PARADIGMA, No.4, 2025, səh.125-131
https://doi.org/10.30546/30015.2025.01.4.1056

# TƏHSİL MÜƏSSİSƏLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

**L.F. Ağamalıyeva, A.V. Rəfiyev**
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: Azar.Rafiyev@student.au.edu.az

**Xülasə**. Məqalədə təhsil müəssisələrində informasiya təhlükəsizliyinin təmin olunmasına təsir edən əsas amillər araşdırılır, müasir rəqəmsal mühitdə yaranan risklərin xüsusiyyətləri qiymətləndirilir və onların idarə olunması üşün kompleks yanaşma təqdim olunur. Təhlil göstərir ki, təhlükəsizlik mexanizmlərin düzgün planlaşdırılması tədris prosesinin davamlılığı üçün həlledici əhəmiyyət daşıyır.

**Açar sözlər.** İnformasiya təhlükəsizliyi, təhsil müəssisələri, kiberrisklər, idarəetmə mexanizmləri, davamlılıq.

## Giriş

Müasir dövrdə təhsil müəssisələri geniş rəqəmsal infrastrukturdan istifadə etdikləri üçün informasiya təhlükəsizliyi onların fəaliyyətində strateji əhəmiyyətə malik bir sahəyə çevrilmişdir. Elektron tədris sistemləri, tələbə məlumat bazaları, universitetin daxili idarəetmə platformaları və müxtəlif bulud əsaslı xidmətlər gündəlik işin ayrılmaz hissəsinə çevrildikcə, bu mühitdə yaranan risklər də paralel şəkildə artır. Təhsil müəssisələrinin əsas vəzifəsi yalnız tədrisin təşkili deyil, həm də bu prosesdə emal olunan şəxsi məlumatların, intellektual mülkiyyətin və kritik əməliyyat resurslarının qorunmasıdır. Bu səbəbdən informasiya təhlükəsizliyinin təmin olunması ənənəvi texniki tədbirlərlə məhdudlaşmır, həmçinin idarəetmə, təşkilati və hüquqi mexanizimlərin də düzgün qurulmasını tələb edir [3].

Tədqiqatlar göstərir ki, təhsil sektorunda yaranan təhlükəsizlik boşluqlarının böyük qismi infrastrukturun sürətli genişlənməsi, müxtəlif şöbələr arasında koordinasiyanın zəifliyi və istifadəçilərin məlumatlılıq səviyyəsinin yetərincə olmaması ilə bağlıdır [1]. Məsələn, ali təhsil müəssisələrində istifadə edilən serverlər və xidmətlər daha çox istifadəçi kütləsi tərəfindən əlçatan olduğundan onlar kiberhücumlar üçün cəlbedici hədəfə çevrilir [2]. Bundan əlavə, universitetlərdə müstəqil fakültələrin və laboratoriyaların öz resurslarını idarə etməsi təhlükəsizlik standartlarının vahid şəkildə tətbiqinə mane olur və risklərin idarə olunmasını çətinləşdirir.

Beynəlxalq standartlar, xüsusilə ISO/IEC 27001 və ISO/İEC 27005 təhsil müəssisələrində təhlükəsizlik mühitinin sistemli şəkildə qiymətləndirilməsi üçün etibarlı çərçivə təqdim edir. Risklərin müəyyənləşdirilməsi, onların təsirinin qiymətləndirilməsi və uyğun idarəetmə tədbirlərinin seçilməsi bu çərçivənin əsas mərhələləridir [4]. Lakin praktik tətbiq zamanı müşahidə olunan əsas çətinlik ondan ibarətdir ki, standartların tələbləri çox vaxt

ümumi xarakter daşıyır və təşkilat daxilində real risklərin operativ şəkildə aşkarlanmasına və aradan qaldırılmasına yönəlmiş konkret mexanizmlərin yaradılmasını tələb edir [2].

