DOI: https://doi.org/10.36719/2789-6919/45/258-261

**Mirzə Talıbov**
Azərbaycan Texnologiya Universiteti
magistrant
https://orcid.org/0009-0001-4692-0481
mirzetalibov7@gmail.com

# Kompüter şəbəkələrində informasiya təhlükəsizliyi mexanizmlərinin işlənməsi və tətbiq edilməsi

## Xülasə

Tədqiqatın aktuallığı. Müasir dövrdə rəqəmsallaşmanın dinamik inkişafı fonunda kompüter şəbəkələri həm fərdi istifadəçilərin, həm də iri təşkilatların gündəlik fəaliyyətində mühüm rol oynayır. Elektron idarəetmə sistemləri, onlayn maliyyə əməliyyatları, bulud texnologiyaları, rəqəmsal ticarət, məsafədən idarə olunan biznes və təhsil modellərinin geniş tətbiqi informasiya resurslarının təhlükəsiz, etibarlı və əlçatan şəkildə mübadiləsini zəruri edir. Tədqiqatın məqsədi. Araşdırmanın əsas məqsədi müasir kompüter şəbəkələrində informasiya təhlükəsizliyi ilə bağlı aktual risk və təhdidləri müəyyənləşdirmək, bu təhdidlərin qarşısını almaq üçün təsirli müdafiə üsullarını işləyib hazırlamaq və onların real mühitdə tətbiq imkanlarını təhlil etməkdən ibarətdir. Tədqiqatda istifadə olunan metodlar. Tədqiqatın məqsəd və vəzifələrinə uyğun olaraq araşdırmada analitik yanaşmalar, simulyasiya modelləri, statistik təhlillər və ümumi analiz metodları tətbiq olunmuşdur. Tədqiqatın informasiya bazası. Tədqiqat zamanı yerli və xarici mütəxəssislərin elmi araşdırmalarından, Azərbaycan Respublikası Statistika Komitəsinin rəsmi məlumatlarından, eləcə də xarici mənbələrdən toplanmış statistik göstəricilərdən istifadə olunmuşdur. Tədqiqatın məhdudiyyətləri. Tədqiqatın əsas məhdudiyyəti kifayət qədər resursların əldə olunmaması ilə bağlıdır.

Tədqiqatın elmi yeniliyi və praktiki nəticələri. Tədqiqatın elmi yeniliyi ondan ibarətdir ki, müasir kompüter şəbəkələrində tətbiq olunan informasiya təhlükəsizliyi mexanizmləri kompleks şəkildə araşdırılmış, onların funksional imkanları ilə yanaşı performansa təsiri də sistemli şəkildə təhlil edilmişdir. Mövcud yanaşmalardan fərqli olaraq, bu tədqiqatda təhlükəsizlik tədbirlərinin yalnız texniki səmərəliliyi deyil, həm də real şəbəkə şəraitində şəbəkə keçirmə qabiliyyətinə, gecikmə müddətinə və resurs sərfiyyatına təsiri müqayisəli şəkildə qiymətləndirilmişdir. Nəticələrin istifadə oluna biləcəyi sahələr. Tədqiqatın praktiki əhəmiyyəti ondan ibarətdir ki, real şəbəkə şəraitində kompüter şəbəkələrində informasiya təhlükəsizliyinin təmin olunması üçün istifadə edilən müxtəlif müdafiə mexanizmlərinin səmərəli seçimi, uyğunlaşdırılması və tətbiqi üzrə tövsiyələr hazırlanmışdır.

***Açar sözlər:*** *texnologiya, kompüter, informasiya, təhlükəsizlik, şəbəkə*

**Mirza Talibov**
Azerbaijan Technological University
Master student
https://orcid.org/0009-0001-4692-0481
mirzetalibov7@gmail.com

# Processing and Application of Informatıon Security Mechanisms in Computer Networks

## Abstract

Relevance of the research. In the modern era of rapidly growing digitalization, computer networks play a crucial role in the activities of all groups, from individual users to large organizations. The widespread use of services such as e-government systems, online banking, cloud technologies, e-commerce, remote business, and education makes the secure, reliable, and efficient exchange of information resources essential.

