

DOI: <https://doi.org/10.36719/2789-6919/50/99-103>

Əli Qafarlı

Azərbaycan Turizm və Menecment Universiteti
magistrant

<https://orcid.org/0009-0008-4839-2505>
aligafarli123@gmail.com

Qonaqpərvərlik sənayesində rəqəmsal risklərin azaldılmasında AI və Bulud sistemlərinin əhəmiyyəti

Xülasə

Bu məqalə qonaqpərvərlik sənayesində süni intellekt (AI) və bulud texnologiyalarının inteqrasiyasını təhlükəsizlik və məxfiliyi artırmaq məqsədilə araşdırır. Məqalədə otaqlara təhlükəsiz giriş üçün üz tanıma, ağıllı video nəzarət və onlayn əməliyyatlarda fırıldaqçılığın aşkarlanması kimi AI tətbiqləri təhlil edilir. Bundan əlavə, məlumatların şifrələnmiş saxlanması, idarə edilməsi və fəlakətdən bərpa üçün bulud əsaslı sistemlər müzakirə olunur. Məxfilik məsələləri və GDPR, CCPA kimi tənzimləmələrə uyğunluq kimi əsas çağırışlar, həmçinin, kvant şifrələmə kimi gələcək tendensiyalar da nəzərdən keçirilir. Həmçinin, hadisə araşdırmaları və müqayisəli təhlillər rəqəmsal riskləri minimuma endirərkən qonaqlar üçün fasiləsiz və səmərəli təcrübə təmin etmək üçün praktik tövsiyələr təqdim edir.

Açar sözlər: *süni intellekt, bulud hesablama, qonaqpərvərlik təhlükəsizliyi, üz tanıma, şifrələnmiş saxlama, kiber təhlükəsizlik, rəqəmsal risk idarəçiliyi, kvant şifrələmə, ağıllı video nəzarət*

Ali Gafarli

Azerbaijan Tourism and Management University
Master student

<https://orcid.org/0009-0008-4839-2505>
aligafarli123@gmail.com

The Importance of AI and Cloud Systems in Reducing Digital Risks in the Hospitality Industry

Abstract

This study explores how artificial intelligence (AI) and cloud computing are being integrated into the hospitality sector to strengthen security and protect privacy. It reviews AI-based solutions, including facial recognition for secure room entry, smart video monitoring, and online transaction fraud detection. The paper also examines cloud-based platforms for encrypted data storage, management, and disaster recovery. Key issues such as privacy concerns and regulatory compliance with standards like GDPR and CCPA are discussed, along with emerging technologies like quantum encryption. Through case studies and comparative analysis, the research offers practical guidance for reducing digital risks while delivering seamless and efficient experiences to guests.

Keywords: *artificial intelligence, cloud computing, hospitality security, facial recognition, encrypted data storage, cybersecurity, digital risk management, quantum encryption, smart video monitoring*

Giriş

Qonaqpərvərlik sənayesi fərdiləşdirilmiş təcrübələr və xidmətlər təqdim etmək üçün şəxsi məlumatlara böyük dərəcədə güvənir. Lakin belə məlumatların toplanması və istifadəsi ciddi etik məsələləri gündəmə gətirir. Qonaqlar bizneslərə əlaqə məlumatları, ödəniş məlumatları və üstünlüklər kimi həssas məlumatlarını etibar edirlər, bu isə onların sui-istifadəsinin və ya məlumat pozuntularının qarşısını almaq üçün diqqətli yanaşma tələb edir. Etik məlumat toplama prosesi məlumat sahiblərinin məlumatlı razılığını almaq, məlumatların necə istifadə olunacağı barədə şəffaflığı təmin etmək və yalnız lazım olan məlumatları toplamaq prinsiplərinə riayət etməyi əhatə edir. Şəffaflığı qorumaq üçün müəssisələr topladıqları məlumatların nə üçün lazım olduğunu və necə qorunacağını açıq şəkildə göstərən aydın məlumat istifadə siyasətlərini qəbul edə bilirlər. Məxfilik yönümlü kommunikasiya, görünən razılıq mexanizmləri və məxfilik siyasətlərinin müntəzəm yenilənməsi kimi strategiyalar qonaqların etibarını qurmağa kömək edir. Qonaqlara öz məlumatları üzərində nəzarət imkanı, məsələn, məlumatları silmək və ya dəyişdirmək imkanı vermək, daha böyük məsuliyyət təmin edir və məlumat idarəetməsində etik praktikalarla uyğunlaşır.

