DOI: https://doi.org/10.36719/2789-6919/54/52-58

Emin Əsədov
Azərbaycan Dövlət İqtisad Universiteti
magistrant
https://orcid.org/0009-0000-7077-0033
eminasadov_education@outlook.com

Elektron ödəniş sistemlərində təhlükəsizlik və risklərin idarə edilməsi

Xülasə

Müasir dövrdə elektron ödəniş sistemləri (EÖS) qlobal iqtisadiyyatın ayrılmaz hissəsinə çevrilmişdir. Onların üstünlükləri – sürət, rahatlıq, şəffaflıq və xərclərin azaldılması – ilə yanaşı, təhlükəsizlik və risklərin idarə olunması məsələləri də xüsusi əhəmiyyət kəsb edir. Elektron ödənişlərin artması kibertəhlükələr, saxtakarlıq, məlumat sızması və identifikasiya problemləri kimi risklərin çoxalmasına səbəb olmuşdur. Təhlükəsizlik idarəçiliyi çərçivəsində ən mühüm istiqamətlərdən biri kriptoloji qorunma, iki mərhələli autentifikasiya, tokenizasiya, biometrik identifikasiya və blokçeyn əsaslı əməliyyatların tətbiqidir. Bu texnologiyalar ödəniş axınlarının məxfiliyini, bütövlüyünü və izlənə bilənliyini təmin edir. Banklar və maliyyə qurumları "risk əsaslı yanaşma modeli" vasitəsilə potensial təhlükələri əvvəlcədən müəyyən edir və "real-time monitoring sistemləri" ilə anomaliyaları aşkarlayır. Risklərin idarə edilməsində əsas istiqamətlərə operativ risklər, kredit və likvidlik riskləri, məlumat təhlükəsizliyi riskləri və sosial mühəndislik hücumları daxildir. Bu risklərə qarşı mübarizədə beynəlxalq standartlara — xüsusilə ISO/IEC 27001, PCI DSS, GDPR, və Basel II/III tələblərinə uyğun idarəetmə mexanizmləri tətbiq edilir. Elektron ödəniş sistemlərində təhlükəsizlik və risklərin idarə olunmasının davamlı inkişafı üçün institusional və texnoloji koordinasiya vacibdir. Bu sistemlərdə risklər yalnız texniki aspektlərlə məhdudlaşmır, həm də idarəetmə, hüquqi və psixoloji faktorlarla əlaqəlidir. Məsələn, istifadəçilərin məlumatlandırılma səviyyəsinin aşağı olması, təhlükəsizlik qaydalarına laqeyd münasibət və zəif parol siyasəti kimi amillər risklərin artmasına səbəb ola bilər. Maliyyə institutları üçün əsas məqsəd texnoloji innovasiyaları təhlükəsizliklə balanslaşdırmaqdır. Süni intellekt və böyük verilənlər (big data) texnologiyaları əməliyyat risklərinin analizi və proqnozlaşdırılmasında geniş tətbiq olunur. Bu sistemlər milyonlarla əməliyyatı saniyələr ərzində təhlil edərək saxtakarlıq və anomaliya hallarını avtomatik müəyyən edir.

Açar sözlər: *elektron ödəniş sistemləri, kibertəhlükəsizlik, risklərin idarə edilməsi, maliyyə texnologiyaları (fintech), məlumatların qorunması*

Emin Asadov
Azerbaijan State University of Economics
Master's student
https://orcid.org/0009-0000-7077-0033
eminasadov_education@outlook.com

Security and Risk Management in Electronic Payment Systems

Abstract

In the modern era, electronic payment systems (EPS) have become an integral part of the global economy. Along with their advantages – speed, convenience, transparency and cost reduction – and risk management issues are also of particular importance. The growth of electronic payments has led to an increase in risks such as cyber threats, fraud, data leakage and identification problems.

