

A. N. Nartai ¹, Ye. S. Shalkharov ¹, A. U. Mansurov ^{1*}, O. B. Dosekeev ¹¹Khoja Akhmet Yassawi International Kazakh-Turkish University,
Turkistan, Republic of Kazakhstan*E-mail: mansa_911@mail.ru**A NEW FORM OF ORGANIZED CRIME: CHALLENGES OF COUNTERACTING
SHADOW GENOMIC LABORATORIES SPREAD THROUGH VIRTUAL COMMUNICATION
CHANNELS****Abstract**

This article examines the phenomenon of shadow genomic laboratories as an emerging form of organized crime developing at the intersection of biotechnology, digital communications, and criminal network practices. The relevance of the study is determined by the transformation of the criminal environment, in which illegal operations involving genetic information and biotechnological resources are increasingly disseminated through virtual communication channels, significantly complicating their detection, legal classification, and suppression. The aim of the study is to identify institutional and legal gaps in the system for countering shadow genomic laboratories and to develop an interdisciplinary model of state response to biodigital crime. The methodological framework comprises content analysis of scientific literature, comparative legal analysis of international practices, an online survey, and structural modeling. The findings demonstrate that in Kazakhstan, this emerging threat is characterized by potentially high levels of latency, insufficient interagency coordination, and regulatory uncertainty concerning new biodigital risks. A national counteraction model is proposed, incorporating six interconnected stages of institutional response: monitoring, detection, risk assessment, interagency coordination, legal suppression, and follow-up control. The model is supplemented by proposals to improve the regulatory framework, strengthen digital monitoring mechanisms, and enhance cooperation among government authorities, research institutions, and law enforcement agencies. The practical significance of the study lies in the potential application of the proposed approaches to developing a national system for preventing and suppressing emerging forms of organized crime associated with the illicit use of genomic and digital technologies.

Key words: organized crime, synthetic biology, bio-digital security, genetic data, digital criminology, law and biotechnology, shadow laboratories.

Introduction

The convergence of biotechnology, digital communication, and organized crime has created a new field of legal and security risk. This article examines shadow genomic laboratories as hybrid bio-digital structures that may combine unauthorized genomic activity, illicit data exchange, and encrypted coordination outside formal oversight.

The importance of this study lies in its focus on the expanding nexus between unregulated genomic research and transnational organized crime. Shadow genomic laboratories, operating outside formal regulatory frameworks, exploit legislative gaps. Critical issues include inadequate legal protection of genetic data, weak controls over the international movement of biological materials, and the absence of clear mechanisms to address biotechnological crimes enabled by virtual infrastructures. These shortcomings underscore the urgent need for a coordinated and enforceable legal framework.

This study explores shadow genomic laboratories that operate via virtual communication platforms, framing them within the context of organized crime theory. It also examines the legal, technological, and institutional factors that shape responses to this evolving threat.

The study pursues four core aims:

1. To analyze how virtual communication technologies enable the functioning of organized criminal networks;
2. To examine the structural design and operational practices of illicit genomic laboratories;
3. To assess the effectiveness of existing legal frameworks and regulatory mechanisms at national and international scales;
4. To develop informed legal and policy proposals for preventing and dismantling these emerging biocriminal infrastructures.

The article's contribution is to interpret shadow genomic laboratories as organized bio-digital crime rather than as isolated breaches of scientific regulation.

The study argues that, without targeted legal and technological responses, shadow genomic laboratories may become stable elements of criminal ecosystems and create long-term risks for global biosecurity. Its main contribution is the reinterpretation of these entities as organized, digitally supported structures rather than isolated violations of scientific regulation. This approach also helps identify practical measures for policymakers, law enforcement bodies, and cybercrime specialists.

The problem is intensified by weak international coordination, insufficient control over digital communication platforms, and inadequate protection of scientific and genetic data. These gaps limit the ability of states to respond effectively to emerging biocriminal threats.

Recent research on synthetic biology, genomics, and cybersecurity addresses biosecurity risks, genetic data protection, and the role of digital infrastructure in criminal activity. However, these studies often examine the issues separately. The present article connects them within a single interdisciplinary framework focused on shadow genomic laboratories as a new form of virtual organized genomic crime.

Existing scholarship addresses related aspects of synthetic genomics, genetic data protection, cyberbiosecurity, encrypted communication, and darknet markets, but it rarely examines these issues as a single criminological problem. Hoffmann et al. (2023) emphasize the principle of “safety by design” in synthetic genomics, while Millett (2020) discusses biosecurity risks linked to commercialization and the need to balance regulation with scientific freedom [1],[2]. However, these works do not analyze how organized criminal structures may exploit synthetic biology.

Studies by Liu et al. (2024), Tuazon et al. (2024), and Jurczyk et al. (2020) focus on genetic data security, DNA-based encryption, forensic genealogy, and the absence of unified international standards [3], [4]. These contributions are important for understanding data protection risks, yet they do not explain illicit acquisition of genetic data or the organization of shadow genomic laboratories.

Research by Son (2022) and Sarhan (2023) examines encrypted messengers from a forensic perspective, while Afzal (2021) analyze darknet markets and their links to organized crime [5],[6],[7]. These studies clarify the digital infrastructure of illegal activity, but they do not address the biotechnological dimension of genomic crime.

Reedy (2023) reviews Interpol's work on digital evidence, and Thomas (2024), Brown and Kayser (2024), and Brown, Kayser (2024) discuss confidentiality, law enforcement access, and genomic data governance [8], [9], [10].

Thus, the literature covers separate issues of biosecurity, cybersecurity, genetic data protection, and digital evidence. It does not fully explain shadow genomic laboratories as organized criminal systems, nor does it examine their use of encrypted platforms, darknet forums, cloud services, and resistance to legal or technical control. The novelty of this study lies in addressing these gaps through the concept of virtual organized genomic crime. The research examines shadow genomic laboratories from an interdisciplinary perspective and proposes legal, technological, and organizational mechanisms for countering them.

