DOI: https://doi.org/10.36719/2789-6919/44/218-225

Rəhimə Rüstəmova
Azərbaycan Dövlət Pedaqoji Universitetinin Şəki filialı
magistrant
https://orcid.org/0009-0008-8033-4532
rr.rahima99@gmail.com

İnformasiya təhlükəsizliyinin təmin edilməsi üsulları: informasiyanın kodlaşdırılması və kompüterin yaddaşında təsviri

Xülasə

İnformasiyanın mövcudluq vahidi kimi təzahür etdiyi müasir qlobal cəmiyyətdə təhlükəsiz həyatın təmin edilməsi ekzistensial xarakter kəsb edən aktual məsələyə və hətta problemə çevrilmişdir. Yüksək zəmanətli təhlükəsiz həyatın təşkil edilməsində ən mühüm vəzifələrdən biri də lokal və qlobal miqyasda informasiya təhlükəsizliyini etibarlı şəkildə nəzarətə götürməkdir. Hazırda informasiya məkanının qorunması və informasiya təhlükəsizliyinin təmin edilməsi üçün müasir dünya elminin möhtəşəm nailiyyətləri sayılan innovasiyalardan, informasiya sektoruna nou-haular kimi daxil olmuş qabaqcıl texnologiyalardan və onları idarə edən mütəxəssislərin xidmətindən istifadə olunur. Lakin bütün bunlar informasiya təhlükəsizliyini mütləq şəkildə təmin etmək üçün kifayət deyil. Odur ki, texniki innovasiyalar sahəsində çalışan tədqiqatçı alimlər informasiya təhlükəsizliyinin təmin edilməsilə bağlı mövcud resursların daha da təkmilləşdirilməsi və modernləşdirilməsi, supermüasir rəqəmsal avadanlıqların və elektron qurğuların yaradılması istiqamətində böyük işlər görürlər. Sözügedən sahədə həyata keçirilən tədbirlər sırasında informasiyanın kodlaşdırılması kimi vacib prosesin əhəmiyyətini də qeyd etmək lazımdır. Təqdim olunan məqalədə məhz kompüterlərdə müxtəlif növ informasiyaların kodlaşdırılması mexanizmlərindən, bu prosesin başlıca məqsədlərindən, həmçinin kodlaşdırma standartlarının məzmunundan, iş rejimindən və təyinatından bəhs olunur. Bu sahədə yeni-yeni kəşflərin, ixtiraların və yeniliklərin edilməsi və mövcud sistemlərin durmadan təkmilləşdirilməsi dayanıqlı inkişaf üçün zəruri olan informasiya təhlükəsizliyinin təminatı vasitəsi kimi ön plana çəkilir.

Açar sözlər: *informasiya, informasiya təhlükəsizliyi, kodlaşdırma, təhlükəsizlik, təminat, kod, Universal kod, ikili kod, qrafik informasiya*

Rahima Rustamova
Sheki branch of Azerbaijan State Pedagogical University
Master student
https://orcid.org/0009-0008-8033-4532
rr.rahima99@gmail.com

Methods of Ensuring Information Security: Encoding of Information and Representation in Computer Memory

Abstract

In the modern global society, where information is a certain unit of sustainable existence, reliable provision of a safe life, which has existentiality in itself, acquires not only the character of a pressing issue, but also a serious problem. In ensuring a highly guaranteed safe life, one of the most important tasks is to take reliable control of information security on a local and global scale. Today, the greatest achievements of world science are used to reliably protect the information space and ensure information security -so-called innovations, advanced technologies that are included in the information technology sector as know-how, as well as the services of specialists managing these technologies. However, all this is not enough to ensure absolute information security.

Therefore, research scientists actively engaged in technical innovations, in connection with reliable information security, carry out important tasks to improve and modernize existing resources for the creation of electronic devices and ultra-modern digital equipment. Among the activities carried out in this area, it is necessary to emphasize the importance of information coding. The presented article tells about the mechanisms of coding information of various types, about the main goals of this process, as well as about the content, about the working mode and purpose of coding standards. All new discoveries, inventions, innovations in this area and continuous improvement of existing information security systems as necessary means for sustainable development are brought to the forefront.

Keywords: *information, information security, graphic information, provision, code, dual code, coding, Universal code*

Giriş

Müasir informasiya texnologiyaları sahəsində ən mühüm və həyati əhəmiyyət kəsb edən məsələlərdən biri də informasiya təhlükəsizliyidir. İnformasiya təhlükəsizliyi (ing. *İnformation Security* və ya qısaca *İnfoSek*) -İnternetdə yerləşən informasiyalar anbarına, verilənlər bazasına və istifadəçinin şəxsi səhifəsinə sanksiyasız daxilolmaların və həmin yerləşən informasiyaları icazəsiz əldə etmələrin, onlardan istifadə etmələrin, onları təhrif etmələrin, yaxud məhv etmələrin qarşısını almaq üçün praktiki tədbirlərin külliyatıdır. İnformasiya təhlükəsizliyinin qarşısında duran əsas vəzifə verilənlərinin bütövlüyünün, konfidensiallığının və əlçatan olmasının qorunmasıdır. Bu sahədə gözlənilən nəticələri əldə etmək üçün real və potensial risklərin idarə oluunması başlıca şərt sayılır. Bu zaman təhlükə mənbələri və sistemin zəif yerləri aşkar edilir və dərhal müvafiq tədbirlər görülür (Kissel, 2013, s. 94).

