Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Қылмыстық құқық. Қылмыстық процесс / Criminal law. Criminal process / Уголовное право. Уголовный процесс

IRSTI 10.81.71 *https://doi.org/10.32523/2616-6844-2026-154-1-170-182*
Scientific Article

Pre-trial investigation of online fraud involving deepfake technologies and social engineering from a biosocial and life-course criminological perspective

K.M. Beaver*[1]

College of Criminology and Criminal Justice, Florida State University, USA, Florida

(E-mail: kevinmichaelbeaver@gmail.com)

Abstract. This article examines the pressing challenges of pre-trial investigations into online fraud involving deepfake technologies and social engineering methods. The primary goal is to provide a comprehensive analysis of digital crime mechanisms through the lenses of biosocial and life-course criminology to enhance investigative effectiveness. The scientific and practical significance of the study lies in the necessity of adapting traditional legal instruments to conditions of technological asymmetry and digital volatility. The research methodology includes analyzing typical criminal scenarios, studying the specifics of digital traces, and modeling offender behavioral patterns based on their criminal trajectories. Key findings demonstrate the multi-level structure of the criminal mechanism and identify systemic barriers such as rapid data loss and the uncertain procedural status of synthetic content. The author concludes that forming interdisciplinary investigative teams and implementing standards for the immediate preservation of the digital environment are essential. The study's value lies in integrating behavioral analysis into criminal proceedings, facilitating a shift from reactive response to proactive profiling. The practical significance of the outcomes consists of improving investigative tactics and modernizing the regulatory framework to counter high-tech crime.

Keywords: deepfake, online fraud, social engineering, pre-trial investigation, biosocial criminology, life-course criminology, digital traces.

Introduction

The digitalization of social relations has transformed not only economic and communicative practices but also the very morphology of crime, giving rise to qualitatively new forms of unlawful behavior based on high-technology tools and manipulative digital practices. In a context where, as aptly noted by the President of the Republic of Kazakhstan, K.-J. Tokayev, humanity has

Received: 21.01.2026. Accepted: 25.03.2026. Available online: 30.03.2026

***[1]the corresponding author**

entered an era of "unprecedented challenges and radical change," and the technological race has acquired the status of a determinant of global development. The digital environment is constituted not merely as a space of economic and social growth but also as a zone of heightened criminogenic vulnerability.

The state's course toward digitalization, articulated in the Address to the People of Kazakhstan of 1 September 2023, objectively increases the importance of legal protection of the individual in the virtual sphere, where traditional mechanisms for detecting and investigating crime demonstrate growing functional insufficiency [1].

Fraud, historically rooted in models of interpersonal contact, in the digital environment acquires a networked, transboundary, and asynchronous character: criminal influence no longer requires the physical presence of the offender, while communication between the perpetrator and the victim is mediated by platform infrastructures, algorithms, and the media environment. This radically modifies the criminal mechanism of the act, its temporal structure, and the modes of procedural detection, shifting the focus from localized episodes to distributed digital interactions [2].

A special place in this transformation is occupied by the convergence of deepfake technologies with methods of social engineering. Deepfake generates the illusion of the authentic visual and auditory presence of a specific person, placing the victim in the position of an ostensible eyewitness to an event and thereby reconfiguring the epistemic status of the information received. As R. Chesney and D. Citron emphasize, audio and video recordings possess exceptional persuasive power, creating an effect of direct testimony and reducing the level of critical perception. In the conditions of the "post-truth era," technological simulation of reality significantly enhances the effectiveness of fraud by appealing to basic cognitive and affective mechanisms of trust, blurring the boundaries between the genuine and the constructed, and complicating both prevention and proof [3; 4].

The choice of this research topic is due to the emergence of a fundamentally new type of criminal threat - technologically mediated deception capable of reproducing a person's identity and behavioral patterns with high realism. Despite the rapid spread of deepfake technologies and the growing number of incidents worldwide, comprehensive criminological and procedural studies devoted specifically to pre-trial investigation of such offenses remain limited, while existing works are predominantly technological or cybersecurity-oriented. This creates a problematic situation characterized by a discrepancy between the scale of the phenomenon and the level of its doctrinal and methodological elaboration.

The technological complexity of such offenses enters into a systemic contradiction with the traditional architecture of criminal procedure, which has historically been oriented toward material traces and spatially localized sources of evidentiary information. Procedural instruments designed for the physical world prove insufficiently adapted to an environment in which the key elements of a crime exist in the form of ephemeral digital data distributed across servers, often located beyond national jurisdiction [5; 6]. Investigative authorities are compelled to operate under conditions of technological asymmetry, where the speed at which relevant information is lost systematically exceeds the capacity for procedural response.

These circumstances determine the growth of the latency of online fraud and the structural complication of proof [7]. A significant proportion of victims either fail to recognize the fact of the offense or refrain from contacting law enforcement agencies, a priori assessing the identification of the offender as impossible [8]. Even when criminal proceedings are initiated,

investigative bodies confront the fragmentary nature of the digital trace, the absence of direct subject identifiers, and institutional dependence on private technological intermediaries, which together generate a persistent gap between the real prevalence of such acts and their statistical representation.