Materials and methods of research

The study used an interdisciplinary design combining criminology, comparative legal analysis, cybercrime studies, and biosecurity assessment. This design was selected because shadow genomic laboratories operate at the intersection of unlawful biotechnology, encrypted digital communication, genetic data misuse, and organized crime. The theoretical basis of the study included 10 peer-reviewed English-language sources published in 2020–2024 and indexed in Scopus or Web of Science. The sources were selected according to their relevance to synthetic biology, genetic data protection, encrypted communication, darknet markets, digital evidence, forensic genetics, and cyberbiosecurity. Empirical data were collected from June to August 2025 through standardized online questionnaires distributed via Google Forms and SurveyMonkey. The survey included 173 respondents from Kazakhstan, Russia, Germany, and the United States. The sample was purposive and not statistically representative; therefore, the findings are interpreted as professional and expert perceptions rather than as population-level results.

The respondent profile was sufficiently diverse for an exploratory study. Men accounted for 56.6% of the sample and women for 42.8%. By age, 21.4% of respondents were under 25, 31.2% were aged 26–35, 27.7% were aged 36–45, and 19.7% were over 45. The professional structure also reflected the research focus: 22.5% represented biotechnology and biomedicine, 16.2% information security, 13.9% law, 30.0% students and postgraduate trainees, 11.0% law enforcement and special services, and 6.4% other fields. The questionnaire measured four indicators: awareness of shadow genomic laboratories, perceived threat of bio-digital crime, trust in state regulation, and perceptions of encrypted platforms as tools for illicit coordination. Closed-ended questions were used for descriptive statistical analysis, while open-ended answers helped identify recurring concerns and expert interpretations.

The survey was supplemented by content analysis of more than 250 texts published in 2023–2025 on Telegram channels, darknet forums, and closed online discussion groups. The materials were selected when they contained direct or indirect references to genomic technologies, biohacking, genetic customization, illegal data exchange, laboratory services, or coded terminology linked to anonymous digital coordination.

A comparative legal review covered Kazakhstan, the European Union, and the United States. The analysis focused on biological safety regulation, genetic data protection, criminal liability, cybercrime investigation, and mechanisms for controlling synthetic biology risks. In Kazakhstan, special attention was given to the 2022 Law “On Biological Safety” and relevant provisions of the Criminal Code [11],[12].

Quantitative data were processed in Microsoft Excel and IBM SPSS Statistics 26.0 using descriptive statistics. Open-ended responses and digital materials were coded thematically in NVivo. The combined results were used to identify legal and institutional gaps and to develop the National Response Model to Bio-Digital Crime (NRMBDC). The main limitation of the study is the absence of officially confirmed cases of shadow genomic laboratories in Kazakhstan, which makes the research exploratory.

Results and their discussion

The analysis shows that Kazakhstan’s main vulnerabilities concern legal qualification, encrypted digital coordination, and limited expert capacity in bio-digital crime investigation.

Existing scholarship has begun to address these risks. Millett (2020) draws attention to security vulnerabilities in synthetic biology, while Hoffmann et al. (2023) propose the principle of “safety by design” for integrating biosecurity measures into synthetic genomics [1.—2]. However, these approaches mainly concern regulated research environments. They do not fully explain how unregistered genomic laboratories operate within decentralized digital spaces.

The commercialization of synthetic biology and the growing use of virtual platforms have intensified global biosecurity risks. According to the 2023 ISBMS report, unregulated biological laboratories have increased by 18–22% annually since 2020, with more than 2,400 documented cases worldwide by 2024. These figures indicate the rapid expansion of illicit genomic activity and confirm the need for stronger legal, technological, and institutional responses (Figure 1).

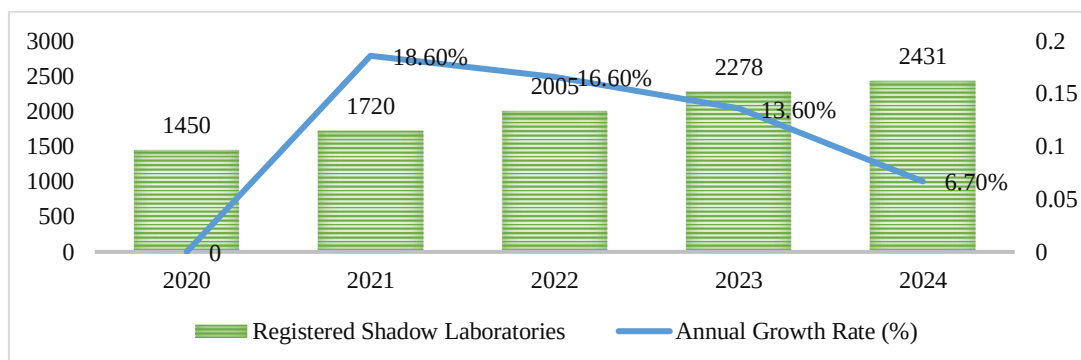


Figure 1 – Global Trends in the Identification of Shadow Genome Laboratories, 2020–2024

Note: Compiled by the authors

Figure 1 indicates an increase in identified shadow genome laboratories, although the slower growth rate may reflect more concealed operating models rather than reduced risk. International regulation of synthetic biology remains uneven: U.S. screening guidance for synthetic nucleic acid providers is still limited in scope, while EU rules focus mainly on data protection and do not fully address transnational bio-digital crime [13].

Kazakhstan regulates biological safety through the 2022 Law “On Biological Safety,” which focuses on epidemiological control, pathogenic agents, and authorized laboratory activity. It does not directly cover unauthorized genomic technologies, unregistered genetic laboratories, or biocriminal coordination through virtual platforms [11.-42].

