

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МИНИСТЕРСТВА
ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(ФГКОУ ВО РЮИ МВД России)

**ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ:
АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ**

**Сборник научных трудов
Всероссийской научно-практической конференции**

24 октября 2025 года

Ростов-на-Дону
2026

© ФГКОУ ВО РЮИ МВД России, 2026
ISBN 978 5 89288 607 9

УДК 351.745.7 (08)

ББК 67.7

О 608

Рецензенты:

А. А. Рясов, профессор кафедры уголовного процесса и криминалистики
Ставропольского филиала Краснодарского университета МВД России,
кандидат юридических наук, доцент;

А. А. Шмидт, начальник кафедры оперативно-разыскной деятельности органов внутренних
дел Барнаульского юридического института МВД России,
кандидат юридических наук, доцент

Составитель – **Яцкина Инна Александровна**, кандидат юридических наук

О 608 Оперативно-розыскная деятельность: Актуальные вопросы теории и практики применения [Электронное издание] : сборник научных трудов Всероссийской научно-практической конференции (24 октября 2025 г.) / под ред. А. В. Варданяна. Электрон. дан. (1,26 МБ). – Ростов-на-Дону : ФГКОУ ВО РЮИ МВД России, 2026. — 1 электрон. опт. диск (CD-R). — Систем. требования: IBM PC, 1 GHz; 512 mb оперативной памяти; 3 mb ОЗУ; CD/DVD-ROM дисковод; операционная система Windows XP и выше; Adobe Acrobat Reader 8.0 и выше.

ISBN 978 5 89288 607 9

Сборник подготовлен по итогам Всероссийской научно-практической конференции. В материалах сборника освещаются актуальные вопросы теории и практики оперативно-розыскной деятельности, рассматриваются современные аспекты совершенствования борьбы с преступными посягательствами.

Предназначен для научно-педагогических работников, докторантов, адъюнктов образовательных организаций МВД России, сотрудников правоохранительных органов Российской Федерации.

Выпускается по решению редакционно-издательского совета
ФГКОУ ВО РЮИ МВД России.

ISBN 978 5 89288 607 9

УДК 351.745.7

ББК 67.7

© ФГКОУ ВО РЮИ МВД России, 2026

СОДЕРЖАНИЕ

Ананьян Е.Н. Проблемы, возникающие при проведении оперативно-розыскных мероприятий в отношении этнических преступных групп	5
Апарин С.В. Перспективы оперативно-розыскной деятельности в условиях цифровизации общества	10
Бондарева Г.В. К вопросу об использовании результатов оперативно-розыскной деятельности при выявлении и расследовании коррупционных преступлений	14
Делов Н.С. Оперативно-розыскная характеристика и оперативно-розыскные мероприятия по преступлениям, связанным с захватом заложников.....	20
Дудниченко А.Н. К вопросу об условиях проведения оперативно-розыскных мероприятий.....	30
Карпика А.Г. Оценка состояния киберпреступности в Российской Федерации	36
Коновалов С.И. Определение понятия «оперативно-розыскное сопровождение» расследования преступлений.....	41
Корниленко А.В. Системная деятельность государства по противодействию киберпреступности.....	47
Коряк Ю.Д. Отождествление личности как оперативно-розыскное средство выявления и разоблачения способов маскировки преступной деятельности.....	53
Кулахсзян С.К. Служебная провокация преступления как способ преступного противодействия правосудию	58
Кулешова Ю.Г. Современные возможности генетической экспертизы при расследовании преступлений прошлых лет: анализ эффективности и ограничение метода.....	63
Лемайкина С.В. Возможности прогнозирования и предупреждения преступлений на основе анализа паттернов	67
Маилян А.В. Проблемы взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности	73
Максимов М.И. Проблемы осуществления оперативно-розыскной деятельности в сфере киберпреступности.....	77
Малянова К.П. Актуальные проблемы наложения ареста на криптовалютные активы	83

Миронов Г.Ю. Проблема противодействия распространению наркотиков через социальные сети	90
Мясников А.П. Проблемные вопросы использования результатов оперативно-розыскной деятельности оперативных подразделений уголовно-исполнительной системы Российской Федерации	98
Назаров С.Н. Информационные технологии, применяемые в оперативно-розыскной деятельности	104
Пономарева А.В. Особенности раскрытия преступлений, связанных с незаконной предпринимательской деятельностью	110
Семенцова И.А., Малявина А.Б. К вопросу об информационном обеспечении оперативно-розыскной деятельности органов внутренних дел	120
Снежкова Ж.Ю. Особенности правового регулирования деятельности субъектов оперативно-розыскной деятельности ОВД	126
Сторожева М.В. Современные методы выявления коррупционных связей при расследовании хищений бюджетных средств	132
Тишкин Д.Н., Крицкая А.А. Актуальные аспекты совершенствования ОРД в сфере противодействия организованной преступной деятельности	137
Торопов Д.С. Организованная преступность: оперативно-розыскная характеристика, меры оперативно-розыскного противодействия	144
Точилкина А.А. Деятельность оперативных подразделений по противодействию преступлениям, совершаемым иностранными гражданами	149
Шувалов А.П. Актуальные вопросы применения методов оперативно-розыскного прогнозирования с целью выявления латентных преступлений	157
Щербаченко А.К., Серебрянников С.В. Деятельность сотрудников уголовного розыска по оперативному сопровождению уголовных дел в суде	164
Ягодина Э.А. Противодействие киберпреступности методами оперативно-розыскной деятельности	168
Яцкина И.А. Особенности выявления признаков незаконной предпринимательской деятельности	175

ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ В ОТНОШЕНИИ ЭТНИЧЕСКИХ ПРЕСТУПНЫХ ГРУПП

Ананьян Е.Н.

Старший преподаватель кафедры криминалистики
и оперативно-розыскной деятельности
Ростовского юридического института МВД России

В современном мире перед сотрудниками правоохранительных органов, осуществляющих оперативно-розыскную деятельность, возникают новые вопросы, связанные с ростом организованной преступности, в том числе с участием этнических преступных групп. В условиях активного роста миграционного потока данный вопрос постепенно трансформируется в угрозу национальной безопасности России, заключающую в себе рост международной, межэтнической и религиозной напряженности. Транснациональная организованная преступность все чаще использует этнический фактор в целях укрепления и маскировки своей деятельности.

Перед тем как перейти к рассмотрению проблематики вопроса, необходимо выявить ключевые признаки понятий «организованная преступность» и «этническая преступность». Как правило, под этнической преступностью подразумевают преступления, совершаемые организованными группами, сформированными с целью совершения преступлений и неустойчивыми группами, сложившимися стихийно без предварительного сговора. Данный вид образуют группы, которые совершают преступления, главным образом, на бытовой почве, личной неприязни, из хулиганских побуждений или под влиянием одномоментных порывов криминального характера, в основном в целях завладения чужим имуществом, изнасилования

или унижения человеческого достоинства представителя другой национальности [3].

В научной литературе организованная преступность определяется как форма преступного посягательства, выраженная в участии двух и более лиц в организованно-управленческой и материально-финансовой структуре, а также имеющая устойчивый и профессиональный характер. Этнические преступные формирования обладают характерными признаками организованной преступности, возникают на основе контакта общества с представителями культурно и социально дистанцированного от него этнического меньшинства. Высокая степень этнокультурной сплоченности, выраженная в знании родного языка, соблюдении традиций и религиозных норм, способствует формированию устойчивых горизонтальных и вертикальных связей внутри сообщества. Члены преступных этнических организаций зачастую объединены не только этнической идентичностью, но и родственными, земляческими и клановыми связями, что затрудняет проникновению в их группы внешних лиц и тем более представителей правоохранительных органов.

Проблематика раскрытия преступлений, совершенных этническими преступными формированиями, встала перед органами внутренних дел в СССР в конце 1970-х годов. Ранее в официальной коммунистической идеологии понятие «этническая преступность» не признавалось, попытка связать противоправные деяния с национальным фактором считалась проявлением «буржуазного национализма» или «великодержавного шовинизма». Национальный состав преступников не публиковался, любая информация подобного характера была засекречена. Расцвет организованной преступности пришелся на постсоветский период, в период коренного изменения основного закона страны — Конституции Российской Федерации и других отраслей законодательства. В условиях ослабленного государства и перелома в деятельности правоохранительных органов организованные преступные группы стали доминировать в таких сферах теневого бизнеса, как торговля оружием, сбыт наркотических веществ, контрабанда.

В современном мире рост тенденции к глобализации обуславливает ускоренное и упрощенное перемещение людей между границами государств, что приводит к интернационализации преступности. В России мигранты совершают относительно небольшую долю преступлений, однако в последние годы наблюдаются определенные изменения, вызывающие обеспокоенность. В 2022 г. мигранты и лица без гражданства совершили около 2 % от общего числа преступлений в России, что составляет примерно 40 150 случаев. В 2023 г. общее количество преступлений, совершенных мигрантами, снизилось на 3 % по сравнению с предыдущим годом, но количество тяжких и особо тяжких преступлений увеличилось на 26–32 %.

Председатель Следственного комитета Российской Федерации А.И. Бастрыкин, выступая на Петербургском международном юридическом форуме, отметил, что в первые три месяца 2025 г. рост числа преступлений, совершенных мигрантами, увеличился на 15 %, составив в абсолютных числах 12 440.

В 2022 г. количество тяжких и особо тяжких преступлений, совершенных мигрантами, увеличилось на 37 % по сравнению с предыдущим годом. В 2024 г. число преступлений, совершенных детьми мигрантов, выросло на 8 %, при этом количество тяжких преступлений увеличилось на 82 %. В Москве за первое полугодие 2024 г. зафиксировано 103 преступления против несовершеннолетних, совершенных иностранными гражданами, что на 87,3 % больше, чем за аналогичный период 2023 г.

К проблемам, возникающим при проведении оперативно-розыскных мероприятий в отношении этнических групп, в первую очередь, относится отсутствие в законодательной базе правового понятия «этническая преступность», что создает неопределенность в выработке единого подхода к квалификации и эффективной профилактике преступлений, совершаемых представителями определенных этнических групп или на межнациональной почве. Как отмечалось ранее, к определению данного явления можно непосредственно обратиться через научную криминологическую

и социологическую литературу. Для эффективного проведения оперативно-розыскной деятельности, требуется четкое и точное закрепление понятия «этническая преступность» в нормативных правовых актах Российской Федерации [1]. Однако, подходя к данному вопросу с иной стороны, стоит отметить, что в таком случае законодателю необходимо сохранить тонкую грань между составлением новой правовой базы или внесением поправок в уже существующую и возможным нарушении конституционных прав и свобод человека и гражданина. Отсутствие законодательной регламентации формирует возрастание рисков правонарушений в области разжигания национальной розни и ксенофобии, поскольку термин может быть использован как в обвинительном, так и в политически мотивированном контексте. На фоне возрастающего уровня миграции и межэтнической напряженности в ряде регионов России, вопрос формализации понятия «этническая преступность» требует четких критериев.

При проведении оперативно-розыскных мероприятий зачастую возникают проблемы, связанные с проникновением в закрытые этнические сообщества. Одним из ключевых факторов возникновения трудностей проникновения является языковой и культурный барьер [2]. Во многих этнических диаспорах внутри России (таджикская, узбекская, азербайджанская) общение преимущественно ведется на родных языках. Кроме того, нормы поведения внутри таких сообществ регулируются неформальными правилами и традициями, в том числе обычным правом, авторитетом старейшин, религиозных лидеров или криминальных лиц. В закрытых сообществах также имеет место параллельная социальная инфраструктура, включающая в себя собственные рынки труда, механизмы разрешения конфликтов (шариатский суд, адаты). Данные факторы обуславливают отсутствие доверия закрытого этнического сообщества к правоохранительным органам, способствуют тому, что при наличии информации о преступной деятельности, представители сообщества не передадут ее исполнительным органам власти, предпочтя решить возникший вопрос «внутри». Выявленные характерные черты приводят

к сложностям при получении достоверной информации изнутри этнических сообществ, формировании сети информаторов, а также при проведении профилактической работы среди иностранных граждан.

В заключение необходимо отметить, что проведение оперативно-розыскных мероприятий в отношении этнических преступных групп выражает сложный характер поставленных задач через ряд выявленных выше проблемных вопросов, содержащих в себе этнокультурную сплоченность, высокий уровень внутренней организованности, языковые и религиозные барьеры. Анализ выявил, что существующие проблемы носят как правовой, так и организационный характер, требующий совершенствования нормативно-правовой базы оперативно-розыскной деятельности, развитие механизмов взаимодействия с представителями диаспор.

Литература

1. Ахмедов А.Г., Насыров Р.Р. Актуальные вопросы оперативно-розыскного противодействия этнической преступности // Вестник Уфимского юридического института. 2024. № 2(104).

2. Лесников Г.Ю., Фомин И.С. К вопросу о правовом регулировании оперативно-розыскной деятельности в сфере предупреждения правонарушений групп отрицательной направленности, сформированных по этническому признаку // Право и государство: теория и практика. 2021. № 6(198).

3. Щукин А.М. Оперативно-розыскная характеристика этнических преступных групп // Научно-методический электронный журнал «Концепт». 2016. № 17.

© Ананьян Е.Н., 2025

ПЕРСПЕКТИВЫ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Апарин С.В.

Старший преподаватель кафедры
информационно-коммуникационных технологий и кибербезопасности
Ростовского юридического института МВД России

С появлением всемирной паутины Интернет, жизнь людей кардинально изменилась. У людей появился доступ к большому объему информации, увеличилась коммуникация между ними, но вместе с этим появились и новые виды преступлений, связанные с сетью Интернет.

С начала XXI в. общество постепенно начало двигаться в сторону всеобщего развития технологий, программ и аппаратных обеспечений, т. е. началась цифровизация общества. Также и преступники идут в ногу со временем, они начали вести свою противоправную деятельность на просторах Интернета. Появились новые виды преступлений, такие как:

1. Мошенничество в сети Интернет.
2. Кража (взлом) персональных данных.
3. Распространение вредоносных вирусов.
4. Кибер-сталкинг (когда на пользователя обрушивается множество сообщений, с «неприятным» содержанием).

Поскольку киберпреступники постоянно придумывают новые схемы совершения преступлений, сотрудникам правоохранительных органов также приходится развиваться. Государство, с появлением новых видов или новых способов преступлений, совершенствует свою законодательную базу.

Первыми, кто сталкивается с последствиями преступной деятельности — это оперативные сотрудники. Сотрудники оперативных подразделений практически ежедневно сталкиваются с новыми преступлениями, в связи с этим

у них не остается другого выхода, как совершенствоваться в этой сфере, т. к. по-другому противостоять протестному сообществу невозможно.

Развитие цифровой сферы создает как новые возможности, так и вызовы для сотрудников оперативных подразделений. Благодаря новым технологиям, таким как искусственный интеллект, нейросети, автоматизированное программное обеспечение, деятельность оперуполномоченных намного облегчилась. Появились новые возможности получения информации, причем гораздо быстрее, чем по старым методам, но и вместе с этим сотрудники сталкиваются с новыми проблемами. Проблема исследования заключается в необходимости найти баланс между использованием цифровых технологий (анализ больших данных, искусственный интеллект, биометрия) для повышения эффективности оперативно-розыскной деятельности и защитой конституционных прав граждан на неприкосновенность частной жизни, тайну переписки и телефонных переговоров, а также в обеспечении законности и прозрачности оперативно-розыскных мероприятий в условиях растущей анонимности и трансграничного характера киберпреступности. Это требует совершенствования законодательства, разработки этических кодексов, внедрения механизмов контроля и подготовки высококвалифицированных специалистов, способных эффективно и законно использовать цифровые инструменты для борьбы с преступностью. В связи с этим требуется усовершенствование Федерального закона Российской Федерации «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ, в том числе ст. 4 данного Закона, т. к. эта статья регламентирует организацию и тактику проведения оперативно-розыскных мероприятий.

В настоящее время уже существуют все необходимые условия для развития и усовершенствования деятельности оперативных подразделений. Создаются новые возможности такие как:

- Использование больших объемов данных с помощью искусственного интеллекта — анализ больших объемов данных позволяет выявить преступные

действия, а также проводить прогнозирование новых возможных преступлений и обнаружить связи между фигурантами.

- Цифровые следы и киберразведка — практически любое преступление оставляет следы, точно так же и преступления в Интернете оставляют свой цифровой след, с помощью которого можно выйти на лицо, его совершившее.

- Блокчейн-анализ — хотя использование криптовалюты в процессе отмыwania денег усложняет процесс выявления противоправной деятельности, существуют такие программы, как Chainalysis, которые позволяют выявлять незаконные денежные операции.

- Автоматизации взаимодействия между подразделениями — внедрение цифровых платформ ускорит обмен информацией между подразделениями, ведомствами, что существенно облегчает документооборот.

Несмотря на это за 2024 г. в сети Интернет было совершено около 477 тыс. преступлений, удельный вес которых составляет 26,5 % от общего количества преступлений, совершенных за год. По заявлению Министра Внутренних Дел Российской Федерации В.А. Колокольцева за последние 5 лет киберпреступность выросла более чем в два раза. Из них 84 % было совершено с использованием интернет-технологий. Наиболее распространенными киберпреступлениями в России являются: мошенническая (ст. 159 УК РФ) — 52 % от общего числа преступлений; кражи (ст. 158 УК РФ) — в том числе кражи личных данных, нарушающих ст. 24 Конституции РФ; незаконный оборот наркотических веществ и психотропных препаратов в сети Интернет (ст. 228 УК РФ) — 12 %.

В связи с этим выделяются перспективные направления для развития оперативно-розыскной деятельности:

1. Необходима разработка AI-платформ — для прогнозной аналитики.
2. Создание специализированных киберподразделений в правоохранительных органах — по возможности с привлечением хакеров «Белые шляпы» (White Hat Hackers), которые будут выявлять недостатки систем безопасности, сетей и давать рекомендации по их улучшению.

3. Развитие OSIT-инструментов — для мониторинга социальных сетей, сети Darknet и криптовалютных транзакций.

4. Использование квантовой криптографии — для защиты данных правоохранительных органов, в том числе баз данных.

5. Разработка законодательства, четко регулирующего правила использования средств массового слежения для избегания злоупотребления, как было с крупнейшим телеграмм-ботом «Глаз бога», который за определенную плату предоставлял пользователям личные данные людей.

Таким образом, цифровизация общества делает оперативно-розыскную деятельность более эффективной, но требует также адаптации и усовершенствования методов ОРД по раскрытию преступлений, улучшение законодательной базы в сфере цифрового регулирования. Главной тенденцией является переход от традиционного личного сыска к смешанным (гибридным) оперативно-розыскным мероприятиям.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993). Доступ из справ. правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

3. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

4. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

© Апарин С.В., 2025

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ РЕЗУЛЬТАТОВ ОПЕРАТИВНО- РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ

Бондарева Г.В.

Профессор кафедры криминалистики
и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук, доцент

В за девять месяцев 2025 г. подразделения Следственного комитета Российской Федерации возбудили более 24 тыс. уголовных дел по коррупционным статьям, что на 16 % больше, чем за аналогичный период 2024 г. Всего было расследовано почти 26,2 тыс. коррупционных преступлений (на 22,5 % больше аналогичного периода прошлого года), в том числе 19 тыс. — по тяжким и особо тяжким статьям [1].

В настоящее время проблемы комплексного расследования преступлений коррупционной направленности обусловлены сложностью установления различных обстоятельств дела. Обобщение и сравнение результатов оперативно-служебной деятельности в сфере расследования коррупционных преступлений демонстрируют, что высокий уровень раскрываемости и привлечения к уголовной ответственности зависит от организованного оперативного сопровождения. Эффективное взаимодействие между оперативными подразделениями и следственными органами является одной из ключевых задач в этой области. Это сотрудничество позволяет более эффективно выявлять и пресекать коррупционные правонарушения, что, в свою очередь, способствует повышению общей правопорядка и доверия к правоохранительным органам.

Выявление и расследование преступлений коррупционной направленности представляет собой комплексный подход и играет ключевую роль в реализации оперативно-розыскной деятельности в борьбе с коррупцией.

Коррупционные преступления по своей природе скрыты и часто не оставляют очевидных следов. Оперативно-розыскная деятельность с использованием негласных методов позволяет выявить скрытые связи, схемы и доказательства коррупционных действий, которые невозможно обнаружить с помощью обычных следственных действий.

Предупреждение и пресечение преступлений при своевременном получении оперативной информации позволяет не только расследовать уже совершенные преступления, но и предотвращать новые. Знание о планируемых коррупционных схемах позволяет принимать упреждающие меры [2]. В случае если предупредить преступление не удалось, то необходимо сосредоточиться на раскрытии преступления. В виду того, что коррупционные схемы часто представляют собой сложную комбинацию, включающую в себя большое количество участников, как должностных лиц, так и представителей бизнеса, оперативно-розыскная деятельность позволяет выявить цепочку участников, их роли и взаимосвязи, а также установить конечного бенефициара.

Для успешной реализации мероприятий по выявлению, раскрытию и противодействию коррупции сотрудникам правоохранительных органов необходимо обладать и использовать в своей деятельности ряд навыков и компетенций, а именно:

- осуществлять сбор и анализ информации из различных источников, анализировать ее;
- выявлять закономерности, связи и признаки коррупционных действий;
- осуществлять наблюдение (гласное и негласное), которое необходимо для установления связей между фигурантами, фиксации встреч и передачи незаконных вознаграждений;
- осуществлять записи переговоров, которые позволят получить ценную информацию о планах, намерениях и деталях коррупционных сделок;

– использовать в своей деятельности оперативно-технические средства, которые в настоящее время постоянно совершенствуются, тем самым упрощают и повышают эффективность реализации оперативной деятельности при раскрытии преступлений, в том числе и коррупционных;

– оперативным сотрудникам осуществлять свои действия в соответствии с установленными законом нормами и процедурами. Это включает получение соответствующих разрешений от компетентных органов, соблюдение прав и свобод граждан, а также обеспечение надлежащей доказательной базы для последующего судебного разбирательства [3];

– документирование деятельности организованных групп и сообществ должно обеспечиваться с соблюдением конспирации для успешности операции. Помимо рассмотренных аспектов реализации оперативной деятельности необходимо учитывать и дополнительные аспекты, к которым относятся:

– контроль появления и распространения коррупции в самих правоохранительных органах, что может повлечь распространение информации преступникам;

– обеспечение строгого внутреннего контроля среди сотрудников правоохранительных органов;

– обеспечение защиты свидетелей, особенно когда осуществляется расследование преступлений совершенных группой или преступным сообществом;

– использование в своей деятельности сотрудниками правоохранительных органов современных информационных технологий.

Актуальной проблемой применения результатов оперативно-розыскных мероприятий (далее — ОРМ) в уголовном процессе также выступает их ограничительный в части конституционных прав и свобод, негласный и конспиративный характер, что само по себе повышает их эффективность, но затрудняет судебный контроль и прокурорский надзор за законностью на допроцессуальной стадии выявления признаков преступления и установления лиц его совершивших. Кроме того, условия проведения ОРМ

в соответствии со ст. 8 Федерального закона «Об оперативно-розыскной деятельности» не детализирует порядок их реализации, ограничиваясь требованиями о целях, уведомлениях, наличии определенной информации. Поэтому ведомственное регулирование выступает здесь основным нормативным регулятором.

Информация, полученная в ходе ОРМ, играет важную роль в уголовном судопроизводстве. Это связано с тем, что уголовное расследование требует использования специальных методов и средств для сбора доказательств, особенно в современных условиях, когда преступления становятся все более изощренными и трудными для расследования. Таким образом, информация, полученная в результате ОРМ, может оказаться критически важной для установления обстоятельств преступления и участников его совершения.

Возбуждение уголовных дел коррупционной направленности без материалов оперативно-розыскной деятельности может быть затруднительным. Фигуранты коррупционных преступлений часто действуют скрытно, используя пробелы в законодательстве и свои коррупционные связи. В таких случаях информация, полученная оперативно-розыскным путем, может стать ключевой для раскрытия коррупционных схем, выявления участников и собраний достаточных доказательств в уголовном деле. Подобная информация позволяет правоохранительным органам эффективнее бороться с коррупцией, т. к. оперативно-розыскные методы обеспечивают доступ к скрытой информации и позволяют выявлять коррупционные схемы, которые могут быть недоступны при использовании обычных методов.

Необходимо расширять возможности использования результатов ОРД в доказывании по уголовным делам и их совершенствования, в том числе путем открытия формы допуска к секретным сведениям следователям, расследующим преступления экономической направленности [4].

Важно понимать, что ошибка при проведении ОРМ относительно события преступления, виновности лица и иных условий их проведения впоследствии сложно устранима в рамках уголовного процесса, следствие

может пойти по неверному пути, а собранные доказательства становятся недопустимыми. Ввиду этого нарушение норм Федерального закона «Об оперативно-розыскной деятельности» и ведомственных норм автоматически ведет к нарушению процессуального порядка формирования доказательственной базы по уголовному делу. Причем некоторые нарушения могут носить неустранимый характер [5].

Если рассматривать преступления коррупционной направленности, то сложилось такое мнение, что рапорт, как документ по своей природе выступает способом процессуального оформления собственно «сообщения о совершенном или готовящемся преступлении», которое, в свою очередь сначала выполняет функцию повода к возбуждению уголовного дела, а потом функцию так называемого «иного документа», выступающего источником доказательственной информации. Представляется, что в контексте ст. 143 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ) целесообразно считать рапорт об обнаружении признаков состава преступления единственным документом представления результатов оперативно-розыскной деятельности, который впоследствии сопровождается постановлением уполномоченного лица о предоставлении результатов оперативно-розыскной деятельности для принятия решения о возбуждении уголовного дела на основании ст. 145 УПК РФ.

Проблема легализации результатов оперативно-розыскной деятельности, имеющих перспективу быть признанными доказательствами со всеми предъявляемыми к ним требованиями, может быть обозначена соблюдением комплекса условий, к которым на основании оперативно-розыскного и уголовно-процессуального законодательства имеет смысл отнести:

- их собирание, проверка и оценка должны осуществляться лицами, перечисленными в ст. 86–88 УПК РФ;
- на них распространяются требования, аналогичные требованиям к доказательствам, предусмотренным УПК РФ (относимость, допустимость, достоверность), а сама информация должна обладать свойством верификации

посредством признания источника ее получения достоверным. Это особо актуально в отношении негласных ОРМ с необходимостью последующего рассекречивания информации. Кроме того, важно указать сведения, которые позволят проверить и оценить доказательства, основанные на проведенных ОРМ.

Таким образом, использование возможностей оперативно-розыскной деятельности позволяет выявлять и раскрывать коррупционные преступления, вместе с тем, нарушение оперативно-розыскного законодательства автоматически ведет к нарушению процессуального порядка формирования доказательственной базы по делам о преступлениях коррупционной направленности. Причем некоторые нарушения могут носить неустранимый характер с двумя видами последствий: вынесение оправдательного приговора (например, отсутствие оснований проведения ОРМ, ненадлежащий орган проведения ОРМ), либо возврат уголовного дела на дополнительное расследование (например, отсутствие обязательной информации в рапорте о представлении результатов ОРМ, ошибка в примененной форме документирования результата ОРМ).

Успешная борьба с коррупцией требует системного и комплексного подхода, в котором оперативно-розыскная деятельность играет ключевую роль. Важно обеспечить правоохранительные органы необходимыми ресурсами, квалифицированными кадрами и современной техникой, а также создать условия для эффективного взаимодействия между различными ведомствами и институтами гражданского общества.

Литература

1. Бастрыкин А. Следственный комитет в 2025 году возбудил более 24 тыс. дел о коррупции [Электронный ресурс]. URL: [https:// www.rbc.ru/politics/09/12/2025/69367d529a7947508c8dd594](https://www.rbc.ru/politics/09/12/2025/69367d529a7947508c8dd594) (дата обращения: 10.10.2025).

2. Харченко С.В., Попова Т.В. К вопросу об оперативно-розыском обеспечении предварительного расследования преступлений // Государственная служба и кадры. 2018. № 3.

3. Солдатов А.В. Оперативно-розыскное обеспечение предварительного следствия по уголовным делам о коррупционных и экономических преступлениях // Научный портал МВД России. 2019. № 1(45).

4. Иванов П.И., Кустов А.М. Оперативно-розыскное сопровождение предварительного расследования экономических и коррупционных преступлений в сфере закупок для нужд оборонно-промышленного комплекса и судебного разбирательства (вопросы организации и тактики) // Труды Академии управления МВД России. 2020. № 1(53).

5. Маркушин А.Г., Аменицкая Н.А. Оперативно-розыскная деятельность полиции в раскрытии и расследовании преступлений: учебник для вузов. М., 2025.

© Бондарева Г.В., 2025

УДК 351.745.7

ОПЕРАТИВНО–РОЗЫСКНАЯ ХАРАКТЕРИСТИКА И ОПЕРАТИВНО– РОЗЫСКНЫЕ МЕРОПРИЯТИЯ ПО ПРЕСТУПЛЕНИЯМ, СВЯЗАННЫМ С ЗАХВАТОМ ЗАЛОЖНИКОВ

Делов Н.С.

Доцент кафедры криминалистики и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

Преступления, связанные с захватом заложников или похищением человека, относятся к тяжким или особо тяжким, и вне зависимости от причин и обстоятельств их совершения рассматриваются как преступления не только против отдельного человека, но и против существования всего общества, т. к. нарушают гарантированные Конституцией Российской Федерации права и свободы человека и гражданина. Государство обязано обеспечить реализацию

конституционно гарантированных прав и свобод, что является незыблемой составляющей существования нашего общества и государства.

Для эффективного выявления и раскрытия таких преступлений необходимо знать элементы оперативно-розыскной характеристики.

Первым элементом является предмет преступного посягательства, а именно общественные отношения в сфере обеспечения общественной безопасности. Но захват заложников многообразен в понимании. В целом такие преступления связывают с действиями террористических и экстремистских организаций. В этом случае вышеуказанное утверждение полностью соответствует событию — своими действиями террористы показывают обществу некомпетентность власти, которая не может обеспечить общественный порядок и личную безопасность каждого гражданина. Захват заложников в исправительных учреждениях, как один из вариантов преступления рассматриваемой категории, миниатюрное подобие террористического акта, но менее глобальной цели — действия направлены на дезорганизацию работы и дискредитацию администрации колонии. Захват заложников при уходе от преследования рассматривается как один из элементов насилия при совершении общеуголовного преступления, в результате которого преследование и происходит.

Второй элемент — обстановка совершения преступления. Тесная связь между этими составляющими максимально выражена именно в этом виде преступлений. Время и место террористами выбирается особенно тщательно. На этот выбор влияют факторы присутствия максимального количества людей, смена дежурства охраной, проверка организации органами полиции или Росгвардии, наличие сигнализации или кнопки экстренного вызова. Охрана объекта играет решающую роль при выборе — отсутствие охраны привлечет однозначно.

Отдельным аспектом стоит время совершения преступления, т. к. захват заложников в большинстве случаев не одномоментный процесс, он включает этапы, распределенные во времени [1].

Как и при совершении любого спланированного мероприятия, на первом этапе осуществляется разведка места совершения преступления. Изучается контингент, время прихода и ухода с объекта, режим работы охраны и расписание занятий, представлений, наличие и функционирование камер видеонаблюдения, реагирование на провокацию. Но могут обойтись и без этой подготовки. Есть объекты, в которые можно войти без предварительной подготовки: больницы, магазины, многофункциональные центры и мн. др.

На втором этапе необходимо обеспечить прибытие террористов без привлечения внимания. В большинстве случаев это не представляет больших трудностей, в большинство организаций вход осуществляется без осмотров и контроля.

На третьем этапе осуществляется непосредственный захват заложников. На этом этапе возможны варианты. В случае длительной подготовки ждут максимального скопления людей. В случае работы «с ходу» этот фактор не важен.

Четвертый этап заключается в удержании заложников либо в месте захвата, либо перемещении их в специально подготовленное помещение, строение или территорию, включая какое-либо транспортное средство.

На пятом этапе террористы перемещают заложников в любое удобное для них место, которых может быть несколько. На количество мест могут повлиять и предварительная подготовка, и складывающаяся обстановка, и предложения при переговорах.

Третьим элементом является способ совершения преступного деяния. Основными способами совершения подобного рода преступлений являются:

- вооруженный захват;
- захват заложников с применением невооруженного насилия;
- захват с применением обмана, но в дальнейшем их удержание происходит с помощью насилия.

Очевидно, что наиболее опасным из вышеперечисленных способов является первый. К такому способу, как правило, прибегают террористические

и экстремистские организации. У таких преступных группировок основными целями являются устрашение населения и максимальное воздействие на органы власти, руководящих должностных лиц или конкретного человека для совершения определенных действий или, наоборот, бездействия для достижения целей преступной группировки. Осуществление захвата вооруженным способом проводится максимально жестко, захват предполагает максимально большое количество заложников, в процессе содержания заложники, зачастую, подвергаются насилию или ликвидируются. Логика террористов проста и очевидна: чем большее количество людей захвачена, тем больше реакция не только властей, но и всего общества на происходящее. Убийство беззащитных заложников, а особенно в «прямом эфире», заставляет органы власти, под воздействием общественного влияния, идти на невероятные уступки. Присутствует и двухэтапность совершения преступлений, связанных с захватом заложников:

- непосредственно захват;
- насильственное удержание.

Возможно развитие событий с возникновением третьего этапа — перемещение заложников в безопасное, с точки зрения захватчиков, место. Одним из вариантов такого развития событий является предоставление, по требованию террористов, транспортных средств — автобусов или самолетов. Как правило, такие ситуации сопровождаются требованием выкупа за заложников, а после его получения, заложники становятся «живым щитом». Побег на средствах транспорта предполагается в другую страну, поддерживающую террористов или негативно относящуюся к России, где за содеянное либо будет незначительное наказание, либо не будет вообще.

Отдельным аспектом стоит захват заложников при уходе от погони от правоохранительных органов. В этом случае преступники могут захватить в заложники людей в магазине, банке, кафе. Целью становится уйти от преследования в обмен на сохранение жизни заложникам. При этом

критическим вариантом развития событий является попытка прорыва через оцепление под прикрытием заложников.

В качестве четвертого элемента выступает следообразование на месте совершения преступления или удержания заложников. Любое событие, совершенное в материальном мире не может не оставить за собой материальных следов. Следы, обнаруженные на месте происшествия, могут иметь доказательственное значение, либо указывать на причастность конкретного лица, либо преступного сообщества. Большинство следов являются скрытыми, невидимыми или слабовидимыми. Их обнаружение требует специальных познаний, но и анализ, обнаруженных на месте происшествия следов дает оперативно значимую информацию для поиска и изобличения преступников. Грамотное исследование обнаруженных на месте происшествия следов и объектов дает направление проведению дальнейших оперативно-розыскных мероприятий.

По делам рассматриваемой категории, для установления всей картины произошедшего, необходимо изучать не только следы преступников, но и следы пострадавших, это позволит воссоздать и механизм, и временное течение преступного события.

Следы преступления обнаруживать необходимо не только на месте происшествия, но и в месте удержания заложников, на местах ожидания, по пути подхода и отхода.

Следы на месте происшествия по данному виду преступлений — это следы обуви, следы взрывчатых веществ и взрывных устройств, баллистические следы (пули, гильзы и следы применения огнестрельного оружия), дактилоскопические следы. В литературе можно встретить ссылки на обнаружение следов транспортных средств на прилегающей территории, но на данный момент информационной значимости они не имеют.