Tədqiqat

Qonaqpərvərlik sənayesi, süni intellekt (AI), bulud texnologiyaları kimi qabaqcıl texnologiyaların tətbiqi ilə əhəmiyyətli bir rəqəmsal transformasiya prosesindən keçir. Bu innovasiyalar qonaq təcrübələrini köklü şəkildə dəyişərək fərdiləşdirilmiş xidmətlərin göstərilməsinə, asan rezervasiya imkanlarına və səmərəli əməliyyatlara şərait yaradır. Süni intellekt əsaslı çatbotlar, bulud əsaslı idarəetmə sistemləri və ağıllı otaqlar, texnologiyanın sənayeni necə yenidən formalaşdırdığının bəzi nümunələridir. Lakin bu rəqəmsal inkişaf eyni zamanda, müəyyən çətinlikləri də gətirib, xüsusilə, təhlükəsizlik və məxfilik sahəsində. Qarışıq və bir-birinə bağlı sistemlərin inteqrasiyası ilə qonaqların şəxsi məlumatları, ödəniş detalları və davranış üstünlükləri kimi həssas məlumatlar rəqəmsal şəkildə saxlanılır və ötürülür. Bu sistemlər kiberhücumlara, məlumat sızmalarına və icazəsiz girişlərə qarşı həssasdır, bu isə güclü kiber təhlükəsizlik çərçivələrinə olan tələbi artırır. Bu sistemlərin təhlükəsizliyi və məxfiliyini təmin etmək həm sənayenin, həm də müştərilərin qorunması üçün əsasdır.

Kiber təhlükəsizlik və məxfilik qonaqpərvərlik sənayesində müzakirə olunmaz prioritetlərə çevrilib. Son illərdə baş verən yüksək səviyyəli təhlükəsizlik pozuntuları, məlumatların pozulmasının dağıdıcı nəticələrini – maliyyə itkilərini, reputasiyanın zədələnməsini və müştəri etibarının azalmasını açıq şəkildə göstərib. Rəqəmsal platformalara yüksək dərəcədə asılılıq nəzərə alınaraq, hətta bir tək hadisə də qonaqların etibarını sarsıda və uzunmüddətli reputasiya zərərlərinə səbəb ola bilər. Qonaqların etimadı qonaqpərvərlik sektorunda uğurun təməl daşlarından biridir (Surendra, 2023, s. 417). Səyahətçilər otellərə, kurortlara və onlayn rezervasiya platformalarına həssas şəxsi və maliyyə məlumatlarını etibar edirlər. Sənayenin bu məlumatları qoruma qabiliyyəti yalnız qanunvericilik tələblərinə riayət etmək üçün deyil, həm də rəqabət üstünlüyünü saxlamaq üçün həyati əhəmiyyət kəsb edir. Effektiv kiber təhlükəsizlik tədbirləri və şəffaf məxfilik praktikaları bu etimadın qorunması və qonaqpərvərlik sənayesinin rəqəmsal dövrdə inkişaf etməsi üçün vacibdir.

Ümumilikdə isə, müasir dövrdə turizmin inkişafını göz önündə saxlayaraq istər turizm şirkətləri səviyyəsində, istərsə də otelçilik biznesində təhlükəsizlik mühüm əhəmiyyət kəsb edir. Bu xüsusda hansı təhlükəsizlik tədbirlərinin görülməsi ilə bağlı məqamlara diqqət etmək lazımdır? Bunlara misal olaraq, ilk öncə müasir dövrümüzün ən çox müraciət edilən süni intellekt əsaslı proqramlarını qeyd edə bilərik. Süni intellekt əsaslı üz tanıma sistemləri qonaqpərvərlik sənayesində otaqlara giriş üsullarını inqilabi şəkildə dəyişir və təmamsız, təhlükəsiz, səmərəli giriş imkanı yaradır. Bu sistemlər inkişaf etmiş alqoritmlər vasitəsilə üz xüsusiyyətlərini saxlanmış məlumatlarla müqayisə edərək yalnız səlahiyyətli qonaqların otaqlarına girişinə icazə verir. Fiziki açar və ya kartlardan istifadə ehtiyacını aradan qaldırmaqla, bu texnologiyalar itmiş və ya oğurlanmış giriş məlumatlarının riskini azaldır və təhlükəsizliyi artırır. Təhlükəsizliyin artırılmasının yanında, üz tanıma qonaqlar üçün böyük rahatlıq təmin edir. Bu, qeydiyyat prosesini sadələşdirərək müasir dövrün sürətli və səmərəli xidmət gözləntilərinə uyğun hamar bir təcrübə təqdim edir (Əlirzayev, 2010; Əliquliyev, 1013). Bundan əlavə, bu sistemlər ağıllı otaq texnologiyaları ilə yaxşı inteqrasiya olunur və qonaq daxil