The topic is also weakly represented in Kazakhstani scholarship. The authors’ review of 254 national publications from 2020–2024 found only two studies on genomic data security and bioethics, while none examined shadow laboratories. This confirms the novelty of the issue and the need for further legal and criminological research (Figure 2).

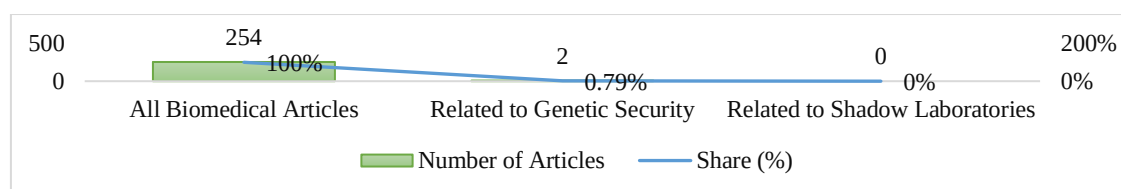


Figure 2 – Representation of Shadow Laboratories in Scientific Publications in Kazakhstan

Note: Compiled by the authors

The data show that shadow genome laboratories are almost absent from Kazakhstan’s scientific discourse. This indicates weak recognition of the threat and limited connection between research and public administration.

The educational gap is also evident. Among 23 biotechnology and medical programs at eight major universities, only five include biosecurity, usually in microbiological or epidemiological terms. Issues of genomic ethics, legal regulation, cybersecurity risks, and illegal genome laboratories are not covered.

At the same time, Kazakhstan’s rapid digitalization creates conditions for new forms of organized crime. Criminal networks are increasingly using encrypted platforms and anonymous digital channels to coordinate activities beyond national oversight. The convergence of cyber tools and illicit biotechnology is therefore becoming a serious biosecurity concern.

No officially confirmed shadow genome laboratories have yet been identified in Kazakhstan. However, the risk of their emergence is increasing due to the wide use of encrypted messengers and weak regulation of anonymous digital platforms. This requires a closer assessment of the country’s legal, technological, and institutional readiness.

Article 273 of the Criminal Code addresses biological weapon threats through media or telecommunication networks, but it does not clearly cover genome-level manipulation, genetic data misuse, or organized digital coordination [14].

Kazakhstan’s high digital connectivity amplifies the risk. By the end of 2024, internet access reached 91.7%. Telegram, WhatsApp, Instagram, and Signal are widely used, while the number of Telegram users grew from 3.9 million to 5.8 million between 2022 and 2024 (Figure 3).

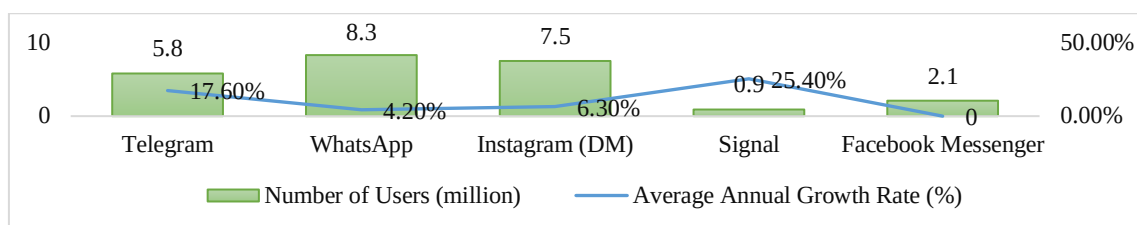


Figure 3 – Primary Digital Messaging and Communication Tools in Use Across Kazakhstan (2024)

Note: Compiled by the authors

Encrypted platforms such as Telegram and Signal provide privacy, limited traceability, and fragmented digital traces, which makes them attractive for illicit coordination. In Kazakhstan, oversight of such platforms remains focused mainly on phishing, financial fraud, extremism, darknet activity, cryptocurrency transactions, and other conventional cybercrimes. Biosecurity risks, including illegal circulation of genome-editing tools, genetic data, and related services, remain weakly covered [15].

This gap is reinforced by limited expert capacity. Genetic forensics and biotechnology require specialized knowledge, while many cybercrime units are not prepared to assess genomic materials or detect shadow genome laboratories. Institutional responsibility is also divided: sanitary-epidemiological authorities oversee biosafety, the Ministry of Digital Development manages cybersecurity policy, and the Ministry of Internal Affairs investigates cyber-enabled crimes. Stronger coordination is therefore needed where biological and digital risks overlap.

The study also assessed public and expert perceptions of shadow genome laboratories. Respondents evaluated the threat on a five-point Likert scale, from 1 — no threat to 5 — extreme threat. These data show how different professional and social groups perceive bio-digital vulnerability and institutional preparedness (Table 1).

Table 1. Assessment Results of the Threat Level of Biocrime

Perceived Threat Levels of Shadow Genome Laboratories	Number of Respondents	Share (%)
1 – No threat	6	3,4%
2 – Low threat	17	9,8%
3 – Moderate threat	38	22,0%
4 – High threat	59	34,1%
5 – Extremely high threat	53	30,6%
Note: Compiled by the authors		

A total of 64.7% of respondents rated biocrimes as a high or extremely high threat. This figure indicates that shadow laboratories are perceived by society as a significant danger and that a concrete response is expected from the state. During the survey, respondents were also asked how much they trust the legal and technical measures currently being implemented by the government. This serves as a key indicator of the level of institutional trust among the public and professionals (Table 2) [15—18], [16], [17].

Table 2. Level of Trust in State Regulation

Level of Trust	Number of Respondents	Share (%)
Fully trust	8	4,6%
Partially trust	43	24,9%
Do not trust	91	52,6%
Difficult to answer	31	17,9%
Note: Compiled by the authors		

The survey shows that 52.6% of respondents do not trust state mechanisms in the field of biosecurity. This indicates weak institutional confidence, limited public communication, and gaps in legal policy.