Особое место имеет судебно-медицинское исследование следов крови, следов повреждения на заложниках и следов их сопротивления преступникам.

Следы сопротивления при совмещении со следами повреждений на преступнике дают информацию о происшедшем.

Особую значимость имеет следовая информация при выдвижении требований: текстовая, голосовая, электронная. По имеющимся следам можно выявить судимости, место проживания, уровень интеллекта, образование и некоторые другие личностные параметры преступника. При исследовании мобильных телефонов и планшетов можно установить знакомства и круг общения, а также перемещения.

Большой удачей для оперативных работников является обнаружение планов, схем или письменных распоряжений по проведению террористической акции. Это позволяет установить количество участников, лидера, а иногда и организатора-руководителя. Бывали случаи, что в таких записях содержались сведения о пособниках в государственных структурах и в правоохранительных органах. Составление субъективных портретов, или использование идеальных следов, так же для оперативной работы имеет существенное значение. Однако их использование должно соответствовать методике, а иначе это становится фиктивным делопроизводством.

Пятым элементом выступает способ сокрытия преступления. Захват заложников не направлен на сокрытие самого преступления, наоборот, он проводится с максимальной оглаской и привлечением максимально возможного количества зрителей и средств массовой информации. Преступление скрывается на подготовительном этапе. Сюда включается и провоз оружия и взрывчатки, замаскированными под продукты питания, бытовую технику, сами террористы проникают к месту совершения преступления по одному или мелкими группами, при этом используются фальшивые паспорта, подкуп охраны или сотрудников правоохранительных органов. Не стоит оставлять без внимания такие действия террористов как попытки обойти контроль при захвате самолетов. Осуществляется доставка на борт оружия и взрывчатки под разными видами бытовых приборов, игрушек,

сувениров. Расчет ведется на некомпетентность или халатность полиции, таможни, служб собственной безопасности.

Шестой элемент — характеристика самих террористов. Начнем рассмотрение личностных характеристик с террористов, захватывающих первую вышеприведенную группу заложников.

Эти лица действуют по «наводке», а значит и ключевой фигурой в совершении данного варианта захвата заложников выступает заказчик. Он, прежде всего, приобретает материальные блага или другие ценности от совершенного преступления. Заказчик не руководит операцией и не расписывает каждый шаг, он определяет общий порядок: что нужно сделать и для какой цели. В некоторых ситуациях для четкого исполнения намеченного плана появляется конкретизирующее каждый шаг операции третье лицо — организатор. Бывает, что организатор не пользуется услугами какой-либо террористической ячейки, а создает новую преступную группу из отдельных не связанных до этого между собой участников, которые, нередко, после выполнения операции могут быть им же и ликвидированы. Статья 33 Уголовного кодекса Российской Федерации (далее — УК РФ) не рассматривает заказчика в качестве соучастника преступления, однако такой субъект весьма реален, и надо обратить внимание на то, что именно заказчик является инициатором совершения преступления.

Что же касается личности исполнителя, то ч. 2 ст. 33 УК РФ его рассматривает как «лицо, непосредственно совершившее преступление, либо непосредственно участвующее в его совершении совместно с другими лицами». Другими словами — это конкретный человек, индивидуально или в составе группы осуществляет непосредственный захват заложников, его действиями кто-то руководит, или же он руководит чьими-то действиями или же осуществляет план в действие сам.

Если обратиться к личности организатора, то он должен обладать твердостью воли, быть хорошим организатором—управленцем, разбираться в психологии, обладать способностью выстраивать сложные

и многоструктурные исполнительские планы. Другой его характеристикой является способность в подчинении себе любого человека. Разносторонность мышления, способность принять не стандартное решение в сложившейся ситуации, цинизм и отсутствие эмпатии, хитрость и изворотливость — это те качества, которые приветствуются при выборе организатора. Организатор должен остаться в живых, даже если потребуются уничтожить всю группу.

Непосредственные исполнители могут обладать различными личностными качествами, от них и зависит их роль в захвате заложников. Но все исполнители могут участвовать в операции:

- в осуществлении всего преступления, от планирования до окончания;
- в осуществлении захвата заложников в месте их первоначального нахождения (расположения);
- в осуществлении перемещения потерпевших от места их захвата до места (мест) их дальнейшего удержания;
- в насильственном удержании заложников в определенном месте (местах).

Возрастные характеристики преступников варьируют в пределах 20–35 лет, редко встречаются 18-летние и лица старше 40. Большая часть преступников мужчины, но не исключено активное участие и женщин. Женщин используют для отвлечения внимания, внедрения в структуры и «шахидские» террористические акты.

Преступники в большей своей части уже привлекались к уголовной ответственности по тяжким или особо тяжким преступлениям (убийства, крупные коррупционные преступления), они обижены на власть, и мотивированы финансовой составляющей. Обязательным является владение в совершенстве стрелковым оружием и обращением с взрывными устройствами. Все участники преступной группы решительны, жестоки, исполнительны и являются ярыми фанатиками, пропагандируемой им идеологии.

Если операция предполагает удержание заложников в другом месте, то туда подбирают более мягких и более контактных. В их задачу не входит проявление агрессии, их задача удержать заложников без бунта и сопротивления. Это скорее дипломаты, но они могут и ликвидировать заложника в случае его активного поведения.

Использование женщин позволяет террористам использовать еще одну уловку — выход из зоны теракта под видом жертвы, и оперативные работники должны учитывать этот нюанс при фильтрации людей при эвакуации с места происшествия.

Седьмой элемент — характеристика заложников. Практики всех заложников условно делят на три группы.

Представители первой группы — это финансовые деятели, олигархи или лица, к которым террористическая организация испытывает неприязнь или какие-либо другие претензии. Захват в заложники такого или таких лиц проводится для приобретения организацией материальных благ, финансовых вложений, устрашения других подобных лиц и некоторых других интересах. Надо отметить, что в качестве заложников могут выступать не только сами такие лица, но и их родственники, супруги, дети, близкие друзья.

Вторая группа — это лица, случайно попавшие в заложники. К таким заложникам относятся люди, попавшие в поле зрения преступников при уходе от погони. Это могут быть любые лица, оказавшиеся в ненужное время в ненужном месте. При попытке скрыться от преследования преступники не выбирают жертв, они заботятся о личном самосохранении, а, соответственно, к таким заложникам можно отнести любого человека.

К третьей группе относят заложников, в отношении которых планы захвата строились заранее и целенаправленно. В данном случае идет речь ни о конкретном человеке, а об определенной группе. К такой категории можно отнести школьников, сотрудников полиции, зрителей кинотеатров и театров. Надо отметить, что, если в качестве заложников в такой ситуации выступают гражданские лица, шанс остаться в живых у них есть, но, если это сотрудники

правоохранительных органов — они однозначно будут ликвидированы, о чем свидетельствует практика.

Случается, и так, что планы на захват заложников, относящихся к третьей группе, срывается, как правило, в результате оказанного сопротивления, тогда террористы используют заложников второй группы.

Итак, в ходе проведенного исследования можно сделать вывод о том, что оперативно-розыскная характеристика захвата заложников весьма многогранна. Это связано с неоднозначными целями при совершении захвата заложников. Широк и перечень личностей террористов, широк и перечень заложников. Многогранны возможные причины совершения заложников, непредсказуемо поведение преступников. Перечень объектов, на которых могут быть совершены захват заложников, настолько велик в каждом городе, что единственным эффективным способом противодействия таким преступлениям является оперативно-розыскная профилактика.

Литература

1. Спица А.Г. Меры противодействия захвату заложника // Студенческий вестник. 2019. № 3–1(53).

© Делов Н.С., 2025

К ВОПРОСУ ОБ УСЛОВИЯХ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

Дудниченко А.Н.

Профессор кафедры криминалистики
и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук, доцент

Прямая направленность на решение задач оперативно-розыскной деятельности является одним из отличительных признаков оперативно-розыскных мероприятий, что отличает их от других видов деятельности правоохранительных органов. Оперативно-розыскные мероприятия (далее — ОРМ) — это целенаправленные действия, строго регламентированные и подчиненные конкретным оперативным задачам (выявлению, предупреждению, пресечению и раскрытию преступлений), неотъемлемым аспектом проведения которых выступает наличие установленных Федеральным законом «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (далее — ФЗ «Об ОРД») оснований и условий. К таким основаниям относится наличие достаточных данных о совершении или подготовке преступления, а также наличия угрозы для жизни и здоровья граждан или государственной безопасности. Несоблюдение правил, ограничивающих применение ОРМ и гарантирующих соблюдение прав и свобод человека и гражданина может привести к признанию результатов ОРМ недопустимыми в судебном процессе.

Условия для проведения ОРМ устанавливаются оперативно-розыскным законодательством, в первую очередь Федеральным законом «Об оперативно-розыскной деятельности» (далее — ФЗ «Об ОРД»). Эти специальные нормы, соблюдение которых обязательно, формируют основу для подготовки

и проведения конкретных мероприятий, что способствует повышению их эффективности и соблюдению ОРД [4].

К первому условию относится соблюдение принципа территориальности: ОРМ могут проводиться на территории Российской Федерации, если федеральным законодательством не предусмотрено иное.

Вторым важным аспектом является то, что гражданство, этническая принадлежность, пол и прочие факторы, упомянутые в ч. 1 ст. 8 Федерального закона «Об ОРД», не могут являться основанием для ограничения проведения ОРМ в отношении отдельных лиц.

В рамках правового регулирования оперативно-розыскной деятельности (далее — ОРД) законодатель разработал комплексную систему исключений, которая структурирована по двум основным категориям оснований. Эти категории формируют особый правовой режим, позволяющий отступать от стандартных процедур при проведении ОРМ.

Начальный набор условий обеспечивает легитимность оперативно-розыскных мероприятий, затрагивающих конституционное право граждан на личную жизнь. Юридическая база для проведения ОРМ опирается на четкие параметры, гарантирующие соблюдение конституционных прав личности. Первоочередные требования нацелены на формирование эффективного правового инструмента, который оберегает базовые права индивида на неприкосновенность частной сферы при осуществлении специализированных оперативно-розыскных процедур.

Нормативная база, закрепленная в ст. 8 Федерального закона «Об ОРД», устанавливает два основополагающих императива: получение официального разрешения судебной инстанции и наличие оснований для проведения ОРМ.

Перейдем к детальному анализу первого ключевого требования. В виде судебного постановления оформляется решение суда. Данный процессуальный документ выступает официальным подтверждением позиции судьи, который, изучив все материалы, приходит к определенному заключению, формализует свое решение относительно результата рассмотрения запроса (ходатайства)

оперативного подразделения, (в соответствии со ст. 9 ФЗ «Об ОРД» судья по итогам рассмотрения материалов может либо разрешить проведение ОРМ, либо отказать в этом).

Следует отметить, что временные рамки реализации судебного постановления играют существенную роль в практической реализации оперативно-розыскной деятельности. Законодатель установил четкие параметры действия данного правового акта, которые исчисляются в календарных сутках с момента его официального оформления. Данный период исчисляется в днях, начиная с момента принятия решения, и ограничивается шестью месяцами, если иное не установлено в самом решении. Важно отметить, что течение этого срока не подлежит приостановлению (согласно ч. 5 ст. 9 Федерального закона «Об ОРД»). Срок истекает в соответствующее число месяца, а если этот месяц не имеет соответствующего числа, то в последние сутки этого месяца.

Вторым условием, ограничивающим выполнение конкретных ОРМ которые могут ограничить конституционные права человека и гражданина, является наличие определенной информации (ч. 2 ст. 8 Федерального закона «Об ОРД») о признаках преступной деятельности, которая готовится, осуществляется или уже совершена, когда производство предварительного следствия является обязательным; о лицах, которые готовят, совершают или совершили правонарушение, требующее обязательного предварительного следствия; событиях или действиях (или их отсутствии), представляющих угрозу для государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

К обстоятельствам, имеющим «экстренный характер», относится вторая категория условий. В Федеральном законе, регулирующем оперативно-розыскную деятельность, выделяются три группы таких специфических обстоятельств (ч. 3, 4 и 8 ст. 8 Федерального закона «Об ОРД»).

Рассмотрим первое из них. В ситуациях, которые требуют незамедлительных действий и могут привести к совершению тяжкого или

особо тяжкого преступления, а также при наличии информации о событиях и действиях (или бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности России, на основании обоснованного решения одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, возможно проведение ОРМ, указанных в ч. 2 ст. 8, с обязательным уведомлением суда (судьи) в течение 24 часов. Также в течение 48 часов с момента начала ОРМ орган, проводящий мероприятия, обязан получить решение суда о продолжении таких ОРМ либо прекратить их (ч. 3 ст. 8).

Второе условие, рассматриваемое в комплексе, представлено в ч. 6 ст. 8 Федерального закона «Об ОРД». При угрозе жизни, здоровью и имуществу граждан, при их письменном согласии или по их просьбе, разрешается прослушивание разговоров с их телефонов. Это осуществляется на основании постановления, утвержденного руководителем оперативно-розыскного органа, с обязательным уведомлением суда (судьи) в течение 48 часов (ч. 6 Федерального закона «Об ОРД»).

Третье условие изложено в ч. 11 ст. 8 ФЗ «Об ОРД», где закреплены правила, касающиеся безопасности оперативно-розыскного органа. ОРМ, направленные на защиту органов, проводятся в соответствии с законом и в рамках их полномочий. В случаях, предусмотренных п. 5 ч. 2 ст. 7 Федерального закона «Об ОРД», указанные действия могут выполняться без судебного решения при наличии письменного согласия гражданина. Важно отметить, что согласие позволяет не получать судебное разрешение для проведения некоторых оперативных мероприятий, однако они возможны лишь для обеспечения безопасности оперативно-розыскного органа.

В статье 8 Федерального закона «Об ОРД» подробно рассматривается также особый порядок осуществления некоторых оперативных мероприятий. Так проверочная закупка или контролируемая поставка предметов, веществ и продукции, свободная реализация которых запрещена либо оборот которых ограничен, а также оперативный эксперимент или оперативное внедрение

должностных лиц оперативно-розыскного органа, а равно лиц, оказывающих им содействие, проводятся на основании постановления, утвержденного руководителем оперативно-розыскного органа. Эти ОРМ могут проводиться исключительно на основании постановления, утвержденного руководителем оперативно-розыскного органа.

Обратимся к Определению Конституционного Суда Российской Федерации от 14 июля 1998 года № 86-О, в котором рассматриваются конституционные аспекты некоторых положений Федерального закона «Об ОРД». В данном определении признается законным порядок, в соответствии с которым разрешение на проведение ОРМ выдается председателями судов второго звена. Как указывается в определении, судебная санкция на прослушивание телефонных переговоров гражданки И.Г. Черновой была предоставлена Волгоградским областным судом, который в данном случае выступал как суд по месту проведения оперативно-розыскных мероприятий и суд по месту нахождения ходатайствующего органа.

Федеральный закон от 10.07.2012 № 114-ФЗ внес изменения в нормативные правовые акты Российской Федерации, регулирующие проведение ОРМ в отношении судей и напрямую реагирует на постановление Конституционного Суда РФ № 12-П от 09.06.2011 года, рассмотренное по жалобе гражданина И.В. Аносова. Жалоба Аносова оспаривала конституционность положений ст. 16 Закона РФ «О статусе судей в Российской Федерации» и ст. 9 Федерального закона «Об оперативно-розыскной деятельности», касающихся проведения ОРМ в отношении судей.

Рассмотрение судом материалов, касающихся ходатайств о проведении ОРМ, — процедура, требующая оперативности и строгого соблюдения законодательства. Поступившие материалы рассматриваются судьей единолично и незамедлительно. Требование незамедлительного рассмотрения подразумевает, что судья, компетентный в данном вопросе, не может откладывать принятие решения без веских причин.

Основанием для рассмотрения ходатайства служит мотивированное постановление руководителя органа, осуществляющего ОРД. Важно отметить, что круг этих руководителей определяется ведомственными нормативными актами, с которыми уполномоченный судья или председатель суда имеют право и, более того, обязаны ознакомиться для проверки полномочий заявителя. Список этих актов должен быть доступен судье, а незнание их содержания не может быть оправданием для принятия неправомерного решения.

Постановление, подающееся в суд, должно содержать исчерпывающую информацию, предписанную п. 1–3 ч. 2 ст. 8 Федерального закона «Об ОРД», и иметь четкое название, например: «Постановление о возбуждении перед судом ходатайства о даче разрешения на проведение оперативно-розыскного мероприятия: (указывается конкретное название мероприятия, например, прослушивание телефонных переговоров, наблюдение)». К постановлению прилагаются все необходимые доказательства и обоснования.

Судья обязан рассмотреть поступившие материалы, касающиеся ограничения конституционных прав граждан, но не обязан выдавать разрешение на проведение ОРМ. Решение судьи должно быть мотивированным и основываться на тщательном анализе представленных документов.

Литература

1. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

2. О внесении изменений в статью 16 Закона Российской Федерации «О статусе судей в Российской Федерации» и статью 9 Федерального закона «Об оперативно-розыскной деятельности». Доступ из справ. правовой системы «КонсультантПлюс».

3. Варданян А.В., Плясов К.А. Оперативно-розыскное обеспечение предупреждения, раскрытия и расследования преступлений в сфере внешнеэкономической деятельности // Юрист-Правоведь. 2022. № 1(100).

4. Варданян А.В. Результаты оперативно-розыскной деятельности как повод для возбуждения уголовного дела в контексте проблемы соотношения уголовно-процессуального и оперативно-розыскного законодательства / Современное уголовно-процессуальное право России — уроки истории и проблемы дальнейшего реформирования: сб. материалов Междунар. научно-практ. конф. Орел, 2017.

5. Князев М.В. Проблемы, возникающие при проведении оперативно-розыскных мероприятий в отношении этнических преступных групп // Молодой ученый. 2018. № 2.

© Дудниченко А.Н., 2025

УДК 343.34:004(470)

ОЦЕНКА СОСТОЯНИЯ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Карпика А.Г.

Доцент кафедры
информационно-коммуникационных технологий
и кибербезопасности
Ростовского юридического института МВД России
кандидат технических наук, доцент

Киберпреступления относятся к наиболее технологичным видам преступлений и предполагают использование информационно-коммуникационных технологий напрямую для совершения преступлений в киберпространстве, либо как инструмент, обеспечивающий совершение традиционных преступлений в реальном мире.

Общемировой тренд роста киберпреступлений различной направленности свидетельствует о расширении спектра применения

информационных технологий в преступной деятельности, чему способствует повышение доступности специфического программного обеспечения, позволяющего снизить профессиональный квалификационный порог потенциального киберпреступника.

Рассмотрим статистику киберпреступлений на примере развитых в технологическом плане стран и групп стран, объединенных политически и экономически в единые структуры.

В 2023–2024 гг. 50 % предприятий Великобритании подверглись той или иной форме кибератаки. За этот период было незаконно прочитано более 1 млрд электронных писем, что затронуло каждого пятого интернет-пользователя, при этом в 2024 г. утечка данных через электронную почту обошлась компаниям в среднем в 4,88 млн долларов.

В первой половине 2024 г. во всем мире произошло около 236,1 млн атак программ-вымогателей и в этот же период времени учетные записи каждого второго американского интернет-пользователя были взломаны и киберинциденты, произошедшие по вине злоумышленников, затронули 53,35 млн граждан США [1].

В связи с тем, что методы атак становятся все более изощренными, организациям по всему миру приходится вкладывать средства в более совершенные меры безопасности, повышать уровень подготовки и, особенно в крупных компаниях, нанимать специалистов по кибербезопасности, поскольку в результате кибератак затраты на устранение бреши и восстановление после простоя могут исчисляться миллионами долларов.

Так средняя стоимость кибератаки в 2023–2024 гг. составила 4,35 млн долларов, при этом, если в 2023 г. киберпреступность обошлась мировой экономике примерно в 7 трлн долларов, то по прогнозам ожидается, что к 2026 г. эта цифра возрастет до 10,5 трлн долларов. На этом фоне растет осведомленность организаций о рисках, связанных с третьими сторонами. По оценкам, к 2026 г. 60 % организаций будут использовать риски

кибербезопасности в качестве ключевого фактора при определении транзакций и деловых контактов с третьими сторонами, при этом 60 % руководителей высшего звена считают атаки на цепочки поставок наиболее вероятным видом киберугроз, которые могут повлиять на их бизнес.

Одной из распространенных технологий, которую «берут на вооружение» киберпреступники, являются устройства интернета вещей. Для функционирования этих устройств не требуется их прямое взаимодействие с человеком, что делает их отличным инструментом в бизнесе для автоматизации утомительных рабочих процессов и снижения вероятности ошибок. Однако это преимущество является главным привлекательным качеством и мишенью для киберпреступлений. GPS-трекеры, «умные» носимые и другие устройства интернета вещей могут хранить ценные данные, но часто не имеют надежного программного обеспечения для обеспечения безопасности.

Этот факт был обнаружен в инциденте с GPS-трекером MiCODUS MV720, который относится к популярным автомобильным устройствам слежения, предназначенным для использования транспортными и другими компаниями, имеющими собственный парк автотранспортных средств. Он встраивается в транспортные средства и обеспечивает защиту от угона, отключение подачи топлива, геозону и дистанционное управление.

Подобные устройства используются в 169 странах физическими и юридическими лицами, правительственными учреждениями, военными, правоохранительными органами и предприятиями. В MV720 было обнаружено 6 серьезных уязвимостей, которые потенциально позволяют злоумышленникам отслеживать поставки, или вымогать выкуп, выводя из строя технику.

Традиционным источником киберинцидентов остается человеческий фактор, который организации относят к критическим уязвимостям. По статистике до 82 % случаев нарушения интересов организаций и отдельных предпринимателей были связаны с этим фактором. Сюда входят ошибки, халатность сотрудников, а также следствие применения злоумышленниками методов социальной инженерии. Инсайдерские угрозы вызывают постоянную

тревогу. Так 83 % компаний сообщили, что в 2024 г. они подверглись как минимум одной инсайдерской атаке.

На этом фоне, граждане и организации Российской Федерации испытывают на себе сходные последствия деятельности киберпреступников и преступных сообществ, использующих информационные технологии в своей деятельности.

Официальные статистические данные МВД России свидетельствуют о том, что в 2024 г. было официально зарегистрировано 1,9 миллиона преступлений, из которых 40 % (760 тыс.) были совершены с использованием информационно-телекоммуникационных технологий. Это на 13,1 % больше, чем в 2023 г., в том числе тяжких и особо тяжких составов — на 7,8 %. В значительной степени этот фактор повлиял на рост в 2024 г. общего числа тяжких и особо тяжких преступлений на 4,8 %.

В период с января по сентябрь 2025 г. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, зарегистрировано на 7,4 % меньше, чем в январе-сентябре прошлого года, а количество дистанционных краж снизилось на 19,2 %, дистанционных мошенничеств — на 5,1 %, а преступлений в сфере компьютерной информации — на 37,5 %. Скорее всего снижение является временным и произошло вследствие искусственного ограничения доступа к мобильному Интернету и звонкам через мессенджеры Whatsapp и Telegram. Ожидается, что в течение следующего года кибермошенники смогут адаптироваться к новым условиям и восстановить свою активность.

Существует серьезная проблема с раскрываемостью подобных преступлений. По статистическим данным, приведенным на официальном сайте МВД России за 2024 г. общая раскрываемость по всем видам преступлений составила 49 %, то раскрываемость преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации» в рассматриваемом периоде только 26,6 % [2].

Статистические данные за 10 месяцев 2025 г. подтверждают эту тенденцию: общая раскрываемость по всем видам преступлений — 52,4 %, раскрываемость преступлений, «совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации» составила 28,4 % [3].

Таким образом, можно сделать вывод о том, что состояние киберпреступности в мире вообще и в Российской Федерации в частности вызывает серьезное беспокойство во всех слоях общества, и требует пересмотра подходов к решению этого вопроса на фоне устойчивого интереса различного вида преступников и преступных сообществ к ведению своего «бизнеса» с активным использованием информационных технологий.

Литература

1. Последняя статистика киберпреступлений за 2025 год (обновлена в октябре 2025 года) [Электронный документ]. URL: <https://aag-it.com/the-latest-cyber-crime-statistics> (дата обращения: 08.10.2025).
2. Состояние преступности в России за январь-декабрь 2024 года [Электронный документ]. URL: file:///C:/Users/kag/Downloads/Sbornik_UOS_2024.pdf. (дата обращения: 08.10.2025).
3. Состояние преступности в России за январь-сентябрь 2025 года // [Электронный документ]. URL: file:///C:/Users/kag/Downloads/Sbornik_dlya_UOS_yanv-sent2025.pdf. (дата обращения: 08.10.2025).

© Карпика А.Г., 2025

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «ОПЕРАТИВНО-РОЗЫСКОЕ СОПРОВОЖДЕНИЕ» РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Коновалов С.И.

Профессор кафедры криминалистики
и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
доктор юридических наук, профессор

Результативность противодействия криминальным вызовам, детерминированная спецификой экономических и коррупционных преступлений, находится в прямой корреляционной зависимости от синергии субъектов, осуществляющих оперативно-розыскную деятельность (ОРД), и институтов предварительного следствия. В современных реалиях доктринальной мысли и правоприменительного вектора в качестве фундаментального связующего звена данных структур постулируется феномен оперативно-розыскного сопровождения (далее — ОРС).

Казалось бы, инструментарий понятен. Однако здесь возникает коллизия. Несмотря на экспансию указанной дефиниции в массив ведомственного нормотворчества и научный оборот, законодатель до настоящего времени не закрепил унифицированную формулировку ОРС в профильном Федеральном законе «Об оперативно-розыскной деятельности».

Почему это критично? Отсутствие легальной детерминации неминуемо провоцирует острые научные дискуссии, касающиеся сущностного наполнения, хронологических границ и, что самое важное, правовой природы данного правового института. Можно ли считать сопровождение лишь вспомогательным техническим алгоритмом? Или же это сложная, многоуровневая система обеспечения доказательственной базы, требующая жесткой процессуальной регламентации?

Теоретические основы и сущность понятия

Этимологический анализ термина «сопровождение» указывает на совершение действий, сопряженных с совместным следованием, пребыванием в непосредственной близости или качественным дополнением некоего процесса. В плоскости уголовного судопроизводства данная лексема трансформируется в концепт перманентной и всеобъемлющей поддержки следственных действий со стороны оперативных подразделений.

Но что скрывается за этой поддержкой на самом деле?

Речь идет не о пассивном наблюдении, а об активном, функциональном содействии, которое обеспечивает бесшовную интеграцию негласных методов получения информации в официальную канву расследования. Такая синергия позволяет следствию оперативно реагировать на меняющуюся обстановку, используя ресурсный потенциал органов дознания для верификации доказательств и нейтрализации противодействия со стороны фигурантов.

Одним из фундаментальных подходов является определение ОРС как системы организационных и правовых мер. Как отмечает Е.В. Стельмах, «цифровая трансформация правоохранительных органов диктует необходимость понимания сопровождения как непрерывного процесса информационного и оперативного обеспечения следствия на всех стадиях — от возбуждения дела до вынесения приговора» [10, с. 42]. Автор подчеркивает, что в современных условиях сопровождение перестает быть разовой помощью и превращается в комплексную технологическую поддержку.

Важно разграничивать ОРС и стадию возбуждения уголовного дела. Если до возбуждения дела оперативные сотрудники осуществляют документирование, то после — они «сопровождают» уже начатое расследование. Федеральный закон № 273-ФЗ «О противодействии коррупции» устанавливает обязанность органов безопасности использовать все доступные средства для пресечения коррупционных схем [1, ст. 3]. Это юридически легитимизирует активную позицию оперативника в рамках уже начатого уголовного процесса.

Содержательные аспекты ОРС

Традиционно содержание сопровождения включает в себя выполнение поручений следователя, проведение оперативно-розыскных мероприятий (далее — ОРМ) по установлению новых эпизодов и обеспечение безопасности участников процесса. Однако, как указывает С.В. Волков, теория цифровых следов меняет саму структуру этого процесса: «Оперативно-розыскное сопровождение сегодня — это прежде всего работа с негласной информацией в цифровой среде, которая позволяет следователю получить доказательства, недоступные при обычных следственных действиях» [2, с. 89].

В современной юридической доктрине сложился консенсус относительно многоаспектности ОРС, что позволяет исследователям дифференцировать его на несколько базовых, тесно взаимосвязанных компонентов.

Во-первых, выделяется **информационный базис**. Он представляет собой не просто формальную передачу сведений, а непрерывную, динамичную циркуляцию данных между оперуполномоченным и следователем, что критически важно для своевременного купирования информационных лакун в ходе расследования.

Вторым эшелоном выступает **тактический элемент**. Насколько жизнеспособно расследование без единого вектора движения? Именно совместное планирование следственных действий и оперативно-розыскных мероприятий (ОРМ) позволяет выстроить монолитную стратегию изобличения виновных лиц, исключая дублирование функций и возможные коллизии ведомственных интересов.

Наконец, нельзя игнорировать **техническую составляющую**. Современная преступность высокотехнологична, что обуславливает необходимость встречного применения специальных познаний и сложнейшего инструментария. Это подразумевает не только использование криминалистической техники в ее классическом понимании, но и активное внедрение систем мониторинга, а также алгоритмов искусственного интеллекта для анализа массивов неструктурированных данных. Именно такая

технологическая синергия преобразует процесс доказывания из ремесленного ремесла в высокоточную аналитическую работу, где каждый бит информации служит укреплению доказательственной базы.

Цифровая трансформация сопровождения

В эпоху «данных» сопровождение приобретает новые формы. Указ Президента РФ № 478 прямо указывает на приоритет цифровых технологий в антикоррупционном мониторинге [2, ст. 6170]. В рамках ОРС это выражается в использовании таких систем, как ГИС «Посейдон».

М.С. Козлов отмечает, что подготовка специалистов для подразделений ЭБиПК теперь должна включать навыки «цифрового сопровождения», где ИИ берет на себя рутинный анализ массивов Big Data, высвобождая время оперативника для аналитической работы [5, с. 140]. ОРС в данном контексте рассматривается как алгоритмизированный процесс. Так И.А. Данилов доказывает, что алгоритмы выявления скрытой аффилированности в госзакупках являются неотъемлемой частью современного сопровождения дел о коррупции [3, с. 68].

Проблемы доказательственного значения

Одной из наиболее острых проблем является легализация данных, полученных в ходе ОРС. А.Д. Петров указывает на сложность использования данных, полученных с применением ИИ, в качестве полноценных доказательств: «Существующий разрыв между оперативной возможностью найти информацию и процессуальной возможностью ее закрепить остается главным барьером эффективности сопровождения» [7, с. 88].

Тем не менее, использование технологий распределенного реестра может решить проблему достоверности. Р. Н. Салихов утверждает, что «блокчейн-технологии позволяют создать неизменяемый след движения активов, что делает оперативное сопровождение дел о взяточничестве более прозрачным и доказательным» [8, с. 210].

Этические и психологические аспекты

Не стоит забывать и о психологической составляющей. В монографии В.А. Зайцева подчеркивается, что оперативное сопровождение требует особого психологического взаимодействия в следственно-оперативной группе (далее — СОГ). Автор указывает на важность «психологической совместимости и единого понимания целей расследования» [4, с. 156].

В то же время, Т.И. Новикова предупреждает об опасности «алгоритмической предвзятости» при сопровождении расследований, когда оперативные сотрудники могут чрезмерно полагаться на выводы автоматизированных систем, игнорируя оправдательные обстоятельства [6, с. 78].

Обобщая результаты проведенного теоретико-правового анализа, представляется возможным эксплицировать авторскую дефиницию рассматриваемого феномена.

Оперативно-розыскное сопровождение расследования преступлений — это детерминированная нормами федерального законодательства и ведомственными предписаниями комплексная система деятельности оперативных аппаратов, функционально ориентированная на предиктивное формирование оптимальной среды для результативного предварительного следствия и последующего судебного разбирательства. Данная цель достигается посредством системной реализации оперативно-розыскных мероприятий, прецизионного задействования специальных технических средств и трансляции следователю массива оперативно-значимой информации, релевантной обстоятельствам предмета доказывания.

Современный этап эволюции ОРС знаменует собой парадигмальный сдвиг. Мы наблюдаем очевидный переход от примитивных форм физического содействия к высокоуровневому интеллектуальному и цифровому обеспечению уголовного процесса. Является ли это просто данью моде? Отнюдь нет. Это объективная необходимость, продиктованная цифровизацией преступности.

Вектор дальнейшего развития доктрины и законодательства должен быть направлен на легитимизацию правового статуса инновационных инструментов. В частности, назрела потребность в четкой регламентации использования искусственного интеллекта и специализированных аналитических систем, таких как программный комплекс «Посейдон», в рамках сопровождения уголовных дел. Только через нормативное закрепление этих цифровых алгоритмов мы сможем обеспечить безупречность доказательств, полученных в ходе высокотехнологичной оперативной работы, и минимизировать риски процессуального оспаривания результатов ОРД.

Литература

1. О противодействии коррупции: федер. закон от 25.12.2008 № 273-ФЗ // Собрание законодательства РФ. 2008. № 52 (ч. 1). Ст. 6228.
2. О Национальном плане противодействия коррупции на 2021–2024 годы: Указ Президента РФ от 16.08.2021 № 478 // Собрание законодательства РФ. 2021. № 34. Ст. 6170.
3. Данилов И.А. Алгоритмы выявления скрытой аффилированности в госзакупках // Экономическая безопасность и IT. 2025. № 2. С. 65–72.
4. Зайцев В.А. Киберкриминалистика и психология оперативной деятельности. М., 2025.
5. Козлов М.С. Кадровый суверенитет в эпоху ИИ: подготовка специалистов для подразделений ЭБиПК // Информационная безопасность и право. 2024. № 4.
6. Новикова Т.И. Алгоритмическая предвзятость в антикоррупционном мониторинге // Правовая мысль XXI века. 2024. № 1.
7. Петров А.Д. Проблемы доказательственного значения данных, полученных с применением ИИ // Современная криминалистика. 2024. № 5.
8. Салихов Р.Н. Блокчейн-технологии как инструмент антикоррупционного контроля // Вестник цифровой криминалистики. 2025. № 4.

9. Волков С.В. Теория цифровых следов в расследовании экономических преступлений // Вестник юридического образования. 2024. № 3.

10. Стельмах Е.В. Цифровая трансформация правоохранительных органов. М., 2024.

11. Шитова С.А. Методы выявления незаконного обогащения в цифровой среде // Юридические технологии будущего. 2024. № 2.

© Коновалов С.И., 2025

УДК 343.97:343.34:004

СИСТЕМНАЯ ДЕЯТЕЛЬНОСТЬ ГОСУДАРСТВА ПО ПРОТИВОДЕЙСТВИЮ КИБЕПРЕСТУПНОСТИ

Корниленко А.В.

Старший преподаватель кафедры
организации оперативно-разыскной деятельности
Академии управления МВД России,
кандидат политических наук

Как известно в последние годы на федеральном уровне предпринимаются значительные меры по борьбе с преступностью в сфере информационно-коммуникационных технологий (далее — ИКТ). Стремительное развитие средств и методов совершения киберпреступлений поставило руководство государства и ведомства перед необходимостью создания единой государственной системы, способной устранить угрозы в данной сфере.

