



GAPS IN OPERATIONAL-SEARCH LEGISLATION IN THE EARLY DETECTION AND DOCUMENTATION OF THE ACTIVITIES OF ORGANIZED CRIMINAL GROUPS AND WAYS TO ELIMINATE THEM

Shukhrat Ochilovich Begmatov

Lieutenant Colonel, First Deputy Chief of the Main Directorate of
Internal Affairs of Tashkent City

<https://doi.org/10.5281/zenodo.20665280>

ARTICLE INFO

Received: 02nd June 2026

Accepted: 08th June 2026

Online: 09th June 2026

KEYWORDS

Organized crime,
operational-search
activity, early detection,
undercover infiltration,
legalization of evidence,
OSINT, cyber intelligence,
professional risk,
electronic evidence.

ABSTRACT

This article comprehensively analyzes the existing legal gaps in operational-search legislation in the context of the transformation of the activities of organized criminal groups into the digital space. From a scientific and practical perspective, the organizational and tactical problems of transforming operational information into criminal procedural evidence, the legal protection of undercover agents during "operational infiltration," and intelligence activities in cyberspace (OSINT) are revealed. As a result of the research, substantiated proposals were developed for introducing the institution of "electronic operational-search measures" into legislation, consolidating the norm of "justified professional risk" in the Criminal Code, and simplifying the procedure for legalizing digital evidence.

ПРОБЕЛЫ В ОПЕРАТИВНО-РОЗЫСКНОМ ЗАКОНОДАТЕЛЬСТВЕ ПРИ РАННЕМ ВЫЯВЛЕНИИ И ДОКУМЕНТИРОВАНИИ ДЕЯТЕЛЬНОСТИ ОРГАНИЗОВАННЫХ ПРЕСТУПНЫХ ГРУПП И ПУТИ ИХ УСТРАНЕНИЯ

Бегматов Шухрат Очилович

Первого заместителя начальника

Главного управления внутренних дел города Ташкента, подполковника

<https://doi.org/10.5281/zenodo.20665280>

ARTICLE INFO

Received: 02nd June 2026

Accepted: 08th June 2026

Online: 09th June 2026

KEYWORDS

Организованная
преступность,
оперативно-розыскная
деятельность, раннее
выявление,
оперативное внедрение,
легализация
доказательств, OSINT,
киберразведка,

ABSTRACT

В данной статье комплексно анализируются существующие правовые пробелы в оперативно-розыскном законодательстве в условиях трансформации деятельности организованных преступных групп в цифровое пространство. С научно-практической точки зрения раскрыты организационно-тактические проблемы преобразования оперативной информации в уголовно-процессуальные доказательства, правовой защиты негласных сотрудников при проведении «оперативного внедрения», а также разведывательной деятельности в киберпространстве (OSINT). По результатам



профессиональный риск, электронные доказательства.

исследования разработаны обоснованные предложения по внедрению в законодательство института «электронных оперативно-розыскных мероприятий», закреплению в Уголовном кодексе нормы «обоснованного профессионального риска» и упрощению порядка легализации цифровых доказательств.

В современном обществе организованная преступность полностью отказалась от своих традиционных (иерархических, локальных) форм и поднялась до уровня сложных транснациональных систем с глобальной, сетевой и цифровой инфраструктурой. Как отмечает социолог Мануэль Кастельс, фундаментально исследовавший эпоху информации и глобализации, сегодня современная организованная преступность стала неотъемлемой "тенью" глобальной экономики, а их сетевое управление гораздо гибче, чем бюрократические и строго ограниченные правоохранные системы государств¹. На сегодняшний день деятельность организованных преступных групп характеризуется крайне высокой латентностью. По научным наблюдениям американского криминолога Дж. Альбанезе, ОГО настолько глубоко проникают в экономические и социальные институты общества, что визуально отделять их незаконную

деятельность от легального бизнеса становится все труднее².

Такое совершенное маскирование организованной преступности привело к кризису традиционных уголовно-процессуальных подходов. Как отмечает один из видных представителей российской криминологической школы В.В.Лунеев, классические следственные механизмы, адаптированные к борьбе с последствиями преступлений (реактивный подход), показали свою полную беспомощность в борьбе с организованной преступностью³. Также профессор А.И.Гуров, анализируя организованную и профессиональную преступность, обосновал, что поскольку руководители и организаторы ОПГ не являются непосредственными исполнителями преступления, практически нет правовой возможности привлечь их к ответственности за фактически совершенное преступление⁴.

¹ Castells, M. *End of Millennium: The Information Age: Economy, Society, and Culture* (Vol. 3). – Oxford: Blackwell Publishers, 1998. – P. 166-170.

² Albanese, J. S. *Organized Crime: From the Mob to Transnational Organized Crime* (7th ed.). – New York: Routledge, 2014. – P. 34-38.

