IRSTI 10.77.35
UDK 343.2.7
JELK14

https://doi.org/10.46914/2959-4197-2026-1-2-247-257

ISSAYEVA Zh.A.,*[1]
c.l.s., associate professor.
*e-mail: jannat1701@mail.ru
ORCID ID: 0000-0001-8191-0281
MUSSABEKOVA I.T.,[2]
c.l.s., associate professor.
e-mail: i.musabekova@turan-edu.kz
ORCID ID:0009-0000-6162-2207
KARZHAUBAYEVA L.M.,[1]
c.l.s., senior lecturer.
e-mail: lyazzat_karzh@mail.ru
ORCID ID: 0000-0001-5936-0295
SANIYAZOVA E.K.,[1]
master of law, senior lecturer.
e-mail: erkem_84@mail.ru
ORCID ID: 0000-0001-9714-8631
[1]Korkyt Ata Kyzylorda University,
Kyzylorda, Kazakhstan
[2]Turan University,
Almaty, Kazakhstan

PHISHING IN THE CRIMINAL LAW OF THE REPUBLIC OF KAZAKHSTAN: LEGISLATIVE GAPS AND LAW ENFORCEMENT CHALLENGES

Abstract

With rapid digital change, phishing has become one of the most common forms of cyber fraud. This article explores challenges in its criminal law qualification in Kazakhstan, pointing out legislative gaps that complicate accurate assessment of acts committed through information technologies. In practice, such actions fall under different Criminal Code articles, reducing consistency and preventive effectiveness. Case analysis highlights difficulties in distinguishing criminal elements and proving intent when electronic resources are the main tool. Comparison with foreign practice shows that many countries already treat phishing as an independent crime, enabling clearer classification and earlier intervention. The study applies formal legal analysis, comparative research, and review of judicial practice. This methodology helps identify core problems and supports practical recommendations. The authors argue for amendments to the Criminal Code of Kazakhstan, including explicit recognition of phishing as network fraud with a clear definition of its features. Implementing these proposals would unify enforcement, improve judicial predictability, and strengthen protection of citizens in the digital environment. The findings hold theoretical and practical significance, advancing criminal law theory and supporting effective measures against cybercrime.

Keywords: phishing, computer fraud, fraud, cybercrimes, computer crime, unauthorized access, information security.

Introduction

The rapid evolution of information and communication technologies, together with the pervasive expansion of the internet, has fundamentally restructured social, economic, and legal frameworks within Kazakhstan. These advancements boosted the rise of digital criminality, a phenomenon characterized by its fluid dynamics and transnational reach. Offences committed in the virtual domain affect not only individuals but also public institutions, while the scale of potential harm may extend to the security of thousands of users.

As outlined in the Concept for Promoting the Ideology of Law and Order for 2025–2030, digital and telephonic fraud have emerged as the most prevalent categories of criminal activity. This trend is corroborated by 2024 statistics, which show that 22,870 online fraud cases were recorded, resulting in aggregate losses of 11.4 billion KZT. A critical observation in these figures is that 81.8% of these investigations were closed during the pre-trial stage. The distribution of these offenses involves 6,500 cases of illicit data access, 5,500 instances of fraudulent e-commerce transactions, and 3,900 further incidents classified as various forms of deception [1]. Although statistical data from 2024–2025 showed the rapid growth of online fraud, by 2026 the problem went beyond simple quantitative increase. Current trends indicate the complication of schemes, especially with the use of artificial intelligence, as well as the persistent difficulties of legal qualification and investigation. These changes indicate that traditional methods of detection and suppression are becoming insufficient, and the legislative framework is updated more slowly than criminal practice develops. As a result, online fraud has turned from a rare phenomenon into a stable element of the crime structure, which is confirmed both by national statistics and by international observations. Thus, online fraud has become a stable element of modern crime, and its dynamics require analysis not only of quantitative indicators but also of qualitative characteristics reflecting new forms of deception and their impact on law enforcement practice.

Phishing deserves particular attention as one of the most common manifestations of cyber fraud, relying on deception to unlawfully obtain access to confidential information. The large-scale spread of such schemes underscores the inadequacy of traditional approaches to criminal legal classification. As digital technologies advance, it becomes urgent to re-evaluate criminal legislation and identify new mechanisms for citizen protection.

Despite its pervasiveness, the criminal legislation of the Republic of Kazakhstan lacks a specific legal provision addressing phishing. This legislative gap complicates its legal classification and creates legal inconsistencies. Conversely, several international jurisdictions have already integrated statutes that account for the specific digital nuances of phishing. Analyzing these international approaches can reveal promising directions for modernizing Kazakhstan's legal framework.

This research aims to provide a comprehensive evaluation of the complexities surrounding the legal classification of phishing and to formulate actionable proposals for reform. To fulfill this objective, the study examines the current criminal legislation, analyses judicial practice in the Republic of Kazakhstan, and compares it with relevant foreign experience.

Materials and methods

The study's materials include normative legal acts of the Republic of Kazakhstan, doctrinal sources, and enforcement practice pertaining to the qualification of fraud involving information technologies, and law enforcement records concerning the classification of information technology-enabled fraud. The normative foundation rests primarily on provisions of the Criminal Code of the Republic of Kazakhstan, notably subparagraph 4 of part 2 of Article 190, which imposes liability for fraud committed through deception or abuse of trust by users of information systems or the Internet network and Article 205, which governs unauthorized access to information.

