АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР / ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ / INFORMATION AND COMMUNICATION TECHNOLOGIES

DOI 10.54596/2958-0048-2025-3-170-180
UDK 343.9.01
IRSTI 81.93.29

ROOT CAUSE ANALYSIS OF MAJOR CYBERSECURITY INCIDENTS AND DATA BREACHES IN KAZAKHSTAN (2017-2025)

Issakov Y.A.[1*]
[1*]*New York University Tandon School of Engineering, New York, USA*
[*]*Corresponding author: yi2038@nyu.edu*

Abstract

This article analyzes the root causes of key cybersecurity breaches in Kazakhstan from 2017 through 2025. Focusing on the DamuMed health-data breach (2019), the Kaspi.kz banking outage (2020), the Zaimer.kz microfinance leak (2024), and the compilation leak of 16 million records (2025), I examine technical vulnerabilities, human factors, legal weaknesses, and infrastructural gaps that enabled these incidents. I synthesize findings from official reports, news accounts, and expert commentary, and compare them with international examples such as the 2015 U.S. OPM breach, GDPR enforcement in Europe, and UK incidents (e.g. NHS and retailer attacks). My analysis reveals common causes: poor system security (outdated software, lack of encryption or multi-factor authentication), insider misuse or error, weak regulatory enforcement, and insufficient cyber-education. I discuss how Kazakhstan's rapid digitalization, while building strong legal frameworks (Cyber Shield strategy), has outpaced investments in security and awareness. Recommendations include strengthening regulation and enforcement (e.g. creating a data protection authority), adopting technical standards (encryption, MFA, regular audits), establishing independent supervisory bodies, expanding cybersecurity education and training, deploying AI-driven monitoring, enhancing organizational accountability (through fines and audits), and deepening international cooperation under frameworks like the Budapest Convention. These measures, grounded in evidence and aligned with best practices (NIST, ENISA, UNESCO), aim to prevent future breaches. The study's novelty lies in an author-developed, four-factor framework applied across domestic cases to enable structured, cross-country comparison.

Keywords: Kazakhstan, Cybersecurity, Data Breaches, Cyber Policy, Digital Infrastructure.

ҚАЗАҚСТАНДАҒЫ КИБЕРҚАУІПСІЗДІК ПЕН ДЕРЕКТЕРДІҢ БҰЗЫЛУЫНЫҢ НЕГІЗГІ СЕБЕПТЕРІН ТАЛДАУ (2017-2025)

Исаков Е.А.[1*]
[1*]*Нью-Йорк Университетінің Тандон Инженерлік Мектебі, Нью-Йорк, АҚШ*
[*]*Хат-хабар үшін автор: yi2038@nyu.edu*

Аңдатпа

Бұл мақалада 2017-2025 жылдар аралығында Қазақстандағы киберқауіпсіздіктің негізгі бұзылуының негізгі себептері талданады. Зақымдалған медициналық деректердің бұзылуына назар аудара отырып (2019), Kaspi.kz банктік қызметтің үзілуі (2020), Zaimer.kz микроқаржыландырудың ағып кетуі (2024 ж.) және 16 миллион жазбаның (2025 ж.) жинақталуының ағып кетуі осы оқиғалардың орын алуына себеп болған техникалық осалдықтарды, адами факторларды, құқықтық әлсіздіктерді және инфрақұрылымдық олқылықтарды зерттейді. Біз ресми есептерден, жаңалықтар репортаждарынан және сарапшылардың түсініктемелерінен алынған нәтижелерді синтездейміз ЖӘНЕ оларды 2015 жылғы АҚШ сияқты халықаралық мысалдармен салыстырамыз. OPM ережелерін бұзу, Еуропадағы GDPR ережелерін сақтау және Ұлыбританиядағы оқиғалар (мысалы, ұлттық денсаулық сақтау қызметі мен бөлшек саудагерлердің шабуылдары). Біздің талдауымыз жалпы себептерді анықтайды: жүйелік қауіпсіздіктің