Open-ended responses from 85 participants were analyzed in NVivo. The most frequent concerns were lack of accessible information on clandestine laboratories, perceived state inaction, suspicion of illegal genetic experiments under medical cover, weak monitoring of Telegram and darknet channels, and insufficient coverage of synthetic biology risks in education.

These responses point to three main problems: low transparency, ineffective oversight, and the absence of a coordinated policy response. Age analysis also showed that older respondents perceived shadow genome laboratories as a more serious threat than younger participants. This may reflect greater professional experience, stronger risk awareness, or broader exposure to bioethical debates (Figure 4).

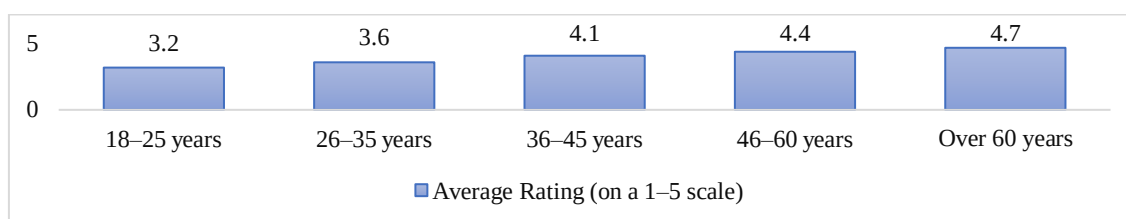


Figure 4 – Perceived Risk Level of Shadow Genome Laboratories by Age Group (Average Score)

Note: Compiled by the authors

The figure shows that perceived threat increases with age. Respondents aged 18–25 gave the lowest average score, 3.2, while those aged 60 and above gave the highest score, 4.7. This suggests a positive link between age and risk perception.

Older and mid-career respondents appear to assess shadow genome laboratories more seriously, likely due to professional experience, stronger exposure to biosecurity issues, or greater familiarity with institutional risk frameworks. However, overall awareness remains limited. Only 38% of participants reported clear knowledge of shadow genome laboratories, which is lower than in countries where biosecurity is more visible in policy and public debate, such as the United States, Germany, and Israel (Table 3) [15-16].

Table 3. Comparative Awareness of Shadow Genome Laboratories Across Selected Countries

Country	Year	Aware Respondents (%)	Source
USA	2021	57%	NAS Public Report

Country	Year	Aware Respondents (%)	Source
Israel	2022	64%	Biosecurity Survey
Germany	2023	48%	Federal Science Panel
China	2022	17%	CAS Biotech Risk Brief
Kazakhstan	2025	38%	Author's Empirical Study
Note: Data compiled by the authors			

Kazakhstan's awareness level (38%) exceeds that of China (17%) yet remains significantly lower than in countries with more advanced technological ecosystems. This disparity reflects persistent gaps in science education, public engagement, and the integration of biosecurity concerns into policy frameworks. A profession-based analysis reveals a distinct trend: experts in genomics and information technology tend to view shadow genome laboratories as a tangible threat. In contrast, respondents from the humanities are more likely to underestimate the severity of the issue (Figure 5).

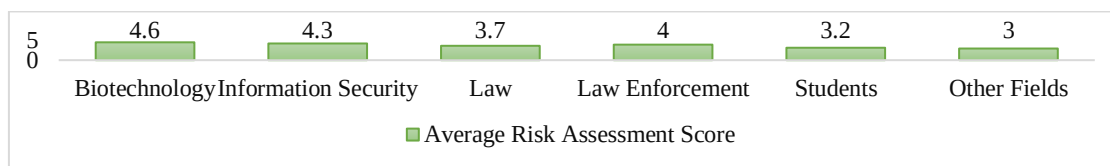


Figure 5 – Estimated risk of shadow genomic laboratories by professional sector (scale from 1 to 5 points)

Note: Compiled by the authors

Perceived risk varied by professional background. Biotechnology and information security respondents rated the threat highest, with average scores of 4.6 and 4.3, while students and non-technical respondents assessed it lower. This suggests that specialized knowledge increases awareness of genomic security risks [15.–17].

Shadow genomic laboratories therefore represent a hybrid risk combining biotechnology, cybersecurity, and criminal law. In Kazakhstan, this risk is intensified by legal gaps, weak technical capacity, and the absence of clear criminal qualification for offenses involving genetic data, synthetic DNA, CRISPR-related tools, and encrypted cross-border coordination.

Technical barriers further complicate investigation. Encrypted platforms, anonymity tools, limited metadata access, and fragmented digital traces make attribution difficult and weaken prosecution (Table 4).

Table 4. Comparative Analysis of Encryption Features in Telegram and Signal Messaging Platforms

Function	Telegram	Signal
End-to-end encryption	Only in “Secret Chat”	All chats
Metadata retention	Yes	No

Function	Telegram	Signal
Temporary message storage	Yes (with timer)	Yes (with timer)
Access to server data	No	No
Note: Compiled by the authors		

Encrypted platforms complicate investigation because lawful access to foreign-based services and metadata remains limited. This restricts the ability of Kazakhstani authorities to trace bio-digital offenses coordinated through secure networks.

Investigation of underground genome laboratories requires cooperation between law enforcement, cybersecurity units, biomedical researchers, genomic experts, lawyers, and bioethicists. At present, this coordination remains weak. Kazakhstan has more than 150 digital forensics experts, but only 12 genetic analysts and three biosecurity legal experts; cybergenetic analysts are effectively absent. This gap limits the investigation of crimes combining biotechnology, cybersecurity, and organized crime.

Public awareness also remains low. Shadow genome laboratories are often perceived as remote or hypothetical, which reduces social support for preventive measures [15.–17].

These limitations justify the National Response Model to Bio-Digital Crime (NRMBDC). The model strengthens detection, analysis, and response through three blocks: Early Warning, Identification and Analysis, and Legal Response and Adaptation (Table 5).

