UOT 336.7.004

Kənan Nüsrət oğlu ATAYEV
Bakı Biznes Universiteti, doktorant
atayevkenan29@gmail.com
https://doi.org/10.30546/4.71.73001.2026.005.010

DAXİLİ NƏZARƏT SİSTEMLƏRİNİN RƏQƏMSAL BANKÇILIĞA İNTEQRASİYASI

Xülasə

Tədqiqatın məqsədi – Bu tədqiqatın məqsədi rəqəmsal bankçılıq şəraitində daxili nəzarət sistemlərinin rolunu, funksiyalarını və müasir texnoloji mühitə uyğun effektiv inteqrasiyasını nəzəri və praktiki baxımdan araşdırmaqdır. Əsas hədəf rəqəmsal texnologiyaların bankların nəzarət mexanizmlərinə necə təsir etdiyini, yeni yaranan risklər fonunda bu sistemlərin necə təkmilləşdirilə biləcəyini ortaya qoymaqdır.

Tədqiqatın metodologiyası – Tədqiqat əsasən **analitik və deskriptiv metodlardan** istifadə etməklə aparılmışdır. Müasir bank sistemində tətbiq olunan rəqəmsal alətlər, daxili nəzarət strukturları və risk idarəetmə mexanizmləri beynəlxalq təcrübə və normativ sənədlər əsasında təhlil olunmuşdur. Tədqiqat həmçinin **komparativ analiz** yolu ilə ənənəvi və rəqəmsal nəzarət metodlarının müqayisəsini təqdim edir. Eləcə də, **təcrübəyə əsaslanan ümumiləşdirmə** və **mənbə araşdırmaları** ilə elmi əsaslandırma təmin olunmuşdur.

Tədqiqatın tətbiqi əhəmiyyəti – Bu tədqiqat bank rəhbərləri, risk menecerləri, daxili auditorlar və tənzimləyici orqanlar üçün praktik dəyərə malikdir. Tədqiqatın nəticələri banklara daxili nəzarət sistemlərini rəqəmsal mühitin çağırışlarına uyğunlaşdırmaqda yardımçı olur. Həmçinin bu araşdırma, bank sektorunda rəqəmsallaşma prosesində təhlükəsizliyin və davamlılığın təmin olunması üçün strateji qərarların verilməsində metodoloji baza yaradır.

Tədqiqatın nəticələri – Tədqiqat göstərir ki, rəqəmsal texnologiyaların inteqrasiyası banklarda daxili nəzarət sistemlərinin effektivliyini əhəmiyyətli dərəcədə artırmaqla yanaşı, yeni risklərin idarə olunmasını da zəruri edir.

Tədqiqatın orijinallığı və elmi yeniliyi – Bu tədqiqatın elmi yeniliyi ondan ibarətdir ki, daxili nəzarət sistemləri ilk dəfə olaraq **rəqəmsal bankçılıq kontekstində kompleks şəkildə** təhlil edilmiş və onların **süni intellekt, blokçeyn və avtomatlaşdırılmış monitorinq texnologiyaları** ilə inteqrasiyası nəzəri əsaslarla izah edilmişdir. Əlavə olaraq, daxili nəzarət sisteminin həm texniki, həm də təşkilati aspektləri üzrə çağırışlar və üstünlüklər detallı şəkildə sistemləşdirilmişdir. Bu baxımdan, tədqiqat Azərbaycan bank sektorunun spesifik tələbləri ilə qlobal trendlər arasında körpü qurmaq baxımından yenilik daşıyır.

Açar sözlər: rəqəmsal bankçılıq, daxili nəzarət sistemi, daxili audit, kibertəhlükəsizlik, avtomatlaşdırma, komplayens.

Giriş

Müasir bank sektoru rəqəmsal transformasiyanın dərin təsiri altındadır. Bank xidmətlərinin rəqəmsallaşması (internet və mobil bankçılıq, fintek həlləri və s.) əməliyyatların sürətini və əlçatanlığını artırsa da, yeni risklər və çağırışlar da meydana çıxarır. Bu şəraitdə banklarda daxili nəzarət sistemlərinin (DNS) rolunun daha da vacibləşdiyi müşahidə olunur. Daxili nəzarətin metodoloji inkişafının təhlili göstərir ki, bu konsepsiya qədim dövrlərdən bu günədək mühüm mərhələlər keçmişdir — ilkin mülkiyyətin qorunmasına nəzarət formalarından tutmuş müasir korporativ idarəetmə və risklərin idarə edilməsi sistemlərinə qədər [2]. Rəqəmsal bankçılıq mühitində əməliyyat riskləri, kibertəhlükələr, məlumat sızmaları kimi təhdidlər yüksəlir və buna uyğun olaraq effektiv daxili nəzarət mexanizmləri olmadan bankların sabit və etibarlı fəaliyyəti təmin edilə bilməz. Tədqiqatlar göstərir ki, dövlət tənzimləməsi ilə yanaşı, bankların daxili nəzarət sistemlərinin mükəmməlliyi rəqəmsal dövrdə risklərin idarə olunmasında həlledici əhəmiyyət daşıyır. Beləliklə,

rəqəmsal bankçılıq şəraitində daxili nəzarət sistemlərinin inteqrasiyası məsələsinin nəzəri və praktiki cəhətdən araşdırılması aktualdır. Bu məqalədə rəqəmsal bank mühitində daxili nəzarət sistemlərinin mahiyyəti, funksiyaları və onların effektiv inteqrasiyasının vacibliyi təhlil olunur. Əvvəlcə banklarda daxili nəzarət sistemlərinin ümumi konsepsiyası, strukturu və ənənəvi nəzarət mexanizmləri şərh edilir. Daha sonra rəqəmsal bankçılığın doğurduğu yeni risk amilləri və çağırışlar fonunda daxili nəzarət sistemlərinin uyğunlaşdırılması və rəqəmsal alətlərdən istifadəsi müzakirə olunur.

