

ELEKTRON JURNALLARDA QIYMƏTLƏNDİRMƏ VƏ DAVAMIYYƏT MƏLUMATLARININ SAXTALAŞDIRILMASINA QARŞI TƏHLÜKƏSİZLİK YANAŞMALARI

Arzu Məsim oğlu Quliyev

Azərbaycan Dövlət Pedaqoji Universitetinin dosenti

ORCID: 0009-0001-3950-3663

E-mail: quliyev.arzu.68@mail.ru

Aytac Etibar qızı Mikayılova

Azərbaycan Dövlət Pedaqoji Universitetinin magistrantı

ORCID: 0009-0000-3127-3405

E-mail: mikayilovaa022@gmail.com

Açar sözlər: elektron jurnal, məlumatların saxtalaşdırılması, biometrik identifikasiya, sosial mühəndislik, müəllimlərin rəqəmsal savadlılığı, kibertəhlükəsizlik

Ключевые слова: электронный журнал, фальсификация данных, биометрическая идентификация, социальная инженерия, цифровая грамотность преподавателей, кибербезопасность

Key words: electronic journal, data falsification, biometric identification, social engineering, teachers' digital literacy, cybersecurity

Rəqəmsal dövrün inkişafı həyatımızın hər bir sahəsinə, o cümlədən təhsil sistemində də dərin təsir göstərir. Müasir texnologiyaların və rəqəmsal alətlərin təhsildə tətbiqi, tədris prosesini daha səmərəli, şəffaf və əlçatan etmək baxımından əhəmiyyətlidir. Rəqəmsal təhsil alətləri arasında elektron jurnalların yanında, tələbələrin məlumatlarına asanlıqla girişi təmin edən öyrənmə idarəetmə sistemləri (LMS) kimi platformalar da mövcuddur. Bu sistemlər tələbələrə dərs materiallarına və akademik resurslara daha asan və sürətli əlçatanlıq imkanı verir. Eyni zamanda, bu cür sistemlər təhsil müəssisələrində məlumatların mərkəzləşdirilmiş şəkildə idarə olunmasını təmin edir.

Bu baxımdan, elektron jurnalların təhsil müəssisələrində istifadəsi, müəllim və tələbələr üçün bir çox üstünlüklər təmin edir. Bununla yanaşı, bu sistemlər məlumatların idarə olunmasını asanlaşdırır və təhsil müəssisələrinin idarəetmə proseslərini optimallaşdırır. Rəqəmsal texnologiyaların təhsil sahəsində tətbiqi ilə bir sıra problemlər də meydana çıxır. Bu problemlər arasında texniki nasazlıqlar, məlumatların təhlükəsizliyinə olan təhdidlər və istifadəçilərin rəqəmsal savadlılıq səviyyəsinin aşağı olması kimi məsələlər yer alır. Həmçinin, bu texnologiyaların istifadəsi zamanı etik məsələlər və məlumatların saxtalaşdırılması riski də diqqətdə saxlanmalıdır. Bütün bu səbəblərə görə, elektron jurnalların tətbiqinin həm müsbət, həm də mənfi tərəflərinin diqqətlə təhlil olunması və onların təhlükəsiz istifadəsini təmin edən strategiyaların hazırlanması zəruridir.

Azərbaycanda elektron jurnalların tətbiqi əsasən beynəlxalq təcrübəyə uyğunlaşdırılıb. Xüsusilə Estoniya, Finlandiya kimi ölkələrin rəqəmsal təhsil sistemlərindən ilham alınıb. Bu sistemlərin təhlükəsizlik prinsipləri – məsələn, istifadəçi identifikasiyası, məlumatların şifrələnməsi və sistemə girişin məhdudlaşdırılması – Azərbaycanda da tətbiq olunmağa çalışılıb. Elm və Təhsil Nazirliyi əsasən mərkəzləşdirilmiş elektron idarəetmə modellərindən istifadə edir, bu da məlumatların izlənməsini və idarəsini asanlaşdırır. Amma praktiki tətbiq zamanı

yerli texniki resurslar və infrastruktur, bəzən bu beynəlxalq modellərin tam effektivliyini təmin etməyə imkan vermir.