To ensure a rigorous conceptual understanding and a standardized application of these provisions, the study references Regulatory Resolution No. 6 of the Supreme Court of the Republic of Kazakhstan, dated June 29, 2017 (as amended on December 22, 2022). This resolution offers critical clarifications regarding the necessity of specifying the method of deception within indictments and verdicts. It further explains the criteria for determining when fraud against information system users is considered completed and provides guidance on the cumulative classification of offenses when actions involve unauthorized system access or computer data interference, factors of immediate relevance to phishing and subsequent unauthorized account access.

Given that digital fraud often involves overlapping elements of unauthorized access and resource interference, this study also integrates provisions of the Criminal Code pertaining to cyber-dependent crimes and judicial approaches to their concurrent application with Article 190. This facilitates an analysis of the boundary between user deception and the specific elements of illegal access or

interference, frequently associated with Article 205, which remains a recurring challenge in judicial practice [2].

The doctrinal framework consists of academic literature and analytical reports focused on the classification of system-based fraud and prevalent enforcement issues in internet-related cases. These sources explain the inconsistencies in the legal assessment of digital schemes, particularly where perpetrators influence victims through fraudulent advertisements, spoofed websites, messaging platforms, or other digital deception channels.

International cybersecurity materials are used to refine the conceptualization of phishing as a criminal modality. These resources characterize phishing as a form of social engineering designed to extract credentials, such as logins, passwords, and other access data, by impersonating trusted entities or services. Such materials support the argument that phishing frequently serves as a distinct, preliminary stage of a criminal attack that precedes the actual misappropriation of funds.

From a comparative legal perspective, this study examines international trends toward specialized phishing regulation. Particular attention is paid to approaches that criminalize the act of inducing users to disclose identification data by impersonating legitimate organizations. These frameworks reinforce the proposition that designating phishing as a standalone offense within the criminal law is a necessary step. The research uses general scientific and specialized legal methods. Juridico-dogmatic analysis was applied to analyze criminal norms and Supreme Court clarifications, isolating the elements of the composition under subparagraph 4 of part 2 of Article 190 of Criminal Code of the Republic of Kazakhstan, defining its scope, and relating it to offense qualifications.

Practice analysis method was employed to detect systemic errors and contentious scenarios. This involved examining characteristic patterns of internet fraud and phishing, the evidentiary requirements for proving deception, the timing of the crime's completion, and the causal link between deception and material loss. It also addressed the necessity of cumulative qualification under statutes governing unauthorized access or computer data interference, specifically in the context of Articles 205 and 206 of the Criminal Code [2].

The comparative-legal method facilitated a contrast between the domestic classification of phishing-related acts and international models that focus on «data elicitation» as a distinct, socially dangerous act. This comparison provided the necessary arguments for refining the criminal law regulation of phishing and resolving the ambiguity between fraud and cyber-specific offenses.

Integration of these materials and methods enabled a holistic examination of qualification issues under subparagraph 4 of part 2 of Article 190 Criminal Code of the Republic of Kazakhstan. It identifies the obstacles in current law enforcement regarding phishing schemes and justifies the introduction of a dedicated criminal provision that accounts for the intersection of phishing with subsequent unauthorized access and other digital manipulations.

Results and discussion

The designation phishing, derived from the English word for fishing, refers to a specific modality of cybercrime where fraudsters trick individuals via fake digital interfaces or messages to reveal sensitive details like passwords, bank credentials, or personal records, which they then exploit for profit. Victims carry out the key actions themselves, unaware of the illegality. The success of these schemes relies heavily on psychological manipulation designed to exploit user trust and direct their behavior.

Currently, three primary forms of phishing are identified:

1. Email phishing occurs when a target receives an electronic message requesting the disclosure of personal information.

2. Online phishing involves the development of fraudulent websites that mimic legitimate services through the use of deceptive domain names and layout designs.

3. Combined phishing utilizes various communication channels, such as social media or messaging platforms, to distribute links leading to counterfeit websites.

Phishing is increasingly recognized as a multifaceted issue that functions as both a method of deception and a means of unauthorized data access.

Evidence from domestic and international research suggests that the absence of a specific phishing statute in the Criminal Code of Kazakhstan creates legal friction and undermines efforts to combat cyber-enabled crimes [2]. The issue of the qualification of digital crimes is being raised in scientificdiscussions. Kazakhstani authors frequently highlight the ambiguity of legal assessments as a primary obstacle in digital crime prosecution. This assessment is echoed by Shcherbakov and Balasyan, who stress the need to revisit criminallaw criteria for ITrelated offences considering ongoing digitalization [3]. The authors note the existence of additional difficulties in determining the objective side of cybercrimes. The use of remote access, automated software tools, malicious software, and anonymizing technologies complicates the establishment of the method of committing the act and the identification of the causal link between the action and the resulting consequences. As a result, in law enforcement practice errors often occur: either qualifying features are unjustifiably attributed, or, conversely, they remain disregarded.