³ Лунеев В.В. *Преступность XX века: мировые, региональные и российские тенденции*. – М.: Норма, 1997. – С. 280-285.

⁴ Гуров А.И. *Профессиональная преступность: прошлое и современность*. – М.: Юридическая литература, 1990. – С. 145-148.



В таких условиях жизненной необходимостью является переход центра тяжести стратегии борьбы с преступностью с метода расследования после совершения преступления на выявление и пресечение преступления на стадии его подготовки и формирования, то есть на проактивную (раннее выявление) превенцию. По мнению американского ученого Х. Абадинского, единственным и наиболее эффективным инструментом проактивного подхода является непрерывная и углубленная оперативно-розыскная деятельность специально уполномоченных органов⁵.

Однако, какими бы широкими ни были организационно-тактические возможности оперативно-розыскной деятельности, ее эффективность напрямую зависит от правовых гарантий и совершенства законодательной базы. Крупные исследователи теории и практики ОРФ В.С.Овчинский и К.К.Горяинов, оценивая состояние современного оперативно-розыскного законодательства, подвергают резкой критике тот факт, что в условиях миграции преступных группировок в цифровое пространство действующие законодательные нормы, вместо правовой защиты оперативных

сотрудников, зачастую сковывают их деятельность⁶. В законодательстве сохраняются серьезные пробелы в вопросах порядка проведения оперативно-розыскных мероприятий по раннему документированию криминальной деятельности ОГО и легализации полученных результатов в качестве допустимых доказательств в уголовном процессе.

Как показано в фундаментальных работах профессора А.Ю.Шумилова, посвященных основам ОРЗ, диспропорции (коллизии) между оперативно-розыскным законодательством и Уголовно-процессуальным кодексом зачастую приводят к потере доказательной значимости в суде уникальных оперативных данных, накопленных годами⁷.

Это мнение поддерживают зарубежные криминологи, в частности, немецкий исследователь Клаус фон Лампе и российский ученый В.А. Номоконов, которые подчеркивают, что консервативность национального законодательства служит наиболее удобным "правовым щитом" для транснациональной преступности при раскрытии сетей организованной преступности⁸.

Исходя из этого, в данной научной статье проводится

⁵ Abadinsky, H. *Organized Crime* (11th ed.). – Boston: Cengage Learning, 2016. – P. 290-295.

⁶ Горяинов К.К., Овчинский В.С. *Оперативно-розыскная деятельность: Учебник* (2-е изд.). – М.: ИНФРА-М, 2018. – С. 112-115.

⁷ Шумилов А.Ю. *Курс основ оперативно-розыскной деятельности*. – М.:

Издательский дом Шумиловой И.И., 2006. – С. 204-208.

⁸ Номоконов В.А. *Транснациональная организованная преступность: дефиниции и реальность*. – Владивосток: Изд-во Дальневосточного университета, 2001. – С. 88-92.



комплексный анализ основных правовых пробелов, возникающих в процессе раннего выявления и документирования в уголовно-процессуальном порядке деятельности организованных преступных групп на стадии их формирования и подготовки, а также предлагаются инновационные законодательные решения по их устранению.

Деятельность организованных преступных групп коренным образом отличается от обычных преступлений своим долгосрочным планированием, строгим распределением обязанностей и уровнем конспирации. Цель оперативно-розыскной деятельности сводится к раннему выявлению и уничтожению этих групп до того, как их преступный замысел превратится в реальное действие, то есть на стадии "формирования" и "подготовки." Как отмечает крупный российский криминолог А.И. Долгова, изучавшая организованную преступность, наиболее уязвимым пунктом ОПГ является его "инкубационный" период (формирование и сговор), но именно этот период является наиболее сложным процессом юридической квалификации и документирования преступления⁹.

Одним из самых больших пробелов в нашем национальном уголовно-процессуальном законодательстве являются взаимные коллизии между нормами

Закона "Об оперативно-розыскной деятельности" и требованиями Уголовно-процессуального кодекса. Ценные сведения, полученные в результате оперативно-розыскных мероприятий (например, прослушивание телефонных переговоров, оперативное наблюдение и т.д.), сами по себе не могут служить доказательствами по уголовному делу. Они приобретают статус допустимых доказательств только после их легализации в порядке УПК.

Известный российский ученый-процессуалист Е.А. Доля фундаментально исследует проблемы превращения оперативно-розыскных данных в доказательства и резко критикует правовые барьеры в этом процессе. Согласно концепции ученого, чрезмерная консервативность уголовно-процессуального законодательства сводит информацию, полученную оперативными сотрудниками, к уровню простого "сигнала" или "предположения"¹⁰. На практике во многих случаях оперативные службы фиксируют с помощью скрытых аудио/видео средств, что члены ОПГ вступают в преступный сговор или планируют транснациональный наркотрафик. Однако в связи с тем, что эти материалы были собраны до возбуждения официального уголовного дела или не были в полной мере соблюдены формальности УПК (например, участие понятых),

⁹ Долгова А.И. *Криминологические оценки организованной преступности и коррупции*. – М.: Норма, 2011. – С. 210-213.