Следует отметить, что ранее предпринимались шаги по стратегическому противодействию IT-преступности, такие как:

– создание в 2018 г. автоматизированной системы обработки инцидентов «ФинЦЕРТ», позволяющей осуществлять взаимодействие участников и ГосСОПКА;

– создание в 2021 г. государственной информационной системы «Антифрод», позволяющей выявлять и блокировать мошеннические звонки, совершаемые с подменных номеров;

– создание в 2022 г. информационной системы национального удостоверяющего центра, в котором предусмотрено создание центральной базы идентификаторов пользовательского оборудования (IMEI).

Учитывая существующие объективные угрозы общественной безопасности, Президентом Российской Федерации в 2024 г. была поставлена задача по созданию «системы эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, и снижения ущерба от их совершения» [1].

Первым шагом на пути решения поставленной задачи стала разработка Министерством внутренних дел Российской Федерации «Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» (далее — Концепция), которая в дальнейшем была утверждена Правительством Российской Федерации [2]. Данным документом были обозначены основные параметры и условия ее функционирования, а также определены ведущие направления обеспечения (кадровое, финансовое).

Концепцией впервые были введены в юридический оборот основные понятия, имеющие существенное значение для реализации поставленных задач в сфере борьбы с киберпреступностью, такие как: «государственная система противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» (далее — государственная система), «информационно-коммуникационная сфера», «информационно-коммуникационные технологии», «противоправные деяния, совершенные с использованием информационно-коммуникационных технологий» и «средства государственной системы».

Исходя из обозначенных функций, создаваемая государственная система должна представлять собой единую цифровую платформу, предназначенную

для обмена информацией «между правоохранными органами, Центральным банком Российской Федерации, кредитными организациями, а также операторами связи» [2] в целях получения и реализации оперативно значимой информации.

Помимо этого, государственной системой планируется выполнение ряда важнейших задач по обеспечению функционирования информационных ресурсов иных органов государственной власти, мониторинг сети Интернет с целью ограничения доступа к запрещенным ресурсам, определенная правотворческая деятельность в рассматриваемой сфере деятельности.

Примечательно, что одной из задач государственной системы поставлено «создание подразделений, специализирующихся на противодействии противоправным деяниям» [2]. Учитывая, что в 2022 г., согласно Указу Президента России, в структуре Министерства внутренних дел Российской Федерации было образовано отдельное профильное подразделение, имеющее функции головного по борьбе с киберпреступностью, то возможно, речь может идти об образовании аналогичных подразделений в других государственных ведомствах (организациях).

В научно-техническую составляющую обеспечения государственной системы включено «систематическое повышение профессиональной подготовки специалистов в области противодействия противоправным деяниям» [2], что имеет важнейшее значение для ее эффективного функционирования. В настоящее время в образовательной системе МВД России проходят повышение квалификации как представители оперативного состава (на базе Всероссийского института повышения квалификации и других ВУЗов), так и руководители профильных оперативных подразделений регионального уровня (на базе Академии управления).

В развитие Концепции Федеральным законом № 41-ФЗ [3] была уже непосредственно создана сама государственная система, а также внесены соответствующие изменения в другие законодательные акты.

Однако, несмотря на важность и своевременность принятия данного закона, представляется, что отдельные его положения не вполне соответствуют требованиям точности, ясности и недвусмысленности правовых норм.

В качестве примера можно привести нормативное закрепление такого понятия как «пользовательское оборудование (оконечное оборудование), использующее программные и радиоэлектронные средства, которое предназначено для пропуска трафика между сетями связи и (или) сетями передачи данных с возможностью одновременного использования нескольких идентификационных модулей, средства связи, которое предназначено для предоставления абоненту возможности пользования услугами электросвязи, выполнения функции систем коммутации, маршрутизации трафика в сети электросвязи» [4]. Исходя из текста пояснительной записки к его законопроекту, под данным термином подразумевалось только конкретное устройство, а именно — «SIM-бокс», высокая опасность использования которых преступниками неоднократно отмечалось различными авторами [5].

Еще на стадии проведения общественной экспертизы законопроекта, Общественной палатой Российской Федерации были высказаны существенные замечания, имеющие прямое отношение к реализации правоприменительной практики.

Так, например, указывалось на «двусмысленность данной правовой нормы, а именно: «определение, предложенное в законопроекте, сформулировано таким образом, что к нему можно отнести все пользовательское оборудование, включая мобильные телефоны, поскольку они обладают аналогичным функционалом», что в дальнейшем может создать предпосылки для широкой интерпретации нормы и правовой неопределенности в ее применении» [4].

Также, несмотря на принятые законодателем меры по предотвращению массовых и (или) автоматических телефонных вызовов в сетях связи общего пользования (что в некоторой степени дублирует положения ст. 18 ранее принятого Федерального закона «О рекламе» [6]), они не предусматривают

превентивных мер в отношении распространения такой информации посредством мессенджеров.

Утвержденным Планом мероприятий по реализации Концепции предусмотрен достаточно большой объем мероприятий нормативно-правового, организационного, технического, кадрового и иного характера, подлежащих выполнению до IV квартала 2027 г. (максимальный срок) а также на постоянной основе [7].

К выполнению мероприятий Плана, ответственным исполнителем (соисполнителем) которого является МВД России, также привлечены иные органы государственной власти, Банк России, Следственный комитет и Генеральная прокуратура Российской Федерации.

В настоящее время Минцифры совместно с МВД России осуществляет разработку концепции Платформы противодействия мошенническим действиям, совершаемым с использованием ИКТ, основное предназначение которой заключается в обеспечении эффективного оперативного взаимодействия уполномоченных государственных органов, Банка России, организаций кредитно-финансовой сферы, электронной торговли, операторов связи и телекоммуникационных компаний.

Таким образом, очевидно, что одним из важнейших направлений реализации государственной политики Российской Федерации является реализация комплекса мер по обеспечению общественной безопасности в IT-сфере, в том числе, путем создания и эффективного функционирования единой системы противодействия федерального уровня.

Литература

1. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: Указ Президента Российской Федерации от 07.05.2024 № 309. Доступ из справ. правовой системы «КонсультантПлюс».

2. О Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-

коммуникационных технологий: распоряжение Правительства Российской Федерации от 30.12.2024 № 4154-р. Доступ из справ. правовой системы «КонсультантПлюс».

3. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 01.04.2025 № 41-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

4. О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: Заключение Общественной палаты Российской Федерации по результатам общественной экспертизы проекта Федерального закона № 842276-8. Доступ из справ. правовой системы «КонсультантПлюс».

5. Марсаков И.С. Отдельные аспекты борьбы органов внутренних дел с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий в кредитно-финансовой сфере // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2025. № 69.

6. О рекламе: федер. закон от 13.08. 2006 № 38-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

7. Об утверждении Плана мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Российской Федерации от 14.08.2025 № 2207-р. Доступ из справ. правовой системы «КонсультантПлюс».

**ОТОЖДЕСТВЛЕНИЕ ЛИЧНОСТИ КАК ОПЕРАТИВНО-РОЗЫСКНОЕ
СРЕДСТВО ВЫЯВЛЕНИЯ И РАЗОБЛАЧЕНИЯ СПОСОБОВ
МАСКИРОВКИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ**

Коряк Ю.Д.

Адъюнкт адъюнктуры
Ростовского юридического института МВД России

Учение о противодействии расследованию и мерах по его преодолению является неотъемлемой частью криминалистической науки. Его стремительное развитие обусловлено политическими, экономическими, социальными изменениями в обществе и их негативными последствиями, которые, в первую очередь, связаны с ростом нераскрытых преступлений. Согласно статистическим данным МВД России за 2024 г. из общего количества 929,7 тыс. преступлений 902,3 тыс. (на 1,5 % больше, чем за 2023 г.) остались нераскрытыми в связи с не установлением лица, подлежащего привлечению в качестве обвиняемого [1]. На наш взгляд, эскалация нераскрытой преступности свидетельствует о низкой эффективности деятельности правоохранительных органов. На протяжении нескольких десятилетий ученые-криминалисты, пытаясь решить как указанную, так и иную научную проблему теоретического и практического характера, сходятся во мнениях о том, что необходимо своевременное совершенствование криминалистической деятельности, направленной на выявление и разоблачение способов и приемов противодействия расследованию [2].

Выявление и разоблачение маскировки является практически неисследованной научной проблемой. Так с начала 90-х годов прошлого века

мы не встретили ни одно комплексного исследования, которое бы раскрывало сущность маскировки как способа сокрытия и приема противодействия, лишь в отдельных трудах ученых-криминалистов частично затрагивались отдельные аспекты изучаемой нами проблемы [3, с. 327–329; 4, с. 367; 5].

Разрешение научной проблемы видится нами в комплексном изучении маскировки во всех сегментах и видах деятельности объекта науки криминалистики. В настоящем исследовании хотелось бы уделить особое внимание оперативно-розыскным средствам выявления и разоблачения маскировки.

В криминалистической и оперативно-розыскной деятельности используется такое понятие как «отождествление». Тождество (идентичность) — это наличие у объекта неповторимой совокупности устойчивых признаков, которая отличает его от всех иных, в том числе ему подобных. В криминалистическом смысле идентификация (отождествление) представляет собой процесс установления факта тождества путем сопоставления объекта и его отображений [6, с. 58–59]. Одной из форм криминалистической идентификации является оперативная идентификация, которую мы рассмотрим далее.

Отождествление личности — оперативно-розыскное мероприятие (далее — ОРМ), заключающееся в негласном опознании и установлении тождества личности по признакам внешности и поведения, оставленным следам и продуктам жизнедеятельности. Следует отметить, что порядок его проведения не предусмотрен в Федеральном законе «Об оперативно-розыскной деятельности», что является значительным недостатком правового регулирования. Различают два вида отождествления личности: непосредственное и опосредованное. Непосредственное отождествление осуществляется лицами, ранее встречавшимися с объектом данного ОРМ, запомнившими характерные черты его внешности либо иные особенности,

и заключается в непосредственном узнавании (или другими словами — опознании). Опосредованное отождествление предполагает распознавание объекта по словесному портрету либо фотоизображению (видеозаписи) лицом, ранее с ним не встречавшимся.

В практической деятельности отождествление личности проводится достаточно редко, что подтверждается результатами проведенного опроса респондентов из числа сотрудников оперативных подразделений и анализом материалов уголовных дел. Тем не менее, на наш взгляд, отождествление личности является одним из необходимых ОРМ, которые позволяют выявить и разоблачить маскировку, поскольку оно может сочетать в себе некоторые элементы наблюдения, опроса граждан, наведения справок, исследования предметов и документов. Если все эти действия объединены общей целью — идентификацией, т. е. установлением личности субъекта преступления, то вероятность установления личности маскировщика (лицо, которое реализует приемы и способы маскировки в преступной и посткриминальной деятельности) значительно возрастает. Кроме того, проведение отождествления личности достаточно часто дает благоприятный результат, позволяет установить личность преступника. Личность маскировщика, бесспорно, установить значительно труднее, однако, все же возможно. Так, хотелось бы привести следующий пример проведения ОРМ «отождествление личности» сотрудниками ОУР ОП № 5 УМВД России по г. Ростову-на-Дону по факту совершения преступления, предусмотренного п. «а», «г» ч. 2 ст. 161 УК РФ в отношении Потерпевшей № 1. ФИО по фотографии опознал ФИО 1, как лицо, которое примерно в 17 часов 45 минут, находясь на аллее, расположенной по адресу: ... совместно с неустановленным лицом совершило грабеж с применением насилия, а именно похитили принадлежащий ему мобильный телефон марки iPhone 7, стоимостью 8 500 рублей. Также, в ходе оперативно-розыскных мероприятий по адресу: ... была получена видеозапись с камер

видеонаблюдения, на которой зафиксировано вышеуказанное преступление и установлено лицо, совершившее преступление в маске [7].

Отождествление личности возможно по внешним анатомическим и функциональным признакам лица, по голосу и речи, особым приметам (шрамы, татуировки, дефекты речи, физические недостатки). Оно осуществляется непосредственно в момент зрительного восприятия опознаваемого, а также по фотографиям, видеозаписям, фонограммам. Условия проведения отождествления должны быть максимально приближены к условиям проведения процессуального опознания по фотографии. Кроме того в настоящее время, все чаще производится отождествление личности с применением информационных технологий. Так цифровая трансформация общества позволяет с помощью технологий распознать лицо по внешнему облику, походке, голосу установить лицо, которое использует различные средства маскировки, например, маску, балаклаву, объемную одежду. Такое отождествление становится возможным при отсутствии очевидцев преступления, то есть происходит практически без участия человека исключительно программными средствами, которые анализируют антропологические и динамические характеристики личности, зафиксированные на фото, видео- или аудиозаписях, оказавшихся в распоряжении оперативных подразделений (записи телефонных переговоров, фото-, аудио-, видео- файлы размещенные в сети Интернет или обнаруженные при проведении других оперативно-розыскных мероприятий) [8, с. 120–121].

В теории оперативно-розыскной деятельности и криминалистической науки возникает ряд вопросов, связанный с многообразием приемов и способов маскировки в преступной и посткриминальной деятельности, закономерностями формирования и реализации данного приема (способа), выбора линии поведения в виде противодействия и виновной осведомленности, а также тактических и методических вопросов выявления и разоблачения

маскировки в процессе раскрытия и расследования преступлений. Разумеется, изучение данных вопросов в рамках одной статьи невозможно, требуется комплексный подход.

Отметим, что разработка положений о выявлении и разоблачении способов сокрытия и приемах противодействия может послужить основой для совершенствования криминалистического учения о личности неизвестного преступника. Кроме того, с учетом постоянно развивающихся технологий, во много способствующих и обуславливающих совершение преступлений, считаем необходимым уделять особое внимание способам маскировки личности в цифровом пространстве.

Литература

1. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года [Электронный ресурс]. URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 10.10.2025).

2. Андреев А.С. Научно-тематический анализ исследований в криминалистике отдельных видов посткриминального поведения лиц, связанных с преступной деятельностью. Азов, 2015.

3. Холевчук А.Г. Фальсификация как способ сокрытия преступления и ее соотношение с другими способами сокрытия // Актуальные проблемы российского права. 2010. № 1.

4. Моисеенко И.Я. Маскировка преступлений в структуре понятия «противодействие расследованию» / Современное законотворчество и правоприменение: тезисы докладов Международ научно-практ конф. Пермь, 2008.

5. Карагодин В.Н. Преодоление противодействия предварительному расследованию. Свердловск, 1992.

6. Белкин Р.С. Курс криминалистики: уч. пособие. М., 2001.

7. Судебные акты судов общей юрисдикции Российской Федерации [Электронный ресурс]. URL: <https://sudact.ru/regular/> (дата обращения: 10.10.2025).

8. Ховавко С.М. Сравнительный анализ оперативно-розыскного мероприятия «отождествление личности» и следственного действия «предъявление для опознания» и его правовое значение // Вестник Уральского юридического института МВД России. 2021. № 1.

© Коряк Ю.Д., 2025

УДК 343.36

СЛУЖЕБНАЯ ПРОВОКАЦИЯ ПРЕСТУПЛЕНИЯ КАК СПОСОБ ПРЕСТУПНОГО ПРОТИВОДЕЙСТВИЯ ПРАВОСУДИЮ

Кулахсзян С.К.

Преподаватель кафедры криминалистики
и оперативно-разыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

Проявление служебных провокаций преступлений можно обнаружить в различных сферах социально-правовой действительности и правоохранительной деятельности, включая оперативно-розыскные мероприятия, уголовно-процессуальные действия, административные функции органов внутренних дел и другие служебные аспекты.

И.М. Комаров справедливо отмечает, что расследование представляет собой специфическую форму познавательной деятельности, направленную на установление всех обстоятельств произошедшего для принятия обоснованного процессуального решения [1]. Выявление обстоятельств,

связанных со служебной провокацией преступления, требует применения комплексного криминалистического подхода.

Рассмотрим основные особенности служебной провокации преступления, как способа преступного противодействия правосудию, отличающие ее от иных видов провокаций (криминальной и виктимной):

1) служебная провокация преступления возникает в реалиях оперативно-розыскной деятельности, уголовно-процессуальной деятельности, административной деятельности ОВД или Федеральной службы войск национальной гвардии Российской Федерации, а также иной правоохранительной деятельности, и выступает составляющей должностной преступной деятельности;

2) в служебной провокации преступления провокатором выступает должностное лицо, осуществляющее правоохранительную деятельность;

3) для служебного провокатора цели уголовного преследования или шантажа спровоцированного более приоритетны и согласованы, как правило, со стремлением повысить «показатели раскрываемости преступлений или иных служебных показателей деятельности»;

4) способы преступного противодействия правосудию в форме служебных провокаций преступлений выступают составляющей объективной стороны преступлений, предусмотренных гл. 31 УК РФ «Преступления против правосудия» или/и гл. 30 УК РФ «Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления»;

5) служебная провокация преступления в большинстве случаев осуществляется только в отношении конкретных(ого) лиц(а) как визави-провокация в отношении граждан, вовлеченных в сферу борьбы с преступностью, или в отношении самого должностного лица;

б) проверка и разоблачение служебной провокации соответствуют целям методик расследования соответствующих преступлений (или задачам расследования коррупционных преступлений, преступлений, связанных с незаконным оборотом наркотиков, оружия, боеприпасов, браконьерства).

Как справедливо отмечает Н.А. Подольный, эффективное расследование — это задача следователя, от решения которой зависит качество расследования и, в конечном итоге, справедливость принимаемых решений [2]. Криминалистическая методика является одним из инструментов, обеспечивающих это качество, в том числе и при расследовании служебных провокаций преступлений.

По нашему мнению, структура познания, лежащая в основе методико-криминалистического обеспечения проверки и разоблачения служебных провокаций преступлений, должна быть многоуровневой и реализовываться как: элемент методик расследования коррупционных преступлений, преступлений, связанных с незаконным оборотом наркотических средств, оружия, боеприпасов, браконьерством и других; отдельные методики расследования конкретных видов служебных провокаций; обобщенная базовая методика расследования служебных провокаций преступлений.

Криминалистическая алгоритмизация, рассматриваемая как специфический научно-прикладной метод в сфере специальных юридических исследований, представляет собой весьма перспективный инструмент для методико-криминалистического обеспечения расследования преступлений, спровоцированных должностными лицами [3].

Ключевыми векторами развития и улучшения методико-криминалистического обеспечения деятельности по выявлению и пресечению служебных провокаций преступлений являются:

- дальнейшая оптимизация элементов, связанных с формированием криминалистических рекомендаций по обнаружению и разоблачению

должностных провокаций преступлений, а также сведение к минимуму противодействия с использованием аналогичных аргументов в контексте методик расследования коррупционных преступлений, преступлений, связанных с незаконным оборотом наркотических средств, оружия, боеприпасов. Кроме того требуется разработка аналогичных рекомендаций для методик расследования преступлений, в основе которых лежат служебные провокации;

- создание и внедрение частных методик расследования конкретных видов служебных провокаций преступлений;

- формирование универсальной методики расследования служебных провокаций преступлений на базе существующих специализированных методик расследования.

Как отмечалось ранее, при служебной провокации преступления субъектом преступления выступает должностное лицо из правоохранительных органов. Оно имитирует или искусственно создает видимость раскрытия, расследования и доказательств вины лица, чтобы начать уголовное преследование (для увеличения эффективности работы) или для шантажа. Подобная провокация происходит в рамках оперативно-розыскной, уголовно-процессуальной и административной деятельности.

При этом, служебная провокация преступления, как отдельный метод незаконного воздействия на правосудие и предательства его целей, совершаемая должностными лицами по преступлениям, предусмотренным ст. 286, 303, 304 УК РФ, может принимать форму речевых провокаций, когда провоцируемого вводят в обман, а также служебной имитации «механизма преступления» и фальсификации уголовного преследования [4]. Речевые служебные провокации, а также письменные документы при фальсификации уголовного преследования, напрямую связаны с уровнем языковой

компетенции сотрудников полиции и других представителей правоохранительных органов.

Следует подчеркнуть, что названные способы преступного противодействия обусловлены объективным фактором, таким как поведение и позиция лица, в отношении которого совершается провокация (активная или пассивная защита, либо нейтральное отношение). Учитывая разностороннюю криминалистическую сущность провокации, мы полагаем, что для всех рассмотренных форм ее объектом выступает назначение уголовного судопроизводства (ст. 6 УПК РФ). Этот вывод согласуется с точкой зрения О.В. Губановой, отмечающей, что провокация взятки или коммерческого подкупа всегда затрагивает интересы правосудия, в частности общественные отношения, обеспечивающие защиту личности от незаконного обвинения, осуждения и ограничения прав [5]. Такое толкование назначения правосудия основывается на положениях ст. 6 УПК РФ. По нашему мнению, служебная провокация преступления оказывает негативное воздействие на оперативно-розыскную деятельность, предварительное расследование и судебное разбирательство, приводя к привлечению к ответственности невиновного лица или уклонению от ответственности виновного, включая провокатора. Уголовное преследование спровоцированного лица при этом может быть как самоцелью провокатора, так и средством искусственного завышения показателей борьбы с преступностью.

Таким образом, для разработки частных методик расследования провокаций преступлений и повышения эффективности правоприменения, считаем целесообразным выделить два этапа: трансформационный (переходный) — до устранения противоречий в понимании служебной провокации между ст. 304 и ч. 4 ст. 303 УК РФ и использования ст. 286 УК РФ и др.), и этап стабилизации (введение нормы о провокации преступления и иные неизбежные изменения в уголовном законодательстве).

Литература

1. Комаров И.М. Метод научного познания и методы практической деятельности по расследованию преступлений (часть I) // Юрист-Правоведь. 2022. № 2(101).
2. Подольный Н.А. Криминалистическая методика расследования: значение ее отдельных видов для установления обстоятельств совершения преступления // Вестник Удмуртского университета. 2023. № 4
3. Варданян А.В., Грибунов О.П. Современная доктрина методико-криминалистического обеспечения расследования отдельных видов преступлений // Вестник Восточно-Сибирского института МВД России. 2017. № 2(81).
4. Андреев А.С. Посткриминальная деятельность как объект познания в криминалистике и практике расследования преступлений: дис. ... д-ра юрид. наук. Ростов н/Д, 2020.
5. Губанова О.В. Особенности расследования провокации взятки либо коммерческого подкупа: автореф. дис. ... канд. юрид. наук. Воронеж, 2006.

© Кулахсзян С.К., 2025

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ГЕНЕТИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ПРОШЛЫХ ЛЕТ: АНАЛИЗ ЭФФЕКТИВНОСТИ И ОГРАНИЧЕНИЕ МЕТОДА

Кулешова Ю.Г.

Преподаватель кафедры криминалистики и оперативно-разыскной
деятельности Ростовского юридического института МВД России,
кандидат биологических наук

В российском федеральном законодательстве термин «преступление прошлых лет» официально не используется. Однако данное понятие введено в ведомственный оборот приказом председателя Следственного комитета Российской Федерации (далее — СК РФ) А.В. Бастрыкина [1]. Под «преступлениями прошлых лет» понимаются уголовные дела, расследование по которым было приостановлено на основании ст. 208 УПК РФ в связи с тем, что следствию не удалось установить лицо, подлежащее привлечению в качестве обвиняемого [2]. На практике сюда относятся все нераскрытые дела за предыдущий год и раньше. Фактически можно отнести также и преступления, которые были выявлены много лет спустя после их совершения. Такие дела продолжают числиться в производстве, поскольку по ним сохраняется обязанность органов предварительного расследования принимать меры к установлению виновных лиц и возобновлению расследования при появлении новых данных.

Как правило, наибольшие трудности при установлении преступника возникают при расследовании насильственных преступлений — убийств и изнасилований, особенно когда отсутствуют очевидцы и свидетели. Со временем эти сложности лишь усиливаются: потенциальные свидетели

забывают детали произошедшего, переезжают, их становится трудно разыскать для допроса, а некоторые и вовсе уходят из жизни. Вследствие длительного промежутка времени многие следы преступления утрачиваются или не поддаются восстановлению, что существенно ограничивает возможности для назначения и проведения необходимых экспертиз. Все это отрицательно влияет на эффективность расследования и затрудняет установление личности виновного.

Многие преступления, совершенные десятилетия назад, так и остались нераскрытыми, в том числе из-за недостаточного уровня технического оснащения, который не позволял провести глубокий анализ доказательств. Однако развитие технологий открыло новые перспективы для их расследования. Современные методы судебных экспертиз и других криминалистических исследований дают возможность получать информацию, ранее недоступную следствию, тем самым значительно повышая вероятность установления причастных лиц.

Особое значение в этом процессе имеют молекулярно-генетические методы. Генетическая экспертиза включает в себя анализ ДНК, что позволяет идентифицировать личность человека, а также установить родственные связи. ДНК, оставленная на месте преступления, например, на орудии преступления, одежде жертвы или в биологических материалах (кровь, сперма, волосы), служит уникальным идентификатором. Генетические различия между людьми возникают из-за разнообразных изменений в ДНК, таких как замены отдельных нуклеотидов, вставки или удаления фрагментов, а также колебания числа повторяющихся последовательностей. Наибольшее практическое значение имеют микросателлитные STR-локусы. Благодаря высокой информативности и индивидуальной специфичности эти молекулярно-генетические маркеры широко применяются в криминалистике. Маркеры позволяют не только точно

идентифицировать, но и обеспечивают возможность анализа ДНК в самых разнообразных условиях. Кроме того, небольшие размеры STR-локусов позволяют получать достоверные результаты даже из небольшого количества генетического материала. Практика показывает, что ДНК-анализ является одним из самых результативных и динамично развивающихся направлений работы с вещественными доказательствами, обеспечивая высокую точность и объективность при идентификации лиц, причастных к преступлению. В ходе подобных исследований специалисты анализируют биологические материалы, изъятые на месте происшествия, что позволяет получать максимально точные и объективные результаты. Значительно расширяет возможности следствия и обязательное формирование ДНК-профилей лиц, числящихся пропавшими без вести [3]. Несмотря на то, что проведение молекулярно-генетических экспертиз требует значительного времени, именно их результаты нередко определяют дальнейший ход уголовного дела и оказывают решающее влияние на установление истины. При соблюдении всех необходимых условий ДНК может сохраняться в течение очень длительного времени, что позволяет использовать образцы даже спустя годы после происшествия. Именно поэтому сегодня данная группа преступлений может быть вновь расследована, если сохранились объекты, содержащие генетический материал, пригодный для анализа.

Показательным примером эффективности ДНК-исследований является дело, расследование которого СК РФ по Кемеровской области возобновил в апреле 2025 г. Речь шла об убийстве, совершенном в сентябре 1995 г. — тогда тело женщины было обнаружено в лесополосе [4].

После направления изъятых объектов на исследование с использованием современных возможностей геномной экспертизы экспертам удалось получить ДНК-профиль предполагаемого преступника. В результате личность фигуранта

была установлена: им оказался местный житель, который в дальнейшем дал признательные показания [5].

Данный пример демонстрирует, что даже спустя десятилетия (при условии надлежащего хранения либо возможности восстановления вещественных доказательств) современные молекулярно-генетические методы позволяют раскрывать преступления, ранее считавшиеся «холодными».

Тем не менее, генетическая экспертиза не всегда выступает универсальным средством в расследовании преступлений. Не во всех случаях удастся собрать достаточный объем биоматериала для исследования, особенно если событие произошло много лет назад. Кроме того, порой возникают трудности, связанные с качеством сохранности улик и высокой деградацией ДНК, что может быть обусловлено как неблагоприятными условиями хранения, так и ошибками изъятия. Нельзя исключать вероятность загрязнения биологического материала при ранее проведенных исследованиях, т. к. методики допускали использование недостаточно стерильных инструментов. Таким образом, к появлению чужеродной ДНК в объекте могут привести как нарушения при отборе, упаковке или транспортировке образцов, так и контаминация объектов при производстве первичных экспертиз. В дальнейшем такие материалы могут дать неточные либо искаженные данные при анализе, что приведет к неправильным выводам.

Несмотря на существующие сложности, современные методы молекулярно-генетической экспертизы дают правоохранительным органам возможность кардинально пересмотреть подход к расследованию преступлений прошлых лет. Вместе с тем, даже при высокой результативности такие исследования имеют свои ограничения и требуют особой тщательности, а также высокой профессиональной подготовки специалистов.

Литература

1. Об организации работы по расследованию уголовных дел о преступлениях прошлых лет: приказ СК России от 31.07.2014 № 65. Доступ из справ. правовой системы «КонсультантПлюс».

2. Следственный комитет РФ: официальный сайт [Электронный ресурс]. URL: <https://sledcom.ru/Proekty/Prestupleniya-proshlyh-let> (дата обращения: 02.10.2025).

3. Кулешова Ю.Г., Грибунов О.П. Современные проблемы использования генетической идентификации при проведении оперативно-розыскных мероприятий лиц, пропавших без вести, и неопознанных трупов в Российской Федерации // Юристъ-Правоведъ. 2025. № 1(112).

4. ТАСС. Геномная экспертиза позволила раскрыть в Кузбассе убийство 30-летней давности [Электронный ресурс]. URL: <https://tass.ru/obschestvo/23754509> (дата обращения: 02.10.2025).

5. Рамблер/Новости. Геномная экспертиза позволила раскрыть в Кузбассе убийство 30-летней давности [Электронный ресурс]. URL: https://news.rambler.ru/incidents/54556329-genomnaya-ekspertiza-pozvolila-raskryt-v-kuzbasse-ubiystvo-30-letney-davnosti/?utm_source=chatgpt.com (дата обращения: 02.10.2025).

© Кулешова Ю.Г., 2025

ВОЗМОЖНОСТИ ПРОГНОЗИРОВАНИЯ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ НА ОСНОВЕ АНАЛИЗА ПАТТЕРНОВ

Лемайкина С.В.

Старший преподаватель кафедры
информационно-коммуникационных технологий и кибербезопасности
Ростовского юридического института МВД России

В последние десятилетия вопрос предотвращения преступности стал одной из центральных задач для правоохранительных органов, т. к. безопасность граждан и общественный порядок находятся на первом месте в их деятельности. В условиях развития компьютерных технологий, а также с внедрением искусственного интеллекта, открываются новые горизонты для прогнозирования и предупреждения преступлений. И как результат, использование аналитических инструментов для изучения паттернов преступной активности, позволяет не только более эффективно распределять ресурсы полиции, но и значительно снижать уровень преступности в обществе. Паттерны преступности формируются на основе методов прогностического анализа, что подразумевает сбор необходимой информации.

Среди методов, которые активно применяются при анализе паттернов преступлений, выделяется несколько ключевых подходов. Так одним из ключевых подходов являются статистико-математические методы прогнозирования преступности, которые содержат в себе исключительно использование различных статистических и математических моделей для анализа данных о преступности и прогнозирования будущих тенденций. Эти методы могут варьироваться от применения временных рядов и анализа корреляции до использования регрессионного анализа. Исследователи

из Чикагского университета Йенс Людвиг и Кевин Шнепель из Университета Саймона Фрейзера в Бернаби, Британская Колумбия, входящем в состав Большого Ванкувера, обнаружили, что бедность и экономическое отчаяние могут толкать людей на имущественные преступления [1].

Сами по себе эти методы статистического анализа не новы: картирование преступности, например, используется правоохранительными органами уже даже не первое столетие. Но теперь сбор информации и ее доступность стали беспрецедентными, а обработкой этих данных занимаются уже не люди, а совсем другие вычислительные мощности. Алгоритм программы PredPol основан на разработках Института чистой и прикладной математики Калифорнийского университета. Систему обучают на статистических данных о преступлениях, совершенных в населенном пункте за последние 3–5 лет. Алгоритму требуются только три параметра каждого правонарушения: тип, место и дата/время его совершения [2]. В силу своей прикладной полезности статистические данные, касающиеся различных видов преступлений, использует полиция Лондона, для выявления временных периодов преступлений. Это позволяет полиции Лондона более эффективно распределять свои ресурсы и адаптировать патрулирование в зависимости от времени года или определенных праздников, когда, как правило, наблюдается рост преступности. Правоохранительные органы, применяя собранные и обработанные статистические данные, вырабатывает комплекс мер, направленных на усиление контроля в уязвимых районах Лондона, что является общей профилактикой преступности [3].

Выработка мер профилактики преступности вырабатывается не только с использованием статистического анализа, но и установлением пространственных характеристик преступлений. Высокую эффективность в данном анализе представляют географические информационные системы, которые позволяют визуализировать данные о преступлениях на картах,

что способствует выявлять районы с высокой концентрацией преступной активности. В Соединенных Штатах многие полицейские департаменты используют платформы типа CrimeMapping, которые позволяют отображать данные о преступлениях на интерактивных картах. Такие системы применяются для визуализации криминальной активности и анализа ее пространственных закономерностей [4]. Другим важным проектом в сфере прогнозирования преступности стала программа CompStat. С ее помощью полиция Нью-Йорка собирает данные о правонарушениях и анализирует их с использованием картографических и статистических методов. Вся информация в программе сосредоточена на картах, что предоставляет правоохрательным органам оценить эффективность полицейских стратегий и тактик. Программа стала основой для различных инициатив, направленных на оптимизацию работы полиции и повысила интерес к использованию данных в правоохрательных системах по всему миру [5].

Прогнозирование преступного поведения все чаще привлекает внимание сотрудников правоохрательных органов, так как возможность предвидеть совершение преступления предопределяет проведение комплекса конкретных мер по недопущению его совершения. Но в условиях стремительного роста преступности традиционные методы прогнозирования правонарушений нередко оказываются недостаточно результативными, т. к. они более медленные и менее эффективные. В связи с этим методы машинного обучения становятся важным инструментом прогнозирования преступности. В настоящее время преступный интеллект совершенствуется благодаря технологическому прогрессу. Следовательно, методы машинного обучения могут быть использованы для прогнозирования преступности благодаря обучению различным математико-статистическим функциям, способности обрабатывать большие объемы данных и множественным факторам. Используя алгоритмы, включая регрессионный анализ и кластеризацию, органы правопорядка могут

выделять факторы, влияющие на вероятность совершения преступления. Это дает возможность не только предсказывать, где и когда может произойти преступление, но и разрабатывать превентивные меры на основе полученных данных. Прогностические алгоритмы машинного обучения применяются, например, в ряде федеральных земель Германии, таких как Бавария, где правоохранительные органы используют системы машинного обучения для анализа сведений о преступлениях. Наиболее известной является система Precobs, которая используется не только в Германии (Бавария, Баден-Вюртемберг), но и в Швейцарии [6]. В этой системе данные о преступлениях обрабатываются с использованием методов машинного обучения, таких как кластеризация и классификация, что позволяет выявлять модели поведения преступников и определять факторы, способствующие совершению правонарушений. Данная информация потенциально может спасти жизнь жертвы, предотвратить психологическую травму и уберечь частную собственность от ущерба.

Прогностическую деятельность как эффективный инструмент применяют и российские правоохранительные органы, такие как МВД России, внедряют современные информационные системы для сбора и анализа данных о преступлениях, которые позволяют отслеживать количество, виды и географию преступлений. Примером таких систем является система «Безопасный город» и другие платформы для мониторинга [7]. В данных системах применяется статистические методы для выявления закономерностей в правонарушениях (например, анализ возрастного состава преступников или временных закономерностей в совершении преступлений).

