İnsan Resursları Sistemlərində İnformasiya Təhlükəsizliyi

Könül Tahirova
Hərbi İdarəetmə İnstitutu, Bakı, Azərbaycan
konul_tahirova@yahoo.com

Xülasə— Məqalədə iqtisadiyyatın qlobal rəqəmsal transformasiyası kontekstində kadr məlumatlarının təhlükəsizliyinin və məxfiliyinin təmin edilməsində müasir informasiya texnologiyalarının kritik rolu tədqiq olunur. Təşkilatların rəqəmsal insan resursları platformalarına keçidi və toplanan şəxsi məlumatların həcminin artması insan resursları sistemlərini kibercinayətkarlar üçün cəlbedici hədəfə çevirir. Məqalədə insan resurslarının idarə edilməsi sistemlərində steqanoqrafik metodların potensialı, eləcə də kriptoqrafik və təşkilati tədbirlərlə yanaşı, məlumatların təhlükəsizliyi strategiyasındakı rolu araşdırılır.

Açar sözlər— informasiya təhlükəsizliyi; insan resursları; rəqəmsal insan resursları təhlükəsizliyi; rəqəmsal transformasiya; steqanoqrafiya

I. GİRİŞ

Müasir dünyada sürətli rəqəmsallaşma prosesi insan resurslarının (İR) idarə edilməsi sahəsində fundamental transformasiyaya səbəb olmuşdur. Belə ki, artıq bütün təşkilatlar işə qəbul və əməkhaqqı hesablanmasından tutmuş, personalın fəaliyyətinin qiymətləndirilməsi və korporativ kommunikasiyaya qədər bütün İR proseslərində rəqəmsal platformalardan intensiv şəkildə istifadə edirlər. İnsan Resurslarının İdarə Edilməsi Sistemləri (İRİS), bulud texnologiyaları və süni intellektin inteqrasiyası həm operativ əməliyyatların, həm də strateji planlaşdırmanın effektivliyini əhəmiyyətli dərəcədə artırmışdır. Bununla belə, rəqəmsal platformalardan artan asılılıq İR məlumatlarının təhlükəsizliyi baxımından ciddi risklər formalaşdırır.

İR strukturları yüksək konfidensiallığa malik böyük həcmdə məlumat axınını – o cümlədən fərdi və bank məlumatlarını, əməkhaqqı reyestrlərini, tibbi arxivləri və fəaliyyətin qiymətləndirilməsi hesabatlarını emal edir. Bu qəbildən olan həssas məlumatların sızması işçilərə aid gizli məlumatların ələ keçirilməsi, maliyyə itkiləri, korporativ nüfuzun zədələnməsi və hüquqi sanksiyalar kimi mənfi nəticələrə yol açа bilər. Konfidensial məlumatların bu dərəcədə təmərküzləşməsi İR strukturlarını kibercinayətkarlar üçün cəlbedici hədəfə çevirir, onları fişinq (*Phishing*) və fidyə proqramları (*Ransomware*) kimi kiberhücumlara qarşı həssas edir.

II. FƏRDİ MƏLUMATLARIN SAXLANILMASI VƏ QORUNMASI

Sürətlənmiş rəqəmsal transformasiya şəraitində işçilərin şəxsi məlumatlarının gizliliyinin təmin edilməsi korporativ təhlükəsizliyin fundamental prioritetlərindən birinə çevrilmişdir. Müasir təşkilati mühitdə işçi heyətinə dair biometrik göstəricilər, davranış analitikası və süni intellekt alqoritmləri tərəfindən generasiya olunan fəaliyyət qiymətləndirilməsi hesabatları daxil olmaqla, irihəcmli verinlənlər toplanır və emal edilir. Parallel olaraq, informasiya texnologiyalarının inkişafı nəticəsində kibertəhdidlərin arxitekturası da təkamül edərək daha mürəkkəb xarakter almışdır. Kibertəhlükəsizlik sahəsində aparılan mövcud statistik tədqiqatlar göstərir ki, fişinq (*Phishing*) kimi kibercinayətkarlıq nəticəsində təşkilatlara dəyən zərər artan templə davam edir. Fərdi məlumatların təhlükəsizliyinin pozulması təşkilatlar üçün aşağıda göstərilən çoxşaxəli və sistemli risklər formalaşdırır [1-7, 9]:

