

Краснодарский университет МВД России

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Материалы
XIV Всероссийской научно-практической конференции
(30 октября 2025 г.)

Краснодар
2026

УДК 343
ББК 67.408
А437

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Редакционная коллегия:

С. И. Иванов, кандидат юридических наук, доцент (председатель);
А. Н. Горбунов, кандидат юридических наук (заместитель председателя);
В. В. Стукалов, кандидат юридических наук (ответственный секретарь);
Н. С. Железняк, доктор юридических наук, профессор;
В. И. Еремченко, кандидат юридических наук, доцент;
Р. Н. Кучмезов, кандидат юридических наук

Актуальные проблемы теории и практики оперативно-розыскной деятельности [Электронный ресурс] : материалы XIV Всероссий. науч.-практ. конф. (30 окт. 2025 г.) / редкол.: С. И. Иванов, А. Н. Горбунов, В. В. Стукалов и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2026. – 1 электрон. опт. диск.

ISBN 978-5-9266-2265-9

Представлены доклады и тезисы выступлений участников XIV Всероссийской научно-практической конференции «Актуальные проблемы теории и практики оперативно-розыскной деятельности», состоявшейся в Краснодарском университете МВД России 30 октября 2025 г.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343
ББК 67.408

ISBN 978-5-9266-2265-9

© Краснодарский университет
МВД России, 2026

СОДЕРЖАНИЕ

Алехин В.П. Криминологическая характеристика преступлений террористического и экстремистского характера: проблемы теории и практики.....	6
Апшев А.А., Стукалов В.В. Деятельность органов внутренних дел по противодействию преступлениям экстремистской направленности.....	12
Бадма-Горяев С.С., Горбунов А.Н. Роль землячеств и этнических диаспор в формировании криминальной активности иностранных граждан на территории Российской Федерации.....	18
Баженов В.А., Маликова А.А. Сеть Интернет как источник информации для оперативно-розыскной деятельности.....	22
Батоев В.Б. О противодействии использованию технологии MESH-сетей в экстремистской деятельности.....	25
Бондарева А.А. Использование обратной социальной инженерии как способ противодействия телефонному мошенничеству.....	29
Бушуев И.В. Международное сотрудничество в сфере оперативно-розыскной деятельности: опыт и перспективы.....	33
Васильев Э.А., Мороз Р.Н. Теоретические и практические проблемы оперативно-розыскной психологии.....	38
Гонтарь С.Н. Проблемы взаимодействия следователя с органами дознания при реализации материалов оперативно-розыскной деятельности.....	43
Ерохин Р.А, Дюкарь Р.М. Проблемы использования результатов оперативно-розыскной деятельности в доказывании по уголовным делам.....	46
Железняк Н.С. Искусственный интеллект в борьбе с преступностью (оценка дилетанта).....	52
Зоз В.А., Скрипка Д.Д. Понятие оперативно-розыскного мероприятия «Отождествление личности».....	55
Иванов С.И. Некоторые аспекты подготовки и проведения оперативно-розыскных операций по борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий.....	60
Коваленко А.А., Студнев А.С. Особенности проведения оперативно-розыскных мероприятий при выявлении и раскрытии преступлений в жилищно-коммунальной сфере с использованием цифровых платежных систем.....	65
Крюк А.Н., Муталимов Р.Р. Особенности проведения оперативно-розыскного мероприятия «Контроль почтовых отправлений, телеграфных и иных сообщений».....	68

Куминов М.В. Актуальные угрозы информационной безопасности, связанные с развитием интернета вещей (IoT): новые вызовы для оперативно-розыскной деятельности.....	71
Кучмезов Р.Н., Старостенко О.А. Соотношение оперативно-розыскной и следственной деятельности: границы взаимодействия и разграничения полномочий.....	75
Лагуточкин А.В., Миронов Д.А. Трансформация роли научно-технического обеспечения в повышении эффективности оперативно-розыскной деятельности органов внутренних дел	78
Легостаев В.П. Правовые и организационные вопросы привлечения представителей казачества к участию в оперативно-розыскной деятельности.....	82
Лузько Д.Н. Перспективы применения синтетических медиа (Deepfake) в борьбе с преступностью.....	86
Меретуков Г.М., Меретуков А.Г. Теоретико-правовые основы и механизм оценки оперативной обстановки	90
Миронов Д.А., Ерохин Р.А. Значение биометрических технологий для установления и розыска лиц, совершивших преступления.....	96
Назаров М.В., Зоз В.А. Содержание принципа уважения и соблюдения прав и свобод человека и гражданина и его соотношение с принципом законности в оперативно-розыскной деятельности.....	103
Николаенко Д.Н. К вопросу организации взаимодействия между оперативными подразделениями МВД России и Следственным комитетом РФ в процессе расследования налоговых преступлений.....	107
Павлишинец А.Ю., Баженов В.А. Проблемы соотношения оперативно-розыскной и уголовно-процессуальной деятельности: вопросы использования результатов ОРД в доказывании по уголовному делу.....	113
Поезжалов В.Б. Актуальные вопросы противодействия хищениям, совершаемым с использованием информационно-телекоммуникационных технологий.....	117
Сардак Д.Б. Оперативно-розыскная деятельность в условиях цифровизации и киберпреступности.....	120
Сафронов А.А. Сущность, содержание и пределы прокурорского надзора за оперативно-розыскной деятельностью.....	125
Свиридов В.В. Использование технологий искусственного интеллекта в правоохранительной деятельности органов внутренних дел.....	131
Семина М.В., Южанинов В.С. Некоторые особенности противодействия незаконному обороту наркотических средств с использованием информационно-телекоммуникационных технологий...	135

Скрипка С.А., Горбунов А.Н. Осуществление взаимодействия при раскрытии и расследовании дистанционных мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий.....	139
Старостенко О.А. Современные подходы к классификации преступлений в сфере компьютерной информации.....	143
Степанов С.М. Розыск военнослужащих сотрудниками полиции: практика и проблемы взаимодействия.....	150
Студнев А.С., Широков И.В. Оперативно-розыскное противодействие при финансировании экстремистской деятельности в сети Интернет.....	155
Стукалов В.В., Сяткин Э.А. Обеспечение прав и законных интересов граждан при проведении оперативно-розыскных мероприятий	162
Фаниев П.А. О некоторых возможностях инструментов OSINT для получения компьютерной информации в рамках проведения оперативно-розыскных мероприятий.....	167
Шатилов А.В., Косенко А.С. Угрозы молодежной среде в информационно-телекоммуникационном пространстве.....	170
Шахматов А.В., Скоков И.Е. Использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве...	174
Шищенко Е.А. Современные аспекты оперативно-розыскной деятельности по выявлению и расследованию компьютерных преступлений.....	181
Южанинов В.С. Некоторые особенности выявления распространения экстремистских материалов в сети Интернет.....	185

Алехин Виталий Петрович,
доцент кафедры уголовного права
Кубанского государственного аграрного
университета имени И.Т. Трубилина,
кандидат юридических наук, доцент
тел.: 8-918-443-95-17; e-mail: 4439517@mail.ru

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОГО И ЭКСТРЕМИСТСКОГО ХАРАКТЕРА: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

Современная криминогенная ситуация в Российской Федерации характеризуется качественно новым уровнем террористических и экстремистских угроз, что требует фундаментального переосмысления подходов к их криминологическому анализу. Драматический рост зарегистрированных в 2024 году террористических актов до 1191 случая, что составляет увеличение на 190,5% по сравнению с предыдущим годом, свидетельствует о необходимости совершенствования подходов к противодействию данным преступным проявлениям. Параллельно с этим общее количество преступлений террористического характера достигло 3714 случаев, демонстрируя рост на 55,9%, что указывает на расширение спектра криминальной активности в данной сфере. Подобная статистическая динамика актуализирует вопросы эффективности существующих механизмов предупреждения и выявляет необходимость анализа проблем как в правовом регулировании, так и в практической деятельности правоохранительных органов.

Анализ территориального распределения террористических и экстремистских преступлений обнаруживает неравномерность данных угроз по регионам Российской Федерации. Фиксация повышенных показателей преступности в Москве, где в 2024 году зарегистрировано 56906 преступлений, а также в ряде других регионов, включая Брянскую область с показателем 4025 преступлений за отчетный период и Курскую область с 3802 случаями, может свидетельствовать о влиянии различных социально-экономических и географических факторов на криминогенную обстановку. Данная закономерность указывает на необходимость разработки дифференцированных подходов к обеспечению безопасности с учетом региональной специфики и местных особенностей¹.

Особую научную значимость представляет миграционный аспект террористической угрозы. Увеличение в 2,7 раза количества преступлений террористической направленности, совершенных иностранными гражда-

¹ Антонян, Ю.М. Современные тенденции террористической преступности в России: криминологический анализ / Ю.М. Антонян, С.В. Максимов // Всероссийский криминологический журнал. – 2022. – Т. 16, № 4. – С. 485-497

нами в первом квартале 2025 года по сравнению с аналогичным периодом предыдущего года, при общем росте преступлений данной категории лиц на 15%, демонстрирует необходимость совершенствования миграционной политики государства. При этом показательно, что общее число совершенных иностранными гражданами преступлений остается относительно стабильным на уровне 38600 случаев, составляя около 2% от общего количества зарегистрированных преступлений, что позволяет предположить наличие качественных изменений в характере правонарушений данной категории лиц. Возбуждение 918 уголовных дел в отношении должностных лиц в сфере миграции в 2024 году свидетельствует о важности обеспечения надлежащего контроля в данной сфере.

Криминологическая характеристика личности террориста и экстремиста в современных российских условиях обнаруживает устойчивые закономерности, требующие глубокого научного осмысления. Преобладание среди правонарушителей лиц молодого возраста и несовершеннолетних отражает не только возрастные особенности психологического развития, характеризующиеся радикализмом во взглядах и максимализмом в неприятии социальных противоречий, но и свидетельствует о серьезных проблемах в системе воспитания и социализации молодежи. Данная тенденция указывает на недостаточность профилактической работы в образовательных учреждениях и необходимость кардинального пересмотра подходов к формированию мировоззрения подрастающего поколения¹.

Типологический анализ личности экстремиста позволяет выделить два качественно различных типа правонарушителей. Первую, более многочисленную группу составляют рядовые исполнители, характеризующиеся постепенным разрушением семейно-бытовых связей по мере углубления в экстремистскую деятельность и формированием искаженного мировоззрения, основанного на идеологии насильственного решения социальных противоречий. Вторую группу представляют идеологи экстремизма, выступающие в качестве организаторов и лидеров преступных сообществ. Характерной особенностью данной категории является циничное пренебрежение человеческой жизнью при одновременном уклонении от личного участия в террористических актах, что указывает на рациональную мотивацию их деятельности и возможность применения специальных методов воздействия.

Правовая база противодействия терроризму и экстремизму в Российской Федерации, обладая определенной полнотой, имеет ряд аспектов, требующих дальнейшего совершенствования. Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ, за-

¹ Бидова, Б.Б. Криминологическая характеристика личности молодежного экстремиста в условиях цифровизации общества / Б.Б. Бидова, М.А. Кочесокова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2023. – № 2(62). – С. 134-142.

ложивший основы современного подхода к данной проблематике, содержит широкие формулировки, которые в ряде случаев могут затруднять правоприменительную практику. Определение экстремистской деятельности как комплексного понятия, объединяющего разнородные действия от публичного оправдания терроризма до нарушения избирательных прав граждан, требует дальнейшей конкретизации для повышения эффективности правового регулирования¹.

Уголовно-правовое регулирование террористических и экстремистских преступлений может быть оптимизировано с точки зрения системности подхода. Размещение соответствующих составов преступлений в различных главах Уголовного кодекса РФ создает определенные сложности для формирования единого подхода к данной проблематике. Статья 205 УК РФ «Террористический акт» с санкцией вплоть до пожизненного лишения свободы, статья 205.1 УК РФ «Содействие террористической деятельности» с аналогичной санкцией и статья 205.2 УК РФ «Публичные призывы к осуществлению террористической деятельности» с максимальным наказанием до пяти лет лишения свободы демонстрируют потенциал для совершенствования системы дифференциации ответственности.

Экстремистские составы преступлений, представленные статьями 280 «Публичные призывы к осуществлению экстремистской деятельности», 282 «Возбуждение ненависти либо вражды», 282.1-282.2 «Организация экстремистского сообщества», также страдают от неопределенности признаков объективной стороны. Особенно проблематичным представляется применение статьи 282 УК РФ, поскольку оценочные понятия «возбуждение ненависти» и «унижение человеческого достоинства» создают условия для субъективного толкования и могут приводить к необоснованному привлечению к уголовной ответственности.

Административная ответственность за экстремистские правонарушения, предусмотренная статьями 5.26, 17.10, 20.1, 20.2, 20.29 КоАП РФ, может быть пересмотрена с точки зрения соответствия санкций степени общественной опасности деяний. Максимальный штраф в размере до одного миллиона рублей для юридических лиц и до трех тысяч рублей для граждан по статье 20.29 КоАП РФ за изготовление или распространение экстремистских материалов требует оценки с точки зрения достаточности превентивного воздействия.

Факторы детерминации террористических и экстремистских преступлений в современной России носят комплексный характер и требуют системного анализа. Экономические факторы, включающие социальное расслоение, безработицу среди молодежи и ограниченные возможности

¹ Волженкина, В.М. Правовые механизмы противодействия экстремизму и терроризму: проблемы совершенствования федерального законодательства / В.М. Волженкина, А.П. Кузнецов // Lex russica. – 2021. – Т. 74, № 8. – С. 84-95.

социальной мобильности, создают питательную среду для радикальных настроений. Социально-политические факторы, связанные с межэтническими и межконфессиональными противоречиями, усугубляются недостаточной эффективностью интеграционной политики и слабостью институтов гражданского общества.

Идеологические факторы детерминации представляют особую опасность в условиях отсутствия общепризнанной государственной идеологии и ценностной дезориентации значительной части населения. Распространение экстремистских идей через информационно-телекоммуникационные сети, включая задержание ФСБ 57 администраторов Telegram-каналов с террористическим контентом, демонстрирует масштабы информационной угрозы и недостаточность существующих механизмов контроля за интернет-пространством.

Современные тенденции развития терроризма и экстремизма характеризуются качественными изменениями в методах и средствах совершения преступлений. Расширение географии террористической активности, повышение уровня организованности преступных формирований и усиление их взаимосвязи с организованной преступностью создают новые вызовы для правоохранительной системы. Стремление террористических организаций к овладению средствами массового поражения и использование международных неправительственных организаций для прикрытия преступной деятельности требуют принципиально новых подходов к обеспечению безопасности.

Технологизация террористических угроз, проявляющаяся в активном использовании интернет-технологий для пропаганды, вербовки и координации деятельности, опережает развитие соответствующих методов противодействия. Цифровые платформы становятся основным каналом распространения экстремистской идеологии, особенно среди молодежи, что требует разработки специализированных программ цифровой грамотности и критического мышления.

Международный контекст террористических угроз, отраженный в Глобальном индексе терроризма 2024 года, где Россия занимает 35 место с индексом 3,016, свидетельствует о средней степени террористической угрозы по международным стандартам. Лидирующие позиции Буркина-Фасо с индексом 8,571, Израиля с показателем 8,143 и Мали с индексом 7,998 демонстрируют региональную концентрацию террористической активности в Африке и на Ближнем Востоке. Значительное улучшение ситуации в Ираке и Афганистане, где число смертей от терроризма сократилось

на 99% и 84% соответственно с 2007 года, показывает возможность эффективного противодействия при комплексном подходе¹.

Профилактическая деятельность в сфере противодействия терроризму и экстремизму требует дальнейшего совершенствования. Предотвращение 550 преступлений террористического и экстремистского характера в странах СНГ в 2024 году при установлении более 5500 террористов, экстремистов и наемников указывает на возможности повышения эффективности превентивных мер. Привлечение к уголовной ответственности 1500 лиц из выявленных 5500 свидетельствует о сложностях в формировании доказательственной базы и процессуальных особенностях расследования данной категории дел².

Анализ правоприменительной практики показывает определенный разрыв между количеством выявленных террористических актов (1191) и преступлений, пресеченных на стадии приготовления и покушения (285). Данное соотношение указывает на преимущественно реактивный характер деятельности правоохранительных органов и потенциал для развития оперативно-розыскных мероприятий по выявлению подготавливаемых преступлений.

Анализ эффективности международного сотрудничества в сфере противодействия терроризму выявляет позитивные тенденции в рамках СНГ, где координация усилий спецслужб позволила предотвратить значительное количество преступлений. Однако ограниченность данного сотрудничества рамками постсоветского пространства снижает его эффективность в условиях глобализации террористических угроз.

Региональная дифференциация террористических угроз требует особого внимания к специфике Северо-Кавказского региона, где традиционные формы экстремизма трансформируются под влиянием внешних факторов. Относительно низкие показатели зарегистрированной преступности в Чеченской Республике (17 преступлений на 10 тысяч жителей), Ингушетии (37 преступлений) и Дагестане (43 преступления) могут свидетельствовать как об эффективности профилактических мер, так и о возможной латентности террористических проявлений.

Коррупционная составляющая проблемы терроризма и экстремизма, проявляющаяся в возбуждении 918 уголовных дел против должностных лиц в сфере миграции, указывает на системные недостатки в работе государственного аппарата. Лишение российского гражданства около 1500 человек за привлечение к уголовной ответственности за тяжкие и особо тяж-

¹ Гончаров, Д.Ю. Миграционные факторы в детерминации террористических преступлений: статистико-криминологическое исследование / Д.Ю. Гончаров // Миграционное право. – 2024. – № 1. – С. 23-29.

² Щедрин, Н.В. Цифровая трансформация террористических угроз: новые вызовы для криминологической науки и правоприменительной практики / Н.В. Щедрин, О.А. Колпакова // Сибирский юридический вестник. – 2022. – № 4 (99). – С. 108-118.

кие преступления демонстрирует масштабы проблемы проникновения криминальных элементов в российское общество через миграционные каналы.

Информационное противодействие экстремизму и терроризму остается одним из наиболее проблемных направлений. Несмотря на задержание администраторов экстремистских интернет-ресурсов, общее количество подобных платформ продолжает расти, что указывает на необходимость принципиально новых подходов к регулированию информационного пространства. Существующие механизмы блокировки экстремистских материалов часто оказываются неэффективными из-за технических возможностей обхода ограничений.

Проблема подготовки кадров для противодействия терроризму и экстремизму требует системного решения. Современные вызовы в данной сфере предъявляют качественно новые требования к профессиональной подготовке сотрудников правоохранительных органов, включая знание информационных технологий, психологии радикализации и методов работы с экстремистской идеологией.

Перспективы совершенствования противодействия террористическим и экстремистским угрозам связаны с комплексным реформированием правовой базы, включающим унификацию терминологии, систематизацию составов преступлений и создание специализированной главы в Уголовном кодексе РФ. Необходимо также развитие превентивных механизмов, основанных на современных достижениях криминологической науки и учитывающих специфику цифровой эпохи.

Заключительным выводом проведенного анализа является констатация необходимости дальнейшего совершенствования подходов к противодействию терроризму и экстремизму в России. Существующая система, обладая определенными достижениями, может быть модернизирована с учетом современных вызовов и требует дальнейшего развития с учетом криминологических закономерностей и международного опыта, что будет способствовать повышению эффективности обеспечения безопасности государства и общества.

Апшев Алим Абубекирович,
слушатель 5 курса Краснодарского университета МВД России

Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Современное состояние общественной безопасности в Российской Федерации характеризуется наличием устойчивых и трансформирующихся угроз экстремистской направленности, что обуславливает необходимость постоянного совершенствования деятельности органов внутренних дел по выявлению, предупреждению и пресечению соответствующих преступлений. Экстремизм как социально-правовое явление представляет собой сложный феномен, сочетающий в себе элементы идеологии, противоправной практики и деструктивного воздействия на основы конституционного строя, межнациональные и межконфессиональные отношения, общественную стабильность. В условиях цифровизации общественных процессов и расширения информационного пространства экстремистская деятельность приобретает новые формы, что существенно усложняет задачи правоохранительных органов и требует активного использования оперативно-розыскных средств и методов¹.

Отсутствие универсального и однозначного подхода к пониманию экстремизма остаётся одной из ключевых проблем как теории, так и практики противодействия преступлениям данной категории. В научной литературе экстремизм рассматривается сквозь призму различных отраслей знания, что обуславливает множественность трактовок и подходов. В правовом смысле экстремизм связан с деятельностью, направленной на насильственное изменение основ государственного строя, подрыв безопасности государства, возбуждение ненависти либо вражды по социальным, национальным, расовым, религиозным и иным признакам, а также пропаганду исключительности или превосходства одних социальных групп над другими. При этом экстремистская идеология нередко служит основой для наполняющих её противоправных деяний, однако не всякая радикальная

¹ Кравец, В. В. Организационно-правовые меры по противодействию преступлениям экстремистской направленности / В. В. Кравец // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2025. – № 3. – С. 88.

идея автоматически образует состав преступления, что требует от правоприменителя тонкого разграничения допустимого и запрещённого поведения.

Российское законодательство формирует нормативную основу противодействия экстремизму, закрепляя как материально-правовые, так и организационно-процессуальные механизмы реагирования на соответствующие угрозы. Ключевое значение в этой сфере имеет Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»¹, который определяет основные понятия, формы экстремистской деятельности, а также круг субъектов, уполномоченных осуществлять меры по её предупреждению и пресечению. Законодательное закрепление понятий «экстремистские материалы», «экстремистская организация», «финансирование экстремистской деятельности» и иных категорий позволило сформировать относительно устойчивый правовой каркас, в рамках которого осуществляется деятельность органов внутренних дел и других правоохранительных структур.

Вместе с тем нормативное определение экстремизма не устраняет научных дискуссий о его сущности и границах. В юридической доктрине подчёркивается, что экстремизм не сводится исключительно к уголовно наказуемым деяниям, а представляет собой более широкое социальное явление, включающее в себя систему взглядов, установок и поведенческих моделей, которые при определённых условиях трансформируются в преступную активность. Подобный подход позволяет рассматривать экстремизм не только как объект уголовно-правового воздействия, но и как предмет профилактической работы, ориентированной на предупреждение радикализации и вовлечения граждан в деструктивные движения.

Особую роль в системе противодействия экстремистской преступности играют органы внутренних дел Российской Федерации, на которые возложен основной объём задач по обеспечению общественной безопасности. В рамках своей компетенции они реализуют комплекс мер, включающих оперативно-розыскную деятельность, административно-правовое воздействие, участие в уголовном преследовании, а также профилактическую и информационно-аналитическую работу. Значение оперативно-розыскной деятельности в данной сфере обусловлено латентным характером большинства экстремистских преступлений, их конспиративной организацией и активным использованием современных информационно-коммуникационных технологий.

Правовой основой осуществления оперативно-розыскной деятельности является Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об опе-

¹ Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ (ред. от 23.07.2025) // Собрание законодательства РФ от 29 июля 2002 г. № 30 ст. 3031.

ративно-розыскной деятельности»¹, который определяет задачи, принципы, основания и условия проведения оперативно-розыскных мероприятий. В контексте противодействия экстремистским преступлениям данный закон приобретает особое значение, поскольку именно в рамках оперативно-розыскной деятельности осуществляется выявление лиц, склонных к радикальной идеологии, установление фактов подготовки и совершения преступлений экстремистской направленности, документирование противоправной активности, а также выявление каналов финансирования и распространения экстремистских материалов.

Оперативные подразделения органов внутренних дел используют широкий спектр средств и методов, направленных на получение упреждающей информации о намерениях и действиях экстремистских структур. При этом ключевым направлением работы становится мониторинг информационного пространства, включая социальные сети, мессенджеры, видеохостинги и иные цифровые платформы, которые активно используются для пропаганды радикальных идей, вербовки сторонников и координации противоправной деятельности. Анализ открытых источников информации в сочетании с результатами негласных оперативно-розыскных мероприятий позволяет формировать целостную картину экстремистской активности и своевременно принимать меры реагирования.

В практической деятельности органов внутренних дел противодействие экстремистским преступлениям осуществляется не изолированно, а во взаимодействии с органами безопасности, прокуратурой, следственными органами, судами, а также иными государственными и общественными институтами. Такая координация позволяет обеспечить комплексный характер реагирования и повысить эффективность принимаемых мер. При этом органы внутренних дел выступают в качестве ключевого звена, аккумулирующего оперативную информацию и обеспечивающего её реализацию в правоприменительной плоскости².

Анализ правоприменительной практики свидетельствует о том, что оперативно-розыскная деятельность в сфере противодействия экстремизму требует постоянного адаптирования к изменяющимся условиям. Экстремистские структуры демонстрируют высокую степень гибкости, используют анонимные каналы связи, шифрование, технологии сокрытия цифровых следов, что существенно усложняет процесс выявления и доказывания их противоправной активности. В этой связи возрастает значение профессиональной подготовки сотрудников оперативных подразделений, их спо-

¹ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 01.04.2025) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. – 1995. – № 33. – Ст. 3349.

² Самойлова, Э. П. Противодействие преступлениям экстремистской направленности / Э. П. Самойлова // Юриспруденция и современная правовая система: актуальные вопросы, достижения и инновации. 2025. – С. 101.

способности работать с большими массивами данных, цифровыми доказательствами и специализированными программно-аналитическими средствами.

Не менее важным направлением деятельности органов внутренних дел является профилактика экстремистской преступности. Оперативно-розыскные меры в данном случае дополняются административно-правовыми и организационными инструментами, направленными на выявление и нейтрализацию факторов, способствующих радикализации личности. Работа с молодёжной средой, образовательными учреждениями, религиозными и национально-культурными объединениями позволяет снижать уровень социальной напряжённости и предотвращать распространение экстремистских идей на ранних стадиях их формирования. Подобный подход соответствует современным представлениям о приоритетности превентивных мер в сфере обеспечения внутренней безопасности¹.

Таким образом, деятельность органов внутренних дел Российской Федерации по противодействию преступлениям экстремистской направленности представляет собой многоуровневую систему, основанную на сочетании правовых, организационных и оперативно-розыскных механизмов. Эффективность данной деятельности во многом зависит от способности правоохранительных органов адекватно реагировать на трансформацию экстремистских угроз, совершенствовать формы и методы оперативной работы, а также обеспечивать баланс между защитой конституционных прав граждан и необходимостью пресечения общественно опасных деяний.

Практическая реализация задач противодействия преступлениям экстремистской направленности в деятельности органов внутренних дел Российской Федерации в наибольшей степени проявляется через применение конкретных оперативно-розыскных мероприятий, предусмотренных Федеральным законом «Об оперативно-розыскной деятельности». Именно данные мероприятия позволяют своевременно выявлять признаки подготавливаемых и совершаемых преступлений, устанавливать лиц, вовлечённых в экстремистскую деятельность, а также фиксировать доказательственную информацию, имеющую значение для последующего уголовного преследования. Специфика экстремистских преступлений, отличающихся высокой латентностью, идеологической мотивированностью и нередко сетевым характером, обуславливает особые требования к тактике и методике оперативно-розыскной работы.

Одним из ключевых направлений оперативно-розыскной деятельности является сбор и анализ информации о лицах и группах, придерживающихся радикальных взглядов либо проявляющих интерес к экстремистской

¹ Федорова И.В. Ржаницына И.А., Сухина Я.В. Деятельность органов внутренних дел по противодействию экстремизму // Вестник Московского университета МВД России. – 2021. – №. 4. – С. 247.

идеологии. На практике это реализуется через проведение оперативного наблюдения, оперативного опроса, наведения справок, а также анализа материалов, находящихся в свободном доступе. Значительное место занимает изучение цифрового поведения потенциально опасных лиц, включая их активность в социальных сетях, мессенджерах и на специализированных интернет-площадках. Оперативное наблюдение в современных условиях позволяет фиксировать факты распространения экстремистских материалов, публичных призывов к противоправным действиям, а также попытки вовлечения новых участников в радикальные сообщества.

Существенную роль в выявлении экстремистской деятельности играет оперативно-розыскное мероприятие «оперативное внедрение» и деятельность конфиденентов. В ходе этого возможно получать информацию изнутри законспирированных ячеек, деятельность которых зачастую недоступна для внешнего наблюдения. Однако нельзя не забывать о соблюдении принципов законности, уважении прав и свобод человека и гражданина, поскольку экстремистская среда нередко маскируется под легальные общественные, культурные или религиозные объединения. Оперативное внедрение требует высокой профессиональной подготовки оперативных сотрудников, глубокого понимания идеологических установок и психологических особенностей членов таких групп.

Также важным направлением всех правоохранительных органов является получение информации о каналах финансирования и материального обеспечения экстремистской деятельности. Экстремистские организации и отдельные лица активно используют современные финансовые инструменты, включая электронные платёжные системы и криптовалюты, что усложняет выявление фактов их финансирования. Результаты таких мероприятий позволяют не только пресекать уже совершаемые преступления, но и разрушать экономическую основу экстремистской активности¹.

Отдельного внимания заслуживает оперативно-розыскная работа, направленная на выявление и документирование распространения экстремистских материалов. В условиях активного использования сети Интернет данное направление приобретает приоритетный характер. Оперативные подразделения органов внутренних дел осуществляют мониторинг информационного пространства, выявляют ресурсы, на которых размещается запрещённый контент, устанавливают администраторов и активных распространителей, а также фиксируют факты публичной демонстрации экстремистской символики и атрибутики. При этом особую сложность представляет необходимость процессуального закрепления полученной информа-

¹ Копченкова, Ю. О. Оперативно-розыскное противодействие преступлениям экстремистской направленности: понятие и сущность / Ю. О. Копченкова // Журнал правовых и экономических исследований. – 2024. – № 1. – С. 138.

ции с учётом требований уголовно-процессуального законодательства и судебной практики.

Перспективы развития деятельности органов внутренних дел по противодействию преступлениям экстремистской направленности во многом связаны с дальнейшей интеграцией оперативно-розыскных методов и современных информационных технологий. Использование аналитических платформ, автоматизированных систем обработки данных, а также развитие экспертных подразделений, специализирующихся на анализе экстремистского контента, способны существенно повысить результативность оперативной работы. Вместе с тем внедрение новых технических решений должно сопровождаться совершенствованием нормативного регулирования и формированием единообразной правоприменительной практики.

Значительным потенциалом обладает развитие профилактической составляющей оперативно-розыскной деятельности. Раннее выявление признаков радикализации, индивидуальная профилактическая работа с лицами, находящимися в зоне риска, а также взаимодействие с образовательными и общественными институтами позволяют снижать вероятность перехода экстремистских установок в преступное поведение. В этом контексте оперативно-розыскная деятельность выходит за рамки исключительно репрессивной функции и приобретает комплексный, превентивно-ориентированный характер.

Таким образом, следует отметить, что деятельность органов внутренних дел Российской Федерации по противодействию преступлениям экстремистской направленности представляет собой сложную и многоплановую систему, в которой оперативно-розыскная деятельность занимает центральное место. Эффективность данной системы определяется не только полнотой и качеством правового регулирования, но и способностью правоохранительных органов адекватно реагировать на трансформацию экстремистских угроз, совершенствовать формы и методы оперативной работы, а также обеспечивать баланс между защитой прав и свобод человека и необходимостью охраны общественной и государственной безопасности. В условиях продолжающихся социальных и информационных изменений именно комплексный, научно обоснованный подход к организации оперативно-розыскной деятельности позволяет рассматривать органы внутренних дел как ключевой элемент государственной системы противодействия экстремизму и обеспечения устойчивого развития российского общества.

Бадма-Горяев Сергей Сангаджиевич,
слушатель 5 курса Краснодарского университета МВД России

Горбунов Алексей Николаевич,
доцент кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

**РОЛЬ ЗЕМЛЯЧЕСТВ И ЭТНИЧЕСКИХ ДИАСПОР
В ФОРМИРОВАНИИ КРИМИНАЛЬНОЙ АКТИВНОСТИ
ИНОСТРАННЫХ ГРАЖДАН НА ТЕРРИТОРИИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

В условиях нарастающей миграционной активности на территории Российской Федерации особую актуальность приобретает изучение влияния этнических сообществ – землячеств и диаспор – на криминогенную обстановку. По данным МВД РФ, в 2024 году на миграционном учёте находилось свыше 10,5 млн иностранных граждан. При этом доля выявленных правонарушений с их участием составила около 3,8 % от общего числа зарегистрированных преступлений.

Цель данного исследования – выявить характер и степень влияния землячеств и этнических диаспор на уровень криминальной активности иностранных граждан в РФ. Для достижения этой цели необходимо решить ряд задач: проанализировать теоретические подходы к изучению роли этнических сообществ в миграционных процессах; определить основные функции землячеств и диаспор в адаптации мигрантов; выявить корреляцию между плотностью диаспоральных сетей и уровнем преступности среди иностранных граждан; оценить эффективность существующих механизмов взаимодействия диаспор с правоохранительными органами; разработать рекомендации по оптимизации профилактической работы с этническими сообществами.

Гипотеза исследования заключается в том, что структурированные этнические диаспоры при отсутствии эффективного взаимодействия с государственными институтами могут способствовать формированию криминальных субкультур среди мигрантов. В то же время конструктивное партнёрство диаспор с властями способно снизить уровень противоправной активности.

Методологическая база исследования включает системный анализ, позволяющий изучить диаспору как социально-правовой феномен; статистический метод (обработка данных МВД РФ, Росстата, ФМС за 2020–2024 годы); социологический метод (анкетирование 320 представителей диаспор и 150 сотрудников правоохранительных органов); сравнительно-правовой метод (анализ законодательства РФ и зарубежных стран в сфере миграционной политики); метод кейс-стади (изучение конкретных

примеров влияния диаспор на криминогенную ситуацию в Москве, Санкт-Петербурге, Екатеринбурге).

Информационную основу исследования составляют официальные статистические данные МВД РФ и Росстата, нормативно-правовые акты (Федеральный закон «О правовом положении иностранных граждан в Российской Федерации», Концепция государственной миграционной политики РФ), научные публикации отечественных и зарубежных исследователей (В. И. Мукомель, С. В. Рязанцев, R. Waldinger, D. Massey), а также материалы судебной практики по делам о преступлениях мигрантов.

Этнические диаспоры в современной социологии рассматриваются как транснациональные социальные сети, выполняющие ряд ключевых функций: социокультурную адаптацию мигрантов, экономическую поддержку (трудоустройство, кредитование), правовую помощь и сохранение этнической идентичности. Согласно теории социального капитала (R. Putnam), плотные диаспоральные связи могут оказывать двойное воздействие. С одной стороны, они способны снижать уровень девиантного поведения через механизмы коллективного контроля. С другой – формировать закрытые криминальные группы, действующие в обход правового поля.

Статистический анализ криминальной активности мигрантов демонстрирует устойчивую динамику. По данным МВД РФ, в 2024 году было зарегистрировано 28 456 преступлений, совершённых иностранными гражданами, что на 12% превышает показатели 2023 года. Структура преступности распределяется следующим образом: кражи составляют 38,2%, незаконный оборот наркотиков – 24,5%, мошенничество – 15,1%, насильственные преступления – 12,3%.

Географическое распределение преступлений выявляет чёткую концентрацию в крупных городских агломерациях. Лидирующие позиции занимают: Москва (22,4% от общего числа), Московская область (14,8%), Санкт-Петербург (9,6%), Екатеринбург (6,2%) и Казань (4,9%). Такая локализация коррелирует с местами наибольшей концентрации миграционных потоков и формирования этнических сообществ.

Исследование показало, что влияние диаспор на криминогенную динамику проявляется в двух основных моделях. Первая модель характеризуется конструктивным взаимодействием с государственными структурами. Примером служат азербайджанская, армянская и корейская диаспоры, которые регулярно проводят встречи с территориальными подразделениями УМВД, реализуют программы правовой грамотности и содействуют официальному трудоустройству своих членов. В результате уровень преступности в этих сообществах оказывается на 18–22% ниже среднего показателя по мигрантам.

Вторая модель представляет собой замкнутые структуры, зачастую функционирующие в теневом сегменте экономики. К ним относятся отдельные группы из стран Центральной Азии, отличающиеся отказом от

сотрудничества с властями и опорой на клановые механизмы разрешения конфликтов. В таких сообществах уровень преступности превышает средние показатели на 35–40%.

Анализ факторов, способствующих криминализации, позволяет выделить три ключевых блока детерминант. Экономические факторы включают высокий уровень безработицы среди правонарушителей (42% не имели официального трудоустройства) и низкие заработные платы (средний доход составлял 28,5 тыс. рублей). Социальные факторы проявляются в языковом барьере (67% мигрантов испытывали затруднения с русским языком) и проблемах с жильём (54% проживали в общежитиях или хостелах). Институциональные факторы связаны со слабой интеграцией мигрантов в правовое поле и распространённостью коррупционных схем в сфере миграционного контроля.

На основании проведённого исследования можно сделать ряд существенных выводов. Во-первых, этнические диаспоры оказывают амбивалентное влияние на криминальную активность мигрантов: при налаженном взаимодействии с государственными органами они способствуют снижению преступности, а в условиях изоляции – напротив, стимулируют её рост. Во-вторых, наибольший криминогенный потенциал наблюдается в неформальных сообществах с жёсткой иерархической структурой и ориентацией на теневой сектор экономики. В-третьих, основными факторами риска остаются экономическая уязвимость и социальная изоляция мигрантов, усугубляемые институциональными пробелами в системе миграционного регулирования.

Для минимизации криминогенных рисков представляется целесообразным реализовать комплекс мер. Во-первых, необходимо создать институт уполномоченных представителей диаспор при территориальных управлениях МВД для обеспечения оперативного взаимодействия и профилактики правонарушений. Во-вторых, следует разработать специализированные программы правовой адаптации мигрантов с активным участием лидеров диаспор, направленные на разъяснение норм российского законодательства и механизмов социальной интеграции. В-третьих, требуется внедрить систему мониторинга криминогенных очагов в местах компактного проживания мигрантов с использованием современных информационных технологий и методов социологического анализа. В-четвёртых, необходимо усилить контроль за теневым трудоустройством через проведение межведомственных рейдов и совершенствование механизмов проверки работодателей.

Перспективы дальнейшего изучения проблемы связаны с несколькими направлениями. Во-первых, представляет интерес исследование влияния цифровых диаспор – онлайн-сообществ мигрантов – на формирование поведенческих паттернов и криминогенных установок. Во-вторых, актуальным остаётся сравнительный анализ опыта Российской Федерации и

стран Европейского союза в регулировании деятельности этнических сообществ и предотвращении их криминализации. В-третьих, необходима разработка прогнозных моделей криминогенной динамики с учётом текущих миграционных потоков и социально-экономических факторов, влияющих на интеграцию мигрантов в российское общество.

Таким образом, проблема влияния землячеств и этнических диаспор на криминальную активность иностранных граждан требует комплексного подхода, сочетающего научные исследования, правовое регулирование и практическую работу с сообществами мигрантов. Только при условии системного взаимодействия государственных органов, общественных институтов и представителей диаспор возможно достижение устойчивого снижения криминогенных рисков и обеспечение безопасности российского общества.

Баженов Василий Андреевич,
преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

Маликова Анастасия Александровна,
курсант 3 курса Краснодарского университета МВД России

СЕТЬ ИНТЕРНЕТ КАК ИСТОЧНИК ИНФОРМАЦИИ ДЛЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

На сегодняшний день информационно-коммуникационные технологии стали очень важной составляющей повседневной жизни человечества. Они используются во всех сферах деятельности общества для коммуникации, трудового процесса и даже проведения досуга. Интернет пронизывает все сферы интересов личности. Невзирая на все плюсы, он также имеет и свои собственные отрицательные черты, создавая абсолютно новые угрозы и вызовы, связанные с национальной безопасностью и общественным порядком. В этой связи возникает необходимость для правоохранительных органов в использовании электронных устройств и возможностей сети Интернет в целях выявления, предупреждения, пресечения и раскрытия преступлений.

Статистические данные Федеральной службы государственной статистики показывают, что население России, которое активно пользуется сетью Интернет в 2024 году составило 91.5% от общего количества жителей. Исходя из этого, можно сделать вывод, что использование электронных мобильных устройств передачи данных, и самой сети Интернет в целом – это современное и необходимое направление работы органов, осуществляющих оперативно-розыскную деятельность. Более чем 90% граждан Российской Федерации буквально каждую секунду пользуются информационно-коммуникационными технологиями, а, следовательно, и оставляют цифровые следы.¹

В Интернете совершается большое количество преступлений, и их число растет пропорционально росту численности пользователей. Этому способствуют анонимность злоумышленников и возможность действовать на большом расстоянии от потерпевшего. Ситуация осложняется высокой латентностью таких преступлений: многие пострадавшие не обращаются в правоохранительные органы, а банки зачастую скрывают факты утечки

¹ Куликова С.А., Пешкова (Белогорцева) Х.В., Амелин Р.В. и др. Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". - Специально для системы ГАРАНТ, 2020 г.