Son dövrlərdə informasiya-kommunikasiya texnologiyalarının intensiv inkişafı və müasir texniki vasitələrin cəmiyyət həyatının bütün sahələrinə nüfuz etməsi ilə əlaqədar informasiya təhlükəsizliyinin təminatı məsələsi fövqəladə şəkildə aktuallaşmışdır. Məhz bu səbəblərdən sözügedən sahədə ən müasir texnologiyaların inkişafı və tətbiqi intensiv templərlə baş verir və informasiya təhlükəsizliyinin təmin edilməsi vəzifəsini öz üzərinə götürən çox sayda professional ixtisaslar, sahələr və xidmətlər meydana gəlir və inkişaf edir. Məsələn, şəbəkə təhlükəsizliyi ixtisası, informasiya infrastrukturunun qorunması üzrə xidmət, verilənlər bankının, məlumat anbarının və verilənlər bazasının mühafizəsi xidməti, müasir informasiya sisteminin auditi və elektron qeydiyyatların aşkar edilməsi sistemi, rəqəmsal kompüter kriminalistikası və ya forenzika (lat. *Foren*-forum qarşısında nitq-kompüter məlumatları ilə bağlı cinayətlərin açılması üzrə xüsusi fəaliyyət növü). İngilis dilində "foren science" (məhkəmə elmi və yaxud kriminalistika) ifadəsinin qısa forması olan "forenzika" dedikdə "kompüter kriminalistikası" başa düşülür (Garfinkel, 2010, s. 65). Hazırda informasiya təhlükəsizliyi sahəsində çalışan professionallara əmək bazarında çox böyük ehtiyac var. 2022-ci ildə bu sahə ilə əlaqədar aparılan sorğular və proqnozlar nəticəsində belə məlum olmuşdur ki, dünya üzrə bu sahədə 2 milyon yüksək ixtisaslı mütəxəssisə ehtiyac var.

Tədqiqat

İnformasiya təhlükəsizliyinin təmin edilməsi davamlı və dayanıqlı inkişafa zəmanət verən amil kimi. Bu gün informasiya təhlükəsizliyi sahəsində çox sayda müəyyənliklər var və onların hər biri konkret sahənin və yaxud istiqamətin xarakterini təyin edir: qorunan informasiya (normativ hüquqi aktlara, informasiya sahibinin müəyyən etdiyi tələblərə uyğun qoruma altında olan məlumat), informasiya sahibi (müstəqil şəkildə məlumatlar yaratmış, yaxud qanunlar və müqavilələr əsasında məlumatlara girişi məhdudlaşdıran şəxs, informasiya sahibi ayrı-ayrı subyektlər, dövlət, hüquqi və fiziki şəxs, yaxud şəxslər qrupu ola bilər), informasiya təhlükəsizliyi (mühafizə rejimində olan, konfidensiallığı və bütövlüyü etibarlı şəkildə qorunan, əlçatan olması ciddi şəkildə nəzarət altında olan informasiya), məlumat mühafizəsinin təşkili (informasiyanın təhlükəsizliyi üçün təhdidlər yaradan elementlərin aşkara çıxarılmasına, aradan qaldırılmasına və qəti ləğvinə istiqamətlənmiş hərəkətlərin külliyatı, həmçinin informasiyanın mühafizəsi və onun vəziyyətinə fasiləsiz nəzarət üzrə planlaşdırma və reallaşdırma işləri), informasiyanın mühafizəsi sistemi (informasiyanın mühafizəsini təmin edən orqanların, icraçıların, eləcə də onların istifadə etdiyi texnikanın və mühafizə etdikləri obyektlərin

külliyyatı) və informasiya təhlükəsizliyinin qorunması siyasəti (informasiya təhlükəsizliyi sahəsində rəsmi şəkildə sənədləşdirilmiş qaydaların, prosedurların, praktiki üsulların və idarəçilik prinsiplərinin külliyatı) (Keyser, 2018).

Yuxarıda qeyd edildiyi kimi informasiya təhlükəsizliyinin yüksək səviyyədə təmin edilməsi 3 təmələ söykənir. İngilisdilli mənbələrdə bu "Triad SIA" (ing. *Confidentiality, Integrity and Availability*) adlanır. "Məxfilik, Bütövlük və Əlçatanlıq" kimi xarakterizə olunan "SİA triadası" informasiya təhlükəsizliyinin etibarlı şəkildə təmin olunması üzrə korporativ infrastrukturun əsaslarını təşkil edir. Qeyd edək ki, informasiya təhlükəsizliyi haqqında ilk müddəalar XX yüzilliyin 70-ci illərində meydana gəlmişdir. 1975-ci ildə kompüter elmləri sahəsində tanınmış ABŞ mütəxəssisi *Maykl Şröder* (1945) "Kompüter sistemlərində informasiyanın mühafizəsi" adlı elmi məqaləsində, ilk dəfə olaraq, informasiya təhlükəsizliyi ilə bağlı pozuntuları 3 növə ayırmışdı: 1. İnformasiyanın müəllifin icazəsi və iştirakı olmadan açılması (ing. *unauthorized information release*). 2. İnformasiyanın müəllifin əvvəlcədən icazəsi və iştirakı olmadan dəyişdirilməsi (ing. *unauthorized information modification*). 3. İnformasiyanın müəllifinin iştirakı və icazəsi olmadan onlara daxil olmalara imtina verilməsi (ing. *Unauthorized denial of use*) (Barr, Ronen, 2018).