Table 5. Phased Structure of the National Response Model to Bio-Digital Crime (NRMBDC)

Phase Title	Content and Focus Areas	Responsible Structures
Phase I: Early Detection	Automated monitoring of suspicious activity in virtual space through algorithms and keyword tracking	Ministry of Digital Development, Cybersecurity Center
Phase II: Analytical Identification	Matching collected data with genomic/biotechnological content, formation of an expert database	National Center for Genetics, Research Institutes
Phase III: Legal Typology	Classification of activities under specific crimes: genome modification, unauthorized data distribution, etc.	Ministry of Internal Affairs, General Prosecutor's Office
Phase IV: Adaptive Legal Response	Introduction of specific legal provisions, amendments to the Criminal Code, and establishment of oversight mechanisms	Parliament of Kazakhstan, Ministry of Justice
Phase V: Multidisciplinary Taskforce	Integration of geneticists, IT specialists, legal experts, and ethicists into investigative and expert groups	Interagency Platform, Ministry of Internal Affairs
Phase VI: Education and Awareness	Development of training modules for students, doctors, and investigators; public awareness via media	Ministry of Education, Universities, Mass Media, NGOs
Note: Compiled by the authors		

The National Response Model to Bio-Digital Crime (NRMBDC) addresses four key weaknesses: legal gaps, institutional fragmentation, personnel shortages, and low public trust. Its implementation requires targeted amendments to the Law “On Biological Safety,” the Criminal Code, and national digital policy [11. —12].

The model may face institutional inertia, interagency competition, limited access to foreign digital platforms, and shortages of specialists in genetics, IT, and law. These risks are significant because 52.6% of respondents expressed mistrust toward existing state mechanisms, while Kazakhstan’s broader biosecurity capacity remains moderate at 46.1 out of 100 according to the Global Health Security Index [14. —16].

The NRMBDC is built around three blocks: Early Warning, Identification and Analysis, and Legal Response and Adaptation. This structure shifts the response from post-factum punishment to early detection, expert assessment, legal qualification, and prevention.

Legal reform should be based on precise criminal-law drafting rather than the mechanical addition of new offences. Proposed Articles 274-1, 274-2, and 274-3 may be retained. Still, their scope should be limited to clearly defined acts: unlawful use of genome-editing tools, illegal circulation of genetic data, and organized coordination of bio-digital criminal activity through virtual platforms. Each provision should specify the protected legal interest, the objective elements of the offence, the form of intent, qualifying circumstances, and proportional sanctions.

Comparative legal analysis is also needed before legislative adoption. Foreign approaches to synthetic biology, genetic data protection, cybercrime evidence, and DNA synthesis screening may serve as reference points. Still, they should be adapted to Kazakhstan’s legal system and investigative practice.

Institutional coordination and personnel training are essential for the NRMBDC. The proposed Interagency Coordination Center on Bio-Digital Threats should consolidate data, ensure rapid notification of genomic and biotechnological risks, support public monitoring, and coordinate international cooperation.

Kazakhstan also needs specialized profiles, including bio-digital investigators, cybergenetics experts, and bioethics legal specialists. Their training should combine genomics, digital forensics, law, biosecurity, and international bioethics standards [15.—20]. Education should also be updated, as only 19.2% of students reported awareness of underground genomic laboratories.

Overall, the study confirms that shadow genomic laboratories are a complex legal, institutional, and social threat. Traditional law enforcement tools are insufficient. Kazakhstan therefore needs an adaptive system for detecting, assessing, classifying, and preventing bio-digital crime.

Conclusion

The study confirms that shadow genomic laboratories represent a hybrid bio-digital threat combining biotechnology, encrypted communication, and weak legal qualification. For Kazakhstan, the key risks are legal uncertainty, fragmented institutional responsibility, limited expert capacity, and low trust in biosecurity measures.

The findings show that respondents recognize bio-criminal risks, while confidence in institutional response remains weak. This requires not only legal reform, but also public communication, professional training, and stronger biosecurity awareness.

The main outcome of the study is the National Response Model to Bio-Digital Crime (NRMBDC). It offers a cross-sectoral framework for legal modernization, institutional coordination, technological oversight, and early prevention.

The article contributes to Kazakhstan’s biosecurity discourse by linking criminal law, biotechnology, and cybersecurity within one analytical framework. Further development of the proposed amendments requires more precise criminal-law design and comparison with international regulatory models.

