DOI: https://doi.org/10.36719/2789-6919/56/178-183

Tunal Həsənov
Azərbaycan Dövlət Neft və Sənaye Universiteti
magistrant
https://orcid.org/0009-0008-6948-8821
tunalhsnov10@gmail.com

İnformasiya təhlükəsizliyinin strategiyalarının müasir üsullarla tətbiqi problemi

Xülasə

Müasir rəqəmsal mühitdə informasiya təhlükəsizliyinin təmin olunması təşkilatların fəaliyyətinin davamlılığı və etibarlılığı baxımından əsas prioritetlərdən birinə çevrilmişdir. İnformasiya sistemlərinin mürəkkəbləşməsi, kibertəhdidlərin dinamik xarakter alması və hücum metodlarının inkişafı mövcud təhlükəsizlik strategiyalarının yenidən nəzərdən keçirilməsini zəruri edir. Qlobal səviyyədə geniş tətbiq olunan ISO 27001, NIST Cybersecurity Framework, SANS və digər beynəlxalq standartlar informasiya təhlükəsizliyinin təmin olunması üçün metodoloji çərçivə təqdim etsə də, bu standartların bütün təşkilatlar üçün eyni səviyyədə effektiv tətbiqi praktikada mümkün olmur.

Bu məqalədə informasiya təhlükəsizliyi strategiyalarının müasir üsullarla tətbiqi problemləri kompleks şəkildə araşdırılmışdır. Tədqiqat çərçivəsində mövcud beynəlxalq təhlükəsizlik standartları təhlil edilmiş, onların ümumiləşdirilmiş xarakteri, "one-size-fits-all" yanaşmasının məhdudiyyətləri, təşkilati, hüquqi və resurs amillərindən irəli gələn tətbiq problemləri müəyyən olunmuşdur. Xüsusilə dövlət və iri təşkilat mühitində infrastruktur heterogenliyi, maliyyə və insan resurslarının məhdudluğu, hüquqi tənzimləmələr və idarəetmə modelləri təhlükəsizlik strategiyalarının birbaşa tətbiqini çətinləşdirən əsas amillər kimi qiymətləndirilmişdir.

Məqalədə adaptiv təhlükəsizlik modeli konsepsiyası əsaslandırılmış və bu modelin mövcud beynəlxalq standartlarla inteqrasiya olunmaqla praktik mühitə uyğunlaşdırılması imkanları göstərilmişdir. Təklif olunan yanaşma risk əsaslı qərarvermə, təhlükəsizlik yetkinliyi səviyyələrinin nəzərə alınması və mərhələli tətbiq prinsiplərinə əsaslanır.

Açar sözlər: *informasiya təhlükəsizliyi, adaptiv təhlükəsizlik modeli, risk əsaslı yanaşma, kibertəhlükəsizlik strategiyası, təhlükəsizlik yetkinliyi, beynəlxalq standartlar, ISO/IEC 27001, NIST çərçivəsi*

Tunal Hasanov
Azerbaijan State Oil and Industry University
Master's student
https://orcid.org/0009-0008-6948-8821
tunalhsnov10@gmail.com

Challenges in the Implementation of Information Security Strategies through Modern Approaches

Abstract

In today's digital environment, ensuring information security has become a key priority for organizational resilience and reliability. The increasing complexity of information systems, the dynamic nature of cyber threats, and the evolution of attack techniques require security strategies to be regularly reviewed and adjusted. Although widely adopted international standards and frameworks such as ISO/IEC 27001, the NIST Cybersecurity Framework, and SANS controls provide a methodological foundation, their direct "one-size-fits-all" application is often ineffective in real organizational contexts.

This paper examines the main challenges of implementing information security strategies using modern approaches. It analyzes prominent international standards and identifies practical limitations driven by organizational structure, legal and regulatory constraints, heterogeneous infrastructure, and limited financial and human resources – especially in large and public-sector environments. To address these gaps, the paper substantiates an adaptive security model that preserves core principles of international standards while enabling contextual tailoring. The proposed approach is based on risk-informed decision-making, consideration of security maturity levels, and phased implementation. A simple decision mechanism – an Adaptive Security Implementation Index (ASI) – is introduced to support selecting an appropriate implementation mode (baseline, hybrid, or adaptive).

