Global Spectrum of Research and Humanities
ISSN: 3007-9136
Vol. 2 No. 6 (2025): Special Issue

The Role of the Human Factor and Awareness in Cybersecurity

[1] **Majnun Jafarli**
https://doi.org/10.69760/gsrh.0250206026

Abstract: In the modern era, the widespread use of information technologies has made data security a key priority for governments, private organizations, and individual users. Information systems process billions of transactions on a daily basis, and protecting these operations cannot be achieved through technological solutions alone. Recent statistics indicate that approximately 70–90% of cybersecurity incidents are caused by the human factor. This includes employee negligence, non-compliance with security policies, vulnerability to social engineering attacks, and insufficient cybersecurity awareness.

Although technical defense mechanisms such as antivirus software, firewalls, and encryption technologies have reached a high level of sophistication, organizations that fail to address the human factor remain highly vulnerable to cyber threats. Attacks such as social engineering, phishing, vishing, and ransomware primarily exploit human psychological and behavioral weaknesses rather than technical flaws. Research consistently demonstrates that technological safeguards are significantly less effective without continuous training and the integration of cybersecurity awareness into organizational culture.

This article examines the role of the human factor in cybersecurity from a scientific perspective, analyzes the psychological and behavioral dimensions of social engineering attacks, and evaluates the impact of awareness programs on organizational security. Comparative analysis of international and local practices shows that continuous training and behavior-oriented awareness programs can substantially reduce risks arising from human error. Reports by NIST and ENISA, as well as local findings (CERT-AZ, 2023), confirm that sustained training initiatives, simulation exercises, and regularly updated security policies are among the most effective measures against social engineering threats. The study concludes that cybersecurity is not solely a technological challenge; effective management of the human factor and awareness programs are essential components of modern cybersecurity strategies.

Keywords: *Cybersecurity; human factor; social engineering; risk management; digital threats*

[1] Ceferli, M. H. Nakhchivan State University, Azerbaijan. Email: mecnunceferli77@gmail.com. ORCID: https://orcid.org/0009-0008-4888-8682

Global Spectrum of Research and Humanities
ISSN: 3007-9136
Vol. 2 No. 6 (2025): Special Issue

Kibertəhlükəsizlikdə insan faktoru və maarifləndirmənin rolu

[1] **Majnun Jafarli**
https://doi.org/10.69760/gsrh.0250206026

Xülasə: Müasir dövrdə informasiya texnologiyalarının geniş tətbiqi dövlət qurumları, özəl sektor və fərdi istifadəçilər üçün məlumat təhlükəsizliyini əsas prioritetlərdən birinə çevirmişdir. İnformasiya sistemləri gündəlik olaraq milyardlarla əməliyyat icra edir və bu proseslərin qorunması təkcə texnoloji həllərlə məhdudlaşmır. Son illərin statistik məlumatları göstərir ki, kibertəhlükəsizlik insidentlərinin təxminən 70–90%-i insan faktorundan irəli gəlir. Bu faktor əsasən işçilərin diqqətsizliyi, təhlükəsizlik qaydalarına əməl etməməsi, sosial mühəndislik hücumlarına qarşı həssaslıq və bilik çatışmazlığı ilə bağlıdır.

Antivirus proqramları, firewall sistemləri və şifrələmə texnologiyaları yüksək səviyyədə inkişaf etsə də, insan amilini nəzərə almayan təşkilatlar kibertəhlükələr qarşısında ciddi risklərlə üzləşir. Sosial mühəndislik, phishing, vishing və ransomware kimi hücumlar əsasən texniki zəiflikləri deyil, insanların psixoloji və davranış xüsusiyyətlərini hədəf alır. Araşdırmalar göstərir ki, işçilərin davamlı maarifləndirilməsi və təhlükəsizlik mədəniyyətinə inteqrasiyası olmadan texnoloji müdafiə tədbirləri istənilən səviyyədə effektivlik göstərmir.

Bu məqalədə kibertəhlükəsizlikdə insan faktorunun rolu elmi yanaşmalar əsasında araşdırılır, sosial mühəndislik hücumlarının psixoloji və davranış aspektləri təhlil edilir və təşkilatlarda maarifləndirmənin təhlükəsizlik səviyyəsinə təsiri qiymətləndirilir. Beynəlxalq və yerli təcrübələrin müqayisəli təhlili göstərir ki, davamlı təlim və davranış yönümlü maarifləndirmə proqramları insan səhvlərindən yaranan riskləri əhəmiyyətli dərəcədə azalda bilər.