- Maliyyə və hüquqi risklər: hüquqi tənzimləmə mexanizmlərinin pozulması nəticəsində tətbiq edilən yüksək məbləğli inzibati cərimələr və məhkəmə iddiaları;
- Etibarın itirilməsi riski: məlumatların sızması nəticəsində korporativ imicin və bazar nüfuzunun zədələnməsi;
- Sosial-psixoloji risk: təşkilatdaxili etimad mühitinin zəifləməsi və loyallıq səviyyəsinin aşağı düşməsi;
- Fərdi təhlükəsizlik riskləri: işçilərin şəxsinə aid məlumatların (FİN kodu, bank kart nömrəsi və s.) ələ keçirilməsi və maliyyə fırıldaqçılığına məruz qalma ehtimalı;
- Əməliyyat riskləri: fidyə proqramlarının (Ransomware) fəaliyyəti nəticəsində biznes proseslərinin fəaliyyətinin tam və ya qismən dayanması.

Qeyri-kafi kibertəhlükəsizlik tədbirlərinin yaratdığı fəsadlara empirik nümunə kimi *"Hellenic Post Services"* (Yunanıstan Poçt Xidməti) insidentini göstərmək olar. Sözügedən hadisədə *Ransomware* hücumu nəticəsində personalın fərdi məlumatları ələ keçirilmiş və sonradan *"dark net"* platformalarında kütləvi şəkildə yayımlanmışdır [10]. Avropa nəzarət orqanları tərəfindən aparılan təhqiqatlar çərçivəsində Ümumi Məlumatların Mühafizəsi Reqlamentinin *General Data Protection Regulation (GDPR)* tələbləri fonunda müəssisənin texniki və təşkilati təhlükəsizlik arxitekturasında ciddi boşluqlar aşkarlanmışdır [1-3, 7-8]. Bu hadisənin təhlili təsdiq edir ki, insan resursları sektorunda məlumat təhlükəsizliyinin təmin olunması yalnız texnoloji aspektlə məhdudlaşmır; rəqəmsal ekosistemdə bu proses texniki, hüquqi, etik və institusional ölçüləri ehtiva edən multidissiplinar idarəetmə modelini tələb edir.

DOI: 10.25045/forensic.gov.2026.65

Bu kontekstdə işçilərin fərdi məlumatlarının mühafizəsi kritik fəaliyyət istiqamətinə çevrilmişdir. Avropa İttifaqının Ümumi Məlumat Mühafizəsi Reqlamenti *General Data Protection Regulation (GDPR)* kimi hüquqi mexanizmlər məlumatların məxfiliyini və korporativ hesabatlılığı gücləndirmək məqsədi daşıyır. Lakin cari tendensiyaların təhlili göstərir ki, bir çox təşkilatlar hələ də işçilərin fərdi məlumatlarının təhlükəsizliyinin təmin edilməsi və risklərin effektiv idarə olunması istiqamətində institusional çətinliklərlə qarşılaşmaqdadırlar.

Tədqiqat işi insan resurslarının idarə edilməsi (İRİ) ekosistemində fərdi və korporativ məlumatların təhlükəsizliyinə yönəlmiş fundamental təhdidlərin sistemli təhlilinə həsr olunmuşdur. Tədqiqat çərçivəsində baş vermiş kiberinsidentlərin retrospektiv nümunə təhlili (*Case Study*) aparılmış, potensial preventiv əks-tədbirlər modulu işlənmiş və məlumatların konfidensiallığının təmin edilməsində steqanoqrafik metodların tətbiq imkanları elmi-praktiki cəhətdən qiymətləndirilmişdir.

İnsan resurslarının idarə edilməsi sistemlərində məlumat təhlükəsizliyinə yönəlmiş konseptual təhdidlər sırasına hədəfli kiberhücumlar və fərdi məlumatların sızması, insan amilindən qaynaqlanan səhvlər, uzaqdan iş rejimi ilə bulud texnologiyalarının tətbiqindən irəli gələn risklər və daxili (insayder) təhlükələri daxildir [11].