olduqda işıqlandırma, temperatur və əyləncə üstünlükləri kimi fərdiləşdirilmiş parametrləri avtomatik olaraq tənzimləyərək ümumi qonaq təcrübəsini daha da yaxşılaşdırır.

Süni intellektlə təkmilləşdirilmiş video nəzarət sistemləri qonaqpərvərlik mühitlərində təhdidlərin aşkar edilməsi və idarə olunma üsullarını dəyişdirir (Surendra, 2023, s. 415; Smith, Patel, & Kim, 2020). Ənənəvi nəzarət sistemlərindən fərqli olaraq, AI əsaslı sistemlər maşın öyrənmə alqoritmlərindən istifadə edərək qeyri-adi nümunələri müəyyən edir, potensial təhdidləri tanıyır və təhlükəsizlik personalına real vaxt rejimində xəbərdarlıqlar göndərir. Bu proaktiv yanaşma reaksiya müddətlərini əhəmiyyətli dərəcədə azaldır və təhlükəsizlik tədbirlərinin effektivliyini artırır. AI əsaslı nəzarətin əsas üstünlüklərindən biri onun zamanla öyrənmə və adaptasiya qabiliyyətidir. Bu sistemlər gündəlik fəaliyyətlə potensial şübhəli davranışları ayırd edə bilir, yanlış xəbərdarlıqların sayını azaldır və təhdidlərin daha dəqiq aşkarlanmasını təmin edir. Məsələn, AI məhdudlaşdırılmış sahələrdə dolaşan şəxsləri və ya izdihamlı ərazilərdə tərk edilmiş əşyaları müəyyən edə bilər. Bu səviyyədə ağıllı texnologiya həm qonaqların təhlükəsizliyini, həm də əməliyyat effektivliyini artırır. AI əsaslı nəzarət iş axını diaqramı süni intellektlə təchiz olunmuş qabaqcıl təhlükəsizlik sistemlərinin addım-addım işləmə prosesini vizual şəkildə göstərir. Proses nəzarət kameralarından alınan videoməlumatlar ilə başlayır və daha sonra nümunələrin tanınması və davranış analizini həyata keçirən AI emalı mərhələsi ilə davam edir. Sistem potensial təhdidləri müəyyən edir və təhlükəsizlik komandalarına real vaxt rejimində xəbərdarlıqlar göndərir, bu da personalın sürətli reaksiya verməsinə imkan yaradır. Bu diaqram təhlükəsizliyin təmin edilməsi üçün texnologiya və insan müdaxiləsinin problemsiz inteqrasiyasını vurğulayır. AI əsaslı anomaliya aşkarlama sistemləri əməliyyat proseslərində qeyri-adi nümunələri və ya şübhəli davranışları müəyyən etməkdə mühüm rol oynayır (Jones, & Wang, 2021; Kaspersky, 2021; Lee, & Park, 2022). AI böyük həcmdə məlumatları real vaxt rejimində təhlil edərək potensial təhlükəsizlik təhdidlərini göstərə biləcək anomaliyaları aşkarlaya bilər, məsələn, icazəsiz giriş cəhdləri, qeyri-adi əməliyyatlar və ya qorunan sahələrdə anormal hərəkət nümunələri. Otellərin idarəetmə şöbələrində işçi fəaliyyətlərinin və giriş qeydiyyatlarının izlənməsi üçün istifadə olunan sistemlər buna nümunədir. Bu sistemlər həssas sahələrə qeyri-adi girişləri qeyd edərək rəhbərliyi potensial təhlükəsizlik pozuntularını araşdırmağa xəbərdar edə bilər. Eyni zamanda, anomaliya aşkarlama rəqəmsal əməliyyatlarda fırıldaqçılıq fəaliyyətlərini müəyyən etmək üçün də tətbiq oluna bilər, məsələn, qeyri-adi sayda rezervasiya ləğvləri və ya anormal ödəniş nümunələri. Anomaliya aşkarlamanın inteqrasiyası yalnız təhlükəsizliyi artırmaqla qalmır, həm də risklərin proaktiv idarə olunmasına şərait yaradır. Problemləri erkən müəyyən edib həll etməklə, qonaqpərvərlik müəssisələri potensial insidentlərin qarşısını ala və qonaqlarının təhlükəsizliyini təmin edə bilər.