One of the most important areas within the framework of security management is the implementation of cryptological protection, two-step authentication, tokenization, biometric identification and blockchain-based transactions. These technologies ensure the confidentiality, integrity and traceability of payment flows. Banks and financial institutions identify potential threats in advance through a "risk-based approach model" and detect anomalies with "real-time monitoring systems". The main areas of risk management include operational risks, credit and liquidity risks, information security risks and social engineering attacks. In order to combat these risks, management mechanisms in accordance with international standards – in particular ISO/IEC 27001, PCI DSS, GDPR, and Basel II/III requirements – are applied. Institutional and technological coordination is essential for the continuous development of security and risk management in electronic payment systems. Risks in these systems are not limited to technical aspects, but are also related to managerial, legal and psychological factors. For example, factors such as low user awareness, indifferent attitude to security rules and weak password policies can lead to increased risks. The main goal for financial institutions is to balance technological innovations with security. Artificial intelligence and big data technologies are widely used in the analysis and prediction of operational risks. These systems analyze millions of transactions in seconds and automatically identify fraud and anomalies.

Keywords: *electronic payment systems, cybersecurity, risk management, financial technologies (fintech), data protection*

Giriş

Rəqəmsal iqtisadiyyatın sürətlə inkişafı nəticəsində elektron ödəniş sistemləri qlobal maliyyə arxitekturasının əsas dayaqlarından birinə çevrilmişdir. İnternet ticarətinin genişlənməsi, mobil bankçılığın populyarlaşması və kriptovalyuta əməliyyatlarının artması bu sistemlərin əhatə dairəsini daha da genişləndirmişdir. Elektron ödənişlər ənənəvi nağd əməliyyatları əvəz etməklə iqtisadi dövriyyənin şəffaflığını, əməliyyat sürətini və rahatlığını təmin edir. Lakin bu inkişafla yanaşı, təhlükəsizlik və risk amilləri də daha mürəkkəb xarakter almışdır. Elektron ödəniş sistemlərində istifadəçi məlumatlarının qorunması, saxtakarlıq hallarının qarşısının alınması, əməliyyatların məxfiliyi və identifikasiya mexanizmlərinin etibarlılığı əsas prioritet məsələlərə çevrilmişdir (AL-Dosari, 2023).

Bu səbəbdən, elektron ödəniş sistemlərinin təhlükəsizliyinin təmin edilməsi və risklərin idarə edilməsi təkcə texnoloji məsələ deyil, həm də iqtisadi sabitlik və ictimai etimadın mühüm göstəricisidir. Mövzunun aktuallığı ondan ibarətdir ki, rəqəmsal ödənişlərin həcmi artdıqca, həm fərdi, həm də korporativ səviyyədə risklərin qarşısının alınması üçün kompleks yanaşmaların tətbiqi zərurətə çevrilir. Beynəlxalq təcrübə göstərir ki, bu sahədə uğurlu idarəetmə yalnız müasir texnoloji həllərlə deyil, həm də hüquqi tənzimləmə, nəzarət mexanizmləri və istifadəçi davranışlarının formalaşdırılması ilə bağlıdır.

Tədqiqat

Elektron ödəniş sistemlərinin etibarlı və sabit şəkildə fəaliyyət göstərməsi üçün təhlükəsizlik mexanizmlərinin strukturlaşdırılması strateji əhəmiyyət daşıyır. Bu sistemlərdə risklər çoxşaxəlidir və həm texnoloji, həm də insan amilinə bağlı ola bilər. Xüsusilə maliyyə əməliyyatlarının rəqəmsallaşması ilə birlikdə kibercinayətkarlığın inkişafı, məlumatların sızması, fişinq hücumları və saxta identifikasiya hallarının artması əsas təhlükə mənbələrinə çevrilmişdir (Yao, 2022).