REFERENCES

- 1 Hoffmann S. A., Diggans J., Densmore D., Dai J., Knight T., Leproust E., Boeke J. D., Wheeler N., Cai Y. (2023) Safety by design: Biosafety and biosecurity in the age of synthetic genomics // iScience. Vol. 26. No. 3. P. 106165. DOI: [10.1016/j.isci.2023.106165](https://doi.org/10.1016/j.isci.2023.106165).
- 2 Millett P. (2020) The synthetic-biology challenges for biosecurity // Health Security. Vol. 18, Suppl. 1. P. 8–14. DOI: [10.1080/10736700.2020.1866884](https://doi.org/10.1080/10736700.2020.1866884).
- 3 Liu T., Wang Q., Yan Y., Chen Y., Du X., Zhang X. (2024) Advancements in DNA-based information security // Patterns. Vol. 5. No. 10. P. 101012. DOI: [10.1016/j.patter.2024.101012](https://doi.org/10.1016/j.patter.2024.101012).
- 4 Tuazon O. M., Wickenheiser R. A., Ansell R., Guerrini C. J., Zwenne G.-J., Custers B. (2024) Law enforcement use of genetic genealogy databases in criminal investigations: Nomenclature, definition and scope // Forensic Science International: Synergy. Vol. 8. P. 100460. DOI: [10.1016/j.fsisc.2024.100460](https://doi.org/10.1016/j.fsisc.2024.100460).
- 5 Son J., Kim Y. W., Oh D. B., Park J., Lee S., Kim K. (2022) Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema // Forensic Science International: Digital Investigation. Vol. 40. P. 301347. DOI: [10.1016/j.fsidi.2022.301347](https://doi.org/10.1016/j.fsidi.2022.301347).
- 6 Sarhan Q. U., Aleroud A., Alenezi M., Sleit A. (2023) A framework for digital forensics of encrypted real-time messaging // Ain Shams Engineering Journal. Vol. 14, No.1. P. 102069. DOI: [10.1016/j.asej.2022.102069](https://doi.org/10.1016/j.asej.2022.102069).
- 7 Afzal S., Mukhtar H., Farooq U., Shahzad F. (2021) A systematic literature review on darknet market analysis and detection techniques // Applied Sciences. Vol. 11. No. 17. P. 7789. DOI: [10.3390/app11177789](https://doi.org/10.3390/app11177789).
- 8 Reedy P. (2023) Interpol review of digital evidence for 2019.2022 // Forensic Science International: Synergy. Vol. 6. P. 100313. DOI: [10.1016/j.fsisc.2022.100313](https://doi.org/10.1016/j.fsisc.2022.100313).
- 9 Thomas M., Shah P., Vora J. (2024) Assessing privacy vulnerabilities in genetic data sets // JMIR Bioinformatics and Biotechnology. Vol. 5, No. 1. P. 54332. DOI: [10.2196/54332](https://doi.org/10.2196/54332).
- 10 Brown T., Kayser M. (2024) Forensic genetics in the shadows: Law enforcement access to clinical DNA // Journal of Law and the Biosciences. Vol. 11. No. 1. Article ID: Isae028. DOI: [10.1093/jlb/Isae028](https://doi.org/10.1093/jlb/Isae028).
- 11 Law of the Republic of Kazakhstan. (2022) On Biological Safety of the Republic of Kazakhstan: Law dated May 21, 2022 No. 122-VII LRK. Adilet Legal Information System. Available at: — URL: <https://adilet.zan.kz/eng/docs/Z2200000122> (accessed: 15.04.2026).
- 12 Penal Code of the Republic of Kazakhstan: Code dated July 3, 2014 No. 226.V // Adilet Legal Information System. 2014 Available at: — URL: <https://adilet.zan.kz/eng/docs/K1400000226> (accessed: 18.04.2026).
- 13 U.S. Department of Health and Human Services. Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids // Administration for Strategic Preparedness and Response. 2023. Available at: — URL: <https://aspr.hhs.gov/S3/Pages/Synthetic-Nucleic-Acids.aspx> (accessed: 20.04.2026).
- 14 European Parliament and Council of the European Union. Regulation (EU) 2016/679, Article 9: Processing of Special Categories of Personal Data // General Data Protection Regulation. 2016. Available at: — URL: <https://gdpr-info.eu/art-9-gdpr/> (accessed: 25.04.2026).
- 15 DataReportal. Digital 2024: Kazakhstan // DataReportal. 2024. Available at: — URL: <https://datareportal.com/reports/digital-2024-kazakhstan> (accessed: 20.04.2026).
- 16 Nuclear Threat Initiative, Johns Hopkins Center for Health Security, Economist Impact. Kazakhstan // Global Health Security Index. 2021. Available at: — URL: <https://ghsindex.org/country/kazakhstan/> (accessed: 20.04.2026).
- 17 World Health Organization. Laboratory Biosafety Manual. 4th ed. // World Health Organization. – Geneva: WHO, 2020. Available at: — URL: <https://www.who.int/publications/i/item/9789240011311> (accessed: 25.04.2026).

ҰЙЫМДАСҚАН ҚЫЛМЫСТЫЛЫҚ ТЕОРИЯСЫ: ВИРТУАЛДЫ КОММУНИКАЦИЯ СЕРВИСТЕРІ АРҚЫЛЫ ТАРАЛЫП ЖАТҚАН КӨЛЕҢКЕЛІ ГЕНОМДЫҚ ЗЕРТХАНАЛАРДЫҢ ТЕТІКТЕРІН ЖОЮ САЛАСЫНДАҒЫ ҚЫЛМЫСТАРМЕН КҮРЕС ЕРЕКШЕЛІКТЕРІ

Аңдатпа

Мақалада биотехнологиялар, цифрлық коммуникациялар және қылмыстық желілік практикалардың тоғысында қалыптасып келе жатқан ұйымдасқан қылмыстың жаңа нысаны ретінде көлеңкелі геномдық зертханалар феномені зерттеледі. Зерттеудің өзектілігі генетикалық ақпарат пен биотехнологиялық ресурстарды заңсыз пайдалануға байланысты операциялардың виртуалды коммуникация арналары арқылы таралуымен айқындалады. Бұл жағдай жаңа қылмыстық әрекеттерді анықтауды, олардың құқықтық саралануын және жолын кесуді едәуір қиындатады. Зерттеудің мақсаты – көлеңкелі геномдық зертханаларға қарсы іс-қимыл жүйесіндегі институционалдық және құқықтық олқылықтарды анықтау, сондай-ақ биоцифрлық қылмысқа мемлекеттік ден қоюдың пәнаралық моделін әзірлеу. Зерттеудің әдіснамалық негізін ғылыми әдебиеттерге контент-талдау, халықаралық тәжірибеге салыстырмалы-құқықтық талдау, онлайн-сауалнама және құрылымдық модельдеу әдістері құрады. Зерттеу нәтижесінде Қазақстанда аталған мәселе ықтимал жоғары латенттілік деңгейімен, ведомствоаралық үйлестірудің жеткіліксіздігімен және жаңа биоцифрлық қатерлерді құқықтық реттеудегі нормативтік айқынсыздықпен сипатталатыны анықталды. Институционалдық өзара байланысты алты кезеңінен

