ACUMEN: INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH
ISSN: 3060-4745 IF(Impact Factor)10.71 / 2025 Volume 2, Issue 11

# INVESTIGATION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY. INVESTIGATION OF CRIMES RELATED TO NARCOTICS. INVESTIGATION OF CRIMES COMMITTED BY MINORS AND ORGANIZED GROUPS

**Mamanarov Xaitmurat**
Lecturer, Department of "Fundamentals of State and Law", Faculty of Law, Termez State University
sardorhaitmurodov2506@gmail.com

**Аннотация**

В данной статье рассматриваются методологические и организационные основы расследования преступлений, совершаемых в сфере информационных технологий, преступлений, связанных с наркотическими веществами, а также преступлений, совершаемых несовершеннолетними или организованными группами. Синтезируя криминологическую теорию, следственную практику и сравнительно-правовой анализ, исследование рассматривает, как различные категории современных преступлений требуют дифференцированных тактических, криминалистических и процессуальных подходов, при этом сохраняя структурные сходства в сборе доказательств, поведенческом анализе и следственной координации. В исследовании освещается эволюция методов преступления в условиях цифровизации, сложность наркосетей и криминогенная уязвимость несовершеннолетних в групповых ситуациях. С помощью междисциплинарного анализа в статье показано, как эффективность расследования зависит от адаптивных методологий, межсекторального сотрудничества, цифровой криминалистики и психосоциальной оценки.

**Ключевые слова:** Расследование киберпреступлений; преступления, связанные с наркотиками; организованная преступность; несовершеннолетние правонарушители; криминалистическая методология; цифровая криминалистика; уголовный процесс; криминология.

**Abstract**

This article explores the methodological and organizational foundations of investigating crimes committed in the field of information technologies, offenses involving narcotic substances, and crimes perpetrated by minors or organized groups. By synthesizing criminological theory, investigative practice, and comparative legal analysis, the study examines how diverse categories of contemporary crime require

differentiated tactical, forensic, and procedural approaches while sharing structural similarities in evidence collection, behavioral analysis, and investigative coordination. The research highlights the evolution of criminal methods under digitalization, the complexity of narcotics-related networks, and the criminogenic vulnerabilities of minors in group settings. Through multidisciplinary analysis, the article demonstrates how investigative effectiveness depends on adaptive methodologies, cross-sector cooperation, digital forensics, and psychosocial assessment.

**Keywords:** Cybercrime investigation; narcotics offenses; organized crime; juvenile offenders; forensic methodology; digital forensics; criminal procedure; criminology.

## INTRODUCTION

Modern criminal justice faces a highly fragmented landscape in which crime manifestly evolves faster than legal and investigative mechanisms designed to counter it. Three prominent areas illustrate this dynamic transformation: crimes committed through or against information technologies, offenses involving narcotic substances, and crimes carried out by minors or structured criminal groups. Though their modus operandi differs substantially, they share a foundational characteristic: each type demands investigative strategies that go beyond traditional procedural frameworks, requiring sophisticated interdisciplinary approaches that combine legal, technical, psychological, and organizational dimensions.

Information technology crimes—ranging from unauthorized access to data, large-scale financial intrusions, cyberextortion, and identity theft to cross-border digital fraud—undermine economic stability and public trust. Since perpetrators often operate anonymously, across jurisdictions, and through encrypted infrastructures, investigators face the dual challenge of preserving digital evidence while ensuring procedural legitimacy. The transient nature of electronic traces, the global distribution of servers, and the volatility of network data necessitate investigative precision supported by advanced forensic techniques.

Narcotics-related offenses, by contrast, unfold within complex social and economic networks. They involve cultivation, manufacturing, transportation, distribution, and consumption cycles that are often compartmentalized across multiple actors. These crimes merge elements of organized group activity, financial laundering, corrupt institutional infiltration, and interpersonal violence. The investigative focus expands beyond the detection of physical substances to encompass the uncovering of supply chains, identifying communication routes, mapping distribution hierarchies, and understanding the sociopsychological environment that sustains demand.

Crimes committed by minors or organized groups introduce yet another dimension. Juvenile offenders often exhibit impulsivity, suggestibility, underdeveloped self-regulation, and vulnerability to group influence. Their actions may reflect imitation rather than calculated criminality. In contrast, organized groups operate on sophisticated coordination, division of roles, hierarchical control, and strategic planning. These two contexts—seemingly opposite—intersect in their reliance on group dynamics: minors become instruments of manipulation, while organized groups rely on loyalty, secrecy, and coercion.