¹⁰ Доля Е.А. *Формирование доказательств на основе результатов оперативно-розыскной деятельности*. – М.: Проспект, 2014. – С. 85-88.



судебные и следственные органы вынуждены отклонить их как недопустимые доказательства.

Научные выводы профессора В.А.Азарова также более глубоко раскрывают эту проблему. Он отметил, что именно этими "процессуальными лазейками" умело пользуются лидеры ОПГ и их высококвалифицированные адвокаты¹¹. Адвокатам удается интерпретировать действия оперативного сотрудника, направленные на раскрытие проступка, как "провокацию" (подстрекательство к преступлению) или исключить полученные оперативные сведения из доказательной базы, ссылаясь на нарушение процессуальной формы. В результате сложные оперативные разработки, проводившиеся месяцами или годами, теряют свою юридическую силу.

Кроме того, сегодня процесс легализации оперативных данных сталкивается с совершенно новым и ждущим своего решения кризисом в цифровой среде (киберпространстве). Современные ОУГ осуществляют взаимодействие через зашифрованные мессенджеры (Telegram, Signal) и Dark Web. Один из ведущих мировых экспертов по киберпреступности и цифровым доказательствам, австралийский криминолог П. Грабоски, проанализировав оперативно-розыскную деятельность в цифровом

пространстве, показал, что чрезвычайно нестабильная (переменчивая и быстро уничтожаемая) природа электронной переписки и крипто-транзакций совершенно не соответствует традиционным уголовно-процессуальным нормам¹².

В нашем национальном оперативно-розыскном законодательстве до сих пор не получили своего правового статуса такие современные институты, как "электронное оперативно-розыскное мероприятие" или "оперативная фиксация и заморозка цифровых следов." Поскольку механизм легализации оперативных данных, полученных оперативниками с серверов или облачных (cloud) баз, четко не прописан в УПК, следователи сталкиваются с трудностями при их признании в качестве вещественных доказательств. Это, в свою очередь, резко снижает возможности раннего выявления и предотвращения высокотехнологичных преступных проектов ОПГ.

Тот факт, что организованная преступность имеет крайне закрытую и иерархическую (или сетевую) структуру, резко ограничивает возможность ее раскрытия с помощью внешнего наблюдения или традиционных оперативных методов. В такой ситуации наиболее высоким и эффективным тактическим методом разрушения деятельности организованной преступной группы

¹¹ Азаров В.А., Тарасов А.А. и др. *Использование результатов ОРД в доказывании по уголовным делам.* – М.: Юрлитинформ, 2018. – С. 142-145.

¹² Grabosky P. *Cybercrime (Oxford Handbooks in Criminology and Criminal Justice).* – Oxford University Press, 2013. – P. 112-115.



изнутри и заблаговременного документирования их преступных намерений является мероприятие "Быстрое внедрение." Однако именно это важное оперативно-розыскное мероприятие сегодня не может в полной мере реализовать свой потенциал из-за серьезных организационно-правовых проблем и отсутствия законодательных гарантий.

Американский ученый Г.Маркс, фундаментально исследовавший скрытую деятельность органов внутренних дел и практику оперативного ввода, в своих работах раскрывает "правовой парадокс" этого процесса. Ученый отмечает, что тайный агент, чтобы войти в полное доверие преступной группы и сохранить свою "легенду," в большинстве случаев вынужден принимать непосредственное участие в мелких и средних незаконных действиях, совершаемых группой. Это создает чрезвычайно сложную юридическую дилемму превращения представителя государства в соучастника преступления¹³.

В нашем национальном оперативно-розыском законодательстве недостаточно детально прописаны процессуальные гарантии, освобождающие оперативного сотрудника или содействующее лицо от уголовной ответственности за это "принудительное участие" (обоснованный риск - институт обоснованного риска). Видный

представитель теории оперативно-розыскной деятельности, профессор А.Г.Маркушин, анализируя эту проблему, справедливо отмечает: "Если в законодательстве не будет создана гарантия абсолютной неприкосновенности действий сотрудника, осуществляющего оперативное проникновение, с целью предотвращения преступления или устранения более серьезного ущерба (имитация преступления), деятельность всего секретного аппарата придет в состояние паралича"¹⁴. На практике неопределенность границ правовой защиты оперативных сотрудников отталкивает их от инициативы и вынуждает переходить на другие, более "безопасные," но менее эффективные методы.