Keywords: *information security, adaptive security model, risk-based approach, cybersecurity strategy, security maturity, international standards, ISO/IEC 27001, NIST Cybersecurity Framework*

Giriş

İnformasiya texnologiyalarının sürətli inkişafı, rəqəmsal xidmətlərin genişlənməsi və məlumat mübadiləsinin intensivləşməsi informasiya təhlükəsizliyini hər bir təşkilat üçün prioritet istiqamətə çevirmişdir. Müasir dövrdə kibertəhdidlər yalnız texniki zəifliklərdən istifadə etməklə məhdudlaşmır; sosial mühəndislik, təchizat zənciri hücumları, daxili təhdidlər, məqsədyönlü və uzunmüddətli hücum ssenariləri (APT) kimi kompleks yanaşmaların artması təhlükəsizlik strategiyalarının daha çevik və sistemli formada qurulmasını tələb edir. Bu şəraitdə informasiya təhlükəsizliyi strategiyası təkcə texniki tədbirlər toplusu deyil, idarəetmə, proses, insan resursu və hüquqi-normativ mühitlə uzlaşdırılmış kompleks idarəetmə mexanizmi kimi formalaşmalıdır.

Qlobal praktikada ISO/IEC 27001, NIST Cybersecurity Framework, SANS və digər standart və çərçivələr təşkilatlarda informasiya təhlükəsizliyinin qurulması üçün metodoloji baza rolunu oynayır. Lakin bu standartlar ümumiləşdirilmiş xarakter daşıdığından "hamı üçün eyni" yanaşma real mühitdə bəzən gözlənilən effekti vermir.

Bu kontekstdə aktual olan yanaşma beynəlxalq standartların üstünlüklərini saxlayaraq onların təşkilati mühitə adaptasiyasını təmin edən modellərin işlənməsidir. Adaptiv yanaşma risk əsaslı qərarvermə, yetkinlik səviyyələrinin nəzərə alınması, mərhələli tətbiq və ölçülə bilən göstəricilər əsasında təhlükəsizlik strategiyasının real şəraitdə qurulmasına imkan verir. Beləliklə, tədqiqatın aktuallığı mövcud standartların tətbiqində qarşıya çıxan uyğunsuzluqların aradan qaldırılması və təşkilatın real risklərinə uyğun, praktik icra oluna bilən təhlükəsizlik strategiyalarının formalaşdırılmasına metodoloji əsas yaratmaq zərurətindən irəli gəlir.

Tədqiqat

İnformasiya təhlükəsizliyi sahəsində qəbul edilmiş beynəlxalq standartlar. İnformasiya təhlükəsizliyi sahəsində beynəlxalq səviyyədə qəbul edilmiş standartlar və metodoloji çərçivələr təşkilatlarda təhlükəsizlik proseslərinin formalaşdırılması üçün vahid yanaşma təqdim edir. Bu standartların əsas məqsədi informasiya aktivlərinin qorunması, risklərin idarə olunması, uyğunluğun təmin edilməsi və təhlükəsizlik idarəetmə sistemlərinin səmərəli təşkilidir. Dünyada ən geniş tətbiq olunan çərçivələr sırasına ISO 27001, NIST Cybersecurity Framework, SANS nəzarətləri, COBIT və Zero Trust modeli daxildir.

1. ISO/IEC 27001: məlumat təhlükəsizliyi idarəetmə sisteminin (ISMS) qurulması, tətbiqi və davamlı təkmilləşdirilməsi üçün çərçivə təqdim edir (ISO/IEC 27001, 2022; Andress, 2019). Standartın əsas elementi risk əsaslı idarəetmədir.

2. NIST Cybersecurity Framework (CSF): ABŞ Milli Standartlar və Texnologiyalar İnstitutu tərəfindən hazırlanmış və beş əsas funksiyanı özündə birləşdirən daha çevik çərçivədir: Identify, Protect, Detect, Respond və Recover (NIST, 2020; NIST, 2012). NIST çərçivəsi daha çox praktiki tətbiq yönümlüdür və müxtəlif növ təşkilatlarda istifadə oluna bilər (ISO/IEC 27001, 2022).

Şəkil 1. NIST çərçivəsinin mərhələləri

3. SANS Top 20 Security Controls: təşkilatların təhlükəsizlik nəzarətlərini prioritetləşdirmək üçün hazırlanmış praktik tövsiyələr toplusudur (SANS Institute, 2020; CIS, 2021). Bu nəzarətlər hücumların qarşısının alınmasına, aşkarlanmasına və cavab tədbirlərinin müəyyən edilməsinə yönəlmiş konkret texniki və prosedur tədbirləri əhatə edir.

4. COBIT (Control Objectives for Information and Related Technologies): əsasən IT idarəetməsi və uyğunluğa yönəlmiş çərçivədir. COBIT informasiya texnologiyalarının biznes məqsədlərinə uyğunlaşdırılması, idarəetmə mexanizmlərinin tənzimlənməsi və audit proseslərinin struktur-laşdırılması üçün nəzərdə tutulub.