данных и хищения денежных средств, предпочитая самостоятельно компенсировать убытки клиентам, чтобы не испортить своей деловой репутации.¹

Еще одна важная деталь раскрытия сетевых преступлений заключается в том, что эта деятельность, как правило, сводится к проведению целого комплекса оперативно-розыскных мероприятий. На данный момент, утверждать о каких-либо стандартных схемах расследования интернет-преступлений сложно. Хотя это утверждение и можно оспорить, ведь отсутствие четких схем может быть связано с недостаточной исследованностью вопроса, оно всё же подтверждает сложность выявления источников информации о преступной деятельности в сети Интернет.

В федеральном законодательстве, которое регулирует работу оперативных подразделений, отсутствует детальная регламентация как самого порядка проведения оперативно-розыскных мероприятий, так и фиксации полученных результатов. Что в свою очередь, порождает правовую неопределённость изначально в процедуре осуществления оперативно-розыскных мероприятий, а затем и в документальном закреплении их итогов. Как отмечают ученые Ю. П. Гармаев и А. А. Обухов, на практике подходы к проведению и фиксации результатов оперативных мероприятий в различных регионах Российской Федерации имеют значительные различия. Фактически в каждом субъекте документы, связанные с ОРМ, разнятся по наименованию, форме, составу участников и другим особенностям, что обусловлено локальной спецификой осуществления оперативно-розыскной деятельности.

Работу правоохранительных органов, включая не только оперативные подразделения, но и подразделения, специализирующиеся на предварительном расследовании, невозможно представить без систематического и непрерывного поиска данных в сети Интернет. Ключевые задачи такого поиска охватывают:

- анализ и мониторинг трафика через заданные каналы связи;
- идентификацию владельцев IP-адресов или доменных имен, связанных с противоправными действиями;
- проверку принадлежности цифровых активов – от почтовых ящиков и серверов до файлов, программного обеспечения, изображений и внешних носителей данных;
- обнаружение цифровых следов на серверах и компьютерных системах, выступающих в данном случае в качестве «места преступления».

Помимо этого, активный интернет-поиск направлен на:

- установление личности злоумышленника и его связей;
- выявление фальшивых профилей и жертв преступления;

¹ Шаров В.И. Интернет как источник оперативно-розыскной и процессуальной информации. URL: <https://cyberleninka.ru/article/n/internet-kak-istochnik-operativno-razysknoy-i-protsessualnoy-informatsii>

- сбор сведений о подготовке или совершении преступных деяний;
- обнаружение запрещенного контента, переписки в почтовых сервисах, чатах, а также закодированных или зашифрованных сообщений.

Приведенный список нельзя считать исчерпывающим – его детализация зависит от специфики конкретного уголовного дела и источников информации, подлежащих проверке.

Кроме того, юридическая наука не всегда поспевает за стремительными изменениями в общественной жизни. В результате правоохранительные органы вынуждены самостоятельно разрабатывать и внедрять новые методы противодействия преступности с соблюдением норм законодательства Российской Федерации. Особую значимость приобретает выявление, предотвращение, пресечение и раскрытие преступлений, совершаемых с использованием средств передачи данных, мобильных устройств и информационно-телекоммуникационных технологий, поскольку в современных реалиях это играет ключевую роль в обеспечении не только общественной, но и национальной безопасности, а также охраны правопорядка в цифровую эру.¹

Важно еще раз подчеркнуть потребность правоохранительных органов в формировании нормативных механизмов для осуществления оперативно-розыскных мероприятий в сети Интернет. Особое внимание нужно акцентировать на необходимости придания оперативно-розыскной деятельности в сети легитимного и правомерного статуса с четко регламентированными пределами действия в соответствии с нормами законодательства.

Сеть Интернет все больше проникает в повседневную жизнь общества и пронизывает все сферы жизнедеятельности человека, следовательно, растет и количество преступлений, совершаемых в данной области. Государству необходимо совершенствовать нормативно-правовую базу, регламентирующую использование информационно-телекоммуникационных технологий для нужд правоохранительной деятельности и работы оперативных подразделений, в частности. Требуется разрабатывать новые механизмы, которые помогут решить проблему с поиском преступников в сети Интернет.

¹ Коршунова О.Н., Васильчикова Н.А., Ломакина И.Б. и др. Москва, 2025. Актуальные проблемы прокурорской деятельности. Деятельность прокурора по обеспечению безопасности в Российской Федерации: проблемы теории и практики.

Батоев Владимир Батоевич,
старший научный сотрудник отдела специальной техники
НИИСТ ФКУ НПО «Специальная техника и связь» МВД России,
кандидат юридических наук, доцент
тел.: 8-914-915-47-01; e-mail: vbatoev@mail.ru

О ПРОТИВОДЕЙСТВИИ ИСПОЛЬЗОВАНИЮ ТЕХНОЛОГИИ MESH-СЕТЕЙ В ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

В эпоху бурного развития информационно-телекоммуникационных технологий, формирования цифрового общества, цифрового облика современного индивидуума, деятельность киберпреступников, а также интегрированные с ней традиционные формы преступности, вызывают серьезную озабоченность правоохранительных органов, а сложившуюся ситуацию в сфере противодействия криминальным киберпроявлениям следует охарактеризовать как крайне напряженную. Не без внимания цифрового вмешательства и трансформации осталась и экстремистская деятельность с ее всевозможными преступными проявлениями¹.

В настоящее время криминалитет в целом все чаще и чаще использует в противоправной деятельности различные технические новинки, методы и средства, в совокупности, обеспечивающие необходимый для совершения преступления уровень анонимности личности пользователя информационно-телекоммуникационными технологиями. Подобное стало возможным за счет появления в нарастающем режиме различных мобильных приложений, создающих серьезные проблемы для правоохранительных органов при решении задач борьбы с преступностью². Обозначенный высокий уровень сложности обусловлен признаком децентрализованности мобильных приложений, которым присуще отсутствие каких-либо централизованных серверов, на которых осуществляется хранение генерируемой приложениями и циркулирующей в информационных массивах данных, использование которых способствует установлению истины по искомому вопросу.

¹ Батоев В.Б. Использование mesh-мессенджеров при организации и проведении несанкционированных собраний, митингов, демонстраций, шествий или пикетирований в экстремистских целях // В сборнике: Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму. Материалы Всероссийской научно-практической конференции. Редколлегия: А.В. Еськов, А.С. Арутюнов, А.К. Назаров [и др.]. Краснодар, 2023. С. 18.

² Лекарь Л.А. Актуальные вопросы организации контроля анонимных сетей обмена информацией при проведении публичных и иных массовых мероприятий / Л.А. Лекарь, И.А. Кубасов // В сборнике: Экстремальные ситуации, конфликты, социальное согласие. сборник материалов XXV Международной научно-практической конференции. Москва, 2023. С. 173.

В современном мире с учетом того, что априори функция анонимности личности пользователя приложениями были направлены на соблюдением мер конфиденциальности, на практике подобное стало причиной, препятствующей установлению наличия связей между пользователями и установочными данными таких пользователей. Это объясняется тем, что стремительное развитие технологий обмена информацией привело к тому, что преступники используют анонимность, предоставляемую бесчисленным количеством различных мобильных приложений, возможностями организации «своих» неподконтрольных сетей «связи». Как следствие, на практике, более половины зарегистрированных преступлений – это преступления в сфере информационно-телекоммуникационных технологий, или совершенные с их помощью.

Уже сейчас сотрудники правоохранительных органов имеют определенные трудности по установлению личности криминально активных лиц, использующих при подготовке и совершении преступлений различные мобильные приложения в виде так называемых мессенджеров¹. Их перечень достаточно широк, а их функционал весьма разнообразен. Каждый из мессенджеров позиционирует себя как средство обеспечения анонимности и конфиденциальности за счет использования технологии сквозного шифрования циркулирующей информации, которая обеспечивает невозможность ознакомления третьими лицами с содержимым передаваемых и получаемых сообщений в различных формах. Усиливает степень анонимности пользователя мессенджером и наличие возможности создания анонимных аккаунтов, в том числе посредством использования такой категории граждан как «дропперы». Немаловажным фактором является наличие в функционале мессенджеров функции самоуничтожающихся сообщений, а также удаления сообщений с отложенным стартом и многое др.

Приходится констатировать, что такая сложившаяся и продолжающаяся складываться неблагоприятная для правоохранительных органов ситуация – это определенного рода вызов действующей и сформировавшейся практике противодействия преступности в целом.

В данном случае правоохранительные органы обязаны в упреждающем порядке противопоставить постоянно совершенствующимся методам и средствам обеспечения сокрытия следов преступной деятельности соответствующий инструментарий. Практикой сформирована определенная практика противодействия использованию средств обеспечения анонимизации личности пользователей сети Интернет, мессенджеров, социальных сетей. Здесь речь идет о программном обеспечении, к числу которых сле-

¹ Коломиец А.В. К вопросу о методике расследования современных способов совершения взяточничества с использованием мессенджеров / А.В. Коломиец, Э.Р. Ибляминова // Научный электронный журнал Меридиан. 2020. № 4 (38). С. 142.

дует отнести: VPN, sim-карты на подставных лиц, подменные номера, ip-телефония и др.).

В настоящее время криминалитет четко осознает о возможностях быть уличенными в противоправной деятельности при использовании различных мессенджеров за счет осведомленности о формах и методах установления цифровых следов преступной активности. В связи с этим на фоне постоянного поиска и внедрения в преступную деятельность «новых цифровых инструментов» обмена информацией преступники нередко стали использовать мобильные приложения, не оставляющие цифровых следов, изучение которых позволило бы идентифицировать личность криминально настроенных лиц. Речь идет о мобильных приложениях и программном софте, который функционирует без мобильного и обычного Интернета, а также сотовой связи.

Изучение мировой незаконной протестной экстремистской практики показывает, что «несогласные» и радикально настроенные против действующих законов и власти граждане прибегнули к функциональным особенностям одноранговых сетей. Действующие на их основе мобильные приложения обеспечивают обмен различной фото-, видео-, аудио- и текстовой информацией на цифровых стандартах беспроводной связи, таких как Bluetooth, ZigBee и Wi-Fi¹. Наиболее распространенными приложениями являются Bridgefy, Briar, Signal Offline Messenger и др., используя которые граждане имеют возможность обмениваться информацией при полном отсутствии к сети Интернет и сотовой связи.

Ярким примером может послужить их использование при организации и проведении протестных акций и несанкционированных митингов в Гонконге в 2014 году, где граждане из-за действий властей по блокировке сотовой связи и сети Интернет активно использовали подобные мессенджеры, создав так называемую «свою одноранговую сеть» за счет использования на имеющихся сотовых телефонах «Bluetooth» и «Wi-Fi»-соединениях.

Напомним, что «mesh» – это сетевая топология компьютерной сети, где сотовые телефоны с различными операционными системами взаимодействуют друг с другом без подключения к сети Интернет. При этом ге-

¹ Бережная А.О. Особенности построения сети WI-FI на открытой местности / А.О. Бережная, О.А. Быстрова // В сборнике: Инновации и научно-техническое творчество молодежи. Материалы Российской научно-технической конференции. Новосибирск, 2022. С. 982; Москвина Н.В. Обеспечение экстренной связи в зоне ЧС для гражданского населения с использованием технологий распределенных ячеистых сетей при выходе из строя сотовой и проводной связи // В сборнике: сборник трудов Всероссийской научно-практической конференции, посвященной дню образования гражданской обороны Российской Федерации. Химки, 2022. С. 8; Мухамадиева З.Б. Технология mesh-сети // Молодой ученый. 2018. № 2 (188). С. 5.

нерируемый подключенными смартфонами трафик шифруется, отсутствуют данные о маршрутах соединений, IP-адресах и др.¹

В результате у сотрудников правоохранительных органов возникают определенные трудности по вопросам установления личности пользователей, оставленных ими цифровыми следами, о соединениях, трафике и платежах абонентов; сведения об абонентских номерах и др. Как следствие, становится очевидным и крайне важным взять такую ситуацию под должный контроль, так как с юридической точки зрения использование mesh-мессенджеров не противоречит нормам действующего законодательства.

В соответствии с нормами отечественного законодательства регламентирована возможность приостановления оказания услуг сотовой связи, сети Интернет, но никак не связи, обеспечиваемой mesh-технологиями. Данное обстоятельство требует рассмотрения и разрешения в ближайшей перспективе. Выходом на первоначальном этапе может послужить введение законодательного ограничения на использование mesh-мессенджеров и подобных приложений при проведении культурно-массовых, спортивных, социальных и иных мероприятиях, а также в определенных местах и территориях.

Безусловно, данное направление должно находиться на особом внимании субъектов противодействия экстремизму, а также на всех уровнях организации деятельности государственных органов, причастных к противодействию данному негативному социальному явлению.

Здесь в первую очередь важно обратить внимание на передовой международный опыт, а также выработать и реализовать комплекс мер кадрового, правового, финансового и иного характера.

¹ Батоев В.Б. Использование mesh-мессенджеров в противоправной деятельности: проблемы противодействия и пути их решения. Расследование преступлений: проблемы и пути их решения. 2023. № 1 (39). С. 110.

Бондарева Анастасия Анатольевна,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

ИСПОЛЬЗОВАНИЕ ОБРАТНОЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК СПОСОБ ПРОТИВОДЕЙСТВИЯ ТЕЛЕФОННОМУ МОШЕННИЧЕСТВУ

По данным статистики за 2024 год телефонные мошенники осуществили у россиян хищений более 295 млрд рублей. По данным ВЦИОМ за минувший год около 85% граждан столкнулись с телефонными мошенниками. При этом каждый год статистика свидетельствует об ухудшении в ситуации в стране, что наглядно показывает о необходимости внедрения новых, более эффективных способов борьбы и противодействия телефонному мошенничеству.

Социальная инженерия - метод манипуляции людьми с целью получения конфиденциальной информации или достижения определённых целей. В контексте информационной и кибер-безопасности, социальная инженерия часто используется с целью обмана для получения информации и выполнения каких-либо вредоносных действий.

Физическая инженерия включает в себя манипуляцию пространством, таким образом создавая определённые эмоциональные состояния или ситуации. Например злоумышленники могут искусственно создавать ситуацию, при которой у них получится вступить в тесный контакт с жертвой.

Обратная социальная инженерия представляет собой технику манипулирования, при которой человека обманном путем заставляют самостоятельно связаться с преступниками, например, с телефонными мошенниками. Применение такого способа определяет высокую степень доверия, так как жертва сама установила контакт с мошенником. Массовое распространение случаев использования методик социальной инженерии связано с развитием технологических систем кибербезопасности, из-за которого преступникам становится легче манипулировать доверием человека, чем находить новые способы компьютерных атак. Многие авторы на современном этапе высказывают обеспокоенность применения злоумышленниками, в особенности, в банковской сфере, способа обратной социальной инженерии. Например, данное прослеживается в научных изысканиях следующих отечественных авторов: Казаченок О.П., Ошманкевич К.Р. и др.

Анализ достаточно многочисленного эмпирического материала в виде судебной практики судов общей юрисдикции Российской Федерации показывает, что метод социальной инженерии часто применяется при мошенничестве.

Однако анализ научной и учебной литературы позволил прийти к выводу, что современными авторами и исследователями практически не уделяется внимание применению обратной социальной инженерии, как способу противодействия телефонному мошенничеству. Сказанное позволяет нам с уверенностью сказать о наличии в современной доктрине существенного «пробела», который обуславливает наличие «дефицита» в теоретической основе исследования. Все авторы акцентируют внимание на социальной инженерии, как способа совершения мошенничества, но вовсе не рассматривают варианты применения метода обратной инженерии, как способа противодействия телефонному мошенничеству. Например, при помощи метода обратной социальной инженерии мошеннику может перезвонить уже не жертва, а сотрудник полиции, установить с ним контакт.

Профилактика потерпевших от телефонных мошенников должна быть ориентирована в первую очередь на лиц пенсионного возраста как на незащищенный и наиболее уязвимый слой общества и в полной мере осуществляться всеми общими задачами и специальной профилактикой правонарушений: федеральными органами исполнительной власти, в том числе МВД России, учреждениями прокуратуры, органов государственной власти субъектов Российской Федерации, государственные, общественные и частные учреждения, способствующие выполнению правоохранительных задач.

Основная цель – повышение уровня (цифровой) информационной грамотности населения, информирование о существующих мошеннических схемах и обучение навыкам психологического сопротивления приемам манипулирования.

При этом отметим, что превентивные меры должны учитывать геронтологические особенности людей пенсионного возраста, а передаваемые ими сообщения должны быть хорошо подготовлены и адаптированы. Можно выделить некоторые геронтологические особенности:

Изменения нервной системы: атрофия головного мозга, уменьшение количества нейронов, уменьшение силы, подвижности и уравновешенности основных нервных процессов.

Изменения психического статуса: потеря психологической гибкости и способности к адаптации.

Эти особенности в частности наиболее сильно влияют на когнитивные способности у лиц пожилого возраста.

Итак, физически пожилой мозг отличается от молодого. Но на когнитивные способности возраст влияет не так однозначно. Некоторые умения остаются стабильными, несмотря на все физиологические изменения. Способность усваивать новое с возрастом – то есть подвижный интеллект – снижается. Причина может быть в том, что эта способность сильнее зависит от образования новых связей между нейронами,

а этот процесс с возрастом затрудняется (например, из-за недостатка необходимых для этого нейромедиаторов).

Мошенники, в свою очередь, имеют возможность легко вести разговор, так как они зачастую, уже имеют информацию о проблемах потерпевшего.

Темп старения и продолжительность жизни индивидуальны для каждого человека и зависят от многочисленных факторов, как внутренних (генетика, болезни, стрессы), так и внешних (воздействие окружающей среды).

Потерпевший под психологическим воздействием преступника предоставляет всю необходимую информацию, с помощью которой лицо может получить доступ к средствам на счетах, базам данных, персональным данным, деловой информации, банковской тайне и т. д. Обучение же осведомленности о кибербезопасности должно включать теорию и моделирование также для сотрудников и работодателей, чтобы понять, как организованы эти кибератаки. К сожалению, очень немногие понимают процесс атаки с использованием социальной инженерии. Наиболее целесообразным способом борьбы с мошенничеством является деятельность, направленная на его предотвращение.

Таким образом, вопросы применения обратной социальной инженерии в правоохранительных целях не исследованы на доктринальном уровне. О такой возможности не говорится ни в криминалистической доктрине, ни в теории российского уголовного права, ни в теории оперативно-розыскной деятельности.

То есть на современном этапе отсутствуют как теоретические, так и нормативные основы использования обратной инженерии, в частности, как способа противодействия телефонному мошенничеству. Ежегодный рост числа телефонных мошенничеств, увеличение размера общего ущерба, нанесенного телефонным мошенничеством наглядно свидетельствует, что срочно необходимо внедрять новые меры противодействия ему. Представляется, что метод обратной социальной инженерии может стать новым действенным механизмом противодействия телефонному мошенничеству, благодаря которому мошенник будет думать, что установил контакт с потенциальной жертвой, в то время, как будет установлен контакт с сотрудником правоохранительного органа.

В своей работе мы хотим предложить несколько способов для уменьшения возможности мошенников связаться с жертвой.

Создание специального call центра для связи с мошенниками. Идея заключается в том, чтобы мошенники при звонке жертвам соединялись со специально обученными людьми, которые будут вводить их в заблуждение и тратить их время. Работниками могут выступать пенсионеры, которые прошли подготовку для общения с мошенниками. Данная работа будет подходить для пенсионеров так как они смогут работать из дома и из любого региона. Для обеспечения деятельности возможно использовать еди-

ную систему межведомственного электронного взаимодействия (при наличии технической возможности и с соблюдением мер по обеспечению конфиденциальности и безопасности передаваемой информации).

Для мобильных операторов, в качестве идей противодействия мошенничеству, можно предложить следующие варианты:

1. При заключении контракта на предоставление услуг связи абонент должен будет давать свое согласие на получение рекламной информации. Также абонентам, которые дали согласие на получение рекламы предоставить возможность в личном кабинете или в салоне оператора, выбирать сферы рекламы о деятельности или услугах о которых он желает получать рекламу.

2. Обязать мобильных операторов, предоставляющих услуги связи, получать информацию об организациях и юридических лицах, о сферах их деятельности. Это понадобится для создания реестра официальных номеров организаций, предоставляющих различные услуги и описание кратких сведений о предоставляемых услугах. Мобильный оператор должен будет указывать название организации при звонке и показывать номер телефона и в случае сомнений, человек сможет обратиться в реестр и узнать информацию о данной организации.

3. Запретить использовать скрытый номер при звонках.

В целях наведения справок при наличии технической возможности и с соблюдением мер по обеспечению конфиденциальности и безопасности передаваемой информации может использоваться единая система межведомственного электронного взаимодействия между правоохранителями, для быстрой передачи информации о мошенниках.

Для call центров обеспечить возможность прохождения их сотрудниками дополнительной аутентификации посредством использования единой биометрической системы в соответствии со статьей 10 Федерального закона от 29 декабря 2022 года № 572-ФЗ.

Таким образом, для предотвращения мошенничества необходимо решать большой спектр вопросов, для организации деятельности качественного противодействия данному преступлению и повышению уровня финансовой и информационной образованности населения, а также совершенствования законодательства в данной сфере.

Бушуев Игорь Венальевич,
начальник кафедры общеправовых дисциплин
Волгодонского филиала Ростовского
юридического института МВД России,
тел: 8-999-471-88-89, e-mail: bushuev.igor.2017@mail.ru

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ: ОПЫТ И ПЕРСПЕКТИВЫ

Стремительное изменение социально-политической и экономической обстановки жизни в современном российском обществе способствовали не только существенному количественному и структурному росту преступности, но и приобретению ею характера транснациональности. В соответствии с ч. 2 ст. 3 Конвенции против транснациональной организованной преступности¹ преступление носит транснациональный характер, если: оно совершено в более чем одном государстве; оно совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля имеет место в другом государстве; оно совершено в одном государстве, но при участии организованной преступной группы, которая осуществляет преступную деятельность в более чем одном государстве; или оно совершено в одном государстве, но его существенные последствия имеют место в другом государстве.

Транснациональные организованные преступные группы совершают противоправные деяния, сопровождающиеся особой жестокостью и цинизмом. Впечатляет разносторонность их интересов и география преступлений, организованность и высокий уровень взаимодействия структурных подразделений этих групп. Международный размах приобрели терроризм и другие общественно опасные преступные проявления. Стало очевидно, что силами правоохранительных органов одной страны обуздать транснациональную преступность невозможно. Международное сотрудничество подразделений правоохранительных органов стран мира в борьбе с транснациональной преступностью представляет собой объективную необходимость².

¹ Конвенция против транснациональной организованной преступности (принята в г. Нью-Йорке 15.11.2000 г. Резолюцией 55/25 на 62-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН).

² Колосович М. С., Чхвимиани Э. Ж. Правовая регламентация международного сотрудничества правоохранительных органов при осуществлении оперативно-розыскной деятельности и использовании ее результатов: современное состояние и перспективы развития // Вестник Волгоградской академии МВД России. 2014. №2 (29).

Международное сотрудничество в сфере оперативно-розыскной деятельности¹ становится все более значимым фактором обеспечения правопорядка и безопасности в эпоху глобализации и интенсивного развития технологий, поскольку современный мир характеризуется ростом транснациональной преступности, проникновением киберпреступлений и усилением террористических угроз, которые не признают государственных границ. В таких условиях национальные правоохранительные органы оказываются вынуждены сотрудничать на международном уровне, чтобы эффективно реагировать на новые вызовы и обеспечивать комплексную защиту общества и государства от преступных действий².

Исторически среда ОРД формировалась как внутринациональная структура, однако с развитием международных связей и появлением организованных преступных группировок, действующих в нескольких странах, уже в XX веке началась координация действий правоохранительных органов различных государств. Важную роль в этом процессе сыграли создание Интерпола в 1923 году и последующая интеграция международных стандартов безопасности. В Российской Федерации законодательное регулирование международного сотрудничества в оперативно-розыскной деятельности закреплено законом № 144-ФЗ от 1995 года, который устанавливает правовые основы взаимодействия с зарубежными коллегами и международными организациями³.

На сегодняшний день международное сотрудничество в сфере ОРД включает широкий спектр мер: обмен информацией и разведданными, проведение совместных расследований и операций, экстрадицию и передачу осужденных преступников, а также совместную подготовку и повышение квалификации сотрудников. Такое сотрудничество осуществляется как посредством двусторонних соглашений между государствами, так и через работу международных организаций, таких как Интерпол, Европол и региональные объединения. Однако, несмотря на успехи, практика международного взаимодействия сталкивается с рядом сложностей, включая разли-

¹ Далее ОРД.

² Яцко А. М., Кривошеев С. В. Международное сотрудничество в области оперативно-розыскной деятельности // Научный лидер. 2024. № 19 (169). URL: <https://scilead.ru/article/6397-mezhdunarodnoe-sotrudnichestvo-v-oblasti-oper> (дата обращения: 01.10.2025).

³ Всероссийская научно-практическая конференция «Актуальные проблемы уголовного процесса и уголовного права в условиях глобальных вызовов современности», 3 октября 2024 г., Восточно-Сибирский филиал Российского государственного университета правосудия (Иркутск) // Конференции. RU. URL: <https://konferencii.ru/info/148591> (дата обращения: 01.10.2025).

чия в национальном законодательстве, языковые барьеры и необходимость строгого соблюдения прав человека¹.

Международное сотрудничество в ОРД опирается на комплекс международных и национальных правовых норм, обеспечивающих эффективное взаимодействие правоохранительных органов различных стран, поскольку правовые основы сформировались посредством долгого развития международных отношений и призваны отвечать на вызовы, связанные с глобализацией и транснациональной преступностью, в их основе лежат ключевые международные документы, обладающие универсальной значимостью, а также специализированные конвенции и соглашения, регламентирующие аспекты оперативной деятельности и сотрудничества.

Среди фундаментальных международных актов выделяются Всеобщая декларация прав человека (1948), Устав Организации Объединённых Наций (1945), Международный пакт о гражданских и политических правах (1966), Устав Совета Европы (1949) и Конвенция о защите прав человека и основных свобод (1950). Данные документы не только декларируют основные права личности на жизнь, свободу и неприкосновенность, но и задают стандарты, обязательные для соблюдения государствами в процессе обеспечения правопорядка, включая меры противодействия преступности².

Специфическим международным нормативным актом в сфере борьбы с транснациональной преступностью, который бы нам хотелось отметить, является Конвенция ООН против транснациональной организованной преступности (2000), которую Россия ратифицировала в 2004 году, направленная на создание основ для организации международного сотрудничества, включая обмен информацией, проведение совместных операций, экстрадицию преступников и оказание взаимной правовой помощи.

Как мы уже отметили выше, на уровне российского законодательства ключевым документом, регламентирующим международное сотрудничество в ОРД, является Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности», содержащий положения о технических средствах, которые могут применяться в рамках международного взаимодействия, а также регулирует порядок обмена информацией и координации с иностранными правоохранительными органами³.

¹ Международное сотрудничество в сфере противодействия преступности и обеспечения безопасности // ГАРАНТ. URL: <https://edu.garant.ru/relevant/main/529796/> (дата обращения: 01.10.2025).

² II Международная научно-практическая конференция на тему «Актуальные проблемы уголовного права, уголовного процесса, криминологии и уголовно-исполнительного права: теория и практика», 11-12 апреля 2013 г. / Институт права Тамбовского государственного университета имени Г.Р. Державина. URL: <https://edu.garant.ru/relevant/main/529796/> (дата обращения: 01.10.2025).

³ Международная научно-практическая конференция «Уголовный процесс и криминалистика: правовые основы», Сочинский государственный университет, 2025 год. URL: <https://si.sseu.ru/content/mezhdunarodnaya-nauchno-prakticheskaya-konferenciya-ugolovnyy-process-i-kriminalistika>

Международное сотрудничество в сфере ОРД осуществляется посредством двусторонних и многосторонних соглашений, участия в международных организациях, создания совместных оперативных групп и проведение скоординированных международных операций, что позволяет объединять ресурсы, обмениваться информацией и опытом, а также проводить комплексные мероприятия по предупреждению и раскрытию преступлений транснационального характера.

Одной из наиболее значимых платформ для международного взаимодействия являются описанные нами выше такие структуры, как Интерпол и Европол. Интерпол объединяет полицию 194 стран, предоставляя сервисы для оперативного обмена информацией, координации трансграничных расследований и поддержки совместных операций. Европол функционирует на уровне Европейского союза и занимается аналитическим сопровождением, обменом оперативными данными и поддержкой национальных правоохранительных органов. Эти организации создают условия для реагирования на современные угрозы, которые включают в себя киберпреступность, терроризм, торговлю наркотиками и оружием.

Несмотря на разные организационные формы, международное сотрудничество сталкивается с рядом серьезных трудностей, где одной из проблем является несоответствие национальных законодательств, которая затрудняет процедуру обмена информацией, совместное проведение операций и экстрадицию преступников. Различия в законодательстве создают барьеры для взаимодействия, что особенно проявляется при борьбе с киберпреступностью и транснациональными организованными преступными группами. Языковые и культурные различия мешают своевременному и качественному обмену информацией между различными правоохранительными структурами, поскольку отсутствие должной координации и обмена опытом приводит к дублированию усилий и неэффективному использованию ресурсов, что в свою очередь негативно отражается на результатах расследований. Политические разногласия и вопросы национального суверенитета также могут ограничивать свободу передвижения сотрудников и доступ к информации, снижая оперативность и результативность такого сотрудничества. Важным вызовом здесь остается обеспечение защиты персональных данных и конфиденциальность передаваемой информации, поскольку увеличение объемов цифровых данных требует внедрения современных средств шифрования и усиленных мер безопасности, и при этом соблюдение международных и национальных правовых норм является необходимым условием доверия между сотрудничающими сторонами. Ведь несоблюдение этих норм может привести к утечкам информации и подрыву доверия между участниками сотрудничества и для преодоления этих проблем необходимо совершенствование международной правовой базы, стандартизация оперативных процедур, развитие технологической поддержки и повышение квалификации специалистов, а также укрепление

политического диалога и взаимодействия на высоком уровне для устранения административных и политических барьеров, что позволит создать более эффективную и устойчивую систему международного взаимодействия.

Международное сотрудничество в сфере ОРД можно сказать является фундаментом современных усилий по борьбе с транснациональной преступностью, поскольку его эффективность зависит от законодательного обеспечения, технической оснащенности, профессиональной подготовки и международных договоренностей, хотя для дальнейшего развития и необходимы системное совершенствование нормативной базы, стандартизация процедур, укрепление международных организаций и расширение обмена опытом и технологиями между странами. В целях улучшения качества информационного обеспечения международного розыска лиц и борьбы с преступностью осуществляется работа по расширению отечественной правовой базы и дальнейшей интеграции в международные полицейские организации. Продолжается работа по включению ресурсов Генерального секретариата Интерпола в единое информационное пространство органов внутренних дел Российской Федерации. Более того, намечено создание системы удаленного и контролируемого доступа сотрудников органов внутренних дел и других правоохранительных органов на всей территории Российской Федерации к информационным ресурсам Интерпола

В итоге можно констатировать, что международное взаимодействие в области ОРД сегодня является важнейшим и неотъемлемым элементом глобальной системы обеспечения общественной безопасности и правопорядка, поскольку рост транснациональной преступности, включая киберпреступления, терроризм, наркобизнес и нелегальный оборот оружия, требует координации действий правоохранительных структур разных государств, а это возможно лишь через эффективно организованные и скоординированные международные механизмы сотрудничества.

Васильев Эдуард Анатольевич,
главный научный сотрудник Всероссийского
научно-исследовательского института МВД России,
доктор юридических наук, доцент,
тел. 8-917-571-91-79; e-mail: vea62@rambler.ru

Мороз Роза Нураддиновна,
старший научный сотрудник Всероссийского
научно-исследовательского института МВД России,
тел. 8-902-555-68-43; e-mail: roza6843@gmail.com

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ОПЕРАТИВНО-РОЗЫСКНОЙ ПСИХОЛОГИИ

Повышение эффективности борьбы с преступностью на современном этапе развития российского общества относится к числу важнейших задач органов внутренних дел. В решение данной проблемы основная роль отводится ОРД и мало кто сомневается, что без применения её сил, средств и методов современному уголовному судопроизводству не под силу подходить к большинству серьезных преступлений. В тоже время ни для кого не секрет, что оперативные подразделения органов внутренних дел в последние годы сильно утратили свои позиции в криминальной среде и не всегда владеют информацией о процессах, происходящих в преступном мире.

Причины снижения эффективности оперативной работы не связаны с малой численностью, некомплектom или с неопытностью личного состава оперативных подразделений. Основной костяк сотрудников (84,5%) – это выпускники учебных заведений системы МВД России, где они успешно прослушали курс лекции по теории ОРД, располагают достаточным опытом работы в должности оперативно-начальствующего состава. Но, как показало многолетнее эмпирическое исследование, большая часть оперативных сотрудников испытывают трудности в установлении контактов с незнакомыми людьми, особенно, если собеседник занимает важное социальное положение в обществе (так указали 75,5% респондентов).

Именно отсутствие навыков работы с гражданами, по мнению участников круглого стола «Оперативно-розыскная психология: современные подходы и перспективы развития», состоявшегося 24 октября 2025 года во ВНИИ МВД России, во многом выступает фактором снижения оперативно-розыскной функции нынешних оперативных подразделений ОВД.

При этом в фондах научной библиотеки по предмету оперативно-розыскной психологии представлено много разнообразной литературы. Значительную работу в этом плане выполняют коллеги из Московского

университета, Омской академии МВД России и других полицейских вузов. Дефицита литературы точно нет.

Однако это только на первый взгляд. В действительности всё обстоит по-другому, часто в опубликованных работах авторы «пристраивают» к нуждам ОРД возможности социальной или юридической психологии и не ведают, что знания в области оперативно-розыскной психологии не являются юридическими, а представляют собой разновидность специальных познаний в ОРД. Вследствие этого психологические проблемы ОРД сегодня не находят соответствующего освещения в учебниках и программах по курсу оперативно-розыскной деятельности, а если и есть полицейские вузы, которые преподают данную дисциплину, то она закреплена за профессорско-преподавательским составом кафедр психолого-педагогического профиля, что, с одной стороны, создает условия для обеспечения прочного усвоения обучающимися общих психолого-педагогических знаний, с другой стороны, порождает вероятность поверхностного учета оперативно-розыскной составляющей, которая должна быть основана на постоянном взаимодействии с оперативными подразделениями¹. По мнению А.В. Агаркова идеальным будет, если оперативно-розыскную психологию будет преподавать (исследовать) специалист-психолог, осведомленный о силах, средствах и методах ОРД². Однако, к сожалению, такие специалисты для системы МВД России в настоящее время большая редкость.

Совокупность отмеченных факторов находится в основе того, что за более чем полувековую историю с начала публикационной активности авторов о проблемах оперативно-розыскной психологии она не стала самостоятельной наукой и по-прежнему развивается в рамках частной теории ОРД. Поэтому основной задачей нынешних авторов ОРД, по нашему мнению, является разработка ее методологических основ, а именно: предмета, задач, методов и возможностей использования психологических познаний в оперативно-розыскной практике.

Вопрос о предмете изучения – самый важный и в классическом понимании представляет собой определение некоторой целостности, выделенной из мира объектов (в другом аспекте – из реальности) в процессе прикладной и познавательной деятельности. Если правильно определить предмет науки, то можно упорядочить существующие знания, очертить круг проблем, сформулировать задачи исследований, а самое главное – выяснить, что относится к ведению данной отрасли и в чем ее отличие от других дисциплин.

¹ Овчинников О.М. Оперативно-розыскная психология в УИС: тенденции, ресурсы, перспективы. // Оперативно-розыскная психология: современные подходы и перспективы развития : сборник научных трудов. – М. : ВНИИ МВД России, 2025. – С. 163

² Агарков А.В. Оперативно-розыскная психология – самостоятельная наука или отрасль знаний? // Оперативно-розыскная психология: современные подходы и перспективы развития: сборник научных трудов. – М. : ВНИИ МВД России, 2025. – С. 3.

Определяя предмет оперативно-розыскной психологии большинство авторов ограничиваются простым перечислением наиболее актуальных с их точки зрения проблем и направлений исследований. Следует уточнить то, что в список анализируемых работ вошли все доступные публикации начиная с 70-х годов прошлого столетия, включая монографические работы О. Г. Ковалева (2001) и В. И. Филипенко (2004).

В длинном списке авторов по оперативно-розыскной психологии исключение, пожалуй, составляют только два автора – это А. К. Семенов и В. А. Черепанов.

Первый полагает, что оперативно-розыскная психология изучает психическую направленность, закономерности поведения и результаты деятельности субъектов оперативно-розыскной деятельности в целях их активного использования для решения задач борьбы с преступностью¹.

Второй автор считает, что оперативно-розыскная психология – это отрасль научного знания о психологических закономерностях оперативной работы и основанных на познании этих закономерностей психологических приемах и методах совершенствования оперативно-розыскной деятельности².

Полагаем, что оба определения заслуживают внимания, но не безупречны. Так, А. К. Семенов необоснованно относит к ведению оперативно-розыскной психологии результаты деятельности субъектов и игнорирует процессы их общения, между собой и с другими участниками ОРД. При этом игнорирует то, что общение – это один из самых больших разделов предмета науки оперативно-розыскной психологии и на практике – важнейший фактор эффективного решения многих её задач. Навыки общения необходимы для участников оперативно-розыскного процесса для адаптации в различной среде, для полного и качественного взаимодействия с другими людьми. С помощью общения субъекты оперативно-розыскной деятельности имеют возможность получить полную картину о внутреннем мире человека, знать его мысли, чувства, цели, поступки. Причем применительно к предмету оперативно-розыскной психологии речь должна идти не только об участниках криминальных структур, а в большей степени о добропорядочных гражданах готовых выступать в роли добровольных помощников оперативных подразделений, очевидцев криминальных деликтов или иных правонарушений и готовых активно противодействовать таким процессам.

В. А. Черепанов считает, что оперативно-розыскная психология – это отрасль научного знания о психологических закономерностях оперативной

¹ Семенов А. К. Некоторые вопросы исследования основ психологии оперативно-розыскной деятельности. – В кн.: Вопросы совершенствования деятельности органов МВД. – Омск, 1970. – С. 31.

² Черепанов В. А. Психологические вопросы оперативно-розыскной деятельности. – М., изд. ВНИИ МВД СССР, 1981, – С. 64с.

работы и основанных на познании этих закономерностей психологических приемах и методах совершенствования оперативно-розыскной деятельности¹.

Безусловно, что применение психологических познаний в том или ином виде человеческой деятельности еще не создает самостоятельной науки. Знание психологии необходимы не только в ОРД, но и в других сферах общественной практики. Право на самостоятельное существование приобретают лишь те дисциплины, которые изучают специфические, только им присущие объективные закономерности.

А это значит, что существование оперативно-розыскной психологии в качестве самостоятельной отрасли знания возможно лишь в том случае, если в предмет ее входят специфические психологические закономерности.

Г. К. Синилов утверждает, что оперативно-розыскная психология должна формировать собственную систему специфических знаний, изучающих скрытые действия преступников, влияние психологической структуры личности на их мотивацию и поступки, установление и развитие доверительных отношений конфиденентов с криминалитетом для выявления их преступных замыслов и планов, психологического разрешения конфликтных и проблемных ситуаций при использовании оперативно-розыскных мероприятий по выявлению, предупреждению и раскрытию криминальных деяний. Поэтому в предмете оперативно-розыскной психологии исследуются объективные закономерности возникновения и развития тех групп явлений, отношений, фактов, которые определяют применение, прежде всего, негласных сил, средств, методов воздействия на криминальную среду².

Следует полагать, что внимательный исследователь заметит схожесть предмета теории ОРД и оперативно-розыскной психологии, которую мы можем объяснить тем, что оперативно-розыскная психология является частной теорией науки ОРД и не может выходить за рамки её предмета, но сущность исследуемых его закономерностей имеет свою специфику.

Оперативно-розыскная психология – это наука, изучающая психические явления и процессы, происходящие в условиях исполнения оперативно-розыскной функции защиты личности, общества, государства от преступных посягательств, исследующая их механизмы и закономерности.

Исходя из предложенной дефиниции, можно предположить, что задачи оперативно-розыскной психологии могут классифицироваться на общие и специальные. Общей ее задачей является содействие борьбе с преступностью психологическими приемами и методами. К специальным относятся задачи познания отдельных сторон предмета науки, которые могут быть сгруппированы по следующим критериям:

¹ Черепанов В. А. Психологические вопросы оперативно-розыскной деятельности. – М., изд. ВНИИ МВД СССР, 1981, – С. 64.

² Синилов Г. К. Введение в оперативно-розыскную психологию. – М.: МосУ МВД России, 2006. – С. 10.

1) задачи, связанные с научным осмыслением закономерностей влияния психических явлений субъектов оперативной работы на эффективность их практической деятельности;

2) исследование личности объектов ОРД и создание их оперативно-психологической типологии, которые могут использоваться для поиска людей способных решить задачи ОРД с учетом установленных требований социального института и видов деятельности;

3) разработка психологических основ обучения и воспитания в оперативно-розыскной деятельности; создание системы тактических приемов общения в ОРД и управления оперативными аппаратами, и т.д.