Digər texnologiya isə Cloud, yəni bulud texnologiyalarıdır. Bulud texnologiyalarının meydana gəlməsi son illər informasiya texnologiyaları sənayesinə böyük təsir göstərmişdir (Əliquliyev, 2013, s. 3; Rzayev, 2023). Bulud texnologiyaları qonaqpərvərlik sənayesində müştəri məlumatlarının qorunmasında əvəzolunmaz rol oynayır. Bu sistemlər həssas məlumatların, məsələn, şəxsi detalları, ödəniş məlumatlarını və rezervasiya tarixçəsini həm ötürülmə zamanı, həm də saxlanma zamanı qorumaq üçün qabaqcıl şifrələmə üsullarından istifadə edirlər. Şifrələmə məlumatların icazəsiz əldə edilməsinə və ya tutulmasına baxmayaraq oxunmaz və təhlükəsiz qalmasını təmin edir. Çoxfaktorlu autentifikasiya (MFA) isə istifadəçilərin öz kimliklərini bir neçə vasitə ilə, məsələn, şifrələr, biometrik məlumatlar və ya bir dəfəlik kodlar vasitəsilə təsdiqləməsini tələb edərək məlumatlara giriş təhlükəsizliyini daha da gücləndirir. Bu çoxqatlı yanaşma icazəsiz giriş riskini minimuma endirir və həssas məlumatların qorunmasını təmin edir. Şifrələmə və MFA-nın inteqrasiyası ilə bulud platformaları qonaq məlumatlarını qorumaq üçün güclü bir çərçivə təqdim edir. Bulud platformaları qonaqpərvərlik müəssisələrinin ehtiyaclarına uyğunlaşdırıla bilən çevik məlumat idarəetmə həlləri təqdim edir. Mərkəzləşdirilmiş sistemlər bütün qonaq məlumatlarını vahid verilənlər bazasında birləşdirərək onlara asan çıxış və məlumatların ardıcılığını təmin edir. Bu yanaşma xüsusilə bir neçə filialı olan böyük otel zəncirləri üçün faydalıdır, çünki müxtəlif yerlərdən gələn məlumatların sinxronlaşdırılması və əlçatanlığı asanlaşdırılmalıdır. Əksinə, desentralizə olunmuş sistemlər məlumatları bir neçə server arasında paylayaraq tək nöqtəli nasazlıq riskini azaldır və məlumatların ehtiyat

nüsxələnməsini artırır. Hər iki yanaşma müasir bulud platformalarının güclü təhlükəsizlik xüsusiyyətlərindən faydalanır, məsələn, avtomatlaşdırılmış yeniləmələr, rol əsaslı giriş nəzarətləri və GDPR və CCPA kimi məxfilik qaydalarına uyğunluq. Bu xüsusiyyətlər yalnız qonaqların məxfiliyini qorumaqla kifayətlənmir, həm də məlumat idarəetmə proseslərini asanlaşdırır və müəssisələrin üstün xidmət göstərməyə fokuslanmasına imkan verir. Bulud sistemləri kiberhücumlar, aparat nasazlıqları və ya təbii fəlakətlər kimi fəvqəladə hallar zamanı məlumat itkisinin qarşısını almaqda və biznesin fasiləsizliyini təmin etməkdə həyati rol oynayır. Avtomatlaşdırılmış ehtiyat nüsxə həlləri bulud platformalarının əsas xüsusiyyətlərindən biridir və müntəzəm, çoxsaylı məlumat surətlərinin yaradılmasını təmin edir ki, bu surətlər lazım olduqda tez bir zamanda bərpa oluna bilsin. Bu yanaşma əməliyyatlarda minimal pozuntuya yol verir və məlumatların daimi itkisindən qoruyur. Bulud əsaslı fəlakətdən bərpa sistemlərinin miqyaslı bilən və çevik strukturu qonaqpərvərlik müəssisələrinə strategiyalarını dəyişən ehtiyaclarla uyğunlaşdırmağa imkan verir. Məsələn, kritik məlumatların real vaxtda surətlənməsi ən yenilənmiş məlumatların belə qorunmasını təmin edir. Bu həllərdən istifadə etməklə müəssisələr qonaqların etibarını qoruyur və çətin şəraitdə belə fasiləsiz əməliyyatları təmin edə bilər.