Banklarda Daxili Nəzarət Sistemlərinin Əhəmiyyəti və Strukturu. Banklar ciddi şəkildə tənzimlənən bir mühitdə fəaliyyət göstərirlər və daxili nəzarət sistemləri beynəlxalq tənzimləyici qurumların diqqətində olan əsas məsələlərdən biridir. Banklarda nəzarət, ümumilikdə, iki əsas istiqamətdə həyata keçirilir: xarici (bankdan kənar) nəzarət və daxili nəzarət. Xarici nəzarət dedikdə əsasən Mərkəzi Bank və digər müvafiq nəzarət orqanları tərəfindən banklara yönəlmiş tənzimləmə və yoxlama tədbirləri nəzərdə tutulur. Məsələn, Azərbaycan Mərkəzi Bankı bankların fəaliyyətini lisenziya vermə, prudensial tələblərin – məsələn, minimum kapital səviyyəsi, likvidlik göstəriciləri, böyük risklərin məhdudlaşdırılması kimi – tətbiqi, dövri hesabatların qəbul edilməsi və yerində yoxlamalar vasitəsilə nəzarətdə saxlayır. Xarici nəzarətin digər bir vacib forması isə müstəqil auditorlar tərəfindən həyata keçirilən xarici auditdir. Qanunvericilik bu sahədə kommersiya banklarına illik maliyyə hesabatlarını müstəqil auditorun rəyi ilə təsdiqləməyi və ictimaiyyətə açıqlamağı tələb edir. Bu cür audit prosesi bankların maliyyə sabitliyini dəstəkləyən əsas struktur elementlərindən biri olmaqla, həm də maliyyə hesabatlarının dürüstlüyünü qiymətləndirmək və uçotun müvafiq standartlara uyğun şəkildə aparılıb-aparılmadığını müəyyənləşdirmək məqsədi daşıyır.

Daxili nəzarət – bankın öz strukturu daxilində formalaşan və icrası bankın səhmdarları, Müşahidə Şurası, idarə heyəti və digər məsul şəxslər tərəfindən yerinə yetirilən nəzarət mexanizmidir. Bu nəzarət sistemi əsasən gündəlik əməliyyatlar zamanı meydana çıxan risklərin minimuma endirilməsi, potensial yanlışlıqların qarşısının alınması və fəaliyyətin həm daxili qaydalara, həm də mövcud hüquqi tələblərə uyğun həyata keçirilməsini təmin etməyə yönəlib. Daxili nəzarət anlayışı yalnız mühasibat sənədlərinin yoxlanılması ilə məhdudlaşmır; o, eyni zamanda bankın bütün əməliyyat sahələrində səmərəliliyin artırılması, resursların – xüsusilə aktivlərin – qorunması və informasiyanın dəqiqliyinin təmin olunması kimi mühüm vəzifələri də əhatə edir. Bankda effektiv və tam əhatəli idarəetmənin qurulması üçün daxili nəzarət sisteminin kompleks və bir-biri ilə əlaqəli elementlər əsasında təşkil olunması vacibdir. Qlobal təcrübədə bu nəzarət sisteminin beş əsas struktur komponenti mövcuddur.

1. Nəzarət mühiti (idarəetmə və etik mühit) – bank rəhbərliyinin nəzarətə verdiyi əhəmiyyət, etik dəyərlər və təşkilati struktur. Bu, effektiv nəzarət üçün fundamental zəmin yaradır.

2. Risklərin müəyyən edilməsi və qiymətləndirilməsi – bankın qarşılaşa biləcəyi risklərin (maliyyə, əməliyyat, hüquqi, reputasiya və s.) vaxtında aşkarlanması və ölçülməsi. Rəhbərlik ortaya çıxan yeni risk trendlərini mütəmadi dəyərləndirməlidir.

3. Nəzarət tədbirləri (prosedurlar) – riskləri azaltmaq və səhvlərin qarşısını almaq üçün tətbiq olunan konkret daxili qaydalar, prosedurlar və siyasətlər. Buraya əməliyyatların səlahiyyətləşdirilməsi (icazələrin verilməsi), vəzifələrin ayrılması (müəyyən bir şəxsin tam proses üzərində nəzarət etməməsi üçün iş bölgüsü), məlumatların üzləşdirilməsi (müxtəlif məlumat mənbələrinin uyğunluğunun yoxlanılması) kimi mexanizmlər daxildir. Məsələn, banklarda kritik əməliyyatlar zamanı “dörd göz prinsipi”nin tətbiqi – yəni bir əməliyyatın iki ayrı şəxs tərəfindən təsdiqlənməsi – tipik nəzarət prosedurudur.

4. Məlumat və kommunikasiya – bank daxilində müvafiq məlumat axınının təmin olunması, düzgün və tam informasiyanın lazımi səviyyələrə çatdırılması. Daxili hesabatlılıq sistemləri, idarəetmə informasiya sistemləri bu komponentin tərkib hissəsidir.

5. Monitorinq (nəzarət sisteminin izlənməsi) – mövcud nəzarət mexanizmlərinin effektivliyinin daimi əsasda izlənməsi və qiymətləndirilməsi. Monitorinq həm davamlı idarəetmə nəzarətləri,

həm də müstəqil qiymətləndirmələr (məsələn, daxili audit tərəfindən) formasında həyata keçirilir. Aşkar edilən çatışmazlıqların aradan qaldırılması üçün düzəldici tədbirlərin görülməsi də monitorinq prosesinin vacib hissəsidir.

