UDC 327
IRSTI 11.25.67; 11.25.19
https://doi.org/10.48371/ISMO.2026.64.2.006

TRANSNATIONAL FINANCIAL FRAUD IN THE CONTEXT OF DIGITALIZATION: INSTITUTIONAL CHALLENGES OF KAZAKHSTAN AND INTERNATIONAL COUNTERMEASURES

Brassilova A.[1], *Sarybayev M.S.[2]
[1, *2] Al-Farabi Kazakh National University, Almaty, Kazakhstan

Abstract. The article examines transnational financial fraud as an institutional security challenge emerging in the context of Kazakhstan's accelerated digitalization. The study argues that the spread of mobile payments, digital public services, remote identification, platform-based communication, and cross-border financial instruments has changed not only the scale of fraudulent activity, but also its organizational logic. Contemporary fraud schemes increasingly combine social engineering, spoofed communications, foreign hosting, money-mule networks, crypto-asset conversion, and international payment routes. As a result, the effectiveness of counteraction depends less on isolated technical barriers than on the ability of institutions to coordinate in real time. The purpose of the article is to explain why digital financial fraud acquires a transnational character in Kazakhstan and to identify foreign institutional mechanisms that may be adapted to national practice. The study uses qualitative comparative institutional analysis based on policy documents, official reports, and academic literature on cybercrime, fraud victimization, governance capacity, and collaborative regulation. The article develops the concept of a digitalization-capacity gap, understood as the mismatch between the speed of criminal adaptation in digital ecosystems and the speed of institutional prevention, information exchange, urgent intervention, and cross-border cooperation. The results show that Kazakhstan's key vulnerabilities are temporal, informational, organizational, and jurisdictional. The comparative assessment of Singapore, the European Union, and the United States demonstrates the value of shared responsibility models, threat-intelligence platforms, complaint-based analytics, and rapid-response coordination. The article concludes that Kazakhstan requires an integrated anti-fraud governance architecture linking financial regulators, banks, telecom operators, law-enforcement bodies, digital platforms, and international partners.

Keywords: transnational financial fraud, digitalization, Kazakhstan, international security, cybercrime, institutional capacity, anti-fraud governance, interagency coordination, cross-border cooperation

Introduction

Digitalization has become one of the central drivers of transformation in contemporary economies, financial systems, and public administration. In

Kazakhstan, the State Programme «Digital Kazakhstan» set a policy framework for the accelerated modernization of infrastructure, public services, and digital interaction between the state, business, and citizens [1]. The development of e-government platforms further normalized remote access to administrative services, while the expansion of payment instruments and online banking strengthened the everyday role of digital financial channels [2; 3]. These processes have produced clear gains in accessibility, speed, and convenience. At the same time, they have created a new environment in which criminal actors can exploit digital trust, the routine use of remote interfaces, and the rapid movement of funds.

Financial fraud in the digital environment is no longer adequately described as a series of isolated incidents involving individual victims. It increasingly operates as a scalable socio-technical system. Fraudsters may contact victims through spoofed phone numbers, redirect them to phishing interfaces, persuade them to disclose authentication data, transfer funds to accounts controlled by intermediaries, and then move assets through multiple layers of transactions or convert them into crypto-assets. Such schemes are economically rational from the offender's perspective because digital communication reduces the cost of reaching large audiences and because the probability of successful intervention declines as funds move faster and across multiple institutional boundaries [4]. The issue is therefore not limited to consumer protection or financial literacy. It concerns the resilience of institutions responsible for financial security, public trust, and cross-border cooperation.

The rapid development of digital identity systems, remote customer onboarding, and app-based financial services makes reliable verification an essential element of security governance. International standards emphasize that digital identity must combine accessibility with risk-sensitive assurance, especially in anti-money-laundering and counter-terrorist-financing environments [5]. The spread of crypto-assets and new payment technologies adds further complexity, because funds may be layered, obfuscated, or transferred through infrastructures that are not easily aligned with national investigative procedures [6]. For Kazakhstan, this creates a specific challenge: the country is expanding digital services at a high pace, while fraudulent actors can appropriate the symbolic authority of banks, government institutions, and recognizable digital platforms in order to influence user behavior.

A substantial body of research shows that online fraud succeeds not only because of technical weaknesses, but also because of social engineering. Victims are often manipulated through urgency, fear, apparent authority, scarcity, and the promise of profit [7]. Fraud should therefore be understood as an interaction between offender strategy, user vulnerability, platform design, and institutional response. Studies of scam ecosystems emphasize that victims encounter fraud through a chain of communications and financial actions, not through a single discrete event [8]. This perspective is important for policy design: measures limited

to awareness campaigns are unlikely to be sufficient if the broader infrastructure of spoofing, mule accounts, and rapid fund transfer remains operational.

Cybercrime scholarship further indicates that digital offences are shaped by a combination of criminological, technological, and governance factors [9]. Wall's analysis of cybercrime demonstrated that the Internet transforms the relationship between place, time, and harm, thereby challenging territorially bounded models of law enforcement [10]. Brenner similarly argued that cybercrime creates structural tensions for international law because the location of offenders, victims, servers, and financial flows may be distributed across several jurisdictions [11]. These observations are particularly relevant to transnational financial fraud: a victim may be located in Kazakhstan, the communication channel may rely on a foreign service, the phishing page may be hosted abroad, the receiving account may be held by a local money mule, and the ultimate beneficiaries may operate elsewhere.

The organizational dimension of digital fraud also deserves attention. Research on cybercriminal groups indicates that such networks often operate through flexible role differentiation rather than rigid hierarchical structures [12]. Online forums and social ties facilitate the distribution of illicit services, including access to compromised accounts, phishing kits, scripts, call-center techniques, and cash-out services [13]. This means that fraud networks can be resilient even when individual participants are detected. The system is modular: if one communication channel is blocked, another can be activated; if one mule account is frozen, funds can be routed through a substitute; if one phishing domain is removed, a new replica can appear. From the perspective of institutional security, this adaptive structure is a fundamental reason why reactive measures often lag behind criminal innovation.

The concept of institutional capacity helps explain this lag. Governance capacity is not reducible to the existence of formal laws or administrative bodies; it concerns the practical ability of institutions to identify problems, coordinate actors, enforce decisions, and adjust to changing circumstances [14]. In the field of cybersecurity, resilience increasingly depends on cooperation among state agencies, regulators, private firms, and international partners [15]. Dupont's argument concerning polycentric regulation is especially relevant: large-scale cybercrime cannot be controlled by police action alone, because the infrastructure enabling criminal activity is distributed across payment systems, telecommunications, hosting services, and platform economies [16]. The effectiveness of anti-fraud policy therefore depends on whether these actors are connected by operational protocols rather than by fragmented responsibilities.

Kazakhstan has already developed elements of a response architecture. Public institutions have strengthened attention to cybercrime, specialized initiatives such as CyberPol have been promoted, and awareness efforts have been expanded [17; 18]. Nevertheless, the rapid diffusion of digital services raises a deeper analytical question: can the speed of institutional response match

the speed of digital fraud? This article argues that the answer depends on the presence or absence of a digitalization-capacity gap. The gap emerges when digitalization increases the scale, speed, and complexity of transactions faster than institutions build the capacity to prevent manipulation, share data, suspend suspicious flows, coordinate across sectors, and work with foreign partners.