Qeyd etmək lazımdır ki, sonralar bu kateqoriyalar qısa və standart adlar almışdır: *Confidentiality* (məxfilik-kimliyi məlum olmayan şəxslər üçün əlçatmaz və yaxud qapalı olan informasiyanın xassəsi), *Integrity* (bütövlük-aktivlərin düzgün və bütöv saxlanması xassəsi), *Availability* (əlçatanlıq-kimliyi məlum olan və informasiyaya daxil olmaq hüququna sahib olan subyektlərin sorğusu ilə informasiyanın əlçatan və istifadəyə hazır olması xassəsi). 1992-ci ildə dünyada cərəyan edən sosial-iqtisadi və ictimai-siyasi proseslərin fonunda "İqtisadi inkişaf və əməkdaşlıq təşkilatının" (ing. *Organisation for Economic Cooperation and Development, OECD*-müstəqil bazar iqtisadiyyatını və nümayəndəli demokratik prinsipləri tam şəkildə qəbul edən inkişaf etmiş dünya dövlətlərinin beynəlxalq iqtisadi təşkilatı, 1948-ci ildə "*Avropa İqtisadi Əməkdalıq Təşkilatı*", AİƏT, ing. *Organisation for European Economic Cooperation, OEEC*-təşkil edilmişdir, mənzil-qərargahı Parisdə yerləşir) nəşr etdirdiyi məqalədə məlumat təhlükəsizliyinin keyfiyyətcə yeni modeli təqdim edildi. "SİA triadası"ndan fərqli olaraq bu modeldə 3 deyil, 10 prinsip əks olunmuşdu: məlumatlılıq; məsuliyyət; etika; demokratiya; riskin qiymətləndirilməsi; təhlükəsizlik tədbirlərinin hazırlanması və tətbiqi; təhülkəsizliyin idarə olunması; vəziyyətə təkrar baxılması. Bu modelin əsasında (ing. *The National Institute of Standards and Technology, NIST, USA-Standartlar və Texnologiyalar Milli İnstitutu, STMİ*) 2004-cü ildə 33 prinsipdən ibarət informasiya təhlükəsizliyi sisteminin mühəndis layihəsi dərc olundu. Həmin layihədə hər bir prinsip üçün praktiki rəhbərlik təlimatı və məsləhətlər hazırlandı. 1998-ci ildə isə İT sahəsində tanınmış ABŞ mütəxəssisi Donn Parker (1929-2021) "SİA triadası"na daha üç mühüm aspekt əlavə etdi: 1. Sahiblik və nəzarət (ing. *Possession or Control*). 2. Həqiqilik (ing. *Authenticity*). 3. Faydalılıq (ing. *Utility*). "Parker heksadası" (ing. *hexad* -6 predmetdən ibarət qrup) adı almış yeni təklif bu gün də mübahisə obyekti olaraq qalır (Hintzbergen, Hintzbergen, Baars, Smulders, 2010, s. 13). Bu və ya digər modelin təklif edilməsinə baxmayaraq, "SİA triadası" bu gün də ən çox yayılmış modeldir.

İnformasiya təhlükəsizliyi sisteminin təsvirinə sistemli yanaşma onun əsas element və komponentlərini aşkar etməyə və müvafiq qaydada sinifləşdirməyə adekvat imkanlar yaradır: 1. Qanunvericilik, normativ-hüquqi və elmi baza. 2. İT təhlükəsizliyini təmin edən orqan və bölmələrin strukturu və vəzifələri. 3.Təşkilati-texniki və rejim tədbirləri, yaxud metodları (İnformasiya təhlükəsizliyi siyasəti). 4. Proqram-texniki üsullar və İT-ni təmin edən vasitələr. Yuxarıda qeyd edilən müddəaları ümumiləşdirərək informasiya təhlükəsizliyi sisteminin başlıca məqsədlərini müəyyən etmək mümkündür: -verilənlərin konfidensiallığını təmin etmək; -informasiya sistemində verilənlər bazasına giriş hüququ olan istifadəçilər üçün müvafiq informasiyanı əlçatan etmək; -informasiyanın bütövlüyünü təmin etmək, məlumatların qeyri-qanuni dəyişdirilməsinə qarşı tədbirlər görmək; -informasiyanın həqiqiliyini və dəqiqliyini təmin etmək; -informasiyanın mənbəyini və müəllifini müəyyən etmək.

Ümumi cizgilərdə informasiya təhlükəsizliyi sisteminin əsas məqsədi verilənləri daxili və xarici təhdidlərdən və real təhlükədən qorumaqdır. İnformasiya sistemində mütləq şəkildə konfidensiallığı (məxfiliyi) təmin etmək üçün bütün formatlarda olan informasiyalar üçün aktual olan 4 metoddan istifadə olunur: -informasiyalara girişi qapamaq və məhdudlaşdırmaq; -informasiyaları şifrələmək; -

informasiyanı hissələrə ayırmaq və mühafizə etmək; -informasiyanın mövcudluğu faktını gizli saxlamaq.

Hazırda həm qlobal, həm də lokal şəbəkələrdə informasiyaların bütövlüyünü və təhlükəsizliyini təhdid altına alan çox sayda mənbə mövcuddur; -texnogen mənbələr; -texniki təminatla bağlı təhlükələr; -antropogen mənbələr -insan amili (məqsədyönlü hərəkətlər və təsadüfi səhvlər) ilə bağlı təhlükələr; -kortəbii mənbələr; -proqnozlara rəğmən yaranan vəziyyət.

Bu gün beynəlxalq səviyyədə informasiya təhlükəsizliyini yüksək səviyyədə təmin etmək üçün bəzi standartlardan istifadə olunur. Onların daha populyar olanları aşağıda qeyd edilmişdir: 1. BS7799-11:2004 - informasiya təhlükəsizliyinin idarə edilməsi üzrə B. Britaniya standartı (ing. *Code of Practice for Information Security Management* -İnformasiya Təhlükəsizliyinə nəzarət edilməsi üzrə 127 mexanizm təsvir edir [Solms, 1998, s. 224]. 2. ISO/IEC17799:2005 -İT üzrə menecmentin praktiki qaydaları. 3. ISO/IEC27001 -İT üzrə idarəçilik sistemi. 4. ISO/IEC27002 -İT üzrə menecmentin praktiki qaydaları (2007).