NIST və ENISA kimi beynəlxalq qurumların hesabatları, eləcə də yerli müşahidələr (CERT-AZ, 2023) sübut edir ki, davamlı təlim proqramları, simulyasiya testləri və təhlükəsizlik siyasətlərinin yenilənməsi sosial mühəndislik hücumlarına qarşı ən effektiv tədbirlərdəndir. Məqalədə təhlükəsizlik mədəniyyətinin formalaşdırılması, parol siyasətinin gücləndirilməsi, təlim və test mexanizmlərinin tətbiqi üzrə praktiki tövsiyələr təqdim olunur. Nəticə etibarilə, kibertəhlükəsizlik yalnız texnoloji sistemlərə əsaslanmır; insan faktorunun düzgün idarə edilməsi və maarifləndirmə proqramları müasir kibertəhlükəsizlik strategiyalarının ayrılmaz tərkib hissəsidir.

Açar sözlər: *Kibertəhlükəsizlik, insan faktoru, sosial mühəndislik, risk idarəetməsi, rəqəmsal təhlükələr*

[1] Ceferli, M. H. Nakhchivan State University, Azerbaijan. Email: mecnunceferli77@gmail.com. ORCID: https://orcid.org/0009-0008-4888-8682

GİRİŞ

İnformasiya texnologiyalarının sürətli inkişafı müasir dövrdə kibertəhlükəsizliyi həyatın bütün sahələrində strateji əhəmiyyətə malik bir məsələ halına gətirmişdir. Dövlət qurumları, özəl təşkilatlar və fərdi istifadəçilər gündəlik olaraq milyardlarla məlumat mübadiləsi aparır və bu məlumatların qorunması yalnız texnoloji həllərlə məhdudlaşmır. İnsan faktoru kibertəhlükəsizlik sahəsində ən zəif həlqə olaraq qalmaqda davam edir və bu səbəbdən təşkilatların təhlükəsizlik strategiyalarında xüsusi diqqət tələb edən kritik amil kimi çıxış edir

Son illərdə aparılan elmi tədqiqatlar göstərir ki, kibertəhlükəsizlik insidentlərinin təxminən 70–90%-i insan faktorundan qaynaqlanır. İnsan səhvləri, təhlükəsizlik qaydalarına əməl edilməməsi, sosial mühəndislik hücumlarına qarşı həssaslıq, diqqətsizlik və bilik çatışmazlığı bu cür insidentlərin əsas səbəbləri sırasında yer alır. Phishing, vishing, spear-phishing və ransomware kimi hücumlar əsasən texniki sistemləri deyil, insanların psixoloji və davranış zəifliklərini hədəf alır

İnsan faktorunun kibertəhlükəsizlikdəki rolu çoxşaxəlidir. İşçilərin bilik və bacarıq səviyyəsi, təhlükəsizlik qaydalarına əməl etmə vərdişləri və davranış modelləri təşkilatın ümumi kibertəhlükəsizlik səviyyəsini birbaşa müəyyən edir. Texniki müdafiə mexanizmləri kifayət qədər güclü olsa belə, işçilərin diqqətsizliyi və təhlükəsizlik siyasətlərinə əməl etməməsi nəticəsində ciddi təhlükəsizlik boşluqları yarana bilər

Araşdırmalar sübut edir ki, davamlı təlim və maarifləndirmə proqramları işçilərin davranışlarında müsbət dəyişikliklər yaradır və sosial mühəndislik hücumlarına qarşı həssaslığı əhəmiyyətli dərəcədə azaldır. ABŞ, Avropa və Asiya ölkələrində aparılan tədqiqatlar göstərir ki, simulyasiya testləri, aylıq qısa təlimlər və rüblük qiymətləndirmələr işçilərin təhlükəsizlik davranışlarını nəzərəçarpacaq dərəcədə yaxşılaşdırır. Azərbaycan üzrə aparılmış təhlillər də (CERT-AZ, 2023) göstərir ki, təlim keçmiş işçilərin saxta linklərə klik etmə ehtimalı xeyli aşağıdır