According to O. Safonova, social engineering tactics in the digital sphere, such as phishing, merge deceptive psychological influence with technical execution. Consequently, the existing criminal law framework necessitates refinement to better address the unique complexities of these offenses [4]. Her position reflects a widely shared view in the academic literature that social engineering constitutes a special form of crime, where psychological and technical elements are closely intertwined.

K. Alseitov reaches a similar conclusion, arguing that the rapid evolution of digital fraud highlights systemic gaps in current legislation. He contends that the existing regulatory framework must be expanded to ensure a more precise legal classification of these offenses [5].

According to the researchers, the use of Article190 «Fraud» and Article 205«Unlawful access to computer information» of the Criminal Code of the Republic of Kazakhstan [2] to qualify for phishing does not reflect the specifics and is thereforeconsideredincorrect.

In numerous international jurisdictions, phishing is categorized not merely as a subset of fraud but as a distinct form of cybercrime. For instance, in Australia, phishingrelated conduct is addressed under federal criminal legislation. Part 10.7 of the Criminal Code Act 1995 (Cth) criminalizes various forms of deception involving digital technologies, including conduct that resembles phishing schemes, while certain computerenabled offences under this part carry penalties of up to ten years' imprisonment [6].

In Canada, phishing falls under Article 380(1) of the Criminal Code as aggravated fraud [7] and is subject to anti-spam legislation (CASL) [8].

Article 380(1) covers fraudulent acts committed through deceit or falsehood and establishes liability for depriving a person of property, money, or services. Thus, phishing is classified as a type of fraud subject to criminal prosecution.

The Anti-Spam Legislation (CASL), adopted in 2014, complements criminal regulation by addressing digital threats such as spam, phishing, malware distribution, and unauthorized collection of personal data. CASL requires organizations to obtain consent before sending commercial electronic messages, thereby protecting consumer rights, reducing the prevalence of spam, and strengthening trust in the digital environment. Since its introduction, the law has contributed to a decline in spam originating from Canada, improved discipline in electronic marketing practices, and reinforced international cooperation in combating cybercrime.

According to Section 202a of the German Criminal Code, phishing in itself isn't a punishable offense. While there's debate over whether phishing data falls under this section, no criminal liability arises because there's no protected access. The victim, even if deceived, hands over the data willingly. A perpetrator can't legally exploit a leaked email address, but if the list is publicly available or shared openly, this section doesn't apply due to the lack of any access safeguards. That said, using phishing data for unauthorized acts like online banking fraud can still trigger liability [9].

Specific American states, most notably California, have enacted specialized legislation to combat phishing directly. These laws recognize it as an autonomous form of digital deception that differs fundamentally from traditional fraudulent schemes [10].

Furthermore, Egypt's Law No. 175 of 2018 regulates information technology crimes [11], determining penalties of up to five years in prison or significant financial fines, whereas in Ghana, the Cybersecurity Act classifies such actions as serious felonies, punishable by up to 25 years of imprisonment [12].

Singapore uses a hybrid model of criminal prosecution and proactive prevention. The state established the Anti-Scam Command [13] and passed the Protection from Online Falsehoods and Manipulation Act. Furthermore, a mandatory SMS Sender ID Registry was introduced to block mass fraudulent transmissions before they reach the user.

In Russian legal practice, phishing is typically prosecuted under general statutes concerning fraud and unauthorized computer access [14]. However, judicial authorities often face difficulties in qualifying such acts, since traditional provisions do not fully reflect the digital specificity of the crime. In academic literature, there is growing advocacy for establishing phishing as a dedicated offense that would account for its mass nature, reliance on electronic communications, and crossborder dimension. Comparative analysis of foreign experience (for example, Canada and Singapore) further confirms the relevance of developing special provisions in Russian criminal law.

A Council of Europe review notes widespread legislative updates addressing risks from psychological tactics to critical infrastructure assaults [15], reflecting a global pivot toward integrated legal-technical strategies.

Consequently, comparative analysis demonstrates that isolating phishing as a specific criminal category enables more effective prosecution and encourages the development of preventative measures, such as technical filters and user education.

Within the CIS region, Kazakhstan has taken initial steps toward addressing these threats. In 2025, Article 232-1 was introduced to the Criminal Code to target «dropper» activities. While significant, this measure is only a partial solution and does not address the specific nature of phishing as an independent violation. Effective regulation requires a dedicated article that penalizes the illicit acquisition of personal, financial, or protected data through deceptive electronic communications and spoofed resources. As phishing has become a standardized component of computer-mediated fraud, its legislative codification and the establishment of targeted sanctions are essential.

The challenge of accurate legal qualification remains a central issue for both Kazakhstani legal theory and international practice. Establishing a balance between punishment and prevention is difficult because the line between legitimate digital interaction and fraudulent intent is often blurred. This complexity is further reinforced by the increasing sophistication of attacks, particularly those involving artificial intelligence.

On top of that, data from a sociological survey reveals how the wide range of methods used in internet fraud complicates precise classification for investigators. The survey found that 68% of respondents, who currently work in investigative units in the Republic of Kazakhstan, reported struggles with pinning down the right category for cyber theft crimes [16].

Current difficulties in qualifying phishing stem not only from its ability to mimic authentic communication but also from the use of advanced technology. Artificial intelligence allows fraudstersto generate highly convincing website replicas, deploy automated bots, and even utilize deepfake voice technology, making the detection and legal processing of these crimes significantly more complex.