Müasir texnologiyalar və onların təhlükəsizlik strategiyalarının formalaşmasına təsiri. Rəqəmsal transformasiya nəticəsində təşkilatların infrastrukturunda baş verən dəyişikliklər informasiya təhlükəsizliyi strategiyalarının formalaşdırılmasına birbaşa təsir göstərir. Müasir texnologiyaların sürətli inkişafı yeni imkanlar yaratmaqla yanaşı, təhlükəsizlik baxımından kompleks risklərin və təhdidlərin ortaya çıxmasına səbəb olur. Bu səbəbdən təhlükəsizlik strategiyaları əvvəlki illərlə müqayisədə daha çevik, dinamik və inteqrasiya olunmuş yanaşma tələb edir.

Mobil texnologiyalar və uzaqdan iş modellərinin artması nəticəsində təşkilatların perimetr əsaslı müdafiə yanaşmaları zəifləyib. Bu mühitdə təhlükəsizlik "device-based trust" və "identity-centric security" kimi yeni prinsiplərə əsaslanır. Mobil cihazların idarə olunması (MDM), tətbiq təhlükəsizliyi, şifrələmə və çoxfaktorlu identifikasiya kimi nəzarətlər strateji təhlükəsizlik yanaşmalarının ayrılmaz hissəsinə çevrilmişdir.

Əşyaların İnterneti (IoT) və sənaye avtomatlaşdırma sistemlərinin geniş tətbiqi təşkilatların hücum səthini daha da genişləndirir. IoT qurğularının çoxu zəif təhlükəsizlik nəzarətləri ilə təchiz olunduğundan onların həm korporativ, həm də dövlət infrastrukturlarında istifadəsi yeni risklər yaradır. Bu yanaşma ənənəvi perimetrlərin əhəmiyyətini minimuma endirir və "heç kimə avtomatik etibar etmə" prinsipinə əsaslanır. Burada identifikasiya, cihaz sağlamlığı, istifadəçi davranış analitikası və dinamik siyasətlərin tətbiqi təhlükəsizliyin əsasını təşkil edir.

Süni intellekt və maşın təlimi də təhlükəsizlik sahəsinə ciddi təsir göstərməkdədir. Bu texnologiyalar kiberhücumların proaktiv aşkarlanması, anomaliyaların müəyyən edilməsi, insidentlərin avtomatlaşdırılmış təhlili və cavab tədbirlərinin sürətləndirilməsi üçün geniş tətbiq olunur.

Beynəlxalq informasiya təhlükəsizliyi standartlarının tətbiqi zamanı qarşıya çıxan əsas problemlərdən biri onların təşkilatın mövcud daxili siyasətləri, prosedurları və əməliyyat qaydaları ilə tam uyğunluq təşkil etməməsidir (Behl və Behl, 2017). Təşkilatlarda uzun illər ərzində formalaşmış daxili normativ sənədlər, idarəetmə mexanizmləri və qərar qəbuletmə prosesləri beynəlxalq standartların tələbləri ilə üst-üstə düşmədikdə təhlükəsizlik strategiyalarının tətbiqi formal xarakter alır.

Adaptiv təhlükəsizlik modelinin formalaşdırılmasının əsaslandırılması. Ənənəvi təhlükəsizlik yanaşmaları çox vaxt "uyğunluq mərkəzli" (compliance-driven) xarakter daşıyır. Bu yanaşmada əsas məqsəd müəyyən edilmiş standartlara formal şəkildə cavab verməkdən ibarət olur. Lakin praktik reallıq göstərir ki, uyğunluq tələblərinin yerinə yetirilməsi həmişə real təhlükəsizlik səviyyəsinin yüksəldilməsi ilə nəticələnmir. Bir çox hallarda təşkilatlar audit və yoxlama tələblərini qarşılasa da,

real kiberhücumlara qarşı müdafiə mexanizmləri zəif qalır. Bu isə təhlükəsizlik strategiyalarının yalnız sənədləşmə və prosedur səviyyəsində qalmasının əsas göstəricisidir.

Adaptiv modelin formalaşdırılmasının əsaslandırılmasında risk əsaslı yanaşma mühüm rol oynayır. Müasir kibertəhlükəsizlikdə bütün riskləri eyni səviyyədə idarə etmək nə mümkün, nə də səmərəlidir. Resursların məhdud olduğu şəraitdə təşkilatlar ən kritik risklərə fokuslanmalı, aşağı riskli sahələrdə isə daha sadə nəzarət mexanizmləri tətbiq etməlidir. Adaptiv təhlükəsizlik modeli bu prioritetləşdirməni sistemli şəkildə həyata keçirməyə imkan verir və təhlükəsizlik resurslarının səmərəli istifadəsini təmin edir.