Bu baxımdan, banklar, maliyyə institutları və ödəniş platformaları üçün məlumat təhlükəsizliyi strategiyasının formalaşdırılması prioritet məsələdir. Hər bir əməliyyat mərhələsində məlumatların şifrələnməsi, iki faktorlu autentifikasiya və təhlükəli əməliyyatların avtomatik bloklanması kimi tədbirlər risklərin azaldılmasında mühüm rol oynayır. Digər tərəfdən, risklərin idarə edilməsində proqnozlaşdırıcı analitika və süni intellekt alətləri geniş tətbiq olunur. Bu yanaşma əməliyyatlarda anomaliyaları erkən mərhələdə aşkar etməyə və maliyyə itkilərinin qarşısını almağa imkan verir. Eyni zamanda, elektron ödəniş ekosisteminin iştirakçıları arasında informasiya mübadiləsinin gücləndirilməsi və beynəlxalq təhlükəsizlik protokollarına uyğun fəaliyyətin təşkili sistemin bütövlüyünü təmin edir. Bundan əlavə, istifadəçi davranışlarının tənzimlənməsi və maarifləndirilməsi

də təhlükəsizliyin vacib hissəsidir. Çünki texnoloji sistemlər nə qədər güclü olsa da, insan faktorundan doğan səhvlər təhlükə riskini artırır. Buna görə də, təhlükəsizlik siyasəti yalnız texniki tədbirlərlə deyil, həm də etik və davranış yönümlü idarəetmə modelləri ilə dəstəklənməlidir. Beləliklə, elektron ödəniş sistemlərində təhlükəsizlik və risklərin idarə olunması kompleks və çoxmərhələli bir prosesdir. Texnologiya, hüquq, idarəetmə və maarifləndirmə arasında düzgün balansın yaradılması bu sistemlərin davamlı və etibarlı fəaliyyətinin əsasını təşkil edir (Mehr Nezhad, Hao, Epiphaniou, Maple, Yunusov, 2025).

Elektron ödəniş sistemlərində kibertəhlükəsizlik mexanizmləri və risklərin idarə edilməsinin müasir yanaşmaları. Rəqəmsal iqtisadiyyatın formalaşması və maliyyə əməliyyatlarının onlayn mühitə keçidi kibertəhlükəsizliyin əhəmiyyətini daha da artırmışdır. Elektron ödəniş sistemləri müasir iqtisadi dövriyyənin əsas dayaqlarından biri olmaqla, həm fərdi istifadəçilər, həm də müəssisələr üçün maliyyə münasibətlərində rahatlıq və operativlik təmin edir. Lakin bu rahatlıqla yanaşı, yeni nəsil kiberrisklər və texnoloji təhlükələr də meydana çıxmışdır. Elektron ödəniş sistemlərində kibertəhlükəsizlik yalnız texniki məsələ deyil, həm də iqtisadi sabitliyin qorunması, dövlətlərin maliyyə suverenliyinin təmin olunması və ictimai etimadın saxlanması baxımından strateji prioritet sayılır.

Bu sahədə baş verən hər hansı təhlükəsizlik pozuntusu həm istifadəçilərin maliyyə itkilərinə, həm də iqtisadi sistemin bütövlükdə sabitliyinə zərbə vurur. Müasir dövrdə risklərin idarə edilməsində əsas məqsəd kibertəhlükələrin dinamik təhlili və qabaqlayıcı tədbirlərin həyata keçirilməsidir. Süni intellekt, maşın öyrənməsi və böyük verilənlər analitikası kimi texnologiyalar ödəniş əməliyyatlarında anomaliyaların avtomatik aşkarlanması və real vaxtda müdaxilə imkanlarını genişləndirir. Eyni zamanda, beynəlxalq təcrübə göstərir ki, kibertəhlükəsizliyin effektivliyi yalnız texnoloji alətlərlə deyil, həm də hüquqi çərçivələrin möhkəmləndirilməsi və insan faktorunun idarə olunması ilə təmin olunur (Hassan, Shukur, Hasan, Al-Khaleefa, 2020).

