yolverilən (mümkün) əməliyyatlar çoxluğunu müəyyən etməkdən və qoyulmuş qaydaların yerinə yetirilməsinə nəzarət etməkdən ibarətdir.

(Subyekt, obyekt) münasibətini cədvəl şəklində təsvir etmək olar. Cədvəlin sətirlərində subyektlər, sütunlarında obyektlər sadalanır. Sətir və sütunların kəsişdiyi xanalarda verilən icazə növləri və əlavə şərtlər (məsələn, vaxt və hərəkətin məkanı) yazılır. İcazələrin məntiqi idarə edilməsi mövzusu - informasiya təhlükəsizliyi sahəsində ən mürəkkəb mövzudur. Səbəb ondadır ki, obyekt anlayışının özü (deməli icazə növləri də) servisdən servisə dəyişir. Əməliyyat sistemi üçün obyekt fayl, qurğu və prosesdir. Fayl və qurğular üçün adətən oxuma, yazma, yerinə yetirmə (proqram faylları üçün), bəzən də silmə və əlavə etmə hüquqlarına baxılır. Ayrıca hüquq kimi icazə səlahiyyətlərinin digər subyektlərə vermə imkanına baxıla bilər (sahiblik hüququ). Prosesləri yaratmaq və məhv etmək olar. Müasir əməliyyat sistemləri digər obyektlərin varlığını da mümkün edə bilər.

İcazə hüququna nəzarət proqram mühitinin müxtəlif komponentləri - əməliyyat sisteminin nüvəsi, əlavə təhlükəsizlik vasitələri, verilənlər bazasını idarəetmə sistemi, ara vasitəçi proqram təminatı (məsələn, tranzaksiyalar monitoru) tərəfindən həyata keçirilir. Protokollaşdırma və audit. Protokollaşdırma dedikdə informasiya sistemində baş verən hadisələr haqqında məlumatın qeyd edilməsi və toplanması başa düşülür. **Audit** - toplanan informasiyanın analizidir. Audit operativ (demək olar ki, real vaxtda) və ya dövri (məsələn, gündə bir dəfə) aparıla bilər. Protokollaşdırma və auditin realizə olunması aşağıdakı məqsədləri güdür:

- istifadəçi və administratorların hesabat verməli olmasını təmin etmək;
- informasiya təhlükəsizliyini pozma cəhdlərinin aşkar olunması;
- problemlərin aşkar olunması və analizi üçün informasiyanın təqdim olunması.

“Narıncı kitabda“ protokollaşdırma üçün aşağıdakı hadisələr sadalanır: sistemə giriş cəhdləri (uğurlu və uğursuz); sistemdən çıxış; kənar sistemlərə müraciətlər; fayllarla əməliyyatlar (açmaq, bağlamaq, adını dəyişmək, silmək); imtiyazların və digər təhlükəsizlik atributlarının dəyişdirilməsi.

Ekranlaşdırma. Ekranlaşdırma vacib təhlükəsizlik mexanizmlərindən biridir. Bu mexanizmin şəbəkələrarası ekran (ingilis termini firewall) adlanan realizələri olduqca geniş yayılıb. Ekranlaşdırma məsələsinin qoyuluşu aşağıdakından ibarətdir. Tutaq ki, iki informasiya sistemi var. Ekran - bir çoxluqdan olan istifadəçilərin digər çoxluğun serverlərinə müraciətlərini nizamlayan vasitədir. Ekran öz funksiyalarını iki sistem arasındakı bütün informasiya axınına nəzarət etməklə yerinə yetirir.

Ən sadə halda ekran iki mexanizmdən ibarətdir, onlardan biri verilənlərin yerdəyişməsini məhdudlaşdırır, digəri isə əksinə, bu yerdəyişməni həyata keçirir. Ən ümümi halda ekranı (yarımşəffaf pərdəni) süzgəclər (filtrlər) ardıcıllığı kimi təsəvvür etmək əlverişlidir. Süzgəclərdən hər biri verilənləri (tutub) saxlaya bilər, və ya onları dərhal "digər tərəfə" "ata bilər". Bundan başqa, analizi davam etdirmək üçün verilənləri növbəti süzgəcə ötürmək, adresatın adından verilənləri emal edərək nəticəni göndərənə qaytarmaq olar. Çox vaxt ekranı 7-səviyyəli OSI etalon modelinin üçüncü (şəbəkə), dördüncü (nəqliyyat) və ya yeddinci (tətbiqi) səviyyələrində realizə edirlər. Birinci halda ekranlaşdırıcı marşrutizator, ikinci halda - ekranlaşdırıcı nəqliyyat, üçüncü halda - ekranlaşdırıcı şlüz alınır. Hər bir yanaşmanın öz üstünlükləri və nöqsanları var; hibrid ekranlara da rast gəlinir, onlarda göstərilən yanaşmaların ən yaxşı cəhətlərini realizə etməyə çalışırlar.

Kriptoqrafiya. Müasir kriptoqrafiyanın predmeti informasiyanı bədniyyətlinin müəyyən əməllərindən mühafizə etmək üçün istifadə edilən informasiya çevirmələridir. Kriptoqrafiya konfidensiallığı, bütövlüyə nəzarəti, autentikasiyanı və müəlliflikdən imtinanın qeyri-mümkünlüyünü təmin etmək üçün tətbiq edilir.

«Kriptoqrafiya» sözü kryptos ('gizli') və graphos ('yazı') yunan sözlərindən yaranmışdır. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmdən və açardan istifadəni nəzərdə tutur. Kriptoqrafik alqoritm – məlumatların çevrilməsinin müəyyən üsuludur. Açar isə çevirmə üsulunu konkretləşdirir. Müasir kriptoqrafiya o prinsipdən çıxış edir ki, kriptoqrafik çevirmənin məxfiliyi yalnız açarın məxfi saxlanması ilə təmin edilməlidir.

İlk kriptosistemlər artıq bizim eranın əvvəlində meydana çıxır. Məsələn, məşhur Roma sərkərdəsi Yuli Sezar (e.ə. 100-44-cü illər) öz yazışmalarında indi onun adını daşıyan şifrdən istifadə edirdi. Müasir ingilis əlifbasına tətbiqdə bu şifr aşağıdakından ibarət idi. Adi əlifba yazılırdı, sonra onun altında həmin əlifba, lakin sola üç hərf dövri sürüşmə ilə yazılırdı:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Şifrləmə zamanı A hərfi D hərfi ilə, B hərfi E ilə və beləcə əvəz olunurdu. Məsələn: VENI VIDI VICI ® YHQL YLGL YLFL. Şifrlənmiş məlumatı alan hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın ikinci sətrindəki sürüşmənin qiymətidir.

Şifrləmənin simmetrik və asimmetrik adlanan iki əsas üsulu var. Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur. Şəkil 2 simmetrik şifrləmənin istifadəsini illüstrasiya edir. Olduqca effektiv (sürətli və etibarlı) simmetrik şifrləmə metodları var. Simmetrik şifrləmə alqoritmlərindən DES, 3-DES, IDEA, FEAL, Skipcack, RC2, RC4, RC5, CAST, Blowfish kimi blok şifrləri və bir sıra axın şifrləri (RC4, A5) daha geniş istifadə olunur.

Simmetrik şifrləmənin əsas nöqsanı ondan ibarətdir ki, məxfi açar həm göndərənə, həm də alana məlum olmalıdır. Bu bir tərəfdən məxfi açarların tam məxfi kanalla göndərilməsi problemini yaradır. Digər tərəfdən alan tərəf şifrlənmiş və deşifrlənmiş məlumatın varlığı əsasında bu məlumatı konkret göndərəndən almasını sübut edə bilməz. Çünki belə məlumatı o özü də yarada bilər.

Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri - açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri - gizli açar (yalnız alana məlum) deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir, hesablama texnikasının hazırki inkişaf səviyyəsində bu məsələ qeyri-mümkün hesab edilir.