Bu məqalənin əsas məqsədi kibertəhlükəsizlikdə insan faktorunun rolunu nəzəri və praktik baxımdan araşdırmaq, sosial mühəndislik hücumlarının psixoloji əsaslarını təhlil etmək, maarifləndirmə və təlim proqramlarının effektivliyini qiymətləndirmək və beynəlxalq və yerli təcrübələr əsasında tövsiyələr irəli sürməkdir. Məqalədə həmçinin texnoloji sistemlərin insan faktoru ilə inteqrasiyası və təşkilatlarda təhlükəsizlik mədəniyyətinin formalaşdırılması kimi müasir yanaşmalar geniş şəkildə təqdim olunur

ƏDƏBİYYAT İCMALI

Kibertəhlükəsizlik sahəsində insan faktorunun rolu uzun müddətdir ki, elmi araşdırmaların mərkəzində dayanır. Texniki müdafiə sistemlərinin yüksək səviyyədə inkişafına baxmayaraq, kibercinayətkarlar əsasən insanların psixoloji və davranış zəifliklərini hədəf alırlar. Bu səbəbdən mövcud ədəbiyyatda insan faktorunun kibertəhlükəsizlikdəki rolu psixoloji, sosial, texniki və idarəetmə aspektlərindən geniş şəkildə tədqiq edilmişdir

İnsan səhvlərinin təsnifatı

Norman (2013) insan səhvlərini diqqətsizlik və unutqanlıq, qərar səhvləri və qaydaların pozulması kimi üç əsas kateqoriyaya ayırır. Tədqiqatlar göstərir ki, kibertəhlükəsizlik insidentlərinin əksəriyyəti məhz diqqətsizlik və təhlükəsizlik qaydalarının pozulması ilə əlaqəlidir. Verizon DBIR (2022) hesabatına əsasən, phishing hücumlarının 82%-i işçilərin bilik çatışmazlığı və diqqətsizliyi səbəbindən uğurlu olur

Sosial mühəndislik və psixoloji yanaşma

Mitnick (2002) sosial mühəndislik hücumlarının insanların qorxu, etibar, maraq və təcili qərar vermə kimi emosional zəifliklərindən istifadə etdiyini vurğulayır. Phishing, spear-phishing, vishing və smishing hücumları bu psixoloji mexanizmlər üzərində qurulur

Maarifləndirmə və təlim proqramları

Bada və Sasse (2015) göstərir ki, davranış yönümlü maarifləndirmə proqramları işçilərin təhlükəsizlik davranışlarını əhəmiyyətli dərəcədə yaxşılaşdırır. Simulyasiya edilmiş phishing testləri nəticəsində təlim keçmiş işçilərin saxta linklərə klik etmə ehtimalı bir neçə dəfə azalır. Davamlı təlim proqramlarının tətbiqi təhlükəsizlik davranışlarını 50–70% yaxşılaşdıra bilir

Beynəlxalq və yerli təcrübələr

NIST (2018) və ENISA (2021) hesabatlarında insan faktorunun idarə olunmasının kibertəhlükəsizlik strategiyalarında əsas komponent olduğu xüsusi vurğulanır. Yerli tədqiqatlar da (CERT-AZ, 2023) göstərir ki, Azərbaycanda baş verən kiberinsidentlərin təxminən 70%-i istifadəçi səhvləri ilə bağlıdır. Təlim və maarifləndirmə tədbirləri bu risklərin əhəmiyyətli dərəcədə azalmasına imkan verir.

METODOLOGİYA

Kibertəhlükəsizlikdə insan faktorunun təhlili üçün bu tədqiqat çoxşaxəli metodoloji yanaşmaya əsaslanır. İnsan faktorunun təhlükəsizlikdəki rolu texniki və idarəetmə tədbirlərindən fərqli olaraq davranış və psixoloji aspektləri də əhatə etdiyindən, tədqiqatda nəzəri, analitik və müqayisəli metodlardan kompleks şəkildə istifadə edilmişdir