The relevance of the study is determined by the practical necessity of developing effective investigative approaches capable of operating under conditions of digital volatility, cross-border infrastructure, and the synthetic nature of evidentiary objects. The lack of comprehensive answers to questions concerning the procedural status of deepfake content, methods of preserving digital traces, and behavioral characteristics of offenders confirms the theoretical and applied significance of this research.

Under these conditions, pre-trial investigation ceases to be an exclusively legal-technical procedure and requires the integration of analytical approaches that take into account the behavioral nature of digital deception, the stability of criminal patterns, and their temporal dynamics [9]. Empirical practice demonstrates that investigative actions in cases of digital fraud are often reactive in character and are undertaken only after critical data have already been lost. Short log-retention periods, dependence on foreign providers, and the absence of unified standards for handling synthetic media content create a situation in which, even when indications of an offense are present, the investigation finds itself in a position of perpetual catch-up [10], while a stable structural gap becomes entrenched between the technological level of criminal groups and the procedural capacities of investigative authorities.

The scholarly development of this problem remains markedly fragmented. Technocratic research is predominantly concentrated on algorithms for generating and detecting deepfake content, as well as on cybersecurity issues, remaining outside the framework of criminal-procedural analysis. Legal doctrine, in turn, focuses on qualification and normative aspects, interpreting deepfake either as a digital object or as a method of committing an offense, without moving beyond the boundaries of a formal-legal paradigm [11]. The divergence of these research vectors impedes the formation of a coherent model of pre-trial investigation of online fraud capable of accounting not only for the technological parameters of the act but also for the behavioral nature of criminal influence.

The object of the research is the system of pre-trial investigation of online fraud committed using deepfake technologies and social engineering methods.

The subject of the research comprises the mechanisms of committing such crimes, the formation of digital traces, the behavioral characteristics of offenders and victims, and the procedural tools used to detect, fix, and prove these acts.

Criminological factors-features of the offender's personality, the stability of deviant strategies, stages of involvement, and the specificities of victim behavior-are virtually not integrated into procedural practice [12]. Investigative activity is constructed around the formal attributes of the event, while the dynamics of criminal behavior remain outside systematic analysis.

The absence of such integration constrains the prognostic and preventive potential of the criminal process. Pre-trial investigation is oriented primarily toward the retrospective reconstruction of the fact of the offense and operates in a mode of point-based response, which reduces its capacity to adapt to persistent and evolving forms of digital fraud. Overcoming this gap requires recourse to interdisciplinary models that link procedural mechanisms with the regularities governing the formation and reproduction of criminal behavior in the digital environment.

The purpose of the study is to develop a comprehensive analytical model of pre-trial investigation of deepfake-enabled online fraud based on biosocial and life-course criminological approaches.

To achieve this purpose, the following research objectives are formulated:

– to analyze the transformation of fraud mechanisms in the digital environment;

– to identify typical scenarios of deepfake-based deception;

– to examine the nature and evidentiary value of digital traces;

– to determine systemic procedural barriers to investigation;

– to assess the behavioral characteristics of offenders through biosocial and life-course perspectives;

– to formulate practical recommendations for improving investigative tactics.

Biosocial criminology proceeds from the premise that criminal behavior is formed through the interaction of biological, psychological, and social factors [13; 14]. Deviance is conceptualized as a dynamic system in which neuropsychological characteristics, cognitive distortions, levels of self-control, and impulsivity correlate with environmental conditions, available opportunities, and cultural norms [15; 16]. Empirical studies reveal a stable correlation between specific neurobehavioral traits and a propensity for manipulative and risk-oriented conduct, a relationship that acquires particular significance in the digital environment, where barriers to entry are minimal and the likelihood of sanctions is perceived as low [17].

A core tenet of this approach is the idea of the stability of criminal patterns: behavior is interpreted not as an isolated act but as a reproducible model of response [15; 18]. Having mastered techniques of manipulation and evasion of control, the subject tends to replicate them across diverse digital contexts, altering their form while preserving the behavioral core. Online fraud, within this logic, is transformed into a stable strategy rather than a situational deviation.

Life-course criminology complements this logic in the temporal dimension, viewing crime as a process unfolding over the life span [19]. The concept of a "criminal trajectory" reflects the stages of involvement, consolidation, and transformation of deviant activity. Research demonstrates that early behavioral traits, social ruptures, and deficits of institutional attachment generate a predisposition toward alternative, including unlawful, forms of self-realization [20]. The digital environment, by providing anonymity and rapid access to resources, accelerates the transition from episodic actions to sustained criminal activity.