Asimmetrik şifrləmə sisteminin istifadəsini illüstrasiya edir. Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA, ElGamal, Şnorr və s. alqoritmlərini göstərmək olar. Asimmetrik kriptoqrafiyanın əsas çatışmayan cəhəti sürətin aşağı olmasıdır. Buna görə onlar simmetrik metodlarla birgə işlədilir. Məsələn, açarların göndərilməsi məsələsini həll etmək üçün əvvəlcə məlumat təsadüfi açarla simmetrik metodla şifrlənir, sonra həmin təsadüfi açarı alan tərəfin açıq asimmetrik açarı ilə şifrləyirlər, bundan sonra məlumat və şifrlənmiş açar şəbəkə ilə ötürülür.

Asimmetrik metodlardan istifadə etdikdə, (istifadəçi, açıq açar) cütünün həqiqiliyinə zəmanət tələb olunur. Bu məsələnin həlli üçün rəqəmsal sertifikatdan istifadə edilir. Rəqəmsal sertifikat xüsusi sertifikasiya mərkəzləri tərəfindən verilir. Rəqəmsal sertifikatda aşağıdakı verilənlər olur: sertifikatın seriya nömrəsi; sertifikatın sahibinin adı; sertifikatın sahibinin açıq

açarı; sertifikatın fəaliyyət müddəti; elektron imza alqoritminin identifikatoru; sertifikasiya mərkəzinin adı və s. Sertifikat onu verən sertifikasiya mərkəzinin rəqəmsal imzası ilə təsdiq edilir. Bütövlüyə nəzarət üçün kriptoqrafik heş-funksiyalar istifadə edilir. Heş-funksiya adətən müəyyən alqoritm şəklində realizə edilir, belə alqoritm ixtiyari uzunluqlu məlumat üçün uzunluğu sabit heş-kod hesablamağa imkan verir. Praktikada 128 bit və daha artıq uzunluqda heş-kod generasiya edən heş-funksiyalardan istifadə edilir.

Heş-funksiyanın xassələri elədir ki, onun köməyi ilə alınan heş-kod məlumatla “möhkəm” bağlı olur. Məlumatın hətta bir biti dəyişdikdə belə heş-kodun bitlərinin yarısı dəyişir. Heş-funksiyaya misal olaraq MD2, MD4, MD5, RIPEMD, SHA1 və s. alqoritmlərini göstərmək olar. Misal. ‘1234567890’ sətri üçün SHA1 heş-funksiya alqoritminin hesabladığı heş-kod 16-lıq say sistemində 01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A simvollar ardıcıllığıdır.

2. Ziyanverici proqramlar. Kompüter virusları

İnformasiyanın qorunması üçün əsas təhlükələrdən biri kompüterə "girmiş" ziyanverici proqramlardır. Belə ziyanverici proqramlar verilənlərin tamlığı üçün təhlükə yarada bilər. Kompüterdə saxlanılan verilənlərə və proqramlara zərər vuran proqramlara ziyanverici proqramlar deyilir.

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

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

Qeyd etmək lazımdır ki, əksər hallarda məhz serverlər kompüter viruslarının hədəfinə çevrilir. Bir qayda olaraq, kompüter şəbəkələri, o cümlədən İnternet virusların yayılması üçün potensial vasitə rolunu oynayır. Belə ki, viruslar serverdə olan proqramları yoluxdursa, şəbəkə vasitəsilə ona qoşulmuş kompüterlərdə (işçi stansiyalara) yayıla və bütün şəbəkəyə ciddi ziyan vura bilər.

Bəzən kompüter virusu yarandığı ilk anda fəaliyyət göstərmir. Kompüterin yaddaşında və ya proqramlarda "yaşayan" belə viruslar yalnız müəyyən olunmuş vaxtlarda işə düşür. Viruslar emasl olunan bütün informasiyaları izləyir və informasiya bir yerdən başqa bir yerə ötürüldükdə virus da onunla birlikdə yerini dəyişir.

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

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

Kompüter virusları proqram təminatında və yaddaş qurğularında yerləşməsi, KSŞ-də yayılması, fəallaşması üsullarına və vurduğu ziyanın xarakterinə görə fərqlənirlər.

Kompüter virusları yazılmış informasiyanın və proqramların təhrif olunması, korlanması və ya məhv edilməsi, istifadəçilərin sorğularına sistemin reaksiya verməsi və proqramların yerinə yetirilməsi üçün tələb olunan vaxtın artması, kompüterin düzgün fəaliyyətinin pozulması, disk qurğularının sıradan çıxması və s. kimi ağır nəticələr verə bilər.

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

Bəzi viruslara inkişaf edən əlamətlər xas olur. Başqa sözlə, "xəstəlik" getdikcə kəskinləşir. Məsələn, aydın olmayan səbəblərdən proqramların həcmi hər istifadə zamanı əhəmiyyətli dərəcədə artır və hyaddaş qurğuları dolur. Nəticədə, bu, faylların silinməsinə və proqram təminatının məhvinə gətirib çıxara bilər.

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

Bəzən proqramı hazırlayanlar öz proqramlarını və disklərini hər hansı virusla qəsdən yoluxdururlar ki, icazəsiz şəkildə proqramı və ya diski köçürənlər kompüterlərində virusların yayılması problemi ilə qarşılassınlar.

Şəbəkə qurdları kateqoriyasına ziyanvericilik fəaliyyətini həyata keçirmək məqsədilə öz sürətlərini aşağıdakı yollarla lokal və ya qlobal kompüter şəbəkələri vasitəsilə yayan ziyanverici proqramlar aid edilir:

- uzaq məsafədə olan kompüterlərə soxulmaq;
- öz sürətini uzaq məsafədə olan kompüterlərdə işə salmaq;
- gələcəkdə şəbəkənin digər kompüterlərinə yayılmaq.

Şəbəkə qurdları disklərdə olan faylları dəyişdirmirlər, lakin kompüter şəbəkələrində yayılır, kompüterin əməliyyat sisteminə girir, digər kompüterlərin və ya istifadəçilərin ünvanlarını tapır və müxtəlif yayma vasitələrindən istifadə etməklə özünün surətlərini həmin ünvanlara göndərir.

Özlərinin yayılması üçün şəbəkə qurdları müxtəlif kompüter və mobil şəbəkələrdən istifadə edirlər. Belə şəbəkələrə misal olaraq aşağıdakıları göstərmək olar:

- İnternet, o cümlədən elektron poçtu;
- məlumatların ani (interaktiv) mübadiləsi sistemləri;
- faylların mübadiləsi şəbəkələri;
- İRC (İnternet Relay Chat) şəbəkələr;
- lokal şəbəkələr;
- mobil qurğular (telefonlar, cib kompüterləri və s.) arasında məlumatların mübadiləsi şəbəkələri.

Əksər məşhur şəbəkə qurdları fayllar şəklində - elektron məktuba əlavə, Veb və ya FTP resurslarda, İCQ və İRC məlumatlarda yoluxmuş fayla istinadlar, P2P (Peer to Peer) mübadilə kataloqunda fayl şəklində yayılırlar. Bəzi şəbəkə qurdları şəbəkə paketləri şəklində yayılaraq kompüterin yaddaşına daxil olur və öz kodunu aktivləşdirir. Belə şəbəkə qurdlarını “faylsız” və ya ”paket” qurdları adlandırırlar.

Şəbəkə qurdları istifadəçi tərəfinfdən hər hansı hərəkət edilmədən yoluxmuş maşınlara daxil olurlar. Onlar öz təbiətlərinə görə bioloji prototiplərinə çox yaxındırlar. Hələ ki, qabaqlayıcı tədbirlər, o cümlədən antivirus skanerləri və vaksinləri şəbəkə qurdları ilə mübarizədə çox qeyri-effektiv olaraq qalırlar. Onlar viruslardan fərqli olaraq, özlərinin yayılması üçün lokal və qlobal şəbəkələrin protokollarından və imkanlarından fəal surətdə istifadə edirlər, ona görə də onları şəbəkə qurdları adlandırırlar.

Uzaq məsafədə olan kompüterə daxilolmaq və öz surətini işə salmaq üçün şəbəkə qurdları müxtəlif üsullardan istifadə edirlər:

- sosial mühəndislik - social engineering (məsələn, qoşma fayl açmağa çağıran elektron məktubun mətni);
- şəbəkənin konfiqurasiyasında olan nöqsanlar (məsələn, tam giriş üçün açıq olan diskə köçürmə);
- əməliyyat sistemlərinin və əlavələrin təhlükəsizlik xidmətlərində səhvlər;
- xüsusi toplayıcı proqram – virus və ya qurd olmayan bu proqram özsü kompüterə daxil olur, sonra isə şəbəkə qurdunu və ya virusu hissə - hissə şəbəkədən kompüterə köçürür. Qurd və ya virus kompüterə hissə - hissə köçürüldüyündən antivirus proqramları onu aşkar edə bilmir.