Kiberhücumlar insan resurslarının idarə edilməsi (İRİ) sferasında məlumatların təhlükəsizlik sistemləri üçün əsas təhlükə mənbələrindən biridir. Hədəfli kiberhücumlar korporativ verilənlər bazalarına icazəsiz girişin təmin edilməsinə yönəlmiş zərərverici proqram təminatı (ZPT), fidyə proqramları (Ransomware), fişinq və sosial mühəndislik metodları daxil olmaqla, geniş spektrli vektorlar vasitəsilə reallaşdırılır. İR strukturlarının yüksək həssaslığı onların operativ fəaliyyətinin spesifikası, xüsusilə də konfidensial məlumatların lazımi şifrələmə formaları tətbiq edilmədən elektron poçt kanalları vasitəsilə intensiv şəkildə mübadilə olunması ilə şərtlənir.

İnformasiya təhlükəsizliyi insidentlərinin qlobal statistikası dayanıqlı artım tendensiyası nümayiş etdirir və hər il milyonlarla subyektin fərdi məlumatlarının bədniyyətli şəxslərin əlinə keçməsinə səbəb olur. Müasir kibercinayətkar qruplaşmalar zəif parol siyasəti və ya çoxfaktorlu autentifikasiyanın tətbiq olunmaması ilə bağlı boşluqlardan yararlanaraq bulud servislərini prioritet hədəf kimi müəyyənləşdirirlər. 2024-cü ildə *"Snowflake"* bulud platformasında qeydə alınan və çoxsaylı korporativ müştərilərinə aid şəxsi məlumatların sızması ilə nəticələnən irimiqyaslı hadisə, xarici kiberhücumların insan resurslarına aid verilənlərin təhlükəsizliyinə törətdiyi təhdidlərin bariz nümunəsidir [12]. Bu hadisə kibertəhlükəsizlik arxitekturasındakı struktur çatışmazlıqların korporativ sektorda fərdi məlumatların icazəsiz ifşası risklərini birbaşa stimullaşdırdığı tezisini təsdiqləyir.

İnsan resurslarının idarə edilməsində insan səhvi məlumat sızmalarının əsas səbəbi olaraq qalır. Bu işçilərin gündəlik fəaliyyəti zamanı yol verdiyi təsadüfi xətalar, o cümlədən gizli sənədlərin qeyri-səlahiyyətli ünvanlara və açıq rabitə kanalları vasitəsilə göndərilməsi, zəif parol siyasətinin yürüdülməsi və ya müəyyən edilmiş korporativ təhlükəsizlik tələblərinin pozması formalarında təzahür edir. İnsan amili risklərinə bariz nümunə kimi, 2024-cü ildə Şimali İrlandiya Polis İdarəsində (PSNI) fərdi məlumatların kütləvi şəkildə ifşası ilə nəticələnən irimiqyaslı hadisəni göstərmək olar. Cədvəl prosessorunda verilənlərin emalı zamanı yol verilmiş səhv ucbatından təxminən 9500 əməkdaşın şəxsiyyətinə aid, o cümlədən adları, xidməti funksiyaları və struktur-təşkilati məlumatlarına icazəsiz giriş imkanı yaranmışdır. Nəticədə həmin idarəyə informasiya daxili proseslərin institusional qeyri-adekvatlığı və təhlükəsizlik sistemindəki nəzarət mexanizmlərinin zəifliyini əsas gətirilərək 750 000 funt-sterlinq məbləğində inzibati cərimə tətbiq olunması proseduruna başlanmışdır [13].

COVID-19 pandemiyasından sonrakı dövrdə distant (məsafədən) iş modellərinin kütləviləşməsi kibertəhdidlərin miqyasını və müxtəlifliyini əhəmiyyətli dərəcədə genişləndirmişdir. Korporativ resurslara daxil olmaq üçün fərdi cihazlardan (*BYOD – Bring Your Own Device* konsepsiyası) və qeyri-təhlükəsiz ictimai şəbəkələrdən intensiv istifadə edilməsi təşkilatların perimetral müdafiə sistemlərində yeni zəifliklər formalaşdırır. Bulud texnologiyaları əməliyyat çevikliyi və resurs əlçatanlığı təmin etsə də, eyni zamanda icazəsiz giriş, üçüncü tərəflərlə bağlı risklər (*Third-Party Risks*) və verilənlərin transsərhəd hərəkəti ilə bağlı hüquqi-texniki xarakterli konfidensiallıq problemləri yaradır. Empirik tədqiqatlar göstərir ki, bulud xidmətlərinin qeyri-kafi konfiqurasiyası və etibarsız distant giriş protokolları müasir dünyada məlumatların sızması hadisələrin kökündə dayanan əsas səbəblərdir.