Applying the biosocial and life-course paradigms to the analysis of online fraud makes it possible to move beyond a purely technological and formal-legal understanding of the act [12]. Deepfake technologies and social engineering function not merely as tools but as means for implementing already formed behavioral strategies. Consideration of the criminal trajectory allows digital fraud to be viewed as a stage in a deviant career rather than as an incidental product of technical accessibility [20].

For pre-trial investigation, this framework is of fundamental importance, as it enables a shift from episodic analysis to the identification of regularities in the formation and reproduction of criminal behavior [21]. The integration of biosocial and life-course factors expands the possibilities for profiling, recidivism prediction, and the selection of procedural tactics in light of the subject's behavioral logic, which is especially significant under conditions of high adaptability and concealment inherent in digital crime.

The scientific significance of the study lies in integrating biosocial and life-course criminology into the analysis of high-tech crime, thereby expanding the theoretical foundations of criminology and criminal procedure.

The practical significance consists in developing recommendations aimed at increasing the effectiveness of pre-trial investigation, improving evidence collection, and adapting legal instruments to the realities of digital criminality.

Literature review

The review of scientific literature shows that foreign studies on online fraud involving deepfake technologies are predominantly interdisciplinary and focus on the technological, psychological, and legal aspects of the phenomenon. Fundamental works in the field of digital evidence and cybercrime (E. Casey, T.J. Holt, A.M. Bossler) have established the theoretical foundation for understanding the specifics of digital traces and the peculiarities of investigating crimes in a virtual environment. Studies by R. Chesney and D. Citron, L. Verdoliva, Y. Mirsky, and W. Lee have made a significant contribution to understanding the nature of deepfake content, its generation, detection, and associated risks for legal systems. At the same time, the works of M. Button and C. Cross, M. Whitty, and other scholars reveal the mechanisms of social engineering and the psychological factors of victimization, demonstrating that the effectiveness of fraud is determined not only by technology but also by the characteristics of human perception and trust.

Contemporary criminological research based on biosocial and life-course approaches (A. Raine, T.E. Moffitt, D.P. Farrington) makes it possible to explain the persistence of deviant behavior, the formation of criminal trajectories, and the recurrence of criminal scenarios in the digital environment. These studies significantly expand the understanding of the offender's personality and the temporal dynamics of criminal activity; however, they are rarely applied directly to the analysis of high-technology forms of fraud.

Despite the substantial volume of scientific publications, the foreign literature still contains a number of significant gaps. Most studies consider deepfakes either as an information security and disinformation problem or as an object of technical expertise, paying insufficient attention to the criminal-procedural aspects of pre-trial investigation and evidence. In addition, issues such as behavioral profiling of offenders, the integration of criminological models into investigative practice, and the prompt collection and preservation of digital evidence under conditions of its rapid disappearance remain insufficiently explored. Therefore, there is an objective need for comprehensive research combining technological, criminological, and procedural analysis, which determines the scientific novelty of the present study.

Research methods

The empirical basis of the study comprises materials from investigative and judicial practice, data from criminological research on online fraud, analysis of typical criminal scenarios ("personalized trust," "institutional simulation," and emotionally dependent schemes), as well as large sets of digital traces (logs, metadata, transaction records) and reports of international organizations, ensuring cross-jurisdictional comparability and the identification of universal patterns of digital crime. The research was conducted in successive stages, ranging from the theoretical synthesis of the biosocial paradigm and life-course criminology to the decomposition of the criminal mechanism, the analysis of procedural barriers in recording digital evidence, and the development of applied tools for profiling and adapting interrogation tactics. The methodological framework integrates biosocial modeling, the life-course approach to examining

criminal careers, scenario analysis and typology, digital forensics for reconstructing distributed traces, criminological profiling based on the "digital footprint," and comparative legal analysis of international practices for data preservation and cooperation with service providers.

Findings/Discussion

Pre-trial investigative practice demonstrates the formation of stable and repeatedly encountered scenarios of online fraud in which deepfake technologies function not as auxiliary tools but as a core structural element of the criminal mechanism [22]. Analysis of investigative materials and judicial decisions shows that such crimes are typically organized according to reproducible models rather than isolated improvisations [8; 17].

The most widespread scenario is "personalized trust," where offenders simulate the appearance or voice of a specific person possessing authority for the victim. In documented cases, victims transferred funds or disclosed confidential information after receiving a synthetic video or audio message perceived as authentic communication [23; 24]. This format proves more effective than classical phishing because it relies on an already established trust relationship.

Another frequently recorded scenario is "institutional simulation," involving imitation of representatives of banks or law-enforcement agencies. Victims are instructed to "protect funds," verify transactions, or temporarily transfer money to "secure accounts." Investigative practice indicates that the combination of visual credibility and authoritative commands significantly increases compliance rates.

A third group consists of long-term manipulative schemes, including romantic and investment fraud [25]. Offenders maintain prolonged communication using synthetic personas, gradually forming trust and introducing financial demands. Such cases often involve repeated transactions over time, which complicates detection and legal qualification.