Bu cür elektron jurnal sistemləri təhsildə şəffaflıq və sürət kimi müsbət cəhətlər gətirsə də, eyni zamanda müxtəlif zəifliklərə də malikdir. Məsələn, saxtakarlıq riski, məlumatların manipulyasiyası, sosial mühəndislik hücumları, sistemin texniki zəiflikləri, məlumatların itirilməsi və ya icazəsiz giriş kimi problemlər önə çıxır.

Beynəlxalq təcrübədə elektron jurnalların kibertəhlükəsizliyi və əsas risklər: Müasir dövrdə bir çox Avropa ölkəsində, xüsusilə də Skandinaviya və Baltik regionlarında təhsil sistemləri rəqəmsallaşma sahəsində ciddi irəliləyişlər əldə edib. Finlandiya, Estoniya kimi ölkələrdə elektron jurnalların tətbiqi yalnız sadə qeydiyyat vasitəsi kimi yox, həm də geniş informasiya axını və təhsil prosesinin şəffaf idarə olunması üçün əsas alət kimi istifadə olunur. Bu sistemlər özlüyündə yüksək səviyyədə kibertəhlükəsizlik tədbirləri tələb edir. Təhlükəsizlik tədbirləri yalnız texniki yanaşmalarla məhdudlaşmır – sosial mühəndislik kimi psixoloji yönümlü təhdidlər də nəzərə alınır. Bu ölkələrin təcrübəsində qarşıya çıxan əsas kibertəhlükəsizlik risklərini aşağıdakı şəkildə ümumiləşdirmək olar:

Birincisi, sosial mühəndislik hücumlarıdır. Bu, texniki zəifliklərdən deyil, insan təsirindən qaynaqlanan bir risk növüdür. Hücumçu istifadəçiləri aldatmaqla, onlardan parolları və ya digər həssas məlumatları əldə etməyə çalışır. Sosial mühəndislik, istifadəçinin diqqətsizliyindən və ya sistemə olan etibarından sui-istifadə etməyə əsaslanır.

İkincisi, məlumatların sızması və dəyişdirilməsi riskidir. Təhlükəsizlik zəifliklərindən istifadə edərək sistemə daxil olan şəxslər qiymətləri dəyişdirir, tələbə məlumatlarını saxtalaşdırır bilirlər. Xüsusilə bu risk, məlumatların şifrələnmədən saxlanıldığı və audit mexanizmlərinin zəif olduğu sistemlərdə yüksək olur.

Üçüncüsü, identifikasiya və autentifikasiya sistemlərinin zəifliyidir. Bir çox ölkə iki mərhələli autentifikasiya (2FA) və ya elektron imza sistemlərindən istifadə edir. Lakin bəzi hallarda istifadəçilər zəif parollar seçir və ya bu əlavə təhlükəsizlik tədbirlərini tətbiq etmirlər. Bu isə sistemə icazəsiz giriş imkanlarını artırır.

Dördüncüsü, təhlükəsizliklə bağlı maarifləndirmənin aşağı səviyyəsidir. Hətta texniki cəhətdən güclü sistemlər belə istifadəçilər bu sistemlərdən düzgün istifadə etmədikdə və riskləri başa düşmədikdə təhlükə altında olur. Bu səbəbdən bir çox ölkədə təhsil sektorunda çalışanlar üçün xüsusi kibertəhlükəsizlik təlimləri keçirilir.