Bütün təhdidlər xarici hakerlərdən gəlmir. Narazı və ya diqqətsiz işçilər qəsdən və ya bilmədən məxfi məlumatları sızdıra bilərlər. Daxili təhdidlər xüsusilə təhlükəlidir, çünki daxili şəxslərin artıq sistemlərə icazəli girişi var. Təkrarlanan məlumat sızmaları ilə qarşılaşan təşkilatlar tez-tez zəif daxili nəzarət və qeyri-kafi monitorinq mexanizmlərindən əziyyət çəkirlər. "Verizon DBIR" (*Data Breach Investigations Report*) hesabatının analitik məlumatlarına əsasən, informasiya sızması insidentlərinin təqribən üçdə bir hissəsi daxili subyektlərin (insayderlərin) fəaliyyəti ilə şərtlənir. Parallel olaraq, *"Securonix"* tərəfindən aparılan tədqiqatların nəticələri göstərir ki, müəssisələrin 76%-i insayder mənşəli kiberhücumların dinamikasında artım müşahidə edir. Bu kontekstdə fundamental elmi və praktiki əhəmiyyət kəsb edən əsas məqam ondan ibarətdir ki, sistemdaxili risklərin əsas hərəkətverici qüvvəsi gizli məlumatların qəsdən oğurlanması cəhdləri deyil, məhz istifadəçi diqqətsizliyi və operativ insan səhvləridir. Statistik göstəricilər də təsdiq edir ki, insayder faktorundan qaynaqlanan bütün kiberinsidentlərin 55%-i birbaşa qeyri-bəsirətli daxili subyektlərin xətaları nəticəsində reallaşır.

Gizli HR (İnsan Resursları) məlumatlarının qorunmasında steqanoqrafiya metodlarının tətbiqi getdikcə daha mühüm strateji əhəmiyyət kəsb edir. Verilənlərin semantik məzmununu gizlədən kriptoqrafik üsullardan (şifrələmədən) fərqli olaraq, steqanoqrafiya birbaşa informasiyanın mövcudluğu faktının özünü gizlətməyə yönəlmişdir. Rəqəmsal steqanoqrafiya çərçivəsində gizli verilənlər vizual və ya struktur dəyişikliyinə məruz qalmadan qrafik təsvirlərin, audio və video faylların, yaxud sənədlərin daxilinə inteqrasiya edilir (embedding). Bu metodoloji yanaşma kibertəhdid subyektlərinin media fayl daxilində kritik məlumatların mövcudluğundan şübhələnmə riskini minimuma endirərək əlavə bir təhlükəsizlik təbəqəsini

formalaşdırır.

Steqanoqrafik üsullar İnsan Resurslarının idarə edilməsi sistemlərində (HRMS) məlumat təhlükəsizliyini aşağıdakı funksional istiqamətlər üzrə dəstəkləyir:

- İşçilərin şəxsi gizli məlumatların təhlükəsiz ötürülməsi: Məsələn, məxfi əmək sənədləri rəqəmsal qrafik obyektlərin daxilinə gizlədilərək ötürülür və bu zaman xarici müdaxilə baş versə belə, kiberfırıldaqçılar tərəfindən gizli məlumatın aşkarlanması ehtimalı kəskin şəkildə aşağı düşür;
- Əməkhaqqı və maliyyə məlumatlarının mühafizəsi.

Steqanoqrafik üsullarının tətbiqi dinamikasını optimallaşdırmaq üçün onun aşağıda göstərilən üstünlük və məhdudiyyətlərini balanslaşdırılmış şəkildə qiymətləndirilməlidir (Cədvəl 1).