Objective of the research. The main goal of the research is to investigate existing risks and threats to information security in modern computer networks, to develop effective security mechanisms to counter these threats, and to assess the possibilities of applying these mechanisms in practical environments.

Using research methods. In accordance with the objectives and tasks of the research, analytical, simulation, statistical, and analytical methods were employed.

Information base of the research. Scientific works of local and foreign researchers and economists, official data from the Statistics Committee of the Republic of Azerbaijan, and statistical data obtained from foreign sources were used.

Limitations of the research. The main limitation lies in the insufficient availability of resources.

Scientific novelty and practical results of the research. The scientific novelty of the research lies in the comprehensive examination of information security mechanisms used in modern computer networks, with a systematic analysis not only of their functional capabilities but also of their impact on performance. Unlike existing approaches, this research comparatively evaluates the impact of security measures not only on technical effectiveness but also on network throughput, latency, and resource consumption in real network conditions.

Areas of practical application of the results. The practical significance of the research lies in the development of recommendations for the efficient selection, adaptation, and implementation of various mechanisms to ensure information security in computer networks under real network conditions.

***Keywords:*** *technology, computer, information, security, network*

## Giriş

Rəqəmsallaşmanın sürətlə inkişaf etdiyi müasir dövrdə kompüter şəbəkələri istər fərdi istifadəçilər, istərsə də iri müəssisələrin gündəlik fəaliyyətində əvəzolunmaz yer tutur. Elektron hökumət, onlayn maliyyə xidmətləri, bulud əsaslı platformalar, e-ticarət, məsafədən idarə olunan biznes və təhsil kimi sahələrdə bu texnologiyaların geniş tətbiqi, informasiya resurslarının etibarlı, təhlükəsiz və rahat şəkildə paylaşılmasını zəruri edir. Nəticə etibarilə, informasiya təhlükəsizliyi texnoloji infrastrukturun əsas elementlərindən birinə çevrilmişdir.

Eyni zamanda, kibertəhlükələrin – zərərli proqramlar, DDoS hücumları, məlumat sızmaları və daxildən gələn təhdidlərin – artan miqyasda yayılması sübut edir ki, ənənəvi müdafiə metodları artıq mövcud risklərə cavab verməkdə yetərli deyil (Barrenechea, Jenkins, 2014). Bu səbəbdən, informasiya təhlükəsizliyinin təmin edilməsi üçün yeni mexanizmlərin hazırlanması və tətbiqi yalnız texniki sahədə deyil, həm də sosial-iqtisadi baxımdan əhəmiyyətli bir tədqiqat istiqaməti kimi çıxış edir.

İnformasiya texnologiyalarının sürətlə inkişaf etdiyi müasir dövrdə kompüter şəbəkələri gündəlik həyatın və iş fəaliyyətinin ayrılmaz bir hissəsinə çevrilmişdir (Galubitskaya, Zhigul'skaya, 2000). Ancaq bu inkişafla yanaşı, informasiya təhlükəsizliyi ilə bağlı risklər də artmış və onların idarə olunması mühüm bir məsələyə dönüşmüşdür. Kompyuter şəbəkələrində informasiya təhlükəsizliyi təhdidləri əsasən, məlumatların sızması, icazəsiz girişlər, zərərli proqram hücumları, şəbəkə zəifliklərı və kibertəhlükələr ilə bağlıdır. Bu təhdidlər həm fərdi istifadəçilər, həm də hökumət orqanları və özəl sektor təşkilatları üçün ciddi risklər yaradır. İnformasiya təhlükəsizliyinə qarşı hücumların nəticələri yalnız maliyyə itkiləri ilə məhdudlaşmır, həmçinin şirkətlərin və təşkilatların nüfuzunun zədələnməsi, məxfi məlumatların ifşası və kritik sistemlərin təhlükə altına düşməsi ilə də nəticələnə bilər (Qasımov, 2007, s.192).