Daxili nəzarət sisteminin əsas vəzifələri bunlardır [3, s.82]:

- Əməliyyatların səmərəliliyi: Bank fəaliyyətinin effektiv və mənfəətli şəkildə aparılmasını təmin etmək, resurslardan səmərəli istifadə olunmasına nəzarət etmək.
- Uyğunluq (komplayens): Bankda aparılan bütün əməliyyatların qanunvericiliyin, tənzimləyici orqanların tələblərinin və daxili qaydaların tələblərinə uyğunluğunu təmin etmək. Bu, həm də kreditorların və əmanətçilərin maraqlarını qorumaq üçündür.
- Maliyyə məlumatlarının doğruluğu: Mühasibat uçotu və maliyyə hesabatlarının düzgün, dəqiq və tam olmasını təmin etmək. Yalnız etibarlı maliyyə məlumatlarına əsasən düzgün qərarlar vermək mümkündür.
- Aktivlərin qorunması: Bankın aktivlərinin (pul vəsaitləri, kredit portfeli, avadanlıq və s.) oğurluq, sui-istifadə və digər itkilərdən qorunmasını təmin edən mexanizmlər yaratmaq. Eyni zamanda öhdəliklərin (məsələn, depozitlərin) dəqiq uçotu və idarə olunması.
- Səhvlərin və saxtakarlıqların qarşısının alınması: İstər qəsdən, istərsə də bilməyərəkdən ortaya çıxan yanlışlıqların vaxtında aşkarlanaraq düzəldilməsi. Məsələn, uçota alınmamış əməliyyat qalmasın, əməliyyatlar real icra olunmadığı halda uçota salınmasın, qeydlərdə müvafiq dövrə aidlik prinsipi pozulmasın və s.

Qeyd olunmalıdır ki, səmərəli daxili nəzarət sistemi bank daxilində bir-birini tamamlayan müxtəlif nəzarət formalarının və yanaşmalarının vəhdətindən ibarətdir. Bu nəzarətə rəhbərlik səviyyəsində həyata keçirilən idarəetmə nəzarəti, struktur bölmələr və filiallarda aparılan özününəzarət mexanizmləri, həmçinin daxili qaydalar və prosedurların icrasına nəzarət tədbirləri daxildir. Daxili nəzarət sisteminin əsas və ayrılmaz komponentlərindən biri isə daxili audit funksiyasıdır. Daxili audit, bankın fəaliyyət sahələrini və əməliyyatlarını müstəqil şəkildə qiymətləndirən və yoxlayan bir mexanizmdir. Audit işçiləri bankdaxili nəzarət alətlərinin effektivliyini, risklərin idarə olunmasına dair prosedurların düzgün həyata keçirilib-keçirilmədiyini araşdırır, aşkar olunan nöqsanları rəhbərliyə məruzə edirlər və həmin çatışmazlıqların aradan qaldırılması üçün tövsiyələr irəli sürürlər. Beləliklə, daxili audit funksiyası daxili nəzarət sistemində “sonuncu müdafiə səddi” rolunu oynayır – digər nəzarət metodlarının çatışmayan tərəflərini üzə çıxarmaqda mühüm vasitəyə çevrilir. Daxili nəzarət sistemində tez-tez qarşılaşılan zəif cəhətlərdən bir neçəsini qeyd etmək olar. Birincisi, risklərin vaxtında müəyyənləşdirilməməsi və ya lazımi səviyyədə qiymətləndirilməməsi – bu, o deməkdir ki, bank yeni yaranan riskləri gec dərk edir və adekvat tədbir görməkdə ləngiyir. İkincisi, əsas nəzarət mexanizmlərinin mövcud olmamasıdır. Məsələn, bəzi maliyyə əməliyyatları üzrə icazə və təsdiqləmə prosesləri qurulmamış olur, vəzifələrin bölüşdürülməsi prinsipinə lazımi diqqət yetirilmir və ya dövri şəkildə üzləşdirmə aparılmır. Üçüncü zəiflik informasiya axınının qeyri-effektivliyidir – yəni bank daxilində müxtəlif idarəetmə səviyyələri arasında məlumat ötürülməsi zəif təşkil olunduğundan, mühüm informasiya aidiyyəti şəxslərə gec çatır. Dördüncüsü, daxili audit və nəzarət fəaliyyətlərinin kifayət qədər inkişaf etməməsidir; bəzi hallarda bu funksiyalar ya ümumiyyətlə təşkil olunmur, ya da mövcud audit strukturları resurs və səlahiyyət baxımından məhduddur. Beşinci nöqsan isə əməkdaşların peşə hazırlığının kifayət qədər olmaması və etik davranış normalarına əməl edilməməsidir. Belə zəifliklər rəqəmsal bankçılıq şəraitində daha təhlükəli nəticələr doğura bilər, çünki texnoloji mühitdə cüzi bir boşluq belə sürətlə ciddi maliyyə itkilərinə gətirib çıxara bilər. Buna görə də banklar daxili nəzarət sistemlərini davamlı olaraq gücləndirməli və onları rəqəmsal yeniliklərin doğurduğu yeni risklərə uyğun şəkildə modernləşdirməlidirlər.