Phishing poses a severe risk to the integrity of sensitive data, including authentication credentials, financial records, and personal identifiers. The prevalence of these attacks is largely attributable to insufficient digital literacy among users and a general inability to distinguish fraudulent communications from legitimate resources.

In one representative case, District Court No. 2 of the Bukhar-Zhyrau District, Karagandy region, adjudicated the prosecution of Citizen B. In October 2025, the defendant posted fraudulent advertisements for saiga meat on WhatsApp, securing a 10,000 KZT advance payment via a third-party «Kaspi Bank» account without fulfilling the order. The court classified the offense as fraud committed by deceiving an information system user. Notably, the court declined to apply provisions regarding unauthorized access under Article 205 of the Criminal Code of the Republic of Kazakhstan. This judicial approach aligns with the prevailing practice of categorizing phishing-based scenarios under Article 190, the general fraud statute [17].

A significant example illustrating the complexities of classifying high-tech theft is the criminal case adjudicated by Court No. 2 of Ust-Kamenogorsk on May 14, 2024. The defendant, referred to as K., used a phishing link that carefully replicated the «OLX Delivery» interface to gain users' bank card details, including CVV codes, subsequently misappropriating funds from their accounts. Despite the clear digital nature of the crime, characterized using a fraudulent online service, the collection of

confidential data, and de facto unauthorized access, the court categorized the defendant's actions only as fraud under Article 190, Part 2, Paragraph 4 of the Criminal Code of the Republic of Kazakhstan. Article 205, governing «Unauthorized access to information», was not invoked in this instance.

The absence of a distinct legal assessment regarding the technological stage of the act, coupled with its classification strictly as fraud, effectively prevents the application of multiple criminal statutes. This judicial tendency leads to an underestimation of the inherent public danger posed by phishing attacks [18].

Similar issues are evident in a case adjudicated by Court No. 2 of Ust-Kamenogorsk on August 27, 2024. In this instance, the defendant, A.A.E., managed to impersonate a deputy akim (deputy head of the regional executive authority in Kazakhstan) by using mobile messaging applications to request purported "flood relief" donations from a private entrepreneur. By using the accounts of unsuspecting third parties, the defendant executed the entire scheme remotely through fraudulent digital identification. This scenario represents a classic phishing model: the perpetrator established a fraudulent digital identity, applied social engineering techniques, operated entirely online, and persuaded the victim to authorize a monetary transfer by exploiting the perceived credibility of an official state source. Nevertheless, the existing statutory framework requires such conduct to be prosecuted under the general fraud provisions of Article 190. This classification persists even though the technical components of the crime, specifically digital impersonation and the falsification of electronic contact, are inherently characteristic of phishing.

Such cases reveal a persistent regulatory gap. Current legislation does not provide a specific criminal provision targeting schemes in which the central element of wrongdoing consists of digital deception and the imitation of legitimate entities to prompt victim action through electronic communication channels. This legislative deficiency substantiates the need to introduce a distinct statutory offense of phishing into the Criminal Code of the Republic of Kazakhstan [19].

The central question remains whether fraud involving information systems is truly covered by paragraph 4, Part 2of Article 190of the Criminal Code of the Republic of Kazakhstan. While the 2017 Resolution of the Supreme Court of the Republic of Kazakhstan emphasizes the need to account for the unique characteristics of digital crime, current practice suggests otherwise [20]. Article 190, while referencing IT-enabled fraud, does not fully address the legal nuances of unauthorized access, particularly when information systems are breached without consent.

A key point to consider is that fundamental distinctions exist between Articles 190 and 205 of the Criminal Code of the Republic of Kazakhstan. The object of fraud is property or the right to property, whereas Article 205of the Criminal Code of the Republic of Kazakhstan protects information security and the integrity of data access regimes. Consequently, if an attacker gains access to data through deception but no material loss occurs, the elements of Article 190 of the Criminal Code of the Republic of Kazakhstan are not met. In contrast, the offense under Article 205 of the Criminal Code of the Republic of Kazakhstan is considered consummated the moment unauthorized access is achieved.

These distinctions are most visible during phishing attacks. If an attacker sends a fraudulent email containing a link to a fake banking site and the victim enters their credentials, the attacker has successfully accessed protected information. If the victim does not transfer money and no financial damage occurs, a fraud charge cannot be sustained. However, the act of unauthorized access has already occurred, constituting a crime under Article 205 of the Criminal Code of the Republic of Kazakhstan.

Additionally, it should be noted that such differentiation has important practical significance for law enforcement authorities. It enables them to respond to cyber threats at early stages, when no property consequences have yet occurred but information security has already been compromised. Thus, Article 205 of the Criminal Code of the Republic of Kazakhstan performs a preventive function, allowing intervention before material damage is inflicted. In academic literature, it is emphasized that this legal construction contributes to the development of a modern model of combating digital crimes, where the focus is placed not only on the protection of property rights but also on safeguarding the state's information infrastructure.

The authors conclude that limiting the legal classification to fraud alone leaves the preliminary stages of the crime unaddressed, missing opportunities for early intervention. This confirms the necessity for a clearer separation of criminal elements and a more precise legislative definition of crimes committed via information technology.