Bəzi şəbəkə qurdları digər ziyanverici proqramların xassələrinə malik olurlar. Məsələn, bəzi şəbəkə qurdları özündə troya funksiyalarını saxlayır və ya kompüter viruslarına analoji olaraq lokal diskdə yerinə yetirilən faylları yoluxdura bilirlər. Başqa sözlə, şəbəkə qurdları troya proqramlarının və ya kompüter viruslarının xassələrinə mzalik olurlar.

Əksər ölkələrdə ziyanverici proqramların yaradılması, istifadəsi və yayılması qanunla qadağandır.

Ziyanverici proqramların ən geniş yayılmış növü kompüter viruslarıdır. Kompüter virusu proqramın, sənədin içərisinə, yaxud verilənlər daşıyıcısının müəyyən sahələrinə daxil olan parazit proqram kodudur. Bu kod daxil olduğu kompüterdə özü-özünü çoxalda, müxtəlif icazəsiz və ziyanlı işlər görə bilər.

Özü-özünü çoxaltma qabiliyyəti virus proqramlarının başlıca xüsusiyyətidir. Bu proqramlar kompüter və digər daşıyıcıların sahiblərinin xəbəri olmadan öz nüsxələrini yaradır. Bir çox viruslar ziyan vurmaqla - verilənləri məhv etmək və kompüterin normal işini pozmaqla da məşğul olurlar. Öz bioloji "qardaşları" kimi, kompüter viruslarının arasında da elələri vardır ki, onlar öz-özünə çoxalıb yayılır, lakin heç bir ziyan vurmur.

Kompüterdə virusun "həyat yolu" yoluxdurma və aktivləşmə ilə başlanır. Yoluxma təxminən bu cür baş verir: istifadəçi öz kompüterində virus daşıyıcısı olan proqramı başladır. Bu proqram İnternetdən də "yüklənə" bilər, tanışlarınızdan köçürüb əldə etdiyiniz proqram da ola bilər. Proqramın yüklənməsindən əvvəl, yaxud sonra virus aktivləşərək fəaliyyətə başlayır. Virusun fəaliyyət ssenarisi təxminən belə olur:

1. Kompüterdə yoluxdurulması mümkün olan bütün proqramları tapmaq.
2. Özünü proqramın əvvəlinə, yaxud sonuna yazmaq.

3. Əgər "kritik" tarix, başqa sözlə, virusun hücuma keçəcəyi gün yetişmişsə, dağıdıcı işlər görmək.

4. Əgər həmin tarix yetişməmişsə, hər hansı "xırda" zərər yetirmək; məsələn, kompüterin sərt diskində hər hansı kiçik sahəni "şifrləmək".

"Kompüter virusu" termini ilk dəfə 1973-cü ildə "Westworld" fantastik filmində istifadə olunmuşdur. Həmin filmdə bu sözbirləşməsi məhz bugünkü anlamda işlədilmişdir: "Kompüter sisteminə geniş yayılmış ziyanverici proqram".

Bəs kompüterin virusa yoluxmasını necə müəyyən etmək olar? Kompüterə ziyanverici proqramların girməsini bildirən bir sıra əlamətlər vardır:

* ekrana nəzərdə tutulmamış məlumatların və görüntülərin çıxması;
* nəzərdə tutulmamış səs siqnallarının verilməsi;
* CD/DVD disksürəninin özü-özünə açılması və bağlanması;
* kompüterdə hər hansı proqramın "özbaşına" başladılması;
* kompüterin tez-tez sıradan çıxması və "ilişməsi";
* proqramlar başladılarkən kompüterin sürətinin az olması;
* fayl və qovluqların yoxa çıxması, yaxud dəyişdirilməsi;
* sərt diskə tez-tez müraciət;
* brauzerin asılıb-qalması, yaxud özünü gözlənilməz aparması (məsələn, proqram pəncərəsini qapatmağın mümkün olmaması).

İnternetin inkişafı virusların da yayılma sürətinə güclü təsir göstərdi. Bundan başqa, viruslar "keyfiyyətcə" də dəyişdi. Əgər təxminən 10-15 il bundan öncə virus müəlliflərinin əsas məqsədi kompüteri sıradan çıxarmaq idisə, XXI əsrin əvvəllərində virusların başlıca fəaliyyəti düşdüyü kompüterdən hər hansı informasiyanı oğurlamağa və həmin kompüterə kənar şəxslərin daxil olmasını təmin etməyə yönəlmişdir. İnformasiyanı oğurlayan virus hər hansı bir şirkətin gizli saxlanılan sənədlərini açıqlamaqla, həmin şirkətin nüfuzuna ciddi zərbə vura bilər. Əgər belə virus məxfi hərbi sənədlərin, yaxud başqa sirlərin olduğu kompüterə düşərsə, nə baş verəcəyini təsəvvür etmək belə çətindir.

Dünyanın inkişaf etmiş ölkələrində kompüter viruslarının vurduğu ziyan yüz milyon dollarlarla ölçülür.

(i) Ziyanverici proqramların yarandığı dövrlərdə, sadəcə, istifadəçilərin işinə mane olan zarafat-viruslar daha populyar idi. Məsələn, bir virus proqramı ekrana belə məlumat çıxarırdı: "L + A + M + E + R + F1 + Alt klavişlər kombinasiyasını eyni zamanda basın". İstifadəçi bu "məsləhətə" əməl edən kimi məlumat verilirdi ki, faylların yerləşmə cədvəli sərt diskdən silinərək, operativ yaddaşa yazıldı və əgər istifadəçi barmağını hər hansı bir klavişin üzərindən götürərsə, o, sərt diskdəki informasiyalarla vidalaşmalı olacaq. Yox, əgər düz bir saat bu vəziyyətdə gözləyə bilsə, hər şey əvvəlki vəziyyətinə qayıdacaq. Bir saat bu cür vəziyyətdə qaldıqdan sonra məlum olurdu ki, bu bir zarafat imiş.

Virus proqramlarının ən ziyanlı növlərindən biri Troya proqramlarıdır. Troya proqramları istifadəçidən icazəsiz olaraq informasiyaları toplayır və onları "cinayətkara" göndərir, eləcə də həmin informasiyaları dağıdır, yaxud ziyanlı məqsədlər üçün dəyişdirir. Bundan başqa, Troya proqramları kompüterin işini poza bilər, yaxud istifadəçidən xəbərsiz olaraq kompüterin resurslarından ziyanlı məqsədlər üçün istifadə edə bilər.

Troya virusları öz adını bir tarixi hadisədən götürüb. Homerin "İliada" poemasında qədim yunanlar tərəfindən Troya şəhərinin mühasirəsi (e.ə. təxminən 1250-ci ildə) təsvir olunub. Yunanlar taxtadan nəhəng at düzəldib, içərisinə öz döyüşçülərini yerləşdirmiş və onu şəhər darvazasının qabağında qoymuşlar. Heç nədən şübhələnməyən troyalılar atı çəkib darvazadan içəri salmış, ancaq gecə yunan döyüşçüləri atın içərisindən çıxıb, şəhəri tutmuşlar.

Troya proqramları, adətən, kompüterə şəbəkə soxulcanı kimi girir. Onlar bir-birindən öz "əməllərinə" görə fərqlənir.

* Uzaqdan idarəetmə utilitləri. Bu qrupa aid proqramlar şəbəkədə olan kompüteri uzaqdan idarə edən utilitlərdir. Belə gizli idarəetmə utilitləri faylları qəbul edə, yaxud müxtəlif ünvanlara göndərə, onları başlada və məhv edə, kompüteri yenidən yüklədə bilər və s.

* Casuslar. Bu qrupa aid troyalılar elektron casusluqla məşğul olurlar: yoluxmuş kompüterdə istifadəçinin klaviaturadan daxil etdiyi informasiya, ekranın şəkli, aktiv proqramların siyahısı və istifadəçinin həmin proqramla yerinə yetirdiyi əməllər müəyyən fayla yazılır və vaxtaşırı "cinayətkara" göndərilir. Bu tipli Troya proqramlarından çox zaman bank və onlayn

ödəmə sistemlərinin istifadəçiləri haqqında məxfi informasiyaların oğurlanması məqəsədilə istifadə olunur.