Rəqəmsal Bankçılıq: Yeni Çağırışlar və Risklər. Rəqəmsal bankçılıq dedikdə, banklar tərəfindən müvafiq proqram təminatı, həqiqiliyin elektron formada müəyyən edilməsi metodu və kommunikasiya vasitələrinin istifadəsi ilə istifadəçilərin öz bank hesabları vasitəsilə ödənişləri həyata keçirməsi, apardıqları əməliyyatlar üzrə məlumatın əldə edilməsi və digər bank xidmətlərinin

məsafədən idarə olunmasına imkan verən informasiya texnologiyaları məhsulu başa düşülür [4, s.306]. Son illərdə yüksək sürətli internetin, ağıllı cihazların və maliyyə texnologiyaları sahəsinin genişlənməsi nəticəsində müştərilər istənilən zaman və istənilən məkandan maliyyə əməliyyatlarını icra etmək imkanına malik olublar. Rəqəmsal bank xidmətlərinin əsas üstünlükləri – sürət, rahatlıq və geniş istifadə imkanları – bank sektorunda rəqabət qaydalarını dəyişmiş və bu istiqamətdə texnoloji yeniliklərin tətbiqini vacib etmişdir.

Bununla yanaşı, rəqəmsal platformaların tətbiqi bank sistemində mövcud olan risklərin həm miqyasını, həm də formasını dəyişdirmişdir. Elektron bankçılıq xidmətləri üzrə baş verəcək riskləri əsasən aşağıdakı kimi qruplaşdırmaq olar: kiber risklər; texnoloji risklər; fəaliyyətin davamlılığı riskləri; reputasiya riski [4, s.333]. Bu sahədə ən aktual problemlərdən biri informasiya təhlükəsizliyinin pozulması ilə bağlıdır. Elektron infrastruktur üzərindən məlumatların emalı və saxlanması, onlayn ödəniş sistemləri kiberhücumlara açıq mühit yaradır. Belə hallarda şəxsi və maliyyə məlumatlarının oğurlanması, istifadəçi hesablarına qanunsuz giriş, xidmətlərin fəaliyyətinin pozulması kimi hallar baş verə bilər ki, bu da həm maddi zərərə, həm də bankın etibarına mənfi təsir göstərir. Məlumatların təhlükəsizliyinin təmin olunması və istifadəçi məxfiliyinin qorunması banklar üçün əsas prioritetlərdən birinə çevrilmişdir. Bu məqsədlə gücləndirilmiş şifrələmə sistemləri, çoxpilləli identifikasiya üsulları, anomaliya aşkarlayan texnologiyalar və s. kimi texniki və inzibati nəzarət mexanizmlərindən istifadə olunmalıdır. Digər mühüm risk isə texnoloji nasazlıqlarla əlaqədardır. Rəqəmsal platformaların fasiləsiz və etibarlı işləməsi üçün banklar genişmiqyaslı informasiya texnologiyaları infrastrukturuna əsaslanırlar. Ümumi olaraq elektron bankçılıq sahəsində baş verəcək risklərin qarşısının alınması məqsədi ilə aşağıdakı tədbirlərin görülməsinə zərurət vardır [4, s.337]:

- giriş səlahiyyətinə nəzarət;
- səlahiyyət bölgüsü;
- əməliyyatlar üzrə limitlər;
- maliyyə savadlılığının yüksəldilməsi;
- agentlərə mütəmadi təlimlərin keçirilməsi;
- əməkdaşlar üçün treninqlər.

Lakin proqram təminatındakı səhvlər, serverlərin dayanması, bulud xidmətlərində nasazlıqlar, rabitə və enerji təminatındakı kəsintilər nəticəsində bank xidmətləri müvəqqəti olaraq dayandırıla bilər. Bu cür hallarda müştərilər əməliyyatlarını vaxtında həyata keçirə bilmədikləri üçün bank həm maliyyə baxımından, həm də müştəri məmnuniyyəti baxımından itkilərlə üzləşir. Rəqəmsal mühitdə fırıldaqçılıq halları da fərqli formalar alıb. Əgər əvvəllər bu hallar əsasən fiziki formada baş verirdisə, indi isə onlayn mühitdə kimlik məlumatlarının oğurlanması, fişinq (aldadıcı e-poçtlar), bank kartı məlumatlarının ələ keçirilməsi, sosial mühəndislik yolu ilə manipulyasiya kimi metodlar yayılmışdır. Bu hallarla mübarizə aparmaq üçün banklar real vaxtda nəzarət edən sistemlərdən, şübhəli əməliyyatları avtomatik təyin edən süni intellekt alqoritmlərindən və istifadəçi davranışlarını təhlil edən vasitələrdən istifadə etməyə başlamışlar. Bu cür texnoloji tədbirlər eyni zamanda bankın daxili nəzarət sisteminin rəqəmsal komponentləri kimi çıxış edir. Nəticə etibarilə, rəqəmsal bankçılıq mühiti banklar qarşısında bir sıra yeni təhlükələr və çətinliklər yaratmışdır: kibertəhlükələr, texnoloji dayanıqlılıq problemləri, fırıldaqçılığın müasir formaları, dəyişən hüquqi tələblər və s. Bu təhlükələrin qarşısını almaq üçün banklar mövcud daxili nəzarət strukturlarını yenidən dəyərləndirməli, rəqəmsal texnologiyalara uyğunlaşdırmalı və zəruri hallarda təkmilləşdirməlidirlər.