Bu məqalədə təhsil müəssisələrində informasiya təhlükəsizliyinin təmin olunmasının mövcud vəziyyəti araşdırılır, risklərin qiymətləndirilməsi üçün istifadə olunan metodların effektivliyi təhlil edilir və idarəetmə, texniki və təşkilati tədbirlərin inteqrasiya olunmuş modeli təklif olunur. Məqsəd təhlükəsizlik mexanizmlərinin yalnız formal sənədləşmədən ibarət olmaması, həm də real əhəmiyyət proseslərində tətbiq oluna bilən praktiki struktura çevrilməsidir.

**Təhsil müəssisələrində informasiya təhlükəsizliyinin əhəmiyyəti və müasir çağırışlar**

Rəqəmsallaşmanın sürətlə inkişaf etdiyi müasir dövrdə təhsil müəssisələri həm məlumatların həcminin, həm də emal olunan məlumat növlərinin artması ilə üz-üzə qalır. Bu təşkilatlar tələbə məlumatları, maliyyə əməliyyatları, elmi-tədqiqat nəticələri və partnyor təşkilatlarla əməkdaşlıqlara dair ən müxtəlif informasiyaları saxladıqları üçün kibertəhlükələrin əsas hədəflərindən birinə çevrilir. Məlumat sızıntısı, icazəsiz daxilolmalar, zərərli proqramlar və xidmətin dayandırılması tipli hücumlar həm tədris prosesinin fasiləsizliyinə, həm də təşkilatın reputasiyasına ciddi zərər vurur [2].

Təhsil müəssisələrinin əhəmiyyətli xüsusiyyətlərindən biri onların çoxsaylı istifadəçi qrupları-tələbələr, müəllimlər, inzibati heyət, qonaq araşdırmaçılar və texniki personal tərəfindən eyni infrastrukturun paylaşılmasıdır. Bu müxtəliflik idarəetmə baxımından çətinlik yaratmaqla yanaşı, təhlükəsizlik tələblərinin vahid şəkildə tətbiqini də mürəkkəbləşdirir. İstifadəçilərin tibbi məlumatlardan qiymətləndirmə nəticələrinə qədər fərqli kateqoriyalı informasiyalara çıxışı olduğundan, məlumatların düzgün təsnifləndirilməsi və onların qorunmasını təmin edən mexanizmlər daha vacib hala gəlir [4].

Müasir çağırışlardan biri də bulud əsaslı xidmətlərə geniş keçid və üçüncü tərəf platformalarından istifadənin artmasıdır. Bulud xidmətləri təhsil müəssisələrinin resurslara qənaət etməsinə və xidmətlərin əlçatanlığını artırmasına imkan yaratsa da, təhlükəsizlik nəzarətinin bir qismi xidmət provayderinə keçdiyi üçün risklərin qiymətləndirilməsi daha mürəkkəb xarakter alır. Bu halda məlumatların hansı ölkədə saxlanıldığı, hansı şifrələmə üsullarının tətbiq olunduğu və insidentlər zamanı məsuliyyət bölgüsünün necə müəyyənləşdirildiyi kimi məsələlər daha çox diqqət tələb edir [7].

Digər mühüm çağırış istifadəçilərin məlumatlılıq səviyyəsi ilə bağlıdır. Araşdırmalar göstərir ki, təhsil sektorunda baş verən insidentlərin əhəmiyyətli hissəsi texniki boşluqlardan deyil, insan faktorundan qaynaqlanır. Zərərli keçidlərə daxil olmaq, şifrələrin zəif seçilməsi,

ictimai Wi-Fi-dan istifadə zamanı təhlükəsizlik qaydalarının göz ardı edilməsi kimi hallar məlumatların sızmasına geniş şərait yaradır [9]. Bu səbəbdən təhlükəsizlik maarifləndirilməsi və sosial mühəndislik risklərinə qarşı davranış qaydalarının tədrisi informasiya təhlükəsizliyinin ayrılmaz elementinə çevrilmişdir.