* Reklam proqramları. Reklam proqramları (ing. Adware: Advertisement - reklam və Software - proqram təminatı) hər hansı bir proqrama reklam kimi yerləşdirilir və Troya casus proqramı funksiyasını yerinə yetirə bilir. Reklam proqramları gizlicə kompüterin istifadəçisi haqqında müxtəlif informasiyalar toplaya, sonra onu "cinayətkara" göndərə bilir.

Virus hücumlarının təsirini heçə endirməyin ən uğurlu yolu mühüm əhəmiyyət kəsb edən verilənlərin ehtiyat üçün surətlərinin saxlanmasıdır. Viruslar aparat vasitələrini sıradan çıxara bilmir. Virus hücumlarının əlamətləri aşkarlandıqda kompüterin verilənlər daşıyıcılarını büsbütün təmizləmək lazımdır. Verilənlərin ehtiyat daşıyıcılardan köçürülməsi kompüter sisteminin normal vəziyyətini bərpa etməyə imkan verir.

Kompüterdə virus əlamətləri aşkarlandıqda nə etməli? İlk addım olaraq yerinə yetirdiyiniz işlərin nəticələrini xarici daşıyıcıda (disketdə, CD- və ya DVD-diskdə, fləş-kartda və s.) saxlayın. Sonra

* kompüteri lokal şəbəkədən və İnternetdən ayırın (əgər qoşulmuşsa);

* əməliyyat sistemi kompüterə düşmüş virus nəticəsində sərt diskdən yüklənmirsə, onda onu CD diskdən yükləməyə çalışın;

* antivirus proqramını başladın.

Antivirus proqramları vasitəsilə informasiyanın mühafizəsi

Kompüter virusunun öz bioloji "qardaşı" ilə bir oxşarlığı da əvvəlcədən hər ikisinin qarşısının alınmasının (profilaktikasının), yoluxmadan sonrakı müalicəyə nisbətən çox-çox asan olmasıdır. Kompüter viruslarından qorunma üç səviyyədə təşkil oluna bilər:

Birinci səviyyədə virusların kompüterə girməsinin qarşısı alınır.

İkinci səviyyədə virus hücumlarının qarşısı alınır.

Üçüncü səviyyədə virus hücumlarının təsiri minimuma endirilir.

Təhlükəsizlik tədbirləri nəticəsində virusların kompüterə düşməsi təhlükəsi azaldılır. Şübhəli mənbələrdən əldə olunan proqram təminatlarından istifadədən qaçmaq lazımdır. Kompüterə kənardan, o cümlədən İnternetdən daxil olan proqram koduna çox ciddi nəzarət olunmalıdır.

Yoluxma faktını aşkarlamaq, virusların çoxalmasına mane olmaq və virus hücumlarının qarşısını almaq üçün antivirus proqramlarından istifadə olunur. Verilənlərin mübadiləsi zamanı viruslara xas olan baytların aşkar edilməsi və viruslar üçün xarakterik hərəkətlərin qeydə alınması onların axtarışının əsasını təşkil edir.

Müqayisə üçün zəruri olan verilənlər antivirus proqramının verilənlər bazasında saxlanılır. Antivirus verilənlər bazasını daim yeni viruslar haqqında məlumatlarla doldurmaq, başqa sözlə, virus bazasını yeniləmək lazımdır. Antivirus proqramlarının uğuru da məhz bundan asılı olur.

Fəaliyyətlərindən asılı olaraq antivirus proqramları bir neçə sinfə ayrılır:

* Detektorlar hər hansı məlum virusa yoluxmuş faylları aşkarlamağa imkan verir.

* Doktorlar (faqlar) təkcə yoluxmuş faylları aşkarlamır, həm də onları ilkin duruma qaytarmağa çalışır.

* Müfəttişlər kompüter hücumları mümkün olan yerlərdəki dəyişikliklərə nəzarət edir; bu məqsədlə proqramların və disklərin sistem sahələrinin ilkin, yoluxmamış hesab edilən durumları haqqında məlumat yadda saxlanılır, sonra istifadəçinin müəyyən etdiyi vaxtda onları cari vəziyyətlə müqayisə edir.

* Doktor-müfəttişlər yuxarıda göstərilən iki növ proqramın imkanlarını özündə birləşdirir.

* Süzgəclər virusların çoxalma və zərərvurma məqsədi ilə əməliyyat sisteminə etdikləri müraciətləri tutur.

* Vaksinlər, yaxud immunizatorlar iş qabiliyyətlərini saxlamaqla proqramları elə dəyişdirirlər ki, onlar viruslar üçün yoluxmuş kimi görünsün. Belə olduqda, viruslar həmin fayllara "ilişmir".

Kompüterdə virusların axtarışı verilənlər daşıyıcılarının, yaxud axınının daranması [scan] yolu ilə yerinə yetirilir. Darama prosesində operativ yaddaşda, daşıyıcılarda virusa yoluxmanın əlamətlərinin olub-olmaması yoxlanılır. Aşkarlanmış viruslar deaktivləşdirilir və məhv edilir. Mümkün olduqda dəyişdirilmiş (yoluxmuş) faylların ilkin vəziyyəti bərpa olunur.

Bu gün Symantec Norton Antivirus, Kasperski antivirusu, Dr. Web, AcAfee VirusScan, Panda Titanium Antivirus kimi antivirus proqramları daha çox tanınır.

3. İnformasiyanın qorunmasının aparat və proqram vasitələri

İnformasiya təhlükəsizliyi (en. Information Security, ru. Информационная безопасность) - informasiya və ona xidmət edən infrastrukturun sahibi və ya istifadəçilərinə ziyan vurmağa səbəb olan təbii və ya süni xarakterli, təsadüfi və ya qəsdli təsirlərdən informasiya və ona xidmət edən infrastrukturun mühafizəli olmasıdır.

İnformasiyanın mühafizəsi - informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

Təhdid dedikdə kiminsə maraqlarına ziyan vurmağa səbəb ola bilən potensial mümkün hadisə, şərait, hərəkət, proses və s. nəzərdə tutulur.

İnformasiyanın təhlükəsizliyinin təmin olunması probleminin vacibliyini və aktuallığını şərtləndirən səbəblərdən aşağıdakıları xüsusi vurğulamaq olar:

- şəbəkə texnologiyalarının geniş yayılması və lokal şəbəkələrin qlobal şəbəkələr halında birləşməsi;
- informasiya təhlükəsizliyinin pozulmasına praktik olaraq mane olmayan qlobal İnternet şəbəkəsinin inkişafı;
- minimal təhlükəsizlik tələblərinə belə cavab verməyən proqram vasitələrinin geniş yayılması.

İnformasiyanın mühafizəsi - informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

Təhlükə dedikdə sistemə dağılma, verilənlərin üstünün açılması və ya dəyişdirilməsi, xidmətdən imtina formasında ziyan vurulmasına səbəb ola bilən istənilən hal, şərait, proses və hadisələr nəzərdə tutulur.

Təhlükələri müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələri təbii və süni xarakterli təhlükələrə ayırırlar. Süni xarakterli təhlükələr də öz növbəsində bilməyərəkdən və qəsdən törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir:

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;

Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service - xidmətdən imtina).

Məxfilik informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Məxfiliyin pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.

Bütövlük - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.

Əlyetərlik - yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik - daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.

Təhlükələr digər əlamətlərinə görə də təsnif oluna bilər:

- Baş vermə ehtimalına görə (çox ehtimallı, ehtimallı, az ehtimallı);
- Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər);
- Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi);
- Təsir xarakterinə görə (aktiv, passiv);
- Obyektə münasibətinə görə (daxili, xarici).

Daxili və xarici təhlükələrin nisbətini təqribi olaraq belə xarakterizə etmək olar. Təhlükələrin 80%-i təşkilatın öz işçiləri tərəfindən onların bilavasitə və ya dolayısı yolla iştirakı ilə baş verir. Təhlükələrin 20%-i kənardan icra olunur.

