

<https://doi.org/10.67471/ITKR6334>

## KİBERMÜDAFİƏ STRATEGİYALARI: İNSAN KAPITALININ İNKİŞAFI VƏ TƏHLÜKƏSİZLİK MEXANİZMLƏRİ

<sup>1,4</sup>Dinarə Şirin qızı İslamova, <sup>2,4</sup>Fatma Mürşüd qızı Əliyeva, <sup>3,4</sup>Məhsəti Rövşən qızı Əliyeva

[dinara.islamova@mdu.edu.az](mailto:dinara.islamova@mdu.edu.az)

[fatma.aliyeva@mdu.edu.az](mailto:fatma.aliyeva@mdu.edu.az)

[mehseti.aliyeva@mdu.edu.az](mailto:mehseti.aliyeva@mdu.edu.az)

<sup>5</sup>Mingəçevir Dövlət Universiteti

**Xülasə:** Rəqəmsal transformasiyanın sürətlənməsi, məlumatların kütləvi şəkildə rəqəmsal mühitə integrasiyası və global şəbəkə infrastrukturunun genişlənməsi kibertəhlükəsizliyi müasir cəmiyyət üçün strateji əhəmiyyət kəsb edən əsas problem sahələrindən birinə çevirmişdir. Müasir təşkilatlar artan kiberhücum intensivliyi, təhdidlərin mürəkkəbləşməsi və kritik informasiya resurslarının yüksək həssaslığı ilə üz-üzədir. Bu məqalə kibertəhlükəsizlik strategiyalarının nəzəri əsaslarını, müdafiə mexanizmlərinin funksional xüsusiyyətlərini və bu prosesdə insan kapitalının rolunu elmi yanaşma çərçivəsində araşdırır.

Tədqiqatın nəticələri göstərir ki, effektiv kibertəhlükəsizlik yalnız texnoloji alətlər və müdafiə sistemləri ilə məhdudlaşmır; o, həmçinin insan resurslarının davamlı təlimini, kadr potensialının institusional səviyyədə gücləndirilməsini, dövlət-özəl sektor əməkdaşlığının optimallaşdırılmasını və adaptiv, risk əsaslı müdafiə arxitekturalarının tətbiqini tələb edir. Məqalə eyni zamanda kibertəhlükələrin dinamik təbiətinə uyğun çevik idarəetmə modellərinin qurulmasının vacibliyini vurğulayır. Beləliklə, əldə olunan nəticələr kibermüdafiə strategiyalarının kompleks, çoxsəviyyəli və davamlı inkişaf edən yanaşma tələb etdiyini təsdiq edir.

**Açar sözlər:** kibermüdafiə strategiyaları, insan kapitalının inkişafı, kibertəhlükəsizlik mexanizmləri, rəqəmsal təhlükələr və risk idarəetməsi, kiberinsidentlərin qarşısının alınması.

### Giriş

Rəqəmsal transformasiyanın sürətlənməsi, məlumat dövryyəsinin genişlənməsi və global kommunikasiya sistemlərinin mürəkkəbləşməsi kibertəhlükəsizlik məsələlərini yeni səviyyəyə qaldırmışdır. Hazırkı şəraitdə informasiya sistemlərinin qorunması təkcə texnoloji yanaşmalarla məhdudlaşmır, həm də idarəetmə, inzibati nəzarət və institusional koordinasiya kimi aspektləri əhatə edir.

Bu kontekstdə kibertəhlükəsizliyin nəzəri-praktik əsaslarının araşdırılması, müdafiə mexanizmlərinin səmərəliliyinin qiymətləndirilməsi və insan kapitalının hazırlıq səviyyəsinin təkmilləşdirilməsi strateji əhəmiyyət kəsb edir. İnkişaf edən rəqəmsal ekosistem kibertəhlükələrin strukturunu daha dinamik, proqnozlaşdırılması çətin və çoxvektorlu formaya saldığı üçün mövzu üzrə kompleks elmi yanaşmanın aktuallığı getdikcə artır.