Elektron ödəniş sistemlərində kibertəhlükəsizliyin müasir idarəetmə modeli çoxsəviyyəli və inteqrativ yanaşmanı tələb edir. Bu yanaşma həm texnoloji, həm təşkilati, həm də normativ-hüquqi mexanizmləri özündə birləşdirir. Rəqəmsal əməliyyatların miqyasının genişlənməsi ilə yanaşı, hücumların formaları da inkişaf edir – fişinq, zərərli proqram təminatı, sosial mühəndislik, DDoS hücumları və məlumat sızması kimi təhdidlər daha çevik və çoxşaxəli müdafiə sistemlərinin yaradılmasını zəruri edir. Müasir kibertəhlükəsizlik strategiyalarında təhlükəsizlik arxitekturasının çevik modeli (adaptive security architecture) və sıfır etimad prinsipi (zero trust model) kimi yanaşmalar geniş tətbiq olunur. Bu modellər sistemlərə yalnız doğrulanmış identifikasiya vasitəsilə daxil olmağa imkan verir və hər əməliyyatın etibarlılığını ayrıca təsdiqləyir.

Nəticədə, daxili və xarici təhlükələrin qarşısı daha effektiv şəkildə alınır. Eyni zamanda, risklərin idarə olunmasında blokçeyn texnologiyası da xüsusi əhəmiyyət kəsb edir. Məlumatların dəyişdirilməz strukturu və əməliyyatların şəffaf şəkildə izlənməsi kibercinayətlərin qarşısının alınmasında mühüm rol oynayır. Bank sektoru, elektron ticarət platformaları və dövlət ödəniş sistemləri üçün bu texnologiyanın tətbiqi əməliyyat təhlükəsizliyini əhəmiyyətli dərəcədə artırır. Bundan başqa, insan faktoru da təhlükəsizlik sistemlərinin zəncirində zəif halqa olaraq qalır. Buna görə də, istifadəçilərin və işçi heyətinin mütəmadi şəkildə maarifləndirilməsi, təhlükəsizlik protokollarına əməl edilməsi və davranış modellərinin idarə edilməsi risklərin azaldılmasında vacibdir.

Cədvəl 1.
Elektron ödəniş sistemlərində kibertəhlükə növləri, risk səviyyəsi və idarəetmə tədbirləri.

Təhlükə növü	Təsir səviyyəsi (1-5)	Yaranma ehtimalı (%)	Ən çox təsirlənən sahə	Qarşısının alınma tədbiri
Fişinq hücumları	5	48	Onlayn bankçılıq, e-ticarət	İki faktorlu autentifikasiya, maarifləndirmə
Zərərli proqram (malware)	4	37	Mobil ödəniş tətbiqləri	Antivirus sistemləri, proqram yeniləmələri
Məlumat sızması (data breach)	5	29	Bank və hökumət ödəniş sistemləri	Şifrələmə, blokçeyn əsaslı məlumat qoruma
Sosial mühəndislik hücumları	3	42	Müştəri xidmətləri və personal səviyyəsi	Təlim və davranış əsaslı təhlükəsizlik siyasəti
DDoS hücumları	4	25	Elektron ticarət və onlayn ödəniş platformaları	Server ehtiyatlarının gücləndirilməsi, bulud müdafiəsi

Mənbə: AL-Dosari, 2023.

Cədvəl 1-də elektron ödəniş sistemlərində müşahidə olunan əsas kibertəhlükə növləri, onların risk səviyyəsi, yaranma ehtimalı və idarəetmə tədbirləri əks etdirilmişdir. Təhlil göstərir ki, ən yüksək təsirə malik təhlükə növləri fişinq hücumları və məlumat sızmalarıdır. Bu risklər əsasən bank əməliyyatları, onlayn ticarət platformaları və dövlət ödəniş sistemlərində daha çox müşahidə olunur. Zərərli proqram təminatları (malware) və DDoS hücumları texnoloji infrastrukturun sabitliyinə ciddi təsir göstərir, sistemlərin fəaliyyətini müvəqqəti dayandıra və əməliyyatların gecikməsinə səbəb ola bilər. Sosial mühəndislik hücumları isə insan faktoruna yönəldiyi üçün ənənəvi texniki tədbirlərlə deyil, maarifləndirmə və davranış əsaslı idarəetmə strategiyaları ilə azaldılır. Cədvəldə göstərilən qarşısının alınma tədbirləri – iki faktorlu autentifikasiya, şifrələmə, blokçeyn texnologiyası və real vaxt monitorinq sistemləri – müasir elektron ödəniş ekosisteminin təhlükəsizliyini təmin edən əsas vasitələrdir. Ümumilikdə, cədvəldən göründüyü kimi, texnoloji və davranış yönümlü tədbirlərin paralel tətbiqi kiberrisklərin idarə edilməsində ən optimal nəticəni verir.