Bu risklərin hər biri ayrı-ayrılıqda vacib olsa da, sosial mühəndislik xüsusilə diqqət edilməli məqamdır. Çünki o, texnologiyanın deyil, insanın zəif nöqtələrinə yönəlir. Bu hücumların qarşısını almaq yalnız texniki vasitələrlə mümkün deyil – burada maarifləndirmə, sistemlərin istifadə rahatlığı və istifadəçi davranışlarının analizi də əsas rol oynayır.

Azərbaycanın təhsil sahəsində elektron jurnallardan istifadə edən, xüsusilə yaşlı nəsil müəllimlərin sosial mühəndislik hücumlarına qarşı daha yaxşı qorunması üçün klassik təlim yanaşmalarından kənara çıxaraq, innovativ və texnoloji əsaslı metodlar təklif edək. Aşağıda bu təkliflər qısa şəkildə təqdim edilir:

1. Girişdə Təhlükəsizlik ipucu: Elektron jurnal sisteminə hər giriş zamanı istifadəçiyə sadə, visual və praktik təhlükəsizlik ipucu göstərilir. Bu, davamlı və gündəlik öyrənməni stimullaşdırır.

2. İnteraktiv mini-testlər: Müəyyən aralıqlarla sistem qısa suallar təqdim edir. Bu testlər müəllimin təhlükəsizlik biliklərini yoxlayır və eyni zamanda maarifləndirici xarakter daşıyır.

4. Səsli təhlükəsizlik mesajları: Sistemdə təhlükəsizlik ipucları vizual yanaşmaya əlavə olaraq, qısa və aydın səsli mesajlarla da təqdim olunur. Bu, xüsusilə oxumaqda çətinlik çəkən yaşlı istifadəçilər üçün əlverişlidir.

5. Parol Gücləndirmə Modulu: Yeni parol yaradılarkən sistem istifadəçiyə parolun gücünü vizual şəkildə yaşıl-sarı-qırmızı şkala şəkildə göstərir və onu daha güclü parol seçməyə təşviq edir.

Bu yanaşmaların həyata keçirilməsi yalnız texniki tədbirlərlə məhdudlaşmır, eyni zamanda təhsil mühitində təhlükəsizlik mədəniyyətinin formalaşmasına xidmət edir. İnnovativ həllərin praktik tətbiqi müəllimlərin gündəlik iş prosesinə inteqrasiya olunduqda, onların davranış modellərində də sabit dəyişikliklər müşahidə olunur. Digər tərəfdən, istifadəçilərin aktiv iştirakı olmadan heç bir texnoloji həllin davamlı nəticə verməyəcəyi unudulmamalıdır. Beləliklə, göstərilən metodlar texnologiya ilə insan amilinin qarşılıqlı tamamlayıcılığını ön plana çıxarır və mövzunun davamlı tədqiqi üçün möhkəm zəmin yaradır.

Elektron jurnalların tətbiqi təhsil sistemində rəqəmsal transformasiyanın əsas istiqamətlərindən biri kimi çıxış edir. Azərbaycanda elektron jurnalların tətbiqi beynəlxalq təcrübəyə əsaslanarsa da, mövcud texniki resurslar bəzi hallarda bu modellərin tam səmərəliliyini məhdudlaşdırır. Xüsusilə sosial mühəndislik hücumları texnoloji zəifliklərdən deyil, insan təsirindən qaynaqlandığı üçün ən aktual təhlükələrdən biri hesab edilir. Bu səbəbdən, yalnız texniki müdafiə mexanizmləri ilə məhdudlaşmaq yetərli deyil, istifadəçilərin maarifləndirilməsi və təhlükəsizlik mədəniyyətinin formalaşdırılması zəruri amil kimi önə çıxır. Təklif edilən innovativ metodlar – təhlükəsizlik ipucları, interaktiv testlər, səsli mesajlar, davranış analizi və parol gücləndirmə modulu – bu istiqamətdə əhəmiyyətli həllər kimi nəzərdən keçirilir.