The article addresses the following research question: why does financial fraud in Kazakhstan acquire an increasingly transnational character under conditions of digitalization, and which international institutional mechanisms may be adapted to the Kazakhstani context? The working hypothesis is that the persistence and scalability of digital financial fraud are driven not by digitalization itself, but by an institutional mismatch between the adaptive capacity of fraudulent networks and the operational capacity of legitimate institutions. This mismatch is expressed in four dimensions: temporal delay, informational fragmentation, organizational coordination barriers, and jurisdictional dependence on cross-border procedures.

The object of the research is transnational digital financial fraud as a security challenge. The subject of the research is the institutional architecture through which Kazakhstan and selected foreign jurisdictions attempt to prevent, detect, and interrupt such fraud. The purpose of the study is to conceptualize the digitalization-capacity gap and to identify anti-fraud governance mechanisms applicable to Kazakhstan. To achieve this purpose, the article pursues five objectives: first, to clarify the relationship between digitalization and the expansion of fraud opportunities; second, to systematize the operational mechanisms of transnational financial fraud; third, to identify institutional vulnerabilities in Kazakhstan's response model; fourth, to compare the experience of Singapore, the European Union, and the United States; and fifth, to formulate policy implications for a more integrated Kazakhstani anti-fraud architecture.

The scientific novelty of the article lies in the combination of international security analysis, cybercrime research, and governance theory within a single institutional model. Rather than presenting digital fraud as a purely criminal-law problem or as an unintended side effect of financial modernization, the article treats it as a transnational risk generated at the intersection of technological acceleration and institutional coordination. This framing is consistent with wider studies of institutions, which show that rules matter most when they are accompanied by enforcement capacity and adaptive coordination [25], and with research on whole-of-government and collaborative governance, which emphasizes that complex risks often require structured interaction among public and private actors [26; 27]. The practical significance of the study lies in its effort to translate international experience into a policy-relevant framework for Kazakhstan.

Description of Materials and Methods

The study is based on qualitative comparative institutional analysis. This

design is appropriate because the article does not seek to prove a linear statistical causality between the overall level of digitalization and a specific number of registered fraud cases. Publicly available statistics are affected by underreporting, changes in legal qualification, differences in complaint behavior, and the fact that a single fraudulent network may generate multiple incidents across jurisdictions. Instead, the article focuses on mechanisms: how digital environments create fraud opportunities, how criminal actors operationalize cross-border infrastructures, and how institutions can reduce the gap between detection and intervention.

The research design combines conceptual modelling with structured comparison. The conceptual component develops the digitalization-capacity gap as an analytical framework. The comparative component examines Kazakhstan alongside three foreign reference models: Singapore, the European Union, and the United States. These cases were selected not as direct equivalents to Kazakhstan, but because each illustrates a different institutional response logic. Singapore is relevant for its shared responsibility approach across banks, telecommunications, and digital platforms [22]. The European Union is relevant for supranational threat assessment and cross-border analytical coordination, particularly through Europol's organized cybercrime reporting [19]. The United States is relevant for complaint aggregation, incident statistics, and targeted public alerts provided by IC3 and FinCEN [20; 21].

The empirical corpus includes four categories of materials. The first category consists of Kazakhstan's policy and institutional documents related to digitalization, e-government, payment infrastructure, and cybercrime response [1; 2; 3; 17; 18]. The second category consists of international policy and risk-reporting documents addressing identity assurance, cybercrime threats, online fraud patterns, public complaint reporting, and cross-sector responsibilities [5; 19 -22]. The third category includes academic literature on online crime economics, victimization, cybercriminal networks, electronic crime, and cybercrime markets [4; 7; 8-13; 23; 24; 28]. The fourth category includes institutional and governance literature that helps interpret capacity, coordination, and adaptive regulation [14-16; 25-27; 29; 30].

The analytical procedure consists of five stages. First, the literature is used to distinguish between fraud as an individual deception event and fraud as a distributed transnational ecosystem. Second, official and analytical sources are used to identify the main operational mechanisms by which fraud is initiated, scaled, and monetized. Third, the Kazakhstani institutional environment is examined through the lens of response capacity, with attention to time, information, coordination, and jurisdiction. Fourth, foreign models are compared according to their dominant institutional mechanism: shared responsibility, supranational coordination, or complaint-based intelligence. Fifth, the article derives an applicability matrix that identifies which mechanisms are potentially transferable to Kazakhstan and under what constraints.

Table 1. Analytical Framework of the Study

Dimension	Analytical question	Operational indicators
Digitalization pressure	How do digital services expand fraud opportunities?	Remote payments; e-government interfaces; instant communication; digital identity dependence
Fraud ecosystem	How is deception transformed into scalable transnational harm?	Social engineering; spoofing; phishing; money mules; crypto conversion; foreign hosting
Institutional capacity	Where does response lag the threat?	Temporal, informational, organizational, jurisdictional, and analytical gaps
International coordination	Which foreign mechanisms may be adapted to Kazakhstan?	Shared responsibility; threat intelligence; complaint analytics; rapid escalation channels

Source: compiled by the author on the basis of [1-3; 5-8; 10; 12-14; 19-22; 25-27; 30].

The comparative method is not used to rank countries according to the absolute effectiveness of anti-fraud policy. Such ranking would be misleading because the jurisdictions differ in market structure, reporting culture, legal regime, and institutional resources. Instead, comparison is mechanism-based. The key analytical questions are: Which actor receives the first signal of fraud? How quickly can that signal be combined with information held by other actors? What type of intervention is possible within the first hours after a suspicious event? How are cross-border elements escalated? Which responsibilities are preventive and which are reactive? These questions make it possible to compare institutional architectures without assuming that one jurisdiction can be copied mechanically into another.

The study applies source triangulation. A conclusion is considered more reliable when it is supported by at least two types of evidence: academic interpretation, official institutional material, or comparative foreign practice. For example, the claim that fraud ecosystems are distributed and role-differentiated is grounded in cybercrime studies [12; 13; 24], while the argument that modern counteraction requires cross-sector coordination is supported by governance literature [16; 26; 27] and by the Singaporean shared responsibility framework [22]. This approach reduces the risk of overreliance on either sensational media cases or purely normative policy documents.

The article also introduces operational definitions. «Digital financial fraud» refers to deceptive practices aimed at the unlawful acquisition or redirection of money, credentials, or financial control through digital communication or digitally mediated financial transactions. «Transnational» refers to fraud schemes in which at least one significant element-offender location, hosting infrastructure, communication service, financial routing, platform governance, or asset conversion-crosses national borders. «Institutional capacity» refers to the ability of responsible actors to prevent, detect, exchange information about, and interrupt fraudulent activity within a time frame relevant to the speed of the scheme. «Digitalization-capacity gap» refers to the discrepancy between the velocity and modularity of fraud networks and the response capacity of legitimate institutions.