Conclusion

Within today's digital landscape, phishing endures as a prevalent and rapidly evolving cybercrime vector.Its persistence is rooted not only in the sophistication of technical exploits but also in the inherent vulnerability of the human element, making it a multilayered challenge.Even with the widespread adoption of advanced defenses such as email filtering, multi-factor authentication, and behavioral analytics, the risk remains substantial because the primary point of failure is often a lack of digital literacy among users.

Ourexamination of the criminal statutes in the Republic of Kazakhstan indicates that phishing has yet to be recognized as a standalone offense. Current judicial practice distributes these acts across various articles, leading to procedural confusion and a less effective response to digital threats. Considering the expansion of information-based crimes and their increasing technical complexity, this legislative gap has become a critical issue.

The findings of this research argue for a direct amendment to the Criminal Code of the Republic of Kazakhstan, such as the introduction of Article 190-1 of the Criminal Code of the Republic of Kazakhstan, to categorize phishing as a specific form of network fraud. Establishing a normative definition is essential to distinguish this crime from other breaches of information security. Such a refinement would standardize how the law is applied and offer stronger protection for citizens in the digital domains.

To implement a systemic approach against this threat, the following measures are proposed:

1. Introduce a dedicated legal definition of phishing as autonomous cyberfraud within the Law of the Republic of Kazakhstan «On Informatization» and the Criminal Code of the Republic of Kazakhstan. This would sharpen distinctions among cybercrime types.

2. Enact Article 191-1 (Phishing) into the Criminal Code of the Republic of Kazakhstan, establishing liability for the intentional creation, deployment, or dissemination of electronic messages, websites, software, interfaces, feedback forms, or other digital communication tools that imitate authentic resources or authorized entities, aimed at stealing funds, personal data, bank card details, identification credentials, or securing unauthorized information access.

Qualifying aggravators should encompass acts against two or more persons; via fake or anonym zed internet assets, including confusingly similar domain registrations; employing automated dispatch mechanisms (bot platforms, SIM boxes, or tools favored by criminal networks); or targeting critical information infrastructure or state systems Introducing a dedicated provision on phishing would improve the accuracy of criminal qualification and draw a clearer line between traditional fraud and cyber-related offences. Such an approach would reduce existing legal uncertainty, as phishing activities are currently assessed under several competing offence definitions, which delays investigations and leads to inconsistent judicial practice.

REFERENCES

1 Ещанов А.Ш. Профилактика мошенничества с использованием информационных систем. URL: https://infozakon.kz/life/26585-profilaktika-moshennichestva-s-ispolzovaniem-informacionnyh-istem.html (дата обращения: 11.02.2026)

2 Уголовный кодекс РК 3 июля 2014 года № 226-V URL: https://adilet.zan.kz/ rus /docs/K1400000226 (дата обращения: 11.02.2026)

3 Щербаков К.А., Баласян Г.В. Проблемы уголовно-правовой квалификации киберпреступлений в условиях цифровизации общества // Вестник науки. – 2025. – № 12(93). – Т. 4. – С. 428–443. URL: https://cyberleninka.ru/article/n/problemy-ugolovno-pravovoy-kvalifikatsii-kiberprestupleniy-v-usloviyah-tsifrovizatsii-obschestva (дата обращения: 11.02.2026)

4 Сафонова О.Н. Социальная инженерия и мошенничество в мессенджерах: правовые риски цифрового доверия. Международно-правовое регулирование. URL: https://kazlawreview.kz/soczialnaya-inzheneriya-i-moshennichestvo-v-messendzherah-pravovye-riski-czifrovogo-doveriya-mezhdunarodno-pravovoe-regulirovanie. (дата обращения: 11.02.2026)

5 Alseitov K. Cybercrime in the Republic of Kazakhstan: problems and solutions. 2020. URL: https://academy-rep.kz/uploads/821-47b224e40f0b736aa6296d9cae019f84.pdf. (дата обращения: 15.02.2026)

6 Criminal Code Act 1995 (Cth), Part 10.7 – Computer offences. URL: https://www.legislation.gov.au/C2004A04868/2025-01-09/2025-01-09/text/original/epub/OEBPS/document_1/document_1.html (accessed: 10.02.2026)

7 Canada. Department of Justice. Criminal Code (R.S.C., 1985, c. C-46). Section 380(1). Fraud URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/section-380.html (accessed: 10.02.2026)

8 Innovation, Science and Economic Development Canada (ISED). Canada's Anti-Spam Legislation (CASL). URL: https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en (accessed: 10.02.2026)

9 Streiber R., Pöhn D. Legal and ethical considerations when conducting phishing experiments in Germany // International Cybersecurity Law Review. 2025. Vol. 6. P. 239–251. DOI: 10.1365/s43439-025-00148-2. URL: https://doi.org/10.1365/s43439-025-00148-2 (accessed: 10.02.2026)

10 California Legislature. Business and Professions Code § 22948.2 (Anti-Phishing Act of 2005). URL: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22948.2 (accessed: 10.02.2026)

11 Egypt. Law No. 175 of 2018 on Anti Cyber and Information Technology Crimes. URL: https://www.wipo.int/wipolex/en/legislation/details/19959 (accessed: 10.02.2026)