Kompüterdə informasiyanın kodlaşdırılması mexanizmləri. Kodlaşdırma standartlarının məqsədləri və təyinatı. Kompüter texnikasında icra olunan vacib funksiyalardan biri də informasiyaların kodlaşdırılmasıdır. İnformasiyanın kodlaşdırılması (ing. *Encoding Information, EI*) -gərəkli olan informasiyaların bir formadan digərinə transformasiya olunması aktıdır. Bu akt informasiya emalını, saxlanmasını, ötürülməsini və istifadəsini asanlaşdırmaq üçün onların daha rahat və məqsədəuyğun şəklə salınmasını nəzərdə tutur. Beləliklə, praktiki mətnlərin yaradılması istifadəçiyə informasiyaları daha dərindən öyrənməyə imkan yaradır (Karpicke, 2012, s. 158).

Müasir informasiya texnologiyaları sahəsində müvafiq məlmatları kodlaşdırmaq üçün çoxlu sayda fərqli sistemlərdən (məsələn, verilənlərin müəyyən kodlar şəklində qeydiyyatını təmin edən qanunauyğunluqlar və qaydalar kompleksi) istifadə olunur. Bir qayda olaraq, kodlaşdırma prosedurları kodların (lat. *codex* -kötük və yaxud yazı üçün taxta lövhə) vasitəsilə həyata keçirlir (Rawson, Zamary, 2019). Ümumi anlamda "kod" müəyyən əlifbaya aid çoxlu sayda nizamlı simvolların olması tələb olunmayan başqa formalarda qarşılıqlı eynimənalı şəkildə əks olunmasıdır. Adətən, kodlardan informasiya texnologiyaları sahəsində hər hansı məlumatın ötürülməsi və saxlanması zamanı istifadə olunur. Beləliklə, informasiya texnologiyası sahəsində "kod" dedikdə xüsusi işarələr sistemi və simvollar baş düşülür. Onların müxtəlif kombinasiyaları sayəsində informasiyanın obrazının dəyişdirilməsi, "kodlaşdırma" (ing. *coding*), informasiyanın şifrədən çıxarılması "koddan çıxarma" (ing. *decoding*) adlanır [Eadie, Robin, 2013].

Bu gün hesablama texnologiyasında ikili koddan (ing. *binary code*) (Olupona, 2014, s. 45) geniş istifadə edilir. İkili kod -verilənlərin kod şəklində elə təqdimatıdır ki, orada hər sıra və yaxud bölmə rəqəmlərlə (0 və 1) müəyyən olunmuş iki mümkün ədəddən birini qəbul edir. Bu zaman sıralar və ya bölmələr ikili sıra və yaxud bölmə adlanır. Kodlaşdırma "0" və "1" rəqəmləri ilə müəyyən olunursa, ikili sıranın və ya bölmənin mümkün vəziyyəti keyfiyyət ("1" > "0") və kəmiyyət ("0", "1") nisbətinə malik olur. İkili kod mövqeli və mövqesiz ola bilir. Mövqeli ikili kod hesablamanın (rəqəmlərlə müəyyən etmək üsullarının külliyatı) ikili sisteminin əsaslarını təşkil edir və ondan müasir rəqəmsal texnikada geniş istifadə olunur. İkili kod informasiyanın 2 variant işarədən ("0","1") istifadə etməklə ötürülməsi, saxlanması və təqdim edilməsi versiyasıdır. İnformasiyanın ikili kodlaşdırılması çeşidli uzunluqda kodların vasitəsi ilə həyata keçirilə bilər. Bu zaman kodda olan işarələrin sayı kodlaşdırılması nəzərdə tutulan məlumatın həcmindən asılıdır. İkili kodlaşdırmada prosesi bitlərin vasitəsi ilə həyata keçirilir. Bir bit yalnız iki variantı (0 və yaxud 1) kodlaşdıra bilir. İki bit dörd variantın (01, 10, 00, 11) kodu ola bilir. 3 bit isə 8 variantın (001, 010, 100, 101, 111, 110, 011) kodlaşdırma işini icra edir. Beləliklə, bitlərin sayının artması kodlaşdırma üçün nəzərdə tutulan informasiyanın kod variantlarını da artırır. Bununla da daha çox informasiyanı kodlaşdırmaq mümkün olunur (, Kschischang, 2007, s. 791).

İkili kodun oxunmasında ən asan üsul kod variantlarında sağ tərəfdəki sonuncu rəqəmdən başlayıb sola hərəkət etməkdir (Bender, Beller, 2013). Daha sonra növbəti rəqəmə keçilir. Əgər bu rəqəm birdirsə (1), o zaman iki bir (1) həddində hesablanır (B). Bu proses sıralarda sonuncu sol rəqəmə çatana qədər davam etdirilir. Prosesi başa çatdırmaq üçün bütün rəqəmlər toplanılır və ikili kodun (rəqəmlərin) ümumi 10-luq ədədi alınır:

128+64+0+0+8+0+2+0=202

Bu prosesin düstur şəklində ifadəsi aşağıdakı kimi qurulur: 1 x 27, 1 x 26 + 0 x 25 + 0 x 24 + 1 x 23 + 0 x 22 + 1 x 22 + 1 x 21 + 0 x 20 = 20.