Several limitations must be acknowledged. The study relies on open sources and does not have access to operational datasets on suspicious-transaction freezes, real-time anti-fraud alerts, bank-telecom information exchanges, or international legal assistance requests. It does not estimate the precise economic loss associated with each fraud mechanism. Nor does it claim that foreign models can be transferred without institutional adaptation. These limitations define the article as an analytically grounded comparative study rather than a statistical impact assessment. They also indicate directions for future research based on interviews with practitioners, incident-level case databases, and quantitative analysis of response time.

Results

The analysis produces six interrelated results. First, digitalization in Kazakhstan expands the opportunity structure for fraud by making remote identification, mobile communication, and instant payment practices routine. Second, transnational digital fraud is sustained by recurring operational mechanisms that combine deception, infrastructure, and liquidity extraction. Third, Kazakhstan's response architecture is developing, but it remains constrained by temporal, informational, organizational, and jurisdictional gaps. Fourth, international experience suggests that sustainable counteraction depends on institutionalized coordination rather than on isolated technical measures. Fifth, the most relevant foreign mechanisms for Kazakhstan are those that shorten the response cycle between signal detection and intervention. Sixth, the effectiveness of anti-fraud governance should be assessed through measurable indicators that capture speed, coordination, learning, and cross-border responsiveness.

Digitalization and the expansion of the fraud opportunity structure

Digitalization changes the context of financial fraud by transforming what citizens perceive as normal interaction. In a less digitalized environment, an unexpected request to transfer funds or provide credentials may appear exceptional. In a highly digitalized environment, however, citizens routinely receive notifications from banks, links to public services, verification messages, delivery updates, and investment offers. This normalization of remote interaction provides fraudsters with a broader symbolic repertoire. They no longer need to invent entirely new scenarios; they can imitate legitimate forms of digital communication already embedded in everyday life. Kazakhstan's policy emphasis on digital transformation, the expansion of e-government, and the growth of digital payment instruments provide the institutional background for this shift [1-3].

The first result is therefore that digitalization increases the «fraud opportunity structure». This does not mean that digitalization causes crime in a deterministic sense. Rather, it lowers the transaction costs of deception, increases audience reach, and compresses the time between persuasion and payment. Economic studies of online crime have long shown that offenders benefit from low-cost communication, large target pools, and the ability to iterate and automate attacks [4]. When these features are combined with instant payment mechanisms, the initial victim-contact

phase and the extraction-of-funds phase can occur within a single uninterrupted communication session. The institutional challenge is that the fraud window becomes shorter, while the cost of verification remains distributed across several actors.

The second element of the fraud opportunity structure concerns digital identity and trust. The more public administration and financial services depend on remote authentication, the more valuable it becomes for fraudsters to appropriate signals of legitimacy: logos, interface design, familiar phone numbers, official language, and references to state or banking procedures. FATF guidance emphasizes that digital identity systems must be risk-sensitive because assurance failures can affect both access and abuse [5]. In the fraud context, this means that confidence in digital identity infrastructure can itself be weaponized. A user may not merely be deceived by a false message; the user may be deceived precisely because the message resembles an expected security notification or official request.

The third element is the widening role of financial instruments that are difficult to trace after rapid redistribution. Crypto-assets are not the only route for laundering or concealing fraudulent proceeds, but they may be used to accelerate cross-border movement or complicate recovery once funds leave the initial banking channel [6]. Fraudulent schemes can therefore be structured in layers: first, the victim is persuaded to make a transfer; second, funds are fragmented through intermediary accounts; third, a part of the amount is transferred abroad or converted into alternative instruments. Each additional layer increases the burden on institutions that must reconstruct the transaction chain under time pressure.

Finally, digitalization reshapes the political meaning of fraud. When fraudsters imitate public institutions, exploit digital financial ecosystems, and operate through transnational infrastructures, the harm is not limited to private monetary loss. Repeated victimization erodes confidence in digital government, online banking, and the reliability of public warnings. It may also generate reputational pressure on regulators and law-enforcement institutions. For a state pursuing digital modernization, maintaining trust in the legitimacy and safety of digital channels becomes a component of institutional resilience, not merely a matter of customer service.

Operational mechanisms of transnational digital financial fraud

The second result concerns the operational architecture of fraud. The academic literature indicates that scams are rarely one-step events. They are sequences in which attention capture, persuasion, credential access, payment initiation, liquidity extraction, and concealment are distributed across several roles [7; 8; 12; 13]. This sequencing explains why single-point interventions are often insufficient. Blocking a phishing page may have little effect if the fraudulent campaign can shift to a new domain; freezing one account may not stop a network that uses many temporary mule accounts; public warnings may not reach victims already embedded in a high-pressure communication script.

A typical fraud scenario can begin with social engineering. The offender

constructs a message that appears urgent, personalized, and institutionally plausible. The communication may refer to suspicious banking activity, unauthorized loans, unpaid taxes, investment opportunities, or urgent changes in account security. Victims are then guided toward an action that appears protective or profitable but is actually harmful. Research on fraud victimization shows that the decision to comply is often influenced by emotional pressure rather than a lack of general intelligence or technological ability [7; 8]. This is crucial for policy because anti-fraud messaging should not stigmatize victims; it should address the manipulative structure of the scheme.

The transnational dimension usually enters through infrastructure. Fraudsters may use foreign VoIP providers, number-spoofing services, rented hosting, anonymous registration, or platform accounts created outside the victim's jurisdiction. The fraudster's physical location may be irrelevant to the victim-facing interface. In practice, the victim experiences a local event an apparent call from a domestic bank or official body-while the technical architecture of the event is geographically dispersed. This mismatch undermines purely national models of intervention and supports the argument that cybercrime challenges traditional territorial assumptions [10; 11; 28].

The payment phase introduces another layer of complexity. Funds may first be sent to an account in Kazakhstan controlled by a money mule or an unwitting intermediary. The use of local accounts makes the transaction appear domestically manageable at the initial stage. Yet the subsequent movement of funds may rapidly cross sectors and jurisdictions. The money mule may transfer funds to other accounts, withdraw cash, purchase digital assets, or forward assets through international services. Cybercrime research shows that such ecosystems rely on division of labor and specialized roles, which increases resilience and makes the network harder to dismantle [12; 13; 24].

Table 2 systematizes the main operational mechanisms of transnational financial fraud and identifies the institutional response each mechanism requires. The table demonstrates that fraud control cannot be assigned to a single institution. Banks, telecom operators, platforms, regulators, and law-enforcement bodies each possess only part of the relevant signal. The policy problem is therefore one of connection and timing.

Table 2. Main Operational Mechanisms of Transnational Digital Financial Fraud

Mechanism	**Fraud function**	**Transnational component**	**Required institutional response**
Social engineering	Triggers compliance through urgency, fear, or profit expectations	Scripts and campaigns can be operated remotely from abroad	Victim-centered warnings; pattern-based analytics; complaint clustering
Spoofed calls and messaging	Imitates banks, regulators, police, or public services	VoIP, foreign telecom routing, anonymized accounts	Telecom filtering; caller authentication; bank–telecom escalation

Phishing and cloned interfaces	Captures credentials or legitimizes fraudulent payments	Foreign hosting, rapidly rotating domains, platform distribution	Fast takedown requests; domain monitoring; public alerts
Money-mule chains	Receives and redistributes stolen funds	Domestic first hop followed by cross-border transfers	Transaction monitoring; mule-account typologies; urgent freezes
Crypto-asset conversion	Obfuscates destination of illicit proceeds	Cross-border exchanges, wallets, and layered routes	Risk-based compliance; financial intelligence cooperation
Fraud-as-a-service resources	Supplies scripts, kits, accounts, and infrastructure	Online forums and market-like ecosystems	Intelligence-led disruption; international cybercrime cooperation

Source: compiled by the author on the basis of [6-8; 10-13; 19; 21; 24; 28].