Rəqəmsallaşmanın artdığı qonaqpərvərlik sahəsində təhlükəsizlik risklərinin müəyyənləşdirilməsi və azaldılması əməliyyatların qorunması və qonaq məlumatlarının müdafiəsi üçün həyati əhəmiyyət kəsb edir. Real vaxt rejimində təhdidlərin izlənməsi və proqnozlaşdırıcı analiz kimi proaktiv tədbirlər müəssisələrə potensial zəif nöqtələri istismar olunmadan əvvəl aşkarlamağa imkan verir. Süni intellekt əsaslı sistemlərdən istifadə etməklə təşkilatlar şəbəkə trafikinə dair anomaliyaları müəyyən edə, icazəsiz giriş cəhdlərini aşkarlaya və ortaya çıxan kiber təhdidləri qabaqcadan görmə imkanına malik olurlar. Müntəzəm auditlər və penetrasiya testləri güclü risk idarəetmə strategiyasının vacib komponentləridir. Auditlər təşkilatın təhlükəsizlik vəziyyətinin geniş qiymətləndirilməsini təmin edir və məlumatların saxlanması, giriş nəzarətləri və ya uyğunluq protokollarındakı zəif nöqtələri üzə çıxarmağa kömək edir. Penetrasiya testləri, kiberhücumları simulyasiya etməklə mövcud müdafiələrin effektivliyini qiymətləndirir və sistemləri gücləndirmək üçün praktik tövsiyələr verir. Bu tədbirlər birlikdə müəssisələrin təhlükəsizlik boşluqlarına vaxtında reaksiya verməsini təmin edir və bəla başa gələ biləcək pozuntuların riskini azaldır.

Qonaqpərvərlik sektorunda kiber təhlükəsizliyi gücləndirmək üçün ixtisaslaşmış təhlükəsizlik texnologiyaları təchizatçıları ilə əməkdaşlıq əsas strategiyalardan biridir. Bu tərəfdaşlıqlar müəssisələrə müasir həllər, ekspertiza və daxili imkanlarla təmin olunmayan resurslara çıxış imkanı verir. Etibarlı təchizatçılarla işləməklə qonaqpərvərlik şirkətləri süni intellekt əsaslı təhdid aşkarlama, biometrik autentifikasiya və şifrələnmiş ödəniş platformaları kimi qabaqcıl sistemləri tətbiq edə bilərlər. Məsələn, Accor Hotels kiber təhlükəsizlik firması Symantec ilə əməkdaşlıq edərək məlumatların qorunması üçün alətlər dəstini tətbiq etmiş və qlobal əməliyyatlarında qonaq məlumatlarının qorunmasını artırmışdır. Oxşar şəkildə, Hyatt Hotels IBM Security ilə əməkdaşlıq edərək genişmiqyaslı hadisələrə cavab planı hazırlamış və potensial pozuntulara reaksiya müddətini əhəmiyyətli dərəcədə azaltmışdır. Bu əməkdaşlıqlar göstərir ki, tərəfdaşlıqlar təşkilatın ümumi təhlükəsizlik çərçivəsini gücləndirə bilər və eyni zamanda, əsas missiya olan müstəsna qonaq təcrübəsi təqdim etməyə fokuslanmasına imkan verir.