нашарлығы (ескірген бағдарламалық жасақтама, шифрлаудың немесе көп факторлы аутентификацияның болмауы), инсайдерлердің теріс пайдалануы немесе қателіктері, нормативтік құқықтық актілердің әлсіз орындалуы және кибербілімнің жеткіліксіздігі. Біз Қазақстанның қарқынды цифрландыруының күшті құқықтық базаны (Cyber Shield стратегиясы) құра отырып, қауіпсіздік пен хабардарлықты арттыруға салынған инвестициялардан қалай асып түскенін талқылаймыз. Ұсыныстарға реттеу мен орындауды күшейту кіреді (мысалы. деректерді қорғау органын құру), техникалық стандарттарды енгізу (шифрлау, CIM, тұрақты тексерулер), тәуелсіз қадағалау органдарын құру, киберқауіпсіздік бойынша білім беру мен оқытуды кеңейту, жасанды интеллектке негізделген мониторингті енгізу, ұйымдық есептілікті арттыру (айыппұлдар мен аудиттер арқылы) Және Будапешт Конвенциясы сияқты құрылымдар шеңберіндегі халықаралық ынтымақтастықты тереңдету. Дәлелдерге негізделген және озық тәжірибелерге (NIST, ENISA, ЮНЕСКО) сәйкес келетін бұл шаралар болашақта бұзушылықтардың алдын алуға бағытталған.

Кілт сөздер: Қазақстан, Киберқауіпсіздік, Деректердің Бұзылуы, Кибер Саясат, Цифрлық Инфрақұрылым.

АНАЛИЗ ОСНОВНЫХ ПРИЧИН КРУПНЫХ ИНЦИДЕНТОВ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ И УТЕЧЕК ДАННЫХ В КАЗАХСТАНЕ (2017-2025 ГГ.)

Исаков Е.А.[1*]

[1*]*Инженерная школа «Тандон» Нью-Йоркского университета, Нью-Йорк, США*

[*]*Автор для корреспонденции: yi2038@nyu.edu*

Аннотация

В этой статье анализируются первопричины ключевых нарушений кибербезопасности в Казахстане в период с 2017 по 2025 год. Сосредоточив внимание на предполагаемой утечке медицинских данных (2019), компания Kaspi.kz сбой в банковской деятельности (2020), Zaimer.kz утечка информации о микрофинансировании (2024) и утечка информации о 16 миллионах записей (2025), мы изучаем технические уязвимости, человеческий фактор, юридические недостатки и инфраструктурные пробелы, которые привели к этим инцидентам. Мы обобщаем выводы из официальных отчетов, новостных сообщений и комментариев экспертов и сравниваем их с международными примерами, такими как исследование в США в 2015 году. Нарушение OPM, применение GDPR в Европе и инциденты в Великобритании (например, атаки на NHS и розничных продавцов). Мой анализ выявил общие причины: слабая безопасность системы (устаревшее программное обеспечение, отсутствие шифрования или многофакторной аутентификации), злоупотребления или ошибки со стороны инсайдеров, слабое соблюдение нормативных требований и недостаточное киберобразование. Мы обсуждаем, как стремительная цифровизация Казахстана при одновременном создании прочной правовой базы (стратегия киберзащиты) опережает инвестиции в безопасность и повышение осведомленности. Рекомендации включают усиление регулирования и правоприменения (например, создание органа по защите данных), принятие технических стандартов (шифрование, MFA, регулярные аудиты), создание независимых надзорных органов, расширение образования и профессиональной подготовки в области кибербезопасности, внедрение мониторинга на основе искусственного интеллекта, повышение организационной подотчетности (посредством штрафов и аудитов) и углубление международного сотрудничества в рамках таких структур, как Будапештская конвенция. Эти меры, основанные на фактических данных и согласованные с передовой практикой (NIST, ENISA, UNESCO), направлены на предотвращение будущих нарушений.

Ключевые слова: Казахстан, Кибербезопасность, Утечка данных, Киберполитика, цифровая инфраструктура.

Introduction

Kazakhstan’s digital transformation in recent years has been rapid and ambitious. The government has expanded online public services, promoted e-government, and launched national strategies (e.g. the Cyber Shield concept) to modernize its economy [1][2]. As one analyst notes, “ensuring cybersecurity in cyberspace during the transformation period is one of the important issues” [1]. At the same time, high-profile cyber incidents worldwide - such as

the 2015 U.S. Office of Personnel Management (OPM) hack (22 million records stolen due to poor internal controls [3]) - highlight the vulnerabilities that accompany digitization. In Kazakhstan, multiple breaches have emerged, raising concern about the security of critical data. For example, in 2019 TSARKA (a citizen-led cyber watchdog) reported the leak of hundreds of thousands of patient records from the Damumed healthcare system [4]; in 2020, a technical glitch in the popular Kaspi.kz banking platform caused widespread service outages [5]; in 2024, personal data of some 2 million Zaimer.kz microfinance clients was exposed; and in mid-2025, an archive containing outdated records of approximately 16 million Kazakh citizens surfaced online [6]. This paper examines the root causes of these and other incidents (including leaks reported by TSARKA in election and medical registries [4]). It explores technical failures, human error or malfeasance, legal/institutional shortcomings, and infrastructural factors. I compare Kazakhstan's challenges and responses with international cases - e.g. the U.S. OPM breach, EU's GDPR enforcement (British Airways, Marriott) [7], UK NHS and retailer (Tesco Bank) incidents [8] - to benchmark best practices. Finally, I offer evidence-based recommendations (regulatory reform, standards, education, AI monitoring, accountability, international cooperation) to prevent future breaches in Kazakhstan's context.