Məlumatların kodlaşdırılması kodlaşdırma standartlarına (ing. *coding standard*) (Makkonnell, 2010, s. 63-64) uyğun həyata keçirilir. Kodlaşdırma standartı tərtibatçı qrupunun istifadə etdiyi proqram kodunun baza prinsiplərini təsvir edən qaydaların və müqavilələrin dəstidir. Kodlaşdırma standartının əsas məqsədi istifadəçi tərəfindən proqram kodlarının qəbulunu sadələşdirmək və proqramın oxunması zamanı insanın yaddaşına və onun görmə orqanına düşən fiziki yükü maksimum azaltmaqdır. Müasir informasiya texnologiyalarında 2 cür-qrafik və mətn tipli kodlaşdırılmalara geniş yer ayrılır. Elektron hesablama maşınlarında və yaxud kompüterlərdə mətn ayrı-ayrı simvollardan təşkil olunur. Simvolların sırasına təkcə hərflər (böyük və kiçik, latın və kiril qrafikasının hərfləri) deyil, həm də rəqəmlər və durğu işarələri, xüsusi simvollar (**“=”**, **“(“**, **“&”** və s.) və sözlər arasında boşluqları bildirən işarələr (-) daxildir. Bu cür simvolların məcmusu kompüter dilində “*alphabet*” (əlifba) adlanır. Onun gücü isə simvolların sayı ilə müəyyən olunur. 256 simvoldan ibarət əlifbalarda bütün mühüm simvolları yerləşdirmək mümkündür və orada hər 1 simvolun çəkisi 8 bitə (8 bit isə 1 bayta bərabərdir) bərabərdir. Qeyd edək ki, kompüter mətnində hər simvolun ikili kodu 1 bayt yaddaşı əhatə edir (Bauer, 2000).

Müasir informasiya cəmiyyətində qrafik informasiya mühüm rol oynayır. Qrafik informasiya veb-saytın dizaynından və tərtibatından tutmuş tibbi diaqnostikaya qədər müxtəlif sahələrdə tətbiq edilir. Qrafik informasiyanın kodlaşdırılması prinsiplərinə sahib olmaqla təsvir və şəkillərlə daha effektli işləmək, onların keyfiyyətini qoruyub saxlamaq və tutduqları məkanın həcmini (ölçüləri) minimuma endirmək mümkündür. Qrafik informasiya dedikdə təsvir, çertyoj, foto, kitab şəkilləri, televizorun və yaxud kinozalın ekranındakı təsvirlər və s. başa düşülür. Qrafik informasiyalar həm analoq, həm rəqəmsal formalarda təqdim oluna bilər. Qrafik təsviri parçalara ayırmaq yolu ilə qrafik informasiya analoq şəklindən rəqəmsal şəkilə salınır, bununla da kodlaşdırma prosesi realizə olunur. Bu zaman təsvirlərin məkanda diskretizasiyası (lat. *discretio* -bir-birindən ayırmaq və ya fərqləndirmək) baş verir (Chakravorty, 2018).

Qrafik informasiya həm *rastrom* (lat. *Rastrom*-qazıyıcı, yaxud dırmıq, piksellər toru şəklində təqdim edilən rəngli təsvir), həm də vektor (qrafik obyekt və təsvirlərin kompüter qrafikası vasitəsilə təqdim edilməsi, adətən primitiv olan elementar həndəsi obyektlərin: nöqtələr, xətlər, çevrələr, ellipslər, düzbucaqlılar, splaynlar, Bezye əyrisi, dairələr və başqa riyazi təsvirlərinə əsaslanır) şəklində təqdim oluna bilər. Təsvirlərin rənglərinin kodlaşdırılmasına gəldikdə, o, ayrı-ayrı modellər vasitəsi ilə icra olunur. Göründüyü kimi rastrom təsvir çoxlu sayda nöqtələrdən təşkil edilmişdir. Bu nöqtələr ciddi şəkildə sətirlərdə və sütunlarda yerləşdirilmişdir. Hər bir nöqtənin ekranda öz koordinatları, rəng çaları və parlaqlıq səviyyəsi var. Nöqtələr (piksellər) çox olduqca təsvirin keyfiyyəti də və dəqiqliyi də artır. Vektorlar vasitəsi ilə təsvir olunan bütün obyektlər koordinatların, parametrlərin və atributların külliyatı kimi təqdim olunur. Vektor qrafikası matrisalı təsvir qurğusuna (monitor, mexaniki qurğular, pribterlər və s.) çıxarılmazdan əvvəl rastrom qrafikasına dönüşdürülür və bu əməliyyatlar proqram vasitəsi ilə və yaxud aparatın (videokart) köməyi ilə həyata keçirilir. Lakin vektorlu monitorlar və plotterlər (geniş formatlı məhsulların-çertyojların, küçə reklamlarının, plakatların və posterlərin çapı üçün istifadə olunan printer) üçün vektor formatından rastrom formatına keçilməsi tələb olunmur. Bu qurğularda primitivlər elektron şüanın və ya qələmin yerdəyişmələri üzərində qurulur. Plazma və mayekristal ekranlı müasir televizorlar 640×480 (4:3 nisbətində tərəfləri olan mayekristal televizorlar), 852×480 (16:9 nisbətində tərəfləri olan plazma televizorlar), 1024×768 (həm 4:3, həm də 16:9 nisbətində tərəfləri olan mayekristal və plazma televizorları), 1366×768 (HD Ready-*High-Definition Ready*-çox yüksək aydın hazırlığı olan) və 1920×1080 (Full HD - bütöv şəkildə yüksək aydın hazırlığı olan panel) qətnamələri əsasında işləyir. Hazırda rəngli şəkillər almaq üçün RGB (ing. *Red, Green, Blue*-qırmızı, yaşıl, göy-əsasən informatika sahəsində istifadə edilir,-3 əsas rəngin köməyilə rəng yaradılması və ya rəng kodlaşdırılması, bu model o müddəaya əsaslanır ki, insanın gözü bütün rəngləri üç əsas rəngin cəmi kimi qəbul edir, buna görə də RGB modelini həm də additiv və yaxud toplayan model adlandırırlar, bu sxemdə rəngin 1 pikselini kodlaşdırmaq üçün 3 bayt və ya 24 bit