Daxili Nəzarət Sistemlərinin Rəqəmsal Bankçılığa İntegrasiyası. Rəqəmsal bankçılıq mühitində daxili nəzarət sistemlərinin inteqrasiyası dedikdə, ənənəvi nəzarət metodlarının müasir rəqəmsal texnologiyalarla birləşdirilərək bank əməliyyatlarına tətbiqi nəzərdə tutulur. Bu, iki əsas aspekti əhatə edir: 1. Rəqəmsal alətlərin daxili nəzarət funksiyasına uyğunlaşdırılması, yəni daxili nəzarətin avtomatlaşdırılması və optimallaşdırılması üçün yeni texnologiyalardan istifadə; 2. Daxili nəzarət sisteminin rəqəmsal bank əməliyyatlarına sirayət etməsi, yəni rəqəmsal kanallarda

baş verən bütün proseslərin nəzarət sistemi çərçivəsində olması. Birinci aspekt üzrə, müasir dövrdə rəqəmsal nəzarət alətləri sürətlə inkişaf edir. Banklar artıq daxili nəzarətin bir çox elementlərini avtomatlaşdırılmış sistemlər üzərinə keçirirlər. Məsələn, ERP (Enterprise Resource Planning) və ya xüsusi bank daxili nəzarət proqramları vasitəsilə bir çox yoxlama prosedurları insan müdaxiləsi olmadan, real-vaxt rejimində aparılır. Proseslərin avtomatlaşdırılması və davamlı monitorinq halları daxili nəzarətin effektivliyini və düzgünlüyünü əhəmiyyətli dərəcədə artırır. Rəqəmsal alətlər təkrarlanan, rutin nəzarət tapşırıqlarını (məsələn, gündəlik tranzaksiyaların üzləşdirilməsi, şübhəli əməliyyatların filtrindən keçirilməsi, limitlərə riayətə nəzarət və s.) avtomatik şəkildə yerinə yetirir və bununla insan səhvlərini minimuma endirir.. Süni intellekt (AI) və Maşın öyrənməsi texnologiyalarının tətbiqi ilə daxili nəzarət tamamilə yeni bir səviyyəyə yüksəlir. Məsələn, böyük həcmli tranzaksiya məlumatlarını real zamanda təhlil edən AI alqoritmləri normadan kənar fəaliyyətləri dərhal aşkar edə bilir. Süni intellekt əsasında risklərin proqnozlaşdırılması sistemləri də formalaşdırılır – yəni tarixi məlumatlar əsasında müəyyən əməliyyatların risk səviyyəsini öncədən müəyyən edib, riskli əməliyyatlar üzrə ya əlavə nəzarət tədbiri tətbiq olunur, ya da həmin əməliyyata blok qoyulur.

Daxili nəzarətin rəqəmsal bank proseslərinə inteqrasiyasının ikinci aspekti nəzarət sisteminin bütün rəqəmsal əməliyyat kanallarını əhatə etməsi də son dərəcə vacibdir. Bankın onlayn bankçılıq platforması, mobil tətbiqi, ATM şəbəkəsi, ödəniş sistemləri kimi bütün rəqəmsal infrastrukturunda nəzarət prinsipləri tətbiq olunmalıdır. Bu o deməkdir ki, istənilən rəqəmsal tranzaksiya üçün bank daxilində uyğun təsdiqləmə prosesləri, limit yoxlamaları, məlumat doğrulama və loglamalar işlək vəziyyətdə olmalıdır. Məsələn, müştəri onlayn olaraq böyük məbləğdə vəsaiti köçürərkən, sistem avtomatik şəkildə həmin əməliyyatı risk meyarlarına görə dəyərləndirməli (məsələn, məbləğ çox yüksəkdirsə, şübhəli kimi işarələməli), lazım gəldikdə əlavə təsdiq tələb etməli (məsələn, bank əməkdaşının təhlili) və ya müştəridən çoxfaktorlu autentifikasiya istəməlidir. Bu cür nəzarət addımları rəqəmsal bankçılıq əməliyyatlarının həm təhlükəsizliyini, həm də tənzimləmələrə uyğunluğunu təmin edir. Blokçeyn texnologiyası da daxili nəzarət sistemlərinin inteqrasiyasına yardım edə biləcək innovativ istiqamətlərdən biridir. Blokçeyn əsaslı həllər tranzaksiyaların dəyişdirilə bilməyən (immutable) qeydlərini təmin etməklə şəffaflıq və izlənəbilirlik gətirir. Məsələn, bir sıra banklar daxili sistem jurnal qeydlərini (log) və ya bəzi əməliyyatları blokçeyn üzərində qeydə almağı sınaqdan keçirirlər ki, sonradan məlumatların dəyişdirilməsi mümkün olmasın və hər bir əməliyyatın mənbəyi tam aşkarlansın.

Bununla yanaşı, rəqəmsal inteqrasiya yeni çətinlikləri də bərabərində gətirir ki, banklar bunlara da hazır olmalıdır. Avtomatlaşdırılmış sistemlərin və kompleks rəqəmsal platformaların tətbiqi iş proseslərini mürəkkəbləşdirə bilər. Texnoloji inteqrasiya yüksək ilkin investisiyalar tələb edir, mövcud sistemlərlə yeni həllərin uyğunlaşdırılması çətin ola bilər, işçi heyətin yeni texnologiyalara öyrəşməsi zaman alır. Daxili nəzarət sisteminin rəqəmsallaşdırılması zamanı kibertəhlükəsizlik riski də xüsusi diqqət tələb edir, nəzarət sistemlərinin özlərinin sındırılması, manipulyasiya edilməsi təhlükəsi vardır. Məsələn, əgər daxili monitorinq sistemi kiberhücum nəticəsində sıradan çıxarılarsa, bank uzun müddət ərzində əməliyyatları nəzarətsiz buraxa bilər. Bu səbəbdən, rəqəmsal nəzarət infrastrukturunun da güclü müdafiə mexanizmləri ilə qorunması, ehtiyat sistemlər və bərpa planlarının mövcudluğu şərtdir. Ümumilikdə, rəqəmsal bankçılığa keçid daxili nəzarət sistemlərinin həm gücləndirilməsi, həm də transformasiyasını tələb edir. Rəqəmsal həllərin inteqrasiyası düzgün aparılarsa, daxili nəzarət prosedurlarının sürəti, dəqiqliyi və səmərəliliyi əhəmiyyətli dərəcədə artır, risklərin aşkarlanması və qarşısının alınması daha proaktiv hala gəlir. Məsələn, ənənəvi manual yoxlamalar günlərlə vaxt ala bildiyi halda, rəqəmsal nəzarət alətləri saniyələr içində minlərlə əməliyyatı yoxlayıb təhlil edə bilir. Bu isə banklarda səhvlərin və fırıldaq cəhdlərinin xeyli azalması deməkdir. Digər tərəfdən, rəqəmsal alətlər düzgün idarə olunmazsa və ya lazımi mədəni dəyişikliklər müşayiət etməzsə, daxili nəzarət sistemində boşluqlar yarana bilər. Məsələn, əməkdaşlar yeni sistemləri qəbul etməzsə və ya onlardan istifadə bacarığı zəif olarsa, texnoloji həllərin nəzərdə tutulduğu effekti verməsi çətinləşər. Buna görə də texnoloji inteqrasiya ilə yanaşı,