Literature Review

Kazakhstan has undertaken significant legal and institutional efforts in cybersecurity. The country's Digital Kazakhstan agenda and Cyber Shield strategies (2017, updated 2022) aim to secure critical infrastructure and promote digital literacy. The Astana Times observes that Kazakhstan "leads Central Asia in cybersecurity" with a "relatively advanced institutional and legal framework" [2]. For example, Kazakhstan established an Information Security Committee within the Ministry of Digital Development, signed the Council of Europe's Budapest Convention on Cybercrime, and enacted a Personal Data Protection Law in 2020 (amended again in 2023) [6][9]. In the ITU's 2024 Global Cybersecurity Index, Kazakhstan ranked Tier 2 (Advancing) with strong legal/cooperative pillars, though the report urged improvements in organizational and technical capacity [10]. In practice, however, experts note gaps. Computer scientist Olzhas Satiev remarks that "more than 90% of Kazakhstan's Internet resources are vulnerable" and cites a shortage of qualified security personnel [1]. A CEUR workshop paper similarly found that "Kazakhstan's major concern is a poor degree of cyber literacy," leading to data losses and financial harm [11]. Indeed, surveys show extremely low public awareness: only 12% of Kazakh internet users feel well-informed about their data-rights, and 60% want to learn more [4].

International comparisons underline these issues. In the U.S., the 2015 OPM breach was blamed on lax practices: the agency "had no IT security staff until 2013" and lacked encryption, system inventories, or multi-factor authentication [3]. In Europe, the GDPR has shifted the burden to organizations - fines for British Airways (£20m) and Marriott (£18.4m) breaches exemplify the accountability expected under modern data laws [7]. The UK experience is instructive: a 2016 cyber-theft from Tesco Bank (£2.26m stolen from 9,000 accounts) led the UK's Financial Conduct Authority to fine Tesco £16.4m for "deficiencies" in card security and fraud controls. UK officials called that attack "deeply troubling" and emphasized "the crucial importance of technical security" in financial systems [8]. Similarly, the 2017 WannaCry ransomware attack crippled about 80 NHS trusts (over 300,000 computers) in Britain, exposing the vulnerability of health systems to unpatched malware. These examples illustrate that without strong security controls, even advanced economies suffer major data incidents. For Kazakhstan, aligning with global standards (e.g. NIST frameworks, ENISA guidance) is crucial. ENISA notes that all EU states have adopted national cybersecurity strategies and

mandates (via NIS2) regular updates of legal frameworks. UNESCO and others also stress investing in cybersecurity education and public awareness. In sum, the literature shows that strong policies must be matched by effective implementation: encryption and multi-factor authentication (NIST advises), continuous monitoring, legal enforcement, and a culture of security are all needed [3][8].

Methodology

I then identified root causes by coding information along technical, human, legal, and infrastructural dimensions.

To systematize this process, I developed an author's analytical framework that classifies causes into four categories: technical, organizational, human, and regulatory/legal. Each case is mapped against this scheme to ensure comparability across incidents. This framework represents the main element of novelty in the study, as it allows both domestic and cross-country incidents to be analyzed under a single structure.

Table 1. Analytical Framework for Categorizing Root Causes of Cybersecurity Incidents

Category	Definition	Examples in Kazakhstani Cases
Technical	Failures of software, hardware, or network security	Outdated systems, missing encryption, lack of MFA
Organizational	Weaknesses in governance, processes, or corporate practices	Absence of audits, poor data governance, weak resilience testing
Human	Insider misuse, negligence, or error	Unauthorized access (Damumed), employee mishandling of data
Regulatory/Legal	Gaps in laws, enforcement, or oversight	Small fines, no independent authority, limited investigations

Comparative analysis draws on published case studies of foreign incidents (e.g., OPM, GDPR fines, UK breaches). All sources are cited to ensure traceability. Where possible, I relied on reputable outlets and official releases; for local news, English-language reports (Astana Times, Times of Central Asia) were used to ensure accurate understanding.