Digər tərəfdən, təşkilatların təhlükəsizlik yetkinliyi səviyyələri eyni deyil. Bəzi təşkilatlar kibertəhlükəsizlik sahəsində ilkin mərhələdədir, digərləri isə inkişaf etmiş idarəetmə və monitorinq mexanizmlərinə malikdir. Eyni təhlükəsizlik tələblərinin fərqli yetkinlik səviyyəsinə malik təşkilatlara tətbiqi praktiki baxımdan real deyil. Adaptiv model bu fərqliliyi nəzərə alaraq təhlükəsizlik tədbirlərinin mərhələli tətbiqini təklif edir. Bu yanaşma təşkilatlara mövcud vəziyyətdən başlayaraq tədricən daha yüksək təhlükəsizlik səviyyəsinə keçməyə imkan yaradır.

Bu tədqiqat çərçivəsində adaptiv təhlükəsizlik yanaşmasının praktik tətbiqini təmin etmək məqsədilə qərar qəbuletmə mexanizmini formallaşdıran sadə, lakin tətbiq oluna bilən model təklif olunur (Huang və b., 2018; Rose və b., 2020; Whitman və Mattord, 2021). Təklif edilən model təşkilatın informasiya təhlükəsizliyi strategiyasının hansı dərəcədə adaptiv şəkildə tətbiq olunmalı olduğunu müəyyən etməyə imkan verən *Adaptiv Təhlükəsizlik Tətbiqi İndeksi (ATI)* anlayışına əsaslanır. Model dörd əsas parametri nəzərə alır.

Adaptiv Təhlükəsizlik Tətbiqi üçün formal model: Hər təşkilat üçün 4 əsas parametr müəyyən edilir:

Cədvəl 1.

Adaptiv modelin əsas parametrləri cədvəli

Parametr	Simvol	Aralıq
Risk səviyyəsi	R	1-5
Təhlükəsizlik yetkinliyi	M	1-5
Resurs imkanları	C	1-5
Hüquqi/normativ sərtlik	L	1-5

Adaptivlik İndeksi (ATI) aşağıdakı kimi hesablanır:

$$ATI = (R * L) / (M + C)$$

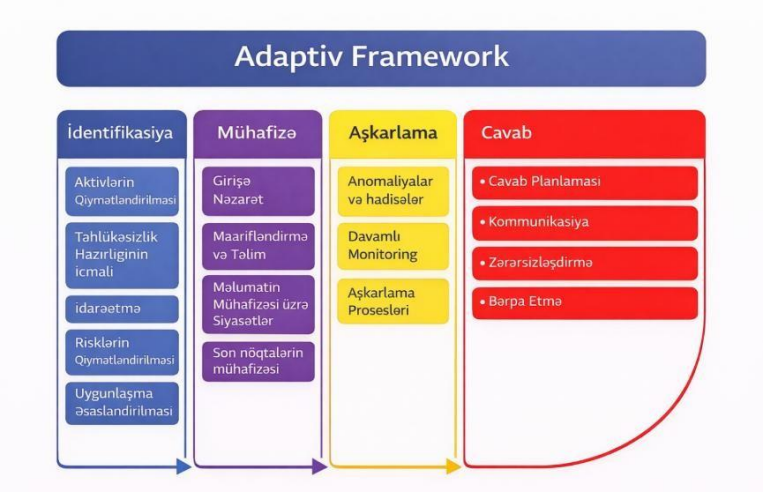
- R yüksəkdirsə → adaptivlik artmalıdır
- L sərtdirsə → birbaşa tətbiq çətinləşir
- M və C zəifdirsə → mərhələlilik vacibdir

Aşağıdakı proqram ilə adaptivliyin təşkili səviyyəsini ölçə bilərik:

```
Input: R, M, C, L
Compute ATI = (R × L) / (M + C)
If ATI > 2:
   Apply adaptive security model with phased controls
Else if ATI between 1 and 2:
   Apply hybrid model
Else: Apply baseline standard controls
```

Təklif olunan adaptiv təhlükəsizlik modelinin praktik mühitdə tətbiq olunması üçün strukturlaşdırılmış icra mexanizminin mövcudluğu zəruridir. Bu məqsədlə tədqiqat çərçivəsində adaptiv təhlükəsizlik yanaşmasının mərhələli və qərar əsaslı tətbiqini təmin edən Application Framework formalaşdırılmışdır. Sözügedən çərçivə təşkilatların beynəlxalq informasiya təhlükəsizliyi standartlarını (ISO/IEC 27001, NIST Cybersecurity Framework və s.) birbaşa və

dəyişdirilmədən tətbiq etməsi əvəzinə, onları təşkilatın real risk profili və imkanlarına uyğun şəkildə adaptasiya etməsinə imkan verir.