İnformasiya sistemləri rəqəmsal iqtisadiyyatın əsas infrastrukturunu kimi çıxış etdikcə, kibertəhlükələr daha mürəkkəb və çoxşaxəli xarakter alır. İstər dövlət qurumları, istərsə də özəl sektor üçün kibertəhlükəsizlik artıq əlavə texniki komponent deyil, müəssisənin strateji idarəetmə sahəsinin ayrılmaz hissəsidir.

Nəticədə, kibertəhlükəsizlik strategiyalarının hazırlanması, işçi qüvvəsinin heyət potensialının inkişafı və dayanıqlı müdafiə mexanizmlərinin formalaşdırılması global səviyyədə prioritet məsələlərə çevrilmişdir.

### **Kibertəhlükəsizlik strategiyalarının mahiyyəti: Strateji planlaşdırmanın rolu.**

Kibertəhlükəsizlik strategiyası təşkilatın informasiya aktivlərini qorumaq üçün sistemli, çoxsəviyyəli və uzunmüddətli yanaşmanı ifadə edir. Bu strategiya aşağıdakı məqsədlərə xidmət edir:

- risklərin azaldılması,
- hücum vektorlarının proqnozlaşdırılması,
- davamlılıq və bərpa mexanizmlərinin qurulması,
- normativ və hüquqi tələblərə uyğunluq.

1. Risk əsaslı yanaşma. Müasir kibertəhlükəsizlik modelləri məlumatların dəyərində, həssaslığında və təşkilat üçün kritikliyində əsaslanan risk təhlilini önə çəkir. Risk əsaslı strategiyalar aşağıdakılara əsaslanır:

- təhdid modelləşdirilməsi,
- zəifliklərin identifikasiyası,
- ehtimal və təsir analizinin aparılması.

2. Dövlət və korporativ səviyyədə strategiyalar: Bir çox ölkələrin milli kibertəhlükəsizlik strategiyaları rəqəmsal suverenliyi qorumağı və kiberhücumlara qarşı kollektiv müdafiəni təmin etməyi hədəfləyir. Korporativ mühitdə isə strategiyalar müəssisənin biznes məqsədləri ilə integrasiya edilərək təhlükəsizliyin idarəolunan, ölçüləbilən və davamlı şəkildə təmin olunmasına xidmət edir.

### **İşçi qüvvəsinin inkişafı: İnsan faktorunun rolu.**

Statistik göstəricilərə görə, kibertəhlükəsizlik insidentlərinin böyük hissəsi insan səhvləri, zəif təlim, sosial mühəndislik hücumları və yanlış konfigurasiyalar ilə əlaqədardır. Buna görə kadr potensialının gücləndirilməsi kiber müdafiənin əsas elementidir. Təlim və peşəkar hazırlıq, işçi qüvvəsinin inkişafı üç istiqamətdə həyata keçirilir:

- Texniki hazırlıq: şəbəkə təhlükəsizliyi, kriptografiya, zərərli proqramlar analizi.
- İdarəetmə bacarıqları: risklərin idarə edilməsi, təhlükəsizlik siyasətlərinin tətbiqi.
- Operativ reaksiya: insidentlərin aşkarlanması və cavab mexanizmləri.

**Kadr çatışmazlığı və global çağırışlar:** Dünya üzrə kibertəhlükəsizlik üzrə peşəkarların çatışmazlığı milyonlarla nəfər təşkil edir. Bunun əsas səbəbləri sürətlə dəyişən texniki trendlər, təcrübəli mütəxəssislərin çatışmazlığı, təhsil proqramlarının texnologiya templərinə uyğunlaşmaması.

Bu çatışmazlıq təhlükəsizlik boşluqlarının artmasına səbəb olur və dövlət–özəl sektor əməkdaşlığını zəruri edir.

Müasir müdafiə mexanizmləri: Çoxsəviyyəli müdafiə (Defense-in-Depth). Bu model sistemə birdən çox təbəqə şəklində müdafiə tədbirlərinin tətbiqini nəzərdə tutur:

- şəbəkə firewalları,
- kriptografiya,
- identifikasiya və autentifikasiya sistemləri,
- davranış analitikası,
- məlumatların şifrələnməsi və ehtiyat nüsxələri.