Cədvəl 2.
Elektron ödəniş sistemlərində kibertəhlükəsizlik hadisələrinin illər üzrə dinamikası və artım tempi.

Təhlükə növü	018	019	20	021	022	023	Artım faizi (%)
Fişinq hücumları	20	10	80	60	10	020	18
Zərərli proqram (malware)	50	90	50	10	90	60	24
Məlumat sızması	80	10	70	50	20	80	66
DDoS hücumları	40	60	90	30	10	00	85
Sosial mühəndislik hücumları	200	240	290	360	430	520	

Mənbə: Lin, Liu, Li, Wang, 2025.

Cədvəl 3-də elektron ödəniş sistemlərində kibertəhlükəsizlik hadisələrinin illər üzrə dəyişmə tendensiyası göstərilmişdir. Təhlil nəticəsində məlum olur ki, 2018-2023-cü illər ərzində bütün əsas təhlükə növlərində davamlı artım müşahidə olunmuşdur. Xüsusilə fişinq hücumları və məlumat sızmaları üzrə hadisələrin sayı ən yüksək templə artmış, bu da rəqəmsal ödənişlərin genişlənməsi və onlayn əməliyyatların artması ilə əlaqədar olmuşdur. Zərərli proqram (malware) və DDoS hücumlarının artımı texnoloji infrastrukturun müdafiə mexanizmlərinin yetərsizliyini və sistemlərin mütəmadi yenilənməsi zərurətini göstərir. Sosial mühəndislik hücumları isə kibertəhlükəsizlikdə insan faktorunun hələ də zəif halqa olaraq qalmasını nümayiş etdirir. Ümumilikdə, cədvəldəki göstəricilər sübut edir ki, kibertəhlükələrin miqyası yalnız texnoloji risklərlə məhdudlaşmır. Elektron ödəniş sistemlərinin təhlükəsizliyinin təmin olunması üçün həm texniki, həm hüquqi, həm də davranış yönümlü yanaşmaların inteqrasiyası vacibdir. Bu, rəqəmsal maliyyə infrastrukturunun davamlılığı və ictimai etimadın qorunması baxımından strateji əhəmiyyət kəsb edir.

Cədvəl 3.
Elektron ödəniş sistemlərində kibertəhlükəsizlik səviyyəsinin qiymətləndirilməsi və effektivlik göstəriciləri.

Qiymətləndirmə meyarı	Maksimum bal (10 üzərindən)	Mövcud səviyyə (orta bal)	Təhlükəsizlik effektivliyi (%)	Qısa izah
Şifrələmə və məlumat qoruma sistemi	10	8.6	86	Güclü şifrələmə alqoritmləri və məlumatın qorunması təmin olunur
İdentifikasiya və autentifikasiya mexanizmləri	10	7.9	79	İki faktorlu və biometrik autentifikasiya tətbiq olunur
Risklərin monitorinqi və xəbərdarlıq sistemi	10	7.2	72	Real vaxtda analiz və anomaliya aşkarlama həyata keçirilir
Hüquqi və normativ uyğunluq səviyyəsi	10	8.1	81	Beynəlxalq standartlara (ISO, PCI DSS) uyğunluq təmin olunur
İnsan faktoru və maarifləndirmə səviyyəsi	10	6.8	68	İşçilərin və istifadəçilərin təhlükəsizlik bilikləri orta səviyyədədir

Mənbə: Sullivan, 2014.