CƏDVƏL 1. STEQANOQRAFİK ÜSULLARININ TƏTBİQİNİN ÜSTÜNLÜKLƏRİ VƏ MƏHDUDİYYƏTLƏRİ

Üstünlüklər	Məhdudiyyətlər
Yüksək konfidensiallıq səviyyəsi: Məlumatın həm məzmunu, həm də varlığı eyni anda qorunur.	Məhdud tutum həcmi: Media fayllarının daxili strukturu yalnız müəyyən ölçüdə gizli məlumat qəbul edə bilir.
Aşkarlanma riskinin minimuma enməsi*:* Hücum edən tərəfin hədəf obyekti vizual olaraq ayırd etməsi çətinləşir.	Keyfiyyət itkisi riski: Rəqəmsal daşıyıcının konteyner strukturunda bəzi vizual və ya akustik pozuntular yarana bilər.
Klassik şifrələmədən kənar multidissiplinar müdafiə*:* Əlavə təhlükəsizlik arxitekturası təmin edilir.	Steqoanaliz təhlükəsi: Müasir məhkəmə-kiber (*Forensic*) alətləri vasitəsilə gizli məlumatların deteksiya edilməsi mümkündür.
Kibercasusluq hücumları ssenarilərinə qarşı effektiv müqavimət	Tətbiq mürəkkəbliyi: Sistemin korporativ infrastruktura inteqrasiyası yüksək texnoloji resurs tələb edir.

İnsan resursları məlumatlarının qorunmasında steqanoqrafik üsullarının əsas tətbiq sahələri:

Rəqəmsal su nişanı (Watermarking): əqli mülkiyyətin qorunması. Sızma halında müəllifliyi sübut etmək üçün məlumatlara gizli bir işarə əlavə olunur.

Bütövlüyə nəzarət: məlumatların müdaxilə edənlər tərəfindən dəyişdirilmədiyini yoxlamaq.

Gizli ünsiyyət: qanuni SQL sorğuları və cavabları daxilində parolların və ya şifrələmə açarlarının ötürülməsi.

NƏTİCƏ

Sürətli rəqəmsallaşma şəraitində işçilərin şəxsi məlumatlarının təhlükəsizliyinin təmin edilməsi müasir idarəetmə və kibertəhlükəsizlik sahəsinin ən aktual prioritetlərindən birinə çevrilmişdir. Böyük həcmli gizli məlumatların saxlanılması və emalı üçün rəqəmsal sistemlərdən intensiv istifadə edən təşkilatlar; kiberhücumlar, insan amili (operativ xətalar), insayder təhdidləri və bulud infrastrukturlarının daxili zəifliklərı də daxil olmaqla çoxvektorlu risk ssenariləri ilə qarşı-qarşıyadırlar. Qlobal miqyasda qeydə alınmış son kütləvi məlumat sızması hadisələri empirik olaraq sübut edir ki, qeyri-kafi kibermüdafiə mexanizmləri müəssisələr üçün ciddi maliyyə itkiləri, hüquqi sanksiyalar və nüfuzdan düşmə ilə nəticələnir. İnsan resurslarına dair verilənlərin effektiv mühafizə strategiyası; mütərəqqi texnoloji həllərin inteqrasiyası, işçilərin sistemli şəkildə təlimatlandırılması, tənzimləyici hüquqi normativlərin icrasına ciddi nəzarət və korporativ məsuliyyət mədəniyyətinin formalaşdırılması prinsiplərinə əsaslanmalıdır.

Bu kontekstdə steqanoqrafik metodlar gizli məlumatların rəqəmsal daşıyıcıların daxilində gizlədilməsini təmin edərək, mövcud müdafiə sistemlərinin gücləndirilməsində innovativ yanaşma formalaşdırır. Özünəməxsus struktur məhdudiyyətlərinə baxmayaraq, steqanoqrafiya ənənəvi kriptoqrafik (şifrələmə) üsullar və müasir kibertəhlükəsizlik praktikaları ilə sintez olunduqda, şəxsi məlumatların ümumi mühafizə təbəqəsini əhəmiyyətli dərəcədə yüksəltmək potensialına malikdir. Strateji perspektivdə təşkilatların innovativ kibertəhlükəsizlik texnologiyalarının işlənib hazırlanmasına investisiya yatırması, süni intellektin analitik potensialından faydalanması və əməkdaşların kiber-məlumatlılıq proqramlarını inkişaf etdirməsi zəruridir. Bu yanaşma, insan resursları sistemlərində verilənlərin gizliliyini, bütövlüyü və əlçatanlığının fundamental üçbucağını qoruyub saxlamaq üçün həlledici şərtdir.