Problemin aktuallığı. Rəqəmsal texnologiyaların sürətli inkişafı təhsil sistemində yeni imkanlarla yanaşı, müxtəlif təhlükəsizlik çağırışlarını da gündəmə gətirir. Elektron jurnalların geniş tətbiqi tədris prosesində şəffaflıq və səmərəlilik yaratsa da, məlumatların saxtalaşdırılması və kibertəhlükəsizlik riskləri mühüm problem olaraq qalır. Beynəlxalq təcrübədə bu risklərin idarə olunması üçün xüsusi yanaşmalar mövcud olsa da, Azərbaycan şəraitində onların tam tətbiqi əlavə çətinliklərlə müşayiət olunur. Xüsusilə sosial mühəndislik kimi psixoloji əsaslı təhdidlərin artması mövzunun aktuallığını daha da artırır. Buna görə də, elektron jurnalların təhlükəsiz istifadəsini təmin edən strategiyaların işlənilib hazırlanması müasir təhsil sisteminin vacib tələblərindən biridir.

Problemin elmi yeniliyi. Tədqiqatda elektron jurnallardan istifadə edən müəllimlərin sosial mühəndislik hücumlarına qarşı müdafiəsi üçün klassik maarifləndirmə üsullarından fərqli, innovativ yanaşmalar irəli sürülür. Təklif edilən metodlar – girişdə təhlükəsizlik ipucları, interaktiv mini-testlər, səsli mesajlar, davranış analizi və parol gücləndirmə modulu – Azərbaycan təhsil mühitinə uyğunlaşdırılmış yeni yanaşma kimi təqdim olunur. Bu yanaşmalar texniki tədbirlərlə məhdudlaşmır, eyni zamanda təhlükəsizlik mədəniyyətinin formalaşmasını

da hədəfləyir. Elmi yenilik ondan ibarətdir ki, insan amili və texnoloji həllər qarşılıqlı tamamlayıcı şəkildə integrasiya olunur. Nəticədə, müəllimlərin rəqəmsal savadlılığının artırılması və elektron jurnalların daha təhlükəsiz istifadəsi üçün praktiki model irəli sürülür.

Problemin praktik əhəmiyyəti və tətbiqi. Təklif olunan yanaşmalar müəllimlərin rəqəmsal təhlükəsizlik biliklərini gündəlik iş prosesinə integrasiya etməklə onların davranışlarında davamlı pozitiv dəyişikliklər yaradır. Bu metodların tətbiqi elektron jurnalların idarə olunmasında şəffaflığı və etibarlılığı artırır. Təhsil mühitində təhlükəsizlik mədəniyyətinin formalaşması sosial mühəndislik hücumlarının təsirini minimuma endirməyə imkan verir. Eyni zamanda, innovativ həllər yaşlı nəsil müəllimlər üçün daha əlçatan və praktik müdafiə mexanizmi təmin edir. Beləliklə, təqdim edilən yanaşmalar təhsil müəssisələrində kibertəhlükəsizlik risklərinin azaldılmasına real töhfə verir.

Ədəbiyyat

1. Nəbiyeva V. İnnovasiyalı inkişafda rəqəmsal platformaların mövqeyi. Bakı: Azərbaycan Dövlət İqtisad Universiteti, 2021
2. Joachim Bjorge Ulven. Ali təhsildə kibertəhlükəsizlik risklərinin sistematik icmalı. Estoniya: Published, 2021
3. Christopher A. Ocheni. Kibertəhlükəsizlik: imtahan pozuntularının qarşısının alınması və genişmiqyaslı təhsil qiymətləndirmələrinin keyfiyyətinin yaxşılaşdırılması üçün alətdir. London: Onlayn nəşr, 2023
4. Andree Emmanuel Widjaja. Öyrənmə sistemlərində kibertəhlükəsizlik: təhsil informasiya sistemlərində və rəqəmsal öyrənmə mühitlərində məlumatların qorunması və məxfilik. İndoneziya: 2024
5. S. AlDaajeh, H. Saleous, S. Alrabae, E. Barka. Kibertəhlükəsizlik təhsilinin təkmilləşdirilməsində milli kibertəhlükəsizlik strategiyalarının rolu. Estoniya, 2022.