Также отметим, что в МВД России реализуется проект «Конъюнктура», призванный использовать современные технологии анализа больших данных и статистических методов для мониторинга социальных и экономических процессов в стране. Основная цель системы — предсказывать и анализировать

состояние криминогенной обстановки на основе имеющихся данных, что позволяет эффективно управлять профилактикой преступности и повышением уровня безопасности. С помощью методов статистической обработки и машинного обучения система анализирует собранные данные для прогнозирования тенденций в области преступности. Это позволяет выявлять «горячие точки» — районы с повышенной вероятностью совершения правонарушений, а также указывать на потенциальные временные пики преступной активности.

Стремление государств обеспечить максимальный контроль за поведением граждан проявляется как в политическом, так и в правовом поле в сочетании с модернизацией цифровой инфраструктуры, необходимой для сбора данных, внедряемой на основе современных научно-технических разработок. Применение статистических методов, геопространственного анализа, машинного обучения и других подходов позволяет правоохранительным органам более эффективно выявлять и прогнозировать преступную деятельность, что, в свою очередь, способствует повышению общественной безопасности и снижению уровня преступности.

Литература

1. Here's why property crime and violent crime have different solutions [Электронный ресурс]. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.5cee6a1d-691c17cb-30a3c2b74722d776562/https/stacker.com/stories/news/heres-why-property-crime-and-violent-crime-have-different-solutions (дата обращения: 10.10.2025).

2. Искусственный интеллект научился предсказывать преступления: как ИИ помогает полиции [Электронный ресурс]. URL: <https://skillbox.ru/media/code/data-science-pomogaet-borotsya-s-prestupleniyami/> (дата обращения: 10.10.2025).

3. Скотланд-Ярд может взять на вооружение ПО, предсказывающее поведение преступников [Электронный ресурс]. URL: https://www.playground.ru/misc/news/skotland_yard_mozhet_vzyat_na_vooruzhenie_po_predskazyvayushee_povedenie_prestupnikov-116735 (дата обращения: 10.10.2025).

4. GIS for Crime Mapping: Smarter Policing with Geospatial Data [Электронный ресурс]. URL: <https://satpalda.com/gis-for-crime-mapping/> (дата обращения: 10.10.2025).

5. CompStat Policing: An Overview — SoundThinking [Электронный ресурс]. URL: <https://www.soundthinking.com/blog/compstat-policing-an-overview/> (дата обращения: 10.10.2025).

6. Применение систем предиктивной аналитики для борьбы с преступностью в Германии [Электронный ресурс]. URL: <https://dzen.ru/a/XVzQ4cbipACtIG6C> (дата обращения: 10.10.2025).

7. Безопасные города без зоопарка [Электронный ресурс]. URL: <https://habr.com/ru/companies/protei/articles/535550/> (дата обращения: 10.10.2025).

© Лемайкина С.В., 2025

ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ С ИНЫМИ СУБЪЕКТАМИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Маилян А.В.

Доцент кафедры криминалистики и оперативно-разыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

Как показывает анализ доктрины, достаточно большое число современных авторов и исследователей обращается к выявлению и изучению проблем, связанных с осуществлением взаимодействия оперативных подразделений с судом, органами прокуратуры и иными субъектами правоохранительной деятельности, так как от такого взаимодействия зависит и результативность правоохранительной деятельности, что является важным аспектом. Выявление имеющихся проблем в обозначенной сфере имеет практический характер, т. к. их разрешение позволит повысить эффективность и результативность взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности в российском государстве.

В целом всю совокупность проблем, возникающих при осуществлении взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности можно подразделить на следующие блоки:

- проблемы правового характера;
- проблемы организационного характера;
- проблемы информационного характера;
- социально-психологические проблемы;
- теоретико-доктринальные проблемы.

Рассмотрим мнения некоторых из исследователей на отдельные проблемы, связанные с осуществлением и реализацией взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности.

З.М. Яндырхарова выделяет такую проблему, как несвоевременное и некачественное выполнение поручений со стороны оперативных подразделений. Например, следователь, направляя в рамках расследования уголовного дела поручение оперативным подразделениям, далеко не всегда указывает срок его выполнения [1].

Данная проблема, выделенная автором, является одной из наиболее распространенной на современном этапе, т. к. не разработано и не установлено единой формы направления поручений.

По нашему мнению, З.М. Яндырхарова выделила важную проблему, которую необходимо разрешать, чтобы повышать степень эффективности и результативности взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности, в частности, со следственными подразделениями.

Схожую точку зрения также высказал А.В. Кудрявцев в своей научной работе и А.А. Сухов. Отметим, что это не единственные исследователи, которые придерживаются такой точки зрения, она получила достаточно широкое распространение в современной доктрине.

В связи со сказанным не редко такие поручения выполняются по истечении разумного срока.

По нашему мнению, для разрешения данной проблемы необходимо внести некоторые поправки в положения Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ) и ФЗ «Об оперативно-розыскной деятельности», предусмотрев статьи, которые будут регулировать порядок и организационное начало взаимодействия следственных и оперативных

подразделений при расследовании уголовных дел с соответствующими отсылками к необходимым подзаконным нормативным правовым актам.

А.В. Кудрявцев выделяет в анализируемой сфере такую проблему, как различие в задачах и приводит пример на оперативных подразделениях и участковых уполномоченных полиции.

Например, основной задачей участкового уполномоченного полиции является предотвращение и предупреждение административных правонарушений и преступлений.

При этом основной задачей оперативных подразделений органов полиции является выявление, пресечение и раскрытие преступлений.

Также А.В. Кудрявцев поднимает такую проблему, как разность в руководстве, что зачастую не позволяет должным образом организовывать и координировать взаимодействие оперативных подразделений с иными субъектами правоохранительной деятельности [2].

По нашему мнению, также следует выделить следующие проблемы осуществления взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности:

- отсутствие единого нормативно-правового регулирования, т. к. ни на уровне федеральных законов, ни на уровне подзаконных нормативных правовых актов российский законодатель не установил формы осуществления взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности; данная проблема должна быть устранена путем принятия нового акта, например, подзаконного ведомственного приказа МВД России;

- психологический аспект;

- отсутствие общих информационных ресурсов и порядка информационного обмена;

- зачастую халатное отношение к поручениям;
- отсутствие или ограниченность человеческого ресурса;
- отсутствие или ограниченность временного ресурса;
- низкий уровень технического оснащения оперативных подразделений;
- недостатки в действующем нормативно-правовом регулировании порядка взаимодействия.

Представляется, что в действующие положения УПК РФ необходимо предусмотреть возможность создания не только следственных групп (ст. 63 УПК РФ), но и следственно-оперативных групп, наделив, тем самым, последние процессуальными полномочиями на производство предварительного следствия.

В связи с этим в ст. 163 УПК РФ целесообразно установить, что руководитель следственного органа вправе принять решение о создании следственно-оперативной группы, о чем необходимо указать в постановлении о возбуждении уголовного дела или в постановлении о производстве предварительного следствия следственно-оперативной группой с указанием состава группы и о назначении руководителя, который принимает дело к своему производству.

Эффективность раскрытия, расследования и предотвращения преступлений в значительной степени зависит от четко налаженной и согласованной деятельности следователя и органов, осуществляющих оперативно-розыскную деятельность, сочетания процессуальных и оперативно-розыскных форм получения доказательств и установления истины по делу [3].

По нашему мнению, является очевидным тот факт, что один следователь и даже группа следователей без помощи органов дознания не в состоянии справиться с расследованием многих преступлений, как и без помощи оперативных подразделений.

Взаимодействие данных субъектов обусловлено, прежде всего, тем, что, как следователь, так и органы дознания, обладают специфическими, только им присущими, средствами раскрытия преступлений.

Также необходимо расширять теоретико-доктринальные основы о проблемах осуществления и реализации взаимодействия оперативных подразделений с иными субъектами правоохранительной деятельности.

Литература

1. Яндырханов, З.М. Проблемы взаимодействия следователя и оперативных подразделений // Молодой ученый. 2013. № 6(53).

2. Кудрявцев А.В. Проблемы правового регулирования взаимодействия оперативных подразделений УИС с иными органами, осуществляющими ОРД // Пенитенциарная наука. 2022. № 18.

3. Суховой А.А. Деятельность оперативных подразделений на стадии предварительного расследования // Вестник Волгоградской академии МВД России. 2022. № 2(61).

© Маилян А.В., 2025

ПРОБЛЕМЫ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ

Максимов М.И.

Доцент кафедры криминалистики и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

Анализируя статистические данные МВД России о состоянии преступности, мы приходим к выводу о том, что, несмотря на снижение количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий в 2025 г. (– 9,5 %), общее количество нераскрытых киберпреступлений ежегодно лишь увеличивается [1].

На наш взгляд, это связано с несколькими факторами:

1. В большинстве случаев киберпреступность носят трансграничный и международный характер.
2. Преступная деятельность, связанная с информационно-телекоммуникационными технологиями, характеризуется многообразием способов (схем) совершения и сокрытия. Кроме того, нередко преступления совершаются высококвалифицированными специалистами в организованной форме.
3. Высокий уровень латентности.
4. Киберпреступность — глобальная угроза национальной безопасности страны.
5. Использование криптовалюты как средства преступления.

В настоящее время человечество сталкивается с измененной реальностью во всех своих отношениях. Люди живут, развиваются и неизбежно

взаимодействуют с высокими технологиями и искусственным интеллектом. Вышеуказанное обуславливает формирование проблемы противодействия киберпреступности, которая остро нуждается в теоретическом осмыслении ведомственной наукой на предмет определения эффективных средств и методов борьбы с ней.

Итак, считаем необходимым отметить, что понятие «киберпреступности» отсутствует в законодательстве, из-за чего возникают проблемы в правоприменении. На наш взгляд, в широком смысле киберпреступность — это преступления, совершаемые с использованием компьютера, сетевого устройства или компьютерной сети. Это широкая категория преступной деятельности, которая включает в себя все: от вредоносного программного обеспечения до социальной инженерии и более сложных нарушений безопасности. К сожалению, согласно данным официальной статистики подобного рода преступления достаточно тяжело выявить и раскрыть.

Как показало проведенное нами выборочное исследование указанной проблемы, на сегодняшний день существуют следующие тенденции киберпреступности, изучение которых позволит разработать механизм оперативно-розыскного противодействия:

Фишинговые атаки — это любой тип сообщения, который обманом заставляет получателя передать конфиденциальную информацию, например, данные для входа, коды безопасности или номер кредитной карты. Хотя фишинг не является «новым» киберпреступлением, атаки становятся все более изощренными и их сложнее идентифицировать [2].

Двумя распространенными типами вредоносных программ являются шпионские программы и рекламные программы.

1. Шпионское программное обеспечение (далее — ПО) отслеживает активность на устройстве и отправляет личную информацию напрямую хакерам, которые затем могут использовать ее для дальнейших атак.

2. Рекламное ПО наводняет систему рекламой и всплывающими окнами, замедляя работу компьютера и в конечном итоге повреждая его. Эти типы вредоносных программ часто маскируются под законные программы, поэтому пользователь не осознает негативных последствий, пока не становится слишком поздно [3, с. 40].

3. Атаки компрометации деловой электронной почты (BEC) — это особый тип фишинга, который в настоящее время находится на подъеме. В этом типе атаки хакер выдает себя за человека, обладающего авторитетом в компании — например, генерального директора или доверенного внешнего поставщика. Подделав адрес электронной почты этого человека, или получив несанкционированный доступ к его учетной записи, хакер отправляет кому-то сообщение, обманным путем заставляя его отправить ему конфиденциальную информацию или даже перевести средства [4].

4. К 2025 г. мошенничество в социальных сетях составило более 25 % всех убытков от онлайн-мошенничества, что вдвое больше, чем годом ранее. В отличие от других кибератак, которые обычно нацелены на пожилых людей, мошенничество в социальных сетях, как правило, более эффективно эксплуатирует молодых людей.

Самая распространенная попытка социального мошенничества, на которую следует обратить внимание, — это ложная реклама. Мошенники создают поддельную рекламу покупок в Интернете, которая побуждает людей покупать, но покупатель никогда не получит свою покупку. Возможности фиктивных инвестиций — еще один особенно успешный метод социального мошенничества, когда мошенник создает ажиотаж с помощью фальшивой учетной записи в социальной сети и пытается собрать средства для мошеннического инвестиционного предприятия.

5. Вредоносный криптомайнинг. Цены на криптовалюту могут падать, но криптоджекинг растет. Объем криптоджекинга во всем мире в первой

половине 2025 г. вырос на 35 % по сравнению с 2024 г. Вредоносный криптомайнинг (также известный как криптоджекинг) предполагает использование чужого компьютера, телефона или планшета для добычи цифровых денег или криптовалют. Проще говоря, это может работать следующим образом: человек по незнанию загружает на свое устройство вредоносное ПО для майнинга криптовалют.

Вредоносная программа незаметно работает в фоновом режиме, добывая криптовалюту. Если криптоджекеру удастся развернуть свое вредоносное ПО на достаточном количестве компьютеров, он сможет запустить прибыльную операцию по добыче криптовалюты, полностью построенную на компьютерах других людей. В отличие от других киберпреступлений, вместо кражи данных или денег криптомайнинг крадет ресурсы (Интернет, электричество, вычислительную мощность компьютера) для финансовой выгоды.

6. Отраслевой таргетинг. Хотя ни одна отрасль не является защищенной от атак, некоторые из них кажутся более привлекательными для киберпреступников, чем другие. После пандемии Covid-19 здравоохранение, в частности, стало огромной целью. Всего за первые 5 месяцев 2023 г. общее количество утечек медицинских данных удвоилось по сравнению с тем же периодом в 2022 г. В 2025 г. произошли массовые атаки на базы данных различных ведомств и служб, включая налоговые органы, МВД России, ФСБ России и т. д.

Проанализировав специальную литературу и правоприменительную деятельность органов внутренних дел, мы с уверенностью можем сделать вывод о том, что в уровень программного обеспечения и подготовки сотрудников достаточно низок, в отличие лиц, осуществляющих преступную деятельность. На наш взгляд, наиболее действенными инструментами противодействия киберпреступлениям являются [5, с. 46]:

1. Тактически грамотная организация и проведение оперативно-розыскных мероприятий.

2. Оперативно-розыскная методика выявления и раскрытия киберпреступлений (дистанционное мошенничество, хищения денежных средств путем присвоения или растрат, фальшивомонетничество), подразумевающая комплексное в указанных целях использование негласных сил, средств, методов и мероприятий [6, с. 89].

3. Совершенствование системы оперативно-розыскного документирования преступных действий лиц, специализирующихся на их совершении, и их соучастников.

4. На основе общей концепции оперативно-розыскной политики разработка частной ее составляющей в области борьбы с киберпреступностью [7, с. 436–437].

5. Нормативно-правовое совершенствование уголовного, уголовно-процессуального и оперативно-розыскного законодательства. В частности, закрепление термина «киберпреступность» и иных, часто используемых в процессе раскрытия и расследования.

Перечень мер противодействия не является исчерпывающим, он может быть дополнен с учетом современных вызовов и новых видов киберпреступлений. На наш взгляд, также необходимо своевременно повышать квалификацию сотрудников специализированных подразделений для того, чтобы они могли «идти в ногу со временем».

Литература

1. Статистика и аналитика МВД России [Электронный ресурс]. URL: <https://мвд.рф/dejatelnost/statistics> (дата обращения: 10.12.2025).

2. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. № 2.

3. Чуб И.С. Мошенничество в сети Интернет: способы совершения и виктимологическая профилактика // Вестник Краснодарского университета МВД России. 2024. № 1.

4. Гаврилин Ю.В., Аносов А.В., Баранов В.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: уч. пособие. М., 2019.

5. Варданян А.В. Криминалистическая характеристика посткриминальной деятельности по делам о преступлениях в сфере информационных технологий // Сибирские уголовно-процессуальные и криминалистические чтения. 2021. № 2.

6. Иванов П.И. Оперативно-розыскное противодействие киберпреступлениям (проблемы и пути их решения) // Труды Академии управления МВД России. 2022. № 4(64).

7. Иванов П.И. Концептуальные основы формирования оперативно-розыскной политики: понятие, сущность и содержание // Вестник Владимирского юридического института. 2022. № 2(63).

© Максимов М.И., 2025

АКТУАЛЬНЫЕ ПРОБЛЕМЫ НАЛОЖЕНИЯ АРЕСТА НА КРИПТОВАЛЮТНЫЕ АКТИВЫ

Малянова К.П.

Заместитель начальника кафедры
криминалистики и оперативно-разыскной деятельности
Ростовского юридического института МВД России
кандидат юридических наук, доцент

За последние десять лет криптовалюты трансформировались из узкоспециализированного феномена цифровых сообществ в глобальный финансовый инструмент, активно используемый в трансграничных расчетах, инвестиционной деятельности и в качестве средства сбережения. Актуальность темы обусловлена стремительным ростом криптовалютного рынка и увеличением числа судебных споров, связанных с цифровыми активами. Отсутствие единых правовых механизмов их ареста и конфискации создает трудности для правоприменительной практики и международного сотрудничества. Возникла необходимость в проведении анализа правовых и практических аспектов наложения ареста на криптовалютные активы, выявление проблем и предложение направлений их решения.

По данным аналитической платформы транзакций блокчейна Chainalysis (2023), в последние годы объем мирового рынка криптовалют превысил триллионы долларов, что неизбежно привело к росту числа гражданско-правовых и уголовных дел, связанных с цифровыми активами. Одновременно с этим усиливается внимание государства и международных организаций к проблемам правового регулирования криптовалют, их налогообложения и использования в противоправных целях. Арест криптовалютных активов

как мера обеспечения исполнения судебных решений или как инструмент пресечения преступной деятельности становится особенно востребованным.

В научной доктрине и нормативных актах отсутствует единое определение криптовалютных активов. С точки зрения экономико-правовой характеристики, криптовалюта представляет собой децентрализованный цифровой код (токен), создаваемый и обращающийся в распределенных реестрах (блокчейне), который может выполнять функции средства обмена, накопления или инвестиционного инструмента. В США криптовалюта в зависимости от контекста рассматривается как товар, ценная бумага либо как средство платежа. Европейский союз в регламенте MiCA закрепил понятие «криптоактива» как цифрового представления стоимости или прав, которое может быть передано и сохранено с использованием распределенного реестра. В Российской Федерации Федеральный закон «О цифровых финансовых активах, цифровой валюте и внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ закрепил понятие «цифрового финансового актива» и «цифровой валюты», но не приравнял криптовалюту к законному средству платежа. Криптовалютные активы признаются имуществом, которое может выступать объектом гражданских прав, однако их использование в расчетах ограничено.

Криптовалютные активы обладают рядом особенностей, которые принципиально отличают их от традиционных объектов гражданского оборота. Традиционные активы имеют материальную форму либо закреплены в централизованных реестрах, привязаны к национальной юрисдикции и регулируются ее законодательством. Банковские счета и ценные бумаги обслуживаются централизованными институтами, что позволяет относительно просто применять меры ареста. Криптовалюта не имеет физического выражения и существует исключительно в цифровой форме как запись

в распределенном реестре (блокчейне), что осложняет ее изъятие и хранение в рамках ареста. Криптовалютные активы существуют в децентрализованных системах, не подчиненных единому эмитенту или регулятору, что, в свою очередь, исключает возможность классической блокировки через государственные или банковские механизмы. Данный цифровой механизм может свободно перемещаться через границы без участия посредников, в данном случае возможны затруднения в области контроля, требуется активное межгосударственное взаимодействие и международное сотрудничество. Дополнительное осложнение создает возможность использования анонимных цифровых монет, например, Monero, Zcash. Для традиционных активов существуют правовые механизмы регистрации, передачи в качестве депозита денег, ценных бумаг на хранение в депозитарий и ведение учета. Для криптовалют, в свою очередь, критическим является владение приватным ключом, который обеспечивает доступ к активу, и потеря которого делает арест фактически невозможным.

Арест имущества в современном российском законодательстве рассматривается как мера принудительного характера, применяемая судебными или исполнительными органами, которая ограничивает право собственника распоряжаться, а в некоторых случаях использовать или владеть имуществом. Целью ареста выступает обеспечение исполнения судебного решения, обязательств должника или предотвращение сокрытия активов. Арест не влечет прекращения вещного права, но непосредственно накладывает государственно-принудительные запреты на распоряжение и пользование соответствующими активами [1].

В гражданском процессе арест имущества выступает средством гарантирования эффективности будущего исполнения судебного решения. Он препятствует отчуждению или сокрытию имущества должником, тем самым

защищая интересы кредиторов и обеспечивая реальность судебной защиты. Объектами ареста могут выступать вещи и имущественные права, включая денежные средства на счетах, бездокументарные ценные бумаги и иные активы, находящиеся в распоряжении должника. В уголовном процессе арест имущества используется преимущественно для обеспечения возможной конфискации, возмещения ущерба потерпевшему и исполнения штрафных санкций. В данном контексте арест служит инструментом, препятствующим легализации или сокрытию доходов, полученных преступным путем, а также обеспечивает сохранность объектов, которые в дальнейшем могут быть признаны орудиями преступления. Особенность правовой природы ареста заключается в том, что он сочетает в себе как частноправовые, так и публично-правовые элементы.

Применение института ареста к цифровым активам, включая криптовалюту, связано с рядом принципиальных особенностей. Арест криптовалюты возможен лишь при установлении контроля над приватным ключом, обеспечивающим управление активом. Отсутствие контроля в данном случае делает фактическое исполнение ареста невозможным. Необходимо отметить, что децентрализованный характер криптовалют затрудняет применение традиционных механизмов блокировки. Отсутствие единого эмитента или посредника означает, что государственные органы не могут возложить обязанность по заморозке актива на финансовую организацию [2]. Единственным исключением являются криптовалютные биржи и кастодиальные сервисы, которые выступают как «точки входа» и позволяют на практике исполнять решения об аресте. В процессе осуществления ареста криптовалютных активов необходимо учитывать специфические технические риски хранения. Нарушение протоколов безопасности способно привести

к утрате ценностей, что выделяет криптовалюту из числа традиционных объектов ареста.

Принятие Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» стало важным шагом к формированию правовой базы регулирования цифровых активов в России. Закон вступил в силу с 1 января 2021 г. и закрепил основные понятия и механизмы, касающиеся цифровых финансовых активов (ЦФА) и цифровой валюты. Цифровые финансовые активы определяются как цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества и право требования передачи эмиссионных ценных бумаг. Фактически они выступают в качестве цифровых аналогов классических финансовых инструментов, выпускаемые и обращающиеся в информационных системах на основе блокчейн-технологий. Несмотря на значительный скачок в реализации технического прогресса, в части закрепления базовых дефиниций закон имеет ряд существенных ограничений, выраженный, в первую очередь, в запрете на использование криптовалюты в качестве средства платежа. В соответствии с законом, криптовалюта может использоваться только как объект инвестиции или обмена, но не как законное средство расчетов на территории РФ, что резко сужает сферу ее практического применения. Закон устанавливает правовой режим цифровых финансовых активов, которые выпускаются в регулируемых информационных системах, но не учитывает глобальный характер криптовалют, не закрепляет за цифровой валютой единого правового статуса: в одних доктринальных описаниях она рассматривается как имущество, в других, в свою очередь, как объект цифровых прав [3].

В качестве предложения по совершенствованию российского законодательства в области регулирования цифровых активов и криптовалюты следует рассмотреть перспективы внедрения смарт-контрактов для правоприменения. Смарт-контракты представляют собой самовыполняющиеся программные коды, работающие на основе технологии блокчейн, которые автоматически реализуют заложенные в них условия при наступлении заранее определенных событий. Смарт-контракт может быть встроен в инфраструктуру цифровых активов, обеспечивая автоматическую блокировку или перевод криптовалюты при вступлении решения суда в силу, что исключает необходимость в посредниках в виде банков и регистраторов и снижает риски уклонения должника от исполнения обязательств. Все операции, закрепленные в смарт-контракте, фиксируются в блокчейне и не могут быть изменены задним числом. Поскольку криптовалютные активы и смарт-контракты функционируют в глобальных сетях, их использование может служить эффективным инструментом при международном сотрудничестве.

Проведенный анализ показал, что феномен криптовалютных активов ставит перед правом и правоприменительной практикой целый ряд принципиально новых вызовов. Правовая природа ареста традиционно понимается как мера обеспечения, направленная на сохранение имущества для последующего исполнения судебного решения либо конфискации. Однако применительно к цифровым активам она приобретает новые черты: эффективность ареста напрямую зависит не только от процессуального решения суда, но и от фактического контроля над приватными ключами или централизованными площадками хранения. В данном случае классические юридические конструкции вынуждены адаптироваться к технологическим особенностям блокчейн-инфраструктуры. Сравнительный анализ зарубежной

практики, в частности дела Silk Road в США, показал, что арест криптовалюты возможен, но требует комплексных решений, сочетающих правовые и технические инструменты. Российское регулирование в рамках закона «О цифровых финансовых активах цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» заложило основу для оборота цифровых прав, но оставило значительные пробелы в отношении криптовалюты, где отсутствует четкий правовой статус цифровой валюты, отсутствуют специальные процедуры ареста и конфискации, а также механизмы международного сотрудничества.

В этой связи особую актуальность приобретает вопрос разработки специальных правовых и технологических решений. Перспективным направлением видится использование смарт-контрактов для автоматизации исполнения судебных актов, а также создание государственных криптокошельков для безопасного хранения арестованных активов. Дополнительно необходима оптимизация национального законодательства с международными стандартами, что позволит повысить эффективность трансграничного правоприменения.

Литература

1. Бодяко А.В., Пономарева С.В., Рогуленко Т.М. Идентификация цифровых прав в качестве объекта учета и контроля // Учет. Анализ. Аудит. 2021. № 5.

2. Кайгородова О.С. Решение вопроса о возможности наложения ареста на цифровые финансовые активы, цифровую валюту // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1(35).

3. Кошелев К.А. Определение категории «цифровые финансовые активы»: экономический, правовой и учетный аспекты // Инновации и инвестиции. 2021. № 2.

4. Рощупкина А.В. Проблемы изъятия, ареста и замораживания виртуальных активов в России и за рубежом // Вестник Удмуртского университета. Серия «Экономика и право». 2025. № 1.

5. Луданина А.В. Наложение ареста на криптовалютные активы в уголовном процессе Российской Федерации: возможные пути развития // Актуальные проблемы Российского права. 2023. № 6.

6. О цифровых финансовых активах, цифровой валюте и внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31. 07. 2020 № 259-ФЗ. Доступ из справ. правовой системы «Гарант».

© Малянова К.П., 2025

ПРОБЛЕМА ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ НАРКОТИКОВ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ

Миронов Г.Ю.

Старший преподаватель кафедры
криминалистики и оперативно-разыскной деятельности
Ростовского юридического института МВД России

Оглядываясь в прошлое, где компьютеры и Интернет в целом существовали лишь в выдумках писателей-фантастов, сложно поверить, что на данный момент мы все живем в высокотехнологичном мире, где почти каждый процесс является в той или иной мере автоматизированным с помощью сложных алгоритмов действий.

Больше не нужно хранить все деньги в кошельке и вечно таскать их с собой — для этого есть более удобная банковская карта, незачем проводить время в библиотеке, чтобы найти нужную информацию — для этого есть поисковые системы. Все сферы жизнедеятельности, в которых, так или иначе, человек является субъектом, получили свою возможность «переродиться» в мире киберпространства — и, к сожалению, не только лишь положительные.

Многие функции, изначально придумывающиеся и разрабатываемые для более комфортного пребывания человека в Сети — ВПН-сервера, позволяющие соблюдать анонимность, защищенная от инфляции криптовалюта, обмен которой происходит свободно от наблюдения вышестоящих банков (по крайней мере, в этом было убеждение до нынешних событий), социальные сети, предусматривающие засекреченное шифрование, роботы для рекламы своей продукции — все это и многое другое стало орудием в руках преступности.

Прогресс, едва лишь его запустишь, уже не остановим — и поэтому, несмотря на попытки со стороны правоохранительных органов и государства пресечь развитие данных инструментов, несмотря на быструю реакцию, на каждый метод защиты пользователей от потенциально вредной информации создаются новые схемы, на каждое действие, направленное на предупреждение — противодействие.

Таким образом, можно сделать вывод, что увеличение числа цифровых аспектов в повседневной жизни сделало преступления и виктимизацию в киберпространстве обычным явлением. Как подмечают представители правоохранительных органов по всему земному шару, уровень киберпреступности неуклонно рос в течение последнего десятилетия, и, вероятно, по-прежнему недостаточно регистрируется — ввиду невозможности полностью охватить это явление. Увеличение активности киберпреступников означает, что транзакции, связанные с доходами от преступлений, все чаще совершаются полностью или частично в киберпространстве.

Особенно актуальной проблемой в современном мире является проблема противодействия незаконному обороту наркотиков через Интернет. Проблема противодействия наркотрафику через Интернет приобрела поистине огромные масштабы.

Управление ООН по наркотикам и преступности (далее — УНП ООН) характеризует незаконный оборот наркотиков как всемирную незаконную торговлю, связанную с выращиванием, производство, распространение и продажа химических веществ, запрещенных законом.

Продавцы наркотиков варьируются от мелких дилеров, продающих скромные количества, до высокоорганизованных групп и корпораций, работающие как реальный бизнес. Покупатели приходят из всех слоев

общества, начиная от рабочего класса до самой верхушки, и принадлежат к любой этнической принадлежности и полу.

Исследования показывают, что молодые люди особенно в подростковом возрасте являются наиболее распространенными потребителями незаконных наркотиков по сравнению с другими поколениями.

В России проблема с распространением наркотиков через сеть Интернет приобрела совершенно новые масштабы после пандемии Covid-19. В конце января 2023 г. Министерство внутренних дел Российской Федерации (далее — МВД России) обнародовало статистику по преступности в стране. В частности, в нее вошли показатели противозаконных действия с использованием информационных технологий. Как отмечает МВД России, показатели киберпреступности в целом остались стабильными — с использованием высоких технологий совершается каждое четвертое преступление. Не то, чтобы эта стабильность могла сильно обрадовать — ее сохранение на прежнем уровне обозначает, что тех мер, что применяются на данный момент, недостаточно.

Более тревожным выглядит то, что в МВД России было зарегистрировано на 21 % больше преступлений по факту сбыта наркотиков через Интернет. Зашифрованные рынки привлекательны для покупателей и продавцов более низкими ценами, бесконтактными транзакциями и большим разнообразием доступных наркотиков. Продавцы и покупатели наркотиков адаптировались, и стали чаще использовать службы зашифрованных сообщений, приложения для социальных сетей, курьерские службы и службы доставки на дом.

Европейский центр мониторинга наркотиков и наркомании также отметил «тревожное развитие» потребления и доступности «крэка» с начала вспышки Covid-19. Еврокомиссар по внутренним делам И. Йоханссон сказала,

что она «особенно обеспокоена очень чистыми и сильнодействующими веществами, доступными на наших улицах и в Интернете, а также 46 новыми наркотиками, обнаруженными в ЕС только в 2020 году».

В глобальном масштабе прибыль рынка наркотических веществ, продаваемых через сеть Интернет, превысила прибыль от международного незаконного наркобизнеса, а предполагаемые затраты для отдельных лиц, корпораций и общества составляют от миллиардов до одного триллиона долларов США. Организованные преступные группы все шире используют Интернет в своей деятельности.

Общий размер нового онлайн-рынка психоактивных веществ неизвестен, но несколько показателей указывают на то, что он стремительно расширяется. Таможня сообщает об увеличении количества изъятий наркотиков, доставляемых по почте и предположительно с онлайн-рынков. Еще одной особенностью нового онлайн-рынка является его повышенная способность уклоняться от вмешательства правоохранительных органов за счет повышенного уровня анонимности и шифрования.

Секретные подсети Интернета, первоначально разработанные для военных целей и широко известные как Даркнет, образуют технологическую платформу для новых онлайн-рынков наркотиков: на маркетплейсах, расположенных в Даркнете, наркотики продаются открыто, но личности и местонахождение участников, а также сам маркетплейс маскируются. Самые сложные из них интегрируют различные анонимизирующие технологии и сервисы, предлагая удобный и относительно безопасный способ продавать и покупать незаконные вещества онлайн.

Технологии, на которых работают торговые площадки, постоянно развиваются, из-за чего методы отслеживания и борьбы с ними устаревают стремительно. Помимо Даркнета, выгодной площадкой для продажи

наркотиков как на территории РФ, так и на территории иностранных государств стал Telegram, с его ориентацией на анонимность и шифрование.

Первое преимущество Telegram, которое предлагает наркоторговцам, — высокая степень анонимности и конфиденциальности. В отличие от некоторых других популярных мессенджеров, Разговоры с использованием «Секретного чата» имеют сквозное шифрование, что означает, что никакие данные из чата не хранятся в каком-либо центре обработки данных, и никто, кроме участников чата, не может прочесть или расшифровать сообщения. Вторым же плюсом является то, что Telegram позволяет пользователям охватить широкую аудиторию и связываться с другими пользователями Telegram, которых они не знают. Приложение позволяет вести большие групповые чаты с участием до 200 000 пользователей, которых можно искать по интересам.

Как только чаты исчезают с мобильных устройств пользователей, они исчезают навсегда. Между тем, самоуничтожающиеся сообщения позволяют дилерам рекламировать свои товары с помощью временных изображений и видео без каких-либо опасений. Хотя WhatsApp предлагает сквозное шифрование для всех разговоров, прошлое участие компании в скандалах с обменом данными сказалось на ее репутации. Те, кто ищет безопасности, переехали в другое место. По данным TechAdvisor, Telegram также собирает меньше информации о пользователе, включая IP-адрес и тип устройства, на котором работает пользователь, чем WhatsApp. Telegram стал популярной альтернативной службой обмена сообщениями во всем мире после того, как WhatsApp, самая популярная в мире служба обмена сообщениями, внесла изменения в свою политику обмена информацией в начале 2021 г. Ранее WhatsApp были замешаны в скандалах с обменом данными и их утечкой, на фоне чего Telegram продвигал свою политику конфиденциальности, утверждая, что никогда не делился данными с властями. Именно это привлекло

к нему не только обычных граждан, нуждающихся в спокойствии за личные данные, но и преступные элементы, рассматривающие потенциал платформы для создания и продвижения рынков наркотиков. Продажа наркотиков в такой социальной сети, как VK, представляется для наркоторговцев сложной задачей ввиду того, что VK по запросу следствия выдает данные страницы, но, тем не менее, при помощи покупных номеров и зарегистрированных на эти номера ботов осуществляется реклама каналов Telegram.

Путем поиска групп, связанных с продажей наркотиков, пользователи могут находить дилеров и общаться с ними. Он также имеет функцию «Найти людей поблизости», которая позволяет людям общаться с другими людьми, включая торговцев наркотиками, в пределах определенного географического диапазона.

Несмотря на то, что онлайн-рынок незаконных веществ по-прежнему составляет небольшую долю от общего рынка наркотиков, его быстрый рост и растущая способность к сокрытию требуют особого внимания.

Анонимные сети на сегодняшний день представляют особый интерес для полиции: по сути, преступники, чувствуя себя в безопасности имеют возможность представить большое количество доказательств своих преступлений, но при этом следует учитывать, что надежное шифрование пока не поддается взлому для всех практических целей, и, конечно же, его невозможно взломать в контексте рутинных полицейских операций. Именно поэтому автор статьи считает целесообразным задуматься об увеличении количества специалистов, обладающих специальными знаниями в области технологий, в полиции, а также обучению основам действующих сотрудников.

