DOI: https://doi.org/10.36719/2706-6185/46/239-242

Bəylər İsmayılov
Azərbaycan Dövlət İqtisad Universiteti
magistrant
https://orcid.org/0009-0002-0067-0509
beyler606@gmail.com

Maliyyə sahəsində informasiyanın mühafizəsinin gücləndirilməsinə yanaşmaların tədqiqi

Xülasə

Müasir dövrdə maliyyə sahəsində informasiya təhlükəsizliyi mühüm əhəmiyyət kəsb edir. Bu sahədə məlumatların qorunması yalnız təşkilatların fəaliyyətinin sabitliyini deyil, həm də müştəri etibarını təmin edən əsas faktorlardan biridir. Rəqəmsallaşmanın geniş vüsət alması və maliyyə əməliyyatlarının əsasən elektron mühitdə aparılması informasiyanın mühafizəsini daha da vacib məsələyə çevirir. Bu səbəbdən, maliyyə qurumlarında informasiyanın mühafizəsinin gücləndirilməsinə yönəlik müxtəlif yanaşmaların tədqiqi aktual və zəruri bir məsələdir.

Xüsusilə kibertəhlükəsizlik tədbirlərinin inkişaf etdirilməsi, məlumatların şifrələnməsi, istifadəçi autentifikasiyası, risklərin qiymətləndirilməsi və idarə olunması kimi metodlar bu sahədə geniş tətbiq edilir. Eyni zamanda, beynəlxalq standartlara və normativ sənədlərə uyğun informasiya təhlükəsizliyi siyasətləri formalaşdırılır. İnsan amili, texnoloji infrastruktur və hüquqi çərçivələr bu sahədə kompleks yanaşmalar tələb edir.

Tədqiqat göstərir ki, yalnız texniki tədbirlərlə kifayətlənmək kifayət deyil; təşkilati və inzibati yanaşmaların da tətbiqi vacibdir. İT risklərinin idarə olunması, informasiya təhlükəsizliyi üzrə təlimlərin keçirilməsi və məlumatların ehtiyat nüsxələrinin saxlanılması bu prosesin əsas tərkib hissələridir.

Nəticə olaraq, maliyyə sahəsində informasiyanın mühafizəsinin gücləndirilməsi kompleks və çoxşaxəli yanaşmalar tələb edir və bu istiqamətdə davamlı inkişaf və tədqiqat mühüm rol oynayır.

Açar sözlər: *informasiya təhlükəsizliyi, informasiya mühafizəsi, kibertəhlükəsizlik, risklərin idarə olunması, məlumatların şifrələnməsi, autentifikasiya, normativ sənədlər, texniki və inzibati tədbirlər, rəqəmsal təhlükəsizlik*

Baylar Ismayilov
Azerbaijan State University of Economics
Master student
https://orcid.org/0009-0002-0067-0509
beyler606@gmail.com

Study of Approaches to Strengthening Information Security in the Financial Sector

Abstract

In the modern era, information security in the financial sector is critical importance. Protecting data in this field ensures not only the stability of institutional operations but also maintains customer trust, which is a fundamental component of financial activity. The rapid digitalization and the dominance of electronic environments in financial transactions have made information protection an increasingly vital issue. Therefore, the study of approaches aimed at strengthening information security in financial institutions is both relevant and necessary.

Particularly, methods such as the development of cybersecurity measures, data encryption, user authentication, risk assessment and management are widely applied in this field.

At the same time, information security policies are developed in accordance with international standards and regulatory documents. The human factor, technological infrastructure, and legal frameworks require a comprehensive approach in this area.

Research indicates that technical measures alone are not sufficient; the application of organizational and administrative strategies is also essential. Managing IT risks, conducting information security training, and maintaining data backups are key components of this process.

In conclusion, strengthening information security in the financial sector requires a multifaceted and integrated approach, where continuous development and research play a crucial role.