Institutional vulnerabilities in Kazakhstan: the digitalization-capacity gap

The third result is that Kazakhstan's anti-fraud environment contains both developing strengths and persistent coordination vulnerabilities. The existence of specialized cybercrime initiatives, public communication, and growing attention to fraud prevention indicates that the problem has been recognized institutionally [17; 18]. However, recognition alone does not resolve the operational challenge. The central issue is whether fraud signals collected by different actors can be combined rapidly enough to prevent irreversible loss. The digitalization-capacity gap is therefore not a claim of institutional absence; it is a claim of institutional asymmetry between the speed of the threat and the speed of coordinated response.

The first dimension of the gap is temporal. Digital fraud often depends on urgency. Victims are encouraged to act immediately, while funds can be transferred within minutes. A response system that relies on sequential complaint registration, manual verification, and delayed coordination may be effective for investigation after the fact but less effective for prevention during the critical early period. The literature on institutional capacity emphasizes that governance should be evaluated by problem-solving ability, not by the mere existence of formal structures [14; 30]. In fraud prevention, problem-solving capacity is inseparable from response time.

The second dimension is informational. A bank may detect an unusual transaction pattern; a telecom operator may notice suspicious traffic or spoofed call characteristics; a platform may identify a fraudulent advertisement or cloned page; the police may receive a cluster of similar complaints. If these data remain isolated, the fraud scheme is visible only in fragments. If they are connected through standardized risk categories and urgent communication protocols, institutions can move from reactive processing to pattern recognition. Whole-of-government literature and collaborative governance theory both suggest that complex risks require structured information-sharing arrangements rather than ad hoc cooperation [26; 27].

The third dimension is organizational. Different actors have distinct legal mandates, commercial incentives, data systems, and internal decision rules.

Banks are concerned with fraud loss, regulatory compliance, and customer relations; telecom operators focus on traffic integrity and service obligations; law-enforcement agencies require procedural certainty; regulators must maintain proportionality and legal safeguards. Without a clear coordination architecture, each actor may fulfill its formal role while the system as a whole remains slow. This illustrates why collaborative governance must be designed, not merely expected [27].

The fourth dimension is jurisdictional. Transnational fraud may depend on servers abroad, messaging services administered outside Kazakhstan, foreign payment intermediaries, and actors located in multiple countries. National institutions may have strong domestic authority but limited ability to compel immediate action by foreign providers. The problem is intensified when urgent financial intervention requires faster cooperation than conventional mutual legal assistance procedures can deliver. International cybercrime scholarship has long emphasized that territorial jurisdiction and digital evidence often operate on different timelines [11; 28]. The digitalization-capacity gap thus includes a cross-border component that cannot be solved solely through domestic reform.

A fifth dimension is analytical. Fraud evolves through imitation, experimentation, and platform migration. New schemes may combine older elements—phone deception, phishing, investment manipulation with newer tools such as synthetic media or AI-generated scripts. FinCEN's alert concerning deepfake-enabled fraud illustrates how rapidly deceptive techniques can evolve and how financial-compliance institutions must be updated accordingly [21]. The challenge for Kazakhstan is not only to block known schemes but also to build a learning system capable of detecting pattern shifts before they become routine.

Table 3 summarizes these dimensions and shows how each gap affects prevention, detection, or response. The table also clarifies that anti-fraud policy should be evaluated as an integrated governance system rather than as a set of isolated measures.

Table 3. Institutional Dimensions of the Digitalization-Capacity Gap in Kazakhstan

Gap dimension	**Manifestation**	**Consequence**	**Priority response**
Temporal	Funds move faster than review, complaint processing, and coordinated blocking	Lower probability of interruption and recovery	First-hour response protocols; temporary risk-based intervention
Informational	Signals are separated among banks, telecom operators, platforms, and police	Fragmented understanding of fraud clusters	Shared risk taxonomy; secure data-exchange procedures
Organizational	Actors have different mandates, systems, and incentives	Coordination remains ad hoc	Permanent interagency and public–private anti-fraud mechanism

Jurisdictional	Hosting, communication, offenders, and assets may be outside Kazakhstan	Domestic authority is insufficient for urgent action	Rapid liaison channels; standardized cross-border referrals
Analytical	Fraud schemes evolve faster than threat classifications	Delayed recognition of new patterns	Unified incident analytics; periodic threat assessment

Source: compiled by the author on the basis of the institutional analysis presented in the article and [14; 21; 25-27; 30].

International institutional models and their relevance for Kazakhstan

The fourth result is that international experience offers three complementary models of anti-fraud governance. The first is the shared responsibility model represented by Singapore. The Shared Responsibility Framework introduced by the Monetary Authority of Singapore and the Infocomm Media Development Authority distributes obligations among banks and telecommunications companies in relation to scam-related harms [22]. The importance of this model lies not only in liability allocation. Its deeper contribution is institutional: it recognizes that fraudulent harm is produced through a chain of interacting services, and therefore prevention requires a chain of responsibility.

For Kazakhstan, the Singaporean experience is relevant because many fraud schemes combine a communication component and a payment component. A bank may be able to identify suspicious transfers, but it cannot alone prevent spoofed calls. A telecom operator may be able to reduce fraudulent traffic, but it cannot independently assess payment risk. Shared responsibility frameworks can reduce the tendency to shift blame after victimization and instead promote ex ante operational standards. Nevertheless, direct copying would be inappropriate. Any Kazakhstani adaptation would need to consider domestic banking structure, telecom regulation, consumer-protection norms, and the legal basis for information exchange.

The second model is the European Union's emphasis on supranational threat intelligence and cross-border coordination. Europol's IOCTA reporting provides a structured assessment of organized cybercrime, including scam ecosystems, criminal services, automation, and transnational infrastructures [19]. The value of such reporting is not limited to public awareness. It helps create a common analytical language among law-enforcement bodies and regulators. For Kazakhstan, this suggests the importance of a standardized national classification of digital fraud mechanisms and a stronger link between domestic incident analysis and international threat intelligence.

The third model is the United States' complaint-based analytical architecture. IC3 collects and publishes structured information on internet-enabled crime, while FinCEN issues alerts that translate emerging fraud patterns into compliance-relevant guidance for financial institutions [20; 21]. These instruments are important because they transform dispersed complaints into a knowledge base. They help identify trends, prioritize threats, and align public

awareness with institutional risk management. Kazakhstan could benefit from a unified fraud-incident registry that integrates complaints, financial indicators, and information from digital service providers, subject to privacy and procedural safeguards.