Despite differences, these scenarios share a multistage structure: data collection on the victim, selection of a suitable persona, initiation of contact, creation of urgency or trust, and extraction of funds. Each stage may be performed by different participants or automated tools, forming a distributed criminal architecture. For investigators, this requires reconstruction of the entire sequence rather than focusing solely on the final fraudulent transaction.

The mechanism of deepfake-enabled fraud can therefore be described as multi-level. The first stage involves the systematic collection of personal data from social networks, open sources, or leaks to create a victim profile [8]. The second stage consists of generating synthetic audio-visual content using image and voice technologies [26; 27]. The third stage includes direct psychological influence through communication designed to induce urgency or anxiety. The final stage involves financial extraction and concealment through intermediary accounts, cryptocurrency, or proxy infrastructure.

In practice, this structure results in significant investigative difficulties because the offense unfolds entirely within a digital environment without stable material traces. Evidence often exists only in the form of temporary files, logs, or network identifiers, many of which may be deleted before procedural fixation.

Visual and auditory communication plays a decisive role in these crimes [27]. Synthetic images and voices activate cognitive mechanisms of face and speech recognition, leading victims to perceive the interaction as genuine [28]. As a result, decisions are made in an emotional rather than rational mode, reducing critical evaluation of instructions received [29].

This psychological effect also influences the victim's behavior during the investigation. Victims frequently remain convinced of the authenticity of the communication even after discovering the fraud, which may delay reporting and complicate testimony [17]. Investigators must therefore consider the distortive impact of synthetic media when assessing evidence and witness statements.

The digital trace in such cases differs fundamentally from traditional forensic traces. It is fragmented, distributed across multiple platforms, and highly volatile [30]. Evidence may consist of metadata, server logs, transaction records, or communication fragments, often stored in different jurisdictions and subject to rapid deletion [31].

Additional complexity arises from the use of disposable accounts, VPN services, encrypted messengers, and automated tools. These technologies allow offenders to change technical parameters without altering the underlying criminal model, making identification of stable markers difficult. Consequently, investigations rely on analysis of correlations between heterogeneous data rather than on single decisive pieces of evidence [32].

A major procedural challenge is the preservation of digital evidence. Investigative practice shows that key data may disappear within hours or days due to platform policies or automatic deletion. Screenshots or copied files provided by victims often lack original metadata, which complicates verification of authenticity, especially in deepfake cases where establishing the origin of content is crucial [33].

Existing procedural approaches based on static physical evidence are insufficient in this context. Effective investigation requires rapid preservation of data and coordinated collection of information from multiple sources, including content, timestamps, network routes, and platform records. Without such measures, reconstruction of the event remains incomplete and vulnerable to procedural challenges.

Another difficulty is the uncertain procedural status of deepfake content. Synthetic audio-visual materials do not fit traditional categories of evidence based on recordings of real events [27]. In practice, they may be treated either as physical evidence or as auxiliary digital files, leading to inconsistent approaches and uncertainty in court [34].

Expert examination also faces methodological problems because traditional forensic methods were designed for authentic recordings rather than algorithmically generated media [35]. This often results in probabilistic conclusions that reduce evidentiary strength.

Investigations are further complicated by dependence on private digital platforms. Communication, data storage, and financial operations are controlled by corporate entities that determine retention periods and access conditions [36]. Delays in responding to official requests may lead to irreversible loss of evidence. Moreover, platform moderation policies may remove suspicious content before investigators can secure it, eliminating valuable metadata [37].

This creates a structural asymmetry between the speed of criminal activity and the tempo of procedural response. Access to critical information frequently depends on international cooperation and corporate compliance rather than solely on investigative authority [38].

Time, therefore, becomes a decisive factor in digital investigations. If reporting is delayed, primary data may already be deleted, leaving only victim testimony. In deepfake cases, such delays are common because victims initially doubt their own interpretation of events. Consequently, investigations often begin under conditions of evidentiary deficit determined by technological factors rather than investigative shortcomings [39; 40].

Online fraud employing deepfake technologies is also characterized by stable behavioral patterns of offenders. Analysis of investigative practice indicates that perpetrators typically

demonstrate high adaptability, risk tolerance, and a pronounced orientation toward manipulative interaction, treating the victim primarily as a resource rather than as a subject of communication [41; 42]. Such behavioral traits contribute to the serial nature of offenses and facilitate the rapid modification of scenarios depending on situational conditions.

From a life-course perspective, involvement in digital fraud often develops through stages—from initial experimentation with simple schemes to systematic activity using specialized tools and participation in organized online networks. Access to technological resources, informal mentorship within criminal communities, and repeated successful episodes reinforce deviant behavior and accelerate the formation of a stable criminal trajectory [45–47].

This trajectory-based nature of online fraud explains the high probability of recurrence. Individual incidents frequently represent only one episode within an ongoing series of criminal activities. Indicators such as technological competence, multistage planning, and the use of synthetic media suggest professionalization of the offender and justify prioritization of investigative resources, including coordinated actions across jurisdictions [48–50].