Nəticə

Bu məqalə süni intellekt (AI) və bulud texnologiyalarının qonaqpərvərlik sənayesində təhlükəsizlik və məxfiliyi gücləndirməkdəki transformativ rolunu vurğulayır. Üz tanıma vasitəsilə otaqlara təhlükəsiz giriş, anomaliya aşkarlama sistemləri və ağıllı video nəzarət kimi AI əsaslı alətlər əməliyyat təhlükəsizliyini və qonaqların təhlükəsizliyini əhəmiyyətli dərəcədə artırır. Bulud əsaslı sistemlər isə məlumatların təhlükəsiz saxlanması, şifrələnməsi və fəvqəladə hallar üçün bərpa imkanları ilə güclü çərçivələr təmin edir, beləliklə, qonaq məlumatlarının bütövlüyü və əlçatanlığı hətta çətin şəraitdə də qorunur. Bu texnologiyalar birlikdə kiber təhlükəsizlik və uyğunluq tələblərini qarşılayır, qonaqların etibarını artırır və qonaqpərvərlik müəssisələrinin nüfuzunu qoruyur.

Gələcək Tendensiyalar Qonaqpərvərlik Təhlükəsizliyində “Qonaqpərvərlik təhlükəsizliyinin gələcəyi kvant şifrələmə kimi qabaqcıl texnologiyaların tətbiqini əhatə etməyə hazırdır. Kvant mexanikası prinsiplərindən istifadə edən bu texnologiya, demək olar ki, qırılmaz şifrələmə metodları yaradaraq həssas məlumatların qorunmasında yeni imkanlar təqdim edir. Lakin belə inkişaf etmiş texnologiyaların integrasiyası özünəməxsus çətinliklər də gətirəcək. Yeni məxfilik çərçivələrinin tətbiqi infraqstruktura, təlim və uyğunluq tədbirlərinə ciddi investisiyaları tələb edəcək. Müəssisələr gələcək GDPR tipli qanunvericiliklərlə uyğunlaşmalı və əməliyyat effektivliyi ilə yüksək məxfilik standartlarını tarazlaşdırmalıdır. Bundan əlavə, qonaqların etibarını qorumaq üçün məlumat istifadəsi barədə şəffaf kommunikasiya və kiber təhdidlərin azaldılması istiqamətində davamlı səylər zəruridir. Bu çətinlikləri qabaqcıdan nəzərə alaraq, qonaqpərvərlik sənayesi innovasiyanı davam etdirir və eyni zamanda, qonaqlarının təhlükəsizliyini və məxfiliyini təmin edə bilər.

Ədəbiyyat

1. Choice Hotels Case Study. (2022). Investigating cloud misconfigurations and data breaches in hospitality. *Journal of Cloud Security*, (421).
2. Cybersecurity Impact Analysis. (2021). Financial repercussions of data breaches in the hospitality industry. *Journal of Cybersecurity Economics*, (587).
3. Əlirzayev, Ə. (2010). *Turizmin iqtisadiyyatı və idarə edilməsi*. İqtisad Universiteti Nəşriyyatı.
4. Əliquliyev, R. (2013) Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi. *İnformasiya texnologiyaları problemləri*, 3–14.
5. Jones, M., & Wang, T. (2021). The role of emerging technologies in enhancing the hospitality experience. *International Journal of Hospitality Management*.
6. Kaspersky, E. (2021). Cybersecurity in the hospitality industry: Protecting data and digital identity. *Journal of Information Security*, 215–228.
7. Qasimov, T, & Əhmədov, E. (2022). Turizm sənayesində rəqəmsal texnologiyaların tətbiqi və təhlükəsizlik məsələləri. *Azərbaycan Turizm Tədqiqatları Jurnalı*, 45–56. ADMIU Nəşriyyatı.
8. Lee, J., & Park, H. (2022). Overcoming technological integration challenges in legacy hospitality systems. *Journal of Hospitality Technology Studies*, 255.
9. Marriott Case Study. (2019). An analysis of data breaches and their impacts on global hospitality brands. *Data Privacy and Security Review*, 321.
10. Rzayev, S. (2023). Bulud texnologiyalarının qonaqpərvərlik sektorunda tətbiqi və məlumat təhlükəsizliyi problemləri. AMEA, *İnformasiya Texnologiyaları və İdarəetmə Jurnalı*, 78–85.
11. Surendra, M. (2023). Enhancing Security and Privacy in Hospitality with AI and Cloud Technologies. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 414–421.
12. Smith, A., Patel, R., & Kim, Y. (2020). *Challenges in integrating cybersecurity frameworks in the hospitality industry*. IEEE Transactions on Industry Applications.

Daxil oldu: 23.06.2025

Qəbul edildi: 22.09.2025