International models also highlight that anti-fraud governance should combine prevention, interruption, and learning. Prevention reduces exposure to fraudulent communication. Interruption stops or slows fund movement during the critical window. Learning transforms incidents into institutional knowledge that improves future detection. A system that performs only one of these functions remains incomplete. Table 4 compares Kazakhstan with Singapore, the European Union, and the United States according to their dominant institutional mechanisms and the lessons most relevant for national adaptation.

Table 4. Comparative Institutional Models for Countering Digital Financial Fraud

Jurisdiction	Dominant mechanism	Strength of the model	Relevance for Kazakhstan
Singapore	Shared responsibility framework	Connects preventive duties of banks and telecom actors	Useful for distributed responsibility and ex ante coordination
European Union	Threat intelligence and supranational coordination	Creates common threat vocabulary and cross-border analytical focus	Relevant for classification systems and international information exchange
United States	Complaint-based analytics and compliance alerts	Transforms dispersed incidents into strategic intelligence	Applicable to a unified incident registry and risk-alert system
Kazakhstan	Developing cybercrime initiatives and public awareness	Institutional recognition of fraud as a security issue	Needs stronger real-time coordination and integrated analytics

Source: compiled by the author on the basis of [17-22].

Applicability of foreign mechanisms to Kazakhstan

The fifth result is that the most transferable foreign mechanisms are those that strengthen coordination without requiring the wholesale transplantation of another country's legal regime. Four mechanisms appear especially relevant. First, Kazakhstan could develop a formal multi-actor anti-fraud coordination protocol connecting banks, telecom operators, regulators, and specialized law-enforcement units. Second, a unified incident analytics system could help detect clusters of similar schemes and generate early warnings. Third, rapid temporary intervention procedures could be defined for high-risk transaction patterns, subject to legal review and proportionality. Fourth, international liaison channels could be strengthened for urgent requests related to fraudulent domains, communication infrastructure, and asset tracing.

The literature on institutions and collaborative governance suggests that transferability depends on fit rather than imitation [25-27; 30]. A model that works in a highly centralized city-state may require adaptation in a larger jurisdiction with different market actors. A supranational system such as the European Union

cannot be reproduced domestically, but its emphasis on shared indicators and common threat classification can be adopted at national and regional levels. Similarly, the United States' complaint-based analytics may inspire a Kazakhstani system even if the institutional histories differ.

Table 5 provides an applicability matrix. It distinguishes between high-priority mechanisms that can plausibly be advanced through national coordination and medium-term mechanisms that require more extensive legal, technical, or international alignment. The matrix is intended as an analytical tool, not as a final legislative blueprint.

Table 5. Applicability Matrix of Foreign Anti-Fraud Mechanisms for Kazakhstan

Mechanism	Priority	Expected effect	Main implementation constraint
Multi-actor anti-fraud coordination protocol	High	Reduces delay between signal detection and escalation	Requires clear legal mandates and responsibility mapping
Unified fraud-incident analytics platform	High	Improves clustering, trend detection, and early warning	Requires interoperable data standards and privacy safeguards
Rapid temporary intervention for high-risk transfers	High	Increases chance of preserving funds during the critical window	Requires proportionality, appeal procedures, and accountability
Telecom and platform anti-spoofing coordination	Medium–High	Limits the initial reach of impersonation campaigns	Depends on technical standards and operator cooperation
Cross-border urgent referral channels	Medium	Improves take-downs, evidence preservation, and asset tracing	Depends on foreign partner responsiveness and legal compatibility

Source: compiled by the author on the basis of the comparative analysis and [22; 25; 26; 27; 30].

Evaluation indicators for anti-fraud governance

The sixth result concerns measurement. Anti-fraud governance is often discussed through legal reforms, public campaigns, or the number of detected cases, but these indicators do not fully reflect institutional effectiveness. A growing number of detected cases may indicate improved enforcement, wider victimization, better reporting, or all three simultaneously. For policy purposes, Kazakhstan needs a more operational set of indicators that measure whether institutions are becoming faster, more coordinated, and more capable of learning from incidents. Governance scholarship emphasizes that institutional capacity should be assessed by problem-solving performance rather than by formal institutional presence alone [14; 30].

A first group of indicators should measure time. These include the interval between the first suspicious signal and its escalation, the time between a victim's report and a temporary transaction freeze where legally permissible, and the time needed to issue sector-wide warnings when a recurring scam pattern is identified.

A second group should measure coordination: the number of standardized cross-sector alerts, the share of major fraud patterns that trigger joint analysis, and the proportion of cases in which banks, telecom operators, and law-enforcement bodies exchange operationally relevant information under defined procedures. Such indicators correspond to whole-of-government and collaborative governance approaches, which evaluate institutions through their capacity to connect fragmented actors [26; 27].

A third group should measure learning and international responsiveness. These indicators may include the frequency of updated fraud typologies, the speed of referral to foreign partners when domains or payment routes are located abroad, and the share of recurring schemes for which preventive guidance was issued before a significant escalation of harm. None of these indicators is simple to implement, and some require legal and technical prerequisites. Yet without a measurement framework, anti-fraud policy risks being evaluated only through general statements rather than through the operational features that determine whether losses can actually be prevented. Table 6 offers a compact indicator set for future institutional monitoring in Kazakhstan.

Table 6. Suggested Evaluation Indicators for Anti-Fraud Governance in Kazakhstan

Indicator group	**Illustrative metric**	**Policy meaning**	**Primary institutional users**
Response speed	Time from first risk signal to escalation	Shows whether institutions can act within the fraud window	Banks; regulator; police
Intervention speed	Time from complaint to legally permissible temporary freeze	Measures practical capacity to preserve funds	Banks; police; judiciary where required
Coordination density	Number of standardized cross-sector alerts and joint analyses	Shows whether fragmented signals are being connected	Banks; telecom operators; platforms; regulator
Learning capacity	Frequency of updated scam typologies and sector guidance	Measures adaptation to evolving fraud scripts	Regulator; police; financial intelligence actors
International responsiveness	Time to urgent foreign referral for infrastructure or asset-tracing requests	Captures the cross-border dimension of response	Law enforcement; international liaison units
Preventive effectiveness	Share of recurring fraud patterns addressed by guidance before large-scale escalation	Assesses whether institutions move from reaction to anticipation	All anti-fraud governance participants

Source: compiled by the author as a prospective monitoring framework, drawing on [14; 26; 27; 30].

Discussion

The findings support the article's central hypothesis: the rise and persistence

of transnational financial fraud in digitalizing environments are best explained not by technological change alone, but by the relationship between technological acceleration and institutional response capacity. Digitalization increases the availability of rapid transactions, normalized remote communication, and platform-mediated interaction. Fraud networks exploit these conditions by operating across multiple infrastructures and by breaking the scheme into modular roles. When institutions detect only fragments of the chain, or when intervention is slower than the circulation of funds, the system creates an opportunity for repeated victimization. The digitalization-capacity gap therefore describes a governance problem rather than a simple technological deficit.

This interpretation adds to the literature in several ways. The economics of online crime emphasizes reduced offender costs and scalable attack models [4]. Fraud victimization studies explain how persuasion, urgency, and authority facilitate compliance [7; 8]. Cybercrime research analyzes the territorial ambiguity of digital harm and the distributed nature of criminal networks [10-13; 23; 24]. Governance scholarship, in turn, focuses on implementation capacity, coordination, and institutional learning [14; 25-27; 30]. The digitalization-capacity gap brings these strands together. It explains why technical measures, user education, and criminal prosecution are all necessary but insufficient when they are not embedded in a coordinated response architecture.