Ümumilikdə, informasiya təhlükəsizliyi təhsil müəssisələrinin yalnız texniki infrastrukturunun deyil, həm də təşkilati idarəetmə sistemlərinin ayrılmaz hissəsi kimi dəyərləndirilməlidir. Təhlükəsizlik mexanizmləri düzgün qurulmadıqda, tədris prosesinin dayandırılması, elmi araşdırmaların pozulması, tələbə məlumatlarının itirilməsi və təşkilatın ictimai etibarının sarsılması kimi ciddi nəticələr qaçılmaz olur. Bu səbəbdən təhlükəsizlik strategiyalarının təhsil müəssisələrinin idarəetmə modelinə inteqrasiya olunması və bütün istifadəçi qruplarını əhatə edən çoxşaxəli yanaşmanın tətbiqi mühüm əhəmiyyət kəsb edir [1].

**İnformasiya təhlükəsizliyi risklərinin növləri və onların təhsil mühitində təzahür formaları**

Təhsil müəssisələrində informasiya təhlükəsizliyinə təsir edən risklər çoxşaxəlidir və onların mənbəyi həm texniki, həm təşkilati, həm də insan faktorundan qaynaqlana bilər. Bu risklərin düzgün müəyyənləşdirilməsi təhlükəsizlik strategiyasının formalaşdırılmasında əsas rol oynayır. Beynəlxalq standartlara görə risklər adətən texniki zəifliklər, proseslərin qeyri-səmərəliliyi və istifadəçilərin davranışı ilə əlaqəli olmaqla üç əsas kateqoriyada qiymətləndirilir [4]. Təhsil mühitində isə bu risklərin özünəməxsus təzahür formaları daha kəskin şəkildə üzə çıxır.

Texniki risklər informasiya sistemlərində mövcud olan boşluqlar, yenilənməmiş proqram təminatı, zəif şifrələmə metodları və kənar hücumlara qarşı dayanıqlığın aşağı olması ilə bağlıdır. Universitetlərdə müxtəlif istehsalçı və fərqli texnologiyalardan ibarət heterogen infrastrukturun olması bu riskləri daha da artırır. Tədqiqatlar göstərir ki, tədris platformalarının, tələbə qeydiyyat sistemlərinin və serverlərin bir qismi hələ də köhnə sistemlər üzərindən fəaliyyət göstərdiyinə görə kiberhücumlara qarşı daha həssasdır [2].

Təşkilati risklər əsasən proseslərin qeyri-standartlaşdırılması, məlumatların idarə olunması qaydalarının qeyri-müəyyən olması və struktur bölmələr arasında koordinasiyanın zəifliyi ilə əlaqəlidir. Təhsil müəssisələrinin özünəməxsus idarəetmə modeli – yəni fakültə, mərkəz və laboratoriyaların müstəqil qərarvermə mexanizmi – vahid təhlükəsizlik siyasətinin tətbiqini çətinləşdirir. Bu da məlumatların saxlanması, ötürülməsi və məxfiliyinin təmin olunmasında uyğunsuzluqlara gətirib çıxarır [1].

İnsan amili ilə bağlı risklər isə ən geniş yayılmış və ən təhlükəli kateqoriyalardan biridir. Tələbələrin və əməkdaşların təhlükəsizlik qaydalarına əməl etməməsi, zəif parollardan istifadə,

cihazların qorunmaması və ya sosial mühəndislik hücumlarına məruz qalması məlumat sızıntısının baş verməsi üçün əsas şərait yaradır. NIST-in hesabatlarına görə, insidentlərin böyük qismi texniki deyil, məhz insan səhvlərindən qaynaqlanır [5].