Limitations: This approach relies on open-source and official reports, which may omit technical detail; some cases lack transparency (e.g., Kaspi.kz outage), making causal attributions partly interpretive. The framework is qualitative and not empirically validated, which constrains generalizability, but it ensures consistent comparison across incidents.

Results

Damumed is a centralized health-records system used by public and private clinics. In mid-2019, TSARKA reported that "medical information of hundreds of thousands of Damumed patients" had appeared online, marking one of the first large-scale leaks of Kazakh patient data [12]. The Ministry of Healthcare and Damumed's IT Center confirmed that the breach was caused by "a person having legal authorized user access" who illicitly transmitted confidential data [12]. Officials emphasized that no external hack had occurred, focusing instead on prosecuting the internal violator.

Root causes lay in weak internal safeguards:

- inadequate access controls;
- lack of privileged-user monitoring;
- insufficient insider-threat awareness;
- limited enforcement under Kazakhstan's personal data laws.

As TSARKA noted, the incident stemmed from "a simple error - an unauthorized access to [the] medical documents" by an insider [12]. In sum, human misuse and governance gaps combined to expose sensitive health records.

In late October 2020, Kaspi Bank (part of the fintech Kaspi.kz) suffered a major outage. Thousands of customers saw erroneous balances (some even showing trillions of tenges) and could not access banking or payment services [5]. Rumors spread of a cyber-theft ("79 million stolen"), but Kaspi emphatically denied any hack, stating that the glitch was technical and all funds remained safe [13]. Kazakhstan's Minister of Digital Development said the outage should be viewed like any technical failure rather than a breach, and no official investigation was launched absent reports of data misuse. Subsequent statements indicated the issue was fixed by November 2020.

The root cause appears to have been a technical failure rather than malicious attack. Experts suggested a misconfigured update or corrupted transaction ledger may have caused the display errors. Underlying factors included:

- software or network bugs in critical systems;
- insufficient resilience and stress testing;
- lack of transparency in incident reporting.

Although no customer data was exposed, the incident created widespread panic, highlighting vulnerabilities in public confidence and the importance of rigorous software testing and resilience planning.

Zaimer.kz, a leading microfinance institution, leaked data on approximately 2 million clients in March 2024 [6], [14]. This included not only borrowers but also many users who never took loans, indicating a massive collection of personal data. The leak was discovered by KZ-CERT, which found Zaimer's customer information "publicly available" on the internet. The Ministry's audit confirmed the loss of 2 million records, and Zaimer.kz was fined KZT 1.846 million for violating data protection rules [15].

The exposure revealed several shortcomings:

- unencrypted and insecurely stored databases;
- poor data governance and weak corporate security practices;
- possible illegal collection of additional customer data "on the side" as TSARKA hinted [14];
- late notification to citizens; modest regulatory penalties that lacked deterrent effect [15].

Together, these organizational and legal weaknesses explain the scale of the breach.

In June 2025, a dataset allegedly containing information on ~16.3 million Kazakh citizens appeared on a Chinese-run website, prompting an official investigation [6]. The government announced that no breach of state systems was found: the leaked database was largely outdated (circa 2022) and compiled from earlier breaches and internal sources. TSARKA founder Bekarys Kabi described it as a "compilation of previously stolen and fragmented data" merged to appear as a new mega-leak. The Ministry's joint inspection (Digital Development Ministry, NSC, STS) confirmed the leak consisted of old, previously exposed records, with no live government system compromised.

Root causes were multifaceted:

- weak protection of earlier datasets (financial, educational, registration records);
- failure to prevent aggregation and resale of leaked data;
- potential misuse of official data by insiders;
- immature enforcement of data protection laws, despite 2023 amendments [6].

Socially, this case eroded public trust: Kabi noted that personal data "will always be of interest to cybercriminals" unless preventive measures are taken.

TSARKA and news reports documented several additional breaches beyond the main four cases. For example, in 2019 TSARKA reported leaks of 11 million votes from the Central Election Commission and data from the Prosecutor General's Office, none of which saw thorough investigation [4]. Authorities often issued denials or attributed these exposures to unnamed insiders.

These incidents highlight systemic deficiencies:

- lack of transparent investigations and official follow-up;
- repeated reliance on "anonymous insider" explanations;
- weak institutional accountability and oversight.

Together, these patterns suggest that beyond technical flaws, a culture of denial and minimal enforcement undermines trust in cybersecurity governance.

To consolidate the case narratives, the author's analytical framework introduced in Methodology was applied to all incidents. Mapping each case across technical, organizational, human, and regulatory/legal dimensions makes the root causes directly comparable and highlights common systemic weaknesses.