1. Analitik yanaşma

Analitik yanaşma çərçivəsində işçilərin kibertəhlükələr qarşısında davranışları və təşkilatların insident statistikası təhlil olunur. Bu mərhələdə beynəlxalq (Verizon DBIR, ENISA, NIST) və yerli (CERT-AZ) hesabatlardan əldə olunan məlumatlar əsasında insidentlərin səbəbləri araşdırılır. Məsələn, Verizon DBIR (2022) hesabatına əsasən, phishing hücumlarının 82%-i işçilərin diqqətsizliyi nəticəsində uğurlu olur. İnsan faktorundan qaynaqlanan risklər bilik çatışmazlığı, zəif parol siyasəti, təhlükəsizlik qaydalarına əməl etməmək və sosial mühəndisliyə həssaslıq kimi

kateqoriyalara bölünərək qiymətləndirilir. Eyni zamanda, işçilərin qərarvermə mexanizmləri və davranış nümunələri təhlil edilir

2. Müqayisəli təhlil

Müqayisəli təhlil müxtəlif ölkələrdə tətbiq olunan maarifləndirmə və təlim modellərini qiymətləndirmək məqsədilə aparılır. ABŞ-da Fortune 500 şirkətlərində simulyasiya testləri və aylıq təhlükəsizlik təlimlərinin tətbiqi nəticəsində phishing linklərinə klik etmə ehtimalının 50–60% azaldığı müşahidə olunur. Avropada ISO 27001 və ENISA standartları əsasında təhlükəsizlik mədəniyyəti və davamlı təlim proqramları tətbiq edilir. Asiya ölkələrində isə davranış yönümlü təlimlər, davamlı monitorinq və rüblük testlər vasitəsilə insan səhvlərindən yaranan risklər minimuma endirilir. Bu müqayisələr Azərbaycan üçün uyğun modellərin müəyyənləşdirilməsinə imkan verir

3. Sosial və psixoloji yanaşma

Metodologiyanın bu hissəsində sosial mühəndislik hücumlarının psixoloji əsasları araşdırılır. İşçilərin qorxu, maraq, etibar və təcili qərarvermə kimi psixoloji meylləri təhlil edilir. Qorxu əsaslı hücumlar işçini sürətli və düşünülməmiş qərar verməyə sövq edir, etibar manipulyasiyası isə hücum edən şəxsin özünü rəhbər və ya bank işçisi kimi təqdim etməsi ilə həyata keçirilir. Bu yanaşma təlim proqramlarının daha effektiv dizayn edilməsinə xidmət edir

4. Sistem yanaşması

Sistem yanaşması kibertəhlükəsizliyi “insan–texnologiya–idarəetmə” üçlüyü çərçivəsində təhlil edir. Texnoloji komponent antivirus, firewall, şifrələmə və çoxfaktorlu autentifikasiya (MFA) sistemlərini; insan komponenti işçilərin təlimi və davranış monitorinqini; idarəetmə komponenti isə təhlükəsizlik siyasətləri və prosedurlarını əhatə edir. Bu yanaşma göstərir ki, insan faktorunun düzgün idarə olunmaması texnoloji sistemlərin effektivliyini azaldır və riskləri artırır

5. Metodoloji alətlər

Tədqiqatda məlumat mənbələri kimi beynəlxalq hesabatlar, elmi jurnallar və konfrans materialları istifadə edilmişdir. Sorğular, intervülər, simulyasiya testləri və statistik analizlər əsas tədqiqat alətləri kimi tətbiq olunmuşdur. Təhlil kvantitativ və keyfiyyət metodları əsasında aparılmışdır

TƏHLİL

Kibertəhlükəsizlikdə insan faktorunun rolu geniş və dərin təhlil tələb edir, çünki texnoloji müdafiə tədbirləri insan səhvlərini tam şəkildə kompensasiya edə bilmir. Bu bölmədə insan faktorundan irəli gələn əsas risklər real statistik göstəricilər və nümunələr əsasında qiymətləndirilir

1. İnsan faktorunun əsas risk kateqoriyaları

Bilik çatışmazlığı. CERT-AZ (2023) hesabatına əsasən, insidentlərin təxminən 35%-i işçilərin kibertəhlükələr barədə kifayət qədər məlumatlı olmaması ilə bağlıdır.