тұратын: мониторинг, анықтау, тәуекелдерді бағалау, ведомствоаралық үйлестіру, құқықтық жолын кесу және кейінгі бақылауды қамтитын, аталған іс-қимылға қарсы ұлттық моделі ұсынылды. Модель нормативтік-құқықтық базаны жетілдіру, цифрлық мониторинг тетіктерін дамыту және мемлекеттік органдар, ғылыми ұйымдар мен құқық қорғау құрылымдарының өзара іс-қимылын күшейту жөніндегі ұсыныстармен толықтырылды. Зерттеу нәтижелерін геномдық және цифрлық технологияларды заңсыз пайдалануға байланысты ұйымдасқан қылмыстың жаңа нысандарының алдын алу және жолын кесудің ұлттық жүйесін қалыптастыруда қолдануға болады.

Негізгі сөздер: ұйымдасқан қылмыс, синтетикалық биология, биоцифрлық қауіпсіздік, генетикалық деректер, цифрлық криминология, құқық және биотехнология, көлеңкелі зертханалар.

НОВАЯ ФОРМА ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ТЕНЕВЫМ ГЕНОМНЫМ ЛАБОРАТОРИЯМ, РАСПРОСТРАНЯЮЩИМСЯ ЧЕРЕЗ ВИРТУАЛЬНЫЕ КАНАЛЫ КОММУНИКАЦИИ

Аннотация

В статье исследуется феномен теневых геномных лабораторий как новая форма организованной преступности, формирующаяся на пересечении биотехнологий, цифровых коммуникаций и криминальных сетевых практик. Актуальность исследования обусловлена трансформацией криминального пространства, в котором незаконные операции с генетической информацией и биотехнологическими ресурсами получают распространение посредством виртуальных каналов коммуникации, что существенно усложняет их выявление, правовую квалификацию и пресечение. Цель исследования заключается в выявлении институциональных и правовых пробелов в системе противодействия теневым геномным лабораториям и разработке междисциплинарной модели государственного реагирования на биоцифровые преступления. Методологическую основу составили контент-анализ научной литературы, сравнительно-правовой анализ международных практик, онлайн-опрос и структурное моделирование. В результате исследования установлено, что в Казахстане проблема характеризуется высоким уровнем потенциальной латентности, недостаточной межведомственной координацией и нормативной неопределённостью в части регулирования новых биоцифровых угроз. Предложена национальная модель противодействия, включающая шесть взаимосвязанных этапов институционального реагирования: мониторинг, выявление, оценку риска, межведомственную координацию, правовое пресечение и последующий контроль. Модель дополнена предложениями по совершенствованию нормативно-правовой базы, механизмов цифрового мониторинга и взаимодействия государственных органов, научных организаций и правоохранительных структур. Практическая значимость исследования заключается в возможности использования разработанных подходов при формировании национальной системы предупреждения и пресечения новых форм организованной преступности, связанных с незаконным использованием геномных и цифровых технологий.

Ключевые слова: организованная преступность, синтетическая биология, биоцифровая безопасность, генетические данные, цифровая криминология, право и биотехнологии, теневые лаборатории.

REFERENCES

- 1 Hoffmann S. A., Diggans J., Densmore D., Dai J., Knight T., Leproust E., Boeke J. D., Wheeler N., Cai Y. (2023) Safety by design: Biosafety and biosecurity in the age of synthetic genomics // iScience. Vol. 26. No. 3. P. 106165. DOI: [10.1016/j.isci.2023.106165](https://doi.org/10.1016/j.isci.2023.106165). [in English]
- 2 Millett P. (2020) The synthetic-biology challenges for biosecurity // Health Security. Vol. 18, Suppl. 1. P. 8–14. DOI: [10.1080/10736700.2020.1866884](https://doi.org/10.1080/10736700.2020.1866884). [in English]
- 3 Liu T., Wang Q., Yan Y., Chen Y., Du X., Zhang X. (2024) Advancements in DNA-based information security // Patterns. Vol. 5. No. 10. P. 101012. DOI: [10.1016/j.patter.2024.101012](https://doi.org/10.1016/j.patter.2024.101012). [in English]
- 4 Tuazon O. M., Wickenheiser R. A., Ansell R., Guerrini C. J., Zwenne G.-J., Custers B. (2024) Law enforcement use of genetic genealogy databases in criminal investigations: Nomenclature, definition and scope // Forensic Science International: Synergy. Vol. 8. P. 100460. DOI: [10.1016/j.fsisy.2024.100460](https://doi.org/10.1016/j.fsisy.2024.100460). [in English]
- 5 Son J., Kim Y. W., Oh D. B., Park J., Lee S., Kim K. (2022) Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema // Forensic Science International: Digital Investigation. Vol. 40. P. 301347. DOI: [10.1016/j.fsi.2022.301347](https://doi.org/10.1016/j.fsi.2022.301347). [in English]
- 6 Sarhan Q. U., Aleroud A., Alenezi M., Sleit A. (2023) A framework for digital forensics of encrypted real-time messaging // Ain Shams Engineering Journal. Vol. 14, No.1. P. 102069. DOI: [10.1016/j.asej.2022.102069](https://doi.org/10.1016/j.asej.2022.102069). [in English]
- 7 Afzal S., Mukhtar H., Farooq U., Shahzad F. (2021) A systematic literature review on darknet market analysis and detection techniques // Applied Sciences. Vol. 11. No. 17. P. 7789. DOI: [10.3390/app11177789](https://doi.org/10.3390/app11177789). [in English]
- 8 Reedy P. (2023) Interpol review of digital evidence for 2019.2022 // Forensic Science International: Synergy. Vol. 6. P. 100313. DOI: [10.1016/j.fsisy.2022.100313](https://doi.org/10.1016/j.fsisy.2022.100313). [in English]