Bütün bu risklərin təhsil mühitində birgə mövcudluğu onların təsir dairəsini daha geniş edir. Məlumat itkiləri tədrisin dayanmasına, tələbə və işçi məlumatlarının kənar şəxslərin əlinə keçməsinə və nəticədə təşkilatın nüfuzuna ciddi xələl gəlməsinə səbəb ola bilər. Buna görə də risklərin düzgün təsnifatı və təzahür formalarının vaxtında müəyyən olunması təhlükəsizlik strategiyasının əsas başlanğıc nöqtəsi hesab olunur.

**Risklərin qiymətləndirilməsi: metodlar, standartlar və tətbiq imkanları**

Təhsil müəssisələrində informasiya təhlükəsizliyinin təmin olunmasında risklərin qiymətləndirilməsi ən mühüm mərhələlərdən biri hesab olunur. Bu proses təşkilatın informasiya aktivlərinə təsir göstərə biləcək mümkün təhlükələri müəyyənləşdirməyə, onların ehtimal və təsir dərəcəsini qiymətləndirməyə və uyğun idarəetmə tədbirlərinin seçilməsinə imkan yaradır. Beynəlxalq standartlarda tövsiyə edilən risk qiymətləndirmə yanaşmaları təhsil mühitinə tətbiq edildikdə daha dəqiq və sistemli nəticələr əldə etmək mümkündür [4].

Risk qiymətləndirməsinin həyata keçirilməsində iki əsas metodoloji istiqamət – kəmiyyət və keyfiyyət üsulları geniş tətbiq olunur. Keyfiyyət yanaşması riskləri ehtimal və təsir baxımından “aşağı”, “orta” və “yüksək” kimi kateqoriyalara ayırmaqla daha çevik qiymətləndirmə imkanı yaradır. Bu üsul çoxsaylı iştirakçıları olan təhsil mühitində daha praktik hesab edilir, çünki ekspert rəyinə əsaslanaraq sürətli nəticələr təqdim edir. Kəmiyyət yanaşması isə risklərin rəqəmsal göstəricilərlə ölçülməsini tələb etdiyi üçün daha dəqiq olsa da, əlavə resurs və analitik bacarıqlar tələb edir [7].

Risklərin qiymətləndirilməsi prosesində standartların tətbiqi də mühüm rol oynayır. ISO/IEC 27005 standartı informasiya təhlükəsizliyi risklərinin idarə olunması üçün nəzərdə tutulmuş metodoloji çərçivə təqdim edir və təhsil müəssisələrinə risklərin müəyyənləşdirilməsi, təhlili və emalı üzrə ardıcıl addımları planlaşdırmağa imkan yaradır [4]. Bundan əlavə, NIST-in 800-30 təlimatında risk qiymətləndirməsinin mərhələləri daha detallı şəkildə təsnif edilir və insan faktorunun, texniki zəifliklərin və təşkilati çatışmazlıqların nəzərə alınmasını tövsiyə edir [5]. Bu standartların tətbiqi təhsil sektorunda risklərin daha real və obyektiv şəkildə qiymətləndirilməsinə şərait yaradır.

Risk qiymətləndirməsinin tətbiq imkanları genişdir və təhsil mühitində həm strategiyanın, həm də gündəlik əməliyyat proseslərinin formalaşdırılmasına təsir edir. Əvvəla, risklərin qiymətləndirilməsi məlumatların təsnifatı və onların qorunma səviyyəsinin müəyyənləşdirilməsi üçün əsas baza rolunu oynayır. Məsələn, tələbə məlumatları və tədqiqat

nəticələri daha yüksək təhlükəsizlik səviyyəsi tələb etdiyi halda, daxili administrativ sənədlər üçün orta səviyyəli nəzarət kifayət edə bilər. Digər tərəfdən, qiymətləndirmə nəticələri risklərin qarşısını almaq, azaltmaq, transfer etmək və ya qəbul etmək kimi müxtəlif idarəetmə qərarlarının verilməsində mühüm rol oynayır [2].