Полагаем, что данный перечень не может считаться исчерпывающим. В процессе становления оперативно-розыскной психологии он будет дополняться и уточняться. Однако на современном этапе ее развития мы считаем, что выделенные задачи достаточно полно раскрывают содержание оперативно-розыскной психологии и определяют основные направления ее разработки.

Гонтарь Сергей Николаевич,
доцент кафедры уголовного права и процесса
Северо-Кавказского федерального университета,
кандидат юридических наук, доцент
тел.: 89624433914; e-mail: gonsernik@gmail.com

ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ СЛЕДОВАТЕЛЯ С ОРГАНАМИ ДОЗНАНИЯ ПРИ РЕАЛИЗАЦИИ МАТЕРИАЛОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Эффективное расследование преступлений, особенно тяжких и совершенных в условиях неочевидности, немыслимо без тесного взаимодействия следствия и оперативных подразделений. Оперативно-розыскная деятельность (ОРД) служит мощным инструментом для выявления преступлений, установления лиц, их совершивших, и сбора ориентирующей информации. Однако процесс трансформации результатов ОРД в полноценные судебные доказательства сопряжен с рядом системных проблем, которые зачастую сводят на нет усилия обеих сторон.

Основная правовая коллизия заложена в самом законодательстве: согласно ст. 89 УПК РФ, результаты ОРД не имеют доказательственного значения сами по себе. Они могут быть использованы в доказывании только при условии их соответствия требованиям УПК, то есть после их процессуального оформления следователем. Именно на этом этапе и возникают наиболее серьезные трудности, одна из которых, несвоевременность и неполнота представляемых материалов.

Оперативные сотрудники зачастую стремятся продолжить разработку, собрать больше информации, что приводит к затягиванию момента передачи материалов. В результате упускается время для проведения неотложных следственных действий (осмотра, обыска, задержания), доказательства могут быть утрачены, а подозреваемые – скрыться.

Кроме того, материалы нередко представляются в виде отчета о проделанной работе, а не в форме, удобной для их немедленной процессуальной проверки и использования. В них может отсутствовать точная информация об источниках, условиях и способах получения сведений, что делает невозможным их быструю легализацию.

Еще одним проблемным моментом является нарушение процедуры представления результатов ОРД.

Закон (ст. 11 Федерального закона «Об ОРД») предусматривает, что результаты ОРД представляются органу дознания, следователю или в суд на основании постановления руководителя органа, осуществляющего ОРД. На практике это положение часто нарушается:

Материалы передаются напрямую оперативным сотрудником следователю без надлежащего оформления, отсутствует мотивированное поста-

новление, объясняющее, почему те или иные данные могут быть полезны для уголовного дела. Такие нарушения являются основанием для признания доказательств, полученных на основе этих материалов, недопустимыми (ст. 75 УПК РФ).

Процедура реализации материалов оперативно-розыскной деятельности зачастую связана с проблемой сохранения конфиденциальности источников информации.

ОРД часто связана с использованием конфиденциальных источников (агентов, негласных сотрудников). Закон об ОРД гарантирует защиту их личности. Однако следователь, получая материалы, зачастую лишен возможности проверить достоверность информации, так как не может допросить самого источник.

Это создает правовую ловушку: с одной стороны, следователь обязан проверить все представленные данные, с другой – он не имеет доступа к первоисточнику. Выходом является проведение следственных действий, которые опосредованно подтверждают полученные сведения (например, проверка показаний на месте, следственный эксперимент, назначение экспертизы), но это не всегда возможно.

Нельзя оставить в стороне и проблемы процессуального характера, а именно низкое качество процессуального оформления данных, представляемых в качестве доказательств по уголовному делу. Получив ценные оперативные данные, следователи иногда формально подходят к их процессуальному закреплению. Вынося постановление о приобщении к делу вещественного доказательства, обнаруженного в ходе ОРМ (например, по результатам негласного наблюдения), следователь не всегда подробно описывает, как именно данное доказательство было обнаружено и каким образом оно связано с расследуемым преступлением.

Вместо того чтобы провести осмотр предмета (например, наркотиков) с участием лица, у которого они были изъяты негласно, следователь может ограничиться его «приобщением», что нарушает процедуру и ставит под сомнение происхождение вещественного доказательства.

Проблемы правового регулирования нередко усугубляются ведомственными барьерами и отсутствием единой практики правоприменения.

Следователи и оперативные сотрудники часто относятся к разным ведомствам (Следственный комитет, МВД, ФСБ и т.д.). Это порождает ведомственную разобщенность, различия в подходах к работе и в системе отчетности. Отсутствие единых, утвержденных на межведомственном уровне методических рекомендаций по взаимодействию приводит к тому, что этот процесс зависит от личных отношений конкретных сотрудников, а не от четкого регламента.

Преодоление указанных проблем требует комплексного подхода.

Во-первых, повышение процессуальной дисциплины. Строгое соблюдение требований ст. 11 Закона об ОРД и ст. 89 УПК РФ. Любые мате-

риалы должны передаваться только через руководителя оперативного подразделения с соответствующим постановлением.

Во-вторых, повышение профессиональной культуры. Совместное обучение следователей и оперативных работников. Следователи должны понимать основы и тактику ОРД, а оперативники – основы уголовного процесса и требования к доказательствам.

В-третьих, активное взаимодействие, в идеальной модели – когда следователь на раннем этапе знакомится с ходом оперативной разработки (в пределах, допустимых законом) и дает оперативным сотрудникам ориентиры, какие данные и в какой форме потребуются ему для дальнейшего доказывания. Это позволяет целенаправленно проводить ОРМ и сразу оформлять их результаты правильно.

В заключение следует отметить, что взаимодействие следователя с органами дознания – не технический, а стратегический элемент современного расследования. Существующие проблемы носят системный характер и требуют преодоления ведомственной разобщенности и повышения процессуальной грамотности всех участников процесса. Только налаживание конструктивного диалога, основанного на взаимном понимании задач и требований закона, позволит эффективно использовать мощный потенциал оперативно-розыскной деятельности для достижения главной цели уголовного судопроизводства – защиты прав и законных интересов личности, общества и государства от преступных посягательств.

Ерохин Роман Анатольевич,
старший преподаватель кафедры
уголовного права и оперативно-розыскной
деятельности органов внутренних дел Крымского филиала
Краснодарского университета МВД России
тел: +7(978)019-68-88; e-mail: roman_erokhin@mail.ru

Дюкарь Руслан Михайлович,
слушатель 5 курса Крымского филиала
Краснодарского университета МВД России
тел: +7(978)710-57-16; e-mail: sas.war3@yandex.ru

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Оперативно-розыскная деятельность является неотъемлемой и важной составляющей борьбы с преступностью, в особенности с её латентными и организованными формами. Результаты данной деятельности зачастую служат отправной точкой для возбуждения уголовного дела, основой для выбора версии расследования и ключом к изобличению виновных. Однако процесс интеграции этих результатов в уголовный процесс, их трансформация из ориентирующей информации в полноценные, допустимые доказательства сопряжены с комплексом системных и правовых коллизий, которые остаются предметом острых дискуссий среди теоретиков и практиков права. Корень этих проблем лежит в фундаментальном различии между самой природой оперативно-розыскной деятельности и уголовно-процессуальным доказыванием.

Оперативно-розыскная деятельность – это гласная и негласная деятельность, регулируемая прежде всего Федеральным законом «Об оперативно-розыскной деятельности»¹, где добываемая информация носит ориентирующий, предварительный характер. Уголовный процесс – это жёстко регламентированная УПК РФ процедура, где доказывание строится на доказательствах, которые должны быть допустимыми, относимыми и достоверными. Вследствие этого возникает центральное противоречие: результат оперативно-розыскной деятельности сам по себе доказательством не является. Он может стать им лишь посредством процедуры легализации, то есть преобразования в один из источников, указанных в ст. 74 УПК РФ, такой как протокол следственного действия или вещественное доказатель-

¹ Об оперативно-розыскной деятельности [Электронный ресурс]: федер. закон от 12.08.1995 № 144-ФЗ (ред. от 04.08.2024) // КонсультантПлюс: справоч. Правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_7033/

ство. Ключевым нормативным актом, регламентирующим этот сложный и зачастую закрытый процесс, является межведомственный Приказ № 776¹, который утверждает Инструкцию о представлении результатов оперативно-розыскной деятельности органу дознания, следователю или в суд. Данная процедура, которую на практике часто называют «рассекречиванием», предполагает не просто механическую передачу материалов, а их оформление в виде рапорта об обнаружении признаков преступления или иного документа, который юридически обосновывает инициацию следственных действий. Однако именно здесь и кроется одна из основных проблем: сама процедура, регламентированная ведомственным актом, носит во многом закрытый характер и оставляет значительный простор для усмотрения оперативных работников. Материалы оперативно-розыскной деятельности зачастую представляются в суд и стороне защиты в виде выжимок и сводок, что серьезно затрудняет их полноценную проверку на предмет допустимости и достоверности, поскольку защита лишена возможности оценить исходные данные, методы их получения и возможные нарушения, допущенные при документировании в рамках дел оперативного учета. Как отметил Констенко А.Б.: «При этом в законодательстве нет однозначного ответа, как необходимо «вводить» результаты оперативно-розыскной деятельности в процессуальное поле доказывания по уголовному делу, ведь сами по себе результаты данной деятельности доказательствами не являются. Это вынуждает правоприменителей искать пути выхода из данного положения, что является, по нашему мнению, пробелом в законодательстве», что подтверждает актуальность данного вопроса и его значимость².

В ходе этой трансформации и возникают основные проблемы. Первой - является проблема допустимости использования результатов оперативно-розыскной деятельности в уголовном судопроизводстве, регламентированная УПК РФ и Приказом МВД России № 776, которая остается одной из наиболее сложных и дискуссионных в правоприменительной практике. Её суть заключается в фундаментальной коллизии между открытыми, состязательными принципами уголовного процесса, закреплёнными в УПК РФ, и ведомственной, закрытой природой оперативно-розыскной деятельности. Уголовно-процессуальный кодекс РФ устанавливает исчерпывающий перечень источников доказательств и жёсткие критерии их допустимости, требующие, чтобы доказательства были получены надлежащим

¹ Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 г. «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд»* // Российская газета. – 2013. – № 282. – Ст. 24.

² Костенко, А. Б. Проблемы использования результатов оперативно-розыскной деятельности в доказывании по уголовным делам / А. Б. Костенко // Вестник Московского университета МВД России. – 2022. – № 5. – С. 112-115.

субъектом в строгом соответствии с процедурой, гарантирующей права личности. Однако результат оперативно-розыскных мероприятий, по своей сути являясь информацией, часто добытой негласными методами, изначально этим критериям не соответствует. Для преодоления этого разрыва и был создан приказ МВД РФ № 776, детализирующий процедуру легализации – преобразования оперативной информации в уголовно-процессуальное доказательство. Но именно этот процесс на практике и порождает ключевые проблемы. Во-первых, возникает проблема формального «рассекречивания» и невозможности проверки исходных данных. Суд и защита получают неполные, «сырые» материалы (например, не полные фонограммы прослушивания, а лишь их обработанные версии – выдержки, сводки и расшифровки). Это лишает сторону защиты возможности удостовериться в законности исходного оперативно-розыскного мероприятия, в частности установить были ли соблюдены, установленные судебным решением, сроки его проведения, не вышли ли оперативники за его рамки, не была ли искажена информация при редактировании. Таким образом, процедура часто создаёт лишь видимость легализации, нарушая принцип состязательности.

Второй, не менее значимой проблемой, выступает системный конфликт между императивом сохранения конфиденциальности источников оперативной информации и конституционным правом обвиняемого на защиту. Нормативной основой данной коллизии служит прямая диспозиция Федерального закона «Об оперативно-розыскной деятельности», которая в императивном порядке предписывает защищать от разглашения сведения о лицах, внедрённых в организованные преступные группы, а также о штатных негласных сотрудниках и лицах, оказывающих содействие на конфиденциальной основе, а именно ст. 12 ФЗ «Об ОРД». Данная правовая установка создаёт практически непреодолимый процессуальный барьер для стороны защиты, которая законодательно лишена возможности провести полноценную проверку достоверности такого источника информации, оценить его мотивы, добросовестность и объективность путём его допроса в качестве свидетеля. Это прямо подрывает фундаментальный принцип состязательности сторон, закреплённый в статье 15 Уголовно-процессуального кодекса РФ.

Важной попыткой разрешения этого противоречия стало Постановление Пленума Верховного Суда РФ от 31.10.2019 № 29 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере экономической деятельности»¹, в котором ВС РФ указал, что при оценке доказательств, основанных на результатах оперативно-

¹ О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере экономической деятельности [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 31 окт. 2019 г. № 29 // Верховный Суд РФ: офиц. сайт. – URL: <http://www.vsrp.ru/documents/own/30930/> (дата обращения: 13.10.2025)

розыскной деятельности, суд должен проверять, не являются ли они результатом провокации. Особое значение имеет пункт 13 данного постановления, где подчеркивается, что при наличии ходатайства защиты о проверке доказательств, полученных с использованием результатов оперативно-розыскной деятельности, суд обязан исследовать вопросы законности и достоверности их получения.

На практике это порождает третью проблему – формализм и так называемое «легендирование» следственных действий. Нормативной основой данной проблемы выступает противоречие между требованием части 1 статьи 86 УПК РФ о том, что доказывание осуществляется только путем производства следственных и иных процессуальных действий, и фактической возможностью использования в качестве отправной точки непроцессуальных данных, полученных в рамках оперативно-розыскной деятельности. Согласно статье 6 Федерального закона «Об оперативно-розыскной деятельности», результаты оперативно-розыскной деятельности могут использоваться для подготовки и осуществления следственных действий. Однако на практике это приводит к ситуациям, когда, например, обыск или выемка, инициированные исключительно на основе данных, полученных от конфиденнта или в ходе прослушивания телефонных переговоров, формально обосновываются в протоколе следственного действия как мероприятия, в ходе которых улики были «внезапно обнаружены». Это создает искусственную картину самостоятельного формирования доказательственной базы в процессе следствия, искажая подлинный генезис доказательств и лишая суд возможности в соответствии с частью 2 статьи 75 УПК РФ объективно оценить законность их происхождения, поскольку скрывается истинный повод и основание для производства следственного действия. Данная проблематика находит свое отражение в исследовании работ Меркулова М.А., который отмечает, что «в ходе проведения обыска или выемки, причем на любой стадии проведения, не исключено возникновение различных трудностей и проблем. При этом многие проблемы и коллизии обусловлены тем, что присутствуют законодательные пробелы, правовые предписания не всегда носят четкий характер, а также лица, которые участвуют в названных следственных действиях, не учитывают некоторые важные тактические рекомендации¹».

Четвертая проблема связана с оценкой достоверности и рисками провокации. Правовое регулирование оперативного эксперимента и проверочной закупки осуществляется статьей 6 Федерального закона «Об оперативно-розыскной деятельности». Однако ключевой вопрос о разграничении правомерных оперативных действий и недопустимой провокации, то

¹ Меркулов, М. А. Актуальные проблемы производства обыска и выемки в контексте обеспечения безопасности прав участников уголовного процесса [Электронный ресурс] / М. А. Меркулов // Lex Russica. – 2023. – № 5. – С. 145-152. – URL: <https://lex-russica.ru/archive/2023/5/merkulov.pdf> (дата обращения: 13.10.2025).

есть искусственного создания условий для совершения преступления, когда у лица не было изначально умысла на его совершение, в данном законе прямо не решен. Это создает правовой вакуум, который приводит к серьезным сложностям на практике. Результаты, полученные в ходе таких оперативно-розыскных мероприятий, всегда требуют тщательной проверки на предмет того, был ли подозреваемый спровоцирован или его действия были самостоятельными. В соответствии с пунктом 4 части 2 статьи 75 УПК РФ доказательства, полученные с нарушением требований УПК, являются недопустимыми. Сложившаяся правовая позиция, выраженная в постановлениях высших судов, признает провокацию преступления грубейшим нарушением, влекущим недопустимость доказательств. Однако отсутствие четких законодательных критериев провокации в рамках оперативно-розыскной деятельности и закрытый характер материалов дела делают такую проверку крайне затруднительной.

Пути решения этих сложных вопросов видятся в комплексном реформировании отечественной системы использования результатов ОРД в уголовном судопроизводстве. Одним из предлагаемых шагов является расширение перечня доказательств в УПК РФ с прямым включением в него результатов оперативно-розыскной деятельности, но лишь при условии создания действенных механизмов, обеспечивающих одновременно и защиту государственной тайны, и право обвиняемого на оспаривание таких доказательств. Ряд процессуалистов, таких как А.В. Федоров, полагает, что «легализация результатов оперативно-розыскной деятельности в качестве самостоятельных доказательств позволит унифицировать практику и повысить эффективность борьбы с преступностью, однако это требует создания адекватных процессуальных фильтров для проверки их допустимости¹».

Другим перспективным направлением считается развитие института «закрытых» судебных заседаний, где защитник, имеющий соответствующий допуск к государственной тайне, мог бы участвовать в исследовании материалов оперативно-розыскной деятельности, не раскрывая их своему подзащитному, что частично сняло бы остроту конфликта между конфиденциальностью и состязательностью. Профессор В.Н. Хрулева в своих работах отмечает, что «подобная модель, при строгом процессуальном регламентировании, могла бы стать разумным компромиссом, позволяющим соблюсти баланс между интересами правосудия и правами обвиняемого²».

Также необходимо совершенствование судебного контроля через ужесточение законодательных требований к материалам, представляемым для санкционирования оперативно-розыскных мероприятий, и повышение

¹ Федорова А. В., Допустимость доказательств в уголовном процессе: проблемы оперативно-розыскной деятельности / А. В. Федоров. – Москва: Юрист, 2020. – 245 с.

² Хрулева В. Н., Конфиденциальность и состязательность в уголовном судопроизводстве: монография / В. Н. Хрулева. – Санкт-Петербург: Изд-во Р. Асланова «Юридический центр Пресс», 2019. – 304 с.

прозрачности путём детального мотивирования судебных решений о допустимости таких результатов. Только при таком комплексном подходе, сочетающем законодательные новации с изменением правоприменительной практики, возможно построение сбалансированной модели использования результатов оперативно-розыскной деятельности, отвечающей как требованиям эффективности уголовного преследования, так и стандартам справедливого правосудия.

В заключение следует отметить, что проблема использования результатов оперативно-розыскной деятельности в доказывании – это, по своей сути, поиск хрупкого баланса между двумя фундаментальными ценностями: эффективностью борьбы с преступностью и незыблемостью прав и свобод личности. Современная российская правовая система находится в непрерывном поиске этого баланса, и дальнейшее развитие уголовно-процессуального законодательства и правоприменительной практики должно быть нацелено на выработку чётких, справедливых и прозрачных процедур, которые позволят использовать весь потенциал оперативно-розыскной деятельности, не поступаясь при этом базовыми принципами правового государства.

Железняк Николай Семенович,
профессор кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
доктор юридических наук, профессор,
заслуженный юрист РФ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ (ОЦЕНКА ДИЛЕТАНТА)

Оперативно-розыскная деятельность (далее – ОРД) преимущественно регулируется положениями Федерального закона «Об оперативно-розыскной деятельности»¹, в ч. 3 ст. 6 которого содержится следующее ключевое для данного исследования предписание: «В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде».

В процессе научного поиска мы неоднократно обращали внимание на те или иные средства ОРД, активно применяемые на практике или только упоминаемые в тех или иных нормативных правовых актах² либо исследовательских трудах.³ Если обратиться к последним, то наиболее современной в этом плане, на наш взгляд, представляется монография «Оперативно-розыскной инструментарий»⁴, где средствам ОРД, под которыми понимается «неограниченный перечень предметов материального мира»⁵ (почему только материального, как быть с виртуальным?), при помощи которых обеспечивается решение задач этой деятельности», уделено значительное внимание. Подавляющее большинство известных нам работ посвящены описанию и оценке роли общепринятых средств ОРД в противодействии преступности. И нигде, за исключением отмеченной выше рабо-

¹ Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ (далее – ФЗ об ОРД).

² Наставление об основах организации и тактики оперативно-розыскной деятельности органов внутренних дел Российской Федерации, объявленного приказом МВД России от 04.01.2013 № 001 (далее – Наставление-001).

³ См., например: Осипенко А.Л. Организованная преступная деятельность в киберпространстве; тенденции и противодействие // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4. С. 181–188; Буряков Е.В. Информационные технологии в розыскной деятельности // Научный вестник Омской академии МВД России. 2018. № 3 (70).

⁴ Тамбовцев А.И., Павличенко Н.В. Оперативно-розыскной инструментарий. - М., 2024.

⁵ Здесь и далее нами курсивом выделяются наиболее значимые термины, словосочетания и выражения – Н.Ж.

ты, а также трудов, в которых внимание уделено информационным технологиям, и собственного видения возможностей использования некоторых средств¹, мы не встретили иного подхода к таким ресурсам.

С движением времени меняется многое – в том числе преступность и, естественно, средства противодействия ей. В этом смысле последние годы характерны для изучения различных возможностей искусственного интеллекта (далее – ИИ), в том числе в области борьбы с криминальными проявлениями.

Для людей, в определенной степени далеких от технологических новелл, знакомство с ИИ следует начать с понимания его сущности, выраженного в определении данного термина. Ознакомившись с некоторыми работами в этой области, мы сделали два основных вывода. Первый (на наш взгляд, не имеющий прямого отношения к предмету исследования) – несмотря на то, что о феномене ИИ заговорили еще в прошлом веке и, как правило, мужчины², основные исследования его возможностей активно осуществлялись не так давно и продолжают осуществляться сегодня преимущественно женщинами.³ Второй вывод на основе прочитанного обеспечил возможность сформулировать, по нашему мнению, весьма упрощенное определение ИИ, которое мы описали как технологию, позволяющую на основе специальных компьютерных программ обрабатывать большие объемы данных и находить в них закономерности, способствующие формулированию выводов, предсказанию событий или принятию на этой основе решений.

Опираясь на такое понимание ИИ, с учетом объема работы попытаемся оценить его значимость для ОРД.

¹ Железняк Н.С. К проблеме детализации телефонных переговоров // В книге: Актуальные проблемы борьбы с преступностью в Сибирском регионе. Сборник материалов международной научно-практической конференции. Ответственный редактор: В.И. Горобцов. 2003. С. 219-223; Железняк Н.С. О ключевом средстве противодействия преступлениям в сфере незаконного оборота наркотиков / Вестник Сибирского юридического института ФСКН России. 2015. № 2 (19). С. 27-30; Железняк Н.С. Использование изъятых средств связи в оперативной игре / Научный вестник Омской академии МВД России. 2019. № 3 (74). С. 27-32; Железняк Н.С. О некоторых нестандартных средствах оперативно-розыскной деятельности в противодействии организованной преступности / Общество и право. 2025. № 2 (92). С. 53-58.

² Кузнецов О. П. и др. Круглый стол «Парадигмы искусственного интеллекта» // Новости искусственного интеллекта. – 1998. – №. 3. – С. 140-161; Петрунин Ю. Ю. Искусственный интеллект как феномен современной культуры Три значения термина искусственный интеллект. – 1994.

³ См. например: Лукьянова Е. Д. Создание искусственного интеллекта: современные достижения и отложенные риски // Социологическая наука и социальная практика. – 2019. – Т. 7. – №. 1 (25). – С. 142-148; Вислова А. Д. Современные тенденции развития искусственного интеллекта // Известия Кабардино-Балкарского научного центра РАН. – 2020. – №. 2 (94). – С. 14-30; Искандерова Ш. Д. Влияние искусственного интеллекта на современный мир // Science and Education. – 2023. – Т. 4. – №. 4. – С. 564-570.

Деятельность сыщика в различных направлениях связана со многими неизвестными, порождающими ряд вопросов:

- в работе по предупреждению преступлений – будут ли оптимальными для устранения тех или иных негативных факторов избранные меры, какие последствия от действий правоохранительных органов могут осложнить оперативную обстановку, дадут ли нужный эффект планируемые в рамках индивидуальной профилактики действия и т.п.;

- в розыскной работе – где может скрываться искомый фигурант, какие оперативно-розыскные мероприятия (далее – ОРМ) и иные действия позволят обнаружить его местонахождение и осуществить задержание;

- в работе по раскрытию преступлений – какие ОРМ и иные действия, в какой последовательности и в какие сроки следует использовать для установления преступника и его привлечения к установленной законом ответственности.

Вопросы..., вопросы, многие из которых длительное время остаются без ответа, на наш взгляд, по двум причинам: во-первых, от недостатка информации и, во-вторых, от неумения грамотно выстраивать алгоритмы целесообразных действий с целью решения поставленных перед оперативными подразделениями задач.

Что касается добывания информации, то спектр таких возможностей достаточно объемён и не представлен в настоящей работе из-за ее открытого характера.

Практика свидетельствует, что с упомянутыми алгоритмами все сложнее потому, что значительная часть сотрудников, имеющая небольшой стаж оперативной работы, не обладает соответствующими компетенциями, а значит – не умеет выстраивать оригинальные и, более того, оптимальные схемы, которые зачастую с легкостью описываются в кинофильмах или книгах детективной тематики.

В связи с этим выход из сложившейся ситуации нам (напоминаем, только делающим первые попытки «подружиться» с ИИ) видится в активном использовании этой технологии в основном на втором этапе оперативной работы (использовании полученной информации)¹. Правда, это не означает наличия запрета на применение ИИ и для добывания оперативно значимых сведений, особенно, в сетевом пространстве.²

Представленные размышления позволяют сделать однозначный вывод о необходимости изучения возможностей ИИ в правоохранительной сфере и последующем активном использовании полученных знаний в противодействии преступности.

¹ Батоев В.Б. Об использовании технологии “Deepfake” в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2023. – №. 1 (61). – С. 70-76;

² См. об этом: Осипенко А.Л. Оперативно-розыскная деятельность по борьбе с преступностью в глобальных компьютерных сетях. Омск: ОМА МВД России, 2010.

Зоз Владимир Александрович,
старший преподаватель кафедры
уголовного права и оперативно-розыскной
деятельности органов внутренних дел
Крымского филиала
Краснодарского университета МВД России,
тел: +7(980)350-75-50; e-mail: spec13_47@mail.ru

Скрипка Дарья Дмитриевна,
слушатель 5 курса Крымского филиала
Краснодарского университета МВД России
тел: +7(978)244-96-84; e-mail: skripka.dash@yandex.ru

ПОНЯТИЕ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ОТОЖДЕСТВЛЕНИЕ ЛИЧНОСТИ»

Научные и юридические термины часто имеют сложный или неочевидный смысл, который не всегда понятен сразу. Чтобы объяснить и усвоить эти понятия, в науке применяют метод определения (дефиницию). Основное назначение дефиниции заключается в том, чтобы прояснить сущность термина, провести четкую границу между ним и схожими понятиями, а также раскрыть его полное значение.

Дефиниции находят широкое применение в правотворчестве. Ясное толкование понятий в нормативных актах способствует их однозначной интерпретации и верному использованию.

В ст. 6 Федерального закона «Об оперативно-розыскной деятельности» (далее - ФЗ «Об ОРД») указано оперативно-розыскное мероприятие (далее - ОРМ) под названием «отождествление личности». Однако, ни в этом законе, ни в других нормативных актах нет четкого определения этого термина. Данное обстоятельство порождает опасность для соблюдения принципа всеобщего равенства перед законом, поскольку правоприменение может оказаться непоследовательным и обусловленным индивидуальным толкованием соответствующего понятия.

Существенной проблемой, затрудняющей понимание, является отсутствие общепринятой доктринальной трактовки исследуемого ОРМ среди ученых. Многие ученые, в том числе авторы комментариев к ФЗ «Об ОРД», выдвигают отличающиеся трактовки понятия отождествления личности. Это приводит к формированию разнородных, варьирующихся по степени детализации и смысловой наполненности, концепций данного ОРМ.

В результате анализа научной юридической литературы было установлено, что ученые предлагают различные определения ОРМ «отождествление личности».

Эти расхождения обусловлены тем, что по-разному трактуется, что именно включает в себя это мероприятие (его содержание и цели) и на что оно направлено (объект). Анализ функциональной стороны мероприятия позволил нам выявить два ключевых подхода к определению понятия «отождествление личности» в контексте ОРМ.

Н.А. Кузьмин, Л.Л. Тузов и И.А. Климов определяют «отождествление личности» как процесс установления и идентификации человека по его признакам.

С.И. Захарцев, Ю.Ю. В.П. Сальников придерживаются схожей точки зрения, рассматривая «отождествление личности» как ОРМ, главной целью которого является оперативная идентификация человека.¹

Вторая группа концептуальных подходов к ОРД определяет ее сущность через призму таких категорий, как **опознание, установление и идентификация**. Среди исследователей, придерживающихся такого подхода, можно назвать А.Е. Чечётина, В.В. Алексеева, С.А. Ярошенко, Н.С. Железняк, А.Н. Халикова и других. По мнению А.Н. Халикова, «отождествление личности» есть метод выявления лиц, связанных с преступлениями, находящихся в розыске или представляющих интерес для правоохранительных органов, путем их идентификации по внешним приметам.²

В рамках профессиональной терминологии понятия «идентификация», «установление» и «опознание» могут применяться синонимично, но при этом обладают отличительными смысловыми нюансами. Д.Н. Ушаков в своем словаре трактует глагол «идентифицировать» как «отожествлять».³ Применение термина «идентификация» для раскрытия понятия «отожествление личности» приводит к тавтологии, представляя собой логическую ошибку, поскольку определение содержит в себе само определяемое. А.Е. Чечётин ранее уже констатировал данную погрешность в определении ОРМ «отожествление личности».

Согласно толковому словарю под редакцией Л.И. Скворцова, глагол «установить» является полисемантичным.⁴ В числе его значений выделяются: обнаружение или выявление чего-либо, определение, организация или налаживание, а также физическое размещение объекта. Эта многозначность создает трудности в однозначном понимании термина. В рамках словосочетания «установление лица» мы ориентируемся на его значение

¹ Захарцев, С.И. Оперативно-розыскная деятельность в XXI веке: монография / С.И. Захарцев, Ю.Ю. Игнащенко, В.П. Сальников. – М.: Норма, 2022.

² Халиков, А.Н. Оперативно-розыскная деятельность: учебник / А.Н. Халиков. – 3-е изд. – М.: РИОР: ИНФРА-М, 2023.

³ Ушаков, Д.Н. Толковый словарь современного русского языка / Д.Н. Ушаков. – М.: Аделант, 2014.

⁴ Скворцов, Л.И. Большой толковый словарь правильной русской речи / Л.И. Скворцов. – М.: Мир и Образование, Оникс, 2009.

«определение». Тем не менее, даже при таком толковании, мы считаем, что его использование в дефиниции данного ОРМ является недостаточно информативным. Помимо этого, применение термина «установление» в определениях не позволяет провести четкое разграничение с понятиями идентификации и опознания личности.

Согласно толковому словарю Д.Н. Ушакова, «опознать» означает установить личность или подлинность кого-либо, или чего-либо, ориентируясь на определенные приметы и признаки. С нашей точки зрения, данное определение, будучи сопоставленным с альтернативными формулировками, наиболее полно и корректно отражает природу ОРМ «отождествление личности».

В результате оценки имеющихся вариантов изложения функционального аспекта (содержательного наполнения) проводимого мероприятия было выявлено, что ни один из них не подразумевает проведение розыскных мероприятий, ориентированных на установление лиц, представляющих оперативный интерес, на основании их характерных признаков. Подчеркивается, что поисковые мероприятия могут быть интегрированы в содержательную часть ОРМ «отождествление личности». Это особенно эффективно при проведении отождествления посредством розыска лиц в местах их возможного нахождения или путем автоматизированного поиска в информационных системах с использованием визуальных данных.

Специалисты в области ОРД неоднократно подчеркивали важность проведения поисковых мероприятий для установления личности. Так, М.С. Десятов, Д.А. Васильченко, А.С. Малахов и В.А. Шипицин отмечали, что поиск лиц, представляющих оперативный интерес, может осуществляться в местах их вероятного появления.¹

Как отмечают А.Г. Маркушин, М.П. Смирнов, В.П. Легостаев, Ю.А. Агафонов и Ю.Ф. Кваша, в ходе идентификации личности активно применяются информационно-поисковые системы. Этот метод автоматически распознает людей по их уникальным физическим особенностям, например, по лицу или отпечаткам пальцев, используя современные биометрические технологии.²

Исходя из вышесказанного, мы приходим к выводу, что ОРМ «отождествление личности» выходит за рамки простой идентификации. Реализация поисковых мероприятий возможна как посредством непосредственного участия сотрудников, проводящих ОРМ, так и с применением автоматизированных систем. К таким системам относятся, в частности, базы данных, предназначенные для идентификации, и системы городского видео-

¹ Основы оперативно-розыскной деятельности: учебное пособие / под ред. М.С. Десятова. – Омск: Омская академия МВД России, 2017.

² Маркушин, А.Г. Оперативно-розыскная деятельность: учебник и практикум для академического бакалавриата / А.Г. Маркушин. – 4-е изд., перераб. и доп. – М.: Издательство Юрайт, 2017. – 157 с.

наблюдения с функцией распознавания лиц, например, АПК «Безопасный город».

Чтобы правильно понять, что такое «отождествление личности» в ОРД, важно отличать простое сравнение от активного процесса установления человека. По нашему мнению, термины «идентификация» и «опознание» не в полной мере описывают оперативно-розыскное мероприятие «отождествление личности», поскольку они сводятся к простому сопоставлению, в то время как само мероприятие включает в себя активный поиск.

Для обеспечения более точной терминологии при описании данного процесса, нами предлагается использовать термин «обнаружение и (или) опознание». В соответствии со словарём Д.Н. Ушакова, глагол «обнаружить» в рассматриваемом контексте имеет значения «найти», «сделать видимым» или «представить на обозрение». Эти значения, как нам кажется, гораздо лучше отражают реальную деятельность, связанную с отождествлением личности в рамках ОРМ.

В отношении того, кого можно считать объектом опознания в рамках ОРМ, мы не разделяем точку зрения В.В. Алексеева, С.А. Ярошенко, А.П. Киселева, которые ограничивают этот круг только преступниками и лицами, объявленными в розыск. По мнению В.В. Алексеева и С.А. Ярошенко, отождествление личности в рамках ОРМ представляет собой установление личности человека по его уникальным приметам, если этот человек подозревается в совершении преступления или находится в розыске.¹

В работе А.Е. Чечётина, Е.С. Лапина и В.В. Важенина представлено, на наш взгляд, спорное расширение понятия «отождествление личности» в контексте ОРМ. Авторы относят к объектам данного мероприятия не только людей, но и предметы, животных и компьютерные программы,² что, по нашему мнению, выходит за рамки общепринятого понимания. Название мероприятия однозначно определяет его как направленное на идентификацию личности. Использование данного ОРМ в отношении других объектов, по нашему мнению, допустимо только после внесения изменений в его название, отражающих расширение области его применения.

Понятие «отождествление личности» в контексте оперативно-розыскных мероприятий требует дальнейшей детализации и проработки. Причина этой потребности кроется в прогрессе науки, изучающей оперативно-розыскную деятельность, и в изменениях, происходящих в современных условиях, инструментарии и методиках ее реализации. Принимая во внимание изложенное, мы предлагаем пересмотреть определение ОРМ «отождествление личности». Оно понимается как набор взаимосвязанных

¹ Правовые основы оперативно-розыскной деятельности: учебное пособие для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / В.В. Алексеев [и др.]. – М.: ЮНИТИ-ДИАНА, 2016.

² Чечётин, А.Е. Актуальные проблемы теории оперативно-розыскных мероприятий: монография / А.Е. Чечётин. – М.: Издательский дом Шумиловой И.И., 2006. – 180 с.

действий, направленных на обнаружение и (или) установление личности интересующего оперативных органов субъекта, посредством анализа его индивидуальных особенностей.

Таким образом, ОРМ «отождествление личности» по своей природе является процессом установления и розыска субъекта. Помимо прямого опознания, она может предусматривать розыск на основании его индивидуальных признаков.

«Отождествление личности» в ОРД – это комплекс действий по установлению или предварительному выявлению человека, представляющего интерес для правоохранителей, на основе его индивидуальных признаков.

Субъектами данного ОРМ могут быть лица, представляющие оперативный интерес. К данной группе относятся, в частности, лица, совершившие противоправные деяния, потерпевшие от них, а также свидетели и лица, обладающие информацией, имеющей оперативное значение для достижения целей ОРД. Правовая возможность идентификации субъектов, не являющихся физическими лицами, при проведении указанного ОРМ предоставляется только в случае его соответствующего переименования.

Иванов Святослав Игоревич,
начальник кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент
тел. +7-978-821-75-00, e-mail: sviatoslavigor@mail.ru

НЕКОТОРЫЕ АСПЕКТЫ ПОДГОТОВКИ И ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ ОПЕРАЦИЙ ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ, СОВЕРШАЕМЫМИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Жизнь современного общества немыслима без использования информационно-телекоммуникационных технологий. Цифровизация стремительно входит в жизнь каждого человека захватывая все новые и новые сферы его жизнедеятельности. В частности, значительной трансформации подвергаются все сферы экономики. Наличные расчеты повсеместно вытесняются безналичными. Получение заработной платы и пенсии, оплата покупок в магазинах, переводы денег родным и близким, все эти процессы сегодня происходят с использованием банковских карт¹ и банковских приложений в смартфонах граждан. Безусловно, что такие вопросы привлекают повышенное внимание к себе со стороны преступного элемента и способствуют дальнейшей трансформации преступности в сторону активного использования информационно-телекоммуникационных технологий для совершения имущественных преступлений. Кроме того, такие технологии, в силу возможности сохранять свою анонимность в сети, используются преступниками для распространения наркотиков, а иностранными спецслужбами – для распространения экстремистских материалов, подготовки и совершения террористических актов на территории Российской Федерации. Сложившаяся ситуация является вызовом для правоохранительных органов и требует эффективных и действенных мер по противодействию преступлениям указанных категорий. В этой связи предлагаем рассмотреть некоторые аспекты подготовки и проведения оперативно-розыскных операций по борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий.

Под оперативно-розыскной операцией по борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, мы предлагаем понимать основную форму осуществления оперативными подразделениями органов внутренних дел своей оператив-

¹ Горбунов А.Н. Способы незаконного использования пластиковых карт при совершении преступлений / А.Н. Горбунов, В.Н. Цимбал // Общество и право. 2013. № 3(45). С. 217.

ной функции, являющуюся системой оперативно-розыскных мероприятий и иных действий, направленных на борьбу с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, осуществляемых в соответствии с единым замыслом, на основе единого плана и согласованных по цели, времени, месту (объектам) и способам действий¹.

Для правильного понимания вопроса борьбы с преступлениями с использованием информационно-телекоммуникационных технологий необходимо осознать, что эти преступления имеют две сферы их осуществления, и как следствие – две сферы формирования следов их подготовки и совершения. Первая сфера связана именно с использованием информационно-телекоммуникационных технологий, то есть это цифровая среда. Вторая сфера – это окружающий нас реальный мир. Особенностью таких преступлений является тот факт, что объективная сторона преступления также находит свое отображение в указанных двух сферах, а, следовательно, такие процессы как, выявление, предупреждение, пресечение и раскрытие преступлений должны производиться также в двух сферах. Действуя только в одной из двух сфер, невозможно полноценно решить задачу по борьбе с преступностью данной категории. Таким образом, мы понимаем, что и оперативно-розыскные операции также должны подготавливаться и проводиться в двух сферах: цифровой и реальной.

Преступники, как правило, используют цифровую среду для:

- совершения преступления дистанционно;
- анонимизации своих преступных действий;
- введения в заблуждение жертвы преступления;
- получения доступа к денежным средствам жертвы посредством информационно-телекоммуникационных технологий.

Однако сама объективная окружающая нас реальность говорит нам о том, что цифровая среда на сегодняшний день управляется из реального мира посредством различных действий и манипуляций людей. В любом случае субъектом преступления по действующему уголовному законодательству является физическое вменяемое лицо, достигшее возраста уголовной ответственности. Именно человек, реализовывая свой преступный умысел, совершает действия или бездействия в реальном мире или, используя свой прямой или опосредованный доступ к информационно-телекоммуникационным технологиям, совершает действия или манипуляции в цифровой среде.

¹ Иванов С.И. Концептуальные основы оперативно-розыскных операций органов внутренних дел как предмет научного исследования / С.И. Иванов // Вестник Волгоградской академии МВД России. 2023. № 1(64). С. 117.

Приведем пример наиболее распространенного шаблона совершения преступления с использованием информационно-телекоммуникационных технологий.:

1. Преступник получил информацию о номере телефона жертвы, ее персональных данных, наличии у нее денежных средств на банковском счете и наличии приложения банка в ее смартфоне.

2. Связавшись по телефону с жертвой преступник, используя различные манипулятивные техники, убеждает жертву совершить транзакцию по переводу денежных средств, находящихся на ее банковском счете, на счет указанный преступником.