Table 2. Classification of Major Incidents in Kazakhstan (2017-2025)

Incident (Year)	Technical Factors	Organizational Factors	Human Factors	Regulatory / Legal Factors	Consequences
Damumed (2019)	Inadequate access controls	Lack of privileged-user monitoring	Insider with legitimate access misuse	Weak enforcement of personal data laws	Exposure of patient data; legal proceedings; loss of trust in e-health
Kaspi.kz (2020)	Software failure, insufficient testing	Lack of resilience/stress testing	-	No investigation, weak accountability	Nationwide outage; user panic; reputational risk to fintech
Zaimer.kz (2024)	No encryption, vulnerable database	Poor company data protection	Possible staff negligence/ misuse	Small fine, weak regulation	~2 M records exposed; affected non-borrowers; delayed notification
16M leak (2025)	Aggregation of old leaks, no controls	Poor data hygiene across orgs	Insider/abusive users involved	Absence of independent supervisory body	Pan-national dataset compilation; broad privacy risk; erosion of e-gov trust

This structured synthesis shows that, although the immediate triggers varied across cases, they all stem from overlapping systemic weaknesses: outdated or insecure technical systems, insufficient organizational safeguards, recurring human factors, and underdeveloped regulatory enforcement. By applying this framework systematically, the study provides the first structured account of cyber breaches in Kazakhstan, addressing a gap in the existing literature that has so far treated such cases primarily in narrative form.

Discussion

My analysis identifies common root causes across these cases:

• Technical vulnerabilities: Outdated systems, lack of encryption, inadequate authentication, and weak network defenses were underlying factors. For instance, Kazakhstan's banks and agencies often operate on legacy platforms without multi-factor authentication; the Kaspi glitch revealed the fragility of digital banking infrastructure. These mirror U.S. findings, where the OPM hack succeeded partly because of "failure to… use multi-factor authentication" and absence of encryption [3]. Similarly, the UK Tesco Bank breach was blamed on "deficiencies in design of its debit card and financial crime controls" [16]. Kazakhstan's security investments have lagged behind its digital rollout [2]; the 2024 GCI report also calls for enhanced technical capabilities [10]. Regular security audits, encryption of databases, and adoption of standards (ISO/IEC 27001, NIST SP800-53 controls) are needed.

• Human factors: Many breaches involved human error or insider actions. The Damumed case was a classic example of an insider with legitimate access misusing data [12]. Poor cyber hygiene (weak passwords, phishing susceptibility), lack of staff training, and absence of a security culture contribute to breaches. CEUR researchers emphasize that "poor cyber literacy" in Kazakhstan leads directly to data losses and financial harm [11]. In the 16M incident, insiders augmenting leaked data underscores the human element in enabling breaches. To address this, Kazakhstan must invest in cybersecurity education at all levels. UNESCO and ITU recommend incorporating digital and media literacy in curricula; similarly, public awareness campaigns (as the 2020 surveys suggest) would reduce risky behavior.

• Legal and regulatory gaps: Kazakhstan's data protection law (initially enacted 2007, major revision in 2020, further amendments in 2023) provides a framework, but enforcement has been weak. The fact that breaches like Damumed and election data were "without proper solution" highlights poor rule-of-law follow-through [4]. While regulators can fine organizations (e.g. Zaimer's ~KZT1.8m penalty [15]), penalties remain modest and rarely deter recurrence. In contrast, GDPR has empowered EU Data Protection Authorities to levy massive fines (e.g. Marriott's £18.4m) [7]. Kazakhstan has also joined the Budapest Cybercrime Convention [9], committing to international cooperation, but domestic institutions lag. As of 2025 there is no independent Personal Data Protection Authority in Kazakhstan; such a body could oversee compliance and investigate breaches impartially. Legislators have recognized the need: the 2023 amendments authorized unscheduled inspections and broadened liabilities [6]. Future legal reforms should include clear breach notification rules (citizens were only notified belatedly after Zaimer) and minimum cybersecurity standards for critical sectors.

• Infrastructural challenges: Kazakhstan's telecom and IT infrastructure are highly centralized, which creates systemic risk. For example, the state-run Internet backbone must route through national checkpoints (there is only one main line to Europe), so a single incident can have a wide impact. The government's deployment of a national security certificate (SORM) for surveillance [17] also means all traffic is potentially inspected, raising privacy concerns and possibly creating centralized points to target. Furthermore, the choice (for expediency) of foreign software and hardware - as one analyst notes, "the choice of Russian

and Chinese software" and lax data regulation has been criticized [4] – can embed hidden risks if not vetted. To strengthen infrastructure, Kazakhstan should diversify connectivity, establish backup routes, and require supply-chain security for critical tech.