Şəkil 2. Adaptiv təhlükəsizlik çərçivəsinin mərhələləri

Nəticə

Aparılan tədqiqat göstərir ki, müasir informasiya təhlükəsizliyi mühitində geniş tətbiq olunan beynəlxalq standart və çərçivələr təşkilatlara metodoloji istiqamət təqdim etsə də, onların birbaşa və dəyişdirilmədən tətbiqi hər zaman gözlənilən təhlükəsizlik nəticələrini təmin etmir. Mövcud yanaşmaların ümumiləşdirilmiş xarakter daşıması təşkilatların risk profili, təhlükəsizlik yetkinliyi səviyyəsi, resurs imkanları və hüquqi-normativ mühiti kimi mühüm amillərin kifayət qədər nəzərə alınmamasına səbəb olur və nəticədə təhlükəsizlik strategiyaları bir çox hallarda formal uyğunluq səviyyəsində qalır.

Tədqiqat nəticələri informasiya təhlükəsizliyi strategiyalarının effektivliyinin adaptiv yanaşmadan birbaşa asılı olduğunu göstərir. Risk əsaslı qərarvermə, təhlükəsizlik yetkinliyi səviyyələrinin qiymətləndirilməsi və mərhələli tətbiq prinsipləri əsasında formalaşdırılan adaptiv yanaşma beynəlxalq standartların əsas prinsiplərini saxlayaraq onların real təşkilati mühitə uyğunlaşdırılmasına imkan verir. Bu yanaşma təhlükəsizlik tədbirlərinin yalnız normativ tələblərin yerinə yetirilməsi məqsədilə deyil, real risklərin idarə olunmasına yönəlmiş şəkildə qurulmasını təmin edir.

Eyni zamanda, tədqiqatda hüquqi və normativ mühitin informasiya təhlükəsizliyi strategiyalarının formalaşdırılmasında həlledici rol oynadığı müəyyən edilmişdir. Təhlükəsizlik nəzarətlərinin hüquqi reallıqlarla uzlaşdırılması onların praktik tətbiqini və davamlılığını artırır. Nəticə etibarilə, təklif olunan adaptiv yanaşma informasiya təhlükəsizliyi strategiyalarının daha çevik, tətbiq oluna bilən və dayanıqlı formada qurulması üçün metodoloji əsas yaradır və bu sahədə gələcək elmi və praktiki araşdırmalar üçün perspektivli istiqamət kimi çıxış edir.

Ədəbiyyat

1. Andress, J. (2019). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress.
2. Behl, A. və Behl, K. (2017). *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford University Press.
3. CIS. (2021). *CIS Critical Security Controls v8. Center for Internet Security.* https://www.cisecurity.org/controls/v8
4. Huang, K., Siegel, M. və Madnick, S. (2018). Systematically understanding the cyber-attack surface. *IEEE Security & Privacy, 16*(5), 35–43. https://doi.org/10.1109/MSEC.2018.2875368

5. ISO/IEC 27001. (2022). *Information Security Management Systems — Requirements*. International Organization for Standardization.
6. ISO/IEC 27002. (2022). *Information Security Controls*. International Organization for Standardization.
7. ISO/IEC 27005. (2018). *Information Security Risk Management*. International Organization for Standardization.
8. NIST. (2006). *SP 800-92: Guide to Computer Security Log Management*. National Institute of Standards and Technology.
9. NIST. (2012). *SP 800-61 Rev.2: Computer Security Incident Handling Guide*. National Institute of Standards and Technology.
10. NIST. (2020). *SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology.
11. NIST. (2024). *Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology*. https://www.nist.gov/cyberframework
12. Rose, S., Borchert, O., Mitchell, S. və Connelly, S. (2020). *Zero Trust Architecture (NIST SP 800-207)*. NIST. https://doi.org/10.6028/NIST.SP.800-207
13. SANS Institute. (2020). *Top 20 Critical Security Controls*. SANS Institute. https://www.sans.org/critical-security-controls
14. Whitman, M.E. və Mattord, H.J. (2021). *Principles of Information Security*. Cengage Learning.

Daxil oldu: 06.12.2025
Qəbul edildi: 09.03.2026