3. Переведенные жертвой денежные средства используются преступником.

Такая схема является самой упрощенной и в реальной жизни имеет множество дополнительных действий со стороны преступника и его соучастников, нацеленных на противодействие раскрытию совершенного им (ими) преступления и невозможность изобличения его (их) виновности. Однако приведенный пример позволяет нам наглядно разобрать, какие действия и в какой среде происходят, где оставляют следы и, как следствие, это позволит нам разобрать пример подготовки и проведения оперативно-розыскной операции.

Разговор преступника с жертвой происходит одновременно в двух сферах и оставляет свою следовую картину в двух сферах. Действия по совершению перевода денежных средств с одного банковского счета на другой также совершаются в двух сферах, но большее отображение имеют в цифровой среде. Причем в цифровой среде выглядит это как обычное некриминальное действие собственника денежных средств, находящихся на его банковском счете. Поступление средств на указанный жертве преступником банковский счет происходит в цифровой среде и находит свое отображение в ней и в реальном мире. Распоряжение похищенными преступником средствами происходит в обеих сферах и отображается в них.

В описанном случае перед оперативным подразделением стоит задача провести проверку по заявлению потерпевшего лица, установить и зафиксировать фактические данные, свидетельствующие о составе преступления, установить личность преступника, собрать и зафиксировать фактические данные, указывающие на его виновность в совершении преступления. Учитывая тот факт, что преступник при подготовке и совершении преступления несомненно предусмотрел и предпринял меры по противодействию правоохранительным органам в его изобличении, а также принял меры по уничтожению возможных следов своей преступной деятельности, шансы на успех в решении стоящей перед оперативным подразделением задачи существенно уменьшаются. Изменить распределение шансов на успех, по нашему мнению, способна профессионально верно подготовленная и проведенная оперативно-розыскная операция.

Подготовка к проведению оперативно-розыскной операции начинается с разработки типовых планов действий имеющихся в распоряжении руководителя оперативного подразделения сил и средств при поступлении информации или заявления о том или ином подготавливаемом, совершаемом или совершенном преступлении с использованием информационно-телекоммуникационных технологий. Такой план должен включать в себя комплекс первоочередных и последующих оперативно-розыскных мероприятий и иных действий, нацеленных на решение стоящих перед оперативным подразделением задач по борьбе с данным видом преступлений. Особенностью плана оперативно-розыскной операции будет то, что он обязательно должен включать в себя систему оперативно-розыскных мероприятий и совместных действий, проведение которых всеми участниками операции должно быть согласовано по месту, времени, объектам, способам действий и целям.

Следует отметить, что согласованность действий участников оперативно-розыскной операции достигается многократно совместно отработанной практикой выполнения таких пунктов плана и таким морально-психологическим климатом в среде участников оперативно-розыскной операции, который обеспечивает взаимопонимание, взаимопомощь, взаимовыручку при совместном выполнении ими тех или иных задач. Создание такой сплоченности в рядах участников оперативно-розыскной операции также, по нашему мнению, относится к этапу ее подготовки. Еще одним важным специфическим элементом подготовки данной категории оперативно-розыскной операции является подбор и обучение специалистов в области информационно-телекоммуникационных технологий¹, которые должны быть готовы к выполнению той части запланированных мероприятий, которые требуют наличия специальных знаний, и иметь опыт их применения на практике для решения задач оперативно-розыскной операции.

Проведение оперативно-розыскной операции по борьбе с преступлениями с использованием информационно-телекоммуникационных технологий, как уже было сказано ранее, имеют своей спецификой действия, направленные на поиск и фиксацию следов преступной деятельности в реальной и цифровой сферах одновременно. В этом плане очень важное значение имеет сплоченность тех участников оперативно-розыскной операции, которые специализируются на работе в различных сферах. Процесс взаимного обмена информацией должен происходить через руководителя операции либо, в случае необходимости, напрямую между исполнителями, но с обязательным незамедлительным последующим уведомлением руководителя. В каждом конкретном случае и на каждом этапе проведения

¹ Осипенко А.Л. Использование информационных технологий в деятельности оперативных подразделений органов внутренних дел / А.Л. Осипенко, А.Н. Лахин // Вестник Волгоградской академии МВД России. 2016. № 2(37). С. 104.

операции необходимо добиваться и достигать преимущества над противоборствующей стороной в: силах, средствах, времени, информированности, конспирации. Успех в достижении намеченных целей зависит от того, каких именно из указанных преимуществ удалось достичь в конкретный момент времени и на конкретном направлении деятельности, а также от умения руководителя операции эффективно и своевременно компенсировать отсутствие преимущества по отдельному направлению другими имеющимися преимуществами. Например, отставание от противника в силах и средствах на конкретном участке компенсировать преимуществом в осведомленности и скорости действий, что способно нейтрализовать отставание в силах и средствах. Отдельным важным вопросом проведения оперативно-розыскной операции является проведение в ее рамках оперативной игры, которая направлена на преодоление любого противодействия со стороны противника и на создание благоприятных условий для решения задач операции.

Коваленко Анна Андреевна,
слушатель 5 курса
Краснодарского университета МВД России
тел.: 8(961)-510-74-22; e-mail: annakovalenko1010101@gmail.com

Студнев Александр Сергеевич,
старший преподаватель
кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
тел.: 8-920-675-56-70; e-mail: alexandr.studneff@yandex.ru

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В ЖИЛИЩНО-КОММУНАЛЬНОЙ СФЕРЕ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ПЛАТЕЖНЫХ СИСТЕМ

Современные процессы цифровизации, затрагивающие все ключевые сферы общественной и экономической жизни, оказывают прямое влияние и на жилищно-коммунальное хозяйство, которое традиционно остается одной из наиболее социально значимых отраслей. Широкое внедрение электронных систем расчетов, мобильных банковских сервисов, онлайн-платежей и специализированных цифровых платформ для оплаты коммунальных услуг существенно облегчило взаимодействие граждан и организаций с поставщиками услуг. Однако одновременно с этим появились новые возможности для совершения противоправных деяний, связанных с хищением бюджетных и частных средств, а также с использованием цифровых технологий для сокрытия следов преступлений. Это обстоятельство предопределяет актуальность исследования особенностей применения оперативно-розыскных мероприятий при выявлении и раскрытии преступлений в жилищно-коммунальной сфере в условиях цифровизации платежных процессов.

Закон определяет ОРД как «вид деятельности, осуществляемый гласно и негласно оперативными подразделениями государственных органов ... 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». Это даёт правовую основу для вмешательства в денежные и информационные потоки, тем самым позволяя выявлять схемы, где цифровые платежи используют как инструмент преступного механизма. Практика оперативно-розыскной работы показывает, что эффективное выявление и раскрытие преступлений, в том числе дистанционных хищений, возможно только в том случае, если оперативные подразделения об-

ладают достоверными сведениями об особенностях преступной деятельности объектов воздействия и могут использовать эти сведения при подготовке и проведении оперативно-розыскных мероприятий (далее – ОРМ). Однако применение ОРМ в сфере ЖКХ подталкивает к ряду специфических проблем. Во-первых, сама структура схем мошенничества часто построена на маскировке: фиктивные лица или организации (например, управляющие компании, ТСЖ) могут привлекаться к сбору платежей, перенаправляя средства на счета, контролируемые преступниками. Эти схемы усложняются, когда используются цифровые платежи или мобильные кошельки, где нет традиционного банковского поручения, а средства движутся быстро и фрагментарно. Во-вторых, доступ к необходимой информации – банковским выпискам, метаданным платежей, идентификация устройств и IP-адресов – ограничен банковской тайной, правами на неприкосновенность частной жизни и законом о персональных данных. Например, ФЗ № 144-ФЗ предусматривает, что органы, осуществляющие ОРД, при проведении мероприятий должны обеспечивать соблюдение прав гражданина на неприкосновенность жилища, тайну переписки и банковских вкладов.¹ Практика показывает, что нарушение этих процедур может привести к недопустимости доказательств.

Следует отметить тенденцию к расширению цифровых каналов в сфере ЖКХ: по данным исследования Doma.ai, доля россиян, оплачивающих коммунальные услуги через банковские онлайн-сервисы, в 2025 году достигла 58% и увеличилась по сравнению с 2024 г.² Это подтверждает рост значимости цифровых платежей и, соответственно, появления новых угроз: перевод средств на «лицевые счета», созданные исключительно для сбора неправомερных платежей; использование QR-код и ссылок-перенаправлений на счета мошенников; применение «экономии масштаба» – когда множество мелких переводов затрудняет отслеживание, а средства быстро «расфокусируются».

Проведение ОРМ в таком контексте требует четкой планировки и межведомственного взаимодействия. Оперативные подразделения должны выстраивать алгоритм действий: выявление аномалий в поступлениях на счета ЖКХ-организаций, сопоставление данных управляющих компаний с банковскими каналами, анализ последовательности переводов, привязка к устройствам и IP-адресам. Важным является использование специальных технических средств и системного, комплексного подхода: мониторинг

¹ Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности». URL: https://www.alfario.ru/doc/ispdn_documents/fz-144.pdf (дата обращения: 09.10.2025).

² Исследование Doma.ai: на 7 % увеличилось число россиян, которые пользуются цифровыми каналами связи с УК. CNews, 27.06.2025. URL: https://www.cnews.ru/news/line/2025-06-27_issledovanie_domaa_i_na_7_uvelichilos (дата обращения: 09.10.25).

движения средств, выявление цепочек переводов через посредников, корреляция с данными операторов платежных систем. Кроме того, закон об ОРД предусматривает, что такие средства, методы и сведения об ОРД могут составлять государственную тайну и подлежат рассекречиванию лишь по решению руководителя органа.¹

Практическая реализация таких мер встречает ряд вызовов: замедленная реакция банков, недостаточная интеграция между правоохранительными органами и финансовыми институтами, отставание нормативной базы от темпов цифровизации, не всегда достаточная квалификация оперативных работников в сфере цифровых финансовых расследований. Всё это заставляет говорить о необходимости совершенствования процедур: введения чётких регламентов запроса информации у банков и платёжных систем, разработки стандартов соответствия обработке метаданных платежей, обучения сотрудников по цифровой криминалистике.

Ключевым элементом становится правовая сбалансированность: обеспечение эффективности расследования и при этом соблюдение конституционных прав граждан – неприкосновенности частной жизни, тайны переписки, банковской тайны. Нарушение этих прав ведёт к признанию полученных доказательств недопустимыми; соответственно, компетенция органов ОРД должна быть выстроена на законных основаниях, включая получение постановлений прокурора или суда при необходимости применения специальных технических средств. Недостаточное законодательное регулирование цифровых платёжных систем в контексте ОРД также создаёт поле для угроз и требует законодательного внимания.

В заключение можно отметить, что успешное применение оперативно-розыскных мероприятий при преступлениях в ЖКХ с использованием цифровых платежей возможно лишь при сочетании правовой чёткости, технической оснащённости, межведомственного взаимодействия и профессиональной подготовки. Рекомендуется разработать пакет типовых процессуальных шагов: мониторинг платежей, запрос данных у банков и платёжных агрегаторов, привязка к устройствам и IP-адресам, внедрение аналитических систем и алгоритмов выявления аномалий, обучение персонала. Вполне целесообразно рассмотреть возможность нормативного закрепления обязанностей платёжных систем по предоставлению транзакционных и метаданных при инициировании расследования преступлений в ЖКХ. Лишь при таком подходе может быть обеспечена адекватная защита прав граждан и надлежащий уровень противодействия преступной деятельности в условиях цифровой трансформации сферы ЖКХ.

¹ Оперативно-розыскная деятельность – основной правовой механизм борьбы с преступностью. АПНИ. URL: <https://apni.ru/article/7092-operativno-rozisknaya-deyatelnost-osnovnoj-pr> (дата обращения: 09.10.2025).

Крюк Антон Николаевич,
преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

Муталимов Радим Расмиевич,
слушатель 5 курса Краснодарского университета МВД России

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «КОНТРОЛЬ ПОЧТОВЫХ ОТПРАВЛЕНИЙ, ТЕЛЕГРАФНЫХ И ИНЫХ СООБЩЕНИЙ»

Оперативно–розыскная деятельность представляет собой особый вид государственной правоохранительной деятельности, направленный на предупреждение, выявление, пресечение и раскрытие преступлений, а также на розыск лиц, их совершивших. В соответствии с Федеральным законом «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ,¹ одним из важнейших инструментов реализации задач оперативно–розыскной деятельности является проведение оперативно–розыскных мероприятий.

Оперативно – розыскное мероприятие контроль почтовых отправлений, телеграфных и иных сообщений – это оперативно-розыскное мероприятие, которое заключается в просмотре письменной и иной зафиксированной на материальном носителе корреспонденции в целях обнаружения сведений о преступной деятельности изучаемого лица, выявления его связей и получения иной информации, способствующей решению конкретных задач ОРД.²

Данное оперативно–розыскное мероприятие направлено на получение информации необходимой для предупреждения, выявления, пресечения и раскрытия преступлений, а также для установления местонахождения лиц. Его сущность заключается в ограничении конституционного права граждан на тайну переписки, что допускается исключительно на основании судебного решения и только в случаях, предусмотренных законодательством.

В современных условиях развитие коммуникационных технологий, цифровизация информационного обмена информацией существенно усложняют процесс контроля за передачей информации. Преступные сообщества активно используют электронные мессенджеры для передачи информации. В связи с чем возникает вопрос, что понимается под иными сообщениями. В оперативно–розыскной науке существует несколько мнe-

¹ Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (последняя редакция) (дата обращения: 10.11.2025)

² Оперативно-розыскная деятельность органов внутренних дел. Общая часть: Электронное учебное издание. – Омск : Омская академия МВД России, 2020. – 206 с.

ний на этот счет. Одни авторы выступают с мнением, что данное оперативно–розыскное мероприятие носит исключительный характер в плане передачи информации по материальным носителям – бумаге, а другие, напротив, считают, что в понятие иные сообщения входят и электронные каналы передачи информации и соответственно информация носит как физический характер, так и электронный.

Так, А.Ю. Шумилов¹ считает, что в категорию «иные сообщения» включается категория информации, которая передается по сети почтовой, электрической связи, т.е. посредством передачи информации через электронную почту.

Напротив, мнение описано в учебном издании Омской академии МВД России,² где указывается, что предметом данного ОРМ являются только те почтовые отправления, которые передаются на материальном носителе, т.е. на бумаге и, как следствие, отправления, распространяемые по каналам электронной почты, являются предметом других ОРМ.

Каждая из точек зрения, конечно, имеет место быть. ФЗ-№144 «Об оперативно–розыскной деятельности»³ был принят во времена, когда Интернет только начинал появляться. В связи с чем и возникают различные споры в научных кругах. Однако отсутствие регламентации в законодательстве вызывает как раз определенные трудности в практике применения ОРМ.

На наш взгляд, оперативно–розыскное мероприятие «контроль почтовых отправлений, телеграфных и иных сообщений» все же подразумевает передачу информации на физическом носителе, так как информация, передаваемая по электронным каналам связи в практической деятельности фиксируется при проведении таких оперативно–розыскных мероприятий, как «снятие информации с технических каналов связи», «прослушивание телефонных переговоров», «получение компьютерной информации».

Как уже ранее было отмечено, данное ОРМ проводится только на основании судебного решения. Но следует отметить, что в некоторых случаях возможно отступление от данного правила в случаях, нетерпящих отлагательств. В таких случаях возможно проведение мероприятия без решения суда. Но следует отметить, что при проведении мероприятия без получения судебного решения, необходимо уведомить суд в течение 48 часов после проведения ОРМ.

В ходе проведения данного ОРМ возможна фиксация информации с помощью различных способов – копирование информации, фотофиксация, видеозапись, изъятие рукописных бланков.

¹ Шумилов, А.Ю. Курс основ ОРД: Учебник для вузов. М.: 2006. – 368с

² Оперативно-розыскная деятельность органов внутренних дел. Общая часть : Электронное учебное издание. – Омск : Омская академия МВД России, 2020. – 206 с.

³ Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (последняя редакция) (дата обращения: 10.11.2025)

Проведение оперативно–розыскного мероприятия «контроль почтовых отправлений, телеграфных и иных сообщений» возможно на срок до шести месяцев со дня получения судебного решения.

Результаты контроля почтовых отправлений, телеграфных и иных сообщений оформляются в установленном законом порядке в форме рапорта, справки, к которым в качестве приложения прилагаются материальные носители информации. Результаты проведенного ОРМ могут использоваться для принятия оперативных решений, построения оперативных версий, а также для передачи информации в следственные органы для решения вопроса о возбуждении уголовного дела.

Следует подчеркнуть, что контроль почтовых отправлений и сообщений играет важную роль не только в раскрытии уже совершенных преступлений. Но и в предупреждении потенциальных угроз. В частности, посредством проведения данного мероприятия удастся выявлять преступные намерения на ранней стадии, предотвращать террористические акты, пересылку различных запрещенных предметов и веществ.

Таким образом, контроль почтовых отправлений, телеграфных и иных сообщений является важнейшим оперативно–розыскным мероприятием, которое способствует предупреждению и раскрытию преступлений. Рациональное применение указанного ОРМ позволяет своевременно пресекать преступную активность, не доводя до общественно опасных последствий.

Куминов Михаил Владимирович,
старший преподаватель кафедры информационной безопасности
Краснодарского университета МВД России
тел.: 8 (918) 396-24-11; e-mail: kumchik@bk.ru

АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С РАЗВИТИЕМ ИНТЕРНЕТА ВЕЩЕЙ (IoT): НОВЫЕ ВЫЗОВЫ ДЛЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Современный этап технологической революции характеризуется тотальной интеграцией в повседневную жизнь и критическую инфраструктуру устройств Интернета Вещей (IoT). Под IoT понимается сеть физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Прогнозируемое количество таких устройств в мире к 2030 году превысит 25 млрд¹. Однако их повсеместное распространение, сопряженное с недостатками в области безопасности, создает принципиально новую, расширенную поверхность для атак, превращая IoT в мощный инструмент и одновременно объект посягательств в руках злоумышленников. Это порождает комплекс новых, слабо изученных вызовов для правоохранительных органов, в чьи задачи входит оперативное раскрытие и пресечение преступлений.

Целью настоящего исследования является систематизация актуальных угроз ИБ, связанных с IoT, с криминологической точки зрения, и разработка на этой основе предложений по адаптации оперативно-розыскной деятельности (ОРД) к новым реалиям.

1. Классификация и анализ IoT-ориентированных угроз в криминальном контексте

Угрозы, связанные с IoT, можно классифицировать по нескольким основаниям. Для целей ОРД наиболее релевантна классификация по роли IoT-устройства в преступной деятельности.

1.1. IoT-устройство как инструмент преступления:

- **Организация масштабных кибератак:** Злоумышленники создают ботнеты из скомпрометированных «умных» устройств (видеокамер, маршрутизаторов, домашней техники) для проведения DDoS-атак. Ярким примером является ботнет Mirai². Такие атаки могут парализовать работу

¹ Statista. (2023). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 (Statista. (2023) - статистические данные и результаты опросов. Количество устройств, подключённых к Интернету вещей (IoT), по всему миру с 2019 по 2023 год, с прогнозами на период с 2022 по 2030 год).

² Обзорная статья обозревателя Евгения Кудрина независимого информационно-аналитического центра компании «АМ Медиа», «Будущее киберугроз: IoT-устройства в центре внимания хакеров» URL https://www.anti-malware.ru/analytics/Threats_Analysis/IoT-devices-attacks#part31

государственных услуг, финансовых институтов и средств массовой информации.

- **Криптоджекинг (cryptojacking):** Несанкционированное использование вычислительных ресурсов IoT-устройств для майнинга криптовалют. Несмотря на низкую производительность отдельного устройства, массовость заражения делает эту схему экономически выгодной для преступников.

- **Нарушение частной жизни и шпионаж:** Взлом «умных» камер, микрофонов (включая детские мониторы, голосовых помощников) для несанкционированного наблюдения, сбора компрометирующей информации и шантажа.

1.2. IoT-устройство как объект посягательства:

- **Взлом систем «Умный дом»:** Получение злоумышленником контроля над системами безопасности (замки, сигнализации), отопления, электроснабжения для совершения краж, вымогательства или причинения физического вреда.

- **Манипуляция данными с датчиков:** Изменение показаний «умных» счетчиков (электроэнергия, вода), медицинских устройств (инсулиновые помпы, кардиостимуляторы) или данных промышленных систем (IIoT – Industrial IoT) с целью хищения ресурсов, причинения вреда здоровью или техногенных катастроф.

- **Блокировка устройств с требованием выкупа (Ransomware):** Шифрование прошивки или блокировка функционала критически важного устройства (например, медицинского) с последующим требованием выкупа за восстановление его работоспособности.

1.3. IoT-устройство как источник криминалистически значимой информации:

Устройства IoT, будучи постоянно подключенными к сети и оснащенными многочисленными датчиками, становятся «цифровыми свидетелями». Данные с фитнес-трекеров, «умных» часов, датчиков движения и голосовых помощников могут содержать ключевую информацию о действиях и местонахождении подозреваемых, что открывает новые возможности для ОРД.

2. Новые вызовы для оперативно-розыскной деятельности

Перечисленные угрозы формируют ряд системных проблем для оперативных подразделений.

2.1. Техничко-криминалистические вызовы:

- **Гетерогенность и фрагментарность:** Огромное разнообразие аппаратных платформ, операционных систем и протоколов связи делает невозможным применение единых методик изъятия и анализа данных.

- **Отсутствие стандартизированных интерфейсов для изъятия evidence:** В отличие от ПК и смартфонов, у многих IoT-устройств отсут-

ствуют физические интерфейсы (USB, UART) для прямого подключения, либо они заблокированы производителем.

- **Проблема «летучих» данных (volatile data):** Критически важная оперативная информация часто хранится только в энергозависимой памяти (RAM) и теряется при отключении питания.

- **Шифрование и облачные хранилища:** Данные часто передаются в зашифрованном виде и хранятся на серверах производителя, расположенных в других юрисдикциях, что затрудняет или делает невозможным их оперативное получение.

2.2. Процедурные и правовые вызовы:

- **Пробелы в законодательстве:** Действующее уголовно-процессуальное законодательство и законы в сфере ОРД не всегда учитывают специфику IoT. Неясен правовой статус данных, собираемых устройством без явного участия человека (например, запись фрагментов разговоров «умным» динамиком).

- **Сложность получения санкции:** Для проведения оперативно-розыскных мероприятий (ОРМ) в отношении IoT-устройства необходимо его точная идентификация и классификация как объекта ОРМ, что технически сложно.

- **Межюрисдикционные барьеры:** Расследование преступлений с использованием IoT часто требует взаимодействия с международными провайдерами и правоохранительными органами, что значительно увеличивает сроки.

2.3. Кадровые и ресурсные вызовы:

- **Дефицит узкоспециализированных кадров,** обладающих знаниями в области embedded-систем, сетевых протоколов IoT и киберкриминологии.

- **Недостаточная техническая оснащенность** оперативных подразделений специализированным оборудованием для анализа широкого спектра IoT-устройств.

3. Методы оперативного реагирования и пути адаптации ОРД

Для противодействия новым угрозам необходима комплексная адаптация оперативно-розыскной деятельности.

3.1. Развитие технического арсенала:

- Создание мобильных криминалистических лабораторий, укомплектованных наборами адаптеров, программаторов и анализаторов протоколов для работы с популярными платформами IoT (ESP32, Arduino, Raspberry Pi и др.).

- Разработка и внедрение программно-аппаратных комплексов для безопасного изолированного анализа IoT-устройств в лабораторных условиях («песочницы»).

- Активное использование средств сетевого анализа (пассивный и активный трафик) для отслеживания коммуникаций между устройствами в ботнетах.

3.2. Совершенствование методик и межведомственного взаимодействия:

- Разработка типовых методических рекомендаций (алгоритмов) по осмотру места происшествия, изъятию и исследованию IoT-устройств.
- Создание единых баз данных «цифровых отпечатков» IoT-устройств (MAC-адреса, идентификаторы, модели) для их оперативной идентификации в сетевом трафике.
- Установление прочных каналов взаимодействия с ведущими производителями IoT-оборудования и национальными CERT/CSIRT-центрами для оперативного обмена информацией об уязвимостях и инцидентах.

3.3. Совершенствование нормативно-правовой базы:

- Инициатива по внесению изменений в законодательство, уточняющих порядок проведения ОРМ в отношении IoT-устройств, включая удаленный доступ к их данным.
- Закрепление на законодательном уровне обязанностей производителей по обеспечению минимального уровня безопасности устройств и сотрудничеству с правоохранительными органами в установленных законом рамках.

3.4. Подготовка кадров:

- Внедрение в программы подготовки и повышения квалификации оперативных сотрудников и следователей специализированных курсов по IoT-криминалистике и кибербезопасности.
- Стимулирование привлечения в правоохранительные органы специалистов из IT-сферы.

Развитие Интернета создало новую, динамично эволюционирующую среду для совершения преступлений. Угрозы, связанные с IoT, носят комплексный характер, затрагивая как частную жизнь граждан, так и национальную безопасность. Низкий уровень защищенности «умных» устройств, их массовость и техническая неоднородность формируют значительные вызовы для оперативно-розыскной деятельности, требуя срочной и системной адаптации.

Эффективное противодействие этим вызовам невозможно без скоординированных усилий по следующим направлениям: техническое перевооружение оперативных подразделений, разработка новых методик сбора и анализа цифровых доказательств, совершенствование законодательной базы и целенаправленная подготовка высококвалифицированных кадров. Только комплексный подход позволит правоохранительным органам не только адекватно реагировать на уже совершенные IoT-преступления, но и вырабатывать проактивные стратегии по их предупреждению.

Кучмезов Рустам Нурбиевич,
старший научный сотрудник научно-исследовательского отдела
Краснодарского университета МВД России,
кандидат юридических наук,
тел.: 8 (918) 220-19-30

Старостенко Олег Александрович,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России,
кандидат юридических наук,
e-mail: olegstaros94@gmail.com; тел.: 8 (961) 857-18-88

СООТНОШЕНИЕ ОПЕРАТИВНО-РОЗЫСКНОЙ И СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ: ГРАНИЦЫ ВЗАИМОДЕЙСТВИЯ И РАЗГРАНИЧЕНИЯ ПОЛНОМОЧИЙ

Оперативно-розыскная деятельность (ОРД) регулируется Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Её основные цели - выявление, предупреждение, пресечение преступлений, а также розыск лиц и установление обстоятельств, имеющих значение для обеспечения безопасности государства. Важнейшая особенность ОРД – её непроцессуальный характер: она осуществляется преимущественно до возбуждения уголовного дела и не подчиняется нормам Уголовно-процессуального кодекса РФ.

Следственная деятельность (СД), напротив, регулируется Уголовно-процессуальным кодексом РФ и осуществляется только после возбуждения уголовного дела. Её цель – полное, всестороннее и объективное установление обстоятельств преступления в строгом соответствии с процессуальными нормами¹. Все следственные действия (допрос, осмотр, обыск и др.) должны быть оформлены процессуальными документами и подлежать судебной проверке.

Таким образом, ключевое различие заключается в том, что ОРД направлена на предварительное выявление признаков преступления, тогда как СД – на доказывание этих признаков в рамках уголовного судопроизводства².

Согласно части 2 статьи 141 УПК РФ, материалы оперативно-розыскной деятельности могут направляться следователю для решения вопроса о возбуждении уголовного дела или приобщения к материалам

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // Доступ из справ.-правовой системы «Гарант». URL: <https://base.garant.ru/12125178/> (дата обращения: 22.10.2025), ст. 155–163.

² Смирнов А.В. Уголовный процесс: учебник. М.: Проспект, 2023. С. 87.

дела¹. Кроме того, следователь вправе давать поручения оперативным подразделениям в соответствии со статьёй 151 УПК РФ². Несмотря на это, на практике такое взаимодействие часто сопряжено с нарушениями. Распространённой проблемой является подмена следственных действий оперативными. Как правило, это связано с недостаточным уровнем профессиональной компетенции молодых следователей. Например, вместо процессуального следственного действия «допрос» проводится «беседа» в рамках оперативного мероприятия, что лишает участника процессуальных гарантий (права на адвоката, фиксацию показаний и др.)³. Такие материалы нельзя приобщить к делу в связи с тем, что нарушен порядок проведения расследования и в большинстве случаев суд не признает полученные сведения законными или легитимными. Другая проблема - неправомерное использование результатов ОРД в качестве доказательств по уголовному делу. Согласно статье 74 УПК РФ, доказательствами по уголовному делу могут быть любые сведения, на основе которых суд, прокурор, следователь или дознаватель устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию⁴. Однако статья 75 УПК РФ устанавливает критерий допустимости доказательств: они признаются недопустимыми, если получены с нарушением требований закона⁵. Результаты оперативно-розыскной деятельности (например, материалы наблюдения, записи переговоров, данные агентурной информации, фото- и видеофиксация) сами по себе не являются доказательствами в уголовном процессе, поскольку получены непроцессуально и не прошли проверку в условиях, предусмотренных процессуальным кодексом. Для того чтобы такие сведения приобрели статус доказательства, они должны быть оформлены в установленной процессуальной форме – путём проведения допроса, осмотра, обыска или иного следственного действия, в ходе которого эти данные фиксируются с соблюдением всех гарантий, либо находят подтверждение.

На практике же нередко наблюдается ситуация, когда следователь напрямую приобщает к материалам уголовного дела оперативные справки, аналитические записки или распечатки переписки, полученные в рамках ОРД, без их процессуального закрепления. Такие материалы не проходят

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // Доступ из справ.-правовой системы «Гарант». URL: <https://base.garant.ru/12125178/> (дата обращения: 22.10.2025), ст. 141, ч. 2.

² Там же. Ст. 151.

³ Гаухман Л.Д. Проблемы соотношения оперативно-розыскной и следственной деятельности // Российский следователь. 2021. № 4. С. 15.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // Доступ из справ.-правовой системы «Гарант». URL: <https://base.garant.ru/12125178/> (дата обращения: 22.10.2025), ст. 74.

⁵ Там же. Ст. 75.

проверку на предмет достоверности и законности получения, а обвиняемый лишается возможности оспорить их содержание в рамках производства.

Яркой иллюстрацией данного нарушения служит апелляционное постановление № 22-5042/2021 от 25 июля 2021 года по делу № 1-12/2021. Суд апелляционной инстанции отменил постановление Темрюкского районного суда Краснодарского края от 3 июня 2021 года о возвращении уголовного дела прокурору для устранения препятствий к его рассмотрению. Основанием для отмены послужило нарушение порядка приобщения материалов оперативно-розыскной деятельности (ОРД) к уголовному делу. Уголовное дело в отношении обвиняемых Р. (по п. «а, б» ч. 3 ст. 228.1 и ч. 2 ст. 228 УК РФ) и Т. (по п. «а, б» ч. 3 ст. 228.1 УК РФ) было направлено на новое судебное рассмотрение со стадии предварительного слушания в тот же суд, но в ином составе судей¹.

Таким образом, использование результатов ОРД в качестве доказательств без соблюдения требований статьи 75 УПК РФ не только нарушает принцип законности, но и подрывает саму основу справедливого правосудия. Это подтверждает необходимость чёткого разграничения между оперативной информацией (исходным материалом для проверки) и процессуальными доказательствами (единственной допустимой основой для обвинения).

ОРД и СД – самостоятельные, но взаимосвязанные виды правоохранительной деятельности. Их разграничение обусловлено различием в правовой природе: в отличие от строго процессуальных следственных действий, допустимых лишь в рамках уголовного судопроизводства, является внепроцессуальной и применяется на досудебной стадии. Их продуктивное взаимодействие требует неукоснительного соблюдения этих различий и уважения процессуальных гарантий.

Основные проблемы современной практики – размытие функций, использование недопустимых доказательств, отсутствие чётких критериев передачи оперативных материалов в следствие. Для их решения необходимы:

- 1) уточнение норм законодательства, регулирующих взаимодействие;
- 2) усиление прокурорского и судебного контроля за законностью ОРД на стадии предварительного расследования;
- 3) повышение правовой культуры сотрудников оперативных и следственных подразделений².

Только при соблюдении этих условий можно обеспечить баланс между эффективностью борьбы с преступностью и защитой конституционных прав личности.

¹ Апелляционное постановление Краснодарского краевого суда от 26.07.2021 по делу № 1-12/2021, № 22-5042/2021 // Электронный ресурс «СудАкт». URL: <https://sudact.ru/regular/doc/Uo0magOBG1R/> (дата обращения: 23.10.2025).

² Иванов С.И. О тактических способах действий оперативно-розыскной тактики и оперативно-розыскных операций // Вестник Уральского юридического института МВД России. 2019. № 2(22). С. 102-106.

Лагуточкин Андрей Владимирович,
доцент кафедры уголовного права
и оперативно-розыскной деятельности органов внутренних дел
Крымского филиала Краснодарского университета МВД России
e-mail: and_ruha@mail.ru; тел. +7(910)320-84-30

Миронов Дмитрий Александрович,
слушатель 5 курса Крымского филиала
Краснодарского университета МВД России
e-mail: lard.boos@mail.ru; тел. +7(978)287-95-71

ТРАНСФОРМАЦИЯ РОЛИ НАУЧНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ В ПОВЫШЕНИИ ЭФФЕКТИВНОСТИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Оперативно-розыскная деятельность традиционно являлась одной из наиболее ресурсоемких и сложных сфер работы органов внутренних дел. Ее эффективность напрямую зависела от профессионального опыта сотрудников, развитой сети осведомителей и применения базовых криминалистических методик. Научно-техническое обеспечение в этом контексте выполняло, главным образом, вспомогательную функцию, фокусируясь на совершенствовании средств фиксации, связи и базовых методов экспертизы.

Однако наступление цифровой эпохи коренным образом изменило саму природу преступности. Транснациональная киберпреступность, использование криптовалют, тотальная цифровизация коммуникаций в повседневной жизни создали принципиально новую оперативную обстановку, в которой традиционные методы оперативно-розыскной деятельности зачастую оказываются неэффективными. Это обусловило настоятельную необходимость в глубокой трансформации научно-технического обеспечения, выводе его на передний край борьбы с преступностью. Настоящая статья посвящена анализу этой трансформации, выявлению ключевых направлений и оценке их влияния на эффективность оперативно-розыскной деятельности.

Исторически сложилось, что научно-техническое обеспечение воспринималось как набор технических средств (фото- и видеоаппаратура, средства аудиозаписи, простейшие лабораторные комплексы), призванные облегчить труд оперативного работника. Техника зачастую применялась постфактум для фиксации следов преступления, проведения экспертиз по уже собранным материалам.

Цифровая эпоха перевернула эту парадигму. Сегодня научно-техническое обеспечение стало проактивным и интегрированным элементом всего цикла оперативно-розыскной деятельности – от прогнозирования

и предупреждения преступлений до раскрытия, расследования и судебного преследования. Это проявляется в следующих аспектах:

Интеграция в планирование: Данные прогнозной аналитики, получаемые с помощью систем на основе Big Data и AI, становятся основой для стратегического и тактического планирования оперативно-розыскных мероприятий. Ресурсы распределяются не интуитивно, а на основе математически выверенных моделей криминогенной обстановки.

Создание новой оперативной среды: научно-техническое обеспечение формирует цифровую экосистему, в которой работает сотрудник. Это единые базы данных, межведомственные платформы обмена информацией, системы криптографированной защищенной связи, геоинформационные системы – все то, что создает принципиально новые возможности для проведения оперативных комбинаций.

Благодаря цифровизации оперативные подразделения могут разрабатывать и внедрять в практику новые способы проведения отдельных оперативно-розыскных мероприятий; так, проведение ОРМ «отождествление личности» теперь доступно в интернете – как непосредственно очевидцами или потерпевшими, так и через цифровые системы распознавания лиц и голоса; кроме того, стало возможным проводить в сети или с помощью мобильной связи ОРМ «опрос» в легендированной форме, например, используя технологии изменения голоса. Так, «наведение справок» трансформировалось в возможность анализа «больших данных» и открытых источников в автоматическом режиме, позволяя составлять цифровые профили лиц, представляющих оперативный интерес, без вступления в непосредственный контакт. «Сбор образцов для сравнительного исследования» теперь может осуществляться путем извлечения цифровых следов (метаданных, файлов) с электронных носителей или из виртуального пространства. Проведение «обследования помещений, зданий, сооружений, участков местности и транспортных средств» получает новое качество благодаря применению беспилотных летательных аппаратов и геоинформационных систем, позволяющих дистанционно фиксировать обстановку на труднодоступных или охраняемых объектах. Таким образом, цифровая трансформация не просто расширяет инструментарий, но и меняет саму природу оперативно-розыскной деятельности, делая её более технологичной и менее зависимой от физического контакта.

Как отмечает Ховавко С.М. «перевод данных в цифровой формат позволяет интегрировать различные базы данных и получать к ним удаленный доступ, что существенно облегчает и ускоряет проведение такого оперативно-розыскного мероприятия, как «наведение справок».¹

¹ Ховавко С.М. Влияние фактора цифровизации на оперативно-розыскную деятельность органов внутренних: Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2023. – Т. 9 (75). № 4. – С. 283 – 286.

Технологии «больших данных» позволяют: выявлять скрытые связи и закономерности. Системы анализа графиков связей (Social Network Analysis) визуализируют коммуникационные и финансовые цепочки между подозреваемыми, выявляя организационную структуру преступных групп; осуществлять прогнозное моделирование. Алгоритмы машинного обучения, анализируя исторические данные о преступлениях, могут с высокой долей вероятности прогнозировать время, место и тип будущего правонарушения (предикативная полиция). Это позволяет перейти от реагирования к упреждающему патрулированию и профилактике. Проводить комплексный анализ личности; формирование цифрового профиля лица, включающего все его цифровые проявления, дает оперативнику беспрецедентно полную картину о привычках, связях, образе жизни и намерениях объекта.

Искусственный интеллект является естественным развитием технологий Big Data и находит применение в следующих областях:

- Компьютерное зрение. Автоматический анализ видеоархивов с камер наблюдения для распознавания лиц, номерных знаков, моделей автомобилей, отслеживания маршрутов перемещения. Это радикально ускоряет процесс идентификации и поиска.

- Обработка естественного языка (NLP). Автоматический анализ текстовой информации (переписки в мессенджерах, электронных писем, документов) для выявления угроз, сленга, планируемых противоправных действий, определения авторства и эмоционального состояния.

- Криптоанализ. Разработка методов вскрытия и обхода шифрования становится одной из приоритетных задач криминалистических лабораторий.

- Транзакционный анализ. Несмотря на псевдоанонимность блокчейна, анализ цепочек транзакций криптовалют позволяет отслеживать движение средств, идентифицировать кошельки и в конечном итоге – деанонимизировать преступников.

- Технологии цифровой подписи и обеспечения целостности данных. Гарантируют юридическую силу цифровых доказательств, защищают оперативные базы данных от несанкционированного доступа и изменений.

- Применение БПЛА (дронов). Обеспечивают скрытое наблюдение за удаленными и труднодоступными объектами, большими территориями, осуществляют фото- и видеосъемку с высоты.

- Бесконтактные методы съема информации. Технологии, позволяющие регистрировать колебания оконных стекол для прослушивания разговоров в помещении, либо считывать электромагнитное излучение с технических средств.

- Мобильные комплексы радиоэлектронного контроля. Позволяют в режиме реального времени детектировать, пеленговать и анализировать работу незаконных средств связи, глушить каналы управления, например, при обезвреживании взрывных устройств.

Несмотря на очевидные преимущества, процесс трансформации научно-техническое обеспечение сопряжен с рядом серьезных вызовов.

Как отмечает О.А. Вагин «с целью усиления мер противодействия киберпреступности в структуре органов внутренних дел созданы подразделения по борьбе с противоправным использованием информационно-коммуникационных технологий, к основным задачам которых относятся предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе МВД России; анализ данных, содержащихся в информационно-телекоммуникационных сетях, в целях выявления запрещенного контента и противодействия преступности».¹

Таким образом, для повышения эффективности противодействия киберпреступности в условиях цифровизации необходим комплекс правовых и организационных мер. В их числе: ужесточение юридической ответственности за киберпреступления; обеспечение оперативным подразделениям доступа к государственным цифровым базам данных; укрепление межрегионального и международного сотрудничества в этой сфере; совершенствование таких оперативно-розыскных мероприятий, как «снятие информации с технических каналов связи» и «получение компьютерной информации»; разработка новых методик оперативно-розыскной деятельности в виртуальном пространстве; активизация оперативного поиска в интернете на основе технологий «больших данных»; постоянный анализ киберобстановки для выявления новых криминальных тенденций; повышение квалификации сотрудников подразделений по борьбе с IT-преступлениями; оснащение подразделений специальных технических мероприятий современным оборудованием и программным обеспечением; внедрение новых форм виктимологической профилактики киберпреступлений, в том числе с использованием современных информационно-телекоммуникационных технологий. Эффективная профилактика невозможна без правовых и организационных решений, а также без вовлечения общества в повышение осведомленности о рисках использования информационно-коммуникационных технологий. Только объединив усилия государства, правоохранителей и гражданского общества, мы сможем создать безопасную цифровую среду и минимизировать последствия киберпреступности.