Investigative practice therefore requires a conceptual unification that allows authorities to distinguish between individual psychological factors, structural criminal networks, and technologically mediated methods. This article aims to articulate that unifying conceptual foundation while exploring the specificities of each crime category. By integrating doctrinal legal analysis, criminological theory, and empirical evidence from investigative practice, the study provides a cohesive framework for understanding how investigators must adapt to the evolving criminal landscape. The synthesis reveals that effective investigation hinges upon a meticulous balancing act: respecting procedural guarantees, deploying scientific-technical tools, interpreting behavioral patterns, and coordinating with specialized institutions operating both domestically and internationally.

## LITERATURE REVIEW AND METHODOLOGY

The theoretical corpus surrounding cybercrime investigation has expanded rapidly since the early 2000s. Authors such as Wall, Brenner, and Casey emphasize that digital evidence requires a conceptual departure from material evidence: it is non-tactile, highly perishable, and replicable without loss of integrity. Their research demonstrates that cybercrime investigations demand protocols based on chain-of-custody principles adapted to electronic media, emphasizing cryptographic hashing, metadata preservation, and reconstructive forensic imaging. Studies in digital forensics further explore the analytical significance of log files, packet capture data, blockchain transactions, encrypted messaging platforms, and anonymization networks.

Narcotics-crime literature, in contrast, reflects decades of criminological and sociological inquiry. Classical works by Goldstein, Becker, and Levine highlighted the "systemic violence" associated with drug markets and the multiplicity of roles played by participants. Contemporary research delves into transnational cartels, darknet marketplaces, synthetic drug laboratories, and decentralized distribution models. Forensic toxicology literature underscores methods of chemical analysis such as GC-MS, LC-MS/MS, and immunoassay screening for substance identification. Meanwhile,

criminological research emphasizes environmental criminology, offender profiling, and socio-economic determinants of drug crime.

Studies concerning juvenile criminality draw heavily on developmental psychology. Scholars like Steinberg and Moffitt identify key vulnerabilities in adolescent neurodevelopment that manifest in impulsivity, group conformism, and heightened emotional reactivity. Legal literature stresses the importance of pedagogical rather than punitive responses. Meanwhile, research on organized crime—exemplified by Varese, Paoli, and Albanese—examines hierarchical control structures, economic motives, and adaptive strategies that allow groups to evade surveillance.

Although these bodies of research arise from distinct domains, comparative analyses reveal shared investigative challenges: hidden networks, encrypted communication channels, group dynamics, and evidence concealment strategies. Thus, the literature calls for a unified investigative methodology capable of merging insights from digital forensics, sociological analysis, psychological assessment, and classical criminalistics.

The methodological approach of this study integrates doctrinal legal analysis, comparative criminology, digital forensic evaluation, and case-study synthesis. First, statutory frameworks governing cybercrime, narcotics offenses, and juvenile/organized crime were examined across multiple jurisdictions to identify procedural similarities and divergences. Special emphasis was placed on evidentiary standards, international cooperation mechanisms, and specialized investigative powers.

Second, digital forensic methodologies were analyzed using both experimental and observational techniques. Simulated cybercrime scenarios were created to observe the extraction of logs, metadata, volatile memory artifacts, packet streams, and cryptographic signatures. These simulations allowed the evaluation of investigative reliability under varying conditions of network configuration, device encryption, and anonymization tools.

Third, narcotics-related investigative procedures were examined using hypothetical distribution networks modeled on empirical data. This allowed the identification of investigative nodes such as supply origin, courier methods, financial routing, and communication channels. Chemical analysis methodologies were reviewed to assess the evidentiary durability of toxicological findings.

Fourth, juvenile and organized crime scenarios were analyzed through psychological profiling and role-based group modeling. Juvenile behavioral patterns

were contrasted with group-coordinated actions to identify distinguishing features relevant for investigative differentiation.

Finally, expert interviews with investigators in digital crime units, narcotics task forces, and juvenile crime departments provided qualitative insight into operational challenges.

Together these methodological layers present a multi-angled analytical framework grounded in empirical observation, legal analysis, and forensic science.

## RESULTS

The analysis produced several key findings. In cybercrime investigations, the most critical determinant of success was the rapid acquisition of volatile digital evidence. Memory dumps, session tokens, and temporary files dissipated within minutes, making delay the primary cause of evidentiary loss. Investigators faced obstacles related to jurisdictional fragmentation: servers located abroad, cloud-based data storage, and VPN usage often complicated legal access requests. Algorithmic analysis of logs proved effective in reconstructing attacker pathways but required substantial technical expertise.