To benchmark Kazakhstan's patterns internationally, the same criteria were applied to well-documented cases.

Table 3. Cross-Country Comparison by Explicit Criteria

Criteria	Kazakhstan (Damumed, Zaimer, 16M)	USA (OPM 2015)	EU (BA, Marriott)	UK (NHS WannaCry, Tesco Bank)
Attack vector	Insider access; legacy data aggregation	External intrusion; lack of MFA	Phishing; unpatched vulns	Ransomware; flawed card systems
Incident response	Limited investigation; low transparency	MFA mandates; IT reforms	Heavy GDPR fines; strict DPIA/controls	NCSC coordination; mandatory reporting
Regulatory setting	Modest fines; no independent DPA	Weak pre-2015 oversight	Strong GDPR enforcement	FCA penalties; sector guidance
Social impact	Trust erosion in e-gov services	Massive federal personnel breach	Corporate losses, brand damage	Health service disruption; public concern

This matrix shows Kazakhstan's cause profile is typical of global breaches, while its response/regulatory profile remains less mature than GDPR/FCA regimes explaining recurring exposures and limited deterrence.

International comparisons yield further lessons. The U.S. OPM case led to mandates for multi-factor authentication across federal agencies (per OPM reforms). The EU's NIS Directive (and new NIS2) now compel Member States to adopt and regularly update national strategies (ENISA notes all EU countries have done so by 2017). Kazakhstan already has a Cyber Shield strategy, but it needs periodic review and concrete benchmarks (cf. targets in the 2017 concept [1]). The UK's response to NHS and retailer incidents (establishing the National Cyber Security Centre, imposing mandatory cyber-incident reporting, and real penalties) provides a model for strengthening deterrence and assistance.

Based on these findings, I propose the following actionable recommendations:

- Regulatory Reforms: Enact a dedicated Data Protection Act with enforcement powers and establish an independent Data Protection Authority. Expand the scope of cybersecurity laws to mandate incident reporting and minimum security controls for all organizations handling personal data. Increase penalties for negligence. Align Kazakhstan's regulations with international standards (GDPR, NIST Cybersecurity Framework) to foster trust and compliance.
- Technical Standards and Best Practices: Require critical infrastructure and large organizations to adopt recognised standards (e.g. ISO/IEC 27001 certification). Enforce encryption of sensitive data at rest and in transit. Mandate multi-factor authentication and network segmentation in high-risk systems. Promote regular independent penetration testing

and security audits (as recommended by experts [6]). The government should publish guidelines (through KZ-CERT) on baseline cybersecurity measures, akin to NIST/ENISA publications.

- Independent Supervisory Bodies: Create a centralized National Cybersecurity Agency (if not already) or empower KZ-CERT and the Digital Development Ministry to perform oversight. This body should coordinate threat intelligence sharing and incident response, and supervise compliance. It could also manage a "critical sectors" registry requiring security clearances (much like the NIS2 authority role in the EU).
- Cybersecurity Education and Literacy: Launch nationwide programs to improve cyber hygiene. Integrate cybersecurity modules into school curricula and professional training (drawing on UNESCO media-literacy guidelines). Offer free or subsidized courses in digital self-protection for the public. Encourage universities to develop specialized cybersecurity degree programs (addressing the 90% vulnerability and skills gap noted by Satiev [1]).
- Use of AI and Monitoring Tools: Invest in AI-driven tools for threat detection, network monitoring, and anomaly detection across government networks. Deploy Security Operation Centers (SOCs) with machine learning to identify breaches quickly. However, ensure these tools respect privacy and do not become surveillance tools of last resort. Kazakhstan should also implement "Bug Bounty" programs and crowdsourced vulnerability disclosure (per Bekarys Kabi's recommendation) [6], as many countries now do.
- Organizational Accountability: Foster a culture of accountability by requiring companies to audit their data practices. Encourage board-level oversight of cybersecurity. Use public-private partnerships to improve sectoral defenses (for example, banks sharing threat information, as Kabi suggested). Learning from the Tesco Bank fine [16], regulators should hold CEOs and CISOs accountable for gross lapses.
- International Cooperation: Strengthen collaboration with international bodies (UN, Interpol, CERT-EU, etc.). Leverage Kazakhstan's participation in the Budapest Convention to work with other signatories on cross-border cybercrime. Join global platforms like the Global Forum on Cyber Expertise and regional initiatives (e.g., Shanghai Cooperation Organisation's cybersecurity cooperation). Work with agencies like ENISA and NIST for best-practice exchange. Joint exercises with partners can improve readiness.