İnformasiya təhlükəsizliyinin idarə edilməsi, texnoloji mühitlərin dəyişməsi ilə zamanla inkişaf etmiş və təşkilatların fəaliyyətlərinin vacib bir hissəsinə çevrilmişdir. Bu inkişaf üç əsas mərhələdən keçmişdir. İlk iki mərhələdə əsasən təhlükəsizliyin texniki və təşkilati yönləri üzərində dayanılıb, üçüncü mərhələdə isə informasiya təhlükəsizliyi korporativ idarəetmə və strateji qərarlarda mühüm bir element kimi qəbul edilməyə başlanmışdır (Mozanlı, 2005, s.160).

Xüsusilə, 2000-ci ildən sonra ortaya çıxan üçüncü mərhələ, informasiya təhlükəsizliyi anlayışına yeni perspektivlər gətirərək texniki standartlar, beynəlxalq sertifikatlaşdırma, standartlaşdırma, informasiya təhlükəsizliyi mədəniyyətinin qurulması və sistemlərin davamlı olaraq təhlil edilməsi kimi prinsipləri daxil etmişdir. Bu dövr göstərdi ki, informasiya təhlükəsizliyi yalnız texniki

tədbirlərlə məhdudlaşmır, həm də təşkilatların strateji məqsədləri və iş prosesləri ilə sıx əlaqəlidir (Aslanbakan, 2016, s.148).

Kriptoqrafiya qədim dövrlərdən başlayaraq məlumatları qorumaq və gizlətmək məqsədilə istifadə olunan mühüm bir elmdir. İnformasiya təhlükəsizliyinin əsas prinsipləri olan məxfilik, bütövlük və autentifikasiya ilə sıx əlaqəli olan bu sahə, texnologiyanın inkişafı ilə daha geniş və mürəkkəb sahələrdə tətbiq edilməyə başlanmışdır. Xüsusilə, internet və rəqəmsal texnologiyaların yayılması ilə kriptoqrafiya, məlumatların təhlükəsiz mübadiləsini təmin etmək, müəllif hüquqlarını qorumaq və icazəsiz girişin qarşısını almaq üçün əsas vasitəyə çevrilmişdir. Kriptoqrafik yanaşmalar, riyazi modellərə və mürəkkəb alqoritmlərə əsaslanan müxtəlif metodları əhatə edir, və bu sahədə riyaziyyat, kompüter elmləri, elektronika və optika kimi elmlərdən geniş istifadə olunur.

İnformasiya texnologiyalarının sürətlə inkişafı və rəqəmsal transformasiya prosesi nəticəsində kompüter şəbəkələri bizim gündəlik həyatımızın və fəaliyyətimizin vacib bir hissəsinə çevrilmişdir. Bu şəbəkələr vasitəsilə məlumatlar ötürülür, saxlanılır və işlənilir. Lakin, informasiya texnologiyalarının geniş istifadəsi ilə birgə kibertəhlükəsizlik riskləri də artmışdır. Məlumatların qorunması, icazəsiz girişlərin qarşısının alınması və sistemlərin sabit şəkildə işləməsinin təmin edilməsi, informasiya təhlükəsizliyi sahəsində ən vacib məsələlərdən biridir. Kompüter şəbəkələrində informasiya təhlükəsizliyi anlayışı, məlumatların bütövlüyü, düzgünlüyü və təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər və mexanizmlərin məcmusudur. Bu sahədə tətbiq olunan metodlar arasında şifrələmə alqoritmləri, autentifikasiya və identifikasiya sistemləri, firewall texnologiyaları, antivirus və casus proqram təminatına qarşı həllər mövcuddur (Abdulragimov, Kagramanzade, 2002).