- əlyetənlik - yolverilən vaxt ərzində tələb olunan informasiya resursunu, informasiya xidmətini əldə etmək imkanı;

- tamlıq - informasiyanın əvvəlcədən müəyyən edilmiş şəkil və keyfiyyəti saxlaması xassəsi;

Məxfilik - informasiyanın icazəsiz girişlərdən məxfi saxlanılması xassəsidir.

İnformasiyanın bu xassələrindən çıxış edərək təhdidlərin üç əsas növünü ayırmaq olar:

- konfidensiallığın pozulmasına yönələn təhdidlər;
- əlyetənliyin pozulmasına yönələn təhdidlər;
- tamlığın pozulmasına yönələn təhdidlər.
- DoS-hücum
- Botnet
- Fişinq

İnformasiya təhlükəsizliyi sahəsində tarixən ilk standart ABŞ Müdafiə Nazirliyinin "Etibarlı kompüter sistemlərinin qiymətləndirilməsi meyarları" olmuşdur. Cildinin rənginə görə çox vaxt "Narıncı kitab" adlanan bu standart ilk dəfə 1983-cü ilin avqustunda nəşr edilmişdi.

"Narıncı kitabda" etibarlı sistemi "giriş hüququnu pozmadan müxtəlif məxfilik dərəcəsinə malik informasiyanın istifadəçilər qrupu tərəfindən eyni zamanda emalını təmin etmək üçün yetərli aparat və proqram təminatı istifadə edən sistem" kimi müəyyən edir.

"Narıncı kitabda" dörd etibar səviyyəsi - D, C, B və A müəyyən edilir.

D səviyyəsi qeyri-qənaətbəxş qəbul edilmiş sistemlər üçün nəzərdə tutulub. C səviyyəsindən A səviyyəsinə keçdikcə sistemlərə daha ciddi tələblər irəli sürülür. C və B səviyyələri etibar dərəcəsinin tədricən artması ilə siniflərə bölünür (C1, C2, B1, B2, B3).

"Narıncı kitabda" daxil edilmiş təsnifatı qısaca belə ifadə etmək olar:

- C səviyyəsi - girişin ixtiyari idarə edilməsi;
- B səviyyəsi - girişin mandatlı idarə edilməsi;
- A səviyyəsi - təhlükəsizliyin verifikasiya edilə bilməsi.

Əlbəttə, "Narıncı kitabın" ünvanına bir sıra ciddi iradlar söyləmək olar (məsələn, paylanmış sistemlərdə meydana çıxan hadisələrin tamamilə nəzərə alınmaması). Buna baxmayaraq qeyd etmək lazımdır ki, "Narıncı kitabın" nəşri heç bir mübaliğə olmadan informasiya təhlükəsizliyi sahəsində çox böyük əhəmiyyətli hadisə oldu. Hamı tərəfindən qəbul edilən anlayışlar bazisi meydana çıxdı ki, bunlarsız informasiya təhlükəsizliyi məsələlərinin hətta müzakirəsi belə çətin olardı.

Qiymətləndirmə standartlarının içərisində ən tamı və müasiri İSO/İEC 15408 "İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları" standartıdır (1 dekabr 1999-cu ildə nəşr olunmuşdur). Bu beynəlxalq standart bir neçə ölkə mütəxəssisinin demək olar ki, onillik işinin nəticəsidir, o özündə həmin dövrə mövcud olan beynəlxalq və milli standartların təcrübəsini cəmləşdirmişdir.

Tarixi səbəblərdən bu standartı çox zaman "Ümumi meyarlar" adlandırırlar. Biz də bu qisaltmadan istifadə edəcəyik.

"Ümumi Meyarlar" əslində informasiya sistemlərinin təhlükəsizliyini qiymətləndirmə alətlərini və onların istifadə qaydalarını müəyyən edən metastandartdır. "Narıncı kitabdan" fərqli olaraq Ümumi Meyarlarda əvvəlcədən müəyyən edilmiş " təhlükəsizlik sinifləri" yoxdur. Belə sinifləri konkret təşkilat və/və ya konkret informasiya sistemi üçün mövcud olan təhlükəsizlik tələblərindən çıxış edərək qurmaq olar.

"Narıncı kitab"dakı kimi Ümumi meyarlarda da təhlükəsizlik tələblərinin iki əsas növü var:

funksional tələblər - mühafizənin aktiv aspektinə uyğundur, təhlükəsizlik funksiyalarına və onları realizə edən mexanizmlərə irəli sürülür;

zəmanət tələbləri - mühafizənin passiv aspektinə uyğundur, yaradılma və istismar texnologiyasına və prosesinə irəli sürülür.

Təhlükəsizlik tələbləri irəli sürülür, onların yerinə yetirilməsi isə müəyyən qiymətləndirmə obyekti üçün - aparat-proqram məhsulu üçün və ya informasiya sistemi üçün yoxlanır.

Funksional tələblərin ingilis dilində ixtisarlarla işarə edilən aşağıdakı sinifləri müəyyən edilir.

Təhlükəsizliyin auditi (FAU). Təhlükəsizlik sisteminin auditi - təhlükəsizlik sisteminə aid informasiyanın tanınması, qeydə alınması, saxlanması və analizidir.

Kommunikasiya (FCO). Bu sinfin tələblərinin yerinə yetirilməsi zəmanət verir ki, informasiyanı göndərən ötürülən informasiyadan, qəbuledən isə onu aldığından imtina edə bilməz.

Kriptoqrafik dəstək (FCS). Sinifdə kriptoqrafik açarların və əməliyyatların idarə edilməsi üzrə tələblər var.

İstifadəçinin verilənlərinin mühafizəsi (FDP). Sinif informasiyanı daxiletmə, xaricetmə və saxlama zamanı istifadəçi verilənlərinin mühafizəsinə aid təhlükəsizlik tələblərini müəyyən edir.

İdentifikasiya və autentifikasiya (FIA). Bu sinfin tələbləri sistemdə istifadəçilərin müəyyən edilməsi və verifikasiyası ilə, onların sistemdə səlahiyyətləri ilə, həmçinin təhlükəsizlik atributlarının hər bir istifadəçiyə düzgün verilməsi ilə işləyir.

Təhlükəsizliyin idarə edilməsi (FMT). Sinfə təhlükəsizlik funksiyaları verilənlərinin və atributlarının, həmçinin təhlükəsizlik rollarının idarə edilməsi üzrə tələblər daxildir.

Konfidensiallıq (FPR). Bu sinfin tələblərinin realizə edilməsi istifadəçini onun səlahiyyətlərinin digər istifadəçilər tərəfindən açılmasından və sui-istifadə edilməsindən mühafizə edəcək.

Təhlükəsizlik funksiyalarının mühafizəsi (FPT). Sinfə sistemin təhlükəsizlik mexanizmlərinin tamlığına və idarə edilməsinə aid funksional tələblər daxildir (realizə edilən təhlükəsizlik siyasətindən asılı olmayaraq).

Resursların istifadəsi (FRU). Bu sinfin tələbləri lazımi resursların əlyetənliyini (emal /və ya saxlama imkanı kimi), həmçinin sistemin imtinaları ilə funksional imkanların meydana çıxan bloklanması halında mühafizəni təmin edir.

Qiymətləndirmə obyektinə giriş (FTA). Sinif istifadəçinin təyin edilmiş iş seansına funksional nəzarət tələblərini identifikasiya və autentifikasiya üzrə tələblərdən asılı olmadan müəyyən edir.

Etibarlı marşrut/kanal (FTP). Sinif aşağıdakı tələbləri təmin edir:

Istifadəçi ilə sistemin təhlükəsizlik funksiyaları arasında etibarlı kommunikasiya marşrutu;

sistemin təhlükəsizlik funksiyaları arasında etibarlı rabitə kanalı.

Standart ingilis dilində ixtisarlarla adlandırılmış aşağıdakı zəmanət siniflərini daxil edir:

Konfiqurasiyanın idarə edilməsi (ACM). Ümumi Meyarlar qiymətləndirilən obyektin tamlığının saxlanmasını onun dəqiqləşdirilməsi və modifikasiyası zamanı idarəetmə və intizam tələb etməklə təmin edir.