Together, these measures can address the systemic vulnerabilities identified. Kazakhstan's own reports confirm the need for stronger organizational measures and capacity-building [10]; the incidents of 2019-2025 underscore it. Benchmarked against international cases, it is clear that legal frameworks alone are insufficient without enforcement and education. For example, after the OPM hack the U.S. mandated stricter ID vetting and technical controls; similarly, Kazakhstan should make security investment commensurate with its digital ambitions. In policy design, Kazakhstan can draw on ENISA's guidance that national strategies must be living documents with clear timelines and resources. At the grassroots, boosting citizens' trust requires transparency: timely breach notifications and public accountability (contrasting with the current "no solution" approach [16]).

Conclusion

The period 2017-2025 saw Kazakhstan transition rapidly into the digital age, but this has exposed critical security gaps. The Damumed health-data leak, Kaspi.kz outage, Zaimer.kz client data exposure, and the 16-million-person compilation all share root causes: technical laxity, human error/insider threats, and immature legal enforcement. Despite strong strategic initiatives (Cyber Shield, GCI progress) [2], [10], implementation has lagged - digitalization outpaced security. International experience shows that addressing these requires comprehensive action: robust technical defenses, well-enforced laws, informed citizens, and global

partnerships. My evidence-based recommendations - spanning regulation, standards, oversight, education, AI, accountability, and international cooperation - aim to close the gaps revealed by past breaches. By adopting these measures, Kazakhstan can harden its infrastructure, cultivate cyber-savvy organizations and populace, and ultimately prevent future incidents.

This research applies an original four-factor framework, covering technical, organizational, human, and regulatory/legal causes, to the analysis of Kazakhstan's cyber incidents. The framework turns case narratives into a structured synthesis that exposes systemic weaknesses and allows direct comparison across incidents. Combined with explicit cross-country criteria (attack vector, incident response, regulatory setting, and social impact), it situates Kazakhstan's experience within the wider global cybersecurity landscape. As a result, the study delivers both actionable policy guidance for Kazakhstan and a methodological approach that can be adapted for examining cybersecurity breaches in other emerging digital economies.

Implications for Policymakers

The analysis highlights not only academic insights but also concrete directions for decision-makers:

- Government: Establish an independent Data Protection Authority with investigative powers; mandate timely breach notification; increase penalties to create real deterrence; ensure national strategies (e.g., Cyber Shield) are periodically reviewed with measurable benchmarks.
- Businesses: Require adoption of international standards such as ISO/IEC 27001; enforce encryption of sensitive data at rest and in transit; mandate multi-factor authentication; conduct regular penetration testing and audits to build resilience.
- Society: Invest in nationwide cybersecurity literacy campaigns; embed digital safety into school curricula and professional training; promote public awareness initiatives to reduce risky online behaviors.
- International Cooperation: Deepen participation in global cyber frameworks (Budapest Convention, ENISA exchanges, NIST collaborations); join regional and international cyber exercises to strengthen readiness and share best practices.

These implications underline that cybersecurity is a shared responsibility across state, corporate, and societal levels. Only through coordinated reforms and capacity-building can Kazakhstan bridge the gap between its ambitious digital agenda and its current security vulnerabilities.

References:

1. Issabaeva A. Cyber security issues in digital Kazakhstan [Elektronnyy resurs]. - Rezhim dostupa: https://www.nispa.org/files/conferences/2019/e-proceedings/system_files/papers/cyber-security-issues-issabaeva.pdf(data obrashcheniya: 12.05.2025).
2. Kazakhstan leads Central Asia in cybersecurity, says new regional study [Elektronnyy resurs] // *The Astana Times*. - 23.07.2025. - Rezhim dostupa: https://astanatimes.com/2025/07/kazakhstan-leads-central-asia-in-cybersecurity-says-new-regional-study (data obrashcheniya: 10.08.2025).
3. Zetter K. Why the OPM breach is such a security and privacy debacle [Elektronnyy resurs] // *Wired*. - 12.06.2015. - Rezhim dostupa: https://www.wired.com/2015/06/opm-breach-security-privacy-debacle (data obrashcheniya: 04.02.2024).
4. Gussarova A. Technology-surveillance nexus beyond COVID-19: the outskirts of digitalisation in Kazakhstan [Elektronnyy resurs] // *Foreign Policy Centre*. - 2021. - Rezhim dostupa: https://fpc.org.uk/technology-surveillance-nexus-beyond-covid-19-the-outskirts-of-digitalisation-in-kazakhstan (data obrashcheniya: 12.03.2025).