Стоит сказать, что первый крипторынок был обнаружен примерно в 2010 г. и что он «подал пример, которому другие следовали с точки зрения

бизнес-модели, безопасности и прибыли». В то время как полиция работает над тем, чтобы закрыть сайты, когда это возможно, появляются новые.

При закрытии одного сайта могут появляться два или три его «зеркала» — аналогичных сайта со слегка измененной адресной строкой, который предлагают доступ к запрещенному полицией контенту. Эта проблема усугубляется, но вовсе не из-за отсутствия усилий со стороны правоохранительных органов, а из-за невозможности контроля в интернете как таковом.

Правоохранительным органам может быть сложно пресечь торговлю наркотиками на международном крипторынке, но разработка и тестирование новых инструментов и методов повысит вероятность того, что незаконный импорт будет перехвачен властями, когда они проходят по почте.

В рамках данного исследования следует выделить несколько рекомендаций. Во-первых, перед Российской Федерацией стоит необходимость увеличения финансирования для борьбы с этой проблемой. Как уже было ранее сказано, рынок наркотиков развивается стремительно, а потому и методы противодействия, отслеживания и сбора криминалистически важной информации должны непрерывно обновляться.

Необходима также совместная деятельность по формированию профессиональной готовности к борьбе с наркоторговлей в социальных сетях. Интернет-торговля наркотиками — это глобальное явление, требующее скоординированных международных действий. Иными словами текущий уровень знаний об анонимных рынках наркотиков довольно ограничен и разбросан, рекомендуемой отправной точкой является сбор существующих на международном уровне знаний и передовой практики. Политические и экономические партнеры, такие как Латинская Америка и Китай, разработали свои методы противодействия распространению наркотиков через сеть Интернет, в том числе и через Telegram. Международные

профессиональные сети полезны как для сбора, так и для распространения знаний. На национальном уровне актуальная и практическая информация должна быть доступна профессионалам на всех уровнях командной цепочки.

Литература

1. О внесении изменений в некоторые акты Правительства Российской Федерации в связи с совершенствованием контроля за оборотом прекурсоров наркотических средств и психотропных веществ: постановление Правительства РФ от 22.02.2019 № 182. Доступ из справ. правовой системы «КонсультантПлюс».

2. Отчет о ситуации с наркотиками в Китае за 2021 г. [Электронный ресурс]. URL: http://www.nncc626.com/2022-06/23/c_1211659746.htm (дата обращения: 10.09.2025).

3. Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. 2016. № 8.

4. Васюков В.Ф. Расследование дел о сбыте наркотиков с использованием мессенджеров и криптовалюты // Уголовный процесс. 2019. № 9(177).

5. Польшерт А.В. Наркотическое средство как элемент криминалистической характеристики его незаконного сбыта путем использования электронных и информационно-телекоммуникационных сетей // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2017. № 15–1.

6. Мельцов В.М., Бекмешова М.А. Противодействие сотрудниками ОВД «бесконтактным» методам сбыта наркотиков / Научное и образовательное пространство: перспективы развития: материалы Междунар. научно-практ. конф. Чебоксары, 2017.

7. Васильева Н.А. Анализ цифровых платформ в сфере незаконного оборота наркотиков для построения криминалистической характеристики данного вида преступлений // Юридическая наука. 2020. № 2.

8. European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) [Электронный ресурс]. URL:http://www.emcdda.europa.eu/publications/emcdda-papers/using-open-source-information_en (дата обращения: 12.04.2023).

9. Hawdon J, Parti K, Dearden T. Changes in Online Illegal Drug Buying during Covid-19: Assessing Effects due to a Changing Market or Changes in Strain using a Longitudinal Sample Design. Am J Crim Justice. 2022. № 47. 712-734. doi: 10.1007/s12103-022-09698-1. Epub. 2022. № 11 (дата обращения: 10.09.2025).

10. Otiashvili, D., Mgebrishvili, T., Beselia, A. et al. The impact of the Covid-19 pandemic on illicit drug supply, drug-related behaviour of people who use drugs and provision of drug related services in Georgia: results of a mixed methods prospective cohort study. Harm Reduct J 2022. № 25<https://doi.org/10.1186/s12954-022-00601-z> (дата обращения: 10.09.2025).

© Миронов Г.Ю., 2025

**ПРОБЛЕМНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ
ПОДРАЗДЕЛЕНИЙ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Мясников А.П.
профессор кафедры
государственно-правовых дисциплин
Ростовского филиала Российской таможенной академии,
доктор юридических наук, профессор

Функционирование оперативно-розыскной деятельности (далее — ОРД) в пенитенциарной среде — это специфический механизм защиты правопорядка. В условиях высокой концентрации криминального элемента ОРД становится единственным способом раскрытия преступлений, совершаемых осужденными или персоналом. Но как трансформировать оперативную информацию в судебное доказательство?

Здесь кроется ключевой изъян системы. Эффективность работы прямо коррелирует с возможностью легитимизации данных в рамках уголовного процесса. Однако существующий разрыв между ФЗ «Об ОРД» и требованиями Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ) порождает неразрешимые коллизии. Почему законодатель до сих пор не синхронизировал эти нормы?

1. Правовая природа результатов ОРД и коллизии их признания доказательствами.

Основным камнем преткновения в теории и практике остается вопрос о том, что именно считать «результатами ОРД». Согласно ст. 11 Федерального

закона «Об ОРД», результаты могут быть использованы в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства [1, с. 14].

Однако статья 89 УПК РФ устанавливает жесткий запрет: в процессе доказывания запрещается использование результатов ОРД, если они не отвечают требованиям, предъявляемым к доказательствам самим Кодексом [2, с. 42]. Подобное положение дел закономерно провоцирует возникновение «процессуального фильтра», становящегося непреодолимой преградой на пути реализации оперативных задач. Оперативный уполномоченный УИС нередко владеет исчерпывающим массивом сведений о готовящейся дезорганизации деятельности исправительного учреждения, однако эти данные остаются юридически мертвыми до момента их легализации. Разве может оперативная осведомленность подменить собой процессуальный акт? Безусловно, нет. Пока добытая информация не будет надлежащим образом облечена в форму протоколов следственных действий, она не приобретет статус доказательства и не будет иметь веса для суда.

Такой разрыв между фактическим знанием и его правовым закреплением неизбежно девальвирует прогностический потенциал ОРД, превращая ценные сведения в «вещь в себе», неспособную повлиять на исход уголовного дела.

Как отмечает профессор К.К. Горяинов, результаты ОРД сами по себе не являются доказательствами, а выступают лишь сведениями об источниках данных, которые могут стать доказательствами после их проверки следственным путем [3, с. 112]. В условиях исправительной колонии это осложняется тем, что «источниками» часто выступают лица из числа спецконтингента, чья явка к следователю или в суд нежелательна по соображениям безопасности или оперативной этики.

2. Процедурные сложности представления результатов ОРД следователю.

Процедура передачи материалов из оперативных подразделений УИС в органы предварительного следствия жестко регламентирована межведомственной Инструкцией. Однако на практике основным препятствием становится избыточный формализм. Нередко сотрудники оперативных отделов СИЗО и колоний допускают критические ошибки еще на этапе вынесения постановлений о проведении ОРМ. К чему это приводит?

Результат предсказуем: дефекты в оформлении документации неизбежно влекут за собой признание полученных доказательств недопустимыми в рамках судебного разбирательства. Такая ситуация обнажает серьезную проблему профессиональной подготовки кадров и несовершенства самих бюрократических механизмов. В итоге кропотливая работа по изобличению преступных деяний нивелируется из-за несоблюдения процедурных нюансов, что позволяет виновным лицам избегать ответственности по сугубо формальным основаниям.

В частности, при проведении «оперативного эксперимента» или «контрольной закупки» (например, при попытке доставки наркотиков в колонию) крайне важно задокументировать отсутствие провокации. С.И. Захарцев подчеркивает, что результаты ОРД должны позволять сформировать доказательства, удовлетворяющие критерию относимости и законности [4, с. 204]. Отсутствие в представленных оперативниками УИС материалах четкого подтверждения законности оснований для проведения ОРМ ставит следователя в крайне затруднительное положение. Он будет вынужден отклонить данные сведения. Почему это происходит так часто? Прежде всего, из-за опасения «развала» уголовного дела непосредственно в судебном заседании. Любое процессуальное упущение на доследственной стадии подрывает фундамент обвинения.

Следовательно, игнорирование правовых критериев при документировании оперативной информации превращает ее в бесполезный балласт, который невозможно интегрировать в доказательственную базу. Такая вынужденная осторожность следственных органов выступает защитной реакцией на системное несоблюдение юридических формальностей оперативными службами, что в конечном итоге нивелирует усилия по борьбе с пенитенциарной преступностью.

3. Проблема рассекречивания сведений и защита источников.

Необходимость обеспечения безопасности вынуждает оперативников максимально скрывать свои методы. Однако закон требует прозрачности. Если использование результатов ОРД в суде неизбежно ведет к деанонимизации негласного сотрудника или раскрытию дислокации технических средств, ведомство зачастую выбирает сохранение тайны, а не успех преследования. Можем ли мы жертвовать агентурной сетью ради разового процессуального успеха? Разумеется, нет.

Такой приоритет конфиденциальности закономерно ограничивает объем информации, передаваемой следствию, что вновь сужает доказательственные возможности. В итоге специфический режим секретности в УИС выступает объективным барьером, препятствующим полноценной легализации оперативных данных и создающим условия для латентности многих преступлений.

Согласно ст. 12 Федерального закона «Об ОРД», сведения об используемых силах, средствах, методах и лицах, оказывающих содействие на конфиденциальной основе, составляют государственную тайну [1, с. 16]. В условиях пенитенциарной системы раскрытие конфиденента равносильно его физическому устранению со стороны преступной среды. Поэтому оперативники УИС часто сталкиваются с дилеммой: либо представить полные

данные и «расшифровать» агента, либо подать информацию в усеченном виде, рискуя, что она не будет принята как доказательство.

В.М. Аتماжитов указывает, что существующий механизм защиты свидетелей и конфиденентов в рамках уголовного процесса (например, допрос под псевдонимом) в условиях замкнутого пространства колонии работает слабо [5, с. 88]. Осужденные легко вычисляют «осведомителей» по косвенным признакам, что делает легализацию результатов ОРД крайне рискованным мероприятием.

4. Использование результатов ОРД в дисциплинарной и профилактической практике.

Использование сведений ОРД для дисциплинарного воздействия или профилактики в рамках УИК РФ — вопрос не менее значимый. Здесь стандарты доказывания ощутимо ниже, чем в уголовном процессе. Однако снимает ли это проблему легитимности? Правовая неопределенность сохраняется и здесь.

Зачастую оперативные данные становятся единственным основанием для взыскания, что при отсутствии четких регламентов порождает риск административного произвола. Такая ситуация размывает грань между правомерным пресечением нарушений и ущемлением прав личности. В конечном итоге, дефицит законодательного регулирования в этой сфере делает профилактическую функцию ОРД уязвимой для оспаривания, что подчеркивает необходимость синхронизации норм УИК и закона об ОРД.

Оперативные подразделения УИС часто используют ОРД для выявления каналов поступления запрещенных предметов (телефонов, дрожей, алкоголя). Если данные предметы изымаются в ходе обыска, основанного на оперативной информации, само «оперативное сопровождение» в протоколе обыска часто не фигурирует. Это создает «серую зону», где законность действий

администрации учреждения может быть оспорена адвокатами осужденных как «беспричинный обыск» [6, с. 54].

5. Проблемы межведомственного взаимодействия.

Оперативные подразделения ФСИН России часто передают материалы в СК РФ или МВД РФ. На стыке ведомств возникают конфликты интерпретации. Следователи нередко предъявляют к результатам ОРД избыточные требования, по сути, требуя от оперативников выполнения следственных функций.

А.В. Шахматов отмечает, что отсутствие единого понимания «достаточности» результатов ОРД для возбуждения уголовного дела приводит к тому, что до 30 % материалов, направляемых из УИС в следственные органы, возвращаются для дополнительной проверки или по ним выносятся отказы [7, с. 142]. Это снижает мотивацию оперативного состава и создает почву для безнаказанности лидеров отрицательной направленности среди осужденных.

Подводя итог, можно выделить следующие ключевые направления решения проблем использования результатов ОРД в УИС:

1. Законодательное закрепление. Необходимо более четко прописать в УПК РФ механизм упрощенного признания результатов ОРД доказательствами, если они получены с соблюдением всех конституционных прав граждан.

2. Техническая модернизация. Широкое внедрение средств аудио- и видео-фиксации при проведении ОРМ в колониях позволит снизить зависимость от показаний конфиденентов.

3. Обучение кадров. Повышение юридической грамотности оперативного состава УИС в вопросах уголовного процесса для минимизации брака при оформлении материалов.

4. Усиление защиты информации. Разработка протоколов использования данных без раскрытия тактических приемов ОРД.

Эффективность борьбы с преступностью в местах лишения свободы возможна только при условии, что «негласная» информация будет находить свое логическое завершение в справедливом судебном приговоре.

Литература

1. Об оперативно-розыскной деятельности: федер. закон № 144-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».
2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон № 174-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».
3. Горяинов К.К., Овчинский В.С., Сенилов Г.К.. Теория оперативно-розыскной деятельности: учебник. М., 2020.
4. Захарцев С.И. Наука оперативно-розыскной деятельности: философский, теоретико-правовой и прикладной аспекты. СПб., 2011.
5. Ахмажитов В.М., Бобров В.Г. О законодательном регулировании использования результатов оперативно-розыскной деятельности в доказывании по уголовным делам // Государство и право. 2015. № 9.
6. Кузнецов С.А. Оперативно-розыскная деятельность в учреждениях уголовно-исполнительной системы: уч. пособие. Рязань, 2018.
7. Шахматов А.В. Использование результатов оперативно-розыскной деятельности в уголовном процессе: вопросы теории и практики. СПб., 2019.
8. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России № 776, ФСБ России № 703, ФСО России № 509, СВР России № 81, ФТС России № 1820, ФСИН России № 534, ФСКН России № 396, Минобороны России № 622 от 27.09.2013.

© Мясников А.П., 2025

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРИМЕНЯЕМЫЕ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Назаров С.Н.
профессор кафедры
криминалистики и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
доктор юридических наук, профессор

Стремительная цифровая интеграция провоцирует качественную мутацию преступности. Криминал осваивает киберпространство. Это факт. Следовательно, перед субъектами оперативно-розыскной деятельности (далее — ОРД) встает вопрос тотальной ревизии имеющегося инструментария.

Насколько сегодня важна скорость работы с «цифровыми следами»? Она критична. Эффективность ОРД теперь жестко детерминирована способностью системы оперативно верифицировать колоссальные массивы данных. С.С. Галахов справедливо характеризует информационное обеспечение ОРД как структурированную совокупность процессов сбора, депонирования и поиска сведений, необходимых для раскрытия преступных посягательств [1, с. 142].

Резюмируя, отмечу: технологический уклад меняет саму природу сыскной работы. Теперь информационный ресурс — это не просто вспомогательный элемент, а базис, без которого правоохранительный механизм теряет свою функциональность.

Правовые основы применения ИТ в ОРД

Применение ИТ-ресурсов в оперативной практике подчинено строгому нормативному вектору. Центральное место здесь занимает Федеральный закон

«Об оперативно-розыскной деятельности». Согласно ст. 6 данного акта, использование информационных систем, аудио- и видео-фиксации легитимно лишь при условии их безопасности для жизни, здоровья и экологии [2]. Допустимы ли здесь исключения? Закон категоричен.

Однако цифровизация не означает правовую вседозволенность. Соблюдение конституционных прерогатив личности остается приоритетом. Внедрение инноваций не может служить оправданием для обхода процессуальных фильтров. Как подчеркивает Конституционный Суд РФ, любая фиксация частных коммуникаций требует судебного санкционирования. Технологический формат передачи данных не меняет правовую суть ограничения тайны переписки [3, с. 88].

Таким образом, законодатель устанавливает жесткий паритет между эффективностью розыска и неприкосновенностью частной жизни. Анализ правоприменительной практики показывает: без судебного контроля любая цифровая улика рискует стать юридически ничтожной.

Автоматизированные информационные системы (АИС)

Специализированные учеты и распределенные базы данных составляют фундаментальный базис информационного обеспечения ОРД. Современные АИС (автоматизированные информационные системы) обеспечивают бесшовную интеграцию ведомственных сегментов — от МВД до Росреестра и ФНС. Зачем это нужно? Такая синергия радикально минимизирует временные затраты на верификацию связей между субъектами.

В доктрине сложилось устойчивое мнение: автоматизация поиска позволяет эксплицировать латентные закономерности в поведении организованных преступных групп [4, с. 215]. Вручную такой массив данных обработать невозможно. Это аксиома. Сегодня инструментарий не ограничивается классическими дактилоскопическими системами вроде АДИС «Папилон». В арсенал внедрены интеллектуальные платформы

распознавания лиц, интегрированные в городские экосистемы (например, АПК «Безопасный город»).

Анализируя текущий технологический стек, можно сделать вывод: современная ОРД эволюционирует в сторону предиктивной аналитики. Эффективность системы теперь измеряется не глубиной архивов, а скоростью межуровневого взаимодействия нейросетевых алгоритмов и государственных реестров.

Технологии Big Data и предиктивная аналитика

Перспективным вектором развития выступает внедрение технологии Big Data. Она открывает доступ к глубокой обработке неструктурированного контента: от массивов OSINT до данных социальных медиа и мессенджеров. Как это работает на практике? Алгоритмы выявляют скрытые корреляции там, где человеческий глаз видит лишь цифровой шум.

Предиктивная аналитика трансформирует саму стратегию контроля, позволяя с высокой точностью детерминировать «горячие точки». Это локации максимальной концентрации криминогенных рисков. Прогнозирование вероятности совершения преступлений перестает быть футуристической теорией, становясь прикладным инструментом оперативного планирования.

Однако, как справедливо замечает В. И. Кузнецов, применение таких методов требует высокой квалификации кадров: «Оперативный сотрудник сегодня должен обладать компетенциями IT-аналитика, чтобы эффективно использовать результаты работы алгоритмов в доказательственной базе» [5, с. 47].

Технологии OSINT и мониторинг открытых данных в ОРД

Вектор информационного обеспечения ОРД смещается в сторону Open Source Intelligence (OSINT). Это динамичное направление. Значимый массив сведений сегодня сосредоточен в публичном доступе: от детализированных профилей в социальных сетях и тематических форумов

до государственных реестров и геолокационных меток. Большая часть данных лежит на поверхности. Нужно лишь уметь их извлекать.

Согласно позиции А.Ю. Шумилова, текущая стадия развития ОРД знаменует переход от инертной аккумуляции сведений к активному мониторингу инфосферы для выявления признаков готовящихся деликтов [4, с. 248]. Применение автоматизированных скраперов позволяет оперативным аппаратам верифицировать скрытые интерперсональные связи. Как это проявляется? Элементарный анализ метаданных фотоснимков, размещенных в разное время, способен неопровержимо подтвердить факт коллизии или совместного пребывания субъектов в конкретной локации.

Параллельно фиксируется запрос на глубокую аналитику криптоактивов. Трансграничный криминал активно эксплуатирует цифровые валюты для легализации преступных доходов. Это заставляет внедрять специализированный софт для аудита блокчейн-транзакций. Специалисты по цифровой криминалистике подчеркивают: вопреки мифу об анонимности, блокчейн представляет собой транспарентный реестр [7, с. 189]. При наличии релевантных IT-инструментов деанонимизация бенефициаров становится лишь вопросом времени и вычислительных мощностей.

Искусственный интеллект и биометрическая идентификация

Внедрение систем искусственного интеллекта (далее —ИИ) в практику ОРД осуществляется по нескольким стратегическим векторам. Во-первых, это биометрическая верификация. Алгоритмы позволяют идентифицировать личность не только по антропометрическим параметрам лица, но и по паттернам походки или акустическим характеристикам голоса. Эффективно ли это? Да, поскольку современные системы способны распознать объект даже при намеренном использовании масок или иных средств маскировки.

Во-вторых, ИИ незаменим в сфере лингвистического анализа. Автоматизированный скрининг контента в экстремистских сообществах

позволяет вычленять латентные призывы к противоправным действиям и идентифицировать вербовщиков. Машина видит то, что скрыто за эзоповым языком.

Однако массированное использование ИИ порождает острые дискуссии о «цифровом профилировании». Правоведы выражают обоснованную обеспокоенность тем, что алгоритмическая предвзятость может деформировать фундаментальный принцип презумпции невиновности [6, с. 112]. Если выводы нейросети будут восприниматься как истина в последней инстанции без надлежащей оперативной верификации, риск необоснованного ограничения прав граждан многократно возрастает. Технология должна помогать, а не замещать процессуальную логику.

Проблемы и вызовы

Несмотря на технологический прогресс, существует ряд проблем:

- **Техническое отставание:** Преступные сообщества зачастую быстрее внедряют средства шифрования и анонимизации (VPN, Darknet).
- **Межведомственные барьеры:** Отсутствие единого информационного контура между правоохранительными органами разных стран затрудняет раскрытие трансграничных киберпреступлений.
- **Защита данных:** Сами базы данных ОРД становятся объектами атак, что требует усиления мер кибербезопасности [7, с. 302].

Информационные технологии в рамках ОРД де-факто перестали быть сугубо прикладным элементом. Сегодня это доминирующий фактор успешной нейтрализации криминальных вызовов. Какое будущее нас ждет? Приоритетным вектором видится глубокая интеграция нейросетевых архитектур с классическими оперативно-розыскными методиками. Разумеется, подобный симбиоз допустим лишь в условиях жесткой приверженности принципам законности и охраны конституционных прав личности.

Цифровой прогресс неумолим. Следовательно, назрела объективная необходимость в оперативной модернизации профильного законодательства. Правовые нормы обязаны коррелировать с темпами технологической экспансии, чтобы не допустить возникновения правовых вакуумов. Только при условии гармонизации нормативной базы и инновационного инструментария государственное принуждение останется эффективным в цифровой реальности.

Литература

1. Галахов С.С. Оперативно-розыскная деятельность: учебник для вузов. М., 2023.
2. Об оперативно-розыскной деятельности федер. закон от 12.08.1995 № 144-ФЗ // Собрание законодательства РФ. 1995. № 33. Ст. 3349.
3. Безруков С.В. Конституционные основы деятельности органов внутренних дел: уч. пособие. Омск, 2021.
4. Шумилов А.Ю. Курс основ оперативно-розыскной деятельности: учебник. М., 2020.
5. Кузнецов В.И. Цифровизация оперативно-розыскной деятельности: современные вызовы // Вестник криминалистики. 2022. № 4(84).
6. Григорьев В.Н. Искусственный интеллект в правоохранительной сфере: научно-практ. пособие. М., 2022.
7. Овчинский В.С. Криминология цифрового мира: учебник. М., 2021.

© Назаров С.И., 2025

ОСОБЕННОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННОЙ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТЬЮ

Пономарева А.В.

Старший преподаватель кафедры криминалистики
и оперативно-разыскной деятельности
Ростовского юридического института МВД России

Правовые основы борьбы с незаконным предпринимательством в России охватывают нормы гражданского, административного, уголовного и налогового законодательства. Комплексный подход к регулированию данной сферы позволяет минимизировать риски для экономики, защищать добросовестных предпринимателей и обеспечивать соблюдение принципов законности в предпринимательской деятельности. Эффективное противодействие нелегальной предпринимательской деятельности требует не только законодательных изменений, но и активной позиции государства. Усиление межведомственного взаимодействия, повышение квалификации сотрудников правоохранительных органов и внедрение современных технологий контроля способствуют снижению уровня теневого бизнеса.

Преступления, связанные с незаконной предпринимательской деятельностью, обладают определенными криминалистическими особенностями, которые проявляются в специфике их субъектов, способов совершения, следов преступлений и используемых доказательств. Анализ криминалистической характеристики данного вида преступлений позволяет эффективно организовывать процесс их расследования, выявлять преступников и минимизировать экономические риски, связанные с подобными правонарушениями.

Раскрытие преступлений, связанных с незаконной предпринимательской деятельностью, представляет собой сложный процесс, требующий детального анализа финансовых потоков, хозяйственной деятельности и документов субъектов, вовлеченных в преступные схемы. В отличие от традиционных преступлений, такие правонарушения нередко носят латентный характер, поскольку их участники стремятся скрыть следы противоправных действий, используя сложные экономические и юридические механизмы.

Анализ следственной практики позволяет выделить три основные ситуации, возникающие при расследовании преступлений, связанных с незаконной предпринимательской деятельностью:

1. Полная картина преступления — имеются документально подтвержденные факты незаконной предпринимательской деятельности, установлены большинство причастных лиц.

2. Частично установленная структура преступления — организатор и основные участники известны, но их местонахождение остается неопределенным.

3. Прекращенная деятельность — предприятие закрылось, деньги со счетов исчезли, личности преступников не установлены.

Наиболее распространенным сценарием является первый, когда у следствия уже имеются значительные доказательства.

Расследование преступлений в сфере незаконного предпринимательства требует комплексного подхода и детального анализа всех обстоятельств. При наличии полной картины нарушения следствие сосредотачивается на сборе и фиксации доказательств, идентификации виновных и установлении масштабов ущерба.

Первым делом производится изъятие документов у компаний, взаимодействующих с незаконными предпринимателями. Следователь получает санкцию на выемку бухгалтерских и юридических документов,

договоров, счетов-фактур, накладных и других финансовых бумаг. Далее анализируется переписка с контрагентами, банковские транзакции, акты выполненных работ и отчеты о поставках. Особое внимание уделяется фиктивным компаниям и подставным лицам, через которых осуществлялись нелегальные сделки.

Второй этап — проведение обысков в офисах и по месту жительства руководителей. Обыски помогают обнаружить скрытые финансовые отчеты, черновую бухгалтерию, электронные носители информации. Изъятие мобильных телефонов и компьютеров позволяет получить доступ к переписке, в том числе через мессенджеры и электронную почту. Важно зафиксировать любые попытки уничтожения улик или уклонения от ответственности.

Далее производится арест и изучение почтовых отправлений, финансовой документации. Отслеживаются почтовые отправления, в которых могут содержаться контракты, счета, документы о переводах средств. Финансовая документация анализируется на предмет сокрытия доходов, использования подставных счетов и офшорных схем.

Следующим шагом рассматриваемой тактики – это проведение ревизий и проверок, анализ их результатов, другими словами, осуществляется налоговый аудит, проверка отчетности о прибыли и убытках, контроль за кассовыми операциями. Ревизия помогает выявить расхождения между официальной отчетностью и реальными оборотами. Особое внимание уделяется неучтенным товарам, услугам и необоснованным расходам.

Путем оперативно-следственных мероприятий осуществляется установление мест ведения незаконной предпринимательской деятельности и их осмотр: производится обнаружение складов, производственных помещений, нелегальных офисов. При осмотре фиксируется состояние оборудования, сырья, полуфабрикатов, готовой продукции. Проводится подробное описание местонахождения, особенностей производства и условий работы.

Допросы подозреваемых, контрагентов и свидетелей проводятся с целью выявления схемы преступной деятельности, ролей участников, источников финансирования, установления реальных поставщиков, покупателей и посредников, а сотрудников контролирующих органов — для получения информации о выявленных нарушениях, ранее проведенных проверках и выявленных несоответствиях.

При осмотре мест ведения бизнеса и анализе финансовых потоков рассматривается движение денежных средств по банковским счетам, выявляются схемы отмывания денег и уклонения от налогов, определяются источники финансирования и конечные бенефициары, осуществляется контроль за наличными расчетами и фиксация неучтенных активов.

В качестве заключительного этапа рассматриваемой тактики расследования выступает назначение и проведение судебных экспертиз:

1. Экономическая экспертиза направлена выявление реального дохода, расчет налогов, подлежащих уплате.

2. В ходе судебно-бухгалтерской экспертизы анализируются бухгалтерские документы и выявляются фальсификации.

3. Дактилоскопическая и почерковедческая экспертизы проводятся с целью установления авторства подписей и почерка в документах.

4. При технико-криминалистической экспертизе документов подлежат выявлению подделки и изменения в документации.

5. Судебно-товароведческая экспертиза позволяет оценить стоимости изъятой продукции и оборудования.

Таким образом, комплексный подход к расследованию позволяет не только выявить всех участников схемы, но и предотвратить последующие преступления, а также привлечь к ответственности как организаторов, так и соучастников незаконной предпринимательской деятельности.

При расследовании преступлений, когда структура преступления установлена частично или деятельность незаконного предпринимателя прекращена, помимо проведения мероприятий, перечисленных выше, первостепенной и главной задачей становится установление местонахождения фигурантов дела и выявление соучастников. Для достижения поставленных задач применяются следующие методы расследования:

- опрос родственников, деловых партнеров, знакомых;
- оперативное наблюдение;
- анализ изъятых документов на предмет наличия информации о местонахождении участников схемы.

После установления подозреваемых проводится их задержание и личный обыск с изъятием документов и носителей информации.

Ключевые особенности построения версий при расследовании незаконного предпринимательства:

1. Опережающая оперативно-розыскная работа — криминалистические версии зачастую выдвигаются еще до возбуждения уголовного дела.

2. Акцент на выявление масштабов преступной деятельности — важно установить не только факт незаконного бизнеса, но и ущерб, причиненный государству.

3. Ограниченность круга подозреваемых — в отличие от общеуголовных преступлений, здесь фигуранты чаще всего связаны с предпринимательской средой.

Расследование преступлений, связанных с незаконным предпринимательством, требует детального анализа обстоятельств и построения различных версий, которые помогают следствию установить истинные мотивы, схемы и масштабы противоправной деятельности. В следственной практике существует ряд типичных версий по делам о незаконном предпринимательстве.

Первая версия предполагает, что деятельность велась без регистрации в налоговых органах, а именно, лицо или группа лиц осуществляли предпринимательскую деятельность, не ставя ее на учет в налоговых органах, что является нарушением ст. 171 УК РФ. Цель подобного ведения дел — избежание уплаты налогов, сборов и других обязательных платежей, а также сокрытие реальных доходов.

В данном случае противоправное деяние осуществляется с помощью подставных лиц для аренды помещений и открытия счетов, использования наличных расчетов без фиксации операций в бухгалтерской отчетности и отсутствия регистрации работников и заключения трудовых договоров.

При выявлении факта данного вида нарушения производится оперативная проверка через налоговые органы о наличии регистрации, изъятие финансовых документов и черной бухгалтерии, а также допрос свидетелей, контрагентов и клиентов.

В основе второй версии заложено предположение о том, что предпринимательская деятельность формально зарегистрирована, однако при подаче документов в налоговые органы или иные контролирующие структуры были предоставлены заведомо ложные сведения. В данном случае преступник преследует такие цели, как получение незаконных налоговых льгот, сокрытие реальных собственников и бенефициаров, уход от ответственности за финансовые нарушения.

Для ухода от ответственности и представления деятельности законной преступные лица осуществляют регистрацию фирмы на подставное лицо (например, безработного или иностранного гражданина), фальсификацию бухгалтерских отчетов, снижение прибыли или увеличение расходов для уменьшения налоговой базы и используют фиктивные договоры и акты выполненных работ.

В ходе следственных действий производится сравнение поданных документов с реальными данными о ведении бизнеса, финансово-экономическая экспертиза, проверка подписей и почерка на документах (почерковедческая экспертиза).

Суть третьей типичной версии заключается в том, что деятельность осуществлялась в сферах, подлежащих обязательному лицензированию, без соответствующего разрешения или с нарушением условий лицензии. Таким образом, преступник преследует избежание контроля со стороны органов лицензирования, увеличение прибыли за счет сокращения расходов на соблюдение нормативов, уклонение от налоговых и страховых выплат. В качестве примера данного типа нарушений из следственной практики можно привести:

1. Оказание медицинских услуг без лицензии.
2. Производство алкоголя или табачной продукции без акцизных марок.
3. Перевозка пассажиров или грузов без соответствующих документов.

Для выявления рассматриваемого правонарушения следствие осуществляет проверку реестра лицензий и разрешительных документов, опрос сотрудников контролирующих органов, осмотр помещений, оборудования и изъятие продукции.

Выдвижение и проверка приведенных типичных версий позволяет следствию установить истинные мотивы и методы незаконной предпринимательской деятельности, а также привлечь виновных к ответственности и предотвратить дальнейшие экономические преступления, а также на основании них планируется расследование, включающее анализ документов, допросы, экспертизы.

Эффективное расследование невозможно без координации с другими государственными структурами. В практической деятельности используются следующие формы взаимодействия:

1. Обмен информацией с контрольно-ревизионными органами на этапе возбуждения дела.
2. Совместные оперативные мероприятия с подразделениями по борьбе с экономическими преступлениями.
3. Оказание экспертной помощи (бухгалтерской, финансовой, товароведческого анализа).
4. Создание следственно-оперативных групп для комплексного расследования данных действий

На каждом этапе следственные органы сталкиваются с особыми задачами и вызовами, которые требуют применения криминалистических методов и участия профильных специалистов, однако некоторые этапы расследования требуют особого подхода, а именно.

1. Осмотр места происшествия для выявления доказательств, подтверждающих факт ведения незаконной деятельности, фиксации материальных следов преступления и идентификации ключевых участников схемы. Проводится в офисах, складах, производственных помещениях, а также жилых помещениях, где могли вестись расчеты или храниться документация. В качестве особенностей данного этапа рассмотрим следующие аспекты:

- 1.1. Фиксация материальных доказательств: оборудования, сырья, готовой продукции, финансовой документации, черновых записей.

- 1.2. Изъятие цифровых носителей (компьютеры, жесткие диски, флеш-накопители, серверы с данными о транзакциях и партнерах).

- 1.3. Анализ бухгалтерии и договоров, поиск расхождений между официальной отчетностью и реальными доходами.

1.4. Работа с цифровыми данными, восстановление удаленной информации, анализ переписки с контрагентами, проверка платежных систем.

1.5. Необходимость привлечения к следственным действиям специалистов (бухгалтеров, IT-экспертов, криминалистов по финансовым преступлениям), которые помогают выявить схемы уклонения от налогов и отмывания доходов.

Например, при выявлении подпольного цеха по производству контрафактной алкогольной продукции изымается оборудование, акцизные марки, накладные на поставку сырья и фиктивные лицензии. Эксперты проверяют подлинность документов и проводят химический анализ продукции.

2. Допрос подозреваемого для получения показаний, которые подтверждают или опровергают выдвинутые версии о незаконной деятельности. Особенности данного мероприятия является необходимость подготовки к допросу, а именно, анализ собранных доказательств, финансовых документов, показаний свидетелей, что позволяет ограничить возможности подозреваемого для манипуляции фактами и сокрытия реальных доходов. В подобном случае подозреваемому следует задать ряд ключевых вопросов для понимания полной картины противоправного деяния:

1. Как долго осуществлялась деятельность?

2. Кто поставлял оборудование и сырье?

3. Какие схемы использовались для уклонения от налогов и получения нелегальной прибыли?

4. С кем сотрудничали и какие финансовые операции проводили?