Çatdırılma və istismar (ADO). ADO zəmanət sinfi qiymətləndirilən obyektin etibarlı çatdırılması, qurulması və istismar istifadəsinə aid tədbirlərə, prosedurlara və standartlara tələbləri müəyyən edir.

Yaratma (ADV). Bu zəmanət sinfi qiymətləndirilən obyektin ümumi spesifikasiyasından təhlükəsizlik funksiyalarının faktiki realizəyə yuxarıdan aşağıya addım-addım dəqiqləşdirilməsi üzrə tələbləri müəyyən edir.

Rəhbər sənədlər (AGD). Bu zəmanət sinfi istehsalçının təqdim etdiyi istismar sənədlərinin anlaşıqlıq və tamlıq tələblərini müəyyən edir.

Həyat dövrünün dəstəklənməsi (ALC). Bu sinif qiymətləndirilən obyektin yaradılmasının bütün addımları üçün həyat dövrü modelini, o cümlədən qüsurların aradan qaldırılması prosedurlarını və siyasətini dəqiq müəyyən edir.

Testlər (ATE). Bu zəmanət sinfi təhlükəsizlik funksiyalarının funksional təhlükəsizlik tələblərini ödədiyini nümayiş etdirən sınaqlara tələbləri müəyyən edir.

Boşluqların qiymətləndirilməsi (AVA). Bu zəmanət sinfi istismar zamanı qalan zəif yerlərin identifikasiyasına yönəlmiş tələbləri müəyyən edir.

Hazırda informasiya təhlükəsizliyi sahəsində ən məşhur standartlar ISO/IEC 2700x standartlar seriyasıdır.

Standartlar seriyasının tarixi belə başlamışdır. Britaniya Standartlar İnstitutu (BSI) tərəfindən işlənilmiş və fəaliyyət dairəsindən asılı olmayaraq şirkətlərin informasiya təhlükəsizliyinin idarə edilməsi üçün 1998-ci ildə BS 7799 milli standartı qəbul edilmişdi. Britaniya standartı BS 7799 dünyanın 27 ölkəsində, o cümlədən Britaniya Birliyi ölkələrində dəstəklənirdi.

2000-ci ilin sonunda ISO (Beynəlxalq Standartlaşdırma Təşkilatı) Britaniya standartı BS 7799 əsasında ISO/IEC 17799 «Information technology - Information security management» («İnformasiya texnologiyaları - İnformasiya təhlükəsizliyinin idarə edilməsi») beynəlxalq standartını işlədi və qəbul etdi.

2005-ci ildə standartın 2000-ci il redaksiyası ilə müqayisədə yenidən əhəmiyyətli işlənmiş ISO 17799:2005 variantı çıxdı. 2005-ci ildə həmçinin BS 7799 standartının ikinci hissəsi ISO

27001 standartı kimi qəbul edildi. ISO 27001 standartı informasiya təhlükəsizliyi sistemlərinin sertifikastlaşdırılması üçün nəzərdə tutulub.

ISO/IEC 17799:2005 standartı 2007-ci ildən ISO/IEC 27002 adını alıb. Bu standartda informasiya təhlükəsizliyini idarəetmə sisteminin elementləri on bir qrup üzrə bölünüb:

Təhlükəsizlik siyasəti - təşkilatın rəhbərliyi tərəfindən informasiya təhlükəsizliyi sahəsində siyasətin dəstəklənməsi;

İnformasiya təhlükəsizliyinin təşkili - təşkilatda informasiya təhlükəsizliyi sisteminin iş qabiliyyətini təmin edəcək təşkilati strukturun yadradılması;

Resursların idarə edilməsi - informasiya resurslarına onların dəyər dərəcələrinə görə prioritet verilməsi və onlara görə məsuluyyətin paylanması;

Əməkdaşların təhlükəsizliyi - insan səhvləri riskinin, oğurluğun və avadanlığın qeyri-düzgün istifadəsinin azaldılması (əməkdaşların təlimi və insidentlərin izlənməsi);

Fiziki təhlükəsizlik - avtorizə olunmamış girişin və təşkilatın informasiya sisteminin işinin pozulmasının qarşısının alınması;

Kommunikasiyanın və əməliyyatların idarə edilməsi - şəbəkələrin və kompüterlərin təhlükəsiz fəaliyyətinin təmin edilməsi;

Girişin idarə edilməsi - biznes-informasiyaya girişin idarə edilməsi;

Sistemin alınması, yaradılması və sistemə xidmət edilməsi - təşkilatın informasiya sisteminin yaradılması və ya inkişafı zamanı informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsi, tətbiqi proqramların və verilənlərin təhlükəsizliyinin dəstəklənməsi;

İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi;

Təşkilatın fasiləsiz fəaliyyətinin idarə edilməasi - fövqəladə hallarda təşkilatın fasiləsiz işinin təmin edilməsi üçün fəaliyyət planı;

Qanunvericiliyin tələblərinə uyğunluq - müvafiq mülki və cinayət qanunvericiliyinin, müəllif hüquqları və informasiyanın mühafizəsi qanunları daxil olmaqla, tələblərinin yerinə yetirilməsi.

4.Sadə şifrləmə üsulları. Sezar şifrləməsi

Bizim eranın I əsrində Yuli Sezar senata göndərdiyi məktubları hərfləri əlifbada 3 mövqe sürüşdürmə yolu ilə şifrləyirdi. Belə ki, bu zaman mətnin hər bir hərfi əlifbada ondan sonra üçüncü mövqedə duran hərflə əvəz olunurdu. Əgər hərf əlifbanın sonunda yerləşirdisə və ondan sonra üç hərf yox idisə, onda dairəvi prinsiplə əlifbanın əvvəlinə keçir və sıranın növbəti hərfləri kimi oradakı hərflərdən istifadə olunurdu. Aydındır ki, şifr əvəzetmə üsulları sinfinə daxildir.

Şifrin açarı: əlifba və sürüşmə.

Məsələn, latın əlifbası üçün Sezar “VENİ VEDİ VİCİ” (Gəldim, gördüm, qalib gəldim) ifadəsini əlifbada 3 hərf sağa sürüşdürməklə “YHQL YHGL YLFL” kimi şifrləmişdi.

Beləliklə, Sezarın sadə əvəzetmə cədvəlini aşağıdakı kimi təxvir etmək olar:

İlkin mətnin hərfləri

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Eramızın I əsrində imperator Avqust şifrləmə üçün mətnin hərflərini əlifbada növbəti hərflə əvəz edirdi: İlkin mətnin hərfləri

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Şifrmətnin hərfləri. *Sütunların (sətirlərin) transpozisiyası.* Məlumatın şifrlənməsi üçün hərflərinin yerdəyişməsi üçün sadə *MxN* ölçülü şifrləmə cədvəlindən istifadə edilir. Burada *M* – cədvəlin sətirlərinin sayı, *N* isə sütunlarının sayıdır. Şifrləmə üçün məlumat cədvəlin içərisinə sətirlərlə (və ya sütunlarla) yazılır və sütunlarla (və ya sətirlərlə) oxuyurlar. Beləliklə, ilkin məlumatın hərfləri yerlərini dəyişmiş olur.

Şifrləmənin açarı: cədvəlin ölçüsü.

Məsələn, “MƏLUMATIN SADƏ ŞİFRLƏNMƏSİ” cümləsini 4x6 ölçülü cədvəl vasitəsilə aşağıdakı kimi şifrləmə olar. Məlumat cədvələ sətirlərlə yazılır:

M	Ə	L	U	M	A
T	I	N	S	A	D
Ə	Ş	İ	F	R	L
Ə	N	M	Ə	S	İ

Belə cədvəldə yazılmış məlumatı sütunlarla oxuduqdan “MTƏƏƏIŞNLNİMUSFƏMARSADLİ” şifri alınar.

5.Sadə şifrləmə üsulları. Yerdəyişmə üsulu

Açara görə sətirlərin (və ya sütunların) yerdəyişməsi. Şifrləmə üçün *MxN* ölçülü cədvəl və *M* və ya *N* simvolu açar söz tələb olunur. Belə ki, əvvəlcə məlumat cədvələ yazılır. Cədvəlin üstündən (və ya qarşısından) *M* (və ya *N*) hərfli açar söz yazılır. Açar sözün hərfləri əlifbada rastgəlinmə ardıcıllığına uyğun olaraq nömrələnir. Əgər açar sözdfə hər hansı hərf birdən artıq sayda olarsa, onda onlar sözdə rastgəlinmə ardıcıllığına görə nömrələnir. Bundan sonra açar sözün hərfləri onların nömrələrinə görə düzülür və uyğun sütunların (sətirlərin) yerləri də müvafiq qaydada dəyişdirilir. Bu zaman məlumat cədvələ sətirlər və ya sütunlar üzrə doldurula bilər.