Keywords: *information security, data protection, cybersecurity, risk management, data encryption, authentication, regulatory documents, technical and administrative measures, digital security*

Giriş

İnformasiya əsrində yaşadığımız bu günlərdə rəqəmsal texnologiyaların sürətli inkişafı cəmiyyətin bütün sahələrinə, xüsusilə də maliyyə sektoruna dərin təsir göstərmişdir. Bankçılıq, sığorta, investisiya və digər maliyyə xidmətləri rəqəmsallaşma ilə tamamilə yeni müstəviyə keçmiş, əməliyyatların böyük hissəsi elektron formada həyata keçirilməyə başlanmışdır. Bu proses bir tərəfdən vəsaitlərin dövriyyəsini asanlaşdırmış, xidmətlərin sürətini və əlçatanlığını artırmış, digər tərəfdən isə ciddi informasiya təhlükəsizliyi problemlərini gündəmə gətirmişdir.

Maliyyə sektorunda hər gün minlərlə əməliyyat yerinə yetirilir, milyardlarla informasiya paketi ötürülür və saxlanılır. Bu məlumatlar arasında fərdi müştəri məlumatları, bank hesabları, kredit tarixçələri, maliyyə hesabatları və digər məxfi informasiyalar yer alır. Bu cür məlumatların təhlükəsiz şəkildə qorunması və yalnız icazə verilmiş tərəflər tərəfindən əldə olunması son dərəcə vacibdir. Əks halda, maliyyə sistemində sabitlik pozula bilər, istifadəçi etimadı sarsılar və iqtisadi itkilər qaçınılmaz olar (Stallings, 2017).

Kibertəhlükələr — haker hücumları, fişinq (phishing), zərərli proqram təminatları və sosial mühəndislik texnikaları vasitəsilə həyata keçirilən kiber cinayətlər — maliyyə qurumlarını ən çox hədəfə alan risklərdəndir. Bu səbəbdən, informasiya təhlükəsizliyi yalnız texnologiya sahəsində çalışan mütəxəssislərin deyil, həm də maliyyə təşkilatlarının rəhbərliyinin və dövlətin prioritet məsələlərindən biri olmalıdır (Gordon, Loeb, 2002).

Müasir tələblərə cavab verən informasiya təhlükəsizliyi strategiyasının formalaşdırılması və uğurla tətbiq olunması üçün bir sıra amillər nəzərə alınmalıdır: texniki infrastrukturun gücləndirilməsi, informasiya təhlükəsizliyi siyasətinin hazırlanması, hüquqi bazanın təkmilləşdirilməsi, risklərin idarə olunması, insan resurslarının təhsili və maarifləndirilməsi. Eyni zamanda, beynəlxalq standartlara (məsələn, ISO/IEC 27001) uyğunluq da vacib faktor kimi çıxış edir (Məmmədov, 2019).

Bu tədqiqatın əsas məqsədi maliyyə sektorunda informasiyanın mühafizəsinə dair mövcud yanaşmaları sistemli şəkildə təhlil etmək, informasiya təhlükəsizliyinin təmin olunması istiqamətində istifadə olunan metod və vasitələri öyrənmək, habelə bu sahədəki mövcud boşluqları müəyyən edərək onların aradan qaldırılması üçün təkliflər irəli sürməkdir. Mövzu üzrə aparılan araşdırma nəticəsində aydın olur ki, informasiya təhlükəsizliyinin təmin olunması kompleks, çoxşaxəli və dinamik yanaşma tələb edir. Bu isə texniki biliklərlə yanaşı, strateji düşüncə və idarəetmə bacarıqlarının vəhdətini də zəruri edir (Əliyev, 2020).

Nəticə etibarilə, maliyyə sektorunda informasiya təhlükəsizliyinin gücləndirilməsi yalnız bir təşkilatın və ya texnologiyanın deyil, bütövlükdə cəmiyyətin və dövlətin maraqları ilə birbaşa bağlı olan vacib bir istiqamətdir. Bu sahədəki effektiv tədbirlər uzunmüddətli maliyyə sabitliyinin və davamlı inkişafın əsasını təşkil edir (Tipton, Krause, 2007).