A.E. Mikayılova

Elektron jurnallarda qiymətləndirmə və davamiyyət məlumatlarının saxtalaşdırılmasına qarşı təhlükəsizlik yanaşmaları Xülasə

Elektron jurnal sistemlərinin geniş tətbiqi ilə birlikdə təhsil müəssisələrində məlumat təhlükəsizliyi məsələləri aktuallaşır. Bu məqalədə əsas diqqət qiymətləndirmə və davamiyyət məlumatlarının saxtalaşdırılmasının qarşısını almaq üçün kibertəhlükəsizlik yanaşmalarına yönəldilmişdir. Xüsusilə Azərbaycanda tətbiq edilən elektron jurnal sistemləri və biometrik identifikasiya üsulları kontekstində, bu sistemlərin səmərəliliyi və zəif cəhətləri araşdırılır. Eyni zamanda, sosial mühəndislik hücumları kimi psixoloji əsaslı təhlükələrə qarşı müəllimlərin nə dərəcədə həssas olduğu məsələsinə toxunulur. Müxtəlif yaş qruplarından olan müəllimlərin kibertəhlükəsizlik bilik səviyyələri müqayisə olunur və bu fərqlərin potensial risklərə təsiri təhlil edilir. Mövcud vəziyyəti təhlil etməklə yanaşı, müəllimlərin maarifləndirilməsi və texnoloji

sistemlərin gücləndirilməsi üçün təkliflər də təqdim olunur. Məqalə, həmçinin beynəlxalq təcrübələrə istinad edərək, Azərbaycanda tətbiq oluna biləcək praktik həll yollarını da işıqlandırır. Məqsəd, elektron jurnal sistemlərində məlumatların etibarlılığını təmin etmək və bu sahədə kibertəhlükəsizlik mədəniyyətini gücləndirməkdir.

A.Ə. Микаилова

**Меры безопасности против мошенничества с данными оценок и посещаемости
в электронных журналах
Аннотация**

С широким применением систем электронных журналов вопросы информационной безопасности в образовательных учреждениях становятся все более актуальными. В данной статье основное внимание уделяется подходам к кибербезопасности, направленным на предотвращение фальсификации данных об оценках и посещаемости. В частности, рассматривается эффективность и уязвимости систем электронных журналов и методов биометрической идентификации, применяемых в Азербайджане. Также затрагивается вопрос восприимчивости преподавателей к психологически ориентированным угрозам, таким как атаки социальной инженерии. Наряду с анализом текущей ситуации, в статье предлагаются меры по повышению осведомленности преподавателей и укреплению технологических систем. Кроме того, ссылаясь на международный опыт, рассматриваются практические решения, которые можно применить в условиях Азербайджана. Цель заключается в обеспечении достоверности данных в системах электронных журналов и укреплении культуры кибербезопасности в данной сфере.

A.E. Mikayilova

**Security approaches against grading and attendance data
fraud in electronic journals
Summary**

With the widespread implementation of electronic journal systems, information security issues in educational institutions are becoming increasingly relevant. This article focuses on cybersecurity approaches aimed at preventing the falsification of assessment and attendance data. Specifically, it examines the effectiveness and weaknesses of electronic journal systems and biometric identification methods used in Azerbaijan. It compares the cybersecurity knowledge levels of teachers from different age groups and analyzes how these differences affect potential risks. In addition to analyzing the current situation, the article offers recommendations for increasing teacher awareness and strengthening technological systems. Furthermore, by referencing international experiences, it highlights practical solutions that can be applied in Azerbaijan. The main goal is to ensure the reliability of data in electronic journal systems and to strengthen the culture of cybersecurity in this area.

Redaksiyaya daxil olub: 01.10.2025