¹ Вагин О. А. Оперативно-розыскные мероприятия и использование их результатов: Учебно-практическое пособие / А. П. Исиченко, Г. Х. Шабанов. Москва: Издательство Юрайт, 2025.

Легостаев Вячеслав Петрович,
профессор кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент,
Legostaev-123@yandex.ru

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ ПРИВЛЕЧЕНИЯ ПРЕДСТАВИТЕЛЕЙ КАЗАЧЕСТВА К УЧАСТИЮ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Положения п. 34 ст.13 Закона «О полиции» и ч. 5 ст. 6 Федерального закона «Об оперативно-розыскной деятельности», содержат предписания об участии в подготовке и проведении оперативно-розыскных мероприятий отдельных граждан с их согласия на гласной и негласной основе, имеющих задачи широкого вовлечения граждан в противодействие преступности.

Одной из специфических общественных объединений правоохранительной направленности, являющихся особенностью Северокавказского региона и принимающих непосредственное участие в борьбе с преступностью является Кубанское казачье войско. Правоохранительная деятельность казачьих дружин осуществляется на основании Федерального закона Российской Федерации от 2 апреля 2014 года № 44-ФЗ «Об участии граждан в охране общественного порядка», Закона Краснодарского края от 28 июня 2007 года № 1267-КЗ «Об участии граждан в охране общественного порядка в Краснодарском крае».

В соответствии с названными нормативными актами в Краснодарском крае организована работа по привлечению представителей казачьих дружин, в целях оказания содействия сотрудникам полиции, в охране общественного порядка на улицах, парках, скверах и других общественных местах, в период проведения массовых мероприятий, оперативно-профилактических мероприятий, в том числе по профилактике безнадзорности и правонарушений несовершеннолетних.

В отчете «О совместной деятельности территориальных органов МВД России на районном уровне края и представителей общественных формирований правоохранительной направленности по итогам 1 полугодия 2025 года было отражено, что 46627 казаков приняли на себя обязанности по несению государственной службы, которые в основном несут службу в составе пеших патрульно-постовых нарядов полиции и задействуются в охране общественного порядка на улицах, площадях, в парках, скверах, а также на территории обслуживания транспортной полиции. При этом, при содействии казачьих дружин за отчетный период было раскрыто 13 преступлений, задержаны 3 лица находящиеся в розыске, установлены 5 лиц пропавших без вести, предотвращено 160 случаев детской безнад-

зорности¹. Так, например, создан и действует во взаимодействии с волонтерскими организациями казачий спасательно-поисковый отряд по поиску пропавших людей, в частности детей, ушедших из дому, заблудившихся в лесу, либо при других обстоятельствах.

Другим примером, привлечения казачества к участию и проведению ОРМ служит ежегодное проведение оперативно-поискового мероприятия «Путина», в процессе которого должностные лица ОВД совместно с казачьими дружинами производят обследование водоемов в целях пресечения случаев браконьерства.

Также, пресс-служба МВД России отметила, что российское казачество зачастую привлекается для проведения различных мероприятий по выявлению и пресечению преступлений, связанных с незаконным оборотом наркотических средств. На территории Краснодарского и Ставропольского края, Волгоградской и Ростовской области казачество привлекается к участию в различных рейдах в местах возможного сбыта и производства запрещенных в обороте веществ. Кроме того, представители казачьих дружин задействованы в рейдах по местам массового пребывания молодежи. Наряду с этим казаки противодействуют рекламе наркотиков в информационной среде, в том числе в сети Интернет.

В условиях проведения СВО, незаменимую помощь представители казачества оказывают правоохранительным органам в совместном дежурстве на блокпостах и проверке граждан на предмет незаконного оборота оружия, боеприпасов, взрывчатых веществ и взрывных устройств, профессионально несут службу по охране государственной границы.

Особую роль казачьи общественные формирования играют в контроле за миграционными процессами в обществе, они способствуют получению информации о незаконном пребывании иностранных граждан на территории Краснодарского края, совместно с органами полиции выявляют таковых лиц, собирают материал, препровождают правонарушителей в специальные миграционные центры.

К этому следует добавить, что в последнее время оперативные сотрудники органов внутренних дел все чаще прибегают к привлечению к подготовке и проведению оперативно-розыскных мероприятий лиц, входящих в состав народных дружин и казачьих объединений. В большей степени это неразрывно связано со спецификой деятельности указанных объединений, а именно с их правоохранительной направленностью. Со-

¹ О совместной деятельности территориальных органов МВД России на районном уровне края и представителей общественных формирований правоохранительной направленности по итогам 1 полугодия 2025 года / Информация об опыте взаимодействия органов государственной власти Краснодарского края и Кубанского войскового казачьего общества по организации государственной и иной службы российского казачества. Официальный сайт министерства внутренних дел Российской Федерации. (дата обращения 13.10.2025).

действие представителей казачества в проведении ОРМ проявляется в проведении проверочных закупок оружия, боеприпасов, наркотиков, осмотрах территорий, сооружений, помещений, транспортных средств, проведении наблюдения, опросах и др.

На протяжении ряда лет свою эффективность в области выявления, предупреждения, пресечения, а также раскрытия преступлений демонстрируют результаты сотрудничества органов государственной власти Краснодарского края и Кубанского войскового казачьего общества, основанного на развитом региональном законодательстве и принципах системного, планового и последовательного подхода к организации государственной и иной службы российского казачества, в том числе привлечения казаков к охране общественного порядка и предупреждению преступности¹.

Учитывая роль и значение представителей казачества в обеспечении правопорядка в государстве и борьбе с преступностью, бывший атаман Всероссийского общества Николай Долуда в 2020 году предложил внести изменения в Конституцию и Российское законодательство по созданию отдельного правоохранительного органа – казачью милицию, с наделением полномочий, присущих органам полиции. Свою позицию Н. Долуда обосновал воеизированным характером Кубанского казачьего войска, самостоятельно нести службу по охране общественного порядка, профессионализмом казаков на которых можно положиться. О необходимости расширения полномочий казаков в борьбе с преступностью, Н. Долуда сослался на такие проблемы полиции как: усиливающаяся текучка и большой некомплектом сотрудников полиции, недостаточный профессионализм сотрудников ОВД, их коррумпированность и нарушение дисциплины².

Во-первых, как нам представляется, создание параллельной правоохранительной организации с элементами государственного принуждения, с нашей точки зрения являются мягко говоря не оправданным вследствие того, что во все времена полиция (милиция) довольно успешно справлялась с ролью борьбы с преступностью, при этом опираясь на помощь отдельных граждан и представителей общественности.

Во вторых, в Российском государстве на законодательном уровне действуют и довольно успешно негосударственные правоохранительные организации, осуществляющие, например, частную детективную и охранную деятельность. На практике те же представители казачества являются сотрудниками частных охранных предприятий, участвуют в охране и режиме безопасности государственных и общественных организаций учре-

¹ Информация МВД России об опыте взаимодействия органов государственной власти Краснодарского края и Кубанского войскового казачьего общества по организации государственной и иной службы российского казачества. Режим обращения URL: https://мвд.рф/Informacija_ob_opite_vzaimodejstvija_org. (дата обращения 13.10.2025).

² Казачья милиция в России: реальность или миф 25 января 2020 года <https://dzen.ru/a/XiwSkYbEqQCys2Wk>. (дата обращения 10.10. 2025)

ждений и предприятий, при этом руководствуются Законом №2487-І от 11.03.93 г. «О частной детективной и охранной деятельности в Российской Федерации».

В-третьих, расширение участия казаков в проведении оперативно-розыскных мероприятий возможно только под непосредственным руководством сотрудника оперативного подразделения, поскольку оперативно-розыскная деятельность осуществляется не только гласно, но и негласно, организация и тактика которой составляет сведения, содержащие государственную тайну.

В-четвертых, что касается вопроса расширения полномочий представителей казачества в противодействии преступности посредством участия их в оперативно-розыскных мероприятиях, то нам видится аналогия с деятельностью помощника судьи на которого возлагаются обязанности по организации подготовки к судебному разбирательству.

С учетом изложенного, представляется оправданным ввести институт помощника сотрудника полиции в число которых привлекать представителей казачества для участия в подготовке и проведению ОРМ, а также изучения его личностных и деловых качеств как будущего кандидата на службу в должности оперативного сотрудника полиции.

П. 34 ст.13 Закона «О полиции» и ч. 5 ст. 6 Федерального закона «Об оперативно-розыскной деятельности», помимо предписаний о привлечении отдельных граждан, должностных лиц и специалистов к ОРМ предлагаем дополнить названные правовые нормы положениями об участии в оперативно-розыскной деятельности «представителей общественности» к которым на сегодняшний день и относятся представители казачества.

Лузько Дмитрий Николаевич,
заместитель начальника кафедры
оперативно-разыскной деятельности и
специальной техники в ОВД
Восточно-Сибирского института МВД России,
кандидат юридических наук,
тел.: 8-983-424-1655; e-mail: luzko-dima@mail.ru

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СИНТЕТИЧЕСКИХ МЕДИА (DEEPFAKE) В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

В условиях информационного шума и повсеместного распространения недостоверных данных, прозрачность становится ключевой ценностью для потребителей¹. Сгенерированный нейросетью медиаконтент все больше стирает грань между реальностью и вымыслом, оказывая воздействие на мышление и образ жизни людей². В современную эпоху, когда «увидеть – значит поверить», рост дипфейков – высокореалистичных и часто обманчивых медиа, созданных искусственным интеллектом, – формирует серьезные проблемы как для отдельных лиц, организаций так и в ближайшем будущем может влиять на безопасность государств.

Этимологический контекст понятия «deepfake» представляет собой симбиоз слов «deep learning» (глубинное обучение) и слова «fake» (подделка), образуя дословно «подделка на глубоком уровне».

Глубокие фейки относятся к синтетическим медиа, включающим изображения, видео и аудио, созданным с использованием алгоритмов искусственного интеллекта (далее – ИИ), чаще всего – генеративных нейросетей, которые постоянно развиваются и совершенствуются.

И хотя сама по себе технология нейтральна, она обладает широким спектром возможностей, которыми могут воспользоваться лица не владеющие специализированными знаниями³ (обычные пользователи), способные образовывать контент различного содержания и целевой направленности, в том числе криминального характера (например, для распространения дезинформации, совершения мошенничества, вымогательства, нанесения

¹ Музыкант, В. Л. Фейковые новости как основа дезинформации на современных медиаплатформах / В. Л. Музыкант, А. М. Мукситх, К. Барек // Культура в фокусе научных парадигм, 2022. С. 14-15.

² Ромаданова С.В., Мухаметшина Н.С. Влияние нейросетей на формирование медиареальности // Вестник Самарского Государственного Технического Университета. Серия «Философия», 2023. Т. 5. № 2. С. 36.

³ Дронова, О. Б. Современные технические средства выявления дипфейков / О.Б. Дронова // XII Балтийский юридический форум «Закон и правопорядок в Третьем тысячелетии» : Материалы международной научно-практической конференции, Калининград, 15 декабря 2023 года. – Калининград: Санкт-Петербургский университет МВД РФ, 2024. С. 9-10.

ущерба репутации, манипулирование общественным мнением, поддержка нарративов экстремистских и террористических групп, разжигание социальных и политических волнений и т. д.).

Фальсифицированные аудиовизуальные материалы, обладая высокой степенью реализма представляют значительную угрозу вследствие их широкого охвата и стремительной скорости распространения и как отмечает ряд российских исследователей подобные вызовы диктуют необходимость правового регулирования рассматриваемой сферы общественных отношений. Цифровая эпоха задаёт вопросы, на которые национальным законодателям необходимо оперативно искать ответы¹.

В данном аспекте вызывает интерес прогрессивный опыт Китайской Народной Республики (далее – КНР) в правовом регулировании рассматриваемого вопроса. Так, в январе 2023 года вступило в силу Положение о дипфейках (далее – Положение)², которое предусматривает инновационные изменения в политику использования сгенерированного контента.

В нормативном правовом акте сформулирован ряд правил, для поставщиков услуг глубокого синтеза, обязывающий обеспечивать информационную безопасность; создавать и совершенствовать системы управления и меры технической поддержки; формулировать правила публичного управления и соглашения платформы; проверять подлинность реальной идентификационной информации пользователей; усиливать управление контентом глубокого синтеза, а также создавать и совершенствовать механизмы опровержения слухов, способы подачи апелляций, жалоб и отчетности.

Как отмечает, в своей научной работе доктор Ли Яо «введение данного Положения знаменует собой тот факт, что глубокий синтез стал первым типом алгоритмических услуг, который был специально законодательно закреплён в области алгоритмического управления в Китае в связи с его важностью и высоким риском»³.

Таким образом мы можем констатировать, что предложенные меры направлены на то, чтобы сделать процесс использования технологий дипфейк прозрачным, предотвратить их применение в незаконной деятельно-

¹ Батоев В. Б. Об использовании технологии «Deepfake» в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2023. – № 1 (61). – С. 70-76; Дремлюга Р. И. и др. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая // Азиатско-Тихоокеанский регион: экономика, политика, право, 2022. Т. 24. №. 4. С. 92.

² Положение о глубоком интегрированном управлении информационными интернет-услугами // Администрация киберпространства Китая: сайт. URL: https://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm (дата обращения: 29.10.2025).

³ Ли Я. Использование технологии «дипфейк» в Китае: проблемы правового регулирования и пути их решения // Lex russica, 2024. Т. 77. №. 11. С. 23.

сти. Указанный законодательный опыт КНР, на наш взгляд, необходимо учесть в отечественной правовой парадигме.

Стоит отметить, что в апреле 2025 года в Государственную Думу Федерального Собрания Российской Федерации вносился законопроект «О внесении изменений в статью 63 Уголовного кодекса Российской Федерации», в котором предусматривалось ответственность за совершение преступления с использованием искусственного интеллекта. В пояснительной записке к проекту закона инициаторы отмечали, что одним из наиболее опасных направлений мошенничества стало использование искусственного интеллекта для создания «дипфейков» – технологий, позволяющих подделывать лица и голоса людей¹. Но проект не нашел своей поддержки у законодателя, хотя на наш взгляд, его принятие создало бы правовую основу для борьбы с данным явлением.

Помимо этого, считаем целесообразным рассмотреть вопрос использования правоохранительными органами возможностей рассматриваемых технологий, как перспективный инструментарий в противодействии преступным проявлениям.

Так, в рамках решения задач оперативно-розыскной деятельности на основе создания синтетических медиа (аудио, видео, изображения) возможна дезинформация участников криминальной среды (например, генерация фальшивых видеозаписей или аудиосообщений от «авторитетных лиц» преступного мира, с целью установления планов или конфликтов внутри группировок; распространение ложных сведений о действиях правоохранителей, чтобы вынудить преступников изменить тактику и раскрыть себя и т. д.). Иначе говоря, применять дипфейки, как способ влияния на лиц представляющих оперативный интерес, с целью воздействия на их сознание и поведение, в интересах оперативных подразделений.

При этом следует констатировать, что как с правовой, так и с морально-этической стороны введение противодействующей стороны в заблуждение, исключаящее прямой обман и строящееся на хитрости, приемлемо в теории и практике оперативно-розыскной деятельности². Противостояние преступности априори носит нравственный характер, соответственно, использование методов, позволяющих эффективно бороться с криминальными проявлениями, является морально допустимым и обу-

¹ Система обеспечения законодательной деятельности: сайт. URL: <https://sozd.duma.gov.ru/bill/885494-8>.

² Воронин, С. Э. Нравственно-психологические основы оперативно-розыскной деятельности и уголовного судопроизводства : монография / С. Э. Воронин. – Красноярск : АНО ВО СИБУП, 2018. 168 с.; Дубоносов, Е. С. Дезинформация криминальной среды при осуществлении оперативно-розыскной деятельности // Известия Тульского государственного университета. Экономические и юридические науки, 2021. № 2. С. 27-33.

словленным потребностью соблюдения конспирации, нейтрализации оказываемого противодействия.

Кроме того, рассматриваемые технологии можно использовать для проникновения в преступную среду (например, создание цифровых «агентов» для онлайн-разведки, способствующих выявлению намерений лидеров и участников криминального мира, оказания на них определенного влияния и возможного разоблачения).

Также с помощью дипфейка возможен поиск разыскиваемых преступников (например, «оживление» фотографии; создание видео с их предполагаемой текущей внешностью, учитывая сгенерированные возрастные изменения, если преступник скрывается много лет).

Для обучения правоохранителей и получения практических навыков возможно применение изучаемых технологий при создании реалистичных тренировочных сценариев с участием «дипфейковых» преступников, в том числе при захвате заложников, а также моделирование криминальных ситуаций для отработки тактики ведения с ними переговоров.

Подводя итог нашему исследованию, необходимо отметить, что технологии «deepfake» являются эффективным инструментом противодействия преступности, но их применение требует тщательной правовой регламентации, технологического контроля и этической оценки. Внедрение таких методов в деятельность правоохранительных органов может значительно повысить результативность борьбы с криминальными проявлениями, но также необходимо предусмотреть риски злоупотреблений и меры защиты от ответного использования указанных технологий уголовным элементом.

С целью совершенствования отечественной юридической системы считаем целесообразным изучение зарубежного опыта в данном вопросе, который обуславливается наличием нормативных положений в праве других стран, и уже предполагает некоторую апробированность выбранного ими пути развития. В свою очередь это дает реальную возможность отечественным исследователям применять сравнительно-правовой метод и принимать оптимальные решения при использовании рассматриваемых технологий в противодействии преступности.

Меретуков Гайса Мосович,
заведующий кафедрой криминалистики
ФГБОУ ВО «Кубанский
государственный аграрный
университет имени И. Т. Трубилина»,
доктор юридических наук, профессор
тел.: 8 (918) 438-51-49: e-mail: crimkubgau@mail.ru

Меретуков Айдамир Гайсович,
доцент кафедры уголовного права
Краснодарского университета МВД России,
кандидат юридических наук
тел.: 8 (918) 395-66-67: e-mail: crimkubgau@mail.ru

ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ И МЕХАНИЗМ ОЦЕНКИ ОПЕРАТИВНОЙ ОБСТАНОВКИ

Рост туристического потока в курортные регионы России, концентрация материальных ценностей и людей, повышенная уязвимость инфраструктуры создают благоприятные условия для совершения преступлений. Это обуславливает необходимость совершенствования оперативно-розыскной деятельности на данных территориях. Данной проблематике посвящены труды ученых и практиков, занимавшихся вопросами ОРД: А. Ю. Шумилов, В. В. Кальницкий, Р. С. Белкин), а но к сожалению недостаточно изучены оценочные компоненты, а именно вопросы связанные с механизмом оценки оперативной обстановки как общие в масштабе субъекта региона, так и частные вопросы связанные в масштабе города, района, поселка или конкретного предприятия. Например, специфическими факторами, определяющими оперативную обстановку в курортной зоне являются: сезонность и маятниковая миграция, т. е. резкое увеличение населения, изменение его половозрастной и социальной структуры, криминогенные факторы (характерные виды преступлений (кражи, мошенничества, незаконный оборот наркотиков, нарушения общественного порядка, преступления в сфере оказания услуг); деятельность организованных преступных групп, «залетных» преступников; социально-экономические факторы (напряженность на рынке труда, высокие цены, концентрация объектов досуга, торговли и общепита); инфраструктурные факторы (уязвимость мест массового пребывания людей (пляжи, вокзалы, аттракционы), сложность транспортной системы); транснациональный аспект: наличие иностранных туристов, что может обуславливать международную преступность.

Особенности проявления основных угроз безопасности в курортной зоне (можно использовать статистические данные по конкретному регио-

ну, например, Краснодарскому краю, Крыму). Такие же особенности присущие производственной деятельности как временного и постоянного вида деятельности и качественного состава трудового коллектива.

Теоретико-правовые основы – это тот «скелет», на котором держится вся оперативно-розыскная деятельность (ОРД). Без их четкого понимания и анализа невозможно ни эффективно применять закон, ни совершенствовать его. С принятием Закона Российской Федерации «Об оперативно-розыскной деятельности в Российской Федерации» от 13 марта 1992 года № 2506-1 и особенно с принятием окончательного, действующего варианта Федерального закона «Об оперативно-розыскной деятельности» (далее в тексте ФЗ РФ «Об ОРД») №144-ФЗ от 12 августа 1995 г. некоторые ученые осторожно высказывают мнение о возможном формировании оперативно-розыскного права. К этому вопросу существует своя предистория. Например, в 20-е годы прошлого столетия практические работники высказали мнение придать оперативно-розыскной деятельности НКВД правовую основу. В 1920 г., 11 февраля на заседании представителей Народного Комиссариата юстиции и Народного Комиссариата внутренних дел рассматривался вопрос об объединении следственных аппаратов НКЮ с уголовно-розыскными подразделениями НКВД. В данной ситуации предполагалось следователю придать полномочия контроля за процедурой получения криминалистической значимой информации (доказательственной или ориентирующей) и ее легализация в материалах уголовного дела. В свете этих идей в апреле 1920 г. Коллегия НКВД постановила признать необходимым слияния уголовного розыска и следствия. Для этого НКВД подготовила Положение и Инструкцию следственно-розыскной милиции. Однако, в июне 1920 г. на заседании 3-го Всесоюзного съезда работников юстиции НКЮ не поддержал эту идею¹. Позднее в 70-х г. прошлого века В. А. Михайлов и А. К. Гаврилов пришли к выводу о необходимости введения в следственные подразделения милиции должность «следственный инспектор» с правом проведения оперативно-розыскных мероприятий по заданию и под руководством следователя². До принятия Федерального закона «Об ОРД» деятельность органов, осуществляющие оперативно-розыскную деятельность руководствовались нормативно-правовыми актами МВД, КГБ СССР и других ведомств³. На основе этих нормативно правовых актов А.Г. Лекарь первым сформулировал определение понятия оперативно-

¹ С.: более подробно работу Белозеров Ю. Н., Чугунов В. Е., Чувилев А. А. Дознание в органах милиции и его проблемы. М., 1972. С. 11–16.

² Михайлов В. А. К вопросу об улучшении деятельности предварительного следствия// XXV съезд КПСС о задачах дальнейшего укрепления законности и правопорядка. Волгоград. 1972. С. 110–112.; Гаврилов А. К. Раскрытие преступлений на предварительном следствии. Волгоград, 1967. С. 189–193.

³ В данной ситуации авторы не приводят ссылки, так как нормативно-правовые акты МВД, КГБ СССР того времени носили гриф «ДСП», «С» или «СС».

розыскной деятельности¹. В это же определение Д. В. Гребельский дополнил «субъекты ОРД»², а В. А. Лукашов указал на отсутствие указания на организационно-управленческий аспект³. Обобщив мнения А. Г. Лекаря, Д. В. Гребельского, В. А. Лукашова и других А. Е. Казак предложила собственное уточненное определение понятия оперативно-розыскной деятельности как, «направленная на защиту жизни, здоровья, прав и свобод личности, собственности, безопасности общества от преступных посягательств»⁴. С принятием действующего УПК РФ учеными внесены предложения по совершенствованию оперативно-розыскной деятельности. Причиной явилось включение в УПК РФ статью 89 «Использование в доказывании результатов оперативно-розыскной деятельности» (2000 г.) и п.36(1) в ст. 5 УПК понятие результаты оперативно-розыскной деятельности, т. е. «сведения, полученные в соответствии с ФЗ об оперативно-розыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия и суда» введенный Федеральным законом от 04.07.2003 г. № 92-ФЗ. На этой основе и с учетом мнения ряда известных ученых и специалистов в сфере ОРД⁵, Е. В. Кузнецов предлагает активизировать формирование новой «отрасли права»⁶. Теоретико-правовые основы оперативно-розыскной деятельности и механизм реализации методики изучения и оценки оперативной обстановки, а также другие аспекты на достаточном уровне рассмотрены в учебнике «Оперативно-розыскная деятельность»⁷. Таким образом, существующая модель теоретико-правовой основы оперативно-розыскной деятельности способна обеспечить механизм оценки оперативной обстановки на любом уровне.

¹ Лекарь А. Г. Основы оперативно-розыскной деятельности. Учебник. М., 1966. С. 8.

² Гребельский Д. В. Теоретические основы и организационно-правовые проблемы оперативно-розыскной деятельности органов внутренних дел. М., 1977. С. 28.

³ Лукашов В. А. Введение в курс «Оперативно – розыскная деятельность органов внутренних дел». Киев, 1976. С. 23.

⁴ Казак А. Е. Оперативно-розыскная деятельность органов внутренних дел и прав человека: автореф. дис. ... канд. юр. наук., СПб, 1997. С.12.

⁵ Чувилев А. А. Оперативно-розыскное право. – М.: НОРМА-ИНФРА- М., 1999. С. 2.; Шаповалов А. А. Отрасль современного российского права(вопросы теории): дис. ... канд. юр. наук.- М., 2011. С. 115–118 и др.

⁶ Кузнецов Е. В. Теоретические основы формирования отрасли оперативно-розыскного права : автореф. дис. ...канд. юр. наук., Волгоград, 2014. – 25 с.

⁷ Меретуков Г. М. Оперативно – розыскная деятельность: учебник для студентов вузов, обучающихся по направлению «Юриспруденция» /Г. М. Меретуков, А.М. Кустов, С. А. Данильян; под ред. Г. М. Меретукова. – М.: ЮНИТИ –ДАНА, 2025. – 191 с.

По мнению С. И. Ожегова и Н. Ю. Шведовой слово «механизм» означает, «система, устройство, определяющее порядок какого-нибудь деятельности» или «последовательность состояний, процессов, определяющих собою какой-нибудь действие, явление»¹. Проведенный анализ научной и специальной литературы, а также опыт работы авторов в уголовном розыске² позволяет высказать мнение, что механизм оценки оперативной обстановки – это «мозг» и «нервная система» оперативно-розыскной деятельности органов внутренних дел. Именно от качества этой оценки зависит распределение сил и средств, выбор форм и методов оперативно-розыскной деятельности, а в конечном счете – выявление, раскрытие и расследование преступлений и обеспечение безопасности государства и общества. Для органов и должностных лиц, осуществляющих оперативно-розыскную деятельность в системе МВД, ФСБ, СВР, ФСИН, ФТС, ГРУ МО и ФСО оценка и прогнозирование оперативной обстановки является ежедневной задачей.

Для системной оценки и прогноза оперативной обстановки на обслуживаемом административно-территориальном районе необходимо знать следующие показатели:

1) границу обслуживаемой территории, количество проживающих, из них мужчины и женщины, взрослые, несовершеннолетние и малолетние; количество ранее судимых и по каким видам преступлений, из них рецидивистов; количество лиц, склонных к совершению преступлений или иных правонарушений; миграционный процесс (количество обучающихся и в каких вузах, работающие на предприятиях, прибывающие и убывающие в течение дня на водном, воздушном, ЖД и автомобильном транспорте) и т. д.;

2) наличие вузов, промышленных, строительных и иных предприятий и их вид деятельности (выпускаемой продукции и их значимость; качественный и количественный контингент);

3) наличие лесопосадок, лесных и водных угодий;

4) уровень организованной преступности;

5) уровень преступности, раскрываемость преступлений с судебной перспективой;

6) время и место совершения отдельных видов и групп преступлений и нарушений общественного порядка;

7) наиболее распространенные способы совершения преступлений, вещей и предметов, наиболее часто являющиеся объектами преступного посягательства, каналы сбыта добытого преступным путем;

¹ Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка / Российская академия наук. Институт русского языка им. В. В. Виноградова. – 4 – е изд., дополненное М.: ООО «ИНФОТЕХ», 2010. С. 329.

8) состояние профилактики, состояние административной практики и гражданско-правовые отношения, рассматриваемые в арбитражном и гражданском судопроизводстве;

9) наличие межведомственного комплексного плана мероприятия;

10) наличие межведомственной комиссии правоохранительных органов с участием представителей органов власти и управления возглавляемой прокурором района, города;

11) знание оперативной обстановки соседних административно-территориальных территорий;

12) количественное и качественное состояние личного состава полиции, отдела СК РФ по субъекту, прокуратуры, суда и адвокатуры, а также подразделений Росгвардии;

13) обеспеченность личного состава транспортом, средствами связи, вооруженность и т.д.;

14) тревожные планы: «Гром», «Перехват», «Ураган», «Сирена» и т. д.;

15) наличие постоянно действующих СОГ;

16) координационные планы взаимодействия с соседними районами;

17) обеспеченность локальными нормативно-правовыми актами обеспечивающими правопорядок, законность, соблюдение прав человека и гражданина.

Применительно к деятельности оперативно-розыскных аппаратов такие данные должны включать в себя: количество предотвращенных и подготавливавшихся преступлений; количество пресеченных покушений на преступления; количество раскрытых преступлений (отдельно замаскированных и совершенных в условиях очевидности); количество разыскиваемых скрывшихся преступников, лиц пропавших без вести и другие факторы; количество конфиденциальных лиц и их статус, сведения о них и их движения, качественном состоянии и результатах выполнения ими заданий (поручений); количество заведенных материалов оперативного учета, а также реализованных материалов собственными силами и с участием органа предварительного следствия и другие с учетом требований вышестоящего руководства.

Оценка оперативной обстановки (ОО) – это фундамент для планирования, принятия управленческих решений и эффективного использования сил и средств оперативных аппаратов. В ходе оценки оперативной обстановки следует использовать следующие методы и средства оценки: статистические методы (анализ статистики преступлений); социологические методы (опросы, анкетирование); аналитические методы (сравнение, группировка, прогнозирование); оперативно-тактические методы (проверочные закупки, оперативное внедрение, опрос граждан); технические средства (системы видеонаблюдения, прослушивания, анализ цифровых данных). Для этих целей необходимо использовать информационную основу оценки, т. е.: результаты ОРМ (ст. 6 ФЗ «Об ОРД»); данные официальной

статистики (МВД, Росстат); сведения от органов местного самоуправления, администраций курортов, предприятий гостеприимства; информация из открытых источников (социальные сети, форумы и т. п.).

Оценка оперативной обстановки позволяет следующий алгоритм действия руководящего состава органа, осуществляющего оперативно-розыскную деятельность. Таковыми могут быть: сбор информации -> анализ и синтез данных -> выявление тенденций, закономерностей и угроз -> формирование вывода (оценки) -> принятие управленческих решений (планирование ОРМ, профилактических мероприятий).

Проведенный анализ научной, специальной и собственного опыта работы в уголовном розыске позволяет предложить формулировку авторского определения понятия оперативная обстановка – это «совокупность условий и факторов, характеризующих состояние, структуру, динамику и тенденции преступности на определенной территории (или в определенной сфере) за конкретный временной период, влияющих на выполнение задач ОРД и требующих адекватного реагирования со стороны оперативно-розыскных подразделений». Выявлены некоторые проблемы: отсутствие единой методики оценки оперативной обстановки на законодательном уровне; высокая доля латентной преступности, искажающая реальную картину; ведомственная разобщенность и проблемы информационного обмена; недостаточный уровень аналитической подготовки части оперативных сотрудников; формализм в подготовке отчетных документов об оперативной обстановке.

Кроме этого авторы, в целях совершенствования деятельности органа, осуществляющего оперативно-розыскную деятельность территориальных органов внутренних дел предлагают: создание единых межведомственных информационных центров в системе МВД; разработка и внедрение специализированных программно-аналитических комплексов для мониторинга оперативной обстановки в режиме реального времени; усиление взаимодействия с частными охранными предприятиями и службами безопасности объектов, инфраструктуры по различным сферам вида деятельности на территории; проведение ежеквартальных оперативных совещаний с анализом обстановки на территории. Далее, закрепить в ФЗ "Об ОРД" базовое определение "оперативной обстановки" и принципов ее оценки; разработать и внедрить межведомственные стандарты и программные комплексы для сбора и анализа информации об оперативной обстановке; усилить аналитическую составляющую в работе оперативных подразделений; активнее использовать методы криминологического и оперативно-розыскного прогнозирования состояния преступности, при этом проводить сравнительный анализ за предыдущие периоды.

Миронов Дмитрий Александрович,
слушатель 5 курса Крымского филиала
Краснодарского университета МВД России
тел. +7(978)287-95-71

Ерохин Роман Анатольевич,
старший преподаватель кафедры уголовного права
и оперативно-розыскной деятельности органов внутренних дел
Крымского филиала Краснодарского университета МВД России
e-mail: roman_erokhin@mail.ru; тел. +7(910)019-68-88

ЗНАЧЕНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ УСТАНОВЛЕНИЯ И РОЗЫСКА ЛИЦ, СОВЕРШИВШИХ ПРЕСТУПЛЕНИЯ

Современная оперативная обстановка характеризуется беспрецедентной мобильностью преступных элементов, глобализацией криминальной деятельности и повсеместным использованием цифровых средств конспирации. В этих условиях традиционные, основанные на анкетных данных и показаниях свидетелей, методы установления и розыска лиц, совершивших преступления, демонстрируют растущую неэффективность. Преступники научились легко скрывать или подделывать документы, использовать анонимные каналы связи и активно противодействовать классическим оперативно-тактическим комбинациям. Ответом на этот вызов со стороны правоохранительной системы стал стратегический переход к технологиям, позволяющим осуществлять идентификацию личности на основе ее уникальных, неизменяемых и объективных характеристик. Таким образом, биометрические технологии, основанные на измерении устойчивых физиологических и поведенческих параметров человека, вышли на передний план, трансформируясь из узкоспециального инструмента криминалистики в краеугольный камень и системообразующий элемент всего научно-технического обеспечения оперативно-розыскной деятельности. Их интеграция в повседневную практику знаменует собой переход от субъективных, опосредованных методов работы к объективным, автоматизированным и высокоточным процедурам, функционирующим в режиме, приближенном к реальному времени.

Исторически первой и наиболее долгое время доминирующей биометрической технологией в правоохранительной практике была дактилоскопия. Однако на протяжении десятилетий ее применение носило сугубо реактивный и вспомогательный характер. Отпечатки пальцев, изъятые с места преступления, направлялись в экспертно-криминалистическое подразделение для сравнительного анализа с картотекой ранее судимых лиц. Этот процесс был длительным, требовал ручного труда и был эффективен

лишь против рецидивистов, чьи данные уже находились в базе. Цифровая революция конца XX – начала XXI веков кардинально изменила эту парадигму. Оцифровка биометрических данных и создание мощных автоматизированных информационно-поисковых систем (АИПС) позволили интегрировать биометрию в контур оперативно-розыскной деятельности, сделав ее инструментом не только раскрытия, но и предупреждения преступлений.

Ключевым следствием этой трансформации стал переход от реактивной идентификации к проактивной и оперативной. Если раньше сравнение отпечатка, найденного на месте кражи, могло занять недели, то сегодня оперативник, используя мобильный сканер, может установить личность задержанного за считанные минуты, прямо на месте происшествия. Биометрические данные превратились в стержневой элемент, вокруг которого формируется комплексный цифровой портрет разыскиваемого лица. Этот портрет объединяет в единой системе биометрические шаблоны, криминальные связи, финансовые операции, данные о перемещениях и коммуникациях, создавая целостную и динамичную модель для анализа и планирования оперативных мероприятий. Кроме того, унификация стандартов и форматов данных обеспечила беспрецедентный уровень межведомственного и межрегионального взаимодействия. Биометрический след, обнаруженный в одном субъекте Федерации, мгновенно проверяется по единым федеральным и даже международным базам, что радикально повышает вероятность установления лица, совершающего преступления в разных регионах.

Современная система биометрического научно-технического обеспечения представляет собой комплекс взаимодополняющих технологий, каждая из которых решает свой круг оперативных задач. Несмотря на появление новых методов, дактилоскопия остается одним из самых надежных, законодательно урегулированных и массово применяемых методов идентификации. Современные автоматизированные дактилоскопические идентификационные системы (АДИС), такие как «Папилон» или аналоги, используемые органами внутренних дел, оперируют базами данных, содержащими десятки миллионов дактилокарт. Скорость обработки запроса исчисляется секундами, а точность – долями процента. Внедрение биометрических систем в оперативно-розыскную работу обладает существенным ресурсом для усиления результативности противодействия правонарушениям. В основе биометрии лежат индивидуальные физиологические и поведенческие параметры личности, например, рисунок пальцев, структура радужной оболочки, характеристики голоса и иные признаки, способные являться персональным «цифровым идентификатором».

Включение биометрических сведений в оперативно-розыскные мероприятия даёт возможность идентифицировать преступника с исключительной точностью и скоростью, что обеспечивает своевременное реагиро-

вание на инциденты и сокращает сроки расследования. Это позволяет уменьшить временные затраты на розыск, усиливает доказательственную базу и оптимизирует борьбу с преступностью.

К ситуациям, разрешающим обработку персональных сведений без согласия субъекта, относятся, в частности, обстоятельства, установленные законодательством об оперативно-розыскной работе, о противодействии терроризму и др.

Биометрические параметры человека условно классифицируются на 2 категории: статические: папиллярный узор пальцев, венозный рисунок кисти, сетчатка глаза, радужная оболочка, изображение лица; динамические: голос, рукописный почерк, клавиатурный почерк, цифровой почерк, походка, сердечный ритм, распознавание жестов.

Среди биологических характеристик для целей биометрической идентификации на современном уровне развития наиболее применима ДНК. Сведения ДНК содержатся в Федеральной базе данных геномной информации (ФБДГИ), где по состоянию на 1 января 2020 г. насчитывалось 965 315 ДНК-профилей, ежегодно ФБДГИ увеличивается на сотни генотипов.

В соответствии с последними законодательными инициативами планируется расширить перечень лиц, которые подлежат обязательной геномной регистрации – предлагается собирать ДНК-карты в том числе у всех лиц, осужденных за совершение преступлений в виде лишения свободы; подозреваемых и обвиняемых; подвергнутых административному аресту¹. В случае реализации этой законодательной инициативы ФБДГИ ежегодно будет пополняться данными о 1,8 млн лиц.

Дактилоскопическая регистрация на сегодняшний день существует в форме добровольной и обязательной регистрации, однако также прослеживается тенденция расширения перечня категорий лиц, подлежащих обязательной дактилоскопической регистрации².

Практическим примером использования биометрических систем в оперативной работе служит применение технологий распознавания лиц для выявления преступников в местах массового скопления людей. Кроме того, биометрические параметры могут применяться для организации доступа на охраняемые объекты, проверки сотрудников и наблюдения за подозреваемыми лицами.

Вместе с тем, при эксплуатации биометрических систем требуется учитывать аспекты защиты и конфиденциальности информации для предотвращения злоупотреблений и нарушений прав личности. Также

¹ Волчихин В. И., Иванов А. И., Фунтиков В. А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза, 2005

² Гейндль Р. Дактилоскопия и другие методы уголовной техники в деле расследования преступлений / Пер. с нем. В. В. Шпеера / Под ред. А. И. Крюкова. М., 2019.

важно сформировать детальные регламенты и порядок применения биометрических технологий в оперативно-розыскной работе для гарантии их продуктивного и правомерного использования.

Таким образом, внедрение биометрических систем в оперативно-розыскную деятельность служит действенным инструментом для установления преступников и усиления общественной безопасности, но требует взвешенного подхода к обеспечению защиты сведений и соблюдению законных интересов граждан.

Структура технического распознавания личности на базе биометрической идентификации включает следующие компоненты:

- аппаратно-программные комплексы, содержащие технические средства записи биометрических параметров лиц, представляющих оперативный интерес (фото-, видео-, аудиооборудование и другие устройства фиксации);
- специализированное программное обеспечение (для идентификации по чертам лица, особенностям походки, голосовым характеристикам и т.д.);
- актуальные банки биометрических данных, интегрированные с аппаратно-программными комплексами.

По методу записи биометрических персональных сведений лиц, представляющих оперативный интерес, для последующего технического распознавания идентификация может производиться как при прямом контакте лица с техническим средством фиксации (например, сканер папиллярного узора, сканер радужной оболочки), так и удалённо (например, видеокамера для захвата изображения лица, походки, глаз).

Наиболее динамично развивающимся и публично обсуждаемым направлением является распознавание лиц. Эта технология эволюционировала от сравнения статических фотографий до сложных систем видеоаналитики, работающих в реальном времени. Интеграция алгоритмов распознавания лиц с сетями уличного, транспортного и объектового видеонаблюдения, включая камеры с встроенными модулями искусственного интеллекта, позволяет создавать «цифровые барьеры». Такие системы в автоматическом режиме сканируют потоки людей в аэропортах, на вокзалах, стадионах и иных местах массового скопления людей, мгновенно сверяя обнаруженные лица с федеральными розыскными и оперативными базами данных. Важным аспектом является кроссплатформенная идентификация, при которой алгоритмы способны сопоставить портретное фото из уголовного розыска с изображением из социальной сети, кадром с камеры видеорегистратора или случайным селфи, определяя тем самым не только

местоположение объекта, но и его социальные связи и привычки, формируя его цифровой след.¹

Хотя эти технологии пока не столь массовы, их оперативный потенциал крайне высок. Сканирование радужной оболочки глаза, обладающее высокой точностью и устойчивостью к подделкам, уже сегодня применяется для контроля доступа на режимные объекты МВД и иных силовых ведомств. Перспективно ее использование в мобильных комплексах, например, для быстрой и достоверной идентификации лиц в полевых условиях, особенно когда дактилоскопия затруднена.