Şifrləmənin açarı: cədvəlin ölçüsü və açar söz.

Məsələn, 8-ci nümunədəki cədvəl və mətni, eləcə də "QARTAL" açar sözünü götürək. Qeyd olunmalıdır ki, açar sözlərinin hərflərinin sayı (*N=6*) cədvəlin sütunlarının sayına bərabər olduğuna görə şifrləmə zamanı cədvəlin sütunlarının yerdəyişməsindən istifadə olunacaq.

Birinci addımda məlumat sütunlarla cədvələ doldurulur, açar söz cədvəlin yuxarısında yazılır və onun hərfləri nömrələnir:

Açar söz	Q	A	R	T	A	L
Hərflərin nömrəsi	3	1	5	6	2	4
Şifrlənən məlumat	M	M	N	Ə	R	M
	Ə	A	S	Ş	L	Ə
	L	T	A	İ	Ə	S
	U	I	D	F	M	İ

İkinci addımda açar sözün hərflərinin nömrələrinə uyğun olaraq cədvəlin sütunlarının yerləri dəyişdirirlir:

Açar söz	A	A	Q	L	R	T
Hərflərin nömrəsi	1	2	3	4	5	6
Şifrlənən məlumat	M	R	M	M	N	Ə
	A	L	Ə	Ə	S	Ş
	T	Ə	L	S	A	İ
	I	M	U	İ	D	F

Üçüncü addımda dəyişdirilmiş cədvəldən sətirlər üzrə hərflər k=öçürülür və şifr mətn alınır:

"MRMMNƏALƏƏSÇTƏLSAİIMUİDF" .

Eyni məlumatın şifrlənməsini sətirlərin yerdəyişməsinə görə də yerinə yetirnək olar. Tutaq ki, "ŞİFR" açar sözdür. Birinci addımda

Açar söz	Hərflərin nömrələri	Şifrlənən məlumat					
Ş	4	M	Ə	L	U	M	A
İ	2	T	I	N	S	A	D
F	1	Ə	Ş	İ	F	R	L
R	3	Ə	N	M	Ə	S	İ

cədvəli tərtib olunur. İkinci addımda cədvəl şəklini alır. Üçüncü addımda cədvəldən hərflər sütunlar üzrə oxunduqda aşağıdakı şifr alınar:

Açar söz	Hərflərin nömrələri	Şifrlənən məlumat					
F	1	Ə	Ş	İ	F	R	L
İ	2	T	I	N	S	A	D
R	3	Ə	N	M	Ə	S	İ
Ş	4	M	Ə	L	U	M	A

"ƏTƏMŞINƏİNMLFSƏURASMLDİA".

Sətir və sütunların ikiqat yerdəyişməsi. Burada məlumat cədvələ doldurulduqdan sonra əvvəlki nümunədə göstərilən hər iki (sətrə və sütuna görə) yerdəyişmə ardıcıl tətbiq olunur. Sətrə və sütuna görə yerdəyişmənin ardıcıllığının fərqi yoxdur.

Şifrləmənin açarı: cədvəlin ölçüsü və iki ədəd açar söz.

Məsələn, əvvəlki nümunədəki məlumatı, açar sözləri götürək. Məlumatı sütunlar üzrə yazaraq həmin ölçüdə cədvələ aqşağıdakı kimi tərtib edək:

		Q	A	R	T	A	L
		3	1	5	6	2	4
Ş	4	M	M	N	Ə	R	M
İ	2	Ə	A	S	Ş	L	Ə
F	3	L	T	A	İ	Ə	S
R	1	İ	I	D	F	M	İ

Birinci mərhələdə birinci açar sözə görə sütunların yerdəyişməsi aparılır:

		A	A	Q	L	R	T
		1	2	3	4	5	6
Ş	4	M	R	M	M	N	Ə
İ	2	A	L	Ə	Ə	S	Ş
F	3	T	Ə	L	S	A	İ
R	1	I	M	U	İ	D	F

Ikinci mərhələdə ikinci açar sözə görə sətirlərin yerdəyişməsi həyata keçirilir:

		A	A	Q	L	R	T
		1	2	3	4	5	6
F	1	T	Ə	L	S	A	İ
İ	2	A	L	Ə	Ə	S	Ş
R	3	I	M	U	İ	D	F
Ş	4	M	R	M	M	N	Ə

Üçüncü mərhələdə cədvəldən hərflər sətirlər üzrə oxunur və aşağıdakı şifrmətn alılnır:

“TƏLSAİALƏƏSŞIMUİDFMRMMNƏ”

5.13.12. Sehrli kvadrat. Sehrli kvadrat dedikdə xanalarında 1-dən 9-a, 16-ya, 25-ə və s. qədər ədədlər yazılmış elə 3, 4, 5 və s. ölçülü kvadrat cədvəllər nəzərdə tutulur ki, həmin kvadratın sətir, sütun və diaqonalları üzrə xanalarda yazılmış ədədlərin cəmi bərabər olsun.

Məsələn, 5x5 ölçülü cədvəldə 1-dən 25-ə qədər olan ədədləri aşağıdakı kimi yazmaq olar:

11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Bi cədvəldə bütün sətirlər, sütunlar və dioqanallar üzrə ədədlərin cəmi 65-ə bərabərdir.

Şifrləmə üçün ilkin mətndə olan hərflər sıra nömrəsinə uyğun olaraq, kvadratdakı ədədlərin yanında yazılır, sonra isə kvadratın sətirləri və ya sütunları üzrə oxunur.

Şifrləmə açarı: sehrli kvadratın ölçüsü və ədədlərin düzülüşü.

Məsələn: “ÜSUL SEHRLİ KVADRAT ŞİFRİDİR” mətninin sehrli kvadrat şifrinin köməyi ilə şifrlənməsinə baxaq. Əvvəlcə mətnin hərfləri nömrələnir:

Ü	S	U	L	S	E	H	R	L	İ	K	V	A
1	2	3	4	5	6	7	8	9	10	11	12	13

D	R	A	T	Ş	İ	F	R	İ	D	İ	R
14	15	16	17	18	19	20	21	22	23	24	25

Mətnin hərfləri 5x5 ölçülü sehrli kvadrata yazılır:

11 K	24 İ	7 H	20 F	3 U
4 L	12 V	25 R	8 R	16 A
17 T	5 S	13 A	21 R	9 L
10 İ	18 Ş	1 Ü	14 D	22 İ
23 D	6 E	19 İ	2 S	15 R

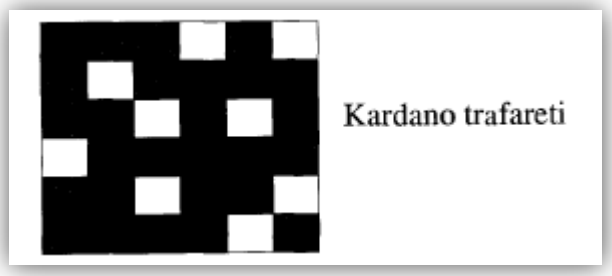
Sonda sehrli kvadratın xanalarında olan hərlər sütunlar üzrə köçürülür və “KLTİDİVSŞEHRAÜİFRRDSULİR” şifri alınır.