Особое внимание стоит уделить тактике допроса. Важно использовать факты, полученные в ходе осмотра места происшествия, проверки финансовых потоков и показаний свидетелей, сопоставлять показания с данными бухгалтерской отчетности, банковскими выписками и цифровыми следами,

а также наблюдать за поведением подозреваемого, отмечать эмоциональные реакции и ложные показания.

В качестве примера приведем следующий случай из следственной практики: в ходе допроса руководитель компании, занимающейся нелегальным производством косметики, отрицает факт ведения бизнеса. Однако следствие предоставляет доказательства закупки сырья через подставные фирмы и данные о реализации продукции через онлайн-платформы.

Комплексный подход на каждом этапе расследования позволяет не только собрать доказательства, но и выявить все звенья преступной схемы — от организаторов до посредников и клиентов. Участие специалистов, анализ цифровых данных и психологическая тактика допроса играют ключевую роль в успешном завершении следствия. Однако наибольшие трудности в расследовании вызывают следующие мероприятия:

Расследование незаконного предпринимательства требует четкого алгоритма действий: от сбора первоначальных данных до выявления полного круга лиц и подтверждения их вины. Важную роль играет взаимодействие между следственными органами, экспертами и контрольно-надзорными структурами. При этом каждое дело имеет свою специфику — от полного контроля ситуации до необходимости искать скрывающихся участников преступления. Соответственно, следственная тактика должна адаптироваться под конкретные условия расследования.

Исходя из всего вышесказанного, можно сделать вывод, что дела, связанные с незаконной предпринимательской деятельностью, требуют серьезного комплекса мероприятий для раскрытия, включая методы финансового анализа, оперативно-розыскные мероприятия, применение информационных технологий и экспертных исследований. Усиление контроля со стороны государства, слаженное взаимодействие его структур в отношении

предпринимательской деятельности способны сократить число экономических преступлений и укрепить правопорядок и честное предпринимательство.

Литература

1. Аксенова Л.Ю., Анешева А.Т. Анализ документов по делам о незаконном предпринимательстве // Закон и право. 2021. № 12.
2. Баканов М.А. Уголовно-правовая характеристика незаконного предпринимательства // Вестник Московского университета МВД России. 2022. № 6.
3. Волохова О.В. Особенности выявления незаконного предпринимательства и проверки сообщения о его совершении // Право и управление. 2023. № 1.
4. Еремян А.А. Незаконная предпринимательская деятельность // Символ науки. 2021. № 12–1.
5. Железников Е.А., Зубкова М.Н. Особенности проведения оперативно-розыскных мероприятий при расследовании экономических преступлений // Международный журнал гуманитарных и естественных наук. 2024. № 10–1.
6. Жилкин М.Г. Незаконное предпринимательство: вопросы межотраслевой дифференциации и квалификации // Имущественные отношения в РФ. 2021. № 3(234).
7. Цыденова Ц.Н. Проблемы квалификации преступлений в сфере экономики // Теория и практика современной науки. 2021. № 12(78).
8. Официальный интернет-сайт Министерства внутренних дел России. [Электронный ресурс]. URL: <https://мвд.рф/> (дата обращения: 10.09.2025).

© Пономарева А.В., 2025

**К ВОПРОСУ ОБ ИНФОРМАЦИОННОМ ОБЕСПЕЧЕНИИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ
ВНУТРЕННИХ ДЕЛ**

Семенцова И.А.

Доцент кафедры уголовного права и криминологии Ростовского
института (филиала) Всероссийского государственного
университета юстиции (РПА Минюста России),
кандидат юридических наук, доцент

Малявина А.Б.

Научный сотрудник научно-исследовательского
и редакционно-издательского отдела
Ростовского юридического института МВД России,
кандидат политических наук

В наши дни успешность оперативной работы органов внутренних дел в раскрытии и выявлении преступлений критически зависит от качества их информационного обеспечения. В условиях бурного развития и постоянного обновления инфокоммуникационных технологий, а также роста технического и финансового могущества преступного мира, совершенствование информационного обеспечения в МВД России становится приоритетным направлением повышения эффективности правоохранительной деятельности.

Оперативно-розыскная деятельность является одним из важнейших элементов выявления, предупреждения, пресечения и раскрытия преступлений. На эффективность и результативность данной деятельности влияет наличие информации, полученной своевременно. К такой информации относятся сведения о лицах, подозреваемых в совершении преступлений, скрывшихся обвиняемых, орудиях преступления, ценностях,

полученных преступным путем, о следах, относящихся к совершенному преступлению и других объектах и предметах, необходимых для раскрытия и расследования преступлений.

На сегодняшний день остро стоит вопрос о максимально эффективном использовании всех доступных ресурсов оперативно-розыскной деятельности для усиления борьбы с преступностью. В этом контексте, возможности информационного обеспечения оперативных подразделений органов внутренних дел играют ключевую роль [1].

Некоторые исследователи определяют обеспечение оперативно-розыскной информацией как совокупность тактических действий, направленных на получение и эффективное использование фактических данных. Однако, раскрытие преступлений — лишь одна из задач оперативно-розыскных органов. Не менее важным является выявление преступлений, которое возможно благодаря анализу входящей информации.

В научной литературе информационное обеспечение расследования преступлений определяется как комплекс мероприятий, осуществляемых различными подразделениями правоохранительных органов, направленных на получение из гласных и негласных источников криминалистической, оперативной и процессуальной информации, ее фиксацию, хранение, обработку, анализ, а также использование первичных и обогащенных данных с целью выполнения следователями и оперативными подразделениями возложенных на них функций [2].

Согласно ст. 6 Федерального Закона «Об оперативно-розыскной деятельности», оперативно-розыскные мероприятия направлены на сбор информации, представляющей оперативный интерес [3]. Информационное обеспечение в оперативно-розыскной деятельности также закреплено в ст. 10 Федерального закона «Об оперативно-розыскной деятельности». В данной

статье засвидетельствовано, что органы, наделенные полномочиями на осуществление оперативно-розыскной деятельности, могут формировать и использовать различные информационные системы, позволяющие хранить и систематизировать собранные результаты работы, а также создавать дела оперативного учета.

Основными информационными ресурсами, используемыми в процессе информационно-аналитической работы в расследовании преступлений, являются:

- оперативные учеты, которые состоят из оперативно-розыскных, криминалистических и оперативно-справочных учетов;
- криминалистические учеты, которые состоят из оперативно-поисковых и информационно-справочных коллекций;
- банки данных криминологической, административной, статистической информации;
- банки данных других министерств, ведомств, предприятий, учреждений и организаций, которые не касаются непосредственно борьбы с преступностью;
- банки данных городских и областных органов власти;
- объекты предоставления и получения охранных услуг;
- операторы мобильной связи;
- обращения и заявления граждан;
- средства массовой информации, в частности Интернет.

Информационные учеты применяются в оперативно-розыскной деятельности как средство систематизации большого потока информации, получаемой в процессе осуществления задач, возлагаемых на органы внутренних дел. Стоит отметить, что содержательный аспект информационного обеспечения состоит в том, что отличие информационной системы от системы информации характеризуется следующим. Система информации представляет

собой определенный набор сведений и фактов, необходимых для реализации управленческой деятельности. В то время, как информационная система предназначена для обеспечения сотрудников ОВД необходимой и актуальной информацией, требуемой в конкретной обстановке и условиях [4].

Таким образом, сбор информации оперативными подразделениями играет важную роль при выявлении и раскрытии преступлений, выявлении преступников, и предопределяет ценность сведений, закладываемых в информационно-поисковые системы органов внутренних дел.

Оперативно-розыскная информация играет ключевую роль в выявлении и раскрытии преступлений. Эффективное использование таких источников, как агентурные данные [5], результаты оперативно-технических мероприятий, информация из уголовных дел и административных материалов, позволяет правоохранительным органам получать сведения о готовящихся, совершаемых или совершенных преступлениях, а также о лицах, к ним причастных [6].

При этом важно подчеркнуть необходимость строгого соблюдения законности и прав граждан при сборе и использовании оперативно-розыскной информации. Баланс между обеспечением безопасности и защитой прав и свобод является определяющим фактором эффективности оперативно-розыскной деятельности. Совершенствование нормативно-правовой базы и повышение профессиональной подготовки сотрудников, работающих с оперативно-розыскной информацией, будут способствовать повышению результативности борьбы с преступностью.

Для эффективного накопления значимой оперативной информации требуется объединенная сеть вычислительных центров с унифицированным ПО и определение оптимальных уровней ее концентрации.

При этом сбор информации — не самоцель оперативно-розыскной работы. Важен анализ и сопоставление поступающих данных. Только

тщательный анализ целенаправленно собранной информации обеспечивает решение задач оперативных подразделений.

Таким образом, постоянное изучение теории информационно-аналитической деятельности ОВД, включающей сбор, систематизацию, анализ и использование информации, а также соблюдение требований при работе с оперативно-розыскной информацией, способствует успеху в выявлении и раскрытии преступлений.

Главный информационно-аналитический центр МВД России координирует информационное обеспечение деятельности ОВД, играя ключевую роль в обработке и предоставлении учетной информации.

Подразделения оперативно-розыскной информации МВД России обеспечивают оперативно-аналитическое сопровождение субъектов оперативно-розыскной деятельности, формируя единое информационное пространство оперативных подразделений полиции и создавая оперативно-розыскные прогнозы. Информация подразделений оперативно-розыскной информации, как правило, оперативного, справочного и аналитического характера, оказывает ценную помощь в раскрытии преступлений.

Интегрированный банк данных (ИБД-Регион) также является источником информации для ОВД, улучшая качество информационного обеспечения.

Единая система информационно-аналитического обеспечения деятельности (ИСОД) МВД России, объединяющая автоматизированные системы обработки информации, служит для организации централизованного хранения и обработки данных.

СМИ и Интернет являются быстрыми источниками актуальной информации для оперативных подразделений.

Международное сотрудничество правоохранительных органов в сфере борьбы с преступлениями также способствует информационному обеспечению ОВД.

Организирующую и направляющую роль, а также функцию информационного обеспечения в деле борьбы с международной преступностью призвана выполнять международная уголовная полиция — Интерпол, в состав которого входит и Российская Федерация [5]. Деятельность оперативных подразделений ОВД по взаимодействию с Интерполом осуществляется, в соответствии с нормативными правовыми актами Российской Федерации, через Национальное центральное бюро Интерпола МВД России.

Резюмируя, нужно сказать, что совершенствование информационного обеспечения деятельности оперативных подразделений ОВД — назревшая необходимость. Оно достижимо формированием собственных оперативных и справочных учетов, а также обеспечением постоянного пополнения информационных систем оперативно-значимой информацией всеми оперативными подразделениями МВД России. Такие информационные системы должны обобщать различные сведения, достаточные для быстрого, оперативного поиска интересующей информации, позволяющей своевременно выявлять преступления, обеспечивать их эффективное раскрытие.

В заключение, эффективность целевого накопления информации является ключевым фактором успеха в любой сфере деятельности. Сосредоточенное накопление релевантной информации позволяет оптимизировать процессы принятия решений, повысить качество исследований и разработок, а также сократить временные и финансовые затраты.

Литература

1. Захарцев С.И., Игнащенков Ю.Ю., Сальников В.П. Оперативно-розыскная деятельность в XXI веке. М., 2015.
2. Белов О.А. Информационное обеспечение раскрытия и расследования преступлений: автореферат дис. ... кандидата юридических наук: М., 2007.

3. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «Гарант».

4. Зорин В.С. Актуальные проблемы прокурорского надзора за исполнением законов органами, осуществляющими оперативно-розыскную деятельность // Legal Bulletin . 2023. № 3.

5. Пронин К.В. Краткий курс по оперативно-розыскной деятельности. М., 2017.

6. Грибунов О.П. Техничко-криминалистическое обеспечение раскрытия и расследования преступлений: отдельные аспекты современного состояния / Криминалистические чтения на Байкале-2015: материалы Междунар. научно-практ. конф. Иркутск, 2015.

© Семенцова И.А., Малявина А.Б., 2025

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Снежкова Ж.Ю.

Старший преподаватель кафедры криминалистики
и оперативно-розыскной деятельности
Ростовского юридического института МВД России

Оперативная обстановка на территории Российской Федерации, особенно в приграничных районах продолжает оставаться сложной. Преступные группы, а также отдельные лица выбирают в качестве объектов преступного посягательства важные объекты инфраструктуры, школы и больницы, инженерные сети, очистные сооружения и объекты благоустройства.

На страже общественной безопасности, а также безопасности личности и государства стоит система государственных правоохранительных органов, которые решают задачи противодействия преступности в рамках своих должностных полномочий. К их числу относятся оперативные подразделения территориальных органов МВД России, играющие существенную роль в выявлении, предупреждении, пресечении и раскрытии преступлений согласно Федеральному закону «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (далее — ФЗ «Об ОРД»).

К оперативно-розыскной деятельности помимо мероприятий, прямо перечисленных в ФЗ «Об ОРД», можно отнести и привлечение к конфиденциальному содействию лиц, ведение специфической финансовой деятельности, информационное обеспечение и документирование. В настоящем законе четко определен перечень возможных оперативно-розыскных

мероприятий, таким образом, применение новых форм и способов оперативного проникновения в криминальную среду приостановлено, т. к. использование любого нового способа сбора оперативной информации требует, чтобы он соотносился с прописанными в законе оперативно-розыскными мероприятиями [1].

В научной литературе проблемы, касающиеся полномочий субъектов оперативно-розыскной деятельности, порядка и специфики осуществления ими своей деятельности рассматривали Г.А. Берестова, Н.Н. Бухаров, О.А. Кислый, М.В. Лукашин, О.Б. Абакумов и др.

Оперативно-розыскная деятельность — это вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то Федеральным законом, в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств [6].

Задача оперативных подразделений выявлять тайно подготавливаемые и совершаемые преступления, применяя при этом особые методы в рамках проведения различных оперативно-розыскных мероприятий, осуществляя их гласно и негласно.

В юридической литературе под субъектами оперативно-розыскной деятельности в узком смысле понимаются органы, реализующие такую деятельность, на которые законодательно возложены полномочия, предоставлены для выполнения права и утверждены юридическая ответственность в случае их ненадлежащего исполнения [3].

Оперативно-розыскная деятельность неизбежно затрагивает права и свободы человека и гражданина, так как осуществляется не только в отношении лиц, совершающих преступления, так и причастных к ним в силу определенных обстоятельств.

В теории оперативно-розыскной деятельности согласно их правовому положению ее субъектов классифицируют следующим образом. К первой категории можно отнести штатных сотрудников органов внутренних дел, осуществляющих оперативно-розыскную деятельность гласно и негласно. Во вторую категорию входят лица, участвующие в осуществлении отдельных оперативно-розыскных мероприятий. К третьей категории относятся субъекты, сотрудничающие с оперативными подразделениями на конфиденциальной основе.

К подразделениям, осуществляющим оперативно-розыскную деятельность по должности и наделенным всеми полномочиями по применению средств и методов оперативно-розыскной деятельности относятся:

- 1) подразделения уголовного розыска;
- 2) подразделения экономической безопасности и противодействия коррупции;
- 3) подразделения собственной безопасности;
- 4) подразделения по противодействию экстремизму;
- 5) подразделения по борьбе с преступными посягательствами на грузы;
- 6) подразделения по обеспечению безопасности лиц, подлежащих государственной защите;
- 7) оперативно-поисковые подразделения;
- 8) подразделения специальных технических мероприятий (оперативно-технические подразделения);
- 9) межрегиональные оперативно-розыскные подразделения территориальных органов МВД России на окружном уровне.

Нормативные правовые акты регулируют деятельность оперативных подразделений на федеральном, региональном и местном уровнях, необходимыми условиями реализации которой являются соблюдение

законодательства Российской Федерации, защита прав и свобод человека и гражданина, неотвратимость применения уголовного наказания на совершение противоправных деяний, активное привлечение граждан для оказания содействия в раскрытии и расследовании преступлений как гласно, так и негласно, соблюдение конфиденциальности при применении технических средств и приемов.

К основным нормативным правовым актам относятся Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Федеральный закон «Об оперативно-розыскной деятельности», Федеральный закон «О полиции». В них закреплены важные положения деятельности подразделений уголовного розыска и других субъектов ОРД в ОВД.

В рамках изменений, вносимых в законодательство, необходимо отметить, что в ст. 15 Федеральном законе «Об ОРД» № 144-ФЗ перечислены не все права, которые предоставляются оперативным сотрудникам. Например, среди них права, которыми наделены сотрудники полиции и нашедшие свое отражение в ст. 13 ФЗ «О полиции». В рамках мероприятий, осуществляемых гласно и негласно, при проведении конкретных мероприятий могут быть изъяты документы, предметы, материалы и сообщения, которые связаны с ограничением конституционных прав граждан, но только в случаях реальной угрозы жизни и здоровью граждан, а также безопасности Российской Федерации. Информация об изъятии материальных носителей обязательно отражается в соответствующем протоколе.

Не менее важными являются вопросы уголовной ответственности сотрудников оперативных подразделений, которые рассматривались такими учеными как Б.В. Волженкин, Б.В. Здравомыслов, Е.В. Львович.

Уголовным кодексом РФ урегулированы ситуации, касающиеся незаконного сбора информации, нарушения неприкосновенности частной жизни, когда сотрудники злоупотребляют должностными полномочиями

в своих целях и нарушают закон. К таким преступлениям относятся: злоупотребление служебными полномочиями, получение взятки, превышение и злоупотребление должностными полномочиями, дача взятки, посредничество во взяточничестве, служебный подлог.

Для предотвращения возможных злоупотреблений осуществление оперативно-розыскной деятельности подвергается внутреннему контролю со стороны непосредственного руководства территориальных органов и подразделений собственной безопасности, судебного контроля, осуществляемый при санкционировании судом проведения таких мероприятий как прослушивание телефонных переговоров, контроль почтовых отправлений, телеграфных и иных сообщений, а также общественный контроль.

При оценке деятельности субъектов ОРД правоприменитель руководствуется принципами, которые закреплены в нормативных документах, регулирующих общественные отношения в этой области. К ним относятся принцип конституционности; принцип законности, предполагающий недопущение требований законодательства; привлечение к ответственности должностных лиц, виновных в нарушениях; ведомственный контроль и прокурорский надзор за осуществлением оперативно-розыскной деятельности.

Оперативно-розыскное законодательство регламентирует некоторые механизмы реализации принципа конспирации. Например, органы ОРД предоставляют письменную информацию о собранных личных данных лица по его требованию, но объем предоставляемых сведений ограничен требованиями конспирации и наличием сведений, составляющих государственную или иную охраняемую законом тайну (ч. 4 ст. 5 ФЗ «Об ОРД») [2]. Одним из необходимых условий успеха деятельности в данном направлении является соблюдение режима секретности при работе с документами и сохранение максимальной конфиденциальности при работе с информаторами. Немаловажным фактором выступает материально-техническое и научно-

методическое обеспечение оперативных подразделений, а также степень обученности сотрудников практическим навыкам конспиративной работы.

Таким образом, понимание полномочий и задач субъектов оперативно-розыскной деятельности помогает обеспечить, что их действия соответствуют законодательству. Это снижает риск превышения полномочий, нарушений прав граждан и способствует законному проведению оперативных мероприятий.

Литература

1. Козлов В.И. Оперативно-розыскные меры противодействия криминальным угрозам правоохранительной функции государства: правовые и методологические проблемы: автореф. дис. ... д-ра юрид. наук. М., 2009.
2. Лапин Е.С. Оперативно-розыскная деятельность: учебник. М., 2021.
3. Серов А.В. О субъектах оперативно-розыскной деятельности органов внутренних дел // Законодательство и практика. 2016. № 2.
4. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. Доступ из справ. правовой системы «Гарант».
5. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001. № 174-ФЗ. Доступ из справ. правовой системы «Гарант».
6. Об оперативно-розыскной деятельности: федер. закон от 12.02.1995. № 144-ФЗ. Доступ из справ. правовой системы «Гарант».
7. О полиции: федер. закон от 07.02.2011 № 3-ФЗ. Доступ из справ. правовой системы «Гарант».
8. Халиков А.Н. Правовые основы оперативно-розыскной деятельности. Курс лекций. М., 2007.

© Снежкова Ж.Ю., 2025

СОВРЕМЕННЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ КОРРУПЦИОННЫХ СВЯЗЕЙ ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ БЮДЖЕТНЫХ СРЕДСТВ

Сторожева М.В.

Адъюнкт адъюнктуры

Ростовского юридического института МВД России

В настоящее время обеспечение экономической безопасности государства играет немаловажную роль в системе национальной безопасности страны. В связи с этим данный процесс приобретает особую актуальность. Немалая часть бюджетных средств, выделяемых на реализацию национальных проектов или государственных контрактов, создают высокие коррупционные риски [1]. Данное обстоятельство позволяет говорить о необходимости выявления и пресечения коррупционных связей посредством применения современных методов расследования.

Коррупционные связи представляют собой взаимоотношения между правонарушителями и должностными лицами государственных органов, направленные на использование своего служебного положения с целью получения личной или иной выгоды обеими сторонами посредством совершения противоправных действий (бездействий) [2]. Такие связи могут включать в себя различные формы взаимодействия, нарушающие законные интересы общества и государства.

Нельзя не обращать внимания на последствия, которые возможны при появлении таковых коррупционных связей в бюджетной системе государства. Стоит отметить, что последствия будут отражаться на многих сферах жизнедеятельности. В частности:

– экономические последствия: малоэффективное распределение материальных и нематериальных благ; выбор в пользу недобросовестных исполнителей государственных контрактов; рост теневой экономики и многое другое;

– политические последствия: значительная утрата доверия граждан к государственным институтам; ослабление правового государства;

– социальные последствия: ухудшение уровня жизни населения в связи с неравномерным распределением бюджетных средств, которое в свою очередь сказывается на уровне оказания услуг в области здравоохранения, образования и инфраструктуры.

Вышеперечисленное выступает лишь малой частью последствий, которые возможны при несвоевременном выявлении или же полном игнорировании коррупционных связей в области бюджетного финансирования [3]. На основании этого следует сделать вывод о необходимости изучения и внедрения современных методов выявления коррупционных связей при расследовании хищений бюджетных средств.

По-нашему мнению, наиболее ключевым инструментом выявления коррупционных схем выступают методы анализа финансовых потоков. К данной группе методов можно отнести:

– анализ банковских операций, который позволяет определить подозрительные переводы денежных средств, указывающих на коррупционные соглашения. Так, например, в случае обнаружения систематических переводов между определенными лицами в крупном размере, можно говорить о возможном коррупционном сговоре между данными лицами;

– методология отслеживания активов, включающая в себя мониторинг имущества лиц, подозреваемых в коррупционных правонарушениях. В случае выявления сотрудниками правоохранительных органов имущества, стоимость

которого значительно превышает официально подтвержденные доходы, может быть начато расследование;

– финансовое моделирование. Данный метод заключается в создании абстрактного представления реальной или предполагаемой финансовой ситуации. В нашем случае с помощью данного метода можно предположить структуру возможных схем отмыwania денежных средств, а также выявить скрытые активы. Такие модели могут учитывать такие факторы риска, как происхождение капитала, использование зарубежных финансовых инструментов, а также страновая принадлежность компаний.

Рассмотренные методы способны выявить подозрительные транзакции, которые могут свидетельствовать о наличии коррупционных связей.

К следующей группе методов можно отнести инструменты цифровой криминалистики, поскольку именно она зачастую играет ключевую роль в раскрытии преступлений, совершенных или связанных с использованием цифровых технологий. К современным инструментам относятся:

– компьютерная экспертиза, которая направлена на извлечение доказательств из электронных устройств, в частности, из компьютеров, мобильных устройств и серверов. В рамках компьютерной экспертизы могут быть восстановлены удаленные файлы, расшифрованы зашифрованные сообщения, а также произведен анализ метаданных;

– интернет-аналитика, предполагающая сбор и анализ данных из социальных сетей, электронной почты и других интернет-ресурсов. Рассматриваемый метод может способствовать выявлению связей между отдельными людьми и организациями, которые могут быть вовлечены в коррупционную деятельность;

– биометрический анализ, использование которого позволяет идентифицировать лиц путем сравнения биометрических данных, таких как отпечатки пальцев, лица или голос. Указанный метод наиболее полезен

в случае установления личности преступников, скрывающихся под псевдонимами.

Таким образом, выявление коррупционных связей при расследовании хищений бюджетных средств выступает одним из ключевых элементов в построении справедливого, эффективного и безопасного государства, поскольку они наносят многогранный ущерб обществу. Выявление таких связей в какой-то мере позволит предотвращать преступные деяния в области распределения бюджетных средств.

Проведенный анализ современных методов выявления коррупционных связей при расследовании хищений бюджетных средств позволяет сделать ряд принципиальных выводов о состоянии и перспективах противодействия этому виду преступности.

В бюджетной системе выявить коррупционные связи достаточно сложно, поскольку они носят высоклатентный характер. На сегодняшний день существуют различные методы выявления таких схем, часть из которых рассматривалась выше. Однако их эффективность сдерживается недостаточной интеграцией данных, отсутствием единых алгоритмов оценки рисков и сопротивлением со стороны заинтересованных лиц.

Поэтому возможна разработка единой цифровой платформы, базирующейся на возможностях искусственного интеллекта, что способствовало бы объединению необходимых данных — госзакупок, налоговой отчетности, банковских транзакций и иных. Основной задачей данного ресурса должно стать автоматическое выявление отклонений цен от рыночных, повторяемость подозрительных схем и прочее. Такая платформа отвечала бы современным реалиям, благодаря чему сотрудникам правоохранительных органов стало возможнее выявлять коррупционные связи на ранних этапах.

Подводя итог, следует отметить, что выявление коррупционных связей в сфере хищений бюджетных средств требует комплексного подхода, сочетающего технологические инновации, правовое регулирование и кадровые реформы. Отмеченные в статье существующие современные методы выявления коррупционных связей при расследовании хищений бюджетных средств должны применяться сотрудниками правоохранительных органов повсеместно для повышения эффективности расследования в целом. Также нельзя забывать о разработке и применении новых методов, отвечающих в полной мере современным реалиям и возможностям информационно-телекоммуникационных технологий.

Литература

1. Попова Е.М., Милюхин А.С. Практические рекомендации по повышению результативности оперативно-розыскной деятельности, нацеленной на выявление преступлений коррупционной направленности в сфере реализации национальных проектов // Полицейская и следственная деятельность. 2024. № 3.

2. Дашиев В.Э., Васильева М.А. Сущность и соотношение понятий «коррупционные связи» и «Криминалистическая характеристика экологических преступлений» // Научные исследования и инновации. 2021. № 4.

3. Айвазова О.В. Преступления, совершенные с использованием лицом своего служебного положения, как объект научного познания: правовые и криминалистические аспекты // Философия права. 2022. № 2(101).

© Сторожева М.В., 2025

**АКТУАЛЬНЫЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ ОРД
В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ОРГАНИЗОВАННОЙ
ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ**

Тишкин Д.Н.

Начальник кафедры тактико-специальной подготовки
Волгодонского филиала Ростовского юридического института МВД России,
кандидат политических наук

Крицкая А.А.

Доцент кафедры политологии и этнополитики
Южно-российского института управления –
филиал Российской академии народного хозяйства и государственной службы
при Президенте Российской Федерации,
кандидат политических наук, доцент

Деятельность профессионально-организованного криминала в современном социуме России находится под воздействием процессов геополитического и глобализационного характера, которые способствуют тому, что организованная преступность (далее — ОП) приобретает качественно новые черты. Преступные формирования, выводя на первый план стремление получения дополнительных доходов, активизируют распространение своего криминально-активного функционала за рамки территории России, стремясь укрепить свои экономические возможности в иностранных государствах. Лидеры ОП, с упорной настойчивостью, пытаются сохранять высокие позиции в криминальном мире и удерживать свое влияние на государственно-общественные системы, посредством коррупционных практик. В данном контексте, следует отметить слова В.В. Путина о том, что «борьба

с коррупцией — очень важная вещь, но она не должна использоваться как инструмент политической борьбы <...> должна вестись постоянно и именно теми людьми, которые сами безупречно исполняют законы» [1].

В настоящее время, для представителей СМИ не является популярным освещение проблем, связанных с ОП, и продолжена тенденция на некоторое замалчивание информации о ней, становясь особенно заметным последние годы, в течение которых трендом массовой информации заслуженно становятся, прежде всего, политические поводы, связанные с проведением Россией специальной военной операции (далее — СВО), политикой, проводимой мировым гегемоном (США и Великобританией), в целях оккупации территории суверенных государств и нелегитимной смене режима (упуская из виду келейное участие в госпереворотах представителей ОП в качестве движущей силы, а иногда в качестве объекта на который якобы направлено «справедливое демократическое» воздействие в виде военных операций).

Все перечисленное формирует такое представление у многих людей, согласно которому ОП не может считаться значимой проблемой российского социума и государства, а также создавать угрозы национальным интересам отчизны. Указанная тенденция по «утрате внимания» лишь способствует скрытной перманентной эволюции ОП, базирующейся на значительных финансовых ресурсах и стремительной динамике в сфере информационных технологий (далее — ИТ). При этом имеет место одновременное отставание контроля социально-правового характера в отношении ее функционирования, растущая криминализация социальных отношений. Эти тенденции, затрагивая многие страны, актуальны и для России, т. к. организованный криминал способен оказывать огромное воздействие негативного характера на многие социально-экономические и политические процессы.

Значительной частью российских криминальных авторитетов в последние годы принято решение уйти в тень. В то же время подобное вовсе не стало основанием для одновременного их ослабления в плане влияния на политические институты и процессы. Как раз, напротив, лидеры криминального мира смогли данное влияние укрепить. Процессы, которые происходят в области криминальной преступности, можно охарактеризовать выходом из тени значительного количества участников криминальной среды, действующей в экономических отношениях, образованием слоя так называемых «авторитетных предпринимателей», что сопровождается тем, что складывается определенная преступная иерархия, происходит раздел криминальных денежных активов или сфер влияния. Как считает известный российский эксперт-практик А.И. Гуров, сейчас преобладающее количество российских мегаполисов находится под «прицелом» криминальных объединений, с характерными признаками сетевых структур [2]. Последующим после проникновения в легальную экономику планомерным этапом трансформации организованных криминальных структур выступает их проникновение в систему государства, определенные государственные учреждения.

Как считает другой известный исследователь организованной преступности В.С. Овчинский, организованный криминал в современной России есть не мнимая, а реальная угроза, так как согласно его позиции, имеются определенные признаки возвращения к криминальным девяностым. Определенные параллели для такого вывода, конечно, выстроить можно, но существенно и качественное отличие, заключено в том, что в девяностых представители организованного криминала стремились к власти. А сейчас они уже сами являются властью, проникнув на все ее этажи, во все ее

разновидности, тем самым, стремительно нарастив антигосударственный потенциал [3].

Далее В.С. Овчинский, учитывая современное состояние IT, определил инновационные параметры ОП, заключающиеся «в стирании юридических граней между терроризмом, гибридными войнами и уголовной преступностью <...> лишении возможности расставить приоритеты между действиями террористов, мафиозных структур или реализацией чьих-либо политических проектов» [4, с. 377]. Таким образом, ОП, затрудняя функционал силовых структур по эффективному государственному противодействию подобным криминальным тенденциям, претендует на монополию государства в применении насилия.

И.Н. Панарин в своих исследованиях обосновывает факт ведущейся многовековой гибридной войны против России (в качестве орудия используются террористические и иные преступные сообщества), финансируемой «доброй старушкой» Англией и ее многочисленными союзниками [5].

В свою очередь, канадским дипломатом П.Д. Скоттом обосновывается причастность различных подразделений ЦРУ к наркотрафику в «смычке» с «акулами» американского бизнеса, активно сотрудничающими с мафиозными группировками. А главное, доказывается, что по «мере «взросления» западного капитализма и национализма третьего мира влиятельные силы в США, сталкиваясь с невозможностью ведения «частных» военных операций, <...> вынуждены для достижения своих целей систематически обращаться к услугам организованных преступных сообществ, используя для этого секретные каналы ЦРУ» [6].

Учитывая вышеописанные мировые тенденции, необходимо принимать во внимание тот факт, что эффективное государственное противодействие

организованной преступной деятельности национального и международного уровня могут осуществлять лишь органы, наделенные правом на осуществление оперативно-розыскной деятельности (далее — ОРД). Потому как функционирование ОП происходит в келейном режиме и основная часть населения может наблюдать лишь «верхушку айсберга» в случае удачной реализации дел оперативного учета в отношении представителей организованного криминала. В соответствии с действующим законодательством РФ таковыми являются МВД, ФСБ, ФСО, таможенные органы, СВР и ФСИН [7]. Базируясь на отслеженных в настоящем исследовании тенденциях (особенно с учетом СВО, в которой против России аффилированно принимает участие более 50 государств мира), взаимодействие между указанными силовыми структурами должно выходить на более высокий уровень с целью противодействия проникновению агентуры недружественных стран (представителей криминала) в политические институты и парирования угроз национальной безопасности в целом.

Эксперты в 2024 г. делают акцент на тот факт, что «количество тяжких преступлений, совершаемых участниками организованных преступных формирований, в том числе этнических, постоянно растет, а их раскрываемость по-прежнему хромает» [8], создавая объективное обоснование целесообразности использования оперативно-розыскного прогнозирования в сфере противодействия вариативным формам и проявлениям ОП [9, с. 182–188].

По данным Генпрокуратуры РФ, «за 2020–2023 годы по ст. 210.1 УК РФ были осуждены 74 человека: 34 вора «в законе» и 40 «положенцев» (смотрящих) [8].

По некоторым данным 2025 г. «всего в мире сейчас 398 воров <...> из них в российских колониях сидят 38 <...> на свободе гуляет не больше 20

<...> остальные за границей» [10]. Другие источники свидетельствуют об осуждении в 2025 г. 10 криминальных авторитетов (6 ожидают суда) и наметившейся тенденции «избегать публичности и контактов с зарубежными «коллегами»[11].

Ряд экспертов полагает, что за счет инновационной ст. 210.1 УК РФ — «Занятие высшего положения в преступной иерархии» в 2025 г. МВД России «удалось снизить число «воров в законе» почти вдвое по сравнению с 2010-и годами» при этом сохраняется уже более десяти лет мораторий на новые коронации, базирующийся по их мнению «не только на личном авторитете, но и <...> на неформальном взаимодействии с силовиками» [12].

Современный подход к решению базисных задач ОРД в сфере государственного противодействия любым проявлением ОП, возможен при внедрении следующих мер:

- корректировки тактики документирования и легализации материалов ОРД по ст. 210.1 УК РФ на основе судебной практики» [13, с. 221];

- ужесточении процедуры получения допуска к государственным секретам в соответствии со ст. 21(1) Федерального закона Российской Федерации «О государственной тайне» [14, с. 199–200].

Опираясь (с учетом проводимой СВО и использованием ОП глобальными акторами в качестве элемента гибридной войны), на перманентное реформирование силового блока, усиливая его разведывательное, контрразведывательное и правоохранительное обеспечение на основе исторических традиций (НКВД, СМЕРШ, МГБ, МВД, КГБ), обеспечить взаимодействие всех органов, осуществляющих ОРД (прежде всего МВД, ФСБ и СВР), более высокого порядка, разработав параллельно объективную «оценочную шкалу» функционирования оперативных органов.