Tədqiqat

Maliyyə sektorunda informasiyanın mühafizəsinin gücləndirilməsi təkcə texnoloji tədbirlərlə məhdudlaşmır, eyni zamanda inzibati və hüquqi yanaşmaların sistemli tətbiqini tələb edir. Araşdırmada göstərilib ki, məlumatların şifrələnməsi, firewall və antivirus sistemləri, çoxmərhələli

autentifikasiya və real vaxt rejimində monitorinq kimi texnoloji həllər maliyyə təşkilatlarının kibertəhlükələrə qarşı müdafiəsində əvəzsiz rol oynayır. Bu tədbirlər, məlumatların icazəsiz əldə edilməsinin qarşısını almaq və mümkün hücumların vaxtında aşkarlanmasını təmin etmək baxımından olduqca effektivdir (Peltier, 2016).

Eyni zamanda, daxili siyasət və prosedurların yaradılması, risklərin qiymətləndirilməsi və idarə edilməsi, kadrların davamlı təlimi və məlumatların yedəklənməsi kimi inzibati tədbirlər, texnoloji həllərlə birlikdə məlumatların mühafizəsini daha da möhkəmləndirir. Bu yanaşmaların hər biri, məlumatların təhlükəsizliyinin təmin olunmasında insan faktorunu nəzərə alaraq, kibercinayətlərə qarşı kompleks müdafiə sistemi yaradır (National Institute of Standards and Technology (NIST), 2018).

Beynəlxalq təcrübə göstərir ki, qabaqlayıcı monitorinq sistemləri və süni intellektin tətbiqi ilə maliyyə təşkilatları kibertəhlükələrə qarşı daha çevik və effektiv mübarizə apara bilirlər. Azərbaycanda son illərdə atılan addımlara baxmayaraq, texnoloji infrastrukturun təkmilləşdirilməsi, işçi heyətinin peşəkarlığının artırılması və hüquqi tənzimləmələrin gücləndirilməsi istiqamətində daha geniş tədbirlər görülməlidir (Smith, 2013).

Nəticə olaraq, maliyyə sektorunda informasiyanın mühafizəsinin gücləndirilməsi üçün həm texnoloji, həm inzibati, həm də hüquqi yanaşmaların inteqrasiyası və davamlı inkişafı zəruridir. Bu sahədə aparılan tədqiqatlar və investisiyalar, ölkənin maliyyə sabitliyinin və rəqəmsal iqtisadiyyatın inkişafının təmin olunmasına mühüm töhfə verəcəkdir (Özkan, Gök, 2017).

Tədqiqat işi, mövcud elmi ədəbiyyat, hüquqi sənədlər, beynəlxalq standartlar və praktik nümunələr üzərində aparılmış təhlil və müqayisələrə əsaslanır. Azərbaycan qanunvericiliyi, beynəlxalq standartlar və qabaqcıl bankların tətbiq etdiyi təhlükəsizlik tədbirləri işin əsas mənbələri kimi istifadə olunub (European Central Bank, 2020).

Məlumatların ötürülməsi və saxlanması zamanı şifrələmə alqoritmlərinin istifadə olunması, məlumat sızması halında belə məlumatların icazəsiz şəxslər tərəfindən oxunmasının qarşısını alır. Müasir şifrələmə texnologiyaları, açar idarəetmə sistemləri ilə birlikdə təhlükəsizliyi təmin edir.

Yeni texnologiyaların, xüsusilə süni intellekt və blokçeyn əsaslı təhlükəsizlik sistemlərinin tətbiqinə daha çox investisiya qoyulmalıdır (Basel Committee on Banking Supervision, 2021).