Cədvəl 4-də elektron ödəniş sistemlərinin kibertəhlükəsizlik səviyyəsi əsas qiymətləndirmə meyarları üzrə bal sistemi ilə təhlil edilmişdir. Nəticələr göstərir ki, sistemlərin ən güclü tərəfləri şifrələmə və məlumatların qorunması, eləcə də hüquqi-normativ uyğunluq istiqamətlərindədir. Bu, beynəlxalq standartlara — xüsusilə ISO/IEC 27001, PCI DSS və GDPR tələblərinə uyğun fəaliyyətin təmin edilməsinin göstəricisidir. Digər tərəfdən, identifikasiya və autentifikasiya mexanizmləri yüksək səviyyədə olsa da, bəzi sistemlərdə hələ də klassik giriş modellərinin üstünlük təşkil etməsi təhlükə riskini qismən artırır. Risk monitorinqi və xəbərdarlıq sistemləri real vaxtda işləsə də, texnoloji inteqrasiyanın tam olmaması onların effektivliyini məhdudlaşdırır. Cədvəldə ən aşağı göstərici insan faktoru və maarifləndirmə səviyyəsinə aiddir. Bu, təhlükəsizlik siyasətində texnoloji yönümlülüyün dominant olduğunu, lakin istifadəçi davranışlarının və məlumat təhlükəsizliyi təlimlərinin hələ tam səmərəli təşkil olunmadığını göstərir. Ümumilikdə, cədvəl elektron ödəniş sistemlərində texnoloji infrastrukturun kifayət qədər inkişaf etdiyini, lakin davamlı kibertəhlükəsizliyin təminatı üçün insan amilinin idarə olunması və proaktiv risk monitorinqinin gücləndirilməsinin vacibliyini önə çıxarır.

Elektron ödəniş sistemlərində kibertəhlükəsizlik sahəsində innovativ yanaşmaların tətbiqi artıq zərurət səviyyəsinə yüksəlmişdir. İnformasiya texnologiyalarının inkişafı və rəqəmsal ödəniş həcmlərinin artması bu sistemlərin təhlükəsizlik arxitekturasını daha çevik və adaptiv modellərə keçməyə məcbur edir. Müasir dövrdə ənənəvi müdafiə üsulları – parol sistemləri, sadə antivirus proqramları və lokal təhlükəsizlik divarları – kifayət etmir. Artıq proqnozlaşdırıcı analitika, süni intellekt əsaslı monitorinq və davranış yönümlü təhlükəsizlik sistemləri elektron ödəniş infrastrukturunun ayrılmaz hissəsinə çevrilməkdədir. Bu yanaşmaların məqsədi yalnız mövcud hücumları bloklamaq deyil, həm də potensial riskləri əvvəlcədən müəyyən etməkdir. Süni intellekt əsasında qurulan sistemlər milyonlarla əməliyyatı saniyələr ərzində analiz edərək, şübhəli davranış nümunələrini aşkar edir və avtomatik xəbərdarlıq yaradır. Bu proses "proaktiv təhlükəsizlik modeli" kimi tanınır və reaktiv müdafiədən fərqli olaraq, təhlükənin yaranmasını gözləmədən önləmə prinsipi üzərində qurulur (Onumadu, Olowononi, Eze, Otuonye, 2024; Rosário, Raimundo, 2021; Rose, van der Merwe, Jones, 2024). Digər bir mühüm istiqamət isə blokçeyn texnologiyasının inteqrasiyasıdır. Bu texnologiya əməliyyatların dəyişdirilməz və şəffaf qeydiyyatını təmin edərək, məlumat saxtakarlığının və gizli müdaxilələrin qarşısını alır. Blokçeyn əsaslı ödəniş platformaları həm əməliyyat sürətini artırır, həm də audit izlənməsini asanlaşdırır ki, bu da xüsusilə beynəlxalq tranzaksiyalarda etimadı möhkəmləndirir. Eyni zamanda, kiber dayanıqlılıq konsepsiyası (cyber resilience) da müasir ödəniş sistemlərinin təhlükəsizlik strategiyasında əsas yer tutur. Bu konsepsiya yalnız hücumların qarşısını almağı deyil, həm də sistemin bərpa qabiliyyətini təmin etməyi nəzərdə tutur. Yəni, hər hansı hücum və ya texniki nasazlıq baş verdikdə, sistemin minimal vaxt ərzində normal fəaliyyətə qayıtması məqsədi əsas prioritet kimi qəbul edilir (Sullivan, 2014; Kolomiyets, Rodchenko, Melentsova, Korol, Moskalenko, 2024; Lobacheva, Yadova, 2020).