5. Kaspi bank: ocheredi i sboi v prilozhenii [Elektronnyy resurs] // *Sputnik Kazakhstan*. - 28.10.2020. - Rezhim dostupa: https://ru.sputnik.kz/20201028/kaspi-bank-ocheredi-video-15316324.html (data obrashcheniya: 17.07.2025).
6. What we know about data leak affecting 16 million Kazakh citizens [Elektronnyy resurs] // *The Astana Times*. - 29.07.2025. - Rezhim dostupa: https://astanatimes.com/2025/07/what-we-know-about-data-leak-affecting-16-million-kazakh-citizens (data obrashcheniya: 01.08.2025).
7. Pierides M., Cavendish C. ICO GDPR fines reduced to £20m and £18.4m to reflect British Airways and Marriott mitigating factors [Elektronnyy resurs] // *Tech & Sourcing@Morgan Lewis*. - 06.11.2020. - Rezhim dostupa: https://www.morganlewis.com/blogs/sourcingatmorganlewis/2020/11/ico-gdpr-fines-reduced-to-20m-and-18-4m-to-reflect-british-airways-and-marriott-mitigating-factors (data obrashcheniya: 20.12.2024).
8. Treanor J. Tesco Bank cyber-thieves stole £2.5m from 9,000 people [Elektronnyy resurs] // *The Guardian*. - 08.11.2016. - Rezhim dostupa: https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m (data obrashcheniya: 03.01.2025).
9. Kazakhstan data breach - an overview [Elektronnyy resurs] // *CERTPro*. - 2024. - Rezhim dostupa: https://certpro.com/kazakhstan-data-breach (data obrashcheniya: 29.01.2025).
10. Ministerstvo tsifrovogo razvitiya Respubliki Kazakhstan. Kazakhstan strengthens positions in Global Cybersecurity Index 2024 [Elektronnyy resurs] // *Gov.kz*. - 12.09.2024. - Rezhim dostupa: https://www.gov.kz/memleket/entities/mdai/press/news/details/845520?lang=ru (data obrashcheniya: 22.08.2025).
11. Alexandrova A., Kuznetcov A., Arkhipova O. Analysis of major factors preventing cybercrime reduction in Kazakhstan [Elektronnyy resurs] // *CEUR Workshop Proceedings*. - Vol. 3680. - 2023. - Rezhim dostupa: https://ceur-ws.org/Vol-3680/S4Paper3.pdf (data obrashcheniya: 22.08.2025).
12. Utechka dannykh tysyach patsientov proizoshla v Kazakhstane [Elektronnyy resurs] // *Tengrinews.kz*. - 07.2019. - Rezhim dostupa: https://tengrinews.kz/kazakhstan_news/utechka-dannyih-tyisyach-patsientov-proizoshla-v-kazahstane-373363 (data obrashcheniya: 22.08.2025).
13. Ministr prokommentiroval sboi Kaspi.kz [Elektronnyy resurs] // *Tengrinews.kz*. - 29.10.2020. - Rezhim dostupa: https://tengrinews.kz/kazakhstan_news/ministr-prokommentiroval-sboy-kaspikz-418520 (data obrashcheniya: 22.08.2025).
14. Kazakhstan probes massive data leak involving 16 million citizens [Elektronnyy resurs] // *Orda.kz* (English ed.). - 17.06.2025. - Rezhim dostupa: https://en.orda.kz/kazakhstan-probes-massive-data-leak-involving-16-million-citizens-6914 (data obrashcheniya: 19.06.2025).
15. Zaimer.kz oshtrafovali na 18 mln tenge za massovuyu utechku lichnykh dannykh [Elektronnyy resurs] // *Orda.kz*. - 03.2024. - Rezhim dostupa: https://orda.kz/zaimerkz-oshtrafovali-na-18-mln-tenge-za-massovuju-utechku-lichnyh-dannyh-384516 (data obrashcheniya: 28.07.2025).
16. Financial Conduct Authority. FCA fines Tesco Bank £16.4 million for IT control failures [Elektronnyy resurs]. - 01.10.2018. - Rezhim dostupa: https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack (data obrashcheniya: 05.02.2025).

Information about the author:

Issakov Y.A. – corresponding author, MS in Electrical Engineering, graduate of NYU Tandon School of Engineering, New York, USA; e-mail: yi2038@nyu.edu.