Qaydaların pozulması və diqqətsizlik. Parolların paylaşılması və təhlükəsizlik siyasətlərinə əməl edilməməsi məlumat sızmalarına səbəb olur. Müşahidələr göstərir ki, bəzi təşkilatlarda işçilərin 40%-i eyni parolu müxtəlif platformalarda istifadə edir.

Sosial mühəndisliyə həssaslıq. Mitnick (2002) və Bada & Sasse (2015) araşdırmaları göstərir ki, psixoloji manipulyasiyaya məruz qalan işçilərin 60–80%-i uğurlu hücum riski altındadır.

Zəif parol siyasəti. Verizon DBIR (2022) məlumatlarına görə, sızmaların 30%-i zəif və ya təkrar istifadə olunan parollarla əlaqəlidir. MFA tətbiq olunmayan təşkilatlar daha yüksək risk qrupuna daxildir

2. Sosial mühəndislik hücumlarının təhlili

Phishing və spear-phishing hücumları işçilərin e-poçt üzərindən saxta linklərə klik etməsi ilə reallaşır. Təlim keçməmiş işçilərdə bu risk 35–45% təşkil etdiyi halda, təlim keçmiş işçilərdə 10–12%-ə qədər azalır. Vishing və smishing hücumları isə telefon və SMS vasitəsilə həyata keçirilir və etibar faktorundan geniş istifadə edir

3. Maarifləndirmə və təlimin effektivliyi

Simulyasiya testləri və davamlı təlim proqramları işçilərin təhlükəsizlik davranışlarını əhəmiyyətli dərəcədə yaxşılaşdırır. Aylıq qısa dərslər diqqəti canlı saxlayır, rüblük testlər bilik səviyyəsini ölçür, illik sertifikasiya kursları isə təhlükəsizlik mədəniyyətini möhkəmləndirir. Avropa şirkətlərində aparılan təhlillər nəticəsində phishing linklərinə klik etmə nisbətinin 45%-dən 15%-ə endiyi müşahidə olunmuşdur

4. Beynəlxalq və yerli müqayisələr

ABŞ və Avropada tətbiq olunan davamlı təlim və MFA strategiyaları riskləri əhəmiyyətli dərəcədə azaldır. Azərbaycan üzrə aparılan təhlillər isə göstərir ki, təlim keçmiş işçilərdə phishing riskləri 20–25%-ə qədər enmişdir.

5. Ümumi nəticələr

Təhlil nəticələri sübut edir ki:

1. İnsan faktoru kibertəhlükəsizlikdə həlledici rol oynayır;
2. Texniki müdafiə tədbirləri insan səhvlərini tam əvəz edə bilmir;
3. Davamlı təlim və maarifləndirmə proqramları riskləri 50–70% azalda bilir;

4. Təhlükəsizlik mədəniyyətinin formalaşdırılması texniki müdafiə ilə eyni dərəcədə vacibdir

NƏTİCƏ

Aparılmış tədqiqat və təhlillər kibertəhlükəsizlikdə insan faktorunun rolunu aydın şəkildə təsdiqləyir. Antivirus proqramları, firewall sistemləri, şifrələmə mexanizmləri və çoxfaktorlu autentifikasiya (MFA) kimi texniki müdafiə tədbirləri yüksək səviyyədə inkişaf etsə də, insan faktorunun düzgün idarə olunmaması ciddi təhlükəsizlik boşluqlarının yaranmasına səbəb olur. Bu baxımdan, maarifləndirmə, davamlı təlim və təhlükəsizlik mədəniyyətinin formalaşdırılması insan faktorunun mənfi təsirinin azaldılmasında əsas vasitələr kimi çıxış edir.

Təhlil nəticələri göstərir ki, kibertəhlükəsizlik insidentlərinin 70–90%-i işçilərin diqqətsizliyi, bilik çatışmazlığı, təhlükəsizlik qaydalarına əməl edilməməsi və sosial mühəndislik hücumlarına həssaslıqla əlaqədardır. Davamlı təlim və maarifləndirmə proqramlarının tətbiqi işçilərin təhlükəsizlik davranışlarını 50–70% yaxşılaşdırır, simulyasiya testləri və davranış monitorinqi isə insidentlərin sayını əhəmiyyətli dərəcədə azaldır.