Nəticə

Bu tədqiqat işi maliyyə sektorunda informasiyanın mühafizəsinin gücləndirilməsi istiqamətində tətbiq olunan yanaşmaları texnoloji, inzibati və hüquqi aspektlərdən geniş şəkildə təhlil edib. Araşdırmanın nəticələri göstərir ki, müasir rəqəmsal dövrdə maliyyə təşkilatları üçün informasiya təhlükəsizliyi sadəcə texnoloji həllərlə məhdudlaşmır; bu sahədə uğurlu müdafiə sisteminin təmin olunması üçün koordinasiyalı və çoxşaxəli yanaşma tələb olunur.

İlk növbədə, texnoloji tədbirlər – məlumatların şifrələnməsi, firewall və antivirus sistemlərinin tətbiqi, çoxmərhələli autentifikasiya və real vaxt monitorinqi – kibertəhlükələrə qarşı ilkin müdafiə xəttini təşkil edir. Bu metodlar vasitəsilə məlumatların icazəsiz əldə olunması və istifadəsinin qarşısı alınır, sistemlərdə yaranan hər hansı bir təhdidin vaxtında aşkarlanması və aradan qaldırılması mümkün olur. Bununla belə, texnoloji yanaşmaların səmərəliliyinin tam təmin edilməsi üçün onları təşkilati və hüquqi tədbirlərlə dəstəkləmək zəruridir.

İnzibati və təşkilati yanaşmalar, daxili siyasət və prosedurların yaradılması, risklərin qiymətləndirilməsi və idarə olunması, kadrların davamlı təlimi və məlumatların yedəklənməsi kimi tədbirlərlə maliyyə təşkilatlarının təhlükəsizlik səviyyəsini daha da yüksəldir. İnsan faktorunun yaratdığı riskləri minimuma endirmək və təhlükəsizlik mədəniyyətini gücləndirmək üçün işçilərin maarifləndirilməsi xüsusi əhəmiyyət daşıyır. Belə yanaşmaların tətbiqi, təşkilat daxilində təhlükəsizlik şüurunun yaranmasına və kibertəhlükələrə qarşı daha çevik reaksiya göstərməyə imkan yaradır.

Hüquqi və normativ çərçivə isə milli qanunvericilik və beynəlxalq standartların tətbiqi yolu ilə maliyyə sektorunda informasiya təhlükəsizliyinin qorunmasına zəmanət verir. Azərbaycan Respublikasının “Fərdi məlumatlar haqqında” və “Elektron imza və elektron sənəd haqqında”

qanunları kimi normativ aktlar, eləcə də ISO/IEC 27001 və PCI DSS standartları, təşkilatların təhlükəsizlik səviyyəsinin beynəlxalq standartlara uyğunluğunu təmin edir. Bu, həm də dövlət orqanlarının və tənzimləyici agentliklərin nəzarəti ilə dəstəklənərək, sektorda etibarlı mühafizə sisteminin formalaşmasına töhfə verir.

Ədəbiyyat

1. Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. https://www.bis.org/
2. Əliyev, R. (2020). *Maliyyə sistemində informasiya təhlükəsizliyi problemləri və onların həlli yolları*. Bakı: İqtisad Universiteti Nəşriyyatı.
3. Məmmədov, A. (2019). *Kibertəhlükəsizlik və maliyyə institutlarında informasiya mühafizəsi*. Bakı: Qanun Nəşriyyatı.
4. International Organization for Standardization. (2013). *ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements*. Geneva: ISO.
5. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. https://doi.org/10.1145/581271.581274
6. Tipton, H. F., & Krause, M. (Eds.). (2007). *Information security management handbook* (6th ed.). Auerbach Publications.
7. Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.
8. Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach Publications.
9. Smith, R. (2013). *Elementary information security*. Jones & Bartlett Learning.
10. European Central Bank. (2020). *Cyber resilience oversight expectations for financial market infrastructures*. https://www.ecb.europa.eu/
11. National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov/
12. Özkan, S., & Gök, M. Ş. (2017). Financial institutions and cybersecurity: Current trends and challenges. *Journal of Financial Crime*, 24(3), 447–456. https://doi.org/10.1108/JFC-10-2016-0066

Daxil oldu: 10.12.2024
Qəbul edildi: 15.03.2025