Голосовая биометрия приобретает важнейшее значение при осуществлении оперативно-розыскных мероприятий, связанных с контролем телефонных переговоров. Современные программно-аппаратные комплексы способны не только идентифицировать целевого говорящего в значительном массиве аудиоданных, автоматически определяя его высказывания, но и выполнять стресс-анализ, устанавливая эмоциональное состояние говорящего, что может свидетельствовать о подготовке к противоправным действиям.

Широкое внедрение биометрических технологий в практику оперативно-розыскной деятельности сопровождается рядом сложных проблем, требующих комплексного решения.

Наиболее актуальной остается проблема нормативно-правового регулирования и этических аспектов. Массовый сбор, хранение и обработка биометрических данных граждан по своей природе представляют собой вмешательство в частную жизнь. Существует тонкая грань между повышением эффективности противодействия преступности и созданием системы тотального наблюдения. Требуется четкое законодательное определение целей, оснований, процедур и сроков хранения биометрической информации, а также механизмов судебного и прокурорского надзора за ее использованием. Перед обществом и законодателем стоит задача найти баланс между обеспечением безопасности и защитой прав и свобод личности.

Технические challenges (вызовы) включают в себя проблему «цифрового шума» и ошибок алгоритмов. Ложноположительное срабатывание системы распознавания лиц может привести к незаконному задержанию и моральному ущербу для гражданина, в то время как ложноотрицательное — к срыву операции и уходу преступника от ответственности.² Точность алгоритмов критически зависит от качества исходных данных (например, размытое или засвеченное изображение с камеры) и от репрезентативности

¹ Барашко Е. Н., Булах Д. А. Анализ биометрических систем и систем идентификации. / Научные достижения и открытия современной молодежи. Сборник статей V Междунар. научно-практ. конф. МЦНС «Наука и Просвещение» 2022. С. 434.

² Использование систем распознавания лиц в деятельности органов внутренних дел: монография / под ред. В. П. Лапина. — М.: Академия управления МВД России, 2023. — 198 с.

обучающих выборок, так как алгоритмы, обученные преимущественно на данных одной этнической группы, могут хуже работать с другими. Не менее важной задачей является обеспечение технической совместимости и интеграции разнородных биометрических систем, находящихся в ведении разных министерств и ведомств (МВД, ФСБ, Росгвардия, ФСИН), а также защита этих централизованных хранилищ от кибератак, последствия которых могут быть катастрофическими.

Наконец, наблюдается постоянная «гонка вооружений» между правоохранительными органами и преступным миром. Последний активно ищет и находит методы противодействия биометрии: от использования специальных маскировочных гримов и контактных линз, искажающих рисунок радужки, до применения глушителей голосовых модуляторов и разработки методов хищения или подделки биометрических шаблонов.

Несмотря на существующие challenges, вектор развития биометрического научно-технического обеспечения очевиден и направлен на дальнейшую глубинную интеграцию и повышение интеллектуальности систем.

Первоочередной задачей является создание Единой федеральной биометрической платформы, которая бы агрегировала в себе все виды биометрических данных (от дактилоскопии и ДНК до лиц и голоса) и предоставляла к ним унифицированный доступ всем уполномоченным правоохранительным и специальным органам. Это позволит сформировать целостный цифровой портрет гражданина для целей оперативно-розыскной деятельности и исключить дублирование и разрозненность информации.

Следующим шагом станет активное развитие поведенческой биометрии. Анализ таких динамических характеристик, как походка, ритм и сила нажатия клавиш при печати, динамика подписи или даже манера вождения автомобиля, открывает возможности для дистанционной, непрерывной и скрытой идентификации и верификации личности, что особенно ценно при наблюдении за объектами, уклоняющимися от прямой фиксации.

Глубокая интеграция искусственного интеллекта переведет биометрию на качественно новый уровень. Речь идет уже не просто о распознавании, а о прогнозной аналитике. AI-системы, анализируя биометрические и контекстные данные (например, микровыражения лица в сочетании с геолокацией и финансовыми операциями), смогут строить прогнозные модели поведения разыскиваемых лиц, оценивать их намерения и потенциальную опасность, предлагая оперативнику упреждающие сценарии действий.

Таким образом, биометрические технологии прочно заняли место центрального, системообразующего элемента научно-технического обеспечения оперативно-розыскной деятельности. Их значение для установления и розыска лиц, совершивших преступления, вышло далеко за рамки вспомогательной криминалистической процедуры. Они обеспечили стратегический переход к объективной, автоматизированной, проактивной мо-

дели работы, основанной на уникальных, трудно скрываемых параметрах человека. Дальнейшая эффективность противодействия криминальным вызовам цифровой эпохи будет напрямую зависеть от способности правоохранительной системы не только адаптировать и развивать технологический арсенал биометрии, но и решить сопутствующие правовые, этические и организационные проблемы. Успех в этой деятельности определится не только технологическим превосходством, но и способностью общества и государства выстроить адекватные правовые рамки, гарантирующие как общественную безопасность, так и незыблемость фундаментальных прав и свобод человека.

Назаров Матвей Викторович,
слушатель 5 курса Крымского филиала
Краснодарского университета МВД России
тел: +7(978)637-34-19;
e-mail: amx1221@mail.ru

Зоз Владимир Александрович,
старший преподаватель кафедры
деятельности органов внутренних дел
Крымского филиала
Краснодарского университета МВД России
тел: +7(980)350-75-50; e-mail: spec13_47@mail.ru

СОДЕРЖАНИЕ ПРИНЦИПА УВАЖЕНИЯ И СОБЛЮДЕНИЯ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА И ЕГО СООТНОШЕНИЕ С ПРИНЦИПОМ ЗАКОННОСТИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Оперативно-розыскная деятельность (далее - ОРД), выступая одним из инструментов правоохранительной деятельности, по своей природе связана с ограничением конституционных прав и свобод личности¹. Это объективное противоречие между интересами общества в безопасности и неотчуждаемыми правами человека разрешается в правовом государстве через систему строгих принципов, закрепленных в законодательстве. Среди них принципы законности и уважения прав и свобод человека и гражданина занимают центральное место².

Принцип соблюдения прав и свобод человека и гражданина в ОРД представляет собой обязанность субъектов ОРД решать задачи с помощью законных действий, которые допускают лишь обоснованное ограничение прав личности, а также обязанность строгого соблюдения предусмотренного законодательством порядка такого ограничения.

Содержание рассматриваемого принципа раскрывается через единство двух категорий: «уважение» и «соблюдение». Уважение прав представляет собой мировоззренческую, ценностную основу принципа. Это

¹ Назаров М.В. Принцип соблюдения и уважения прав и свобод человека и гражданина в оперативно-розыскной деятельности: исторический аспект // Актуальные вопросы науки и практики: XIII Междунар. науч.-практ. конф. курсантов, слушателей, студентов и адъюнктов, 7–10 апр. 2025 г. / редкол.: А. Л. Осипенко, Д. Б. Данилов, Н. В. Агаронова и др. – Электрон. дан. – Краснодар: Краснодарский университет МВД России, 2025. – с. 681

² Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (в последней редакции) // СПС КонсультантПлюс

признание достоинства личности, закрепленного ст. 21 Конституции РФ¹, в качестве абсолютной ценности, не зависящей от правового статуса лица (будь то потерпевший, свидетель или объект ОРД). Уважение проявляется в форме почтительного отношения, запрета на унижающее обращение, пытки, насилие, защиту чести и репутации. Эта составляющая находит свое нормативное выражение, в частности, в ст. 5 ФЗ «О полиции»², обязывающей сотрудников полиции проявлять уважение к национальным обычаям и традициям, учитывать культурные и иные особенности различных социальных групп.

Принцип уважения прав и свобод человека и гражданина в оперативно-розыскной деятельности формирует особую правовую парадигму взаимодействия между уполномоченными субъектами и участниками оперативно-розыскных отношений. В основе данного взаимодействия лежит конституционное признание человеческого достоинства как абсолютной ценности, исключающее любые формы его умаления, независимо от процессуального статуса лица, вовлеченного в сферу оперативно-розыскной деятельности.

Соблюдение прав и свобод человека и гражданина выступает в данном случае юридической, деятельностной составляющей рассматриваемого принципа. Оно включает в себя:

- пассивную обязанность – воздержание от действий, нарушающих права и свободы человека и гражданина;
- активную обязанность – создание государством условий и механизмов для реальной реализации прав и свобод человека и гражданина;
- легитимное ограничение прав и свобод человека и гражданина – в контексте ОРД соблюдение прав не означает их абсолютной неприкосновенности. Следует обратить внимание на то, что ст. 55 Конституции РФ предусматривает возможность ограничения прав и свобод человека и гражданина федеральным законом, однако такие ограничения допускаются лишь в объеме, необходимом для достижения конституционно значимых целей³.

Необходимо отметить, что ограничение прав и свобод человека и гражданина должно быть: законным, обоснованным, соразмерным достижимой цели, процессуально обеспеченным.

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС КонсультантПлюс

² Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (в последней редакции) // СПС КонсультантПлюс

³ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС КонсультантПлюс

Принцип законности выступает универсальным требованием, распространяющимся на все без исключения сферы государственной деятельности, и ОРД не является исключением. В контексте ОРД его сущность раскрывается через систему взаимосвязанных требований:

1. Требование нормативной регламентированности. Все общественные отношения, возникающие в сфере ОРД, должны быть урегулированы нормами права. Деятельность оперативных подразделений может осуществляться только на основании и во исполнение законов (Конституция РФ, ФЗ «Об ОРД», ФЗ «О полиции» и др.).

2. Требование компетентности. ОРД вправе осуществлять только специально уполномоченные на то государственные органы, исчерпывающий перечень которых закреплен в ст. 13 ФЗ «Об ОРД»¹. Выход за рамки установленной компетенции является грубейшим нарушением законности.

3. Требование соблюдения установленной процедуры. Проведение оперативно-розыскных мероприятий, их документальное оформление, использование полученных результатов строго регламентированы законом. Нарушение процессуальных норм влечет признание полученных доказательств недопустимыми.

4. Требование верховенства закона. В случае коллизии между ведомственными нормативными актами и федеральным законом приоритет всегда должен отдаваться последнему. Подзаконное регулирование может лишь конкретизировать положения закона, но не противоречить им.

Таким образом, принцип законности в ОРД – это императивное требование строгого и неуклонного соблюдения и исполнения конституционных норм, федеральных законов и иных нормативных правовых актов, регламентирующих оперативно-розыскную деятельность, всеми субъектами, ее осуществляющими.

Проведенный анализ сущности рассматриваемых принципов позволяет выявить их взаимосвязь и различия. Взаимосвязь рассматриваемых принципов состоит в:

- единой правовой природе (конституционное происхождение и дальнейшее развитие в отраслевом законодательстве);
- общей целевой направленности – построении правового государства, в котором эффективная борьба с преступностью не подрывает фундаментальные основы свободы и достоинства человека;
- взаимообусловленности, так как реализация принципа уважения прав и свобод человека и гражданина невозможна без соблюдения принципа законности.

Несмотря на тесную взаимосвязь, рассматриваемые принципы не тождественны и выполняют в механизме правового регулирования каче-

¹ Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (в последней редакции) // СПС КонсультантПлюс

ственно различные роли. Их соотношение характеризуется функциональным распределением, где каждый принцип отвечает за свою сферу правового воздействия:

- Основная функция принципа уважения и соблюдения прав и свобод человека и гражданина – ценностно-ориентирующая. Так как он задает содержательные ориентиры, цели и пределы регулирования. Основная функция принципа законности – регулятивная и он создает формально-юридические рамки, регламентирует непосредственно процесс деятельности.

- Требования принципа уважения прав и свобод человека и гражданина являются по своей природе содержательными и ценностными. Они касаются обоснованности вмешательства, соразмерности применяемых мер, уважения достоинства личности и минимизации вреда частной жизни. Оценка их соблюдения требует не только юридического, но и этического анализа. Требования принципа законности носят в основном формальный и процедурный характер. Они касаются компетенции органов, порядка санкционирования мероприятий, правил документооборота и использования результатов. Соблюдение этих требований можно проверить путем внешней проверки на соответствие установленным нормам.

- Принцип законности выступает необходимым условием и основой для реализации принципа уважения прав и свобод человека и гражданина. Без правовой регламентации и процедурных гарантий любые декларации о уважении прав останутся благими пожеланиями. В то же время, принцип уважения прав является смысловым наполнением, целью и системообразующим стержнем принципа законности. Он определяет, какое содержание должна иметь правовая регламентация, чтобы не превратиться в инструмент произвола. Законность без уважения к правам вырождается в формализм, а уважение к правам без законности – в необеспеченную декларацию.

Таким образом, можно утверждать, что принцип уважения и соблюдения прав и свобод человека и гражданина и принцип законности в ОРД представляют собой самостоятельные, но диалектически взаимосвязанные правовые категории. Принцип законности формирует формальный каркас ОРД, обеспечивая ее нормативную определенность, предсказуемость и контролируемость. Принцип уважения прав наполняет этот каркас гуманистическим содержанием, определяя его цели и смысл, задавая содержательные границы допустимого ограничения прав в интересах борьбы с преступностью.

Игнорирование автономности принципа уважения прав и свобод человека и гражданина и его сведение лишь к аспекту законности создает риск легитимации формально правильных, но по своей сути произвольных и нарушающих права личности действий. Для построения современной, отвечающей стандартам правового государства модели ОРД необходим системный подход, при котором неукоснительное соблюдение принципа законности служит надежным инструментом для реализации высшей цели – гарантирования уважения и защиты прав и свобод человека и гражданина.

Николаенко Денис Николаевич,
доцент кафедры оперативно-разыскной деятельности ОВД
и применения информационных технологий
Московского областного филиала Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук
тел.: 8-920-831-07-17; e-mail: sihik-ord@mail.ru

К ВОПРОСУ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ МЕЖДУ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ МВД РОССИИ И СЛЕДСТВЕННЫМ КОМИТЕТОМ РФ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ НАЛОГОВЫХ ПРЕСТУПЛЕНИЙ

Эффективное и своевременное расследование налоговых преступлений, выявление виновных и обеспечение защиты прав участников уголовного процесса требуют тесного взаимодействия следственных органов Следственного комитета Российской Федерации с оперативными подразделениями органов внутренних дел, наделёнными полномочиями по осуществлению оперативно-розыскной деятельности. Создание такого механизма требует комплексного и профессионального сочетания уголовно-процессуальных и оперативно-розыскных инструментов.

Особенности налоговых преступлений, таких как их латентный характер, использование фиктивных документов, конспиративность и высокая организованность преступников, делают качественное взаимодействие между следователями и оперативными подразделениями не просто полезным, а необходимым. Эти обстоятельства диктуют потребность в применении правоохранными органами современных, эффективных и разнообразных форм и методов совместной работы.¹

Взаимодействие между данными ведомствами понимается как основанная на законе согласованная деятельность, направленная на достижение общих целей по предупреждению, пресечению, раскрытию и расследованию преступлений налоговой направленности. В уголовном судопроизводстве эта деятельность подчиняется государственной стратегии в сфере борьбы с преступностью, где оперативно-розыскная деятельность играет обеспечительную роль, а интересы предварительного следствия являются приоритетными.

¹ Бражников, Д. А. Взаимодействие СК России с органами, осуществляющими оперативно-разыскную деятельность при расследовании налоговых преступлений / Д. А. Бражников // Следственный комитет Российской Федерации: второе десятилетие на службе Отечеству : Материалы Международной научно-практической конференции, Москва, 07 февраля 2019 года / Под общей редакцией А.М. Багмета. – Москва: Московская академия Следственного комитета Российской Федерации, 2019. – С. 63-67

Эффективность раскрытия и расследования налоговых преступлений напрямую зависит от слаженного взаимодействия оперативных и следственных подразделений. Наиболее значимым это взаимодействие является на этапе, предшествующем возбуждению уголовного дела, поскольку именно здесь формируется его фактическая и доказательственная основа. Вступившие в силу в 2022 году законодательные изменения, установили особый порядок возбуждения уголовных дел по статьям 198 – 199.2 Уголовного кодекса Российской Федерации, которые предусматривают использование исключительно материалов налоговых органов. Это обстоятельство актуализировало вопрос о необходимости интеграции результатов оперативно-розыскной деятельности в процессуальную проверку.¹

Новый порядок формально исключил возможность инициативного представления оперативными подразделениями материалов ОРД в следственные органы в качестве самостоятельного повода для возбуждения дела. Это создало правовой вакуум, при котором сведения, однозначно указывающие на признаки состава преступления, не имеют регламентированного механизма передачи следователю. В отсутствие четких нормативных предписаний на практике сформировался устойчивый, хотя и не формализованный, алгоритм сотрудничества, основанный на принципах взаимной координации и планирования.

Данный алгоритм включает в себя широкий комплекс контактов между специализированными подразделениями ЭБиПК и Следственного комитета РФ, выходящих за рамки уголовного процесса. Ключевыми элементами этого взаимодействия являются предварительная оценка материалов. На ранних стадиях, включая этап камеральных и выездных налоговых проверок, оперативные сотрудники привлекаются к ознакомлению с материалами налогового контроля для оценки их полноты и определения необходимости проведения необходимых ОРМ.

Так, например, в рамках консультаций со следствием СК РФ, оперативные сотрудники на добровольной основе получают правовую оценку собранных материалов и рекомендации по перечню дополнительных мероприятий, необходимых для документирования состава преступления. Эта практика, несмотря на отсутствие прямого нормативного регулирования, осуществляется в рамках работы межведомственных рабочих групп.

Нормативной базой для такого взаимодействия служат положения пункта 3 статьи 82 Налогового кодекса РФ, допускающие межведомственный обмен информацией, а также двусторонние соглашения между МВД России, ФНС России и Следственным комитетом РФ. Однако регламента-

¹ Федеральный закон «О внесении изменений в статьи 140 и 144 Уголовно-процессуального кодекса Российской Федерации» от 09.03.2022 № 51-ФЗ (последняя редакция) // КонсультантПлюс (дата посещения 29.09.2025).

ция конкретных процедур, особенно консультативных, остается недостаточной.

После официального поступления материалов из налогового органа в следствие взаимодействие приобретает более формализованный характер. Оно заключается в исполнении поручений следователя, официальном представлении результатов ОРД и совместной подготовке к проведению неотложных следственных действий.

Необходимо напомнить, что специфической чертой расследования налоговых преступлений является их тесная связь с параллельно идущими административными и арбитражными процессами по обжалованию решений налоговых органов. Исследование судебных актов арбитражных судов показывает, что данные решения не обладают для уголовного судопроизводства преюдициальной силой в полном объеме. Фактические обстоятельства, установленные арбитражем, оцениваются в совокупности с другими доказательствами по уголовному делу, а отмена решения ФНС сама по себе не влечет автоматического прекращения уголовного преследования.

В этой связи одним из важных направлений взаимодействия становится оперативное обеспечение положительной для обвинения позиции в арбитражном процессе. Оперативные подразделения в координации со следователем СК проводят мероприятия, направленные на документирование попыток фальсификации доказательств налогоплательщиком и выявление коррупционных связей способствующих освобождению от налоговой и уголовной ответственности.

Так в ходе расследования часто выявляются сведения об иных эпизодах преступной деятельности, не входящих в предмет доказывания по конкретному уголовному делу. Их процессуальная фиксация затруднена, так как для возбуждения нового дела требуется проведение самостоятельной налоговой проверки. Это приводит к использованию вне процессуального механизма – направления информации в налоговые органы в рамках межведомственного взаимодействия без формального выделения материалов в отдельное производство.

Таким образом, взаимодействие подразделений ЭБиПК и следственных органов СК РФ по налоговым преступлениям после 2022 года характеризуется развитой системой внепроцессуальных, консультативно-совещательных форм, компенсирующих недостатки нормативного регулирования.

Сложившаяся практика доказала свою эффективность, однако нуждается в законодательной легитимации и детальной регламентации для обеспечения единообразия и соблюдения прав участников процесса. Дальнейшее совершенствование этого взаимодействия должно быть направлено на создание прозрачных и сбалансированных механизмов интеграции результатов ОРД в процессуальную деятельность на доследственной стадии.

В ходе заседания коллегии Федеральной налоговой службы, состоявшегося 9 апреля 2025 года, представлены ведомства, вовлечённые в процесс противодействия налоговым преступлениям. В их числе – Федеральная налоговая служба, Министерство внутренних дел и Следственный комитет. Такой комплексный подход обеспечивает синергетический эффект в выявлении, пресечении и расследовании налоговых правонарушений. Как подчеркнул глава Федеральной налоговой службы Егоров Д. В., «без слаженного взаимодействия с правоохранительными органами нам не удастся достичь успеха». Статистические данные, представленные на коллегии, свидетельствуют, что половина всех выездных проверок осуществляется совместно с подразделениями ЭБ и ПК МВД России, что в свою очередь отражается на повышении эффективности межведомственного взаимодействия: 67% всех доначислений обеспечено благодаря плотному взаимодействию с органами МВД. Количество возбужденных уголовных дел по материалам совместных проверок увеличилось с 50% в 2021-2023 годах до 70% в 2024 году. В последнее время налогоплательщики, уклоняющиеся от уплаты налогов, всё чаще обращаются за помощью к лицам, которые предоставляют целый комплекс услуг, связанных с уклонением от уплаты налогов. Речь идёт об организованных преступных сообществах, специализирующихся на оказании услуг по уклонению от уплаты налогов. В ответ на эту угрозу в ноябре 2024 года в Уголовный кодекс Российской Федерации была внесена статья 173.3, которая предусматривает ответственность за организацию деятельности, связанной с представлением в налоговые органы Российской Федерации и (или) сбытом заведомо подложных счетов-фактур и (или) налоговых деклараций (расчётов).¹

Одной из ключевых проблем в расследовании налоговых преступлений остается доказывание умысла. Согласно разъяснениям Верховного Суда РФ, уклонение от уплаты налогов возможно только с прямым умыслом.² Для установления умысла налоговики и правоохранительные органы анализируют совокупность обстоятельств, свидетельствующих о целенаправленном характере действий налогоплательщика.

Еще одной сложной задачей является привлечение бенефициаров – лиц, которые фактически управляют компанией, но формально не имеют к ней отношения. По данным ФНС, 68,9% бенефициаров были установлены среди руководителей, учредителей и главных бухгалтеров, в то время как

¹ Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 28.1 и 151 Уголовно-процессуального кодекса Российской Федерации» от 23.11.2024 № 406-ФЗ (последняя редакция) // КонсультантПлюс (дата посещения 29.09.2025).

² Постановление Пленума Верховного Суда РФ от 26.11.2019 № 48 «О практике применения судами законодательства об ответственности за налоговые преступления» // КонсультантПлюс (дата посещения 29.09.2025).

31,1% – среди лиц, которые неформально управляют деятельностью должника и извлекают из этого неправомерную выгоду.

Если в период с 2021 по 2023 год уголовные дела возбуждались в 50% случаев на основе собранных материалов, то в 2024 году было возбуждено более 70% дел, связанных с выявленными фактами уклонения от уплаты налогов организациями. При этом среднее доначисление по результатам совместных проверок увеличилось с 78 млн рублей в 2022 году до 109 млн рублей в 2024 году.¹

Основываясь на вышеизложенные статистические факты, можно сделать вывод, что взаимодействие подразделений экономической безопасности и противодействия коррупции с органами предварительного следствия Следственного комитета в контексте противодействия налоговым преступлениям в значительной степени осуществляется вне рамок процессуальных норм, установленных уголовно-процессуальным законодательством. Для налоговых преступлений характерна универсальная модель процессуального взаимодействия, реализуемая через последовательность стадий. К ним относятся: оценка полноты и достаточности материалов ОРД, проведение процессуальной проверки, направление материалов в следственные органы, а также их рассмотрение как на доследственной стадии, так и после возбуждения уголовного дела.

Стоит отметить, что все упомянутые этапы сопровождаются интенсивным информационным обменом с налоговыми органами, что приводит к взаимному влиянию мероприятий налогового контроля и процессуальной деятельности следствия. Тем самым создаётся симбиоз между успешностью доказывания факта налогового правонарушения в административном порядке и результативностью расследования соответствующего уголовного дела.²

В текущей оперативной обстановке перед подразделениями экономической безопасности и противодействия коррупции, в рамках осуществления оперативно-розыскной деятельности, актуализируется комплекс специфических оперативно-тактических задач, направленных на документирования признаков состава налоговых преступлений. Информационный обмен, положенный в основу данного комплекса позволяет обеспечивать ведомства необходимыми сведениями, но и позволяет собрать доказательства уличающие налогоплательщика в совершении налогового преступле-

¹ Актуальные вопросы межведомственного взаимодействия по выявлению и пресечению налоговых правонарушений обсудили на заседании коллегии ФНС России / Официальный сайт ФНС России https://www.nalog.gov.ru/rn77/news/activities_fts/16167047/ (дата посещения 29.09.2025)

² Ларичев, В. Д. Взаимодействие налоговых органов с органами внутренних дел и следственными органами при возбуждении уголовных дел по налоговым преступлениям / В. Д. Ларичев, Е. В. Милякина, А. Н. Панкратьев // Lex Russica (Русский закон). – 2023. – Т. 76, № 12(205). – С. 86.

ния, достаточные для не только для возбуждения уголовного дела, но и для идентификации бенефициаров, возмещения причинённого ущерба и т.д.

Резюмируя стоит указать, что в настоящее время отсутствие единой нормативной базы, регулирующей межведомственное взаимодействие, при существовании лишь фрагментарных предписаний в разрозненных ведомственных актах, определяет потребность в разработке консолидированного регламентирующего документа. Наиболее приемлемой формой для такого акта представляется трехстороннее соглашение между СК РФ, МВД РФ и ФНС России, конкретное наполнение которого требует отдельного научного обсуждения.

Павлишинец Анна Юрьевна,
курсант 3 курса Краснодарского университета МВД России

Баженов Василий Андреевич,
кафедры оперативно-розыскной деятельности ОВД
Краснодарский университет МВД России

ПРОБЛЕМЫ СООТНОШЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ И УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ: ВОПРОСЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОРД В ДОКАЗЫВАНИИ ПО УГОЛОВНОМУ ДЕЛУ

Понятия уголовно-процессуальной и оперативно-розыскной деятельности находятся в тесной взаимосвязи между собой. Это обусловлено наличием общих понятий, присущих любому виду правовой деятельности.

Оперативно-розыскная деятельность является одним из важнейших компонентов в процессе раскрытия и расследования преступлений. Но в настоящее время в теории права, имеется множество спорных вопросов, связанных с использованием результатов оперативно-розыскной деятельности в доказывании по уголовным делам.

В рамках теории уголовного процесса существуют различные способы применения информации, полученной в рамках оперативно-розыскной деятельности. Так возможно прямое использование результатов оперативно-розыскной деятельности при соблюдении условий, предусмотренных уголовно-процессуальным законодательством, либо формирование новых доказательств, посредством проведения различных процессуальных действий.

Согласно современному толкованию норм уголовно-процессуального права и сложившейся юридической практике, основания для проведения следственных действий можно получить как процессуальными способами, так и посредством оперативно-розыскной работы. Но могут возникнуть противоречия при использовании данных, полученных в рамках ОРД. Например, основанием для проведения обыска, может являться только наличие процессуально закрепленных доказательств, поскольку данное следственное действие нарушает конституционные права и свободы личности. Однако, при реализации оперативных мероприятий, зачастую требуется срочное проведение таких следственных действий, как допрос и осмотр мест совершения преступления, непосредственно после стадии возбуждения уголовного дела.

Статья 11 ФЗ-144 «Об оперативно-розыскной деятельности» закрепляет что, результаты оперативно-розыскной деятельности могут быть использованы в процессе доказывания по уголовным делам при условии их

представления в ходе судебного производства и в порядке, закрепленном уголовно-процессуальным законодательством.¹

Так же в соответствии с нормами уголовно-процессуального кодекса, не одно доказательство не обладает заранее установленной юридической силой. (ч.2 ст.17 УПК).²

Статья 75 УПК закрепляет перечень доказательств, считающихся недопустимыми, однако аналогичной процессуальной нормы для доказательств, полученных в рамках проведения оперативно-розыскных мероприятий не существует. Это делает более сложным процесс оценки допустимости доказательств, полученных в рамках оперативно-розыскной деятельности.

Данная проблема объясняется тем, что вопросы тактики и методики проведения оперативно-розыскных мероприятий составляют государственную тайну, охраняемую законом. В связи с этим оперативные сотрудники имеют право не комментировать обстоятельства, связанные с организацией и ходом проведения оперативно-розыскных мероприятий при предъявлении доказательственной информации.

В рамках проведения оперативно-розыскных мероприятий, могут быть получены сведения о возможных свидетелях, о предметах и документах, которые могли быть использованы в качестве орудия совершения преступления или содержащих следы противоправного деяния. Так же оперативный сотрудник имеет право принимать меры, направленные на предотвращение уничтожения доказательств, способствующих идентификации преступника. Оперативно-розыскные мероприятия осуществляются параллельно с неотложными следственными действиями и способствуют установлению истины в максимально сжатые сроки. Для трансформации информации, полученной непроцессуальным путем, возможно проведение дополнительных следственных действий, позволяющих придать юридически значимым обстоятельствам надлежащую процессуальную форму.

Для формирования допустимых доказательств результаты оперативно-розыскной деятельности должны содержать:

- сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию по конкретному уголовному делу;
- ссылку на источник потенциального доказательства или объекта, который может быть использован в качестве доказательства;
- информацию, позволяющую проверить доказательства в процессуальном порядке

¹ Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения 17.10.2025г.)

² Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.10.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_34481/989cf5fde0b4d552c3c4debbad2399a655b43fac/ (дата обращения 17.10.2025)

Значимость доказательств, полученных в ходе осуществления оперативно-розыскной деятельности выражена в ситуации приостановления предварительного следствия по уголовному делу в соответствии со ст. 208 УПК РФ

Согласно ч.3 ст. 208 УПК РФ «после приостановления предварительного следствия производство следственных действий не допускается»¹ Данное обстоятельство исключает проведение дальнейшего расследования. Однако приостановление предварительного следствия, не означает окончательного прекращения производства по уголовному делу. Если в ходе оперативно-розыскной деятельности станут известными сведения, подтверждающие необходимость дальнейших следственных действий, следствие может быть возобновлено. В данном случае, результаты оперативно-розыскной деятельности выступают единственным законным основанием для последующего производства следственных действий.

Проблема оценки результатов доказательств, полученных в рамках оперативно-розыскной деятельности остается одной из наиболее сложных задач, особенно для судопроизводства.

Например, в Апелляционном Постановлении № 22-5187/2017 от 21 декабря 2017 г. по делу № 22-5187/2017² суд постановил исключить из числа доказательств результаты оперативно-розыскных мероприятий и признать их недопустимыми.

Европейский Суд по правам человека, рассматривая жалобы российских граждан, часто обращает внимание на отсутствие в законодательстве Российской Федерации норм права, обеспечивающих защиту прав личности при проведении негласных оперативно-розыскных мероприятий.

Вопросы защиты прав личности в сфере оперативно-розыскной деятельности широко охватываются на законодательном и научном уровнях, однако между теорией и практикой продолжают существовать противоречий. Значимой фигурой в процессе защиты прав граждан, может выступать адвокат, но Федеральный закон «Об оперативно-розыскной деятельности»³ не закрепляет четкого юридического статуса адвоката.

Для решения указанной проблемы, целесообразно использовать аналогию права и обратиться к положениям норм уголовно-процессуального права, а также использовать нормы закона, содержащиеся в Федеральном законе

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.10.2025) URL: https://www.consultant.ru/document/cons_doc_LAW_34481/989cf5fde0b4d552c3c4debbad2399a655b43fac/ (дата обращения 18.10.2025)

² Апелляционное постановление № 22-5187/2017 от 21 декабря 2017 г. по делу № 22-5187/2017 URL: <https://sudact.ru/regular/doc/b7GcdQwG12h/>

³ Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения 17.10.2025г.)

«Об адвокатской деятельности и адвокатуре»¹, определяющего статус защитника в процессе уголовного судопроизводства.

Различия в оперативно-розыскной и уголовно-процессуальной деятельности так же заметны в полученных результатах и кругу уполномоченных на ее осуществление субъектов. Оперативно-розыскная деятельность не имеет уголовно-процессуальной регламентации и в целом направлена на решение задач, содержащихся в Федеральном законе «Об оперативно-розыскной деятельности». В то время как уголовно-процессуальная деятельность образует строго организованную систему производства по уголовному делу. Недопустим произвольный порядок осуществления процессуальных действий. Тем не менее уголовный процесс не может не взаимодействовать с оперативно-розыскной деятельностью, поскольку последняя представляет значимую информационно-доказательственную базу.

В заключении можно сказать о необходимости совершенствования нормативно-правовой базы в сфере уголовного судопроизводства. Например, ст.74 УПК РФ, содержащую перечень доказательств, можно дополнить пунктом, звучащим: «Результаты оперативно-розыскной деятельности, полученные в соответствии с требованиями законодательства». Так же можно внести изменения в ст.140 УПК РФ, содержащую перечень поводов и оснований для возбуждения уголовного дела, дополнив ее положением о процессуальном использовании результатов оперативно-розыскной деятельности, документированных соответствующим образом.

¹ Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31.05.2002 № 63-ФЗ (последняя редакция) URL: https://www.consultant.ru/document/cons_doc_LAW_36945/ (дата обращения 18.10.2025)

Поезжалов Владимир Борисович,
доцент кафедры оперативно-разыскной деятельности ОВД
Уфимского юридического института МВД России,
кандидат юридических наук, доцент,
тел.: 8-917-341-55-85; e-mail: poezvb_75@mail.ru

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ХИЩЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Сложность оперативной обстановки в сфере противодействия хищениям, совершаемым с использованием информационно-телекоммуникационных технологий (далее – ИТТ), связывают с развитием научно-технического прогресса, доступностью подключения к глобальной сети Интернет, невысокой стоимостью интернет-услуг и мобильной связи, низкой грамотностью населения в вопросах информационных технологий и нерешенностью ряда правовых проблем в этой сфере.

Хищения с использованием ИТТ относятся к наиболее динамичным видам преступных посягательств, способы совершения которых меняются ежегодно.

Полагаем, что в самом общем виде способы совершения наиболее распространенных хищений, совершенных с использованием ИТТ, по которым проведение оперативно-розыскных мероприятий (далее – ОРМ) осуществляется силами оперативных подразделений территориальных ОВД, можно разделить на два вида.

Первый вид – это хищения с использованием средств мобильной телефонной связи. Ко второму виду следует отнести дистанционные хищения с использованием сети Интернет.

Основная часть лиц на момент совершения ими указанных преступлений не находится в регионе проживания потерпевшего, а именно (по некоторым данным – в 90% случаев) и нередко ведет свою преступную деятельность из-за границы России (чаще всего с территории Украины), поэтому раскрытие подобных преступлений «по горячим следам» затруднено.

Вместе с тем, лица, осуществляющие телефонные звонки и находящиеся за границей Российской Федерации, для реализации преступных действий нуждаются в соответствующей технической инфраструктуре связи, которая поддерживается соучастниками, находящимися на территории Российской Федерации, также они обращаются к помощи иных участников преступной деятельности, обеспечивающих обналачивание или вывод похищенных денежных средств. В отношении таких лиц возможно проведение соответствующих ОРМ и раскрытие преступлений «по горячим следам».

В настоящее время стала достаточно распространенной преступная схема «фейк босс» (или Fake Boss Scam) – это разновидность мошенничества, при которой злоумышленники выдают себя за руководителей компаний, чтобы обмануть сотрудников и заставить их перевести деньги или передать конфиденциальные данные. Эта афера особенно популярна среди международных преступных группировок. Схема «фейк босс» работает следующим образом:

1. Сбор информации о компании: мошенники тщательно изучают организацию. Для этого они используют открытые источники (сайт компании, социальные сети, отчеты); определяют ключевых сотрудников (бухгалтеров, финансовых директоров, менеджеров); узнают стиль общения руководства, чтобы имитировать его манеру письма.

2. Создание поддельного контакта: злоумышленники создают фальшивую почту или аккаунт в мессенджере, схожий с реальным контактом руководителя. Например: Оригинал: boss@company.com Фальшивый: boss@с0mpany.com (замена «о» на «0»). В ряде случаев они могут взломать аккаунт топ-менеджера и вести переписку от его имени.

3. Операция по обману сотрудника: мошенник отправляет письмо или сообщение с просьбой срочно перевести деньги на «новый» счет (под предлогом сделки, инвестиций, налогов и т.д.); переслать конфиденциальную информацию (данные клиентов, отчеты, пароли); купить подарочные карты и передать коды. Главный используемый в данном случае прием – игра на срочности: мошенники требуют выполнить задание «немедленно», «секретно», «не ставя в известность никого».

4. Вывод денег и исчезновение: после перевода средств мошенники быстро обналичивают деньги через офшорные счета, криптовалюту или другие теневые схемы.

У данной схемы достаточно большое число вариаций. Так, 18 февраля 2025 г. МВД России сообщило о новом варианте мошеннической схемы «фейк босс», направленной на детей. Злоумышленники звонят ученикам, представляясь завучем школы, и создают видимость взлома аккаунта на «Госуслугах». Затем находящемуся в стрессе подростку набирает «следователь» с предложением провести «видеообыск» в его доме, чтобы найти ценные вещи. После этого их забирают через курьера.

Дети в настоящее время вообще достаточно часто становятся объектами воздействия со стороны мошенников через компьютерные онлайн-игры и звонки. Чаще всего злоумышленники звонят детям, представляясь правоохранителями, создают фейковые акции и выигрыши в онлайн-играх и под предлогом защиты данных пытаются убедить жертв установить программы удаленного доступа к гаджетам родителей.

19 февраля 2025 г. Департамент образования Москвы в Telegram-канале сообщил, что мошенники придумали новую схему обмана с электронным дневником. Они звонят детям, представляясь кем-нибудь из

школьной администрации, чтобы подтвердить доступ в электронный журнал. Потом злоумышленники выманивают у учеников код из смс-сообщения, который позволяет зайти в аккаунт МЭШ (Московская электронная школа) или на портал mos.ru.

Схемы преступного изъятия у граждан денежных средств многогранны и в ряде случаев мошенники используют для своих преступных целей «помощников», в том числе «услуги» так называемых «дропперов».

Дропперами, или дропами (от английского «drop» – бросать) называют людей, которые задействованы в нелегальных схемах мошенников по выводу средств с банковских карт.

В самом общем виде дропперы – это посредники между мошенниками и их потерпевшими, чья роль сводится к предоставлению собственной банковской карты, на которую жертвы переводят свои средства. Задача дроппера, получив указанные деньги, передать их заранее оговоренным путем (налично или переводом) организатору этой преступной схемы, получив за это «свой процент».

Дроповоды вербуют людей на стройках, территориях школ, общежитий, техникумов и колледжей, то есть в местах, где информацию легко распространять и, опираясь на невысокий уровень финансовой грамотности, «собрать урожай» – завлечь людей.

Вовлекая таким образом желающих «легко» подзаработать граждан, мошенники обычно рассказывают, что ничего незаконного в таких действиях нет. Вместе с тем стоит отметить, что действия «дропперов» в соответствии с Федеральным законом от 24 июня 2025 г. № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» образуют признаки одного из составов преступлений, предусмотренных чч. 3-6 ст. 187 УК РФ «Неправомерный оборот средств платежей».

Сардак Дмитрий Борисович,
старший преподаватель кафедры общеправовых дисциплин
Волгодонского филиала Ростовского юридического института
МВД России, подполковник полиции,
Тел: 8-909-414-74-29, e-mail: sdb07@mail.ru

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И КИБЕРПРЕСТУПНОСТИ

Современная цифровизация кардинально меняет облик оперативно-розыскной деятельности¹, создавая одновременно и новые возможности, и значительные вызовы, поэтому активное внедрение информационных технологий, рост количества цифровых данных, а также распространение киберпреступности радикально трансформируют методы преступной деятельности и требуют адаптации традиционных оперативных подходов к новым реалиям. В условиях глобальной цифровой инфраструктуры киберпреступники получают доступ к разнообразным средствам совершения преступлений, включая хакерские атаки, мошеннические схемы с криптовалютами, распространение вредоносного программного обеспечения, что значительно усложняет работу правоохранительных органов².

Особенности цифровых доказательств заключаются в их хрупкости, сложности извлечения, а также необходимости обеспечения надежности и допустимости в уголовном процессе, при этом традиционные методы фиксации и анализа надлежащим образом не всегда применимы к цифровым носителям информации, поскольку требуют разработки специализированных технических и правовых механизмов. Но, помимо технических сложностей, значительную проблему представляет и международный характер киберпреступлений, что в свою очередь требует активного развития механизмов международного взаимодействия и координации между правоохранительными и судебными органами различных государств³.