Praktiki tətbiq baxımından risk qiymətləndirməsi daimi monitorinq və təhlil mexanizmləri ilə dəstəkləndikdə daha effektiv olur. Təhsil müəssisələrinin infrastrukturunda tez-tez yenilənən xidmətlər, yeni tətbiqlər və dəyişən istifadəçi davranışları təhlükəsizlik mühitini dinamik edir. Bu səbəbdən risk qiymətləndirməsi yalnız bir dəfə deyil, mütəmadi olaraq aparılmalı, nəticələr idarəetmə siyasətlərinə inteqrasiya edilməlidir [1]. Beləliklə, risklərin qiymətləndirilməsi təhsil müəssisələrinin informasiya təhlükəsizliyini möhkəmləndirmək üçün həm strateji, həm də operativ səviyyədə vacib alətə çevrilir.

**İdarəetmə, texniki və təşkilati tədbirlər: inteqrasiya olunmuş təhlükəsizlik modeli**

Təhsil müəssisələrində informasiya təhlükəsizliyinin effektiv şəkildə təmin edilməsi yalnız texniki həllərlə məhdudlaşmır; idarəetmə, təşkilati və texnoloji komponentlərin vahid çərçivədə birləşdirildiyi inteqrasiya olunmuş model tələb olunur. İdarəetmə səviyyəsində təhlükəsizlik siyasətlərinin formalaşdırılması, məlumatların təsnifatı, istifadəçi hüquqlarının müəyyən edilməsi və insidentlərin idarə olunması üzrə prosedurların hazırlanması əsas rol oynayır [4]. Bu çərçivə müəssisənin bütün struktur bölmələrində vahid yanaşmanın tətbiqini təmin etməklə risklərin koordinasiyalı şəkildə idarə olunmasına şərait yaradır.

Texniki tədbirlər informasiya resurslarının bilavasitə qorunmasına yönəlmiş infrastruktur həllərini əhatə edir. Bunlara şifrələmə mexanizmləri, çoxfaktorlu autentifikasiya, təhlükəsizlik divarları, antivirus sistemləri və şəbəkə trafikinə nəzarət vasitələri daxildir. Təhsil müəssisələrində geniş istifadəçi kütləsi mövcud olduğundan, texniki müdafiə vasitələrinin mütəmadi yenilənməsi və zəifliklərin vaxtında aradan qaldırılması xüsusi əhəmiyyət daşıyır [2].

Təşkilati tədbirlər isə əməkdaşların və tələbələrin təhlükəsizlik qaydalarına əməl etməsini təmin edən maarifləndirmə proqramlarını, daxili təlimləri və məsuliyyət bölgüsünü əhatə edir. NIST təlimatlarına görə, insan faktorunun təhlükəsizlik insidentlərinin əsas mənbələrindən biri olması bu istiqamətdə davamlı monitorinq və maarifləndirmənin vacibliyini göstərir [5]. Bu tədbirlər istifadəçi davranışının təhlükəsizlik tələblərinə uyğunlaşdırılması ilə risklərin azalmasına əhəmiyyətli şəkildə təsir edir.

İnteqrasiya olunmuş təhlükəsizlik modeli idarəetmə, texniki və təşkilati elementlərin bir-birini tamamladığı çoxşaxəli yanaşmanı formalaşdırır. Bu modelin tətbiqi təhsil müəssisələrində məlumat təhlükəsizliyinin yalnız reaktiv müdafiə tədbirləri ilə deyil, həm də

qabaqlayıcı və davamlı mexanizmlərlə təmin edilməsinə imkan yaradır. Beləliklə, təhlükəsizlik mühiti daha dayanıqlı olur və tədris prosesinin fasiləsizliyi təmin edilir.