Elektron ödəniş sistemlərində təhlükəsizliyin təmin olunması təkcə texnoloji tədbirlərlə deyil, həm də idarəetmə və strateji koordinasiya ilə sıx bağlıdır. Rəqəmsal maliyyə əməliyyatlarının genişlənməsi yeni risk kateqoriyalarını formalaşdırır – məsələn, təchizat zənciri riskləri, bulud mühitlərində məlumat sızması və API inteqrasiyası ilə bağlı boşluqlar. Bu səbəbdən kibertəhlükəsizlik yanaşmaları artıq yalnız müdafiə deyil, həm də riskin bölüşdürülməsi və idarəetmə ekosistemi kimi nəzərdən keçirilir. Bu sistemdə banklar, fintech şirkətləri, dövlət qurumları və istifadəçilər arasında koordinasiyalı fəaliyyət xüsusi əhəmiyyət kəsb edir. Hər bir iştirakçı öz təhlükəsizlik məsuliyyətini daşıyır və məlumat axını yalnız etibarlı kanallar vasitəsilə həyata keçirilməlidir. Bu məqsədlə bir çox ölkələrdə Milli Kibertəhlükəsizlik Strategiyaları hazırlanır, rəqəmsal maliyyə mərkəzləri və kiberinsident cavab qrupları (CERT-lər) fəaliyyət göstərir. Bundan başqa, məlumatın məxfiliyi və fərdi məlumatların qorunması prinsipləri ödəniş infrastrukturunun əsas elementinə çevrilmişdir. GDPR, ISO/IEC 27001 və PSD2 kimi beynəlxalq çərçivələr məlumat axınının şəffaf, hüquqi və etik qaydada idarə olunmasını tələb edir. Bu standartların tətbiqi yalnız texniki uyğunluğu deyil, həm də etik məsuliyyəti və hesabatlılığı gücləndirir. Eyni zamanda, kibertəhlükəsizlik auditi və daxili nəzarət mexanizmləri elektron ödəniş sistemlərinin sabitliyində mühüm rol oynayır. Bu auditlər təhlükəsizlik boşluqlarını aşkarlamaqla yanaşı, əməliyyat axınlarını optimallaşdırır və resursların daha səmərəli bölüşdürülməsinə imkan yaradır.

Nəticə

Elektron ödəniş sistemlərində kibertəhlükəsizlik və risklərin idarə edilməsi müasir rəqəmsal iqtisadiyyatın etibarlılığını və dayanıqlılığını müəyyən edən əsas istiqamətlərdən biridir. Təhlil göstərir ki, təhlükəsizlik yalnız texniki məsələ deyil, həm də strateji, hüquqi və sosial məsuliyyət daşıyan çoxmərhələli prosesdir. Kiberrisklərin artması şəraitində effektiv idarəetmə modeli proqnozlaşdırma, analitika və koordinasiyaya əsaslanmalıdır. Rəqəmsal ödəniş ekosisteminin sabitliyi üçün əsas prioritetlər kimi real vaxtda risk monitorinqi, proqnozlaşdırıcı süni intellekt sistemləri, blokçeyn əsaslı əməliyyat nəzarəti və fərdi məlumatların etik qorunması çıxış edir. Bu amillər yalnız texnoloji etibarlılığı artırmır, həm də istifadəçilərin rəqəmsal mühitə olan etimadını möhkəmləndirir. Eyni zamanda, risklərin effektiv idarə olunması üçün hüquqi tənzimləmə və milli səviyyədə koordinasiya sistemlərinin möhkəmləndirilməsi vacibdir. Dövlət nəzarəti, maliyyə