təşkilati strukturun çevikliyi, əməkdaşların davamlı təlimi və innovasiyalara açıq mədəniyyətin formalaşması da vacibdir.

Daxili Audit funksiyasının rəqəmsal mühitdə inkişafı. Daxili nəzarət sistemlərinin əsas elementlərindən biri olan daxili audit rəqəmsal bankçılıq dövründə öz funksiyalarını genişləndirməkdədir. Daxili audit sistemi müəssisə daxilində yoxlama, qiymətləndirmə və nəzarət funksiyasını həyata keçirir, menecerlər və ya direktorlar tərəfindən müəyyən olunur [1]. Banklarda daxili audit bölməsi əvvəlki bölmələrdə qeyd olunduğu kimi, daxili nəzarətin müstəqil qiymətləndirilməsi və zəifliklərin aşkarlanması ilə məşğuldur. Rəqəmsal transformasiya daxili auditin metod və alətlərinə də təsir göstərir. İlk növbədə, daxili auditorların bilik və bacarıqları müasirləşməlidir. Rəqəmsal bankçılıq sahəsində effektiv audit aparmaq üçün auditorlar informasiya texnologiyaları üzrə yetərli biliklərə sahib olmalıdırlar. Yəni auditor, məsələn, bankın kibertəhlükəsizlik mexanizmlərini, verilənlər bazası sistemlərini, şəbəkə infrastrukturunu ümumi şəkildə də olsa anlaya bilməli, onlarda boşluq qalma ehtimallarını qiymətləndirə bilməlidir. Bir çox banklar daxili audit əməkdaşlarını IT audit üzrə ixtisaslaşdırır və ya kənardan bu sahə üzrə mütəxəssislər cəlb edirlər. Xarici auditorlarla əməkdaşlıq da aktuallıq qazanır, bəzi hallarda daxili auditin keyfiyyəti və qərəzsizliyinin təmin olunması üçün banklar müstəqil audit şirkətlərinin məsləhət xidmətlərindən yararlanır, yaxud audit komitəsi vasitəsilə daxili auditə nəzarət edirlər.

Yuxarıdakı bölmələrdə müzakirə olunduğu kimi, rəqəmsal transformasiya daxili nəzarət sistemləri üçün həm yeni imkanlar, həm də yeni çağırışlar gətirir. Bu hissədə qısaca olaraq həmin üstünlükləri və riskləri ümumiləşdirək. Üstünlüklər: Rəqəmsal texnologiyaların inteqrasiyası daxili nəzarətin səmərəliliyini misilsiz dərəcədə artırır. Avtomatlaşdırma nəticəsində insan səhvləri azalır, rutin proseslər sürətlənir, nəzarət prosedurlarının icra xərcləri aşağı düşür. Məsələn, əməliyyatların əl ilə yoxlanılması tələb olunmadığından əməyə və vaxta qənaət olunur; bunun əvəzində həmin resurslar daha təhlili işlərə yönəldilə bilər. Real vaxt rejimində nəzarət mümkün olur, artıq aylıq və ya rüblük yoxlamaları gözləmədən riskli vəziyyətlər anındaca müəyyən edilir. Böyük məlumatların analizi sayəsində fəaliyyətin elə aspektləri aşkarlana bilər ki, ənənəvi üsullarla onları görmək çox çətin idi (məsələn, mürəkkəb fırıldaq sxemləri, qeyri-tipik müştəri davranışları və s.). Rəqəmsal alətlər eyni zamanda qanunvericiliyə uyğunluğun avtomatlaşdırılmasını təmin edir – misal üçün, müəyyən bir qaydanın pozulması (limit excess, sanksiyalı şəxsə ödəniş cəhdi və s.) dərhal sistem tərəfindən bloklana və ya xəbərdarlıqla müşayiət oluna bilər. Ümumilikdə, daxili nəzarət sisteminin effektivliyi rəqəmsal texnologiyaların köməyi ilə güclənir və banklar əməliyyatlarını daha etibarlı şəkildə genişləndirə bilir. Tədqiqatlar göstərir ki, rəqəmsal alətlərin tətbiqi daxili nəzarət prosedurlarının dəqiqliyini, sürətini və xərc səmərəliliyini əhəmiyyətli dərəcədə yaxşılaşdıra bilər. Bu, nəticə etibarilə bankların maliyyə göstəricilərinə də pozitiv təsir edə bilər. Güclü nəzarət sistemi olan banklar uzunmüddətli perspektivdə daha sabit və mənfəətli fəaliyyət göstərməyə meylli olurlar.