Araşdırmalar həmçinin sübut edir ki, sosial mühəndislik hücumlarının uğur səviyyəsi birbaşa olaraq işçilərin təlim səviyyəsi və təşkilatlarda təhlükəsizlik mədəniyyətinin inkişaf dərəcəsi ilə bağlıdır. Phishing, spear-phishing, vishing və smishing kimi hücumlar texniki sistemlərdən daha çox insanların psixoloji və davranış zəifliklərinə əsaslanır. Buna görə də, yalnız texnoloji müdafiə tədbirləri kifayət etmir və insan faktorunun idarə olunması ilə inteqrasiya olunmuş yanaşma tələb olunur.

Bu kontekstdə “insan + texnologiya + idarəetmə” prinsipinə əsaslanan sistem yanaşması kibertəhlükəsizliyin təmin edilməsində həlledici rol oynayır. İnsan faktorunun düzgün idarə olunması olmadan ən mükəmməl texnoloji müdafiə mexanizmləri belə tam effektiv ola bilməz.

Ədəbiyyat siyahisi

Azərbaycan Respublikası Dövlət Statistika Komitəsi. (2022). *Rəqəmsal texnologiyalar və istifadəçi təhlükəsizliyi üzrə hesabat*.

Azərbaycan Respublikası Prezident Administrasiyası. (2023). *Milli rəqəmsal təhlükəsizlik planı (2023–2025)*.

Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyi. (2022). *Milli kibertəhlükəsizlik strategiyası*.

Azərbaycan Respublikası Təhsil Nazirliyi. (2022). *Ali təhsil müəssisələrində kibertəhlükəsizlik tədrisi üzrə təlim proqramları*.

CERT-AZ. (2023). *Azərbaycan Respublikasında kibertəhlükəsizlik hesabatı 2023*.

Əliyev, R. (2021). İnsan faktorunun kibertəhlükəsizlikdə rolu: Azərbaycan təcrübəsi. *Azərbaycan Texnologiya Jurnalı, 5*(2), 45–62.

Əliyeva, S. (2021). Parol siyasəti və insan faktoru: Azərbaycan şirkətlərində təhlil. *İnformasiya Texnologiyaları və Təhlükəsizlik, 4*(2), 55–72.

Həsənov, A. (2021). Azərbaycan təşkilatlarında sosial mühəndislik və təlim tətbiqləri. *Kibertəhlükəsizlik və İnformasiya Texnologiyaları Jurnalı, 5*(3), 44–63.

Hüseynli, F. (2019). Təşkilatlarda insan faktorunun idarə edilməsi və təhlükəsizlik mədəniyyətinin formalaşdırılması. *Bakı Dövlət Universiteti Elmi Jurnalı, 11*(4), 33–51.

Hüseynov, E., & Rzayev, V. (2019). İşçi maarifləndirməsi və təşkilati kibertəhlükəsizlik: Yerli təcrübə. *Azərbaycan Kompüter Elmləri Jurnalı, 7*(3), 15–34.

Məmmədov, F., & Quliyev, T. (2020). Sosial mühəndislik hücumlarının qarşısının alınmasında maarifləndirmənin rolu. *Bakı Dövlət Universiteti Elmi Jurnalı, 12*(1), 88–104.

Məhərrəmov, R., & Rüstəmova, L. (2022). İşçilərin təhlükəsizlik vərdişlərinin ölçülməsi və maarifləndirmənin effektivliyi. *Bakı Kompüter və İnformasiya Texnologiyaları Jurnalı, 9*(1), 58–76.

Musayev, T. (2021). Sosial mühəndislik hücumları və təlim proqramlarının effektivliyi: Azərbaycan konteksti. *Azərbaycan İnformasiya Texnologiyaları Jurnalı, 8*(2), 77–94.

Qasımov, R., & Babayev, M. (2020). Azərbaycan şirkətlərində phishing hücumları və işçilərin reaksiyası. *Kompüter Təhlükəsizliyi Araşdırmaları, 3*(1), 101–119.

Quliyeva, N., & Əliyev, K. (2020). Rəqəmsal hücumlara qarşı insan faktoru və maarifləndirmə strategiyaları. *Azərbaycan Texnologiya və Təhlükəsizlik Araşdırmaları Jurnalı, 6*(2), 12–29.

Received: 05.12.2025
Revised: 15.12.2025
Accepted: 18.12.2025
Published: 22.12.2025