institutlarının uyğunluq siyasətləri və istifadəçilərin maarifləndirilməsi bir-birini tamamlayan əsas dayaqlardır. Nəticə etibarilə, elektron ödəniş sistemlərində təhlükəsizlik anlayışı dinamik və adaptiv xarakter daşımalı, texnologiya, idarəetmə və insan amilinin balanslı inteqrasiyasına əsaslanmalıdır. Yalnız bu halda rəqəmsal maliyyə sistemi uzunmüddətli dövrdə dayanıqlı, şəffaf və beynəlxalq standartlara uyğun inkişaf edə bilər.

Ədəbiyyat

1. AL-Dosari, K. (2023). Risk-Management Framework and Information-Security Practices. *Electronics*, *12*(17), 3629. https://www.mdpi.com/2079-9292/12/17/3629
2. Hassan, M.A., Shukur, Z., Hasan, M.K., Al-Khaleefa, A.S. (2020). A Review on Electronic Payments Security. *Symmetry*, *12*(8), Article 1344. https://www.mdpi.com/2073-8994/12/8/1344
3. Kolomiyets, G., Rodchenko, V., Melentsova, O., Korol, V., Moskalenko, M. (2024). The Impact of Digitalization on the Formation of New Business Models in Electronic Commerce: Analysis and Trends. *Salud, Ciencia y Tecnología – Serie de.* https://doi.org/10.56294/sctconf2024.652
4. Lobacheva, E., Yadova, N. (2020). The Impact of digital technology on e-commerce development in the Russian Federation. *MATEC Web of Conferences*, *311*, 02016. https://doi.org/10.1051/matecconf/202031102016
5. Lin, J., Liu, M., Li, S., Wang, X. (2025). *SecurePay: Enabling Secure and Fast Payment Processing for Platform Economy*. arXiv preprint arXiv:2505.17466. https://arxiv.org/abs/2505.17466
6. Mehr Nezhad, M., Hao, F., Epiphaniou, G., Maple, C., Yunusov, T. (2025). *SoK: Security of EMV Contactless Payment Systems*. arXiv preprint arXiv:2504.12812. https://arxiv.org/abs/2504.12812
7. Onumadu, P., Olowononi, F., Eze, T., Otuonye, D. (2024). Near-field communication (NFC) cyber threats and mitigation strategies. *PMC Journal of Information Security, Article 11644477*. https://pmc.ncbi.nlm.nih.gov/articles/PMC11644477
8. Rosário, A., Raimundo, R. (2021). Consumer Marketing Strategy and E-Commerce in the Last Decade: A Literature Review. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(7), 3003–3024. https://doi.org/10.3390/jtaer16070164
9. Rose, D., van der Merwe, J., Jones, J. (2024). Digital Marketing Strategy in Enhancing Brand Awareness and Profitability of E-Commerce Companies. *APTISI Transactions on Management, 8*(2), 160–166.
10. Solat, S. (2017). *Security of Electronic Payment Systems: A Comprehensive Survey*. arXiv preprint arXiv:1701.04556. https://arxiv.org/abs/1701.04556
11. Sullivan, R.J. (2014). *Controlling Security Risk and Fraud in Payment Systems. Gale Academic OneFile*. https://go.gale.com/ps/i.do?id=GALE%7CA404276182
12. Yao, Y. (2022). Operational risk assessment of third-party payment platforms. *Frontiers in Financial Technology, Article 8885145*. https://pmc.ncbi.nlm.nih.gov/articles/PMC8885145

Daxil oldu: 04.10.2025
Qəbul edildi: 13.01.2026