These findings support the need for an interdisciplinary investigative approach involving digital forensics specialists, information security experts, and behavioral analysts. Such teams are better equipped to reconstruct complex digital mechanisms, preserve volatile evidence, and interpret synthetic media.

Modernization of procedural standards is therefore essential. Effective investigation of deepfake-enabled fraud requires emergency data preservation mechanisms, specialized expert methodologies for synthetic content, and clear rules for the admissibility and evaluation of digital evidence [26].

Overall, the analysis shows that combating deepfake-based online fraud demands a shift from a reactive model focused on isolated events to an analytical model capable of reconstructing distributed criminal mechanisms and responding to the rapid dynamics of the digital environment.

Conclusion

The conducted study demonstrates that digitalization has not only expanded the toolkit of criminal activity but has also altered the very morphology of crime, giving rise to a qualitatively new form of online fraud grounded in the synergy of deepfake technologies and social engineering methods. The findings substantiate the author's hypothesis that traditional criminal procedural mechanisms, in their current configuration, prove functionally inadequate under conditions of technological asymmetry and the specific features of the digital environment, where the boundaries between the real and the synthetic become operationally indistinguishable.

In this context, the transformation of scientific knowledge in the field under consideration is manifested in a shift from a narrowly technocratic or purely formal-legal understanding of cybercrime toward an interdisciplinary biosocial and life-course paradigm. The application of this approach makes it possible to conceptualize digital fraud not as an isolated episode, but as the realization of stable behavioral patterns and "digital criminal trajectories" characterized by seriality and high adaptability. This perspective expands the explanatory capacity of criminological analysis and enables a more precise understanding of the mechanisms through which digital crime is reproduced.

Within the framework of the present study, a set of generalized conclusions has been formulated, bearing significance for the development of criminology and criminal procedure.

First, the multi-layered nature of the criminal mechanism has been established: deepfake technology functions as its core element, exploiting fundamental cognitive mechanisms of trust

and shifting the interaction with the victim from a rational domain to an emotionally reactive one. This transformation fundamentally alters the nature of victim behavior and substantially increases the effectiveness of criminal influence.

Second, it has been demonstrated that digital traces in cases of deepfake-based fraud are characterized by a fragmented, distributed, and ephemeral nature. This feature necessitates a reorientation of the investigative paradigm from reliance on static material evidence toward the analysis of aggregated data, network correlations, and behavioral "imprints" formed within the digital environment.

Third, systemic barriers hindering pre-trial investigation have been identified, among which particular importance is attached to the institutional dependence of law enforcement agencies on private technological platforms, as well as to the uncertainty surrounding the procedural status of synthetic content, which often lacks a direct analogue in physical reality.

In light of the identified patterns, the need to modernize the regulatory framework and investigative tactics is substantiated. The following priority directions are proposed:

– the establishment of interdisciplinary investigative teams bringing together legal professionals, digital forensics specialists, and behavioral analysts for the comprehensive reconstruction of criminal events;

– the legislative recognition of deepfake content as an independent object of proof, functioning as a carrier of criminal impact;

– the implementation of standards for the prompt capture of the digital environment, ensuring the emergency preservation of data prior to its automatic deletion or modification by service providers;

– the integration of criminological profiling methods and adapted interrogation tactics that take into account the biosocial characteristics of offenders, including impulsivity, deficits in empathy, and cognitive distortions.

Prospects for further research are associated with the development of automated systems for the proactive profiling of digital threats, as well as with the improvement of mechanisms of international legal cooperation. This orientation is driven by the transboundary nature of digital crime and the objective impossibility of countering it effectively within the confines of exclusively national jurisdictions.

The contribution of the authors

K.M. Beaver has done research and written the entire article.

This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26103625 «Online fraud using deepfake-technologies and social engineering: problems of criminal law counteraction, prospects for legislative regulation»).

References

1. The Head of State delivered an Address to the People of Kazakhstan. – Режим доступа: https://www.akorda.kz/ru/glava-gosudarstva-vystupil-s-poslaniem-narodu-kazahstana-184959 (date of access: 15.10.2025).

2. Casey E. Digital Evidence and Computer Crime. Academic Press, 2011. 840 p.

3. Chesney R., Citron D. Deepfakes and the New Disinformation War. 2018. – Режим доступа: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war (date of access: 20.09.2025).

4. Vaccari C., Chadwick A. Deepfakes and Disinformation // Social Media + Society. 2020. Vol.6. No.1. https://doi.org/10.1177/2056305120903408

5. National Institute of Justice (NIJ). Digital & Multimedia Evidence. – Access mode: https://nij.ojp.gov/topics/forensics/digital-multimedia-evidence (date of access: 05.10.2025).

6. Council of Europe. Electronic Evidence in Civil and Administrative Proceedings. – Режим доступа: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 (дата обращения: 12.10.2025).