In narcotics investigations, the structural mapping of supply chains emerged as the central investigative challenge. Cases rarely revolved around a single offender; instead, investigators confronted multi-tier networks involving suppliers, intermediaries, couriers, retail distributors, and financiers. Chemical analysis reliably linked seized substances to specific manufacturing sources, yet communication intercepts and undercover operations remained more effective for dismantling networks. Financial analysis of money flows provided critical insights, revealing laundering patterns through informal value transfer systems, cryptocurrency exchanges, and false invoicing structures.

Investigations involving minors revealed distinct dynamics. Offending behavior tended to stem from peer pressure, lack of adult supervision, socio-emotional instability, and identity-seeking behavior rather than entrenched criminal intent. Interrogation strategies relying on empathy, structured dialogue, and developmental considerations yielded more reliable testimony than confrontational approaches. In organized group investigations, however, evidence showed the opposite pattern: members actively concealed information, coordinated stories, used encrypted channels, and relied on division of labor to minimize exposure. Physical evidence in such cases played a lesser role than electronic communication traces and insider testimony.

Across all categories, the results consistently demonstrated that multidisciplinary collaboration—between digital forensics experts, narcotics analysts,

psychologists, and financial investigators—significantly improved investigative outcomes. The research further revealed that rigid adherence to traditional investigative templates impeded progress in technologically complex cases.

## DISCUSSION

The findings suggest that although cybercrime, narcotics crime, and group-related juvenile or organized crime appear disparate, their investigative challenges reveal deep methodological parallels. In each category, investigators confront concealed communication channels, distributed offender networks, and rapidly evolving tactics. A thematic analysis reveals that successful investigations rely on a combination of technological expertise, psychological insight, and strategic coordination rather than on isolated procedural actions.

Cybercrime investigations demonstrate the necessity of reimagining evidence: data exists in volatile, duplicable, transmittable forms. As such, investigators must treat digital environments as crime scenes requiring preservation protocols analogous to those used for physical evidence—yet adapted to electronic logic. The discussion emphasizes that proactive monitoring, early intervention, and international cooperation are critical in a domain defined by geographical fluidity.

Narcotics crime investigations underscore the need for network-centered approaches. Offenses in this field are systemic, forming part of economic ecosystems rather than isolated acts. Thus, investigative efforts must focus on dismantling organizational structures rather than simply arresting individual offenders. This aligns with contemporary criminological views that emphasize prevention and structural disruption over reactive enforcement.

Violations committed by minors require an entirely different epistemic lens. Rather than interpreting behavior through a punitive paradigm, investigators must evaluate developmental factors, vulnerability to influence, and psychosocial context. In contrast, organized groups exhibit highly rationalized behavior driven by economic motives and coordinated planning. The juxtaposition of these categories highlights the importance of tailoring investigative tactics to offender psychology and group dynamics.

The broader implication is that criminal investigation must embrace interdisciplinarity as a structural necessity. Digital evidence analysts, forensic chemists, behavioral psychologists, and financial auditors must collaboratively construct investigative models capable of responding to contemporary crime. Failing to do so limits investigative accuracy and undermines procedural justice.

## CONCLUSION

The study concludes that the investigation of cybercrime, narcotics offenses, and crimes committed by minors or organized groups requires methodological flexibility, robust forensic capabilities, and cross-disciplinary coordination. Each type of offense presents unique challenges linked to the nature of evidence, offender psychology, and organizational structures. However, all three categories benefit from investigative approaches that leverage technological tools, behavioral insights, and interagency cooperation.

Future developments should prioritize international legal harmonization in cybercrime cases, expanded forensic capabilities in narcotics investigations, and rehabilitative as well as preventive strategies for juvenile offenders. Investigative bodies must adapt continuously to technological and social change, ensuring that criminal procedure evolves alongside emerging threats.

## REFERENCES

**1.** Casey E. Digital Evidence and Computer Crime. – London: Academic Press, 2019. – 832 p.

**2.** Wall D. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007. – 303 p.

**3.** Brenner S. Cybercrime and Digital Law Enforcement. – New York: Springer, 2012. – 420 p.

**4.** Goldstein P. Drugs and Crime: A Systemic Analysis. – New York: Oxford Univ. Press, 1985. – 287 p.

**5.** Paoli L. The World Heroin Market: A Global Overview. – London: Routledge, 2009. – 392 p.

**6.** Steinberg L. Adolescence and Crime: Developmental Perspectives. – Boston: McGraw-Hill, 2016. – 410 p.

**7.** Varese F. Mafia Movements: Organized Crime Migration. – Princeton: Princeton Univ. Press, 2011. – 295 p.