ƏDƏBİYYAT

[1] Azərbaycan Respublikasının "Şəxsi məlumatlar haqqında" Qanunu. – 2010, – 20 s.

[2] "Fərdi məlumatların mühafizəsinə dair Tələblər"in təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin qərarı. – Bakı şəhəri, – 6 sentyabr 2010-cu il – nömrə 161.

[3] "Hökumət buludu"nun (G-cloud) yaradılması və "bulud" xidmətlərinin göstərilməsi sahəsində tədbirlər haqqında Azərbaycan Respublikası Prezidentinin Fərmanı. – Bakı şəhəri, – 3 iyun 2019-cu il – № 718.

[4] M. Novruzova, K. Tahirova, İnformasiya texnologiyaları kontekstində insan resursları məlumatlarının təhlükəsizliyi. // Ümummilli lider Heydər Əliyevin anadan olmasının 103 illiyinə həsr olunmuş "Fövqəladə hallarla mübarizənin aktual problemləri" adlı XI elmi-texniki konfransın materialları, – Bakı: Fövqəladə Hallar Nazirliyi Akademiyası, 7 may, – 2026, – 5 s.

[5] A.M. Mustafayeva, Şəbəkə təhlükəsizliyi. Dərslik. - Bakı, - AKTA, MDU, - 2024.

[6] X.İ.Abdullayev, N.T.Nağıyev, R.M. Muxtarov, Müəssisənin informasiya təhlükəsizliyi /Dərslik. – Bakı, MAA-nın Poliqrafiya Mərkəzi. 2019, – 270 səh.

[7] D. B. Parker Fighting Computer Crime: A New Framework for Protecting Information. – Wiley, – 1998. – pp.532

[8] Information security, cybersecurity and privacy protection – Information security management systems. ISO/IEC 27001, – 2022.

[9] European Data Protection Board (EDPB). Hellenic SA: fine on a company for failure to implement technical and organisational measures resulting in unauthorised access by third parties. 2024.

[10] P. Srivastava, Kirti. Cyber security challenges in human resource technology: protecting employee data in the digital age. Journal of Social Review and Development, 2025; 4 (Special Issue 1) : 114-121. doi:10.64171/JSRD.4.S1.114-121.

[11] Cost of a Data Breach Report 2025. (Статистика и экономическое обоснование ИТ-защиты). – IBM Security, – 2025.

[12] Lizzie Danielson. Snowflake Data Breach. Huntress; https://www.huntress.com/threat-library/data-breach/snowflake-data-breach

[13] Information Commissioner's Office (ICO). What price privacy? Poor PSNI procedures culminate in £750k fine. 2024 Oct 3

[14] Nathan House. Insider Threat Statistics [2026]: Costs, Trends & Key Data. May 2026. https://app.stationx.net/articles/insider-threat-statistics

Protection of Human Resources DATA in the Context of Information Security

Konul Tahirova
Military Administration Institute, Baku, Azerbaijan
konul_tahirova@yahoo.com

Abstract- This article examines the critical role of modern information technologies in ensuring the security and privacy of personal data in the context of the global digital transformation. The transition of organizations to digital HR platforms and the increasing volume of collected personal data make HR departments an attractive target for cybercriminals.
.

This article provides a detailed classification and analysis of the main information security threats, focusing on two main risk categories: internal threats associated with deliberate leaks or illegal actions by employees, and external cyberattacks, including phishing, ransomware, and social engineering. It also analyzes modern information security methods, highlighting steganographic methods as a promising approach for ensuring the confidentiality of classified information. Also the potential of steganographic methods in HR management systems is explored.

Keywords- information security; human resources; digital human resources security; digital transformation; steganography