12 Ghana. Cybersecurity Act, 2020 (Act 1038). URL: https://ghalii.org/akn/gh/act/2020/1038/eng@2020-12-29/source.pdf (accessed: 10.02.2026)

13 Ministry of Home Affairs Singapore. Remarks on Anti-Scam Command. URL: https://www.mha.gov.sg/mediaroom/speeches/transcript-of-remarks-by-mrs-josephine-teo-minister-for-communications-and-information-second-minister-for-home-affairs-session-1-of-the-global-fraud-summit/ (accessed: 10.02.2026)

14 Уголовный кодекс Российской Федерации (Федеральный закон № 63-ФЗ от 13 июня 1996 г., с изменениями и дополнениями). URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 07.02.2026)

15 Council of Europe. Cybercrime Convention Committee (T-CY): Assessments of legislation on cybercrime and electronic evidence (2024). URL: https://www.coe.int/en/web/cybercrime/t-cy (accessed: 10.02.2026)

16 Khamit E., Mukhamadieva G., Togaibaeva S., Mashabayev A., Salykova A., Karakushev S. Criminological Characterization of Internet Fraud: Experience of the Republic of Kazakhstan // Pakistan Journal of Criminology. 2024. Vol. 16. No. 4. P. 809–822. URL: https://www.pjcriminology.com/publications/criminological-characterization-of-internet-fraud-experience-of-the-republic-of-kazakhstan/ (accessed: 10.02.2026)

17 Бухар-Жырауский районный суд Карагандинской области. Приговор от 23 января 2026 года по делу № 3541-26-00-1/1 в отношении Бадельханье О. по ст. 190 ч. 2 п. 4 УК РК. Банк судебных актов Верховного Суда Республики Казахстан. URL: https://office.sud.kz (дата обращения: 11.02.2026)

18 Суд № 2 города Усть-Каменогорска Восточно-Казахстанской области. Приговор от 14 мая 2024 года по делу № 6310-24-00-1/245 в отношении Кузнецова А.В. по ст. 190 ч. 2 п. 4 УК РК. Банк судебных актов Верховного Суда Республики Казахстан. URL: https://office.sud.kz (дата обращения: 11.02.2026)

19 Суд № 2 города Усть-Каменогорска Восточно-Казахстанской области. Приговор от 27 августа 2024 года по делу № 1-353/2024 в отношении Абдрахманова А.Е. по ст. 190 ч. 4 п. 2 УК РК. Банк судебных актов Верховного Суда Республики Казахстан. URL: https://office.sud.kz/form/courtActs/lawsuitList.xhtml (дата обращения: 11.02.2026)

20 Нормативное постановление Верховного Суда Республики Казахстан № 6 от 29 июня 2017 года «О судебной практике по делам о мошенничестве». URL: https://adilet.zan.kz/rus/docs/P170000006S (дата обращения: 11.02.2026)

REFERENCES

1 Eshhanov A.Sh. Profilaktika moshennichestva s ispol'zovaniem informacionnyh sistem. URL: https://infozakon.kz/life/26585-profilaktika-moshennichestva-s-ispolzovaniem-informacionnyh-istem.html (data obrashhenija: 11.02.2026). (In Russian)

2 Ugolovnyj kodeks RK 3 ijulja 2014 goda No. 226-V URL: https://adilet.zan.kz/rus /docs/K1400000226 (data obrashhenija: 11.02.2026). (In Russian)

3 Shherbakov K.A., Balasjan G.V. (2025) Problemy ugolovno-pravovoj kvalifikacii kiberprestuplenij v uslovijah cifrovizacii obshhestva. // Vestnik nauki. No.12(93). V. 4. P. 428–443. URL: https://cyberleninka.ru/article/n/problemy-ugolovno-pravovoy-kvalifikatsii-kiberprestupleniy-v-usloviyah-tsifrovizatsii-obschestva (data obrashhenija: 11.02.2026). (In Russian)

4 Safonova O.N. Social'naja inzhenerija i moshennichestvo v messendzherah: pravovye riski cifrovogo doverija. URL: https://kazlawreview.kz/soczialnaya-inzheneriya-i-moshennichestvo-v-messendzherah-pravovye-riski-czifrovogo-doveriya-mezhdunarodno-pravovoe-regulirovanie (data obrashhenija: 11.02.2026) (In Russian)

5 Alseitov K. (2020) Cybercrime in the Republic of Kazakhstan: problems and solutions. URL: https://academy-rep.kz/uploads/821-47b224e40f0b736aa6296d9cae019f84.pdf (accessed: 15.02.2026) .(In English)

6 Criminal Code Act 1995 (Cth), Part 10.7 – Computer offences. URL: https://www.legislation.gov.au/C2004A04868/2025-01-09/2025-01-09/text/original/epub/OEBPS/document_1/document_1.html (accessed: 10.02.2026). (In English)

7 Canada. Department of Justice. Criminal Code (R.S.C., 1985, c. C-46). Section 380(1). Fraud. URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/section-380.html (accessed: 10.02.2026). (In English)

8 Innovation, Science and Economic Development Canada (ISED). Canada's Anti-Spam Legislation (CASL). URL: https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en (accessed: 10.02.2026). (In English)