The concept also clarifies the limits of an exclusively victim-centered approach. Public campaigns warning citizens against suspicious links, unknown callers, or unrealistic investment returns remain important. Yet they cannot neutralize fraud at scale if offenders continuously imitate legitimate communication channels and if payment infrastructures allow rapid extraction after a victim's initial compliance. A mature anti-fraud system must place responsibility not only on individual caution but also on institutional design. In this respect, the article aligns with research on electronic crime, which emphasizes that technological systems create specific opportunity structures that require corresponding prevention models [28].

A second implication concerns public–private coordination. In many fraud cases, no single actor sees the entire threat. Telecom providers may detect anomalous call patterns without knowing whether a payment follows. Banks may detect unusual transfer behavior without knowing that the customer is simultaneously speaking to a spoofed caller. Platforms may identify fraudulent advertisements without access to downstream transaction data. Law-enforcement bodies may receive complaints after the funds have already moved. Collaborative governance theory suggests that such problems require structured interaction based on clear roles, information protocols, and shared objectives [27]. Whole-of-government approaches also indicate that complex risks should not be split into rigid administrative silos when effective response depends on synchronization [26].

The Singaporean shared responsibility framework is important in this regard because it recognizes the chain character of scam-related harm [22]. Its

relevance for Kazakhstan lies less in the specific legal allocation of losses and more in the institutional principle of distributed prevention. Fraud prevention should be organized before the moment of loss, not only through post-factum dispute resolution. Banks, telecom operators, regulators, and digital platforms should know in advance which alerts can be transmitted, which temporary actions are legally permissible, and which authority coordinates escalation when a scheme appears to be spreading.

The European Union and the United States provide different but complementary lessons. Europol's threat assessments demonstrate the value of continuously updated analytical knowledge that connects separate fraud categories to wider organized cybercrime markets [19]. IC3 and FinCEN show how complaint collection and compliance alerts can transform incident reporting into strategic intelligence [20; 21]. For Kazakhstan, a comparable system would not necessarily require a large new institution. It could begin with standardized fraud typologies, shared incident tags, interoperable reporting channels, and periodic analytical reviews involving the regulator, financial sector, telecom operators, and law-enforcement bodies.

The article also has implications for international cooperation. Transnational fraud frequently depends on infrastructure located outside the victim's jurisdiction. Rapid take-down requests, domain suspension, exchange of payment-risk indicators, and asset tracing may require communication with foreign authorities or private entities that operate under different legal regimes. Traditional mutual legal assistance remains relevant, but its timelines may not always match the urgent phase of fraud interruption. This does not mean that due process should be bypassed. It means that states need parallel channels for operational indicators, emergency referrals, and standardized evidence preservation. International cybercrime research has long noted that the velocity of digital evidence challenges conventional jurisdictional routines [11; 28].

The Kazakhstani case is particularly significant because it reflects a broader dilemma faced by rapidly modernizing states. Digital transformation strategies frequently focus on infrastructure, access, and service delivery. Those priorities are justified. However, the legitimacy of digital modernization depends on whether citizens experience the system as trustworthy. If public institutions promote digitalization while fraudulent actors exploit the same channels more effectively than responsible authorities can respond, a credibility deficit may emerge. The digitalization-capacity gap thus concerns not only fraud reduction but also the political sustainability of digital governance.

The institutional perspective also helps avoid two simplifications. The first is technological determinism, the assumption that fraud increases simply because digital tools exist. The article shows that organizational and jurisdictional conditions determine whether tools become systematic vulnerabilities. The second is formal legalism, the assumption that new laws alone solve coordination problems. Institutional theory emphasizes that rules matter when

they are implemented through incentives, routines, capacities, and enforcement mechanisms [25]. Problem-solving capacity requires not only legal authority but also trained personnel, compatible data systems, actionable metrics, and institutional feedback loops [30].

From a policy perspective, five priorities follow. First, Kazakhstan would benefit from a permanent anti-fraud coordination platform that includes financial regulators, banks, telecom operators, specialized police units, and selected digital-service providers. Second, high-risk fraud indicators should be standardized so that actors can exchange operationally meaningful signals rather than unstructured complaints. Third, urgent intervention procedures should be designed for the first hours after a suspicious transaction, when interruption may still be feasible. Fourth, complaint data should be converted into analytical intelligence rather than remaining a record of completed harm. Fifth, international liaison mechanisms should focus on speed, evidence preservation, and infrastructure disruption in addition to conventional investigative cooperation.

These recommendations require legal safeguards. Expanded coordination should not become a justification for indiscriminate surveillance, opaque blocking, or disproportionate restrictions on digital access. Anti-fraud governance must balance effectiveness with data protection, due process, and transparency. A citizen whose transaction is temporarily delayed because of a risk trigger should have access to clear procedures and correction mechanisms. A financial institution sharing risk information should operate within defined legal boundaries. A telecom operator limiting suspicious traffic should do so through accountable technical standards. The legitimacy of anti-fraud policy depends on both protection and restraint.

The article also opens a regional research agenda. Kazakhstan shares with several Central Asian states a combination of rapid digitalization, expanding mobile connectivity, and evolving institutional capacity. Comparative research could examine whether similar fraud ecosystems emerge across the region, how regulatory and law-enforcement structures differ, and whether regional cooperation mechanisms could improve early-warning systems. Such analysis would enrich both international relations scholarship and practical policy debate by connecting cyber-enabled fraud to broader questions of regional resilience and transboundary risk governance.

Finally, the proposed model should be tested empirically. Future studies could use incident-level datasets to measure the time between victim contact, transaction initiation, bank response, complaint registration, and fund freezing. Interviews with banks, telecom operators, regulators, and investigators could identify bottlenecks in real-time coordination. Comparative case studies could examine failed and successful interventions to determine which mechanisms most effectively reduce loss. The digitalization-capacity gap is designed as a starting framework for such inquiry, not as a closed explanation.

Conclusion

Transnational financial fraud in the context of digitalization should be understood as a multidimensional security challenge located at the intersection of financial modernization, cybercrime, institutional capacity, and international cooperation. The Kazakhstani case demonstrates that the expansion of digital services and payment instruments creates major benefits for citizens and the economy, but it also increases the relevance of rapid and coordinated anti-fraud governance. Fraudsters do not merely exploit technical weaknesses; they exploit the interaction between digital trust, urgent communication, fragmented institutional signals, and the speed of financial flows.

The article proposed the concept of a digitalization-capacity gap to explain this problem. The gap arises when the adaptive speed of fraudulent networks exceeds the speed with which legitimate institutions can prevent, detect, exchange information about, and interrupt fraudulent activity. In Kazakhstan, this gap is expressed through four core dimensions: temporal delay, informational fragmentation, organizational coordination barriers, and jurisdictional dependence on cross-border procedures. An additional analytical challenge lies in the ability of institutions to learn from emerging fraud patterns before they become routine.