Kriptoqrafiya, məlumatları qorumaq üçün şifrələmə üsullarını araşdıran sahə, kriptoanaliz isə bu şifrələmə əməliyyatlarını pozmağa çalışan sahədir. Hər iki istiqaməti birləşdirən elm sahəsinə kriptoqrafiya adı verilir. Bu sahə əsasən riyaziyyat, kompüter elmləri və rabitə texnologiyaları ilə əlaqəlidir və informasiya təhlükəsizliyinin təmin edilməsində mühüm rol oynayır (E-Government in European Union, 2018). Kriptoqrafiyanın başlanğıcda yalnız dövlət, diplomatik və hərbi sahələrdə tətbiq olunduğu və bağlanmış bir elm sahəsi olaraq inkişaf etdiyi qeyd edilir. Lakin 1960-cı illərin sonlarından etibarən, bankçılıq və kommersiya sahələrində istifadəyə maraq artmışdır. Bu dəyişiklik açıq tədqiqatların yaranmasına və kriptoqrafiya sahəsində yeni yanaşmaların inkişafına yol açmışdır. 1970-ci illərdə baş verən iki mühüm hadisə, kriptoqrafiyanın sürətli inkişafını təmin etmişdir (Əlizadə, Musayev, Əliyev, 2016).

İnformasiya texnologiyalarının inkişafı ilə yanaşı, məlumatların təhlükəsiz şəkildə ötürülməsi və qorunması müasir kibertəhlükəsizlik sahəsinin əsas prioritetlərindən birinə çevrilmişdir (Varakin, 2001). Təhlükəsizlik protokolları, məlumatların ötürülməsi zamanı məxfilik, bütövlük və autentifikasiyanın təmin olunmasına xidmət edən texnologiyalardır. Bu protokollar hücumlardan, icazəsiz girişlərdən və məlumatların sızmasından qorunmaq üçün tətbiq edilir. Bu sahədə ən geniş istifadə olunan təhlükəsizlik protokollarına aşağıdakılar daxildir: IPSec (İnternet Protokolu Təhlükəsizliyi) – Şəbəkə səviyyəsində məlumatların şifrələnməsi və autentifikasiyasını təmin edən bir protokoldur. VPN (Virtual Özəl Şəbəkə) texnologiyaları isə geniş şəkildə istifadə edilir (Chadwick, 2006).

Müasir informasiya cəmiyyətində kompyuter şəbəkələri, həyatın bütün sahələrində əlaqə qurmaq və məlumat mübadiləsi aparmaq üçün əsas vasitə olmuşdur. Texnologiyanın sürətli inkişafı və rəqəmsallaşmanın artması ilə, fərdi istifadəçilərdən tutmuş iri təşkilatlar və dövlət qurumlarına qədər hər bir şəxsin gündəlik fəaliyyəti kompüter şəbəkələri üzərindən həyata keçirilir. Bu şəbəkələr, insanlara bir-biri ilə əlaqə qurmaq, məlumatları mübadilə etmək, çoxsaylı prosesləri uzaqdan idarə etmək və avtomatlaşdırmaq imkanı verir (Kolachalam, 2002).

## Nəticə

Müasir dövrdə, informasiya təhlükəsizliyi mexanizmlərinin inkişafı və onların effektiv şəkildə tətbiqi kompüter şəbəkələrinin təhlükəsiz və fasiləsiz işləməsi üçün vacib və qaçılmaz bir tələbdədir. Rəqəmsallaşmanın sürətlə irəliləməsi və kibertəhlükələrin gündən-günə artması ilə ənənəvi təhlükəsizlik metodları artıq kifayət etmir. Buna görə də, təhlükəsizlik sahəsində kompleks, elastik və qabaqlayıcı yanaşmaların tətbiqi daha da önəmli hala gəlmişdir. Tədqiqatın nəticələri olaraq aşağıdakı əsas məqamlar qeyd olunmuşdur: Texniki təhlükəsizlik mexanizmləri – şifrələmə, firewall,

IDS/IPS, SIEM, VPN, MFA və s. şəbəkə mühitində mövcud olan real təhdidlərə qarşı təsirli müdafiə təmin edir (European Union, 2017).

Bu sahənin əsas məqsədi informasiya sistemlərini həm daxili, həm də xarici təhlükələrdən qorumaq, icazəsiz müdaxilələrin qarşısını almaq, zərərli fəaliyyətləri müəyyən etmək və potensial riskləri idarə etməkdir. Bu bölmədə informasiya təhlükəsizliyi anlayışına ümumi yanaşma verilir, onun əsas mahiyyəti, prinsipləri, kateqoriyaları, mövcud təhdid növləri və onlardan qorunma üsulları açıqlanır. Eyni zamanda, müasir dövrdə informasiya təhlükəsizliyinin əhəmiyyətinin artması, bu sahədə qarşılaşılan problemlər və onların aradan qaldırılması yolları da araşdırılır.