9 Streiber R., Pöhn D. (2025) Legal and ethical considerations when conducting phishing experiments in Germany // International Cybersecurity Law Review. Vol. 6. P. 239–251. DOI: 10.1365/s43439-025-00148-2. URL: https://doi.org/10.1365/s43439-025-00148-2 (accessed: 10.02.2026). (In English)

10 California Legislature. Business and Professions Code § 22948.2 (Anti-Phishing Act of 2005). URL: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22948.2 (accessed: 10.02.2026). (In English)

11 Egypt. Law No. 175 of 2018 on Anti Cyber and Information Technology Crimes. URL: https://www.wipo.int/wipolex/en/legislation/details/19959 (accessed: 10.02.2026). (In English)

12 Ghana. Cybersecurity Act, 2020 (Act 1038). URL: https://ghalii.org/akn/gh/act/2020/1038/eng@2020-12-29/source.pdf (accessed: 10.02.2026). (In English)

13 Ministry of Home Affairs Singapore. Remarks on Anti-Scam Command. URL: https://www.mha.gov.sg/mediaroom/speeches/transcript-of-remarks-by-mrs-josephine-teo-minister-for-communications-and-information-second-minister-for-home-affairs-session-1-of-the-global-fraud-summit/ (accessed: 10.02.2026). (In English)

14 Ugolovnyj kodeks Rossijskoj Federacii (1996) Federal'nyj zakon No. 63-FZ ot 13 ijunja 1996 goda (s izmenenijami i dopolnenijami). URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (data obrashhenija: 07.02.2026). (In Russian)

15 Council of Europe. Cybercrime Convention Committee (T-CY): Assessments of legislation on cybercrime and electronic evidence (2024). URL: https://www.coe.int/en/web/cybercrime/t-cy (accessed: 10.02.2026) (In English)

16 Khamit E., Mukhamadieva G., Togaibaeva S., Mashabayev A., Salykova A., Karakushev S. (2024) Criminological Characterization of Internet Fraud: Experience of the Republic of Kazakhstan // Pakistan Journal of Criminology. Vol. 16(4). P. 809–822. URL: https://www.pjcriminology.com/publications/criminological-characterization-of-internet-fraud-experience-of-the-republic-of-kazakhstan/ (accessed: 10.02.2026) (In English)

17 Buhar-Zhyrauskij rajonnyj sud Karagandinskoj oblasti. Prigovor ot 23 janvarja 2026 goda po delu No. 3541-26-00-1/1 v otnoshenii Badel'han'e O. po st. 190 ch. 2 p. 4 UK RK. Bank sudebnyh aktov Verhovnogo Suda Respubliki Kazahstan. URL: https://office.sud.kz (data obrashhenija: 11.02.2026). (In Russian)

18 Sud No. 2 goroda Ust'-Kamenogorska Vostochno-Kazahstanskoj oblasti. Prigovor ot 14 maja 2024 goda po delu No. 6310-24-00-1/245 v otnoshenii Kuznecova A.V. po st. 190 ch. 2 p. 4 UK RK. Bank sudebnyh aktov Verhovnogo Suda RK. URL: https://office.sud.kz (data obrashhenija: 11.02.2026). (In Russian)

19 Sud No. 2 goroda Ust'-Kamenogorska Vostochno-Kazahstanskoj oblasti. Prigovor ot 27 avgusta 2024 goda po delu No. 1-353/2024 v otnoshenii Abdrahmanova A.E. po st. 190 ch. 4 p. 2 UK RK. Bank sudebnyh aktov Verhovnogo Suda RK. URL: https://office.sud.kz/form/courtActs/lawsuitList.xhtml (data obrashhenija: 11.02.2026). (In Russian)

20 Normativnoe postanovlenie Verhovnogo Suda Respubliki Kazakhstan No. 6 ot 29 ijunja 2017 goda «O sudebnoj praktike po delam o moshennichestve». URL: https://adilet.zan.kz/rus/docs/P170000006S (data obrashhenija: 11.02.2026). (In Russian)

ИСАЕВА Ж.А.,*[1]
з.ғ.к., қауымдастырылған профессор.
*e-mail: jannat1701@mail.ru
ORCID ID: 0000-0001-8191-0281
МУСАБЕКОВА И.Т.,[2]
з.ғ.к., қауымдастырылған профессор.
e-mail: i.musabekova@turan-edu.kz
ORCID ID: 0009-0000-6162-2207
КАРЖАУБАЕВА Л.М.,[1]
з.ғ.к, аға оқытушы.
e-mail: lyazzat_karzh@mail.ru
ORCID ID:0000-0001-5936-0295
САНИЯЗОВА Е.К.,[1]
з.ғ.м., аға оқытушы.
e-mail: erkem_84@mail.ru
ORCID ID: 0000-0001-9714-8631
[1]Қорқыт Ата атындағы
Қызылорда университеті,
Қызылорда қ., Қазақстан
[2]«Тұран» университеті,
Алматы қ., Қазақстан

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚЫЛМЫСТЫҚ ҚҰҚЫҒЫНДАҒЫ ФИШИНГ: ЗАҢНАМАЛЫҚ ОЛҚЫЛЫҚТАР ЖӘНЕ ҚҰҚЫҚ ҚОЛДАНУДАҒЫ ҚИЫНДЫҚТАР