Çoxsəviyyəli müdafiə bir müdafiə xətti dağıdılsa belə, digər səviyyələrin təhlükəsizliyi qorumağa davam etməsinə imkan verir.

**Süni intellekt və avtomatlaşdırılmış müdafiə sistemləri:** Süni intellekt əsaslı təhlükəsizlik sistemləri anomaliyaları real vaxtda aşkarlayır, davranış modellərini analiz edir və hücumları proqnozlaşdırır. Bu texnologiyalar hücumların sürətini aşmaq üçün vacibdir.

**Zero Trust (Sıfır Etimad) modeli:** Zero Trust yanaşması ən çox qəbul edilən müasir müdafiə mexanizmlərindən biridir.

- heç bir quruluşa, istifadəçiyə və ya şəbəkə segmentinə avtomatik etimad edilmir;
- hər addımda autentifikasiya və avtorizasiya tələb olunur;
- minimal imtiyaz prinsipi tətbiq olunur.

Bu model daxili təhdidlərin qarşısını almaqda yüksək effektiv hesab edilir.

**Təhdid kəşfiyyatı (Threat Intelligence):** Bu mexanizm hücum vektorları, zərərli proqramlar, qlobal kiberhücum tendensiyaları haqqında məlumat toplayır və sistemləri əvvəlcədən hazırlıqlı edir.

Kibertəhlükəsizlik strategiyalarının effektivliyi yalnız texnoloji infrastrukturla məhdudlaşmır. İnsan amili, idarəetmə strukturları, təhsil proqramlarının modernləşdirilməsi və real-time təhdid analizləri kibermüdafiənin ayrılmaz komponentləridir. Nəqliyyat, enerji, səhiyyə kimi kritik infrastruktur sahələri üçün bu mexanizmlər daha böyük əhəmiyyət kəsb edir. Elmi yanaşmalar göstərir ki, adaptiv, süni intellektlə gücləndirilmiş və risk əsaslı müdafiə modelləri ən yüksək dayanıqlığa malikdir.

### Nəticə

Kibertəhlükəsizlik strategiyaları müasir rəqəmsal ekosistemdə təşkilatların fəaliyyətinin dayanıqlığını təmin edən əsas struktural çərçivə kimi çıxış edir. Effektiv kibermüdafiə yalnız texnoloji alətlərin tətbiqi ilə məhdudlaşmır; eyni zamanda, işçi qüvvəsinin müasir bacarıqlarla təmin olunması, davamlı peşəkar təlimlərin sistemli şəkildə təşkil edilməsi və çoxsəviyyəli müdafiə mexanizmlərinin inteqrasiyası zəruridir. Bu yanaşma nəticəsində kiberrisiklər minimuma endirilir, insidentlərin qarşısının alınması və sistemlərin bərpa prosesi daha sürətli və effektiv olur.

Məqalədə göstərilənlər kimi, kibertəhlükəsizlik yalnız texniki bir proses deyil, həm də idarəetmə, sosial və iqtisadi aspektləri özündə birləşdirən kompleks və çoxölçülü konsepsiyadır. Bu, təşkilatların strateji planlaşdırma, risk idarəetməsi və davamlı inkişaf proseslərində kibermühafizəni ayrılmaz element kimi nəzərə almalarını tələb edir. Gələcək inkişaf perspektivləri süni intellektin və maşın öyrənməsinin kibermüdafiə alətlərinə inteqrasiyasını, adaptiv təhlükəsizlik arxitekturalarının tətbiqini və beynəlxalq kiber əməkdaşlığın genişləndirilməsini ehtiva edəcəkdir.

Eyni zamanda, kibertəhlükəsizlik sahəsində davamlı elmi tədqiqatlar və kadr potensialının artırılması, təşkilatların texnoloji infrastrukturunun möhkəmləndirilməsi və qlobal kibermühitdə qarşılıqlı məlumat mübadiləsinin effektiv təşkili, gələcəkdə kibermüdafiənin səmərəliliyini daha da yüksəldəcək əsas amillər kimi çıxış edir. Bu yanaşma həm dövlət, həm də özəl sektor üçün strategiyanın çoxsəviyyəli, çevik və davamlı olmasını təmin edərək rəqəmsal ekosistemin dayanıqlığını gücləndirir.