6.Sadə şifrləmə üsulları. Kardonanın sehirli kvadratı

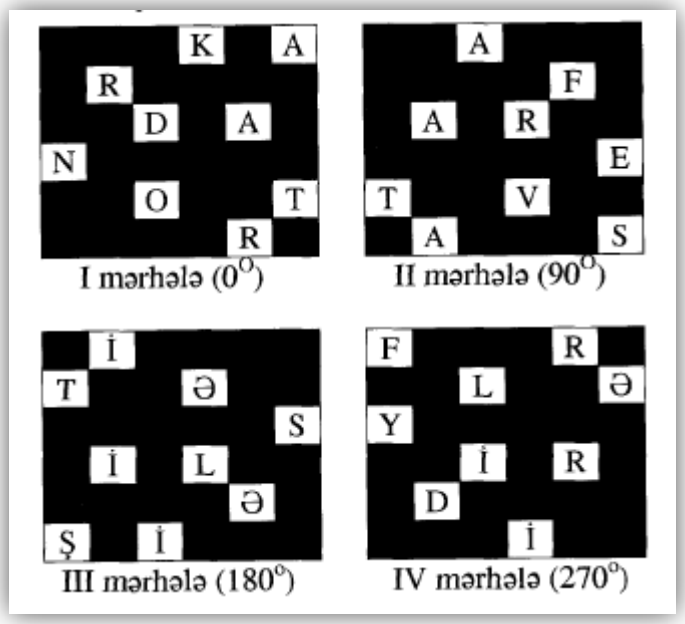
Kardano kvadratı - sətir və sütunlarının sayı cüt olan kvadrat cədvəldir. Onun xanalarının dörddəbiri (25%) elə şəkildə kəsilin çıxarılır ki, belə kvadratı dörd dəfə 90° fırlatmaqla ilkin kvadratın bütün xanalarını örtmək mümkün olsun. Xanaları kəsilmiş kvadrat *trafaret* və ya *qəfəs* adlanır. Şifrləmə üçün trafaret kvadratın üzərinə qoyulur və mətnin hərfləri sətirlər üzrə kəsik xanalara yazılır və növbəti hərflər kəsik xanalara yazılır. Bu proses kvadratın bütün xanaları dolanadək davam etdirilir.

Şifrin açarı:kvadratın ölçüsü və trafaret.

Tutaq ki, "KARDANO TRAFARET VASİTƏSİLƏ ŞİFRLƏYİRDİ" mətni verilmişdir. Aşağıdakı şəkildə trafaret götürək.



Bu trafaretin kəsilmiş xanalarında sətirlər üzrə yazıb 90° fırlatmaqla dörd mərhələdə ilkin kvadrat doldururlur.



Nəticədə kvadrat aşağıdakı şəkildə doldurulmuş olur:

F	İ	A	K	R	A
T	R	L	Ə	F	Ə
Y	A	D	R	A	S
N	İ	İ	L	R	E
T	D	O	V	Ə	T
Ş	A	İ	İ	R	S

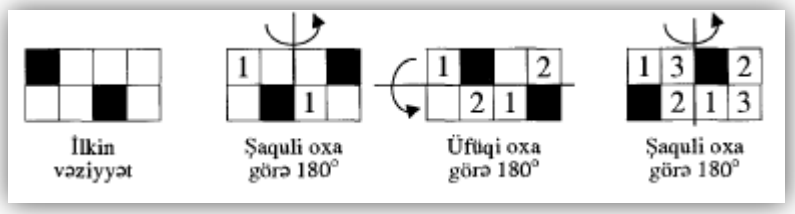
və hərflər kvadratdan sətirlərlə oxunmaqla

"FİAKRATRLƏFƏYADRASNİİLRETDOVƏTŞAİİRS"

şifrmətni alınar.

Bu üsulda 90° fırlatma əvəzinə üfüqi və şaquli oxlara görə 180° çevirmədən istifadə oluna bilər.

Bu üsulda, həmçinin, kvadrat əvəzinə düzbucaqlı cədvəldən istifadə etmək olar, lakin bu zaman yalnız 180° çevirmələ tətbiq edilə bilər. Məsələn, əvvəlcə şaquli oxa görə çevirmə, sonra üfüqi oxa görə çevirmə, yenidən şaquli oxa görə çevirmə. Əyani nümayiş etdirmək üçün 2x4 ölçülü düzbucaqlı cədvəlin çevrilməsinə baxaq.



7. Sadə şifrləmə üsulları. İkiqat biqram cədvəli

1854-cü ildə Ç. Uinston tərəfindən təklif olunmuşdur. bu üsul əvvəlki bənddəki üsula oxşarlıq təşkil edir. Bu üsul əvvəlki bənddəki üsula oxşarlıq təşkil edir. Lakin burada bir cədvəl əvəzinə əlifbanın hərfləri ilə təsadüfi qaydada doldurulmuş iki cədvəldən istifadə olunur. Şifrləmə üçün ilkin biqramın hərflərinin biri birinci cədvəldən, digəri isə ikinci cədvəldən götürülür. Onların əsasında da elə düzbucaqlı qurulur ki, biqramın hərfləri onun diaqonalboyu qarşılıqlı təpələrində yerləşmiş olsun. Bu düzbucaqlının digər iki təpəsində yerləşən hərflər şifrlənmiş biqramı əmələ gətirir.

Əgər biqramın hər iki hərfi eyni sətirdə yerləşərsə, onda şifrmətnin biqramı aşağıdakı kimi tapılır. Şifrmətnin biqramının birinci hərfi ikinci cədvəlin həmin sətrindən götürülür. Sütun nömrəsi isə ilkin biqramın birinci hərfinin birinci cədvəldə yerləşdiyi sütunun nömrəsi qəbul edilir. Şifrmətnin biqramının ikinci hərfi isə birinci cədvəlin həmin sətrindən götürülür. Sütun nömrəsi ilkin biqramın ikinci hərfinin ikinci cədvəldə yerləşdiyi sütunun nömrəsi ilə müəyyən edilir.

Şifrin açarı: əlifbanın hərfləri ilə təsadüfi qaydada doldurulmuş iki cədvəl.

Tutaq ki, 8x4 ölçüdə iki cədvəl verilmişdir və onlar Azərbaycan əlifbasının hərfləri ilə təsadüfi qaydada doldurulmuşdur:

Ğ	S	D	J				Ə	M	Ç	H
Q	A	P	G				B	Ö	S	İ
I	T	O	C				K	X	U	N
Y	E	L	Ü				R	J	Y	E
N	Z	B	R				P	Ğ	F	Q
Ş	İ	V	X				U	C	I	T
Ç	U	K	Ə				D	O	Ş	G
F	Ö	H	M				L	Z	A	V

Nümunə qismində 19-cu bənddəki misala baxaq: “OBYEKT YERİNDƏDİR” məlumatının şifrlənməsi üçün onu biqramlara bölür və şifrləyirlər. Qeyd olunan qaydalara uyğun olaraq “OB” biqramı “KP”, “YE” biqramı “RÜ” və s. şifrlənmiş biqrama çevrilir. Beləliklə, verilmiş məlumat aşağıdakı kimi şifrlənmiş olar:

OB	YE	KT	YE	Rİ	ND	ƏD	İR
KP	RÜ	GV	RÜ	QG	PÇ	GÇ	UE

Nəticədə “KPRÜGVRÜOGPÇGÇUE” şifrmətni alınar.

8.Sadə şifrləmə üsulları. Qoşa şifr

Əvəzetmə cədvəlini düzəltmək üçün burada 16 hərfdən az olmayaraq (əlifbanın hərflərinin yarısından az olmayaraq) uzunluğa malik açar ifadə götürülür. Bu ifadə bir sətirdə yazılır, onun hərflərinin altından əlifbanın bu ifadəyə olmayan hərfləri ardıcıl şəkildə yazılır: Məsələn, “SABAHKI REYS GÖZLƏNİLİR”.

S	A	B	A	H	K	I	R	E	Y	S	G	Ö	Z	L	Ə	N	İ	L	İ	R
1	2	3		4	5	6	7	8	9		10	11	12	13	14	15	16			
C	Ç	D		F	Ğ	X	J	Q	M		O	P	Ş	T	U	Ü	V			

Beləliklə, aşağıdakı əvəzetmə cədvəli alınır:

A	B	C	Ç	D	E	Ə	F	G	Ğ	H	X	I	İ	J	K
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Ç	D	S	A	B	Q	U	H	O	K	F	I	X	V	R	Ğ

Q	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	T	Y	Ü	G	P	Ö	J	C	Z	L	Ə	N	İ	M	Ş

Şifrin açarı: açar ifadə. Belə qurulmuş şifrləmə cədvəlinə əsasən “UÇUŞ TƏXİRƏ SALINDI” məlumatı “ƏAƏZ LUIVJU CÇTXÖBX” kimi şifrlənər.