Çağırışlar və Risklər: Rəqəmsal inteqrasiya ilə bağlı əsas çətinliklərdən biri sistem mürəkkəbliyinin artmasıdır. Yeni texnologiyaların əlavə edilməsi bankın idarəetmə sistemini daha çox mürəkkəbləşdirir, bu da bəzən anlayışın çətinləşməsinə, idarəetmədə çevikliyin azalmasına gətirə bilər. İkinci ciddi çağırış kibertəhlükəsizlik və məlumatların qorunmasıdır. Yuxarıda qeyd olunduğu kimi, rəqəmsal nəzarət sistemləri belə hücumlara məruz qala bilər və onların işləməməsi bankı nəzarətsiz qoya bilər. Odur ki, bu sistemlərin güclü müdafiəsi, mütəmadi təhlükəsizlik testləri, personalın kibertəhlükəsizlik təlimi mütləqdir. Üçüncü məsələ implementasiya xərcləri və dəyişikliklərin idarə edilməsidir. Rəqəmsal həllərə yatırım etmək, onları mövcud infrastrukturla sintezləşdirmək böyük investisiya və bacarıq tələb edir. Bəzi banklar üçün bu maddi-texniki yük çətin ola bilər. Bundan əlavə, işçilərin yeniliklərə müqaviməti (rezistentliyi) də problem kimi ortaya çıxır – dəyişikliklərin idarə edilməsi (change management) doğru aparılmazsa, əməkdaşlar yeni sistemləri tam mənimsəyə bilməz, nəticədə nəzərdə tutulan faydalar reallaşmaz. Daxili nəzarət sisteminin rəqəmsallaşması eyni zamanda yüksək ixtisaslı kadr ehtiyacı yaradır, belə kadrların çatışmazlığı və ya mövcud heyətin çatdırılmaması riski var. Ümumilikdə, rəqəmsal transformasiya şəraitində

daxili nəzarət sistemlərinin gücləndirilməsi banklar üçün alternativi olmayan bir tələbə çevrilmişdir. Bu prosesin uğurlu olması üçün banklar strateji və düşünülmüş yanaşma qəbul etməlidirlər. Yalnız texnologiyaya sərmayə qoymaq kifayət deyil, eyni zamanda insan kapitalına (davamlı təlimlər, ixtisasartırma), dəyişikliklərin idarə edilməsinə və güclü kibertəhlükəsizlik tədbirlərinə investisiya qoyulmalıdır. İnnovasiya ilə risklərin prudent idarəedilməsinin balansı düzgün qurulsa, rəqəmsal əsrdə daxili nəzarət sistemləri bankların həm rəqabətqabiliyyətliliyini, həm də sabitliyini təmin edəcək güclü bir alət kimi çıxış edə bilər.

Nəticə

Rəqəmsal bankçılıq dövründə daxili nəzarət sistemlərinin inteqrasiyası bank idarəetməsinin təməl istiqamətlərindən birinə çevrilmişdir. Aparılan təhlillər göstərir ki, rəqəmsal texnologiyalar banklarda daxili nəzarət və risk idarəetmə proseslərini həm keyfiyyətcə yeni mərhələyə çıxarır, həm də onların əhəmiyyətini artırır. Güclü daxili nəzarət sistemi olmadan rəqəmsal mühitdə bankların dayanıqlı fəaliyyətini təmin etmək mümkün deyil. Məqalədə vurğulanan əsas məqamları yekunlaşdırsaq:

1. Daxili nəzarət sistemləri bankların maliyyə dayanıqlığı və etibarlılığı üçün həyati əhəmiyyət kəsb edir. Xüsusilə rəqəmsal bankçılıq şəraitində ICS (Internal Control System) bank əməliyyatlarının fasiləsizliyini, düzgünlüyünü və qanunauyğunluğunu təmin edən sütun rolunu oynayır.
2. Rəqəmsal transformasiya bank risklərinin spektrini genişləndirərək onları daha mürəkkəb hala gətirmişdir (kiber risklər, əməliyyat riskləri, saxtakarlıq və s.). Bu, daxili nəzarət sistemlərinin adaptasiyasını qaçılmaz edir. Tədqiqat nəticələri də təsdiqləyir ki, rəqəmsal dövrdə risklərin effektiv idarəsi üçün güclü daxili nəzarət sistemi həlledici faktorlardandır.
3. Daxili nəzarət sistemlərinin rəqəmsal bankçılığa inteqrasiyası banklara öz nəzarət funksiyalarını avtomatlaşdırmağa, sürətləndirməyə və daha proaktiv etməyə imkan verir. Avtomatlaşdırılmış nəzarət vasitələri və süni intellekt tətbiqləri sayəsində insan faktorundan irəli gələn xətalar azalır, nəzarət proseslərinin izlənəbilərliyi və səmərəliliyi artır.
4. Rəqəmsal inteqrasiyanın çağırışları da unudulmamalıdır: sistemlərin mürəkkəbləşməsi, kibertəhlükəsizlik riskləri, yüksək implementasiya xərcləri, kadrların yeni biliklərə ehtiyacı və s. Bu problemlərin öhdəsindən gəlmək üçün banklar strateji planlama aparmalı, dəyişiklikləri idarəetmə, personalın treninqi və təhlükəsizlik sahələrinə xüsusi önəm verməlidirlər.
5. Daxili audit və ümumilikdə daxili nəzarət funksiyası rəqəmsal şəraitdə təkamül edir. Daxili auditin rolu artaraq, texnoloji biliklərlə zənginləşmiş bir fəaliyyət kimi bankın bütün rəqəmsal əməliyyatlarını əhatə etməlidir. Audit komitələri və həm daxili, həm də xarici auditin koordinasiyası, eləcə də zəruri hallarda audit funksiyasının qismən autsorsinqi, rəqəmsal mühitdə nəzarətin səmərəliliyini yüksəldə bilər.