tələb olunur, rəngli qrafikanın bu növü üç rəngli-ing. *True Color* adlanır), CMYK (ing. *Cyan, Magenta, Yellov*, Key və ya Black,-Mavi, Bənövşəyi, Sarı, Aşar və yaxud Qara rənglərin formalaşdırılmasının subtraktiv sxemi, dördrəngli avtotip, -poliqrafiya sahəsində əsas rəng modeli sayılır və triad rənglərin köməyi ilə ondan "standart triad" adlanan çap işlərində istifadə olunur) modellərindən (RGB və CMYK) istifadə olunan modellərinin təsviri verilmişdir.

Nəhayət, səs tipli informasiyanın kodlaşdırılması dedikdə isə analoq şəklində səs siqnallarının kompüterlərin prosessorunun başa düşdüyü formata, başqa sözlə, ikili koda dönüşdürülməsi başa düşülür. Səsin rəqəmsallaşdırılması prosesində yaddaşda siqnalın ayrı-yarı draqmentləri qalır və onları dinamikə, yaxud qulaqcıqlara ötürmək tələb olunur. Bu zaman 1 saniyə ərzində yadda saxlanılan sayım diskretizasiyanın tezliyi ilə müəyyən olunur. 1 saniyə ərzində edilən sayım 1 Hz (1 hers) təşkil edir. 8 kKz (kiloherz) isə 1 saniyədə 8000 sayımın olması anlamına gəlir. Kodlaşdırmanın dərinliyi dedikdə isə 1 sayımda ayrılan bitlərin sayına bərabər olur. İnformasiyanı N saniyə uzunluğunda x Hz diskretizasiyası tezliyi və Z bit dərinliyi ilə kodlaşdırılmış şəkildə yaddaşda saxlamaq üçün N -x -Z bit yaddaşı tələb olunur. Məsələn, 8 kHz, 1 sayımda 16 bit kodlaşdırma dərinlikli və uzunluğu 128 saniyə olan səs üçün 2 Mbayt tələb olunur: 8000 * 16 * 128 = 1 638 400 bit = 2000 Kbayt.

Kompüterin yaddaşında mətn informasiyaları müəyyən qaydalara uyğun şəkildə təqdim olunur. Məlumdur ki, mətn kompüterin yaddaşına klaviatura vasitəsi ilə daxil edilir. Klaviaturanın düymələrində hərflər, rəqəmlər, durğu işarələri və digər rəmzlər olur. Onlar operativ yaddaşa ikili kod şəklində düşür. Bu o, deməkdir ki, hər simvol 8 bitli ikili kod vasitəsi ilə təqdim olunur. Mətnin kodlaşdırılması isə ondan ibarətdir ki, hər simvola 0-dan 255-ə qədər müvafiq unikal onluq kodu və yaxud ona uyğun gələn ikili kod (00000000-dan 11111111-ə qədər) qoyulur. Bu cür kombinasiya istifadəçiyə simvolları cizgilərinə uyğun, kompüterləri isə onun koduna uyğun fərqləndirməyə və təyin etməyə imkan verir. Windows əməliyyat sistemləri mətnin kodlaşdırılmasını iki formada həyata keçirir: 1. Ənənəvi 8 bitli kodlaşdırılmış səhifə formasında. 2. UTF-16 (ing. *Unicode Transformation Forma*-informatikada kodlaşdırma üsulu, 16 bitli ardıcıllıq şəklində beynəlxalq Unicode rəmzlərindən istifadə edilməsini nəzərdə tutur) şəklində.

Bu gün müxtəlif tip kompüterlər (EHM) üçün fərqli kodlaşdırma cədvəllərindən istifadə edilir və onların çoxu qlobal (beynəlxalq) xarakter kəsb edir. Fərdi kompüter üçün nəzərdə tutulmuş qlobal əhəmiyyətli standartlar arasında məlumat mübadiləsi üçün nəzərdə tutulmuş Amerika (US) standart kodu -ASCII (ing. *American Standard Code for İnformation*) və Unikode kimi çox populyar standartları xüsusi qeyd etmək lazımdır. ASPII müasir latın əlifbası işarələrinin, rəqəmlərin, bəzi xüsusi işarələrin və idarəçilik ardıcıllığının kodlaşdırılması üzrə xüsusi standartdır. O, EHM-lərdə mətn verilənlərinin təqdimatı vasitəsi kimi 1963-cü ildə Amerika Milli Standartlar İnstitutu (ing. *American national standards institute,* ANSI) tərəfindən yaradılmışdır. Bu gün fərdi kompüterin əsas komponetlərini təşkil edən ASPII standartı xüsusi cədvəl kimi təqdim olunur. Müxtəlif kodlarla təmsil olunan ASPII standartı iki hissəyə bölünür və yalnız cədvəlin birinci hissəsi, yəni ki, 0-dan (00000000) 127-yə (01111111) qədər beynəlxalq standart hesab olunur. Göründüyü kimi ASPII standartı cütlüklərlə bağlı göstərişlərin nəzərə alınmadığı və 128 kod mövqeyindən ibarət olan 7 sıra kodların məcmusudur və o, aşğıdakı rəmzlərin kodlaşdırılması üçün nəzərdə tutulmuşdur: -onluq rəqəmlər; -latın əlifbası; -milli əlifba; -durğu işarələri; -idarəedici simvollar.