Следующий, самый крупный и современный пласт организационно-тактических проблем связан с ранним выявлением деятельности ОПГ в цифровом пространстве (киберпространстве). Сегодня логистические центры, вербовщики и финансовые транзакции транснациональных преступных группировок переместились в скрытые слои интернета. Как отмечает известный британский киберкриминолог Д.Уолл, информационные технологии разрушили традиционную "пирамидальную" иерархию организованной преступности, превратив их в "децентрализованные криминальные сети," которые не

¹³ Marx G. T. *Undercover: Police Surveillance in America*. – University of California Press, 1988. – P. 55-58.

¹⁴ Маркушин А.Г. *Оперативно-розыскная деятельность: Учебник для вузов*. – М.: Юрайт, 2012. – С. 234-236.



знают друг друга в реальной жизни, а объединяются только в виртуальном пространстве¹⁵.

В таких условиях традиционные методы физического оперативного наблюдения или сбора вещественных доказательств совершенно бесполезны. Их место должны занять оперативно-розыскные мероприятия нового поколения, такие как разведка открытых источников (OSINT - Open Source Intelligence), "виртуальное проникновение" и кибер-наблюдение. Однако в действующем национальном законодательстве до сих пор не определен правовой статус этих инновационных тактических приемов.

Например, если оперативный сотрудник создает себе поддельный профиль в социальных сетях, заходит в закрытые Telegram или WhatsApp-каналы организованной преступной группы и фиксирует там преступную переписку, что это за мероприятие? В законе нет четкого ответа на вопрос, является ли это "мониторингом электронной переписки" (для этого требуется санкция суда), "оперативным наблюдением" или "мониторингом технических каналов связи." Из-за неопределенности юридического статуса критически важные электронные доказательства, полученные посредством ОСИИТ и киберразведки, IP-адреса и история транзакций криптокошельков часто отклоняются в судебно-следственной практике как недопустимые доказательства. Это дает

современным УГО ощущение абсолютной безнаказанности в киберпространстве и технологическое превосходство над оперативно-розыскными системами государства.

Проведенные нами криминологический, оперативно-тактический и уголовно-процессуальный анализы показывают, что в то время как деятельность организованных преступных групп сегодня полностью перешла в цифровое пространство и приобрела сетевой и децентрализованный характер, традиционные (реактивные) подходы правоохранительных органов и действующее оперативно-розыскное законодательство не могут адекватно реагировать на эти угрозы. Процессуальные барьеры при легализации оперативной информации и правовые пробелы при проведении специальных оперативных мероприятий резко снижают возможности раннего предупреждения транснациональной преступности.

В целях устранения данных проблем и адаптации национального оперативно-розыскного законодательства к современным угрозам мы выдвигаем следующие концептуальные и научно-практические предложения:

Во-первых, внедрение в законодательство института "Электронные оперативно-розыскные мероприятия."

¹⁵ Wall D. S. *Cybercrime: The Transformation of Crime in the Information Age*. – Polity Press, 2007. – P. 45-48.



Необходимо внести новую статью в Закон Республики Узбекистан "Об оперативно-розыскной деятельности," в которой необходимо определить строгий правовой статус оперативных мероприятий нового поколения, таких как "Разведка открытых электронных источников," "Виртуальный (цифровой) доступ" и "Оперативная фиксация и замораживание электронных следов." В частности, необходимо признать, что проникновение оперативного сотрудника в закрытые группы ОПГ с помощью ложного профиля (аватара) является законным оперативно-розыскным мероприятием, осуществляемым без санкции суда.

Во-вторых, включить в Уголовный кодекс норму "Обоснованный профессиональный риск." В целях процессуальной защиты оперативного сотрудника или агента, тайно включенного в УГО, предлагается добавить новую норму в главу "Обстоятельства, исключающие преступность деяния" нашего национального Уголовного кодекса. Согласно этой норме: "Исключается уголовная ответственность за менее тяжкие преступления (имитация

преступления), совершенные принудительно лицом, осуществляющим оперативное проникновение в целях предотвращения тяжких или особо тяжких преступлений, разоблачения организованной преступной группы, для сохранения своей легенды и вступления в доверие к преступной группе."

В-третьих, упрощение процедуры легализации оперативно-розыскных данных. Пересмотр соответствующих статей Уголовно-процессуального кодекса и создание механизма признания результатов оперативно-розыскных мероприятий, таких как аудио-и видеозаписи, электронная переписка и история крипто-транзакций, непосредственно в качестве вещественных доказательств по уголовному делу. При этом в законе должно быть закреплено, что допустимость этих электронных доказательств гарантируется не участием понятых, а криптографическими (ХЭШ) алгоритмами и заключениями цифровой экспертизы, подтверждающими их неизменность.