Современная цифровая реальность оказывает влияние на способы и методы совершения преступлений, что в свою очередь неизбежно отражается и на оперативно-розыскной деятельности. С распространением интернет-технологий и цифровых коммуникаций преступное сообщество адап-

¹ Далее ОРД

² Актуальные проблемы уголовной и уголовно-процессуальной политики Российской Федерации: материалы XIII международной научно-практической конференции / Сибирский юридический университет, 2024. URL: <https://www.iuaj.net/node/3435> (дата обращения: 01.10.2025).

³ Всероссийская научно-практическая конференция «Актуальные проблемы уголовного процесса и уголовного права в условиях глобальных вызовов современности»: информационное письмо, 2024. URL: <https://konferencii.ru/info/148591> (дата обращения: 01.10.2025).

тировалось к новым условиям, активно используя информационные и телекоммуникационные сети для реализации своих противоправных целей, наряду с традиционными формами преступности появились и получили развитие совершенно новые виды преступлений, которые базируются на использовании цифровых технологий и отличаются высокими уровнями анонимности, виртуальности и транснациональности¹.

Отметим, что рост числа противоправных действий в цифровом пространстве связан с доступностью и распространённостью таких технологий и существенно расширяет круг потенциальных жертв и увеличивает масштаб ущерба. К примеру, использование вредоносного программного обеспечения, фишинг, кража персональных данных, мошенничество с криптовалютами стали обыденными для злоумышленников инструментами, масштаб данной проблемы подтверждают статистические данные российских правоохранительных органов, согласно которым количество зарегистрированных киберпреступлений продолжает расти, а финансовый ущерб, причинённый ими, исчисляется сотнями миллиардов рублей ежегодно. Цифровая трансформация преступности характеризуется высокой скоростью изменений и развитием новых методов, и как следствие создает сложные вызовы для правоохранительных органов. Злоумышленники используют анонимайзеры, виртуальные частные сети (VPN), криптографию и другие средства, которые позволяют скрывать следы своей деятельности и осложняют процессы расследования, преступность в цифровом пространстве становится более изощрённой, гипертаргетированной и мультипликативной, что требует от оперативно-розыскных подразделений постоянного обновления компетенций и технических ресурсов².

И, априори, в условиях цифровизации и широкого распространения информационных технологий значительную долю доказательной базы в уголовном процессе стали составлять цифровые доказательства, что непосредственно привело к возникновению ряда существенных проблем при их сборе и легализации. Одной из главных сложностей здесь является оперативность и правильность фиксации цифровой информации, которая имеет высокую уязвимость к уничтожению, изменению и искажениям в процессе извлечения или хранения, поэтому очевидно, что для успешного применения таких доказательств необходимо соблюдение специальных требований, включая использование технических средств и компетенцию специа-

¹ Трансформация преступности в эпоху цифровых технологий // Молодой ученый. 2024. № 11. URL: <https://moluch.ru/archive/547/119763> (дата обращения: 01.10.2025).

² Распоряжение Правительства Российской Федерации от 14 августа 2025 г. № 2207-р «О плане мероприятий по реализации Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий» // Официальный сайт Правительства РФ. URL: http://government.ru/dep_news/55975/ (дата обращения: 01.10.2025).

листов в области IT, что далеко не всегда доступно при проведении следственных мероприятий¹.

Нельзя так же не отметить тот факт, что кроме технических трудностей, значимой проблемой остаётся нормативно-правовое регулирование, которое в сравнении с динамикой развития технических средств и методов преступной деятельности часто отстаёт. В российском уголовно-процессуальном законодательстве отсутствует чёткое и однозначное определение цифровых или электронных доказательств, что приводит к неоднородной практике их применения и оценке в судебных инстанциях. И в конечном итоге проблематичным становится признание допустимости таких доказательств, особенно в случае использования скриншотов, копий переписок и иных «электронных следов», полученных без соблюдения всех процессуальных норм.

Хранение цифровых доказательств и обеспечение их неизменности также представляют серьёзную задачу, важна не только сохранность самих носителей информации, но и целостность данных на них, а это уже требует создания специализированных цифровых хранилищ и внедрения систем идентификации и аутентификации данных. Поэтому разработка таких инструментов позволит повысить доверие к цифровым доказательствам в рамках уголовного судопроизводства, обеспечивая возможность их достоверной проверки и использования в суде².

Несомненно значительное значение имеет и профессионализм следователей и экспертов, участвующих в сборе и экспертизе цифровых доказательств, поскольку недостаток квалификации в IT-сфере и отсутствие закреплённых законодательством процедур по изъятию, копированию и анализу цифровой информации снижают эффективность расследования и ставят риски признания доказательств недопустимыми. В связи с этим научное сообщество и правоохранительные органы подчеркивают необходимость совершенствования нормативной базы и специализированной подготовки кадров в данной сфере.

Современные вызовы цифровой эпохи актуализировали необходимость активного внедрения инновационных технологий в практику ОРД. По мере того как преступные группы осваивают криптовалюты, анонимные онлайн-платформы и расширяют использование цифровых средств, правоохранительные органы вынуждены развивать новые методы и ин-

¹ Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. №5. URL: <https://cyberleninka.ru/article/n/problemy-sobiraniya-i-ispolzovaniya-tsifrovyyh-dokazatelstv> (дата обращения: 01.10.2025).

² Янин М. Г., Кочедыкова К. М. Проблемы сбора, проверки и оценки электронных доказательств в уголовном судопроизводстве // Управление в современных системах. 2019. №2 (22). URL: <https://cyberleninka.ru/article/n/problemy-sbora-proverki-i-otsenki-elektronnyh-dokazatelstv-v-ugolovnom-sudoproizvodstve> (дата обращения: 01.10.2025).

струменты, которые обеспечивают более глубокий и всесторонний анализ информации, а также ускоряют процессы установления подозреваемых и раскрытия преступлений. Следует отметить, что законодательство Российской Федерации, в частности Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности», предусматривает возможность использования технических средств и специальных научных методов, что несомненно создает правовую основу для внедрения современных технологий в оперативную практику¹ [8].

Однозначно одной из ключевых технологий является биометрическая идентификация, которая позволяет оперативно устанавливать личность и отслеживать передвижения подозреваемых через распознавание лиц, отпечатков пальцев и ДНК. Точность и скорость таких методов значительно повышают эффективность расследований и дают возможность выявлять связи между членами преступных группировок с минимальными временными затратами. Параллельно развивается применение искусственного интеллекта² и аналитики больших данных³, которые способны автоматически обрабатывать огромные объемы информации, выявлять закономерности и создавать профили поведения подозреваемых. ИИ-алгоритмы анализируют данные из социальных сетей, телефонных разговоров и электронной переписки, что существенно расширяет возможности ОРД в области профилирования и прогнозирования преступных действий⁴.

Становится очевидным, что цифровая криминалистика также занимает важное место в современной оперативной практике. Извлечение информации с цифровых носителей, таких как смартфоны, компьютеры, сервера, позволяет получать ключевые доказательства, раскрывать финансовые потоки и структурировать преступные сети. И здесь законодательные нормы Российской Федерации по статье 6 ФЗ № 144-ФЗ поддерживают использование таких методов для предотвращения и раскрытия преступлений, также создавая правовую основу для технического сопровождения оперативной деятельности⁵.

Отметим так же, что для повышения прозрачности и результативности работы правоохранительных органов активно рассматривается воз-

¹ Оперативно-розыскные мероприятия в борьбе с организованной преступностью: современные технологии и методики / Апни.ру. URL: <https://apni.ru/article/12550-operativno-rozysknye-meropriyatiya-v-borbe-s-organizovannoj-prestupnostyu-sovremennye-tehnologii-i-metodiki> (дата обращения: 01.10.2025).

² Далее ИИ

³ Далее Big Data

⁴ Иванов В.И. Оперативно-розыскная деятельность в условиях цифровизации / Молодой ученый. 2025. № 5(570). URL: <https://articles.moluch.ru/archive/570/125061> (дата обращения: 01.10.2025).

⁵ Цифровая оперативно-розыскная деятельность и современные тенденции / Вестник СПб МВД России. 2025. URL: <https://vestnikspbmvdr.ru/ru/nauka/article/97350/view> (дата обращения: 01.10.2025).

возможность интеграции блокчейн-технологий, которые уже применяются за рубежом для отслеживания финансовых транзакций и контроля передвижения подозреваемых.

Немаловажным является и то, что в условиях глобализации и развития транснациональной преступности международное сотрудничество в сфере оперативно-розыскной деятельности играет ключевую роль в обеспечении государственной и общественной безопасности. Преступные организации и схемы зачастую распространяются за пределы нескольких стран. Все это требует координации усилий правоохранительных органов разных государств для проведения совместных операций и координации расследований. В России основой для такого сотрудничества служит Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности», который регулирует вопросы взаимодействия с зарубежными правоохранительными структурами, включая обмен разведанными, экстрадицию, возвращение осужденных и иные формы сотрудничества¹.

Правовое обеспечение международного сотрудничества включает в себя действующие международные соглашения и двусторонние договоры, которые устанавливают стандарты взаимодействия и процедуры обмена информацией. Россия активно участвует в работе международных организаций, таких как Интерпол, Европол и также в таких региональных объединениях как Совет глав государств СНГ, которые способствуют развитию правового и практического взаимодействия в сфере борьбы с преступностью на постсоветском пространстве. Эти институты обеспечивают платформу для согласования действий и обмена оперативной информацией между государствами, что существенно повышает результативность совместных операций². Но, несмотря на важность международного сотрудничества, в его практической реализации возникают определённые сложности.

Таким образом, подводя итоги, мы видим, что цифровизация и рост киберпреступности существенно повлияли на оперативно-розыскную деятельность, предъявив новые требования к методам и средствам работы правоохранительных органов. Для успешного противодействия современным угрозам необходимы инновационные решения, правовое обеспечение и международное сотрудничество. Обеспечение баланса между эффективностью борьбы с преступностью и защитой прав граждан остаётся приоритетной задачей оперативно-розыскной деятельности в цифровую эпоху.

¹ Яцко А.М., Кривошеев С.В. Международное сотрудничество в области оперативно-розыскной деятельности // Научный лидер. 2024. № 19 (169). URL: <https://scilead.ru/article/6397-mezhdunarodnoe-sotrudnichestvo-v-oblasti-oper> (дата обращения: 01.10.2025).

² Поздняков А. Н., Глазков А. А. Международное сотрудничество в сфере оперативно-розыскной деятельности по борьбе с этническими преступными структурами // Социально-политические науки. 2018. №2. URL: <https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-sfere-operativno-rozysknoy-deyatelnosti-po-borbe-s-etnicheskimi-prestupnymi-strukturami> (дата обращения: 01.10.2025).

Сафронов Андрей Алексеевич,
заведующий кафедрой юриспруденции Краснодарского
кооперативного института (филиала) автономной некоммерческой
образовательной организации высшего образования
Центросоюза РФ «Российский университет кооперации»,
кандидат юридических наук, доцент

СУЩНОСТЬ, СОДЕРЖАНИЕ И ПРЕДЕЛЫ ПРОКУРОРСКОГО НАДЗОРА ЗА ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТЬЮ

Одной из высших ценностей, провозглашаемых Конституцией Российской Федерации¹ и гарантируемых ею всем гражданам нашей страны, является защита прав и свобод человека и гражданина. Признание данного факта нормативно-правовым источником, имеющим высшую юридическую силу на территории России, относится к одному из признаков демократического строя, гуманизации действующего права и стремления общества к обеспечить свободу и интересы каждой отдельной личности. Закрепление прав и свобод человека и гражданина как высшей ценности на страницах Конституции РФ и, следовательно, отождествление указанной ценности как основополагающего принципа права и осуществления правосудия и правоохранительной деятельности в пределах Российской Федерации указывает на то, что обязанность по охране, обеспечении и восстановлении прав и свобод человека и гражданина возлагается на государство и его органы осуществления власти. Однако в целях защиты самого государства, общества, а также каждой отдельной личности от противоправных посягательств как от внешних, так и от внутренних угроз, зачастую используются санкционированные законодателем методы, которые могут ограничивать права и свободы личности в том или ином объеме, затрагивать её интересы.

Логично предположить, что подобная деятельность является прямым нарушением Конституции и иных нормативно-правых актов (Уголовного кодекса, Уголовно-процессуального кодекса и т.д.) Но, как нами уже было указано выше, если такая деятельность получает санкцию государства, значит, опасность от деятельности лица, чьи права ограничиваются по какой-либо причине, представляет собой большую угрозу, чем временное ограничение её интересов. Подобная деятельность, осуществляемая негласно и конфиденциально, имеющая своей целью своевременное пресечение преступлений, предупреждение преступности в целом, а также результативное раскрытие уже совершённых правонарушений, на территории

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС Консультант Плюс [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (Дата обращения: 08.10.2025).

Российской Федерации урегулирована Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».

Несмотря на то, что деятельность сотрудников оперативных подразделений имеет негласную основу и зачастую тем или иным способом ограничивает права граждан, она также подвергается особому контролю извне в целях недопущения превышения должностных полномочий, их злоупотреблением и соблюдения ими принципа законности как фундаментального для российского правоприменительного поля. Данный контроль можно условно разделить на две группы:

- внутриведомственный контроль, осуществляемый согласно иерархии и подчинения одних сотрудников другим;
- внешневедомственный контроль, который в свою очередь подразделяется на судебный контроль и прокурорский надзор.

В данном случае особый интерес представляет прокурорский надзор, так как на данный вид деятельности нашим государством возлагается высшее, приоритетное значение в области соблюдения правоприменителями предписаний закона и соблюдения прав и свобод человека и гражданина. На сегодняшний день мы можем отметить достаточно ярко выраженную тенденцию внутри общества и отстаиванию своих законных прав и интересов, что, в контексте нашего исследования, лишь подтверждает актуальность выбранной темы. Итак, целью данной статьи является изучение сущности прокурорского надзора за оперативно-розыскной деятельностью и её пределы в указанном направлении, так как по закону ОРД осуществляется на конфиденциальной основе и при сочетании гласных и негласных методов, что является одной из обеспечительных мер результативности данного вида правоохранительной деятельности.

Так как деятельность прокурора направлена на защиту прав и свобод личности и контроль за соблюдением должностных лиц предписанных им законом полномочий, мы можем с уверенностью сказать, что существование в России такой отрасли государственной деятельности является одной из демократических побед, потому что именно прокурор вправе выразить сомнение в законности того или иного решения, в том числе, в области оперативно-розыскной деятельности и стать инициатором для проведения специальных проверок в целях уточнения законности и целесообразности тех или иных действий. В области прокурорского надзора за ОРД, который является отдельным видом деятельности прокуратуры в нашей стране, был принят Приказ Генерального прокурора РФ от 09.07.2015 г. № 364 «О внесении изменений в приказ Генерального прокурора Российской Федерации от 15.02.2011 № 33 «Об организации прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности», который внёс существенные изменения в действующий нормативно-правовой акт. Они во многом являются продолжением демократических

настроений, царящих в нашем обществе на сегодняшний день, и одновременно показателем результатов деятельности органов прокуратуры.

Указанным выше документом были внесены изменения в Приложение 1, раздел 2, они касаются отражения деятельности уполномоченного прокурора о количестве обжалованных в процессе судебных решений о даче разрешений на проведение оперативно-розыскных мероприятий, ограничивающих конституционные права человека и гражданина. Данную практику можно оценить как положительную, так как она позволяет оценить тенденцию количества нарушений закона сотрудниками оперативно-розыскных подразделений, темпы её роста или снижения, а также реакцию других должностных лиц на подобные факторы, принятые меры по ликвидации последствий и восстановления социальной справедливости. Однако для того, что говорить об отчётности прокурора о фактах нарушения сотрудниками оперативных подразделений прав и свобод человека и гражданина, мы должны изучить механизм реализации прокурорской проверки, её основные этапы и сущность.

В соответствии с законодательством России при выявлении факта нарушения должностным лицом, уполномоченным осуществлять оперативно-розыскную деятельность, самого закона в области ограничения прав и свобод личности, что может проявиться в превышении должностных полномочий или злоупотребления ими, прокурор обязан принять соответствующие меры по восстановлению социальной справедливости и возмещению ущерба (ч. 9 ст. 5 закона об ОРД). Инициировать данную деятельность может сам прокурор при проведении проверки или на основе жалобы или заявления лица, чьи права были нарушены. Уточним, что мы имеем виду те случаи, когда прокурор непосредственно участвует в судебном заседании при рассмотрении вопроса о негласном ограничении конституционных прав граждан в связи с необходимостью осуществления оперативно-розыскных мероприятий. В п. 4 приказа Генерального прокурора Российской Федерации от 15.02.2011 № 33 уполномоченным прокурорам предписано обеспечить законность при проведении оперативно-розыскных мероприятий, в том числе тех, на проведение которых разрешение дано судом.¹ К ним в соответствии со ст. 6 ФЗ «Об ОРД» относятся:

- контроль почтовых отправлений, телеграфных и иных сообщений;
- прослушивание телефонных переговоров;
- снятие информации с технических каналов связи.

При этом указанный перечень не является исчерпывающим. Вновь обращаясь к тексту Конституции отметим, что одним из гарантированных ею прав является право человека на неприкосновенность жилища (ст. 25).

¹ А.Л. Аристархов, А.Н. Дощицын, М.В. Зяблина. Работа прокурора по обеспечению прав и свобод человека и гражданина//Вестник Академии Генеральной прокуратуры Российской Федерации № 1(51), 2016. С. 40.

Следовательно, проведение таких оперативно-розыскных мероприятий как наблюдение в помещении и его обследование тоже относятся к списку тех, что являются санкционированным ограничением прав граждан и требуют судебного разрешения. Таким образом, любое ОРМ, тем или иным способом затрагивающее указанных в Конституции РФ прав и свобод человека и гражданина, относится к области пределов прокурорского надзора, что справедливо и для проведения соответствующих следственных действий. Важное различие здесь заключается в том, что следственные действия абсолютно всегда носят гласный характер, в то время как ОРМ могут быть проведены и негласно, втайне от самого лица.

Проанализируем порядок проведения оперативно-розыскных мероприятий, форма которого во многом определяет момент начала действия прокурорского надзора и, как его основы, принятия судебного решения. В соответствии с сущностью и сроками проведения ОРМ их порядок можно разделить на общий и неотложный.

В соответствии с общим порядком ОРМ, тем или иным способом ограничивающие права граждан, допускаются только после принятия судебного решения, которое наделяет факт ограничения свобод личности характером санкции государственного органа власти. Говоря о неотложной форме проведения ОРМ, необходимо отметить, что о ней решение может быть принято только в случае, когда любое промедление может привести к совершению тяжкого или особо тяжкого преступления или в случае, когда имеются достаточные данные предполагать, что может быть нарушена охраняемая государством тайна, а также в случае, когда потеря времени для санкционирования судом на проведение ОРМ может стоить государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. В таком случае проведение ОРМ возможно на основании мотивированного постановления руководителя оперативного подразделения. В данном контексте законодатель устанавливает следующие обязательные сроки: 24 часа – вынесение соответствующего постановления уполномоченным на то руководителем; 48 часов с начала проведения ОРМ – получение утвердительного судебного решения, в отсутствии такого – прекращение проведения ОРМ.

Рассмотрим пределы прокурорского надзора при обжаловании вступивших в законную силу решений суда о проведении ОРМ, которое должно быть своевременным и целесообразным. Серьёзным пробелом в законодательстве считаем отсутствие в ФЗ «Об ОРД» закреплённого на государственном уровне механизма уведомления уполномоченного на надзорную деятельность за законностью проведения ОРД прокурора о проведении ОРМ, которые каким-либо образом ограничивают права граждан, и о вступлении в законную силу постановления суда. Законодатель наделяет прокурора правом рассматривать целесообразность и законность проведения ОРМ спустя 72 часа после его окончания при том, что своевремен-

ность проверки соответствия ОРМ закону, особенно в случае неотложной формы проведения, должна быть своевременной, так как любое промедление может означать существенное нарушение конституционных гарантий. Соответственно в целях обеспечения деятельности уполномоченного прокурора по проверке правомерности постановлений руководителей органов, осуществляющих оперативно-розыскную деятельность, об ограничении конституционных прав граждан в Федеральном законе об ОРД необходимо определение порядка такого обжалования, который, как нами уже отмечено выше, не предусмотрен на сегодняшний день российским законодательством.

Одним из способов инициирования проведения прокурорской проверки по факту незаконного осуществления оперативно-розыскного мероприятия является подача лицом жалобы на действия сотрудников правоохранительных подразделений. Указанное право гарантируется Конституцией России по смыслу содержания статьи 33 – каждый имеет право лично или в составе коллектива обращаться в государственные органы власти, а также в органы местного самоуправления. Также анализируемое право личности декларируется частью 2 статьи 45 Конституции – право на защиту своих прав любыми не запрещёнными действующим законодательством способами. Таким образом, подача жалобы лица на действия сотрудников оперативных подразделений является законным способом отстаивания своих интересов, так как рассмотрение жалоб граждан на действия или бездействия должностных лиц – прямая обязанность прокурора, указанная в соответствующем Федеральном законе.¹ Подача жалобы гражданином предполагает обязательность получения ответа на неё с указанием мер, которые были предприняты в соответствии с содержанием обращения, их результатов и принятых управленческих решений.

При поступлении прокурору жалобы от лица, которое полагает, что его права, свободы и законные интересы были нарушены в ходе осуществления сотрудником оперативного подразделения своих должностных обязанностей, возникает вопросы о возможности предоставления прокурору доступа к оперативным сведениям, которые в соответствии с законом представляют собой государственную тайну. Возможны случаи, например, когда рассматривается вопрос об использовании результатов ОРД в ходе предварительного расследования, их рассекречивания и предоставления следователю или дознавателю. Данный процесс осуществляется в соответствии с постановлением сотрудника. Однако далеко не всегда прокурор может получить доступ к сведениям об ОРМ в связи со спецификой деятельности оперативных подразделений. В таком случае достаточно слож-

¹Федеральный закон «О прокуратуре Российской Федерации» от 17.01.1992 № 2202-1 (последняя редакция) СПС Консультант Плюс [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_262/ (Дата обращения: 08.10.2025).

но говорить о качественном прокурорском надзоре за данным видом государственной деятельности и об обеспечении законности.

Законодателем предусмотрена возможность ознакомления прокурора со сведениями, составляющими элементы ОРД и её результатами в соответствии со ст. 21 ФЗ «О прокуратуре». Прокурор, уполномоченный на то Генеральным Прокурором Российской Федерации, вправе обратиться к руководителю органа, осуществляющего оперативно-розыскную деятельность с мотивированным требованием для ознакомления с соответствующими служебными документами и локальными нормативно-правовыми актами. Однако ознакомиться с засекреченными сведениями о лицах, которые осуществляют ОРД, внедрены в организованные преступные группы, осуществляют свою служебную деятельность на негласной основе или конфиденциально сотрудничают с подразделением ОРД прокурор может только при наличии письменного согласия указанных лиц, только если речь не идёт о привлечении их к уголовной ответственности. Данное условие является исключительным.

Знакомясь со сведениями, составляющими предмет оперативно-розыскной деятельности, прокурор берёт на себя обязанность по их защите. Неисполнением им своих служебных обязанностей или ненадлежащее их исполнение, которые могут привести ознакомлению с ними третьих лиц, к обнародованию указанных выше сведений или которые повлекли более серьёзные последствия влечёт за собой уголовную ответственность.

Таким образом, мы установили, что прокурорский надзор за осуществлением оперативно-розыскной деятельности является одним из обеспечительных инструментов законности на территории нашей страны. При этом деятельность прокурора в указанной сфере ограничена законом и режимом секретности, в условиях которого проводятся оперативно-розыскные мероприятия, что не позволяет нам говорить о каком-либо вмешательстве прокуратуры в сферу оперативно-розыскной деятельности.

Свиридов Виталий Витальевич,
доцент кафедры оперативно-разыскной деятельности ОВД
Дальневосточного юридического института
МВД России имени И.Ф. Шилова,
тел: 8-962-501-07-41; e-mail: sviridofdv@yandex.ru

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Современные технологии искусственного интеллекта (далее – ИИ) – это не футуристическая концепция, а реальный инструмент, который уже сегодня помогает нам работать эффективнее.

Главное преимущество ИИ – его способность обрабатывать огромные массивы данных, находить закономерности в различных процессах и освобождать сотрудников от рутины, чтобы они могли сосредоточиться на сложных задачах.

Возможности ИИ успешно используются практически во всех сферах современной жизни: в здравоохранении, в экономике, в транспорте и логистике, в образовании, в финансовой деятельности, в промышленности и многих иных. В последнее время все чаще стали рассматриваться возможности использования ИИ и в различных областях правоохранительной деятельности. На сегодняшний день внедрение в органах внутренних дел различных программно-аппаратных комплексов, предназначенных для выполнения основных функций, постоянно расширяется. И результаты уже есть. Автоматизация рутинных операций сократила время на обработку данных, а прогнозные модели повысили эффективность раскрытия преступлений.

Биометрические системы помогают задержать тех, кто скрывается от правосудия, а также усиливают контроль на границах страны, положительно отражаясь на соблюдении требований в сфере миграционного законодательства. Распознавание лиц позволяет оперативно выявлять подозреваемых, будь то проверка на государственной границе Российской Федерации или сверка с базами данных разыскиваемых лиц. Это не только ускоряет работу оперативных служб и дежурных частей, но и повышает точность решений. При этом технология работает исключительно в рамках текущих задач ведомства, не затрагивая права и законные интересы законопослушных граждан. Полиция сочетает эффективность проводимых мероприятий и соблюдение законных прав граждан. Это достигается путем реализации как организационных, так и технических мер. Обработка и хранение информации осуществляется в территориально распределенных центрах обработки данных, что исключает возможность несанкционированного получения сведений посторонними лицами.

Алгоритмы анализа видео с городских камер уже используются для оперативного поиска подозреваемых и профилактики преступлений. Внедрена система прогнозирования, которая на основе первичных данных помогает оценить шансы на раскрытие дела. Это не случайная вероятность, а математика, подкрепленная опытом специалистов. В равной степени система прогнозирования обеспечивает упреждающей информацией об изменениях в трафике людей в период проведения общественно-массовых, праздничных и спортивных мероприятиях.

Еще одним способом применения ИИ является поиск деструктивного контента в открытых источниках. Мессенджеры, блоги, форумы, социальные сети, информационные каналы, сайты предприятий и государственных органов, информационно-справочные системы сети Интернет, являются бесценным источником информации для сотрудников правоохранительных органов. Оперативными подразделениями органов внутренних дел используются специализированные АПК с применением технологии OSINT. Комплексы подобного рода предназначены для получения данных из открытых источников информации сети Интернет путем выполнения запросов с последующим проведением их аналитической обработки. Система позволяет производить поиск информации по различным источникам данных в сети Интернет, в том числе социальным сетям, мессенджерам, базам данных, электронным СМИ, новостным лентам, электронным сервисам и другим ресурсам сети Интернет, предусматривающим регистрацию пользователей и последующую публикацию информации: форумы, блоги, интернет-магазины, официальные реестры и информационные порталы.

Наравне с уже используемыми новыми технологиями осуществляется тестирование экспериментальных решений. Именно сейчас активно изучается как ИИ и беспилотники могут помочь органам внутренних дел в поиске пропавших людей в труднодоступной природной местности. Это очень актуально применительно к географическим условиям Российской Федерации с ее обширными территориями, особенностями ландшафта, климатическими условиями и временными поясами. Основная цель его использования заключается в обеспечении оперативного и точного определения местонахождения людей в сложных условиях, когда классические методы могут оказаться малоэффективными. Особо важно это в условиях, когда искомое лицо не в состоянии подать ответный сигнал. Применение этих технологий в повседневной деятельности полиции помогает спасать человеческие жизни и является мощным инструментом для полицейских, работающих в условиях, требующих быстрого реагирования, высокой эффективности поиска и своевременного оказания помощи гражданам, оказавшимся в сложной ситуации.

В журналы, карточки, системы первичного учета, информационные системы и иные носители ежедневно вносятся, корректируется и постоян-

но хранится оперативно значимая, конфиденциальная и справочная информация. В этих системах содержатся сведения о правонарушениях, преступлениях, лицах, их совершивших, о владельцах транспортных средств, огнестрельного оружия, о похищенных и изъятых вещах, паспортных данных лиц, а также другая информация, подлежащая хранению.

С момента создания единой системы информационно-аналитического обеспечения деятельности МВД России весь массив этих данных хранится и обрабатывается централизованно. Кроме структурированных данных большое значение имеет хранение огромного количества неструктурированных документов, возникающих в ходе оперативно-служебной деятельности многих подразделений, таких как рапорты, протоколы, акты и другие документы, отражающие ход и результат работы по различным направлениям деятельности.

Программно-технический комплекс «Розыск-Магистраль» ежедневно пополняется внушительными массивами данных о передвижениях всех лиц железнодорожным, воздушным, морским, речным транспортом и рейсовыми междугородними автобусами. Там же аккумулируется информация о совместных поездках с другими лицами, всех этапах поездки: от момента бронирования билета до окончания поездки.

В системах фото- и видеофиксации комплексов «Безопасный город» и специальном программном обеспечении «Паутина» накапливаются данные о передвижениях автотранспорта, дорожной обстановке, состоянии дорожной сети, соблюдении правил дорожного движения. Кроме того, события, происходящие на городских улицах, дорогах, во дворах и в подъездах домов, фиксируются видеокамерами наружного наблюдения государственных, а также различных негосударственных организаций, учреждений и частных лиц.

Немаловажным элементом деятельности как МВД России, так и ряда других государственных органов является предоставление широкого спектра государственных услуг. Результатом данной деятельности является, в частности, постоянное возникновение и накопление большого объема данных социального характера.

Тем не менее, так называемую цифровую реальность следует понимать не как веяние моды, не как некий тренд, а как закономерное явление, развивающееся вне зависимости, желаем ли мы его наступления или нет. Причем субъекты преступной деятельности в этой сфере, по умолчанию, будут опережать субъектов выявления, раскрытия и расследования преступлений, поскольку их стимулирует нечто большее, чем показатели раскрываемости.

Имеющаяся система показателей, по которым оценивается деятельность правоохранительных органов, в частности, органов предварительного следствия, изначально дефектна: она заставляет следователей стремиться не к восстановлению нарушенных прав и свобод или защите от необос-

нованного ограничения прав и свобод, а к направлению уголовного дела с обвинительным заключением сначала к прокурору, а после – в суд. Такая практика негативно сказывается на всей системе правосудия. Исходя из этого, требуется пересмотреть направления оценки деятельности субъектов расследования.

ИИ – это атрибут современной и эффективной оперативно-розыскной и уголовно-процессуальной деятельности, а не основание для отказа от должностных лиц. Потенциал ИИ должен использоваться в той степени, которая позволит успешно реализовывать возложенные функции, а не в противовес имеющейся системе. Поэтому сотрудникам полиции, исходя из своей компетенции, необходимо проходить соответствующее обучение, повышение квалификации по данному направлению работы.

Кроме этого, использование технологий ИИ накладывает ряд требований на аппаратное, программное и сетевое обеспечение. Это одна из важнейших задач, без решения которой применение новых технологий в деятельности полиции невозможно. На сегодняшний день одна из главных проблем применения ИИ в расследовании и раскрытии преступлений заключается в том, что современные технологии пока что далеки от совершенства – не редки случаи ошибок. Естественно, совершенствование ИИ – это вопрос времени. Он постоянно обучается на основе все более разнообразных вводных данных самостоятельно корректировать свои алгоритмы, развивать свои функциональные возможности. Возможно, однажды человечество получит такой автономный ИИ, который будет способен к самостоятельному решению большинства сложных, ресурсозатратных или нестандартных для человека задач, в том числе и в правоохранительной деятельности, а со стороны человека будет требоваться только планомерный контроль либо вмешательство в исключительных случаях (например, сбой в системе).

Для внедрения в деятельность полиции современных технологий необходим комплекс мероприятий по созданию центров обработки данных, строительству высокоскоростных сетей передачи данных, а также обеспечению необходимого уровня информационной безопасности.

При всем этом, важно понимать, что ИИ не заменяет человека. Он не принимает решения – он лишь предоставляет информацию. Окончательный вердикт всегда остается за сотрудником, который учитывает и закон, и человеческий фактор. ИИ – это «цифровой напарник», который усилит профессионализм правоохранителей, а не подменит его.

Семина Мария Владимировна,
слушатель 4 курса Краснодарского университета МВД России

Южанинов Василий Сергеевич,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

НЕКОТОРЫЕ ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В Российской Федерации нелегальная торговля наркотиками остается актуальной проблемой, требующей незамедлительного решения. Применение специализированных знаний во время расследования преступлений, связанных с незаконным оборотом наркотических веществ, играет важную роль в сборе доказательной информации для установления степени виновности подозреваемых лиц.

В 2024 года выявлено 198 тыс. преступлений, связанных с незаконным оборотом наркотиков, что на 3,7% больше, чем за аналогичный период 2023 года. По сравнению с 2023 годом на 7,0% увеличилось число выявленных преступлений, совершенных с целью сбыта наркотических средств, психотропных веществ или их аналогов. Также увеличился их удельный вес в числе преступлений, связанных с незаконным оборотом наркотиков, с 66,1% - в 2023 году до 68,2%. Кроме этого, почти каждое восьмое (12,4%), совершенное с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, совершается с целью незаконного производства, сбыта или пересылки наркотических средств: 94,6 тыс. (+16,1%).

Физическое и психическое состояние населения страны подвергается серьезной угрозе, так как преступления, связанные с незаконным оборотом наркотиков их аналогов и прокуроров, в первую очередь посягают на общественные отношения в сфере общественной нравственности и здоровья населения.

Основным нормативно-правовым актом, регламентирующим отношения в области оборота наркотических средств и определяющим их перечень, является Федеральный закон № 3 от 1998 года «О наркотических средствах и психотропных веществах»¹, кроме этого говоря о нормативной базе нельзя не упомянуть о Указе Президента РФ № 1374 от 2007 года

¹ Федеральный закон «О наркотических средствах и психотропных веществах» от 08.01.1998 № 3-ФЗ (последняя редакция)

«О дополнительных мерах по противодействию незаконному обороту наркотических средств, психотропных веществ и их прекурсоров»¹, который определил основные положения о Государственном антинаркотическом комитете и об антинаркотической комиссии в субъекте Российской Федерации.

Кроме этого, в нашей стране на законодательном уровне определен перечень наркотических средств, психотропных веществ и их прекурсоров, которые подлежат контролю на территории Российской Федерации, закрепленный и регулярно обновляемый постановлением Правительства РФ от 1998 года № 681 «Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации»². В постановлении закреплены 4 списка в соответствии с законодательством Российской Федерации и международными договорами Российской Федерации:

- наркотических средств, психотропных веществ и их прекурсоров, оборот которых в России запрещен;
- наркотических средств и психотропных веществ, оборот которых в России ограничен и в отношении которых устанавливаются меры контроля;
- психотропных веществ, оборот которых в России ограничен и в отношении которых допускается исключение некоторых мер контроля;
- прекурсоров, оборот которых в России ограничен и в отношении которых устанавливаются меры контроля.

Нелегальный рынок наркотических средств, психотропных веществ и их прекурсоров формируется за счет множества источников. Значительная часть запрещенных веществ изготавливается в подпольных лабораториях, которые могут располагаться в жилых и нежилых помещениях, а также на территории научных и образовательных учреждений. Хищения с фармацевтических производств, в том числе подмена препаратов или их неучтенный оборот по поддельным рецептам – это еще один из каналов поступления наркотических средств в незаконный оборот.

Прогресс в сфере информационных технологий привел к значительным изменениям криминальной обстановки. От прямых контактов при продаже наркотиков злоумышленники переходят к дистанционным схемам, задействуя зашифрованные мессенджеры и анонимные платежные сервисы. Благодаря этому снижается риск появления улик и затрудняется поимка преступников на месте преступления. В эту сферу все активнее

¹ Указ Президента РФ от 18.10.2007 № 1374 (ред. от 31.10.2022) «О дополнительных мерах по противодействию незаконному обороту наркотических средств, психотропных веществ и их прекурсоров»

² Постановление Правительства РФ от 30.06.1998 № 681 (ред. 10.07.2023) «Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации»

втягиваются программисты и иные IT-специалисты, создающие автоматизированные площадки для нелегальной торговли, включая специализированные телеграм-боты и сайты.

В целях собственной безопасности преступные сообщества внедряют новейшие разработки: используют защищенные каналы связи и применяют условные обозначения. Для управления процессами применяются приложения с опциями скрытых диалогов и энд-ту-энд шифрованием, гарантирующие удаление истории сообщений. Такие площадки, как Telegram, позволяют сохранять анонимность, не раскрывая содержание переписок, так как информация не хранится на центральных серверах, что создает серьезные препятствия для следственных органов.

Вышеизложенное сильно усложняет выполнение основных задач правоохранительных органов и их оперативных подразделений по противодействию незаконному обороту наркотиков, заключающихся в выявлении, документировании и раскрытии преступлений. Традиционные методы работы, такие как получение показаний свидетелей или опознание, зачастую теряют эффективность.

В связи с этим к оперативным сотрудникам и следователям предъявляются повышенные требования: они должны владеть навыками работы с компьютерной техникой, уметь выявлять, изымать и анализировать цифровые следы на различных электронных устройствах и в сети Интернет.

Практика показывает, что в этих условиях наиболее результативными являются определенные негласные оперативно-розыскные мероприятия. К ним относятся получение компьютерной информации от провайдеров, контроль технических каналов связи, наблюдение с применением аудио- и видеоконтроля, а также проведение проверочной закупки. Выбор и последовательность этих мер должны определяться с учетом всех обстоятельств дела, включая личность преступников, уровень организации их группы и используемые ими технологии.

Важным аспектом расследования является установление IT-квалификации подозреваемых, их навыков в области программирования и защиты информации, а также возможных связей с хакерскими сообществами. Нередко возникает необходимость в сборе материалов, характеризующих биографию и криминальные связи обвиняемых, для их последующего отождествления и проведения необходимых исследований и экспертиз.

В заключение следует отметить, что трансформация незаконного оборота наркотиков под влиянием IT-технологий представляет собой серьезный вызов для правоохранительной системы, так как современный нелегальный наркорынок представляет собой высокоадаптивную гибридную систему, сочетающую традиционные каналы поставок с цифровыми технологиями сбыта и конспирации. Борьба с цифровыми методами преступности невозможна без соответствующего технологического и кадрового оснащения оперативных подразделений. Поэтому преодоление существующих

ющего разрыва между возможностями преступных групп и методами противодействия видится в необходимости разработки и реализации долгосрочной стратегии. Таковая должна включать в себя не только техническое перевооружение, но и фундаментальную переподготовку кадров, развитие проактивных форм оперативно-розыскной деятельности, а также укрепление международного сотрудничества в киберпространстве. Только опережающая подготовка и способность к быстрой адаптации позволят правоохранительным органам успешно противостоять постоянно эволюционирующим угрозам в сфере незаконного оборота наркотиков.

Скрипка София Алексеевна,
слушатель 5 курса
Краснодарского университета МВД России

Горбунов Алексей Николаевич,
доцент кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

ОСУЩЕСТВЛЕНИЕ ВЗАИМОДЕЙСТВИЯ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Специфика и особенности осуществления взаимодействия при раскрытии и расследовании мошенничеств, которые были совершены с применением информационно-коммуникационных технологий (далее - ИКТ), то есть с применением удаленного способа совершения преступления, осуществляется не только правоохранительными органами между собой, но также и со специализированными субъектами ИТ-сферы.

По нашему мнению, осуществления взаимодействия является «залогом успеха» в деятельности по раскрытию дистанционных мошенничеств, которые были совершены с применением ИКТ.

К.И. Озеров¹ отмечает, что повышение численности киберпреступлений в Российской Федерации за последние несколько лет требует объединения усилий правоохранительной системы и субъектов ИТ-сферы, с чем стоит согласиться, поскольку дистанционные мошенничества, как и в целом группа киберпреступлений, тяжело выявляется и расследуется, в особенности если такому преступлению присущ признак транснациональности. В последнем случае взаимодействие должно осуществляться уже на международном уровне, что в свою очередь, может быть усложнено из-за непростого геополитического положения российского государства.

Р.В. Кудрявцев² выделяет следующих субъектов взаимодействия, которые принимают участие (основное или второстепенное) при расследова-

¹ Озеров К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2021. №1 (89). URL: <https://cyberleninka.ru/article/n/raskrytie-moshennichestv-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy> (дата обращения: 19.12.2025).

² Кудрявцев, Р. В. Организация деятельности по раскрытию дистанционных мошенничеств / Р. В. Кудрявцев. – Текст : непосредственный // Молодой ученый. – 2023. – № 24 (262). – С. 218-221.

нии и раскрытии дистанционных мошенничеств, совершаемых с применением ИКТ:

- МВД России и территориальные органы внутренних дел, включая оперативные подразделения;

- ФСБ России, включая оперативные подразделения;

- СК РФ;

- органы прокуратуры;

- международные правоохранительные органы;

- иные государственные органы;

- общественные организации;

- частные компании, специализирующиеся в IT-сфере, например, компания «Лаборатория Касперского», иные компании, занимающиеся разработкой систем и технологий в обозначенной сфере;

- граждане, обладающие навыками и познаниями в сфере информационно-коммуникационных технологий.