Литература

1. Путин: борьба с коррупцией не должна использоваться как инструмент политической борьбы [Электронный ресурс]. URL: <https://tass.ru/politika/12181413> (дата обращения: 20.12.2025).
2. Гуров А.И. Об оргпреступности: Наша мафия уже построила развитой капитализм. Мы — еще нет, а они — уже да // Комсомольская правда. 2013. № 6.
3. Овчинский В.С. Мафия как форма жизни [Электронный ресурс]. URL: <http://www.mospravda.ru/issue/2011/07/28/article28403> (дата обращения: 20.12.2025).
4. Овчинский В.С. Мафия: новые мировые тенденции. М., 2016.
5. Панарин И.Н. Гибридная война против России (1816–2016). М., 2019.
6. Скотт П.Д. Наркотики, нефть и война. США в Афганистане, Колумбии и Индокитае. М., 2012.
7. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «Гарант».
8. Сухаренко А.Н. «Антиворовская пятилетка» дала результаты [Электронный ресурс]. URL: https://www.ng.ru/vision/2024-04-11/2_8992_freedom.html (дата обращения: 20.12.2025).
9. Шувалов А.П., Тишкин Д.Н. Актуальные вопросы совершенствования научно-методического обеспечения оперативно-розыскного прогнозирования в сфере противодействия религиозному экстремизму // Юрист-Правоведъ. 2018. № 3(86).
10. Рогоза А. Из 400 воров в законе в России на воле осталось только 30. Остальные сидят или сбежали за границу [Электронный ресурс]. URL: <https://www.kp.ru/daily/27667/5056805/> (дата обращения: 20.12.2025).

11. Бороздин Д. В 2025 году в России осудили 10 воров в законе [Электронный ресурс]. URL: https://dzen.ru/a/aUykhbUjyiBtZJ_j (дата обращения: 25.12.2025).

12. Енцов Ю. Криминальный передел: Короли преступного мира стараются соблюдать политес [Электронный ресурс]. URL: <https://svpressa.ru/society/article/499805/> (дата обращения: 24.01.2026).

13. Тишкин Д.Н., Осяк В.В. К вопросу совершенствования оперативно-розыскной деятельности в сфере противодействия организованным формам преступной деятельности современной России: сб. материалов Междунар. научно-практ. конф. Ростов н/Д, 2020.

14. Тишкин Д.Н. Политические аспекты борьбы с проникновением организованного криминалитета во властные структуры различных уровней как необходимый элемент парирования угроз «гибридной войны» // Государственное и муниципальное управление. Ученые записки. 2019. № 2.

© Тишкин Д.Н., Крицкая А.А., 2025

ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ: ОПЕРАТИВНО РОЗЫСКНАЯ ХАРАКТЕРИСТИКА, МЕРЫ ОПЕРАТИВНО РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ

Торопов Д.С.

Адъюнкт адъюнктуры

Ростовского юридического института МВД России

Вопрос об актуальности настоящего исследования определяется устойчивой тенденцией увеличения числа преступлений, совершаемых организованными преступными группами и сообществами на территории Российской Федерации. Статистические данные свидетельствуют о росте: так, в 2016 г. было зафиксировано 11 186 зарегистрированных преступлений, совершенных организованными группами, в 2017 г. — 12 135(+ 8,4 %), в 2018 г. — 13 744 (+ 13,3 %), в 2019 г. — 14 647 (+ 6,5 %), в 2020 г. — 17 742 (+ 21,1 %), в 2021 г. — 22 216 (+ 25,2 %), в 2022 г. — 27 234 (+ 25,5 %), в 2023 г. — 31 865 (+ 17 %). В 2024 г. число преступлений, совершенных организованными группами или преступными сообществами составило 38 103 (+ 19,6 %). В результате деятельности таких групп было совершено более 16 тыс. тяжких и особо тяжких преступлений [1].

Организованная преступность — это форма преступной деятельности, для которой характерно устойчивое и систематическое совершение общественно опасных деяний. Кроме того для преступных формирований характерны иерархическая структура, финансовая база, а так же связи в государственных структурах. Преступления, связанные с организованной преступностью связаны со ст. 210, 210.1 [2]. В современной жизни

организованная преступность приобрела новый характер деятельности, это выражено в трансформации деятельности субъектов данного вида преступлений. В настоящее время организованные преступные группы имеют устойчивую тенденцию развития своей деятельности, а именно используют социальные сети, средства шифрования связи и иные сетевые ресурсы для: рекламы и распространения нелегальной продукции, маскировки IP-адресов, зашифровки каналов связи между членами и лидерами преступных групп, конспирации своих преступных умыслов.

Исходя из этого, можно сказать, что современные преступные группы открыли для себя новую ветвь преступной деятельности связанную с информационно-телекоммуникационной сетью. Создаются новые преступные группы, чья деятельность частично или полностью связана с телефонным мошенничеством, сбором персональных данных граждан для использования в преступных целях. Стоит отметить, что в пятилетнем тренде наблюдается развитие пропаганды в сети Интернет, антисоциального поведения, что, как следствие, пагубно влияет на граждан.

Ярким примером современной организованной преступной группы является преступное сообщество, действовавшее в 2024 г. на территории Ленинградской области. «Сотрудники БСТМ МВД России с участием оперативников ГУУР МВД России, УЭБиПК ГУ МВД России по Москве, УЭБиПК ГУ МВД России по Санкт-Петербургу и Ленинградской области пресекли деятельность преступного сообщества. Его участники подозреваются в незаконной банковской деятельности, неправомерном доступе к компьютерной информации и неправомерном обороте средств платежей. Предварительно установлено, что злоумышленники причастны к созданию анонимной платежной системы UAPS и крипто-валютной биржи Cryptex, а также ряда интернет-сервисов. С их помощью велась нелегальная

деятельность по приему и выдаче денежных средств, обмену валюты и криптовалюты [3]. При этом фигуранты выпускали свои банковские карты и предоставляли доступ к операциям через личный онлайн-кабинет. Пользователями разработанных соучастниками программных продуктов чаще всего были люди, которые занимались противоправной деятельностью. Они получали возможность анонимно совершать переводы, легализовать и обналичивать криминальные доходы.

Исходя из этого, следует обратить внимание на оперативно-розыскную характеристику организованной преступности. Она представляет собой информационную модель, которая собрана на основе криминологической, криминалистических, уголовно-правовых и психологических признаках.

Таким образом, можно выделить следующие оперативно-розыскные элементы, характеризующие оперативно розыскную деятельность в сфере противодействия организованной преступности:

1. Организованный характер совершения преступлений.
2. Вид деятельности организованной преступной группировки
3. Характеристика личности лидеров и членов организованной преступной группировки (далее — ОПГ).
4. Характеристика личности жертвы в зависимости от направленности деятельности ОПГ.
5. Наличие оперативных позиций в среде предполагаемых преступных группировок
6. Наличие информационных баз данных правоохранительных органов, содержащих сведения об организованных преступных группировках прошлых лет и действующих группах.

Изучение данных характеристики позволяют изобличить проблематику в раскрытии и расследовании данного вида преступлений

и найти пути решения. Следует также рассмотреть понятие мер оперативно-розыскного противодействия, которое предполагает оперативную деятельность уполномоченных лиц по предупреждению, выявлению, пресечению и раскрытию преступлений, а так же предотвращение причин и условий, сопутствующих совершению общественно опасных деяний. Перечень оперативно розыскных мероприятий, направленных на противодействие организованной преступности, определены ст. 6 Федерального закона «Об оперативно-розыскной деятельности» [4]. Кроме того, при анализе практической деятельности оперативных подразделений в сфере противодействия организованной преступности можно выделить следующие методы.

Оперативное внедрение в среду организованной преступности, для получения оперативной информации изучения внутренней структуры и выделение лидера группировки. Этот метод является наиболее действенным в противодействии организованной преступности. Процедура внедрения включает в себя тщательное планирование и отбор сотрудников. Однако стоит учитывать риски такого внедрения, поэтому необходимо обеспечить защиту и поддержку агента во время выполнения поставленных задач, а также разработать план немедленного извлечения агента из организованной группы.

Контроль за интернет-ресурсами и закрытыми интернет платформами. Мероприятие, включающее в себя анализ информационно-телекоммуникационной среды, выявление и пресечение деятельности организованной преступности в киберпространстве. В современных реалиях данное направление является актуальной средой для совершения преступлений.

Немаловажным методом в противодействии организованной преступности является — сбор и анализ оперативной информации, информации. Сбор информации о преступных действиях и применяемых методах ОПГ

не заканчивается после задержания подозреваемых. На этом этапе проводится анализ полученных данных и определение последующих шагов по пресечению деятельности ОПГ [4, с. 248].

Большую роль в противодействии так же играет межведомственное взаимодействие, благодаря которому осуществляется быстрый, сбор и анализ оперативной информации. Такое взаимодействие включает в себя: обмен оперативно-розыскными данными, межведомственный анализ оперативной информации, проведение совместных оперативных операций.

Таким образом, государственная стратегия борьбы с организованной преступностью требует постоянной корректировки, основанной на научно-обоснованных подходах, в мониторинге преступной среды и своевременном законодательном реагировании на происходящие в ней изменения. Такая корректировка [6 с. 182].

Проведенный анализ оперативно розыскной характеристики и мер противодействия позволяет сделать следующие выводы. Организованная преступность представляет собой сложно-структурированное явление, которое обладает устойчивой системой иерархии, коррупционными связями, транснациональными каналами взаимодействия, высокой степенью адаптации к современным реалиям. Отсюда следует, что успешное противодействие организованной преступности требует не только совершенствования ОРД, но и системного применения мер оперативно-розыскного противодействия, а также их постоянной адаптации к меняющимся криминальным способам совершения преступлений.

Литература

1. Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития [Электронный ресурс]. URL: <http://crimestat.ru/> (дата обращения: 15.10.2025).

2. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. Доступ из справ. правовой системы «Гарант».
3. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «Гарант».
4. Сотрудники МВД России задержали подозреваемых в киберпреступлениях, совершенных в составе преступного сообщества [Электронный ресурс]. URL: <https://мвд.рф>. (дата обращения: 15.10.2025).
5. Халиуллин Т.М., Вяткин А.Н. оперативно-розыскные меры противодействия организованной преступной деятельности // International Journal of Humanities and Natural Sciences. 2024. №. 9–5(96).
6. Катков Д.В., Огурцов А.Е. К вопросу правового регулирования борьбы с организованной преступностью в сфере экономики // Вестник Московского университета МВД России. 2020. № 8.

© Торопов Д.С., 2025

**ДЕЯТЕЛЬНОСТЬ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ
ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ,
СОВЕРШАЕМЫХ ИНОСТРАННЫМИ ГРАЖДАНАМИ**

Точилкина А.А.

Старший преподаватель кафедры криминалистики
и оперативно-разыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

Глобализационные процессы привели к возникновению контролируемых и неконтролируемых потоков миграции. В последние годы все большую актуальность приобретает вопрос обеспечения миграционной политики на территории Российской Федерации, что обусловлено рядом экономических, геополитических и мировоззренческих условий. Первостепенной угрозой, связанной с незаконной миграцией, является возможность проникновения в страну как отдельных преступных лиц, так и преступных группировок. Современные мигранты весьма изощрены в плане преступных схем и нелегального проникновения, и проживания на территории России, что ставит под угрозу как внутреннюю, так и внешнюю безопасность страны.

Так, иностранными гражданами на территории России в 2024 г. совершено более 23,8 тыс. криминальных деяний, а число тяжких преступлений возросло на 12 %. При этом число тяжких преступлений, совершенных приезжими, возросло на 12 % (с 4 390 до 4 935). Втрое увеличилось число преступлений, совершенных лицами, незаконно находящимися на территории России, а количество трудовых мигрантов и вовсе увеличилось на 69 %, что обуславливает актуальность исследуемого вопроса [5]. Также наблюдается отрицательная динамика в количественных показателях миграционной

преступности в целом: в январе 2025 г. иностранцы и нелегальные мигранты совершили на 17,3 % больше преступлений, чем в январе 2024 г. [6].

В этих условиях возрастает потребность в разработке эффективных стратегий профилактики и пресечения правонарушений среди мигрантов. Оперативные подразделения органов внутренних дел выполняют ключевую функцию в системе обеспечения общественного правопорядка и защиты прав и законных интересов граждан. Оперативно-розыскное противодействие миграционной преступности должно состоять из трех взаимозависимых компонентов, а именно:

- 1) предупреждения преступлений миграционной направленности;
- 2) выявления и их раскрытия;
- 3) минимизации (ликвидации) и последствий названной категории преступлений [2].

В рамках противодействия преступлениям, совершаемым иностранными гражданами, оперативные сотрудники должны исследовать условия и причины, способствующие их совершению, включая социально-экономические, культурные и правовые факторы. Специфика взаимодействия с иностранными гражданами диктует необходимость учета их национально-правовых традиций, языковых особенностей и культурных установок. Это, в свою очередь, предъявляет повышенные требования к профессиональной подготовке сотрудников правоохранительных органов, уровню их правовой грамотности, межкультурной компетентности и способности адаптировать методы работы в условиях правового плюрализма.

В виду таких обстоятельств можно сформулировать основные задачи оперативно-розыскных подразделений по противодействию миграционной преступности:

1. Выявление и пресечение преступлений, совершаемых иностранными гражданами, включая преступления в сфере незаконной трудовой деятельности, организованной незаконной миграции, торговли людьми, мошенничества,

а также преступлений экстремистской и террористической направленности, совершаемых на почве межнациональной розни.

2. Раскрытие преступлений, связанных с фиктивной регистрацией, использованием поддельных документов и легализацией незаконного пребывания на территории Российской Федерации.

3. Осуществление розыска иностранных граждан, скрывающихся от органов дознания, следствия или суда, а также лиц, уклоняющихся от административного выдворения или уголовного наказания, с последующим обеспечением их задержания и передачи компетентным органам.

4. Предупреждение преступлений, связанных с незаконной миграцией, посредством проведения профилактических мероприятий, мониторинга миграционных потоков, анализа криминогенной обстановки в регионах с высокой концентрацией иностранных граждан и выявления групп риска.

5. Информационное обеспечение правоохранительных органов путем сбора, анализа и систематизации сведений о лицах, нарушающих миграционное законодательство, включая формирование и ведение специализированных баз данных.

6. Обеспечение межведомственного и международного взаимодействия с целями обмена оперативной информацией, проведения совместных операций, выработки единых подходов к классификации и квалификации миграционных правонарушений, а также реализации двусторонних и многосторонних соглашений в области правовой помощи и экстрадиции.

7. Обеспечение соблюдения прав и свобод иностранных граждан в ходе проведения оперативно-розыскных мероприятий.

Отметим, что в задачи оперативно-розыскных подразделений, при противодействии этническим преступным группам, входит не только установление факта совершения преступления и всех причастных к нему лиц, но и установление состава всей преступной группы, иерархию и роли участников, связи вне преступной группы, в том числе и в органах власти

и коммерческих структурах. Эффективность получения информации напрямую зависит от грамотного сочетания гласных и негласных методов проведения ОРМ, а получение максимально полной информации о преступлениях и преступниках позволяет сформировать доказательственную базу еще задолго до возбуждения уголовного дела.

В продолжение вышесказанного прямо прослеживается, что оперативно-розыскная деятельность имеет строгую организацию. И прежде всего, это касается ответственности каждого субъекта, определяемого его компетенциями. Субъектами ОРД являются сотрудники оперативных подразделений ОВД, охраны общественного порядка, миграционных подразделений органов внутренних дел, инспектора уголовно-исполнительных инспекций, другие сотрудники правоохранительных органов. Каждый из субъектов планирует и осуществляет ОРД на различных уровнях. В связи с этим устанавливаются обязанности и ответственность за реализацию профилактических мероприятий, их эффективность, выполнение задач и достижению целей оперативно-розыскной профилактики среди иностранцев.

Оперативно-розыскное предупреждение преступлений в целом, и в отношении иностранных граждан в частности, заключается в осуществлении гласного или негласного надзора за индивидуумом или группой лиц. Только воздействием на конкретную личность можно добиться не допущения распространения криминального воздействия как на отдельного человека, так и на определенную группу. Целью надзора является выявление криминогенных наклонностей личности или группы путем сбора, обобщения и анализа поступающей информации. Задачей надзора выступает разработка мер профилактического воздействия для недопущения подготовки и, тем более, совершения преступления.

При осуществлении надзора у оперативных сотрудников должны вызывать интерес лица, явно противопоставляющие себя общественным нормам или пренебрегающие нормами административного и (или) уголовного

законодательства. Еще одна категория, представляющая оперативный интерес, это лица, склонные к употреблению алкоголя и особенно наркотиков: прогнозировать поведение данной категории практически невозможно. Без сомнений, любой иностранец, высказывающий экстремистские или террористические взгляды, распространяющий или читающий литературу подобного толка является объектом пристального внимания. Нельзя представить себе проведение профилактических мероприятий без контроля и надзора за лицами, прибывшими из мест лишения свободы, находящимися под административным надзором, причастных к незаконному обороту или употребляющими наркотические вещества. Такие действия должны проводиться как гласно, так и негласно, что предусмотрено российским законодательством.

Особое значение приобретает профилактическая функция оперативных подразделений, включающая мониторинг миграционных потоков, выявление лиц, находящихся в незаконном положении на территории Российской Федерации, а также предупреждение совершения преступлений, связанных с незаконной трудовой деятельностью, торговлей людьми, незаконным предпринимательством и другими формами правонарушений. Оперативно-розыскная профилактика — организационно-тактическая форма оперативно-розыскной деятельности подразделений органов внутренних дел, отражающая в своем становлении и развитии требования уголовной политики о приоритетном значении предупредительно-профилактических мер в структуре борьбы с преступностью.

Научные исследования и практическая деятельность по оперативно-розыскной профилактике преступлений, совершаемых в отношении иностранных граждан, показывают ее многоцелевой и много аспектный характер. Заключается оперативно-розыскная профилактика в следующем:

- организация учета иностранных граждан, требующих осуществления оперативного контроля и профилактического воздействия;

- получение и анализ оперативной и иной информации, ее концентрацию и использование в качестве информационной базы для проведения оперативно-розыскных и предупредительно-профилактических мероприятий в отношении иностранцев-нелегалов;

- осуществление оперативно-профилактических мероприятий с учетом национальных особенностей личности иностранного гражданина и его окружения; предупреждение замышляемых и пресечение подготавливаемых преступлений.

Имеются некоторые отличия оперативно-розыскной профилактики в отношении иностранцев от тех же мероприятий в отношении россиян, связанные с некоторыми обстоятельствами:

- действие Федерального закона № 64-ФЗ на большинство иностранцев не распространяется, т. к. значительная часть из них к уголовной ответственности не привлекалась;

- замкнутость этнических и национальных групп практически не позволяет осуществить оперативное внедрение;

- прямо следующее из предыдущего пункта, задействовать иностранцев в качестве негласного аппарата практически невозможно;

- большинство иностранцев не имеют постоянного места жительства.

Ввиду вышесказанного, оперативно-розыскная профилактика должна строиться таким образом:

- сбор информации о существовании ОПГ из числа иностранцев, занимающихся нелегальной трудовой миграцией;

- участие в организации и проведении рейдов по выявлению иностранцев, незаконно находящихся на территории России;

- профилактическая работа с юридическими лицами, использующими труд незаконных мигрантов;

- выявление из числа трудовых мигрантов-иностранцев лиц, имеющих документы на право проживания и трудовую деятельность на территории

России, но склонных к совершению преступлений, и постановку их на профилактический учет;

– использование негласных методов ОРД по осуществлению оперативного контроля за трудовыми мигрантами.

Для достаточной эффективности оперативно-розыскной профилактики необходимо проводить постоянные проверочные мероприятия в местах проживания, работы или сосредоточения иностранных граждан: проверки документов, рейды, привлечение негласного аппарата. Нельзя исключать из действий проверку по оперативно-справочным и криминалистическим учетам, особенно дактилоскопическим.

Эффективность оперативного воздействия напрямую зависит от качества собранной информации, в определении точек оперативного воздействия, слаженного и организованного взаимодействия между субъектами оперативно-розыскной профилактики и от полноценного и всеобъемлющего изучения объекта оперативного воздействия. Мы хотим сказать, что сотрудники, занимающиеся оперативно-розыскной профилактикой должны иметь достаточную подготовку, быть, что называется, профессионалами в своей области деятельности. Деятельность оперативных подразделений в данной сфере не только способствует снижению уровня преступности, но и укрепляет доверие общества к правоохранительным органам, что в свою очередь создает более безопасную среду для всех граждан, независимо от их национальности.

В заключении, необходимо отметить, что деятельность правоохранительных органов, направленная на противодействие преступлениям, совершаемым иностранными гражданами, зачастую носит транснациональный характер. Иными словами, проблема преступности среди мигрантов выходит за пределы возможностей правового регулирования в рамках единого государства, что обуславливает потребность в интеграции международного опыта в систему российского правового регулирования. Изучение механизмов противодействия преступности, применяемых в странах

с развитыми правовыми системами, включая практики межведомственного взаимодействия, системы реадaptации иностранных граждан, а также модели профилактики правонарушений в мигрантских общинах, может стать важным ресурсом для совершенствования российского законодательства. Таким образом, формирование эффективной правовой политики в сфере противодействия преступности, связанной с иностранными гражданами, невозможно без межгосударственного сотрудничества.

Противодействие преступности, связанной с иностранными гражданами, требует от оперативных подразделений комплексного, междисциплинарного и межведомственного подхода, основанного на сочетании оперативно-розыскных методов, правового регулирования, профилактической работы и международного сотрудничества. Эффективность такой деятельности напрямую зависит от уровня профессиональной подготовки сотрудников, развития информационных технологий и совершенствования правовой базы в сфере миграции и борьбы с преступностью.

Литература

1. Гамзаева А.Б. Противодействие миграционной преступности // Проблемы правоохранительной деятельности. 2025. № 2.
2. Иванов П.И. Противодействие незаконной миграции (оперативно-розыскной аспект) // Право и государство: теория и практика. 2025. № 3.
3. Осипов Д.Д. К вопросу об организационных основах раскрытия преступлений на современном этапе // Право и государство: теория и практика. 2024. № 8(236).
4. Семенов Г.В. Об актуальных проблемах и путях противодействия миграционной преступности в Российской Федерации // Вопросы российской юстиции. 2025. № 37.
5. Следственный комитет Российской Федерации [Электронный ресурс]. URL: <https://sledcom.ru/press/smi/item/1918181>. (дата обращения: 10.10.2025).

6. МВД России зафиксировало рост преступлений иностранцев на 17,3 % год к году [Электронный ресурс]. URL: <https://iz.ru/1843237/2025-02-22/mvd-rossii-zafiksirovalo-rost-prestupleniiinostrancev-na-173-god-k-godu> (дата обращения: 15.05.2025).

© Точилкина А.А., 2025

УДК 343.985 + 351.745.7

АКТУАЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ МЕТОДОВ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОГНОЗИРОВАНИЯ С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ЛАТЕНТНЫХ ПРЕСТУПЛЕНИЙ

Шувалов А.П.

Старший преподаватель кафедры
тактико-специальной подготовки
Волгодонского филиала Ростовского
юридического института МВД России

Латентная преступность всегда представляла не только научный интерес для ученых-исследователей и специалистов-практиков, но и волновала обычных законопослушных граждан, которые наблюдали ее проявления в обыденной жизни, либо обладали той или иной, в том числе и недостоверной информацией о совершенных либо подготавливаемых преступлениях, а также иных противоправных действиях. Безусловно, латентная преступность является реальной преступностью, но по различным причинам не подлежала регистрации в установленном порядке и не получила правовую оценку после необходимой проверки соответствующей информации. Таким образом, сам факт совершения противоправных действий не может быть ни подтвержден, ни опровергнут, а имеющаяся информация может перейти в разряд слухов и домыслов, пока не будет доказано обратное. Латентизация преступлений

является характерной для всех стран, однако отличается не только по масштабам, но и по многочисленным национальным, религиозным, морально-нравственным и другим особенностям [1]. В каждой конкретной стране (регионе) латентная преступность имеет свои качественные и количественные характеристики, а также пространственные границы [2]. Исходя из того, что латентная преступность является скрытой, но, как и любая преступность оставляет следы, в том числе и в виде специфической информации, которую можно выявить и проанализировать, данную задачу можно эффективно решить в ходе оперативно-розыскной деятельности с использованием ее методов и средств. Полученная таким образом информация должна быть всесторонне рассмотрена на предмет ее проверки и реализации, а весь выявляемый массив подобной информации после необходимой структуризации и классификации представляет безусловный интерес для аналитического аппарата, который может выявить тенденции и спрогнозировать развитие ситуации с латентизацией преступлений как в конкретном регионе, так и в масштабах всего государства. Глобальный характер проблем борьбы с преступностью, обусловленный динамизмом обстановки, многообразием процессов и явлений, связанных с ее развитием и распространением в социальной жизни, особенно в теневой сфере, обуславливает актуальность комплексного прогнозирования развития ситуации. «Оперативно-розыскное прогнозирование (далее — ОРП) является одним из самых эффективных и проверенных временем подходов к решению системных, комплексных задач» [3, с. 184]. Специальная литература свидетельствует, что термин «оперативно-розыскное прогнозирование» впервые появляется в научном обиходе с конца 1970-х — начала 1980-х годов уже встречается в понятийном аппарате теории оперативно-розыскной деятельности. Считается, что теоретические основы оперативно-розыскного прогнозирования были впервые обоснованы С.С. Овчинским [4], который,

по праву считается основателем этого достаточно нового для советской юридической науки направления, однако объективности ради стоит упомянуть В.А. Лукашова, который в начале 1970-х годов впервые поставил вопрос о необходимости вероятностного прогнозирования в оперативно-розыскной деятельности, однако, данное направление не развил [5]. Однако данные исследователи не занимались вопросами оперативно-розыскного прогнозирования комплексно, а лишь в рамках освещения своих тем основных научных интересов. Первой успешной попыткой комплексного исследования вопросов оперативно-розыскного прогнозирования была только в 1990-х годах, когда А.Г. Обложко, исследовал прогностическое содержание деятельности сотрудников уголовного розыска в ходе проведения оперативно-розыскных мероприятий [6]. Кроме того, исследователь актуализировал проблему постоянного совершенствования оперативно-розыскного прогнозирования. Однако, на сегодняшний день существенно изменились жизненные реалии, в том числе, появились такие новые глобальные угрозы, как терроризм и экстремизм, а также вырос уровень латентной преступности, в борьбе с которой также успешно применяется оперативно-розыскное прогнозирование. Необходимо понимать, что «в основе оперативно-розыскного прогнозирования лежит неполучение оперативно значимой информации, а ее обработка и моделирование предстоящих событий» [7; 8]. В связи с этим достаточно актуальным является вопрос соответствующего научно-методического обеспечения этой деятельности, кроме того, в зависимости от разновидностей проявлений преступности необходимо при разработке материалов учитывать данные особенности. Важно учитывать, что за истекшее время изменилась и структура правоохранительных органов, в том числе и ОВД, появились специализированные подразделения по противодействию экстремизму (ЦПЭ) и другие новые подразделения. Поэтому теоретические основы оперативно-розыскного прогнозирования, заложенные С.С. Овчинским, А.Г. Обложко

и другими авторами, требуют дальнейшего комплексного исследования и адаптации к конкретным сферам применения. Для специальных служб и правоохранительных органов оперативное получение научно обоснованных прогнозов служит решению одной из первоочередных задач — предупреждению нежелательных событий, своевременному реагированию не только на общественно-опасные ситуации, но даже на гипотетическую возможность их возникновения, что в целом способствует эффективности управления и контроля над ними. В последние годы в криминогенной ситуации в России произошли определенные изменения. Осложнились социально-экономические и миграционные процессы в обществе, повысилась изменчивость показателей, которые отражают их; существенно изменилась нормативно-правовая база правоохранительной деятельности; выросла не стационарность показателей динамики преступности; в условиях острого дефицита личного состава продолжается реформа правоохранительной системы страны. При таких условиях усложнился процесс прогнозирования преступности, снизилась точность прогнозных оценок. В связи с проведением Россией специальной военной операции (далее — СВО), присоединением Крыма и новых территорий не удалось верно определить все тенденции общеуголовной преступности и спрогнозировать состояние латентной преступности в этих регионах. России пришлось решать множество проблем системного характера, которые десятилетиями «копила» украинская власть. Вследствие постоянных обстрелов российской территории со стороны Украины, а также прорывов вооруженных формирований противника в Курской области произошло определенное ухудшение экономической и социальной ситуации в приграничье, что не могло не отразиться на криминогенной ситуации. Все это показало необходимость существенного совершенствования прогнозной деятельности, получения более оперативных и точных оценок будущего состояния, структуры и динамики

преступности. Соответствующая задача была поставлена и руководством МВД России. По результатам анализа предыдущей практики прогнозирования латентной преступности нами были определены следующие направления повышения его уровня. Первым из них является постоянное пополнение информационных баз для прогнозирования латентной преступности. Речь идет как об уточнении данных в блоках информации, которые уже использовались в предыдущие годы, так и о включении в них новых видов информации. В частности нуждается в дополнении блок статистической информации о факторах преступности. В настоящее время он включает несколько десятков факторов и около сотни показателей, которые характеризуют их состояние. Необходимо инициировать и организовать проведение специальных социологических опросов среди населения и шире использовать уже опубликованные материалы. С целью уточнения значений отдельных показателей, а также получения информации о новых показателях, которые целесообразно включить в этот перечень, целесообразно использование аналитических материалов федеральных и региональных министерств и ведомств, результатов мониторинговых социально-экономических исследований, осуществленных отечественными научно-исследовательскими учреждениями и организациями, в том числе и общественными. Предполагается также включить в этот блок новые виды информации, а именно: результаты мониторинга оперативно-значимых событий религиозного, экономического, социального, демографического, политического, нормативно-правового, социально-психологического и организационно-управленческого характера. Имеются в виду знаковые события, своеобразные маркеры процессов, которые только начинаются, но дальнейшее развитие которых, может повлиять на криминальную ситуацию; результаты мониторинга информации о мнениях, оценках, установках, которые распространяются в социальных сетях, на форумах, в комментариях на сайтах

в Интернете. Стремительный рост значения указанной информации для формирования поведения населения, особенно молодежи, свидетельствует о том, что выборочные исследования такого рода необходимо начинать уже сейчас. Блок информации о преступности рекомендуется дополнить следующими видами информации: результатам ежегодного репрезентативного опроса населения России по степени его виктимизации, уровня латентности наиболее распространенных преступлений, оценки состояния преступности и деятельности полиции по противодействию ей. Данные предложения не новы, но до сих пор в полном объеме не были реализованы. На постоянной основе руководством МВД России проводится работа по опросу населения страны о степени доверия населения к полиции и оценки ее деятельности. Значит, есть реальная возможность расширить содержание опроса и, наконец, реализовать эту идею, дополнив результатами исследования выборочного репрезентативного массива данных о конкретных преступлениях, в том числе и латентных. Несмотря на методическую и организационно-техническую сложность получения таких данных, эту работу необходимо проводить, т. к. успешное решение этой задачи позволит не только поднять на качественно новый уровень прогнозирование структуры преступности, но и решить важную проблему предупреждения и выявления латентных преступлений. Вторым направлением совершенствования прогнозирования преступности в стране является расширение круга методик, которые используются при его осуществлении и разработка в случае необходимости новых методик. До этого времени прогнозные оценки показателей динамики преступности в целом, отдельных групп и видов преступлений осуществлялись помощью, так называемого метода «случайных блужданий с дрейфом» с обязательной корректировкой прогнозных данных с помощью экспертных оценок. Считаем целесообразным применить в опытном режиме другие методы прогнозирования, которые бы позволили определять количественные

параметры влияния факторов, которые отражаются количественными показателями, на показатели преступности, включая и латентную. Это в частности многофакторные регрессионные модели. На наш взгляд, было бы полезно ввести также регулярное использование при подготовке прогноза латентной преступности метода экспертных оценок специалистов-практиков. Такой ежегодный экспертный опрос позволит получить информацию о латентных криминогенных процессах в обществе, новых видах преступлений и способах их совершения, то есть дополнить и конкретизировать качественный прогноз преступности. В современных условиях есть необходимость разработки специальной методики прогнозирования влияния на криминальную ситуацию изменений в нормативно-правовой базе противодействия преступности и организационно-управленческих решений, направленных на реформирование правоохранительной деятельности. Она должна обеспечить определение как качественного характера такого воздействия, так и его приблизительных количественных параметров.

Таким образом, дальнейшее развитие и совершенствование методов оперативно-розыскного прогнозирования с целью выявления латентных преступлений является актуальным и перспективным, но более серьезной проблемой является внедрение их в оперативно-служебную деятельность территориальных и региональных ОВД, где соответствующие научно-методические наработки, к сожалению, используются не в полном объеме, что, несомненно, снижает эффективность противодействия преступности.

Литература

1. Лунеев В. В. Преступность XX века: мировые, религиозные и российские тенденции. М., 2005.
2. Сазонова Н. В. Латентная преступность: понятие, причины и измерения: дис. ... канд. юрид. наук. Красноярск, 2004.

3. Шувалов А.П., Тишкин Д.Н. Актуальные вопросы совершенствования научно-методического обеспечения оперативно-разыскного прогнозирования в сфере противодействия религиозному экстремизму // Юристъ-Правоведъ. 2018. № 3(86).

4. Овчинский С.С. К вопросу о прогнозировании индивидуального преступного поведения // Научная информация по вопросам борьбы с преступностью: сборник. М. 1972. № 30.

5. Овчинский С.С. Информационно-поисковое обеспечение прогнозирования преступного поведения ранее несудимых // Труды ВНИИ МВД СССР. 1974. № 29.

7. Лукашов В.А. Проблемы оперативно-розыскной деятельности: избранные работы. М., 2005.

8. Обложко А.Г. О результатах исследования прогностического мышления сотрудников оперативных аппаратов // Проблемы повышения эффективности деятельности ОВД: межвузовский сборник научных трудов. М., 1992.

9. Шувалов А.П., Тишкин Д.Н. Оперативно-розыскное прогнозирование в сфере противодействия религиозному экстремизму: актуальные вопросы комплексного взаимодействия с институтами гражданского общества // Юристъ-Правоведъ. 2020. № 1(92).

10. Шувалов А.П., Тишкин Д.Н. актуальные вопросы применения метода индикаторов в оперативно-розыском прогнозировании в сфере противодействия религиозному экстремизму // Юристъ-Правоведъ. 2019. № 1(88).

© Шувалов А.П., 2025

**ДЕЯТЕЛЬНОСТЬ СОТРУДНИКОВ УГОЛОВНОГО РОЗЫСКА
ПО ОПЕРАТИВНОМУ СОПРОВОЖДЕНИЮ
УГОЛОВНЫХ ДЕЛ В СУДЕ**

Щербаченко А.К.

Начальник кафедры уголовного процесса
Ростовского юридического института МВД России,
доктор юридических наук, доцент

Серебрянников С.В.

Преподаватель кафедры уголовного процесса
Ростовского юридического института МВД России

Оперативно-розыскная деятельность является важнейшим компонентом системы обеспечения законности и правопорядка. Особую значимость она приобретает в ходе судебного разбирательства, когда возникает необходимость в сохранении объективности процесса, защите участников, а также в выявлении новых обстоятельств, способных повлиять на исход дела. В этой связи деятельность сотрудников уголовного розыска по оперативному сопровождению уголовных дел в суде приобретает особую значимость и требует теоретического осмысления.