Nəticə etibarilə, daxili nəzarət sistemlərinin rəqəmsal bankçılıq proseslərinə səmərəli inteqrasiyası bankların risklərin idarə olunmasında çevikliyini artırmaqla yanaşı, normativ tələblərə riayət olunmasını və müştəri etimadının gücləndirilməsini təmin edir. Müasir rəqəmsal iqtisadi mühitdə bank sektorunda rəqabətqabiliyyətli və uzunmüddətli fəaliyyətin qorunması üçün daxili nəzarət mexanizmlərinin mütəmadi olaraq təkmilləşdirilməsi və innovativ texnoloji həllərlə dəstəklənməsi zəruridir. Qeyd olunmalıdır ki, rəqəmsal bankçılıq modelinin uğurla həyata keçirilməsi, birbaşa şəkildə, daxili nəzarət sistemlərinin effektiv və güclü şəkildə təşkil olunmasından asılıdır.

ƏDƏBİYYAT

1. Hüseynov, N.H. AMEA-nın Xəbərləri. İqtisadiyyat seriyası 2020. Risk yönümlü idarəetmə sistemində daxili audit və nəzarətin inkişafı.
2. Васильев Алексей Дмитриевич. Совершенствование системы внутреннего контроля в банковском секторе: методические подходы и практические решения. 2025.
3. Əliyev Müseyib. Bankların inkişaf istiqamətləri. Monoqrafiya. 2011.
4. Tağıyev, X.R., Rüstəmov, T.H. Rəqəmsal ödənişlər və elektron bankçılıq xidmətləri. 2020.

Кенан Нусрат оглы Атаев
Бакинский Университет Бизнеса, докторант
ataevkenan29@gmail.com

Интеграция систем внутреннего контроля в цифровой банкинг

Резюме

Цель исследования- Цель данного исследования заключается в теоретическом и практическом анализе роли, функций и эффективной интеграции систем внутреннего контроля в условиях цифрового банкинга с учётом современных технологических реалий. Основное внимание уделяется тому, каким образом цифровые технологии влияют на механизмы контроля в банках и как эти системы могут быть усовершенствованы на фоне возникающих новых рисков.

Методология работы- Исследование проведено с использованием преимущественно аналитических и дескриптивных методов. Цифровые инструменты, применяемые в современной банковской системе, структуры внутреннего контроля и механизмы управления рисками проанализированы на основе международного опыта и нормативных документов. Кроме того, в работе представлен сравнительный анализ традиционных и цифровых методов контроля, а также обеспечено научное обоснование посредством обобщения практики и анализа источников.

Прикладная значимость исследования- Данное исследование представляет практическую ценность для руководства банков, риск-менеджеров, внутренних аудиторов и регулирующих органов. Его результаты способствуют адаптации систем внутреннего контроля к вызовам цифровой среды. Кроме того, настоящее исследование формирует методологическую основу для принятия стратегических решений, направленных на обеспечение безопасности и устойчивости в процессе цифровизации банковского сектора.

Результаты исследования- Исследование показывает, что интеграция цифровых технологий существенно повышает эффективность систем внутреннего контроля в банках, одновременно обусловливая необходимость управления новыми видами рисков.

Оригинальность и научная новизна исследования-Научная новизна данного исследования заключается в том, что системы внутреннего контроля впервые были комплексно проанализированы в контексте цифрового банкинга, а их интеграция с технологиями искусственного интеллекта, блокчейна и автоматизированного мониторинга была теоретически обоснована. Кроме того, вызовы и преимущества систем внутреннего контроля были систематизированы как с технической, так и с организационной точек зрения. В этом аспекте исследование представляет собой новшество, поскольку оно выстраивает мост между специфическими требованиями банковского сектора Азербайджана и глобальными тенденциями.

Ключевые слова: цифровой банкинг, система внутреннего контроля, внутренний аудит, кибербезопасность, автоматизация, комплаенс.

Kenan Nusrat ATAYEV
Baku Business University, PhD Student
atayevkenan29@gmail.com

Integration of internal control systems into digital banking

Summary

The purpose of the study- The purpose of this study is to investigate the role, functions, and effective integration of internal control systems in the context of digital banking from a theoretical

and practical perspective. The main goal is to reveal how digital technologies affect banks' control mechanisms and how these systems can be improved in the light of emerging risks.

The methodology of the work- The research was conducted mainly using analytical and descriptive methods. The digital tools, internal control structures and risk management mechanisms applied in the modern banking system were analyzed based on international experience and regulatory documents. The research also presents a comparison of traditional and digital control methods through comparative analysis. Also, scientific justification was provided through experience-based generalization and source research.

The applied significance of the study – This study has practical value for bank executives, risk managers, internal auditors, and regulators. The results of the study help banks adapt their internal control systems to the challenges of the digital environment. This study also creates a methodological basis for making strategic decisions to ensure security and sustainability in the process of digitalization in the banking sector.

The results of the study – The study shows that the integration of digital technologies not only significantly increases the effectiveness of internal control systems in banks, but also necessitates the management of new risks.

The originality and scientific novelty of the study – The scientific novelty of this study is that for the first time, internal control systems are comprehensively analyzed in the context of digital banking and their integration with artificial intelligence, blockchain and automated monitoring technologies is explained on theoretical grounds. In addition, the challenges and advantages of both technical and organizational aspects of the internal control system are systematized in detail. In this regard, the study is innovative in terms of bridging the specific requirements of the Azerbaijani banking sector with global trends.

Key words: digital banking, internal control system, internal audit, cybersecurity, automation, compliance.