7. OECD. Financial Consumer Protection Policy Approaches in the Digital Age: Protecting Consumers' Assets, Data and Privacy. 2020. – Access mode: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/financial-consumer-protection-policy-approaches-in-the-digital-age_dc8c14b2/3f205e60-en.pdf (date of access: 01.10.2025).

8. Button M., Cross C. Cyber Fraud, Scams and Their Victims. Routledge, 2017. – Access mode: https://crpf.gov.in/writereaddata/images/pdf/Cyber_Frauds_Scams_and_their_Victims.pdf (date of access: 18.09.2025).

9. Berger A.N., Molyneux P., Wilson J.O.S. The Oxford Handbook of Banking. 4th edn. Oxford University Press, 2025. Oxford Academic 2015. https://doi.org/10.1093/oxfordhb/9780198897071.001.0001

10. World Economic Forum. Global Cybersecurity Outlook 2024. – Режим доступа:https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf (date of access: 10.10.2025).

11. Cascone G. The Use of Artificial Intelligence in EU Criminal Justice Systems: First Insights and Emerging Trends in an Evolving Landscape // Open Research Europe. 2025. Vol. 5. Art.361. https://doi.org/10.12688/openreseurope.21780.1

12. Leukfeldt E.R. Cybercrime and Social Ties: Phishing in Amsterdam // Trends in Organized Crime. 2014. Vol.17. No.4. Pp. 231–249. https://doi.org/10.1007/s12117-014-9229-5

13. Beaver K.M. Biosocial Criminology: A Primer. Dubuque: Kendall Hunt, 2019. 298 p.

14. Raine A. The Anatomy of Violence: The Biological Roots of Crime. New York: Pantheon, 2013. 478 p.

15. DeLisi M., Vaughn M.G. The Routledge International Handbook of Biosocial Criminology. Routledge, 2015. 688 p.

16. Gottfredson M.R., Hirschi T. A General Theory of Crime. Stanford: Stanford University Press, 1990. 361 p.

17. Holt T.J., Bossler A.M. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. New York: Routledge, 2016. 236 p.

18. Moffitt T.E. Adolescence-Limited and Life-Course-Persistent Antisocial Behavior: A Developmental Taxonomy // Psychological Review. 1993. Vol.100. No.4. Pp. 674–701. https://doi.org/10.1037/0033-295X.100.4.674

19. Farrington D.P. Developmental and Life-Course Criminology: Key Theoretical and Empirical Issues – The 2002 Sutherland Award Address // Criminology. 2006. Vol. 41. Pp. 221–255. https://doi.org/10.1111/j.1745-9125.2003.tb00987.x

20. Moffitt T.E. Male Antisocial Behaviour in Adolescence and Beyond // Nature Human Behaviour. 2018. Vol. 2. Pp. 177–186.

21. White V., Applegarth D., Hunt J., Hudgins C. The NIJ Recidivism Forecasting Challenge: Contextualizing the Results. 2022. – Access mode: https://www.researchgate.net/publication/368984590_THE_NIJ_RECIDIVISM_FORECASTING_CHALLENGE_CONTEXTUALIZING_THE_RESULTS (date of access: 14.10.2025).

22. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union, Luxembourg, 2024. https://doi.org/10.2813/442713

23. Kietzmann J., Lee L., McCarthy I., Kietzmann T. Deepfakes: Trick or Treat? // Business Horizons. 2020. Vol.63. No.2. Pp. 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

24. Vaccari C., Chadwick A. Deepfakes and Disinformation // Social Media + Society. 2020. Vol.6. No.1. https://doi.org/10.1177/2056305120903408

25. Whitty M. The Psychology of the Online Dating Romance Scam. 2012. – Режим доступа: https://fido.nrk.no/d6f57fd73b9898b42c8c322c961c8255f370677fbac5272b71d86047a5359b66/Whitty_romance_scam_report.pdf (дата обращения: 02.10.2025).

26. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. 2019. Vol. 107. No.6. Pp. 1753–1820. https://doi.org/10.15779/Z38RV0D15J

27. Verdoliva L. Media Forensics and DeepFakes: An Overview // IEEE Journal of Selected Topics in Signal Processing. 2020. Vol. 14. No.5. Pp. 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

28. Todorov A. Face Value: The Irresistible Influence of First Impressions. Princeton: Princeton University Press, 2017. 336 p.

29. Kahneman D. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011. 499 p.

30. Kessler G. Digital Forensic Evidence Examination // Journal of Digital Forensics, Security and Law. 2010. Vol. 5. Art. 6. Pp. 85–88. https://doi.org/10.15394/jdfsl.2010.1077

31. Europol. Facing Reality? Law Enforcement and the Challenge of Deepfakes: An Observatory Report from the Europol Innovation Lab. Publications Office of the European Union, Luxembourg, 2022. – Access mode: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf (дата обращения: 16.10.2025).