Оперативное сопровождение уголовных дел в ходе судебного разбирательства представляет собой комплекс мероприятий, направленных на содействие суду в обеспечении законности, недопущении давления на свидетелей, выявлении новых эпизодов преступной деятельности и предупреждении противоправных действий способных повлиять на объективность правосудия.

В ходе судебного разбирательства сотрудники уголовного розыска выполняют свои задачи, опираясь на положения Федерального закона № 144-ФЗ «Об оперативно-розыскной деятельности».

Сотрудники уголовного розыска не являются субъектами судебного разбирательства, однако их роль опосредованно реализуется через:

- 1) предоставление оперативной информации прокурору;
- 2) исполнение поручений суда и прокуратуры;
- 3) участие в обеспечении мер безопасности;
- 4) даче показаний по эпизодам, выявленным в ходе оперативной работы;
- 5) обеспечение режима секретности и сохранности информации.

Особое значение имеет слаженное взаимодействие с судебными приставами, органами прокуратуры и подразделениями Федеральной службы безопасности, если дело имеет повышенный уровень угрозы.

Рассматривая правовые основы деятельности сотрудников уголовного розыска, осуществляющих сопровождение уголовных дел, необходимо указать на следующие нормативные правовые акты:

1. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ.

2. Уголовно-процессуальный кодекс Российской Федерации (в части, касающейся взаимодействия следствия и суда).

3. Ведомственные приказы МВД России, в том числе касающиеся взаимодействия с органами прокуратуры и суда.

4. Приказы совместного характера между МВД России и Генеральной прокуратурой.

Уяснив вкратце суть исследуемой нами темы, предлагается классифицировать «оперативное сопровождение» уголовных дел общеуголовной направленности исходя из специфики на 3 основные группы:

1. Оперативное сопровождение уголовных дел общеуголовной направленности, относящихся к подследственности Следственного комитета Российской Федерации.

2. Оперативное сопровождение уголовных дел общеуголовной направленности, относящихся к подследственности органов внутренних дел.

3. Оперативное сопровождение уголовных дел общеуголовной направленности по преступлениям, совершенным в составе организованных преступных групп.

Анализ деятельности сотрудников органов внутренних дел показал, что создание следственно-оперативных групп, является наиболее эффективной формой внутреннего взаимодействия органов внутренних дел при раскрытии и расследовании преступлений. Обеспечивает сбор полной и объективной доказательственной базы сторона обвинения. Однако, как и любая человеческая деятельность, деятельность сотрудников следственно-оперативной группы имеет свои упущения, связанные, например, с несвоевременным выполнением пунктов намеченного плана, формальным подходом к исполнению своих обязанностей.

Многие исследователи подчеркивают значимость деятельности сотрудников уголовного розыска в процессе оперативного сопровождения расследуемых уголовных дел. По мнению А.В. Бородина, эффективное оперативное сопровождение способствует не только своевременному выявлению и пресечению преступлений, но и повышает доказательственную базу уголовного дела, укрепляя тем самым позиции следствия в суде. В свою очередь, И.П. Грачев акцентирует внимание на необходимости тесного взаимодействия оперативных работников с органами предварительного расследования, подчеркивая, что несогласованность действий может привести к утрате значимой информации и снижению эффективности расследования.

На современном этапе в деятельности сотрудников уголовного розыска по оперативному сопровождению уголовных дел наблюдается ряд проблем, снижающих эффективность данной работы. Одной из ключевых проблем является отсутствие должного уровня взаимодействия между оперативными подразделениями и органами предварительного расследования. Разобщенность

действий нередко приводит к дублированию функций, потере ценной информации и снижению общего качества расследования.

Кроме того, остается актуальной проблема недостаточного кадрового обеспечения. Имеет место нехватка квалифицированных оперативных сотрудников, перегрузка делами негативно сказывается на оперативности и результативности сопровождения уголовных дел в суде.

Еще одной важной проблемой является недостаточная правовая регламентация взаимодействия между подразделениями, участвующими в расследовании. Отсутствие четко прописанных алгоритмов совместных действий и правовых оснований для оперативных мероприятий в ходе следствия создает риски нарушения процессуального законодательства.

Для устранения данных проблем нами предлагается:

1. Разработка и внедрение межведомственных регламентов взаимодействия между оперативными подразделениями и следственными органами, с четким разграничением полномочий, обязанностей и ответственности.

2. Повышение уровня профессиональной подготовки оперативных сотрудников, включая обучение современным методам криминального анализа, основам цифровой криминалистики, работе с аналитическими платформами.

3. Расширение законодательного регулирования оперативного сопровождения уголовных дел, с целью устранения пробелов и повышения правовой определенности действий сотрудников уголовного розыска.

Деятельность сотрудников уголовного розыска на этапе судебного разбирательства является важнейшим элементом обеспечения эффективности всего уголовного процесса. Оперативное сопровождение уголовных дел в суде требует от сотрудников высокого уровня профессионализма, правовой и психологической подготовки, а также умения взаимодействовать с другими участниками уголовного судопроизводства.

Резюмируя все вышесказанное можно сделать вывод, что деятельность сотрудников уголовного розыска на стадии судебного разбирательства является

важной частью общей системы обеспечения законности и правосудия. Их участие в оперативном сопровождении позволяет эффективно выявлять и пресекать попытки вмешательства в процесс, обеспечивать безопасность его участников и повышать уровень доверия к судебной системе. Необходимость четкой правовой регламентации этой деятельности и межведомственного взаимодействия делает ее предметом постоянного научного и практического интереса.

Литература

1. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «Гарант».

2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.01 2001 г. № 177-ФЗ. Доступ из справ. правовой системы «Гарант».

© Щербаченко А.К., Серебрянников С.В., 2025

УДК 351.745.7:343.34:004

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ МЕТОДАМИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Ягодина Э.А.

Адъюнкт адъюнктуры

Ростовского юридического института МВД России

Активное внедрение цифровых технологий во все сферы общественной жизни неизбежно влияет и на характер преступности. Киберпространство постепенно превращается в самостоятельную криминальную среду, где совершаются деяния, способные причинить значительный ущерб как отдельным гражданам, так и государству в целом. Масштаб и темпы роста подобных преступлений обуславливают необходимость совершенствования

механизмов противодействия им, в частности — инструментов оперативно-розыскной деятельности (далее — ОРД).

Киберпреступность отличается повышенной скрытностью, использованием сложных способов сокрытия следов и возможностью совершения противоправных действий дистанционно, в том числе с использованием зарубежных ресурсов и технологий, позволяющих действовать анонимно. Эти факторы существенно снижают эффективность традиционных оперативных методов, выработанных для борьбы с преступлениями офлайн. В современных условиях оперативные подразделения сталкиваются с задачами, требующими не только правовой адаптации существующих процедур, но и внедрения инновационных технических средств и алгоритмов анализа информации.

По этой причине научный анализ и исследование возможностей оперативно-розыскной деятельности в сфере кибербезопасности становится одним из ключевых направлений современной криминалистической науки и практики. Комплексное исследование проблем и перспектив применения оперативных методов в цифровой среде позволит сформировать более эффективные подходы к выявлению, предупреждению и пресечению преступлений, совершаемых с использованием информационных технологий.

Киберпреступность — это совокупность противоправных деяний, совершаемых с использованием информационно-коммуникационных технологий, компьютерных систем, сетей или данных, направленных на нарушение общественной безопасности, посягательство на информацию ее носителей, а также на имущественные, личные и иные права граждан, организаций и государства.

В последние годы киберпреступность превратилась из локального явления в масштабную глобальную угрозу. В отличие от традиционных форм преступного поведения, киберпреступления не имеют строгих территориальных границ, а цифровая среда способна обеспечить преступникам

некоторую анонимность, мобильность и возможность совершать противоправные действия в транснациональном масштабе.

К числу наиболее распространенных видов киберпреступлений относятся хищения денежных средств с банковских счетов с использованием вредоносных программ, несанкционированный доступ к компьютерной информации, распространение персональных данных, вымогательство с использованием шифровальщиков, фишинговые атаки, а также манипуляции с криптовалютными активами.

Сложность борьбы с данным видом преступности связана с рядом специфических особенностей. Во-первых, высокий уровень латентности: многие инциденты, связанные с киберпреступлениями, не фиксируются правоохранительными органами, поскольку потерпевшие предпочитают не обращаться в полицию, опасаясь утечки информации или репутационных потерь. Во-вторых, постоянное совершенствование технических средств и методов, которыми пользуются преступники. В-третьих, трудности в идентификации лиц, совершающих преступления с использованием программ, дающих возможность замаскировать себя и свое местонахождение (VPN, прокси-серверы, браузеры и различные программы).

Именно эти обстоятельства обуславливают необходимость адаптации существующих методов оперативно-розыскной деятельности к специфике цифровой среды, а также выработки новых подходов к сбору и анализу доказательственной информации.

Основой правового регулирования оперативно-розыскной деятельности в Российской Федерации является Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ. Его положения распространяются на широкий спектр оперативных мероприятий, включая те, что могут быть применены в цифровой среде. Однако изначально данный закон разрабатывался в период, когда киберпреступность не имела такого масштаба, это и порождает определенные коллизии и правовые проблемы.

К оперативно-розыскным мероприятиям, имеющим особое значение в сфере противодействия киберпреступлениям, относятся: контроль и запись сообщений, снятие информации с технических каналов связи, оперативное наблюдение и оперативный эксперимент, получение компьютерной информации, имеющей значение для раскрытия преступлений.

Серьезной проблемой является то, что цифровая информация может находиться за пределами юрисдикции Российской Федерации. В таких случаях применяются механизмы международного сотрудничества, предусмотрены, в частности, Будапештской конвенцией о киберпреступности [3]. Практика показывает, что без участия зарубежных партнеров доступ к значимым цифровым доказательствам часто оказывается невозможным.

Отдельного внимания заслуживает вопрос допустимости оперативных материалов, полученных в ходе работы в цифровой среде. При проведении оперативно-розыскных мероприятий (далее — ОРМ) необходимо строгое соблюдение прав граждан. Несоблюдение этих условий может повлечь признание доказательств недопустимыми и повлиять на исход уголовного дела.

В условиях стремительного развития технологий оперативные подразделения вынуждены применять не только традиционные, но и инновационные методы сбора информации. Среди них важное место занимают мониторинг сетевого трафика с целью выявления подозрительной активности, анализ данных из открытых источников (OSINT), применение программных средств для отслеживания криптовалютных транзакций, технические мероприятия по деанонимизации пользователей, причастных к противоправной деятельности.

Необходимо отметить, что немаловажную роль играет агентурная работа. Несмотря на то, что киберпреступления совершаются в виртуальном пространстве, за ними всегда стоят реальные лица или группы. Использование агентурного аппарата, внедрение сотрудников в криминальные сообщества

в Даркнете, установление оперативных контактов — эффективные инструменты в борьбе с киберпреступлениями при правильной организации.

Тактические особенности проведения ОРМ в цифровой среде заключаются в точной фиксации времени, источника и способа получения информации. Это необходимо для того, чтобы в дальнейшем собранные данные могли быть приобщены к материалам уголовного дела в качестве допустимых доказательств.

Если анализировать все вышесказанное, то можно прийти к тому, что одной из ключевых проблем является несоответствие между скоростью развития технологий и темпами обновления правовой базы. Ведь законодательство не всегда успевает адаптироваться к новым видам киберугроз, что приводит к неопределенности в вопросах допустимости и процедуры проведения отдельных ОРМ.

Кроме того, значительное влияние оказывает недостаток квалифицированных кадров, способных грамотно работать с цифровыми следами, ко всему этому так же ограниченность материально-технических ресурсов в подразделениях. Серьезной проблемой остается межведомственная разобщенность — отсутствие единого механизма оперативного обмена информацией между различными структурами, включая МВД России, ФСБ России и Следственный комитет Российской Федерации.

Перспективным направлением развития является расширение применения технологий искусственного интеллекта и машинного обучения для автоматической фильтрации массивов данных и выявления подозрительных цифровых паттернов. Не менее важно совершенствовать способы осуществления мирового сотрудничества, упрощать процедуры обмена данными и обеспечить совместимость информационных систем.

Но одним из ключевых условий для эффективности предотвращения киберпреступлений методами ОРД является баланс между обеспечением национальной безопасности и соблюдением конституционных прав граждан,

включая тайну личной жизни и переписки. Только лишь комплексный подход позволит выработать устойчивую модель противодействия киберпреступности.

Проведенный анализ показывает, что киберпреступность представляет собой сложный и динамично развивающийся феномен, обладающий рядом особенностей, отличающих его от традиционных форм преступной деятельности [4]. Основные сложности связаны с трансграничным характером правонарушений, высокой степенью анонимности преступников, а также быстрым технологическим развитием средств, используемых в преступных целях.

Безусловно, действующая система ОРМ имеет значительный потенциал и неоспоримую эффективность в раскрытии преступлений, но она не в полной мере соответствует темпам цифрового развития.

Законодательная база требует дальнейшего совершенствования, а тактика и методы оперативных подразделений – регулярного обновления и адаптации к новым угрозам. Особое значение приобретают технические средства, позволяющие оперативно выявлять, фиксировать и анализировать цифровые следы киберпреступлений.

С учетом всего изложенного представляется целесообразным:

1. Усовершенствовать нормативно-правовое регулирование ОРД в цифровой сфере, включая более четкое определение процедур получения, хранения и использования цифровых доказательств.

2. Усилить техническое оснащение оперативных подразделений современными средствами анализа сетевого трафика, деанонимизации и криптографической экспертизы [6].

3. Развивать систему межведомственного взаимодействия между правоохранительными структурами, а также с зарубежными партнерами, с целью оперативного обмена данными.

4. Повысить уровень подготовки кадров, в том числе за счет внедрения специализированных курсов по кибербезопасности и цифровой криминалистике в систему профессионального обучения сотрудников.

5. Расширять применение технологий искусственного интеллекта и анализ большого объема данных и их использование в строгих правовых рамках.

Реализация этих предложений позволит повысить результативность ОРД в сфере кибербезопасности, обеспечить более эффективную работу по предупреждению, выявлению и пресечению преступлений в цифровой среде, а также укрепить национальную безопасность в целом.

Литература

1. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

2. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31. Ст. 3448.

3. Будапештская конвенция о киберпреступности: Конвенция Совета Европы ETS № 185 от 23 ноября 2001 г.

4. Гришин, Д.А. Киберпреступность и проблемы противодействия ей в современном обществе. М., 2021.

5. Интерпол. Global Cybercrime Strategy 2022–2025. Lyon: INTERPOL, 2022.

6. Сборник МВД РФ Современные технологии в оперативно-розыскной деятельности. М., 2022.

7. Кузнецов С.Н. Киберпреступность и возможности ОРД по ее раскрытию // Вестник криминалистики. 2024. № 1(57).

ОСОБЕННОСТИ ВЫЯВЛЕНИЯ ПРИЗНАКОВ НЕЗАКОННОЙ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Яцкина И.А.

Старший преподаватель кафедры
криминалистики и оперативно-разыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

По данным правоохранительных органов, ежегодно выявляются тысячи случаев ведения бизнеса без государственной регистрации и лицензий, что не только подрывает легальный рынок, но и создает благоприятные условия для финансовых махинаций, отмывания денежных средств и коррупции. Современные тенденции экономической преступности требуют совершенствования методов выявления и раскрытия незаконного предпринимательства. Особые трудности вызывает доказательство состава преступления, установление лиц, организовавших нелегальную деятельность, а также выявление и изъятие материальных следов преступления, включая финансовую документацию и электронные носители информации. В связи с этим изучение криминалистических особенностей расследования незаконного предпринимательства является важной научной и практической задачей.

Актуальность темы исследования обусловлена значительным распространением незаконной предпринимательской деятельности, которая оказывает негативное влияние на экономическую безопасность государства, конкурентную среду и поступления в бюджет.

Незаконное предпринимательство — это экономическое преступление, представляющее собой деятельность, осуществляемую без регистрации, лицензий либо с нарушением установленных законодательством требований.

Возбуждение уголовного дела по данному составу преступления напрямую связано с работой правоохранительных органов, которые выявляют признаки незаконной предпринимательской деятельности в различных сферах экономики.

С криминалистической точки зрения, признаки преступления представляют собой конкретные факты и обстоятельства, указывающие на возможное совершение противоправных действий. Одной из особенностей незаконного предпринимательства является его латентный характер, а именно:

1. Оно может вестись либо в скрытой форме (например, без регистрации юридического лица или индивидуального предпринимателя);

2. Под видом легальной деятельности, но с грубыми нарушениями законодательства, такими как предоставление ложных сведений при регистрации, работе без лицензий или с их несоблюдением.

Возбуждение уголовного дела о незаконном предпринимательстве и дальнейшее производство предварительного расследования по данному делу непосредственно связано с деятельностью правоохранительных органов выявлению признаков осуществления незаконной предпринимательской деятельности в определенной сфере экономики.

Эти признаки не всегда однозначно указывают на преступление, однако они дают основания для проверки хозяйственной деятельности субъекта и формирования версий о возможных нарушениях.

Выявление и документирование преступной деятельности осуществляется, как правило, на этапе проведения оперативно-розыскных мероприятий и проверок контрольных органов. К наиболее эффективным методам можно отнести:

1. Опрос лиц, владеющих информацией — беседы с сотрудниками, партнерами, клиентами или конкурентами незаконного предпринимателя.

2. Запрос данных в государственные органы — налоговые органы, лицензирующие структуры, торгово-промышленные палаты.

3. Сбор образцов продукции и документов — изучение товаров, сырья и отчетности, используемых в незаконной деятельности.

4. Контрольная закупка — фиксация факта продажи товаров или услуг без надлежащего оформления.

5. Исследование предметов и документов — анализ документации для выявления несоответствий.

6. Оперативное наблюдение — слежка за объектом, проверка мест хранения продукции и источников поставок;

3. Контроль связи — анализ почтовых, телефонных и интернет-коммуникаций.

4. Оперативное внедрение — проникновение в преступную группу для сбора доказательств.

При этом подавляющее большинство (81 %) сотрудников следственных подразделений указывают, что основную часть первичных материалов по ст. 171 Уголовного кодекса Российской Федерации (незаконное предпринимательство) предоставляют оперативники подразделений по борьбе с экономическими преступлениями.

Для эффективного расследования на первоначальном этапе проводится ряд мероприятий.

Во-первых, проводятся документальные проверки и ревизии, направленные на установление факта незаконной предпринимательской деятельности, выявления финансовых нарушений, уклонения от налогов и других преступлений в экономической сфере. В качестве методов реализации данного мероприятия выступают анализ бухгалтерских документов, договоров, накладных, счетов-фактур, выявление несоответствий между официальной отчетностью и реальными оборотами бизнеса и проверка кассовых операций, банковских счетов, движения денежных средств. В результате проведенного мероприятия формируется акт проверки или ревизии, который может служить основанием для дальнейших следственных действий.

Во-вторых, осуществляются следственные действия, допустимые до возбуждения уголовного дела. Цель мероприятия — сбор доказательств, подтверждающих факт незаконной предпринимательской деятельности, без формального возбуждения уголовного дела. Оно реализуется за счет оперативно-розыскных мероприятий (например, контрольной закупки или скрытого наблюдения), выемки документов, осмотра места ведения бизнеса и получения данных от налоговых органов, банков и других государственных учреждений. Таким образом, производится накопление доказательной базы, достаточной для принятия решения о возбуждении уголовного дела.

В-третьих, необходимо проведение опроса причастных лиц для получения показаний от лиц, имеющих информацию о незаконной деятельности. К числу опрашиваемых относятся работники организации, поставщики, клиенты, контрагенты, свидетели, которые могли наблюдать незаконную деятельность. В результате данного мероприятия у следствия имеются показания, которые могут подтвердить факт незаконной деятельности, схемы уклонения от налогов, а также личности организаторов и исполнителей.

Приведенные мероприятия позволяют собрать достаточную доказательную базу для последующего возбуждения уголовного дела и привлечения виновных к ответственности. В ходе них особое внимание уделяется выявлению ключевых аспектов незаконной предпринимательской деятельности [1]:

1. Факты ведения бизнеса без регистрации или лицензии.
2. Источники поступления товаров и финансов.
3. Механизмы документооборота и учета доходов.
4. Установление партнеров и контрагентов.
5. Способы уклонения от контроля и ответственности.

Раскрытие незаконного предпринимательства требует слаженной работы оперативных, следственных и контрольных (например, Федеральной налоговой службы, Роспотребнадзора, Росфинмониторинга, трудовой инспекции,

Федеральной таможенной службы и других) органов. Тактическое планирование, использование методов оперативно-розыскной деятельности и проверочных мероприятий позволяют не только выявить преступную схему, но и собрать доказательства, достаточные для возбуждения уголовного дела и последующего судебного разбирательства.

Таким образом, выявление признаков незаконного предпринимательства является важной задачей для обеспечения экономической безопасности государства и защиты прав добросовестных предпринимателей. Эффективное выявление незаконного предпринимательства требует использования комплексного подхода, включающего правовой, экономический и криминалистический анализ. Совершенствование методов контроля и усиление ответственности за незаконную деятельность являются важными мерами для защиты экономической системы и прав добросовестных участников рынка.

Раскрытие преступлений, связанных с незаконной предпринимательской деятельностью, представляет собой сложный процесс, требующий детального анализа финансовых потоков, хозяйственной деятельности и документов субъектов, вовлеченных в преступные схемы. В отличие от традиционных преступлений, такие правонарушения нередко носят латентный характер, поскольку их участники стремятся скрыть следы противоправных действий, используя сложные экономические и юридические механизмы.

Анализ следственной практики позволяет выделить три основные ситуации, возникающие при расследовании преступлений, связанных с незаконной предпринимательской деятельностью.

1. Полная картина преступления — имеются документально подтвержденные факты незаконной предпринимательской деятельности, установлены большинство причастных лиц.

2. Частично установленная структура преступления — организатор и основные участники известны, но их местонахождение остается неопределенным.

3. Прекращенная деятельность — предприятие закрылось, деньги со счетов исчезли, личности преступников не установлены.

Наиболее распространенным сценарием является первый, когда у следствия уже имеются значительные доказательства.

Расследование преступлений в сфере незаконного предпринимательства требует комплексного подхода и детального анализа всех обстоятельств. При наличии полной картины нарушения следствие сосредотачивается на сборе и фиксации доказательств, идентификации виновных и установлении масштабов ущерба.

Первым делом производится изъятие документов у компаний, взаимодействующих с незаконными предпринимателями. Следователь получает санкцию на выемку бухгалтерских и юридических документов, договоров, счетов-фактур, накладных и других финансовых бумаг. Далее анализируется переписка с контрагентами, банковские транзакции, акты выполненных работ и отчеты о поставках. Особое внимание уделяется фиктивным компаниям и подставным лицам, через которых осуществлялись нелегальные сделки.

Второй этап — проведение обысков в офисах и по месту жительства руководителей. Обыски помогают обнаружить скрытые финансовые отчеты, черновую бухгалтерию, электронные носители информации. Изъятие мобильных телефонов и компьютеров позволяет получить доступ к переписке, в том числе через мессенджеры и электронную почту. Важно зафиксировать любые попытки уничтожения улик или уклонения от ответственности.

Далее производится арест и изучение почтовых отправлений, финансовой документации. Отслеживаются почтовые отправления, в которых могут содержаться контракты, счета, документы о переводах средств. Финансовая

документация анализируется на предмет сокрытия доходов, использования подставных счетов и офшорных схем.

Следующий шаг рассматриваемой тактики — это проведение ревизий и проверок, анализ их результатов, другими словами, осуществляется налоговый аудит, проверка отчетности о прибыли и убытках, контроль за кассовыми операциями. Ревизия помогает выявить расхождения между официальной отчетностью и реальными оборотами. Особое внимание уделяется неучтенным товарам, услугам и необоснованным расходам.

Путем оперативно-следственных мероприятий осуществляется установление мест ведения незаконной предпринимательской деятельности и их осмотр: производится обнаружение складов, производственных помещений, нелегальных офисов. При осмотре фиксируется состояние оборудования, сырья, полуфабрикатов, готовой продукции. Проводится подробное описание местонахождения, особенностей производства и условий работы.

Допросы подозреваемых, контрагентов и свидетелей проводятся с целью выявления схемы преступной деятельности, ролей участников, источников финансирования, установления реальных поставщиков, покупателей и посредников, а сотрудников контролирующих органов — для получения информации о выявленных нарушениях, ранее проведенных проверках и выявленных несоответствиях.

При осмотре мест ведения бизнеса и анализе финансовых потоков рассматривается движение денежных средств по банковским счетам, выявляются схемы отмывания денег и уклонения от налогов, определяются источники финансирования и конечные бенефициары, осуществляется контроль за наличными расчетами и фиксация неучтенных активов.

В качестве заключительного этапа рассматриваемой тактики расследования выступает назначение и проведение судебных экспертиз [2]:

1. Экономическая экспертиза направлена выявление реального дохода, расчет налогов, подлежащих уплате.

2. В ходе судебно-бухгалтерская экспертизы анализируются бухгалтерские документы и выявляются фальсификации.

3. Дактилоскопическая и почерковедческая экспертиза проводится с целью установления авторства подписей и почерка в документах.

4. При технико-криминалистической экспертизе документов подлежат выявлению подделки и изменения в документации.

5. Судебно-товароведческая экспертиза позволяет оценить стоимости изъятой продукции и оборудования.

Таким образом, комплексный подход к расследованию позволяет не только выявить всех участников схемы, но и предотвратить последующие преступления, а также привлечь к ответственности как организаторов, так и соучастников незаконной предпринимательской деятельности.

При расследовании преступлений, когда структура преступления установлена частично или деятельность незаконного предпринимателя прекращена, помимо проведения мероприятий, перечисленных выше, первостепенной и главной задачей становится установление местонахождения фигурантов дела и выявление соучастников. Для достижения поставленных задач применяются следующие методы расследования:

1. Опрос родственников, деловых партнеров, знакомых.

2. Оперативное наблюдение.

3. Анализ изъятых документов на предмет наличия информации о местонахождении участников схемы.

После установления подозреваемых проводится их задержание и личный обыск с изъятием документов и носителей информации.

Ключевые особенности построения версий при расследовании незаконного предпринимательства:

1. Опережающая оперативно-розыскная работа — криминалистические версии зачастую выдвигаются еще до возбуждения уголовного дела.

2. Акцент на выявление масштабов преступной деятельности — важно установить не только факт незаконного бизнеса, но и ущерб, причиненный государству.

3. Ограниченность круга подозреваемых — в отличие от общеуголовных преступлений, здесь фигуранты чаще всего связаны с предпринимательской средой.

Расследование преступлений, связанных с незаконным предпринимательством, требует детального анализа обстоятельств и построения различных версий, которые помогают следствию установить истинные мотивы, схемы и масштабы противоправной деятельности. В следственной практике существует ряд типичных версий по делам о незаконном предпринимательстве.

Первая версия предполагает, что деятельность велась без регистрации в налоговых органах, а именно, лицо или группа лиц осуществляли предпринимательскую деятельность, не ставя ее на учет в налоговых органах, что является нарушением ст. 171 Уголовного кодекса Российской Федерации. Цель подобного ведения дел — избежание уплаты налогов, сборов и других обязательных платежей, а также сокрытие реальных доходов.

В данном случае противоправное деяние осуществляется с помощью подставных лиц для аренды помещений и открытия счетов, использования наличных расчетов без фиксации операций в бухгалтерской отчетности и отсутствия регистрации работников и заключения трудовых договоров.

При выявлении факта данного вида нарушения производится оперативная проверка через налоговые органы о наличии регистрации, изъятие финансовых документов и черной бухгалтерии, а также допрос свидетелей, контрагентов и клиентов.

В основе второй версии заложено предположение о том, что предпринимательская деятельность формально зарегистрирована, однако при подаче документов в налоговые органы или иные контролирующие структуры были предоставлены заведомо ложные сведения. В данном случае преступник преследует такие цели, как получение незаконных налоговых льгот, сокрытие реальных собственников и бенефициаров, уход от ответственности за финансовые нарушения.

Для ухода от ответственности и представления деятельности законной преступные лица осуществляют регистрацию фирмы на подставное лицо (например, безработного или иностранного гражданина), фальсификацию бухгалтерских отчетов, снижение прибыли или увеличение расходов для уменьшения налоговой базы и используют фиктивные договоры и акты выполненных работ.

В ходе следственных действий производится сравнение поданных документов с реальными данными о ведении бизнеса, финансово-экономическая экспертиза, проверка подписей и почерка на документах (почерковедческая экспертиза).

Суть третьей типичной версии заключается в том, что деятельность осуществлялась в сферах, подлежащих обязательному лицензированию, без соответствующего разрешения или с нарушением условий лицензии. Таким образом, преступник преследует избежание контроля со стороны органов лицензирования, увеличение прибыли за счет сокращения расходов на соблюдение нормативов, уклонение от налоговых и страховых выплат. В качестве примера данного типа нарушений из следственной практики можно привести:

1. Оказание медицинских услуг без лицензии.
2. Производство алкоголя или табачной продукции без акцизных марок.
3. Перевозка пассажиров или грузов без соответствующих документов.

Для выявления рассматриваемого правонарушения следствие осуществляет проверку реестра лицензий и разрешительных документов, опрос сотрудников контролирующих органов, осмотр помещений, оборудования и изъятие продукции.

Выдвижение и проверка приведенных типичных версий позволяет следствию установить истинные мотивы и методы незаконной предпринимательской деятельности, а также привлечь виновных к ответственности и предотвратить дальнейшие экономические преступления, а также на основании них планируется расследование, включающее анализ документов, допросы, экспертизы.

Эффективное расследование невозможно без координации с другими государственными структурами. В практической деятельности используются следующие формы взаимодействия:

1. Обмен информацией с контрольно-ревизионными органами на этапе возбуждения дела;
2. Совместные оперативные мероприятия с подразделениями по борьбе с экономическими преступлениями;
3. Оказание экспертной помощи (бухгалтерской, финансовой, товароведческого анализа);
4. Создание следственно-оперативных групп для комплексного расследования данных действий.

На каждом этапе следственные органы сталкиваются с особыми задачами и вызовами, которые требуют применения криминалистических методов и участия профильных специалистов, однако некоторые этапы расследования требуют особого подхода, а именно.

1. Осмотр места происшествия для выявления доказательств, подтверждающих факт ведения незаконной деятельности, фиксации материальных следов преступления и идентификации ключевых участников схемы. Проводится в офисах, складах, производственных помещениях, а также

жилых помещениях, где могли вестись расчеты или храниться документация.

В качестве особенностей данного этапа рассмотрим следующие аспекты:

1.1. Фиксация материальных доказательств: оборудования, сырья, готовой продукции, финансовой документации, черновых записей.

1.2. Изъятие цифровых носителей (компьютеры, жесткие диски, флеш-накопители, серверы с данными о транзакциях и партнерах).

1.3. Анализ бухгалтерии и договоров, поиск расхождений между официальной отчетностью и реальными доходами.

1.4. Работа с цифровыми данными, восстановление удаленной информации, анализ переписки с контрагентами, проверка платежных систем.

1.5. Необходимость привлечения к следственным действиям специалистов (бухгалтеров, IT-экспертов, криминалистов по финансовым преступлениям), которые помогают выявить схемы уклонения от налогов и отмывания доходов.

Например, при выявлении подпольного цеха по производству контрафактной алкогольной продукции изымается оборудование, акцизные марки, накладные на поставку сырья и фиктивные лицензии. Эксперты проверяют подлинность документов и проводят химический анализ продукции.

2. Допрос подозреваемого для получения показаний, которые подтверждают или опровергают выдвинутые версии о незаконной деятельности. Особенности данного мероприятия является необходимость подготовки к допросу, а именно, анализ собранных доказательств, финансовых документов, показаний свидетелей, что позволяет ограничить возможности подозреваемого для манипуляции фактами и сокрытия реальных доходов. В подобном случае подозреваемому следует задать ряд ключевых вопросов для понимания полной картины противоправного деяние:

1. Как долго осуществлялась деятельность?

2. Кто поставлял оборудование и сырье?

3. Какие схемы использовались для уклонения от налогов и получения нелегальной прибыли?

4. С кем сотрудничали и какие финансовые операции проводили?

Особое внимание стоит уделить тактике допроса. Важно использовать факты, полученные в ходе осмотра места происшествия, проверки финансовых потоков и показаний свидетелей, сопоставлять показания с данными бухгалтерской отчетности, банковскими выписками и цифровыми следами, а также наблюдать за поведением подозреваемого, отмечать эмоциональные реакции и ложные показания.

В качестве примера приведем следующий случай из следственной практики: в ходе допроса руководитель компании, занимающейся нелегальным производством косметики, отрицает факт ведения бизнеса. Однако следствие предоставляет доказательства закупки сырья через подставные фирмы и данные о реализации продукции через онлайн-платформы.

Комплексный подход на каждом этапе расследования позволяет не только собрать доказательства, но и выявить все звенья преступной схемы — от организаторов до посредников и клиентов. Участие специалистов, анализ цифровых данных и психологическая тактика допроса играют ключевую роль в успешном завершении следствия. Однако наибольшие трудности в расследовании вызывают следующие мероприятия:

Расследование незаконного предпринимательства требует четкого алгоритма действий: от сбора первоначальных данных до выявления полного круга лиц и подтверждения их вины. Важную роль играет взаимодействие между следственными органами, экспертами и контрольно-надзорными структурами. При этом каждое дело имеет свою специфику — от полного контроля ситуации до необходимости искать скрывающихся участников преступления. Соответственно следственная тактика должна адаптироваться под конкретные условия расследования.

Исходя из всего вышесказанного, можно сделать вывод, что дела, связанные с незаконной предпринимательской деятельностью, требуют серьезного комплекса мероприятий для раскрытия, включая методы финансового анализа, оперативно-розыскные мероприятия, применение информационных технологий и экспертных исследований. Усиление контроля со стороны государства, слаженное взаимодействие его структур в отношении предпринимательской деятельности способны сократить число экономических преступлений и укрепить правопорядок и честное предпринимательство.

Литература

1. Верченко Н.И., Сейбол Е.М. Незаконное предпринимательство: вопросы теории правоприменения // Вестник Омского государственного университета Серия. Право. 2024. № 4.

2. Христинина Е.В. Структура и содержание криминалистической характеристики преступлений, связанных с незаконным предпринимательством // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 2(44).

© Яцкина И.А., 2025

Научное электронное издание

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник научных трудов
Всероссийской научно-практической конференции

(24 октября 2025 г.)

Составитель:

Яцкина Инна Александровна, кандидат юридических наук

Редактор *Н.А. Тапашева*

Корректор *Н.А. Тапашева*

Технический редактор *Н.А. Тапашева*

Компьютерная верстка *И.К. Беницкий*

Издатель: федеральное государственное казенное образовательное
учреждение высшего образования
«Ростовский юридический институт
Министерства внутренних дел Российской Федерации».

Адрес: 344015, г. Ростов-на-Дону, ул. Еременко, 83.

Тел.: 8 (863) 224-58-15. Сайт: <https://рюи.мвд.рф>

Подписано к использованию: 05.03.2026

Тираж 10 экз., Электрон. дан. (1,26 МБ),

1 электрон. опт. диск (CD-R).

ISBN 978-5-8928-8607-9