### İstifadə edilmiş ədəbiyyat siyahısı

1. Smith, J., & Coleman, R. 2024. Cyber Defense Strategies and Workforce Competency Development in Digital Organizations. *Journal of Cybersecurity Research*, 18.2, 45–62.
2. Ivanov, A. 2023. Human Capital Formation in Cybersecurity: Challenges and Strategic Priorities. *International Review of Information Security*, 12.4, 77–91.
3. Rahman, M., & Lee, H. 2022. Advanced Cybersecurity Mechanisms: Adaptive Defense Models and Threat Intelligence. *Computers & Security*, 117, 102723.
4. Petrova, N., & Sokolov, D. 2021. Risk Management and Digital Threat Mitigation in Critical Infrastructure Systems. *Information Systems & Control Journal*, 9.1, 55–70.
5. Anderson, T. 2020. Developing Cybersecurity Workforce Capacity: Strategic Approaches for Modern Cyber Defense. *IEEE Security & Privacy*, 18.6, 31–39.

## CYBER DEFENSE STRATEGIES: HUMAN CAPITAL DEVELOPMENT AND SECURITY MECHANISMS

D.Sh.Islamova, F.M.Aliyeva, M.R.Aliyeva  
Mingachevir State University

**Abstract:** The acceleration of digital transformation, the massive integration of data into digital environments, and the expansion of global network infrastructures have made cybersecurity one of the most strategically significant challenges for contemporary society. Modern organizations face increasing cyber-attack intensity, the growing complexity of threats, and the high sensitivity of critical information assets. This paper examines the theoretical foundations of cybersecurity strategies, the functional characteristics of defense mechanisms, and the role of human capital in this process within a scientific framework.

The findings of the study indicate that effective cybersecurity is not limited to technological tools and defense systems; it also requires continuous training of human resources, institutional strengthening of workforce capacity, optimization of public–private sector collaboration, and the implementation of adaptive, risk-based defense architectures. The paper further emphasizes the necessity of establishing flexible management models that align with the dynamic nature of cyber threats. Accordingly, the results confirm that cybersecurity strategies demand a comprehensive, multi-layered, and continuously evolving approach.

**Keywords:** cyber defense strategies, human capital development, cybersecurity mechanisms, digital threats and risk management, prevention of cyber incidents.

## СТРАТЕГИИ КИБЕРОБОРОНЫ: РАЗВИТИЕ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА И МЕХАНИЗМЫ БЕЗОПАСНОСТИ

Д.Ш.Исламова, Ф.М.Алиева, М.Р.Алиева  
Мингячеврский государственный университет

**Резюме:** Ускорение цифровой трансформации, массовая интеграция данных в цифровую среду и расширение глобальной сетевой инфраструктуры сделали кибербезопасность одной из наиболее стратегически значимых проблем современного общества. Современные организации сталкиваются с ростом интенсивности кибератак, усложнением угроз и высокой чувствительностью критически важных информационных ресурсов. В данной статье рассматриваются теоретические основы стратегий кибербезопасности, функциональные характеристики механизмов защиты и роль человеческого капитала в этом процессе в рамках научного подхода.

Результаты исследования показывают, что эффективная кибербезопасность не ограничивается только технологическими инструментами и системами защиты; она также требует постоянного обучения персонала, институционального укрепления потенциала рабочей силы, оптимизации сотрудничества между государственным и частным секторами, а также внедрения адаптивных, основанных на управлении рисками архитектур защиты. В статье также подчеркивается необходимость создания гибких моделей управления, соответствующих динамическому характеру киберугроз. Таким образом, полученные результаты подтверждают, что стратегии кибербезопасности требуют комплексного, многоуровневого и непрерывно развивающегося подхода.

**Ключевые слова:** стратегии киберобороны, развитие человеческого капитала, механизмы кибербезопасности, цифровые угрозы и управление рисками, предотвращение киберинцидентов.