32. Edewaard D.E., Szubski E.C., Tyrrell R.A. The Conspicuity Benefits of Rear-Facing Bike Lights in Daylight // Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2019. Vol. 63. No.1. Pp. 1937–1938. https://doi.org/10.1177/1071181319631427

33. Mirsky Y., Lee W. The Creation and Detection of Deepfakes: A Survey // ACM Computing Surveys. 2020. Vol. 53. No.1. Art. 1. 38 p. https://doi.org/10.48550/arXiv.2004.11138

34. Maras M.-H., Alexandrou A. Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos // The International Journal of Evidence & Proof. 2018. Vol. 23. No.3. Pp. 255–262. https://doi.org/10.1177/1365712718807226

35. Agarwal S., Farid H., Gu Y., et al. Protecting World Leaders Against Deep Fakes // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2019. Pp. 38–45.

36. Vermeer M.J.D., Woods D., Jackson B.A. Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers. Santa Monica, CA: RAND Corporation, 2018. – Access mode: https://www.rand.org/pubs/research_reports/RR2240.html (date of access: 08.10.2025).

37. Hubley H. Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations // International Criminal Law Review. 2022. Vol.22. No.5–6. Pp. 989–1015. https://doi.org/10.1163/15718123-bja10124

38. Kerr O.S. The Fourth Amendment Limits of Internet Content Preservation. 2021. – Access mode: https://www.grubaughlaw.com/wp-content/uploads/sites/394/2020/12/The-Fourth-Amendment-Limits-of-Internet-Content-Preservation.pdf (date of access: 11.10.2025).

39. Tanveer M., Khan N., Ali M., Islam R., Sattar M.M., Shoaib M. Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review // Spectrum of Emerging Sciences, 2025. https://doi.org/10.5281/zenodo.15165447

40. Al-Khanafseh M., Surakhi O. Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography // Electronics. 2024. Vol. 13. Art.3729. https://doi.org/10.3390/electronics13183729

41. Rodrigues H., Medina J.C. Police Legitimacy and Procedural Justice among Young Brazilian Adolescents: A Cross-Sectional and Time-Ordered Analysis // The British Journal of Criminology. 2021. Vol. 61. No.5. Pp. 1206–1224. https://doi.org/10.1093/bjc/azab004

42. Cook S., Giommoni L., Trajtenberg Pareja N., Levi M., Williams M.L. Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory // The British Journal of Criminology. 2023. Vol. 63. No.2. Pp. 384–406. https://doi.org/10.1093/bjc/azac021

43. Raji H., Dinesh S., Sharma S. Inside the Impulsive Brain: A Narrative Review on the Role of Neurobiological, Hormonal and Genetic Factors Influencing Impulsivity in Psychiatric Disorders //

Egyptian Journal of Neurology, Psychiatry and Neurosurgery. 2025. Vol. 61.4. https://doi.org/10.1186/s41983-024-00930-9

44. Palmieri M., Shortland N., McGarry P. Personality and Online Deviance: The Role of Reinforcement Sensitivity Theory in Cybercrime // Computers in Human Behavior. 2021. Vol. 120. 106745. https://doi.org/10.1016/j.chb.2021.106745

45. Whittaker A., Densley J., Moser K.S. No Two Gangs Are Alike: The Digital Divide in Street Gangs' Differential Adaptations to Social Media // Computers in Human Behavior. 2020. Vol. 110. 106403. https://doi.org/10.1016/j.chb.2020.106403

46. Martineau M., Spiridon E., Aiken M. Pathways to Criminal Hacking: Connecting Lived Experiences with Theoretical Explanations // Forensic Science. 2024. Vol. 4. No.4. Pp. 647–668. https://doi.org/10.3390/forensicsci4040045

47. Hoffman C.J., Howell C.J., Perkins R.C., Maimon D., Antonaccio O. Predicting New Hackers' Criminal Careers: A Group-Based Trajectory Approach // Computers & Security. 2024. Vol. 137. 103649. https://doi.org/10.1016/j.cose.2023.103649

48. Piquero A.R. "We Study the Past to Understand the Present; We Understand the Present to Guide the Future": The Time Capsule of Developmental and Life-Course Criminology // Journal of Criminal Justice. 2023. Vol. 85. 101932. https://doi.org/10.1016/j.jcrimjus.2022.101932

49. Paquet-Clouston M., Paquette S.-O., Garcia S., Erquiaga M.J. Entanglement: Cybercrime Connections of a Public Forum Population // Journal of Cybersecurity. 2022. Vol.8. No.1. https://doi.org/10.1093/cybsec/tyac010

50. Laub J.H., Sampson R.J. Life-Course and Developmental Criminology: Looking Back, Moving Forward – ASC Division of Developmental and Life-Course Criminology Inaugural David P. Farrington Lecture // Journal of Developmental and Life-Course Criminology. 2020. Vol. 6. Pp. 158–171. https://doi.org/10.1007/s40865-019-00110-x

К.М. Бивер*
Флорида штатының университетінің Криминология және қылмыстық сот төрелігі колледжі, АҚШ, Флорида
(E-mail: kevinmbeaver@hotmail.com)