Şəbəkə təhlükəsizliyində tətbiq olunan vasitələr – şifrələmə üsulları, firewall sistemləri, IDS/IPS texnologiyaları, identifikasiya və autentifikasiya metodları, eləcə də təhdidlərin aşkarlanması platformaları – müxtəlif təhlükə səviyyələrinə qarşı mübarizə aparmaq və sistemlərin təhlükəsizliyini təmin etmək məqsədi daşıyır. Bu fəsildə kompüter şəbəkələrində istifadə edilən əsas təhlükəsizlik alətləri geniş şəkildə araşdırılır, onların funksional imkanları, texniki çətinlikləri və sistem performansına olan təsirləri təhlil edilir. Bundan əlavə, müasir təhlükəsizlik yanaşmaları, bulud əsaslı texnologiyalar və risk əsaslı müdafiə modelləri də bu fəsildə tədqiqat predmeti kimi təqdim olunur.

VPN texnologiyaları, autentifikasiya üsulları, IDS/IPS sistemləri və digər oxşar vasitələrin həm real, həm də simulyasiya olunmuş şəbəkə mühitlərində fəaliyyət mexanizmləri və sistemin ümumi performansına təsirləri araşdırılır. Təhlil prosesində əsas diqqət gecikmə vaxtı, ötürmə sürəti, resursların istifadəsi və cavab müddəti kimi texniki göstəricilərə yönəlir. Bununla yanaşı, təhlükəsizliklə məhsuldarlıq arasında optimal tarazlığın təmin olunması, müasir təhlükəsizlik həllərinin elastik və genişlənə bilən arxitekturalarda tətbiqi, eləcə də təşkilatlar üçün faydalı və tətbiq edilə bilən tövsiyələrin hazırlanması bu fəsildə önəmli müzakirə mövzuları sırasındadır.

## Ədəbiyyat

1. Aslanbakan, E. (2016). *Bilgi güvenliği ve uygulamalı hacking yöntemleri*. Pusula.
2. Abdulragimov, K.F., Kagramanzade, G.A. (2002). O tekhnologii IPTelefoniya. *"Uchenye zapiski AZTU",* № 3.
3. Alizade, M.N., Musaev G.R., Aliev E.B. (2016), *Upravlenie sovremennymi informatsionnymi sistemami*. MSV.
4. Akhundov, B.M. (2000). *Osobennosti razvitiya svyazi v Azerbaidzhane*. Chashyogly.
5. Arcaris, C., Sood, R. (2013). *User Survey Analysis: IT Spending Priorities in Government, Worldwide, 2013*. Gartner, Inc.
6. Barrenechea M. J., Jenkins T. (2014), *E-Government or Out of Government*. First Printing.
7. Best practices in eGovernment: on a knife-edge between success and failure. (2008). European Journal of ePractice.
8. Chadwick A. (2006). *Internet Politics: States, Citizens and New Communication Technologies.* Oxford Univ.
9. *Department of Economic and Social Affairs (UNDESA).* (2018). United Nations.
10. *E-Government in European Union*. (2018).
11. European Union. (2017). Government Benchmark 2017: Taking stock of user-centric design and delivery of digital public services in Europe. *Final background report*. Volume 2.
12. Galubitskaya, E.A., Zhigul'skaya, G.M. (2000). *Ehkonomika svyazi.* Radio i svyaz.
13. Kolachalam, S. (2002). *An Overview of E-Government*. University of Bologna.
14. Qasımov, V.Ə. (2007). *İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq*. Elm.
15. Mozanlı, İ.A. (2005). *Söz azadlığı və informasiya təhlükəsizliyi: milli və beynəlxalq təminat*. UniPrint.
16. Varakin L.E. (2001). *Global'noe informatsionnoe obshchestvo: kriterii razvitiya i sotsial'no-ehkonomicheskie aspekty*. MAK.

Daxil oldu: 11.02.2025
Qəbul edildi: 21.05.2025