The comparative analysis of Singapore, the European Union, and the United States shows that successful anti-fraud policy is not limited to public warnings or post-incident prosecution. It depends on shared responsibility, structured threat intelligence, complaint-based analytics, rapid coordination, and the ability to convert isolated signals into timely interventions. These lessons are directly relevant for Kazakhstan, although they must be adapted to national legal, administrative, and market conditions rather than copied mechanically.

The practical conclusion is that Kazakhstan would benefit from an integrated anti-fraud governance architecture. Such an architecture should include a permanent coordination mechanism among banks, telecom operators, regulators, law-enforcement bodies, and digital platforms; standardized fraud typologies; a unified incident-analytics layer; clear procedures for urgent temporary intervention; and strengthened international channels for infrastructure disruption and asset tracing. These mechanisms should be accompanied by safeguards for data protection, proportionality, and transparency.

The broader significance of the article lies in its attempt to connect digitalization policy with questions of international security and institutional resilience. States that digitize quickly must not treat fraud prevention as a secondary technical issue. It is part of the trust infrastructure of the digital state. Further research should test the proposed framework with empirical datasets, regional comparisons, and expert interviews. Such work would help move the debate from reactive fraud control toward a more anticipatory model of transnational digital risk governance.

REFERENCES

[1] Adilet. Об утверждении Государственной программы «Цифровой Казахстан» [Электронный ресурс]. – 2017. – https://adilet.zan.kz/rus/docs/P1700000827

[2] eGov.kz. Что такое электронное правительство и для чего оно нужно? [Электронный ресурс]. – 2025. – https://egov.kz/cms/ru/information/about/help-elektronnoe-pravitelstvo

[3] National Bank of Kazakhstan. Statistics of Payment Instruments [Electronic resource]. – 2025. – https://nationalbank.kz/en/news/statistika-po-platezhnym-instrumentam

[4] Moore T., Clayton R., Anderson R. The Economics of Online Crime // Journal of Economic Perspectives. – 2009. – Vol. 23, No. 3. – P. 3–20. – DOI: 10.1257/jep.23.3.3.

[5] FATF. Guidance on Digital Identity [Electronic resource]. – Paris: FATF, 2020. –https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html

[6] Kethineni S., Cao Y. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity // International Criminal Justice Review. – 2020. – Vol. 30, No. 3. – P. 325–344. – DOI: 10.1177/1057567719827051.

[7] Button M., Nicholls C.M., Kerr J., Owen R. Online Frauds: Learning from Victims Why They Fall for These Scams // Australian & New Zealand Journal of Criminology. – 2014. – Vol. 47, No. 3. – P. 391–408. – DOI: 10.1177/0004865814521224.

[8] Button M., Cross C. Cyber Frauds, Scams and Their Victims. – London: Routledge, 2017.

[9] Holt T.J., Bossler A.M. An Assessment of the Current State of Cybercrime Scholarship // Deviant Behavior. – 2014. – Vol. 35, No. 1. – P. 20–40. – DOI: 10.1080/01639625.2013.822209.

[10] Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge : Polity Press, 2007.

[11] Brenner S.W. Cybercrime and International Law: Challenges and Responses // Journal of International Affairs. – 2007. – Vol. 61, No. 1. – P. 77–90.

[12] Broadhurst R., Grabosky P., Alazab M., Chon S. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime // International Journal of Cyber Criminology. – 2014. – Vol. 8, No. 1. – P. 1–20.

[13] Leukfeldt E.R., Kleemans E.R., Stol W.P. Cybercriminal Networks, Social Ties and Online Forums: Social Opportunity Structures in Cybercrime // British Journal of Criminology. – 2017. – Vol. 57, No. 3. – P. 704–722. – DOI: 10.1093/bjc/azw009.

[14] Fukuyama F. What Is Governance? // Governance. – 2013. – Vol. 26, No. 3. – P. 347–368. – DOI: 10.1111/gove.12035.

[15] Christou G. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy. – London : Palgrave Macmillan, 2015.

[16] Dupont B. Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime // Crime, Law and Social Change. – 2017. – Vol. 67, No. 1. – P. 97–116. – DOI: 10.1007/s10611-016-9649-4.

[17] Ministry of Internal Affairs of the Republic of Kazakhstan. Countering Cybercrime (CyberPol Project) [Electronic resource]. – 2025. – Available at: https://www.gov.kz/memleket/entities/qriim/activities/25086?lang=ru (accessed: 25.06.2026).

[18] Polisia.kz. The CyberPol Project Shows Results [Electronic resource]. – 2023. –https://polisia.kz/ru/proekt-cyberpol-pokazyvaet-rezul-taty/

[19] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024 [Electronic resource]. – Hague: Europol, 2024. – https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

[20] FBI Internet Crime Complaint Center (IC3). 2024 IC3 Annual Report [Electronic resource]. – 2024. – https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[21] FinCEN. FinCEN Alert on Fraud Schemes Involving Deepfake Media in BEC and Other Scams [Electronic resource]. – 2024. – https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

[22] Monetary Authority of Singapore (MAS), Infocomm Media Development Authority (IMDA). MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024 [Electronic resource]. – 2024. – https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024

[23] Yar M. Cybercrime and Society. – 2nd ed. – London: SAGE Publications, 2013.

[24] Lusthaus J. Industry of Anonymity: Inside the Business of Cybercrime. – Cambridge, MA: Harvard University Press, 2018.

[25] North D.C. Institutions, Institutional Change and Economic Performance. – Cambridge: Cambridge University Press, 1990.

[26] Christensen T., Lægreid P. The Whole-of-Government Approach to Public Sector Reform // Public Administration Review. – 2007. – Vol. 67, No. 6. – P. 1059–1066.

[27] Ansell C., Gash A. Collaborative Governance in Theory and Practice // Journal of Public Administration Research and Theory. – 2008. – Vol. 18, No. 4. – P. 543–571.

[28] Grabosky P. Electronic Crime. – Upper Saddle River, NJ: Pearson Prentice Hall, 2007.

[29] Ostrom E. Polycentric Systems for Coping with Collective Action and Global Environmental Change // Global Environmental Change. – 2010. – Vol. 20, No. 4. – P. 550–557.

[30] Lodge M., Wegrich K. The Problem-Solving Capacity of the Modern State: Governance Challenges and Administrative Capacities. – Oxford: Oxford University Press, 2014.

ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ ТРАНСҰЛТТЫҚ ҚАРЖЫЛЫҚ АЛАЯҚТЫҚ: ҚАЗАҚСТАННЫҢ ИНСТИТУЦИОНАЛДЫҚ СЫН-ҚАТЕРЛЕРІ ЖӘНЕ ХАЛЫҚАРАЛЫҚ ҚАРСЫ ІС-ҚИМЫЛ ТЕТІКТЕРІ

Брасилова А.[1], *Сарыбаев М.[2]
[1,*2] Әл-Фараби атындағы Қазақ ұлттық университеті,
Алматы, Қазақстан Республикасы

Аңдатпа. Мақалада трансұлттық қаржылық алаяқтық Қазақстандағы жедел цифрландыру жағдайында қалыптасып отырған институционалдық қауіпсіздік сын-қатері ретінде қарастырылады. Мобильді төлемдердің, цифрлық мемлекеттік қызметтердің, қашықтан сәйкестендіру жүйелерінің, платформалық коммуникацияның және трансшекаралық қаржы құралдарының кеңеюі алаяқтық әрекеттердің ауқымын ғана емес, олардың ұйымдасу логикасын да өзгертетіні негізделеді. Қазіргі схемалар әлеуметтік инженерияны, байланыс арналарын бұрмалауды, шетелдік хостингті, дропперлер желісін, қаражатты криптоактивтерге конвертациялауды және халықаралық төлем маршруттарын ұштастыра қолданады. Нәтижесінде қарсы іс-қимылдың тиімділігі жекелеген техникалық тосқауылдарға емес, институттардың қауіптің даму жылдамдығымен салыстырмалы режимде үйлесімді әрекет ету қабілетіне тәуелді болады. Мақаланың мақсаты -Қазақстандағы цифрлық қаржылық алаяқтықтың не себепті трансұлттық сипат алып отырғанын түсіндіру және ұлттық тәжірибеге бейімдеуге болатын шетелдік институционалдық тетіктерді айқындау. Зерттеу саясат құжаттарын, ресми есептерді және киберқылмыс, алаяқтықтан виктимизация, институционалдық әлеует пен бірлескен реттеу мәселелеріне арналған академиялық әдебиеттерді сапалық салыстырмалы-институционалдық талдау негізінде жүргізілді. Мақалада «цифрландыру мен институционалдық әлеует арасындағы алшақтық» тұжырымдамасы дамытылады; ол цифрлық экожүйелердегі қылмыстық бейімделу қарқыны мен институционалдық алдын алу, ақпарат алмасу, жедел араласу және трансшекаралықынтымақтастықмүмкіндіктерініңжылдамдығыарасындағы сәйкессіздік ретінде түсіндіріледі. Зерттеу нәтижелері Қазақстанның негізгі осал тұстары уақыттық, ақпараттық, ұйымдастырушылық және юрисдикциялық өлшемдерде көрінетінін көрсетеді. Сингапур, Еуропалық одақ және АҚШ тәжірибесін салыстырмалы бағалау бөлінген жауапкершілік модельдерінің, қауіптерді талдау платформаларының, шағымдарға негізделген аналитиканың және жедел әрекет ету механизмдерінің маңызын айқындайды. Қорытындыда Қазақстанда қаржы реттеушілерін, банктерді,

телекоммуникация операторларын, құқық қорғау органдарын, цифрлық платформаларды және халықаралық серіктестерді біріктіретін алаяқтыққа қарсы интеграцияланған басқару архитектурасын қалыптастыру қажеттігі негізделеді.

Тірек сөздер: трансұлттық қаржылық алаяқтық, цифрландыру, Қазақстан, халықаралық қауіпсіздік, киберқылмыс, институционалдық әлеует, алаяқтыққа қарсы басқару, ведомствоаралық үйлестіру, трансшекаралық ынтымақтастық

ТРАНСНАЦИОНАЛЬНОЕ ФИНАНСОВОЕ МОШЕННИЧЕСТВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ИНСТИТУЦИОНАЛЬНЫЕ ВЫЗОВЫ КАЗАХСТАНА И МЕЖДУНАРОДНЫЕ МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ

Брасилова А.[1], *Сарыбаев М.[2]
[1,*2] Казахский национальный Университет имени Аль-Фараби,
Алматы, Казахстан

Аннотация. В статье транснациональное финансовое мошенничество рассматривается как институциональный вызов безопасности, формирующийся в условиях ускоренной цифровизации Казахстана. Обосновывается, что распространение мобильных платежей, цифровых государственных услуг, дистанционной идентификации, платформенной коммуникации и трансграничных финансовых инструментов изменило не только масштабы мошеннической активности, но и её организационную логику. Современные схемы всё чаще сочетают социальную инженерию, подмену коммуникаций, зарубежный хостинг, сети дропперов, конвертацию средств в криптоактивы и международные платежные маршруты. В результате эффективность противодействия определяется не столько отдельными техническими барьерами, сколько способностью институтов координироваться в режиме, сопоставимом со скоростью развития угрозы. Цель статьи - объяснить, почему цифровое финансовое мошенничество в Казахстане приобретает транснациональный характер, и определить зарубежные институциональные механизмы, которые могут быть адаптированы в национальной практике. Исследование выполнено на основе качественного сравнительно-институционального анализа документов политики, официальных отчётов и академической литературы по киберпреступности, виктимизации от мошенничества, институциональной ёмкости и совместному регулированию. В статье развивается концепция «разрыва между цифровизацией и институциональной ёмкостью», понимаемого как несоответствие между скоростью криминальной адаптации в цифровых экосистемах и скоростью институциональной превенции, обмена информацией, срочного вмешательства и трансграничного сотрудничества. Результаты показывают, что ключевые уязвимости Казахстана имеют

временное, информационное, организационное и юрисдикционное измерения. Сравнительная оценка опыта Сингапура, Европейского союза и США демонстрирует значимость моделей распределённой ответственности, платформ аналитики угроз, жалобо-ориентированной аналитики и механизмов быстрого реагирования. Делается вывод о необходимости формирования в Казахстане интегрированной архитектуры антифрод-управления, объединяющей финансовых регуляторов, банки, телеком-операторов, правоохранительные органы, цифровые платформы и международных партнёров.

Ключевые слова: транснациональное финансовое мошенничество, цифровизация, Казахстан, международная безопасность, киберпреступность, институциональная ёмкость, антифрод-управление, межведомственная координация, трансграничное сотрудничество

Received / Мақала түсті / Статья поступила: 04.05.2026.
Accepted / Жариялауға қабылданды / Принята к публикации: 26.06.2026

Information about authors:

Brassilova Akzhunis - 1-year PhD candidate. Department of International Relations and World Economy. Farabi University, Almaty, Kazakhstan, ORCID ID 0009-0004-7926-6924, e-mail: vida@inbox.ru

Sarybayev Meiram Seisenbayevich – PhD., Associate Professor. Farabi University, Almaty, Kazakhstan, ORCID ID 0000-0001-8420-92, e-mail: smeiram81@gmail.com

Авторлар туралы мәлімет:

Брасилова Ақжүніс – 1-курс PhD докторанты. Халықаралық қатынастар және әлемдік экономика кафедрасы. Фараби университеті, Алматы, Қазақстан, ORCID ID 0009-0004-7926-6924, e-mail: vida@inbox.ru

Сарыбаев Мейрам Сейсенбаевич - PhD, қауымдастырылған профессор. Фараби университеті, Алматы, Қазақстан, ORCID ID 0000-0001-8420-92, e-mail: smeiram81@gmail.com

Информация об авторах:

Брасилова Ақжүніс - PhD докторант 1 курса. Кафедра международных отношений и мировой экономики. Университет Фараби, Алматы, Казахстан, ORCID ID 0009-0004-7926-6924, e-mail: vida@inbox.ru

Сарыбаев Мейрам Сейсенбаевич - PhD, ассоциированный профессор. Университет Фараби, Алматы, Казахстан, ORCID ID 0000-0001-8420-92, e-mail: smeiram81@gmail.com