ASPII standartının ilk versiyası 36 idarəedici simvoldan (10 ərəb rəqəmi və 27 simvol) ibarət idi və bu simvollar aşağıda təsvir olunduğu kimi qruplaşdırılmışdır: 1. 8 durğu işarəsi (. , : ! ? ' "). 2. 5 maliyyə və birja əməliyyatları nişanı (#$%&@). 3. 2 cüt mötərizə (() []). 4. 8 riyazi simvol (+ - * /\ = < >)/. 5. 2 blok sxem üçün ox (↑←). ASPII standartının 1967-ci ildə təzələnmiş versiyasında idarəedici simvolların sayı 33-ə endirilmişdir. Oxlar ləğv olunmuş, onların əvəzinə kiçik hərflər və 7 əlavə simvol (^ _ `{ | } ~) daxil edilmişdir. Beləliklə, cədvəl tamamlanmışdır.

ASPII standartı üzrə verilənlərin bölünməsi 4 kateqoriya üzrə həyata keçirilir. ASPII standartının köhnə versiyalarında bütün idarəedici simvollar isə böyük həcmdə əməliyyatları icra edirdi. Lakin tədricən onlar öz əhəmiyyətini itirdi və bu gün müasir kompüter sistemlərində

onlardan istifadə olunmur. Göründüyü kimi ASPII standartını ifadə edən cədvəldə bütün simvollar konkret əməliyyatların, müxtəlif tapşırıqların və vəzifələrin icrası üçün nəzərdə tutulmuşdur.

İnformasiya texnologiyalarında müstəsna rolu və əhəmiyyəti olan kodlaşdırma standartlarından biri də *Unicode* (ing. *Universal Code*-yazılı simvollardan istifadə etməklə kodlaşdırmaları həyata keçirir) hesab olunur. *Unicode* standartı 1991-ci ildə ABŞ-ın Koliforniya ştatının Mantin-Vyu şəhərində *Unicode Consortium Unicode Inc* şirkəti tərəfindən yaradılmışdır. *Unicode,* platformasından, dilindən və proqramından asılı olmayaraq, hər bir simvol üçün unikal koddur. *Unicode* standartı XX əsrin 80-ci illərində kodlaşdırma sahəsində yaranmış problemləri aradan qaldırmaq məqsədi ilə yaradılmışdır. Həmin problemlər içərisində koddan çıxarmaq çətinlikləri, simvollar dəstinin kifayət qədər olmaması, bir kodlaşdırmanı digərinə çevirmək, şriftlərin sadə dublikasiyası və s. daha kəskin şəkildə ifadə olunur və çox ciddi çətinliklər yaradırdı. *Unicode* standartının tətbiqilə müxtəlif dillərdən çoxlu sayda simvolları kodlaşdırmaq mümkün oldu. Bu gün isə *Unicode* sənədlərində riyazi simvollardan, yunan və latın əlifbasının hərflərindən, hətta Çin iyeroqliflərindən istifadə olunur və kodlaşdırmada prosesində kod səhifələrini dəyişdirməyə ehtiyac qalmır. Hazırda *Unicode* standartı İnternetdə əsas kodlaşdırma standartı hesab olunur və 16 bitli ardıcıllıqla icra olunan UTF-16 (ing. *Unicode Transformation Format*) adlı kodlaşdırma üsulu sözügedən bu standartlaşdırmada üstünlük təşkil edir. UTF-16 kodlaşdırılmasında hər hansı rəmzin şifrələnməsi işinə, adətən 2 bayt sərf olunur. *Unikode* standartı 2 hissədən ibarətdir: 1. Rəmzlərin universal dəsti (ing. *Universal character set, UCS*). 2. Kodlaşdırma dəstləri (ing. *Unicode transformation format, UTF*) (Soubiran, 2020).

Simvolların universal dəsti *Unicode* standartının icazə verdiyi rəmzləri sayır və onların hər birinə mənfi olmayan rəqəm şəklində U+ prefiksli (lat. *Praefixus* -"öndən qoşulmuş", informatika elmində sətirin əvvəli) simvol kodu (məsələn, U+040F) verir. Kodlaşdırma dəstləri isə faylda və axında ötürülməsi üçün simvolların əsas kodlarını dəyişdirən üsulları müəyyən edir (Laurent, 2013, s. 62).

Unicode standartında kodlar bir neçə sahəyə bölünmüşdür. U+0000 kodundan U+007F koduna qədər sahədə ASPII simvollarından istifadə olunur. Daha sonra digər yazı sistemlərinin simvollarından ibarət səhifə gəlir. Kodların bir qismi isə gələcəkdə istifadə etmək məqsədilə rezervdə yerləşdirilir. Unicode standartında qrafik və yaxud çap simvolları bir neçə qrupa bölünür: - müxtəlif əlifbalarda istifadə olunan hərflər; -rəqəmlər; - durğu işarələri; - xüsusi simvollar (ideoqramlar, riyazi və texniki işarələr); -bölən işarə və diakritik (yun. *Diakritikos*-fərqləndirici) nişan (Blinova, 2019, s. 7).

Bu gün Unicode kodlaşdırma standartı sabitlik prinsipi, dinamik şəkildə yığılan, məntqi ardıcıllıqlı, mətnlərin və simvolların forma və semantik cəhətdən sadə olması və asanlıqla dəyişdirilməsi, unikallığı, unifikasiyalılığı və effektliliyi ilə informasiya texnologiyaları sahəsində liderliyi əldə saxlayır.