**Nəticə**

Aparılan təhlillər göstərir ki, təhsil müəssisələrində informasiya təhlükəsizliyinin təmin olunması çoxsahəli prosesdir və texniki müdafiə tədbirləri ilə məhdudlaşmır. Rəqəmsal platformaların genişlənməsi, istifadəçi sayının artması və müxtəlif məlumat növlərinin emalı təhlükəsizlik risklərini daha da mürəkkəbləşdirir. Bu səbəbdən risklərin düzgün müəyyənləşdirilməsi, onların təsir dərəcəsinin qiymətləndirilməsi və uyğun idarəetmə tədbirlərinin seçilməsi təhlükəsizlik strategiyalarının əsasını təşkil edir.

Tədqiqat göstərir ki, idarəetmə, texniki və təşkilati tədbirlərin ayrı-ayrılıqda deyil, vahid və inteqrasiya olunmuş model çərçivəsində tətbiqi təhlükəsizliyin effektivliyini əhəmiyyətli dərəcədə artırır. ISO/IEC 27001 və ISO/IEC 27005 kimi beynəlxalq standartlara əsaslanan yanaşma risklərin ardıcıl və sistemli şəkildə idarə olunmasına imkan verir, NIST çərçivələri isə insan faktoru da daxil olmaqla təhlükəsizlik zəifliklərinin daha geniş spektrini nəzərə almağa şərait yaradır.

Nəticə etibarilə, informasiya təhlükəsizliyi təhsil müəssisələrinin fəaliyyətinin davamlılığı, tələbə məlumatlarının qorunması və təşkilatın reputasiyasının saxlanılması üçün strateji əhəmiyyətə malikdir. İnfrastrukturun düzgün idarə olunması, istifadəçilərin maarifləndirilməsi və standartlaşdırılmış idarəetmə proseslərinin tətbiqi bu sahədə əsas prioritetlər olaraq qalmalıdır. İnformasiya təhlükəsizliyinin kompleks şəkildə qurulması təhsil müəssisələrinə həm mövcud risklərin qarşısını almağa, həm də gələcəkdə yaranacaq təhdidlərə qarşı daha dayanıqlı mühit formalaşdırmağa imkan yaradır.

**Ədəbiyyat**

1. BSI, (2013), IT-Grundschutz Catalogues, 13-cü buraxılış, Bonn, Federal Office for Information Security.
2. Hommel W., Metzger S., Steinke M., (2015), Information security risk management in higher education institutions: From processes to operationalization, EUNIS 2015 Konfransı.
3. ISO/IEC 27001, (2022), Information security, cybersecurity and privacy protection — information security management systems, Geneva, International Organization for Standardization.
4. ISO/IEC 27005, (2018), Information security risk management, Geneva, International Organization for Standardization.

5. NIST, (2012), Special publication 800-30 Rev. 1: Guide for conducting risk assessments, Gaithersburg, National Institute of Standards and Technology.
6. NIST, (2020), Special publication 800-53 Rev. 5: Security and privacy controls for information systems and organizations, Washington, U.S. Department of Commerce.
7. OECD, (2015), Digital security risk management for economic and social prosperity: OECD recommendation, Paris, OECD Publishing.
8. Pardo T. A., Burke G. B., (2021), Information sharing and information security in public sector organizations, Government Information Quarterly.
9. Siponen M., Oinas-Kukkonen H., (2019), A review of information security issues and practices in the education sector, Information Management & Computer Security.
10. Von Solms B., Van Niekerk J., (2013), From information security to cybersecurity, Computers & Security.

## INFORMATION SECURITY IN EDUCATIONAL INSTITUTIONS

**L.F. Agamalieva, A.V. Rafiyev**
Azerbaijan University, Ceyhun Hacıbeyli str.71, Baku, Azerbaijan

**Abstract.** The article explores the key factors influencing the assurance of information security in educational institutions, evaluates the characteristics of emerging risks in the modern digital environment, and proposes an integrated approach for their effective management. The analysis demonstrates that properly structured security mechanisms play a decisive role in ensuring the continuity and stability of educational processes.

**Keywords:** İnformation security, educational institutions, cyber risks, management mechanisms, continuity.