- 9 Thomas M., Shah P., Vora J. (2024) Assessing privacy vulnerabilities in genetic data sets // JMIR Bioinformatics and Biotechnology. Vol. 5, No. 1. P. 54332. DOI: [10.2196/54332](https://doi.org/10.2196/54332). [in English]
- 10 Brown T., Kayser M. (2024) Forensic genetics in the shadows: Law enforcement access to clinical DNA // Journal of Law and the Biosciences. Vol. 11, No. 1. Article ID: Isae028. DOI: [10.1093/jlb/Isae028](https://doi.org/10.1093/jlb/Isae028). [in English]
- 11 Law of the Republic of Kazakhstan. (2022) On Biological Safety of the Republic of Kazakhstan: Law dated May 21, 2022 No. 122-VII LRK // Adilet Legal Information System. URL: <https://adilet.zan.kz/eng/docs/Z2200000122> [in English] (accessed: 15.04.2026).
- 12 Penal Code of the Republic of Kazakhstan: Code dated July 3, 2014 No. 226.V // Adilet Legal Information System. 2014. URL: <https://adilet.zan.kz/eng/docs/K1400000226> [in English] (accessed: 18.04.2026).
- 13 U.S. Department of Health and Human Services. Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids // Administration for Strategic Preparedness and Response. 2023. – URL: <https://aspr.hhs.gov/S3/Pages/Synthetic-Nucleic-Acids.aspx> [in English] (accessed: 20.04.2026).
- 14 European Parliament and Council of the European Union. Regulation (EU) 2016/679, Article 9: Processing of Special Categories of Personal Data // General Data Protection Regulation. 2016. URL: <https://gdpr-info.eu/art-9-gdpr/> [in English] (accessed: 25.04.2026).
- 15 DataReportal. Digital 2024: Kazakhstan // DataReportal. 2024. URL: <https://datareportal.com/reports/digital-2024-kazakhstan> [in English] (accessed: 20.04.2026).
- 16 Nuclear Threat Initiative, Johns Hopkins Center for Health Security, Economist Impact. Kazakhstan // Global Health Security Index. 2021. URL: <https://ghsindex.org/country/kazakhstan/> [in English] (accessed: 20.04.2026).
- 17 World Health Organization. Laboratory Biosafety Manual. 4th ed. // World Health Organization. – Geneva: WHO, 2020. URL: <https://www.who.int/publications/i/item/9789240011311> [in English] (accessed: 25.04.2026).

Information about authors:

Nartai Azhar Nartaiqyzy - Senior Lecturer at the Department of Criminal Law Disciplines, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Republic of Kazakhstan

E-mail: sarapshy.tk@mail.ru

ORCID: <https://orcid.org/0000-0002-6230-3651>

Shalkharov Yernar Sailaubekovich - Chief executive of criminal law disciplines branch, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Republic of Kazakhstan.

E-mail: yernar_shalkharov@list.ru

ORCID: <https://orcid.org/0000-0002-7996-7657>

Mansurov Ardaq Usenovich - **corresponding author**, PhD student, Department of Criminal Law Disciplines, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Republic of Kazakhstan

E-mail: mansa_911@mail.ru

ORCID: <https://orcid.org/0009-0006-3696-3329>

Dosekeev Olzhas Bekboldyuly - Senior lecturer, Department of Criminal Law Disciplines, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Republic of Kazakhstan

E-mail: olzhas.dossekeyev@ayu.edu.kz

ORCID: <https://orcid.org/0009-0006-6222-5194>

Информация об авторах:

Нартай Ажар Нартайкызы - старший преподаватель кафедры уголовно-правовых дисциплин, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, г. Туркестан, Республика Казахстан.

E-mail: sarapshy.tk@mail.ru

ORCID: <https://orcid.org/0000-0002-6230-3651>

Шалхаров Ернар Сайлаубекевич - заведующий кафедрой уголовно-правовых дисциплин, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, г. Туркестан, Республика Казахстан.

E-mail: yernar_shalkharov@list.ru

ORCID: <https://orcid.org/0000-0002-7996-7657>

Мансуров Ардак Усенович - **основной автор**, докторант PhD, кафедра уголовно-правовых дисциплин, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, г. Туркестан, Республика Казахстан.

E-mail: mansa_911@mail.ru

ORCID: <https://orcid.org/0009-0006-3696-3329>

Досекеев Олжас Бекболдылы - старший преподаватель, кафедра уголовно-правовых дисциплин, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, г. Туркестан, Республика Казахстан.

E-mail: olzhas.dossekeyev@ayu.edu.kz

ORCID: <https://orcid.org/0009-0006-6222-5194>

Авторлар туралы ақпарат:

Нартай Ажар Нартайқызы - Қылмыстық-құқықтық пәндер кафедрасының аға оқытушысы, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан қ., Қазақстан Республикасы

E-mail: sarapshy.tk@mail.ru

ORCID: <https://orcid.org/0000-0002-6230-3651>

Шалхаров Ернар Сайлаубекович - Қылмыстық-құқықтық пәндер кафедрасының меңгерушісі, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан қ., Қазақстан Республикасы

E-mail: vernar_shalkharov@list.ru

ORCID: <https://orcid.org/0000-0002-7996-7657>

Мансуров Ардақ Үсенович - **негізгі автор**, PhD докторанты, қылмыстық-құқықтық пәндер кафедрасы, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан қ., Қазақстан Республикасы

E-mail: mansa_911@mail.ru

ORCID: <https://orcid.org/0009-0006-3696-3329>

Досекеев Олжас Бекболдыұлы - аға оқытушы, қылмыстық-құқықтық пәндер кафедрасы, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан қ., Қазақстан Республикасы

E-mail: olzhas.dossekeyev@ayu.edu.kz

ORCID: <https://orcid.org/0009-0006-6222-5194>