Nəticə

Göründüyü kimi müasir cəmiyyətin adekvat məzmununu ifadə edən informasiya insan fəaliyyətinin bütün sahələrində daim fövqəladə tələbat duyulan bir fenomendir. O, insanların elmi və ictimai-mədəni dünyagörüşünü durmadan artıran, onun əqli və inetellektual imkanlarının davamlı inkişafına əlverişli şərait yaradan, onu idarə edən, yönləndirən və müvafiq qərarlar qəbul etməyə sövq edən vacib element kimi varlığın keyfiyyət meyarlarını təşkil edir. Beləliklə, informasiya ictimai tərəqqinin lokomotivi qismində bəşəriyyəti daha keyfiyyətli, yüksək nailiyyətlər vəd edən uğurlu gələcəyə aparır. Məhz onun sayəsində ən yaxın gələcəkdə bir çox ölkələrdə yüksək təşəkküllü ümumi rifah cəmiyyəti yaratmaq mümkün olacaq. Buna görə də parlaq gələcəyimizin yol göstəricisi olan informasiyanın adekvat şəkildə qiymətləndirilməsi və informasiya təhlükəsizliyinin təmin edilməsi ümumbəşəri dəyərlərə vicdanla xidmət edən hər bir kəsin ümdə vəzifəsi olmalıdır. Buna görə də həyatımızın belə bir mühüm komponenti olan informasiyanın ciddi mühafizə altına alınmasını yüksək tərzdə təmin etmək üçün akademik səviyyədə effektli tədbirlərin görülməsi, texniki innovasiyaların durmadan inkişaf etdirilməsi, bununla da informasiya təhlükəsizliyinə etibarlı zəmanət verilməsi şərtdir.

Ədəbiyyat

1. Barr, A., Ben David, R. (2021). "*Kubernetes Autoscaling: Yo Yo Attack Vulnerability and Mitigation*". *Proceedings of the 11th International Conference on Cloud Computing and Services Science*. pp. 34-44. arxiv: 210500542.doi:10. 5220/0010397900340044
2. Bauer, F.L. (2000) *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie.* 3., überarbeitete und erweiterte Auflage. Springer, Berlin u. a.
3. Bender, A., Beller, S. (16 December 2013). "*Mangarevan invention of binary steps for easier calculation*". *Proceedings of the National Academy of Sciences*. 111 (4): 1322-1327. doi:10.1073/pnas.1309160110
4. Blinova, O.A. (2019). *Diakritiçeskie znaki v sovremennıx russkom i italyanskom yazıkax: proisxojdenie, problemı i sravnitelnıe osobennosti* / O.A. Blinova.-Tekst: neposredstvennıy // Filoloqiçeskie nauki v Rossii i za rubejom: materialı VI Mejdunarodnoy nauçnoy konferentsii. S.Peterburq: Svoyo izdatelstvo. S. 7
5. Chakravorty, P. (2918). What Is a Signal? (Lecture Notes) IEEE Signal Processing Magazine. (t. 35, № 5). - P. 175
6. Eadie, W, Robin G. (2013). "*Theories and models of communication: foundations and heritage*." Theories and Models of Communication, edited by Paul Cobley et al., Berlin, Boston: De Gruyter Mouton, 2013, pp. 17-36.
7. Garfinkel, S.L (2010). *Digital forensics research: The next 10 years.* Digital Investigation № 7. P. 65. http://dx.doi.org/10.1016/j.diin
8. Hintzbergen, Jule; Hintzbergen, Kees; Baars, Hans; Smulders, André. (2010). *Foundations of Information Security Based on Iso27001 and Iso27002.* Best Practice. Van Haren Publishing. P. 13
9. Karpicke, Jeffrey D. (2012). "*Retrieval-Based Learning: Active Retrieval Promotes Meaningful Learning*". Current Directions in Psychological Science. 21 (3): P.158. doi:10.1177/0963721412443552
10. Keyser, T. (2018), "*Security policy*", *The Information Governance Toolkit*, CRC Press, pp. 57-62, doi:10.1201/9781315385488-13, ISBN 978-1-315-38548-8, retrieved May 28, 2021
11. Kissel, L. Richard. (2013). *NIST Interagency or Internal Report 7298: Glossary of Key Information Security Terms*: Richard L. Kissel, editor, Computer Security Division, Information Technology Laboratory. - Revision 2. - Gaithersburg, MD, US: National Institute of Standards and Technology. - Pp. 94. – 222 p. https. //. doi. Org /10.6028/NIST.IR.7298r3
12. Koetter R., Kschischang F.R. (2007). *Coding for errors and erasures in random network coding* // IEEE International Symposium on Information Theory. Proc. ISIT-07.-2007.-P. 791. https://doi.org/10.48550/arXiv.cs/0703061
13. Laurent, S. (2013). *Introducing Erlang*. - O'Reilly Media, Inc. - P. 62. – 185 p.
14. Olupona, J.K. (2014). *African Religions: A Very Short Introduction*. Oxford University Press. P. 45
15. Rawson, A.; Zamary, A. (2019). *"Why is free recall practive more effective then recognition practice for enhancing memory?"// Evaluating the relational processing hypothesis*. *Journal of Memory and Language*. 105: 141-152. doi: 10. 1016 / j.jml.2019.01.002. ISSN: 0749-596X. S2CID 149703416.
16. Solms, R. (1998). "Information security management (3): the Code of Practice for Information Security Management", *Information Management Computer Security* Vol. 6 No. 5, p. 224. https://doi.org/10.1108/ 09685229810240158
17. Soubiran, T. (2020). *UTF: Unicode Transformation Format*. *NUMA*. Retrieved April 9, 2025 from https://doi.org/10.58079/sgoo

Daxil oldu: 03.01.2025
Qəbul edildi: 16.04.2025