Биоәлеуметтік және өмірлік жол криминологиясы тұрғысынан deepfake технологиялары мен әлеуметтік инженерияны қолданатын онлайн-алаяқтық бойынша сотқа дейінгі терген-тексеру практикасын талдау

Аңдатпа. Мақала дипфейк технологиялары мен әлеуметтік инженерия әдістерін қолдану арқылы жасалатын онлайн-алаяқтықты сотқа дейінгі тергеп-тексерудің өзекті мәселелерін кешенді түрде зерттеуге арналған. Жұмыстың негізгі мақсаты – биоәлеуметтік және өмірлік жол криминологиясы тұрғысынан цифрлық қылмыстардың механизмдерін терең талдау арқылы тергеу қызметінің тиімділігін арттыру. Зерттеудің ғылыми және практикалық маңыздылығы дәстүрлі құқықтық құралдарды технологиялық асимметрия мен цифрлық құбылмалылық жағдайларына бейімдеу қажеттілігімен айқындалады, бұл қазіргі қылмыстық процестің шынайы талаптарына жауап береді. Әдіснама типтік қылмыстық сценарийлерді жүйелі талдауды, цифрлық іздердің табиғаты мен сақталу ерекшеліктерін зерттеуді, сондай-ақ құқық бұзушылардың мінез-құлық траекторияларын модельдеуді қамтиды. Алынған нәтижелер қылмыстық механизмнің көпдеңгейлі құрылымын ашып, деректердің тез жоғалуы, трансшекаралық цифрлық орта және синтетикалық контенттің белгісіз процестік мәртебесі сияқты жүйелі кедергілерді анықтайды. Автор пәнаралық тергеу топтарын қалыптастыру және цифрлық ортаны жедел бекіту стандарттарын енгізу қажеттігін негіздейді. Жұмыстың құндылығы қылмыстық процестік қызметке мінез-құлық талдауын интеграциялауда, бұл ретроспективті талдаудан проактивті профильдеуге көшуге мүмкіндік береді. Зерттеу қорытындылары тергеу тактикасын жетілдіруге, жоғары технологиялық қылмысқа қарсы іс-қимылды күшейтуге және нормативтік базаны жаңғыртуға бағытталған практикалық ұсынымдар қалыптастырады.

Түйін сөздер: дипфейк, онлайн-алаяқтық, әлеуметтік инженерия, сотқа дейінгі тергеп-тексеру, биоәлеуметтік криминология, өмірлік жол криминологиясы, цифрлық іздер.

Бивер К.М*
Колледж криминологии и уголовного правосудия Университета штата Флорида, США, Флорида (E-mail: kevinmbeaver@hotmail.com)

Анализ практики досудебного расследования онлайн-мошенничества с использованием deepfake-технологий и социальной инженерии в биосоциальной и жизненно-путевой криминологической перспективе

Аннотация. Статья посвящена исследованию актуальных проблем досудебного расследования онлайн-мошенничества, совершаемого с применением технологий дипфейк и методов социальной инженерии. Основная цель работы заключается в комплексном анализе механизмов цифровых преступлений через призму биосоциальной и жизненно-путевой криминологии для повышения эффективности следственной деятельности. Научная и практическая значимость исследования обусловлена необходимостью адаптации традиционных правовых инструментов к условиям технологической асимметрии и цифровой волатильности. Методология исследования включает анализ типичных криминальных сценариев, изучение специфики цифровых следов и моделирование поведенческих паттернов правонарушителей на основе их криминальных траекторий. Основные результаты демонстрируют многоуровневую структуру преступного механизма и выявляют системные барьеры, такие как быстрая утрата данных и неопределенный процессуальный статус синтетического контента. Автор делает вывод о необходимости формирования междисциплинарных следственных групп и внедрения стандартов оперативной фиксации цифровой среды. Ценность работы заключается в интеграции поведенческого анализа в уголовно-процессуальную деятельность, что позволяет перейти от реактивного реагирования к проактивному профилированию. Практическое значение итогов исследования состоит в возможности совершенствования следственной тактики и модернизации нормативной базы для противодействия высокотехнологичной преступности.

Ключевые слова: дипфейк, онлайн-мошенничество, социальная инженерия, досудебное расследование, биосоциальная криминология, жизненно-путевая криминология, цифровые следы.

Information about the author:

Beaver K.M. **–** PhD, Judith Rich Harris Professor of Criminology, Florida State University, 222 S. Copeland Street, Tallahassee, FL 32306, USA.

Бивер К.М. **–** PhD, криминология профессоры (Judith Rich Harris), Флорида штаты университеті, 222 S. Copeland Street, Таллахасси, FL 32306, АҚШ.

Бивер К.М. **–** PhD, профессор криминологии (Judith Rich Harris), Университет штата Флорида, 222 S. Copeland Street, Таллахасси, FL 32306, США.