Аңдатпа

Қоғамның қарқынды цифрлық трансформациясы жағдайында фишинг киберқылмыстың ең кең тараған түрлерінің бірі болып отыр. Мақалада оның Қазақстандағы қылмыстық-құқықтық саралану мәселелері қарастырылып, ақпараттық технологияларды пайдалана отырып жасалған әрекеттерді дәл бағалауға кедергі келтіретін заңнамалық олқылықтар анықталады. Іс жүзінде мұндай әрекеттер Қылмыстық кодекстің әртүрлі баптары бойынша сараланады, бұл қылмыстардың алдын алу тиімділігін төмендетеді. Сот істерін талдау электрондық ресурстар негізгі құрал болған кезде қылмыс құрамдарын ажырату және қасақана ниетті анықтау қиындықтарын көрсетеді. Шетелдік тәжірибемен салыстыру көптеген елдерде фишингтің дербес қылмыс ретінде танылғанын көрсетеді, бұл әрекеттерді дәлірек саралауға және ерте араласуға мүмкіндік береді. Зерттеудің әдіснамасы формалды-құқықтық талдауды, салыстырмалы-құқықтық зерттеуді және сот тәжірибесін зерделеуді қамтиды. Мұндай тәсіл негізгі проблемаларды анықтауға және практикалық шешімдер ұсынуға көмектеседі. Авторлар Қазақстан Республикасының Қылмыстық кодексіне өзгерістер енгізу қажеттілігін негіздейді, оған фишингті желілік алаяқтықтың бір түрі ретінде нақты нормативтік анықтамасымен бірге тікелей бекіту кіреді. Бұл ұсыныстарды іске асыру құқық қолдануды біріздендіреді, сот шешімдерінің болжамдылығын арттырады және азаматтарды цифрлық ортада қорғауды күшейтеді. Нәтижелер теориялық және практикалық маңызға ие болып, қылмыстық құқық теориясының дамуына және киберқылмысқа қарсы тиімді шараларды қалыптастыруға ықпал етеді.

Тірек сөздер: фишинг, компьютерлік алаяқтық, алаяқтық, киберқылмыстар, компьютерлік қылмыстылық, ақпараттық жүйеге заңсыз қол жеткізу, ақпараттық қауіпсіздік.

ИСАЕВА Ж.А.,*[1]
к.ю.н., ассоциированный профессор.
*e-mail: jannat1701@mail.ru
ORCID ID: 0000-0001-8191-0281
МУСАБЕКОВА И.Т.,[2]
к.ю.н., ассоциированный профессор.
e-mail: i.musabekova@turan-edu.kz
ORCID ID: 0009-0000-6162-2207
КАРЖАУБАЕВА Л.М.,[1]
к.ю.н., ст. преподаватель.
e-mail: lyazzat_karzh@mail.ru
ORCID ID:0000-0001-5936-0295
САНИЯЗОВА Е.К.,[1]
з.ғ.м., ст. преподаватель.
e-mail: erkem_84@mail.ru
ORCID ID: 0000-0001-9714-8631
[1]Кызылординский университет
им. Коркыт Ата,
г. Кызылорда, Казахстан
[2]Университет «Туран»,
г. Алматы, Казахстан

ФИШИНГ В УГОЛОВНОМ ПРАВЕ РЕСПУБЛИКИ КАЗАХСТАН: НЕСОВЕРШЕНСТВО ЗАКОНОДАТЕЛЬНЫХ КОНСТРУКЦИЙ И ТРУДНОСТИ ПРАВОПРИМЕНЕНИЯ

Аннотация

В условиях стремительной цифровой трансформации фишинг стал одной из наиболее распространенных форм кибермошенничества. В статье рассматриваются проблемы его уголовно-правовой квалификации в Казахстане, выявляются пробелы законодательства, затрудняющие точную оценку деяний, совершаемых с использованием информационных технологий. На практике такие действия квалифицируются по разным статьям Уголовного кодекса, что снижает эффективность предупреждения преступлений. Анализ судебных дел показывает трудности в разграничении составов и установлении умысла, когда основным инструментом выступают электронные ресурсы. Сравнение с зарубежным опытом демонстрирует, что во многих странах фишинг уже признан самостоятельным преступлением, что позволяет точнее квалифицировать действия и вмешиваться на ранних стадиях. Методология исследования сочетает формально-правовой анализ, сравнительно-правовое исследование и изучение судебной практики. Такой подход помогает выявить ключевые проблемы и предложить практические решения. Авторы обосновывают необходимость внесения изменений в Уголовный кодекс Казахстана, включая прямое закрепление фишинга как формы сетевого мошенничества с четким нормативным определением его признаков. Реализация этих предложений обеспечит единообразие правоприменения, повысит предсказуемость судебных решений и усилит защиту граждан в цифровой среде. Результаты имеют как теоретическую, так и практическую значимость, способствуя развитию уголовно-правовой теории и формированию эффективных мер противодействия киберпреступности.

Ключевые слова: злоупотребление доверием, компьютерное мошенничество, мошенничество, киберпреступления, фишинг, компьютерная преступность, судебная практика.

Article submission date: 08.04.2026