Приведём примеры из практики, где при раскрытии дистанционного мошенничества, совершенного с применением ИКТ, было реализовано взаимодействие:

- дело № 1-308/2025 (УИД 91RS0018-01-2025-003072-20)¹;

- дело № 1-155/2025 (УИД 34RS0041-01-2025-001146-87)²;

- дело № 1-121/2025 (УИД 23RS0039-01-2025-000604-57)³;

- дело № 1-89/2025 (УИД 23RS0024-01-2025-000083-87)⁴;

- дело № 1-206/2025 (УИД 34RS0003-01-2025-001438-61)⁵.

Л.О. Ястребова⁶ особо подчёркивает важность осуществления междугородного взаимодействия при расследовании любых видов преступле-

¹ Приговор Сакского районного суда Республики Крым от 10.10.2025 № 1-308/2025 (УИД 91RS0018-01-2025-003072-20) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

² Приговор Урюпинского городского суда Волгоградской области от 23.09.2025 по делу № 1-155/2025 (УИД 34RS0041-01-2025-001146-87) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

³ Приговор Павловского районного суда Краснодарского края от 11.08.2025 по делу № 1-121/2025 (УИД 23RS0039-01-2025-000604-57) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

⁴ Приговор Крымского районного суда Краснодарского края от 05.08.2025 по делу № 1-89/2025 (УИД 23RS0024-01-2025-000083-87) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

⁵ Приговор Кировского районного суда города Волгограда от 23.07.2025 по делу № 1-206/2025 (УИД 34RS0003-01-2025-001438-61) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

⁶ Ястребова Л.О. О некоторых проблемах международного взаимодействия субъектов расследования и противодействия киберпреступлениям // Закон и право. 2022. №7. URL: <https://cyberleninka.ru/article/n/o-nekotoryh-problemah-mezhdunarodnogo-vzaimodeystviya-subektov-rassledovaniya-i-protivodeystviya-kiberprestupleniyam> (дата обращения: 19.12.2025).

ний, которые были совершены с применением информационно-коммуникационных технологий, если такие преступления носили трансграничный характер, поскольку при наличии признака транснациональности мошенничества его физически не возможно раскрыть и расследовать лишь силами национальной правоохранительной системы.

Безусловно, первоначальными действиями при раскрытии мошенничеств с использованием информационно-телекоммуникационных технологий будут считаться оперативно-розыскные мероприятия, закреплённые в статье 6 Федерального закона «Об оперативно-розыскной деятельности»¹, которые связаны с использованием технических средств, а именно, прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации. Но не стоит забывать об особенностях таких преступлений, когда оперативным подразделениям для получения эффективного результата зачастую необходимо рассмотреть целый комплекс мероприятий оперативно-розыскного и технического характера, разработанный практиками и теоретиками в области ОРД.

Приведем примеры из практики, где именно благодаря своевременному проведению ОРД удалось выявить и пресечь дистанционное мошенничество с применением ИКТ:

- дело № 1-104/2025 (УИД 61RS0017-01-2025-000175-08)²;
- дело № -46/2025 (УИД 23RS0054-01-2025-000363-82)³;
- дело № 1-19/2025 (УИД 08RS0011-01-2025-000118-76)⁴;
- дело № 1-20/2025 (УИД 23RS0029-01-2024-001638-88)⁵;
- дело № 1-27/2025 (УИД 91RS0023-01-2025-000102-32)⁶.

Подводя итоги необходимо отметить, что судебная практика судов общей юрисдикции Российской Федерации по делам о мошенничествах, совершенных с применением информационно-коммуникационных технологий, наглядно свидетельствует, что при расследовании данной категории

¹ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 01.04.2025) «Об оперативно-розыскной деятельности» // Российская газета, № 160, 18.08.1995.

² Приговор Красносулинского районного суда Ростовской области от 05.05.2025 по делу № 1-104/2025 (УИД 61RS0017-01-2025-000175-08) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

³ Приговор Туапсинского городского суда Краснодарского края от 28.04.2025 по делу № 1-46/2025 (УИД 23RS0054-01-2025-000363-82) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

⁴ Приговор Черноземельского районного суда Республики Калмыкия от 15.04.2025 по делу № 1-19/2025 (УИД 08RS0011-01-2025-000118-76) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

⁵ Приговор Лазаревского районного суда города Сочи от 07.04.2025 по делу № 1-20/2025 (УИД 23RS0029-01-2024-001638-88) // СПС «КонсультантПлюс» 2025 (дата обращения 19.12.2025).

⁶ Приговор Черноморского районного суда Республики Крым от 03.04.2025 по делу № 1-27/2025 (УИД 91RS0023-01-2025-000102-32)

преступлений очень важно реализовывать взаимодействие как между субъектами правоохранительной деятельности, так с институтами гражданского общества - общественными организациям, субъектами IT-сферы, а также с гражданами, которые обладают соответствующими специальными знаниями.

Также необходимо на современном этапе развивать и расширять сферу международного сотрудничества, так как на современном этапе все большее число преступлений, в частности, совершаемых дистанционных мошенничеств, приобретают признак трансграничности, что делает невозможным их раскрытие и расследования без реализации международного сотрудничества.

Старостенко Олег Александрович,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России,
кандидат юридических наук
e-mail: olegstaros94@gmail.com; тел.: 8 (961) 857-18-88

СОВРЕМЕННЫЕ ПОДХОДЫ К КЛАССИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Использование возможностей технического прогресса в повседневной деятельности позволяет повышать эффективность и расширять человеческие возможности практически во сферах жизни. Например, различные инструменты искусственного интеллекта и Больших данных могут предсказывать тренды, создавать уникальные продукты, самообучающиеся компьютерные системы, в том числе, нейросети и др. Интернет вещей (IoT) автоматизирует рутинные задачи (например, использование системы умного дома позволяет дистанционно с помощью смартфона или планшета управлять бытовыми приборами, регулировать комнатную температуру и др.), оптимизирует работу коммунальных служб, предоставляет расширенную аналитику для выполнения бизнес-задач и мн. др. Облачные технологии продолжают трансформировать различные сферы жизни, предоставляя инновационные решения для эффективного управления информацией (управляют CRM-системами, оптимизируют бизнес-процессы, обеспечивают высокую производительность сервисов и др.). Блокчейн-технологии сокращают время, затрачиваемое на идентификацию происхождения приобретаемого продукта, способствуют проведению транзакций без посредников, созданию смарт-контрактов и др.¹.

Вместе с тем вышеуказанные технологические новшества породили и ряд негативных тенденций: информационные войны, информационный терроризм, различные преступления в сфере компьютерной информации (неправомерный доступ; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации; мошенничество в сфере компьютерной информации) и др.². Так за январь-декабрь 2024 г. в России зарегистрировано 765,4 тыс. преступлений в сфере компьютерной информации, что на 13,1% больше, чем за аналогичный период прошлого года. Четыре преступления из пяти совершаются с ис-

¹ Шарипова А.А. Проблемы противодействия киберпреступности в России // Моя профессиональная карьера. 2024. Т. 1, № 57. С. 162-168.

² Овчинский А.С. Информационное противоборство с деструктивными сетевыми сообществами / А. С. Овчинский, К. К. Борзунов // Информация и безопасность. 2024. Т. 27, № 2. С. 159-168.

пользованием сети Интернет (649,1 тыс.), почти половина (45,2%) – средств мобильной связи¹.

Проведенные нами ранее исследования в области компьютерных преступлений позволяют сделать вывод о том, что основной их массив составляют кражи и мошенничества, совершаемые путем обмана или злоупотребления доверием. Данная категория преступлений характеризуется относительной простотой их совершения (не требует от преступника глубоких познаний в области IT-технологий²), направлена, как правило, на самые незащищенные слои населения (подростки, пожилые), обусловлена использованием методов социальной инженерии. Правоохранительными органами в целях противодействия указанным преступлениям выработан достаточно неплохой алгоритм действий: практически в каждом подразделении уголовного розыска на районном уровне имеются методические рекомендации по раскрытию наиболее распространенных телефонных и интернет-мошенничеств, образцы запросов. Практически все такие преступления выявляются оперативными подразделениями органов внутренних дел³.

Наибольшую тревогу вызывают более технологичные преступления, совершаемые путем уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств ее защиты. На расширенном заседании коллегии МВД России В. Колокольцев отметил, что самыми противоречивыми противоправными деяниями, связанными с использованием лжи, манипулирования и эксплуатации чужой доверчивости, являются преступления, совершаемые путем искусственного видоизменения компьютерной информации. Ущерб от таких деяний за текущий год превысил 75 млрд. руб⁴. Значительную его часть формируют посягательства, совершаемые с использованием высокотехнологичных программных средств.

Низкая доля раскрываемости таких преступлений, отсутствие понимания механизмов их совершения, высокий общественный резонанс⁵ обу-

¹ Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года [Электронный ресурс]. URL: <https://мвд.рф/> (дата обращения 27.10.2025).

² Старостенко О.А. Виктимологическое предупреждение дистанционных хищений / Москва: Издательский дом «Юрлитинформ», 2024. 152 с.

³ Глава МВД: каждое второе преступление в РФ совершается в киберпространстве [Электронный ресурс]. URL: <https://tass.ru/proisshestviya/21951535> (дата обращения 26.10.2025).

⁴ Владимир Путин выступил на ежегодном расширенном заседании коллегии Министерства внутренних дел России [Электронный ресурс]. URL: <http://www.kremlin.ru/events/president/transcripts/73770> (дата обращения 27.10.2025).

⁵ Иванов С.И. Особенности взаимодействия при ведении оперативно-розыскной операции органами внутренних дел / С. И. Иванов // Вестник Казанского юридического института МВД России. 2020. Т. 11, № 1(39). С. 108-112.

словливают необходимость разработки основных классификационных моделей преступлений в сфере компьютерной информации.

Анализ приговоров суда (произведен анализ 212 приговоров суда за период 2017-2024 гг. по фактам совершенных преступлений в сфере компьютерной информации) и контент-анализ в сети Интернет позволили определить основные классификационные модели преступлений в сфере компьютерной информации:

1. «Новичок». Неправомерный доступ к компьютерной информации осуществляется должностными лицами в корыстных интересах. Данная категория преступлений является самой простой и требует от преступника комплекса навыков и знаний в области использования IT-технологий на уровне «Новичок» (как правило, ограничивается вводом логина и пароля, позволяющего осуществить доступ к сайту организации). Неправомерный доступ осуществляется должностными лицами при осуществлении своих профессиональных обязанностей в целях получения незаконного денежного вознаграждения.

Так, например, заведующая поликлиникой «XXX» получила в Единой системе идентификации и аутентификации доступ к учетной записи (логин и пароль), выделенной для внесения сведений о вакцинированных против коронавирусной инфекции гражданах.

С июня 2021 года у нее из корыстной заинтересованности возник преступный умысел, направленный на внесение за денежное вознаграждение недостоверных сведений в ЕГИС в сфере здравоохранения о вакцинации против коронавирусной инфекции без фактического её прохождения, путем осуществления неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ.

15 августа 2021 года вышеуказанная гражданка за денежное вознаграждение внесла сведения о прохождении К. вакцинации от COVID-19 и выдачи последнему сертификата без фактического ввода вакцины в организм последнего, тем самым произвела модификацию компьютерной информации путем ввода в регистр персональных данных, что повлекло за собой нарушение целостности, достоверности, объективности и актуальности информации¹.

2. «Пользователь». Неправомерный доступ к компьютерной информации осуществляется должностным лицом, действующим в корыстных интересах. Данная модель является более усложненной и требует от преступника определенных навыков работы со специализированным про-

¹ Приговор № 1-25/2024 1-308/2023 от 22 февраля 2024 г. по делу № 1-115/2023 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/aM5NTfvRN6j/?regular=®ular-lawchunkinfo=®ular-date_from=®ular-date_to=®ulkflow_stage=®ular-area=®ular-judge=&snippet_pos=2696#snippet (дата обращения 27.10.2025).

граммным обеспечением (программы для бухгалтерского учета, издательские системы и др.), предназначенным для нормального функционирования малого и большого бизнеса или созданным под конкретные профессиональные потребности, работающим по заранее проверенным алгоритмам. Воздействие на компьютерную информацию происходит при осуществлении трудовых обязанностей.

Так, сотрудник офиса продаж АО «YYY» (г. XXX) обладал доступом к конфиденциальной информации клиентов ПАО L, а также был хорошо знаком с функционалом специализированного ПО – системы «1С Предприятие», применяемой компанией для обслуживания абонентов.

В период с января по июнь 2024 года неизвестное лицо предложило ему денежное вознаграждение за незаконную передачу персональных данных абонентов ПАО L, не имея на это прав. Это сподвигло сотрудника на злоупотребление служебным положением: с корыстной целью он осуществил несанкционированный доступ к защищённой законом информации о звонках абонентов и скопировал её.

С целью реализации преступного умысла, специалист, находясь в помещении фирменного салона продаж и обслуживания, обладая в силу своего служебного положения возможностью пользоваться в служебных целях ресурсами и техническими средствами организации, действуя из корыстной заинтересованности, посредством использования штатного программного обеспечения для просмотра абонентской базы и служебной ЭВМ через принадлежащую ему учетную запись, не имея запроса абонента либо иных законных оснований, осуществил неправомерный доступ к охраняемой законом компьютерной информации, находящейся в программном модуле «1С предприятие» (информации о персональных данных владельцев абонентских номеров), после чего незаконно копировал её путем фотографирования на свой сотовый телефон и с помощью мессенджера «Телеграмм» отправлял неустановленному лицу¹.

3. «Уверенный пользователь». Копирование, модификация, блокирование компьютерной информации осуществляется лицами (не только должностными), обладающими достаточно глубокими познаниями, связанными с эксплуатацией средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Они, как правило, уверенно работают с операционными системами, умеют управлять файлами и папками, знают основы программирования. Обобщение изученных приговоров позволяет констатировать, что основными мотивами совершения компьютерных преступлений представителями рассматриваемой модели выступают корысть, любопытство, состояние недо-

¹ Приговор № 1-353/2023 1-40/2024 от 26 января 2024 г. по делу № 1-353/2023 [Электронный ресурс]. URL: <https://sudact.ru/regular/doc/nnDVOPbpMhNJ> (дата обращения 28.10.2025).

влетворенности доходом, протестное настроение, месть (в том числе против работодателя).

25 апреля 2023 года гражданин Х, бывший системный администратор компании Y, уволенный по собственному желанию, из чувства неприязни к руководству незаконно проник в корпоративную информационную систему предприятия. Используя смартфон с доступом в интернет и административные данные от веб-ресурса L, он авторизовался в панели управления сайтом. Далее злоумышленник скопировал исходные файлы главной страницы, после чего заменил её содержимое: разместил изображение радиопрозрачного укрытия с оскорбительной надписью, а также добавил два аналогичных файла с нецензурными выражениями в адрес руководства компании. Все изменения были сохранены на сервере, а оригинальные данные - удалены¹.

4. «Продвинутый пользователь». Преступления в сфере компьютерной информации осуществляются лицами, обладающими глубокими знаниями и навыками работы с компьютером (не только должностными), включая профессиональные программы и более сложные технические задачи. Они свободно ориентируются в операционных системах, могут не только выполнять стандартные задачи, но и адаптировать программное обеспечение под свои потребности, знают принципы работы «Даркнета», стараются использовать в работе инструменты анонимизации. Основными мотивами совершения преступлений рассматриваемой модели выступают корысть, любопытство, влияние извне, самоутверждение.

Так в период с 8 по 28 сентября 2023 года гражданин Х, воспользовавшись своими знаниями в сфере IT, предпринял попытку незаконного доступа к защищённой компьютерной информации. Для этого он зашёл через предустановленный браузер Tor в даркнет, где приобрёл у анонимного продавца вредоносный софт. Установив его на свою игровую консоль Sony PlayStation 3, он осознанно использовал пиратское ПО, предназначенное для обхода систем защиты. Данное программное обеспечение позволяло отключать встроенные механизмы безопасности консоли, включая проверку цифровых подписей, что давало несанкционированный доступ к модификации системного ПО устройства².

5. «Эксперт». Киберпреступник является высококвалифицированным специалистом в области программирования, администрирования, разведки сети, манипулирования реестром, обслуживания сетевой архитектуры. В своей деятельности с целью обеспечения высокого уровня маскировки, из-

¹ Приговор № 1-439/2023 1-50/2024 от 17 января 2024 г. по делу № 1-439/2023 [Электронный ресурс]. URL: <https://sudact.ru/regular/doc/m9BSsgO0B7dw/?page=4®ular-txt=неправомерный+доступ®ular-case> (дата обращения 29.10.2025).

² Постановление № 1-44/2024 от 23 января 2024 г. по делу № 1-44/2024 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/2J5z2u3vKzYc/?-case_doc=®ular-lawchunkinfo=®ular-date_from (дата обращения 29.10.2025).

бежания обнаружения и обхода ограничений использует исключительно специализированное программное обеспечение (I2P, Tor Browser, VPN-сервисы с автообновлением и платной подпиской). Основным источником заработка у данной классификационной модели является черный хакинг (незаконная деятельность в киберпространстве, направленная на предоставление услуг в «Анонимном Интернете¹»): кража финансовых данных, промышленный шпионаж, создание и распространение вредоносного программного обеспечения, взлом аккаунтов социальных сетей и др. Данная категория лиц является одной из самых опасных, так как посягает на безопасность не только отдельных пользователей, но и государства в целом, а также практически не выявляется правоохранными органами. Их мотивация может быть разнообразной, но в основном это финансовая выгода, идеологические или политические убеждения, престиж и признание, жажда неограниченной свободы, любопытство и озорство.

Так, 01.02.2023 г., гр. Х., У., Р., действуя незаконно, являясь высококвалифицированными специалистами в области программирования, осуществили неправомерный доступ к компьютерной информации различных организаций.

Действуя в группе лиц, арендовали иностранные сервера и установили на них разработанное в составе группы вредоносное программное обеспечение, предназначенное для нейтрализации средств защиты компьютерной информации путём перебора логина и пароля; сканирования диапазона IP-адресов в целях выявления открытых портов, блокирования и модификации компьютерной информации; зарегистрировали кошельки виртуальных активов криптовалюты «Биткойн», которые использовали для выдвижения требований пользователям атакованных ЭВМ, а также по распределению преступной прибыли.

Таким образом, путем брутфорс-атаки² осуществили модификацию и блокирование охраняемой компьютерной информации, содержащейся в информационных системах и информационно-телекоммуникационных сетях, функционирующих в субъекте оборонной промышленности - АО «Восточная верфь», которые являются объектом критической инфраструктуры³.

Резюмируя вышеизложенное, отметим, что представленные классификационные модели не могут претендовать на абсолютную полноту и до-

¹ Хакеры Черные шляпы, Белые шляпы и Серые шляпы – определение и описание [Электронный ресурс]. URL: <https://www.kaspersky.ru/resource-center/definitions/hacker-hat-types> (дата обращения 29.10.2025).

² Брутфорс-атака: определение, примеры, защита [Электронный ресурс]. URL: <https://www.kaspersky.ru/resource-center/definitions/brute-force-attack> (дата обращения 29.10.2025).

³ Приговор № 1-376/2019 от 25 сентября 2023 г. по делу № 1-376/2019 [Электронный ресурс]. URL: <https://sudact.ru/regular/doc/ltnpYevhAgdP/?regular-txt> (дата обращения 29.10.2025).

стоверность ввиду интенсивного изменения диапазона и структуры преступлений, совершаемых в сфере компьютерной информации (на фоне не прекращающегося технического прогресса). В то же время полученный нами результат (предложенные модели) может быть использован в следующих целях:

1. Единообразное понимание феномена. Классификация способствует разграничению преступлений по критериям, что, в свою очередь, облегчает процесс раскрытия и расследования преступления.

2. Системные исследования преступной деятельности. Представленные модели могут послужить базой для последующих научных изысканий в области киберпреступлений и разработки практических рекомендаций по их раскрытию и расследованию.

3. Выявление признаков преступлений. Разработанные классификационные модели могут создать благоприятные условия для выявления признаков преступлений как на этапе расследования, так и на этапе производства оперативно-розыскного мониторинга сети Интернет на предмет преступных действий.

4. Квалификация преступлений. Предложенные модели могут быть использованы для установления соответствий между признаками совершенного деяния и признаками состава преступления.

5. Разработка основных тактических приемов для эффективного раскрытия киберпреступлений (служат теоретической и информационной базой).

6. Построение оперативно-розыскных и следственных версий. Классификация помогает структурировать, детализировать, конкретизировать информацию относительно обстоятельств совершения преступления, что облегчает процесс выдвижения обоснованного предположения о его событии.

7. Предупреждение преступлений. Указанная типология, а также выделенные в ее составе признаки (мотивы, способы и др.), позволяют определить закономерности и тенденции преступлений в сфере компьютерной информации, что, в свою очередь, может быть использовано при разработке целевых профилактических мер.

Степанов Сергей Максимович,
преподаватель кафедры оперативно-разыскной
деятельности ОВД учебно-научного комплекса
противодействия экономическим и налоговым преступлениям Нижегород-
ской академии МВД России

РОЗЫСК ВОЕННОСЛУЖАЩИХ СОТРУДНИКАМИ ПОЛИЦИИ: ПРАКТИКА И ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ

В каждом территориальном органе МВД России, функции по розыску лиц осуществляет отделение уголовного розыска. С учетом начала специальной военной операции, на территории Нижегородской области получилось, что подразделения министерства обороны, отвечающие за розыск военнослужащих, не справляются с потоком таких лиц, в связи, с чем вынуждены обратиться за помощью в полицию. В настоящей статье, мы с Вами рассмотрим, кто и в какой мере обязаны следить за мероприятиями по установлению местонахождения солдат и матросов, оставивших места службы, совершивших преступные деяния, а также определим организаторов и исполнителей в лице, военной полиции, комендатуры, оперативного состава полиции.

Законодатель в пункте 12 статьи 12 Федерального закона № 3-ФЗ «О полиции»¹ определил основные задачи отделения розыска лиц отдела уголовного розыска, а именно: разыскивать лиц, совершивших преступления или подозреваемых и обвиняемых в их совершении, скрывшихся от органов дознания, следствия и суда, несовершеннолетних самовольно ушедших из семей или из специализированных учреждений, лиц уклоняющихся от недобровольной госпитализации, назначенной судом, пропавших без вести, иностранных граждан, подлежащих административному выдворению, осуществлять мероприятия по установлению похищенного имущества. В указанной статье закона, нет прямой обязанности стражей правопорядка осуществлять розыск солдат. Каким образом законодатель разграничил полномочия полиции и военных, для этого следует изначально обратиться к терминологии.

Правовой статус определяется статьей 2 Федерального закона от 27.05.1998 года № 76-ФЗ «О статусе военнослужащих», где указаны офицеры, прапорщики, мичманы, курсанты военных образовательных организаций, проходящие службу по контракту. В пункте 6 статьи 14 Федерального закона от 07.02.2011 года №3-ФЗ «О полиции» определено, что сотрудники МВД могут задержать военнослужащих и граждан России, при-

¹ Федеральный закон // Федеральный закон "О полиции" от 07.02.2011 № 3-ФЗ (последняя редакция) URL: https://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 10.10.2025).

званных на военные сборы, подозреваемых в совершении преступления – до передачи их военной полиции Вооруженных сил России, командирам воинских частей или военным комиссарам. На первый взгляд довольно просто и понятно, оперативный состав оказывает содействие последним, ловит вышеуказанных лиц и ждет группу. Однако возникает вполне закономерный вопрос, о силах и средствах, затраченных ресурсах МВД, поскольку сотрудникам уголовного розыска приходится заводить розыскное дело, проводить мероприятия на установление местонахождения, осуществлять доставку в отдел внутренних дел. Со стороны военной комендатуры лишь функция конвоирования. Обращаю ваше внимание, что комендант, сотрудники военной полиции не задерживают граждан по линии общеуголовной преступности, для передачи, например, участковым-уполномоченным полиции.

В теории, законодатель предусмотрел конкретные разграничения, а именно, на основании Федерального закона от 28.03.1998 года №53-ФЗ «О воинской обязанности и военной службе»¹ в статье 4 «обязанности должностных лиц ...», пункт 3 отведен представителям ОВД России, где определены компетенции, в частности «осуществлять розыск и при наличии законных оснований задерживать граждан, уклоняющихся от призыва на военную службу, лиц, самовольно оставивших воинскую часть, либо место прохождения военной службы, если в отношении указанных граждан осуществляется уголовное преследование». Для полномочий по розыску солдат и матросов существует указ Президента РФ от 25.03.2015 года №161 «Об утверждении Устава военной полиции Вооруженных Сил Российской Федерации и внесении изменений в некоторые акты Президента Российской Федерации», где установлены пункты 189-191, в которых определено, что меры по розыску военнослужащих и военного имущества, их местонахождение, уклоняющиеся от прохождения службы, оказание содействия ОВД РФ в розыске и задержании военнослужащих, оставивших воинские части, подозреваемых и обвиняемых в совершении преступлений, скрывшихся от органов следствия или суда, возложены на военного коменданта гарнизона или лицо, его замещающее, на командиров воинских частей, на сотрудников военной полиции. В пункте 194 данного нормативно-правового акта указано, что меры по розыску военного, самовольно оставившего место службы с оружием и его задержание, проводятся во взаимодействии с ОВД России.

При анализе приведенного законодательства, можно подвести итог:

¹ Федеральный закон // Федеральный закон «О воинской обязанности и военной службе» от 28.03.1998 N 53-ФЗ (последняя редакция) URL: https://www.consultant.ru/document/cons_doc_LAW_18260/ (дата обращения: 10.10.2025).

Полиция	Военные структуры (ВП, комендатура)
Могут задерживать военнослужащих – передавать военным	Розыск и задержание военных, установление похищенного имущества
Розыск уклонистов	Розыск уклонистов
Розыск в отношении кого есть уголовное преследование	Оказание содействия ОВД РФ в розыске лиц – уголовное преследование
Розыск самовольно оставивших ВЧ	Оказание содействие ОВД РФ в розыске военных оставивших ВЧ (с оружием)

Таким образом, можно обратить внимание, что в одном случае, сотрудники полиции выступают вспомогательным элементом для военных, в другом варианте наоборот.

Даже с учетом разграничения обязанностей, на практике, к сожалению, выстраивание работы проходит в одну сторону – розыск лиц на основании Федерального закона «О полиции», а так же солдат и матросов ложится на плечи системы МВД России. Для подтверждения доводов, предлагаю обратиться к практике Нижегородской области. В силу грифа секретности, мной не будут приводиться определенные данные.

Сотрудникам уголовного розыска отделов полиции поступают сведения от следователей военно-следственного отдела по Нижегородскому гарнизону об оказании содействия в розыске лиц, оставивших воинскую часть. Так, оперативным службам приходится заводить розыскное дело и проводить мероприятия, как мной, указывалось выше, другие же готовят лишь анкетные сведения подозреваемого, при результативности поиска – конвоируют солдат, сотрудники военной комендатуры. Получается, что основная работа находится в ведении стражей правопорядка. Такая система выстроенной работы имеет недостаток и в оперативности совместных действий, поскольку на практике, встречаются случаи, когда военнослужащий в силу ранения, утери связи при выполнении служебно-боевых задач, по умолчанию становится преступником – возбуждается уголовное дело по статье 337 УК РФ «Самовольное оставление части или места службы»¹. В случае выздоровления бойца, установления контакта с начальством воинской части, от следователей военно-следственного отдела, информации, для полиции не поступает. Поскольку база данных – розыск лица, ведется правоохранительными органами, а сведения от следова-

¹ Уголовный кодекс РФ // УК РФ Статья 337. Самовольное оставление части или места службы URL: https://www.consultant.ru/document/cons_doc_LAW_10699/cf4cd66e4abf91af27d26fb3a88f3c792d1fa26a/ (дата обращения: 10.10.2025).

теля отсутствует, представителям уголовного розыска приходится устанавливать местонахождение и задерживать солдата, однако, если инициатор военного ведомства передал данные и рапортом попросил бы снять с розыска, количество затраченных сил и ресурсов МВД России сократилось. Так, в одном из отделов полиции г. Нижнего Новгорода, заведено розыскное дело в отношении водителя воинской части, оперуполномоченными уголовного розыска проводились мероприятия на установление нахождения разыскиваемого, в результате обнаружилось, что лицо вернулось в воинскую часть пол года назад – в связи с чем, уголовное преследование прекратилось. Представители следственных органов пояснили, что воинские части расформировались и создались другие, поэтому новый сотрудник не знал с кем можно обменяться информацией из полиции. В других случаях, когда военнослужащие получают ранение, их эвакуируют в военный госпиталь, те в свою очередь не могут сообщить, какие именно места лечения у них будут. Поскольку могут быть переполнены койкоместа, данных солдат распределяют по заполняемости медицинского учреждения. Поэтому следователям военного гарнизона ничего не остается, как снова обращаться к помощи полиции. Хотелось бы уточнить, что существуют разного рода ситуации и служебно-боевые задачи, однако не от руководства воинской части, не от медицинской службы министерства обороны, не от сотрудников комендатуры¹ не поступает информации о нахождении бойцов, а наоборот – первая инстанция для рассмотрения отсутствия солдата выступают представители системы МВД России. Такая же практика наблюдается и в пунктах отбора на военную службу по контракту, где граждан не проверяют должным образом, и такие лица, с судимостью, в статусе нахождения в федеральном розыске, выполняют боевые задачи.

При указанной работе, на текущий момент на территории Нижегородской области уже зафиксирована перегрузка оперативных подразделений, статистическая отчетность по линии – преступники, настолько завысила показатели, что при заведении новых розыскных дел приходится оформлять с пометкой «утрата родственных связей». С учетом кадрового дефицита в системе полиции, выполнением основной работы по розыску лиц, следует констатировать факт – либо необходимы изменения в совместную деятельность подразделений, либо в скором времени искать военных будет не кому.

В связи с чем, могут быть предложены следующие варианты решения проблемы: до заведения розыскного дела необходим бланк, в котором

¹ Приказ Министра обороны России // Приказ Министра обороны РФ от 16 июля 2021 г. № 424 «Об утверждении типовых положений о региональном и территориальном органах военной полиции Вооруженных Сил Российской Федерации» URL: <https://base.garant.ru/402958222/3e22e51c74db8e0b182fad67b502e640/?ysclid=mgrxrk1nsd582451567> (дата обращения: 10.10.2025).

будут стоять подписи следователя, руководителя, заместителя воинской части, представителя военной полиции, либо комендатуры, в котором будут указаны мероприятия на установление местонахождения лица, вот в таком случае, когда бойца нет ни в новой части, ни в больнице, ни прикомандирован, задействованные силы не позволяют дальше проводить поиски, следует обращаться за помощью в МВД. Еще один вариант, сотрудникам правопорядка заводить розыскное дело, только при наличии информации, что солдат покинул место службы с оружием, в иных случаях необходимо проработать вопрос о поисковых мероприятиях, только усилиями военного учреждения. Следующая альтернатива, сотрудники уголовного розыска в рамках розыскного дела проводят мероприятия на установление местонахождения лица, обязанность же представителей министерства обороны¹, ежемесячно уведомлять оперативные службы полиции об их деятельности, путем составления плана, предоставлением контактных данных сотрудников, направлением сведений на служебную почту.

Мной предложены лишь малая часть решения возникших проблем по розыску военнослужащих, к сожалению, некомплект уполномоченных сотрудников свойственен и оборонному ведомству, поэтому сокращение бюрократии, налаживание контактов обмена известиями, создание совместных рабочих групп, могут повлиять на результат. При текущих тенденциях, как мной было указано ранее, будут перегружены обе структуры.

¹ Юриспруденция // Меры по розыску военнослужащих и военного имущества Вооруженных Сил России URL: https://www.consultant.ru/document/cons_doc_LAW_177125/939ee11399523e6403e8fb52e29a78b2bbe51564/ (дата обращения: 10.10.2025).

Студнев Александр Сергеевич,
старший преподаватель
кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
тел.: 8-920-675-56-70; e-mail: alexandr.studneff@yandex.ru

Широков Илья Владимирович,
слушатель 5 курса
Краснодарского университета МВД России
тел.: 8-909-445-58-50; e-mail: iliuha.shirokov@yandex.ru

ОПЕРАТИВНО-РОЗЫСКОЕ ПРОТИВОДЕЙСТВИЕ ПРИ ФИНАНСИРОВАНИИ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

Проблема финансирования терроризма остается важнейшей в борьбе с экстремистскими организациями. Они используют различные стратегии для получения и перемещения средств, начиная от традиционных методов, таких как контрабанда, незаконный оборот наркотиков и вымогательство, и заканчивая электронными средствами платежа, такими как криптовалюты или замаскированные сборы с граждан. По данным Организации Объединенных Наций, почти 40% финансовых операций, связанных с терроризмом, осуществляются через предприятия, что затрудняет выполнение задачи по выявлению такой деятельности.

В последние годы наблюдается заметный сдвиг в сторону цифровых платежных систем. Выявленные тенденции актуализируют необходимость формирования у правоохранительных органов, прежде всего в системе Министерства внутренних дел Российской Федерации, профессиональных компетенций в сфере мониторинга и выявления противоправных финансовых операций, совершаемых с использованием современных информационно-телекоммуникационных технологий. Особую обеспокоенность вызывает использование интернет-пространства и цифровых валют в целях финансового обеспечения террористической деятельности. В качестве иллюстрации можно привести функционирование анонимных торговых площадок в даркнете, таких как Hydra (деятельность которой была пресечена в 2022 году), обеспечивавших возможность проведения нелегальных транзакций в условиях повышенной анонимности. Дополнительным фактором, осложняющим противодействие, выступает применение криптовалют (в частности, Bitcoin), обладающих расширенными механизмами конфиденциальности.

По данным Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), в 2023 году зафиксирован прирост объема криптовалютных транзакций, имеющих признаки связи с террористической дея-

тельностью, на 27% по сравнению с предшествующим периодом. Указанная статистика убедительно свидетельствует о насущной потребности в разработке для сотрудников правоохранительных органов специализированных методик выявления и документирования фактов финансирования экстремистской деятельности, совершаемых в сети Интернет.

Вовлечение молодежи в процессы финансирования терроризма детерминировано комплексом социально-психологических факторов. Их изучение и учет в оперативно-розыскной и профилактической деятельности представляется необходимым условием для выстраивания эффективной системы противодействия данному негативному явлению.

Подростки и молодые люди, особенно в возрасте 16-24 лет, часто подвержены вербовке из-за своей социальной значимости, ограниченной правовой осведомленности и частого использования цифровых сервисов. Террористические организации пользуются этими уязвимостями, используя такие платформы, как Telegram-каналы, онлайн-казино и стриминговые платформы для привлечения молодежи. Например, в 2020 году фонд «Мухаджирун», маскируясь под благотворительность, собирал деньги в социальных сетях и переводил их на счета лиц, связанных с ИГИЛ (организация, запрещенная на территории РФ).

По данным следствия, собранные средства использовались для приобретения оружия, обмундирования, боеприпасов, продуктов питания и медикаментов. На учредителей фонда, Исраила Ахмеднабиева и Амину Лорсанову, были заочно возбуждены уголовные дела по ч. 4 статьи 205 УК РФ «Организация финансирования терроризма». Феномен неосознанного вовлечения молодежи в механизмы финансового обеспечения террористической деятельности получил распространение в ряде субъектов Российской Федерации. Как свидетельствуют эмпирические данные, молодые люди, не идентифицируя себя в качестве участников противоправных финансовых схем, оказывались интегрированными в структуры террористических сетей посредством участия в онлайн-азартных играх и активности, сопряженной со стриминговыми мероприятиями. Подобные формы цифрового взаимодействия, маскируясь под легитимные развлекательные практики, фактически выполняют функцию каналов транзакционной поддержки деструктивных элементов. Выявленная закономерность актуализирует необходимость углубленного изучения механизмов трансформации рекреационной онлайн-активности в инструментарий теневого финансирования, а также разработки превентивных мер, ориентированных на молодежную аудиторию как наиболее уязвимую категорию пользователей глобальной сети¹.

¹ Под маской исламской благотворительности мошенники спонсируют терроризм. URL: <https://kavtoday.ru/article/5642> (дата обращения: 07.10.2025).

Масштаб и системный характер проблемы вовлечения молодежи в финансирование террористической деятельности находят свое подтверждение в результатах оперативно-служебной деятельности правоохранительных органов. Так, в 2022 году сотрудниками Федеральной службы безопасности Российской Федерации была пресечена противоправная деятельность, связанная с функционированием специализированного канала в мессенджере Telegram, посредством которого осуществлялся сбор денежных средств в пользу международной террористической организации «Исламское государство» (запрещена в Российской Федерации). Данный случай является эмпирическим подтверждением трансформации методов финансового обеспечения деструктивных структур, активно использующих современные информационно-коммуникационные технологии и вовлекающих в противоправную деятельность различные категории граждан, включая молодежь¹. Криминологический анализ указанного канала выявил, что доминирующую возрастную категорию его участников составляли лица от 18 до 24 лет. Финансовые операции по переводу средств осуществлялись преимущественно с применением криптовалютных кошельков и сервисов электронных платежных систем, что обеспечивало повышенную анонимность транзакций. Параллельно зафиксированы прецеденты использования блогерского сообщества: отдельные лидеры мнений через популярные видеохостинги (YouTube) и социальные платформы (Instagram) агитировали свою аудиторию инвестировать в лжеблаготворительные «криптопроекты». Последующие оперативно-следственные мероприятия установили, что аккумулированные подобным образом финансовые ресурсы перенаправлялись на организацию и осуществление террористических актов. Данные факты свидетельствуют о трансформации методов финансовой подпитки терроризма, где социальные медиа и цифровые валюты выступают в качестве единого криминального конвейера, а молодежная аудитория – в качестве ресурсной базы для сбора средств. По данным МВД РФ, в 2023 году было закрыто более 20 таких платформ, а их создателям были предъявлены обвинения по статье 205.1 Уголовного кодекса России.

Для того, чтобы уменьшить ущерб от вышеназванных действий, сотрудники оперативных подразделений ОВД используют различные методы и средства, для их выявления. К ним относятся такие действия как мониторинг информации в социальных сетях, а также взаимодействие с банками, для отслеживания подозрительной финансовой деятельности. Однако эксперты утверждают, что успех этих мер зависит от законодательных ре-

¹ В России заблокировано 450 сайтов по сбору средств для боевиков ИГИЛ. URL: <https://www.ridus.ru/v-rossii-zablokirovano-450-sajtov-po-sboru-sredstv-dlya-boevikov-igil-204029.html> (дата обращения: 07.10.2025).

форм, в частности от поправок к Федеральному закону № 35-ФЗ «О противодействии терроризму», который регулирует движение криптовалют¹.

Сложившаяся ситуация в стране и мире требует немедленных и инновационных изменений. Одним из ключевых подходов является устранение экономической составляющей террористических и экстремистских организаций путем создания надежной национальной системы противодействия их финансированию. С этой целью 30 мая 2018 года Президент России утвердил концепцию, определяющую развитие национальной системы борьбы с отмыванием денег и финансированием терроризма². В этом документе определены основные цели, задачи и области риска, подчеркивается важность сокращения числа преступлений, связанных с финансированием терроризма, с помощью передовых методов обнаружения, расследования и раскрытия преступлений. Эффективное решение этой проблемы требует скоординированных усилий уполномоченных органов, осуществляющих оперативно-розыскную деятельность, а также систематической организации их работы.

Одним из приоритетных направлений деятельности органов внутренних дел является противодействие финансированию терроризма, которое предполагает применение целого ряда методов выявления и пресечения незаконных финансовых потоков при одновременном предотвращении вовлечения молодежи в подобные схемы. В условиях продолжающейся цифровой трансформации экономических отношений и изменений интернет-технологий во все сферы общественной жизни особую актуальность приобретают задачи мониторинга финансовых потоков, выявления каналов онлайн-финансирования деструктивной деятельности и укрепления межведомственного взаимодействия с банковским сектором и иными финансовыми институтами. Указанные направления деятельности выступают в качестве необходимого условия для своевременного обнаружения и пресечения каналов финансовой подпитки террористических структур.

Ключевым инструментом в решении данной задачи выступает системный анализ транзакционной активности, позволяющий идентифицировать операции, обладающие признаками связи с финансированием терроризма. Нормативно-правовую основу соответствующей деятельности образует Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным

¹ Федеральный закон "О противодействии терроризму" от 06.03.2006 N 35-ФЗ (последняя редакция). [Электронный ресурс]// КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_58840/ (дата обращения 10.10.2025).

² "Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (утв. Президентом РФ 30.05.2018). [Электронный ресурс]// КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_299375/ (дата обращения 10.10.2025).

путем, и финансированию терроризма». В соответствии с положениями указанного нормативного акта, на организации, осуществляющие операции с денежными средствами или иным имуществом, возложена обязанность по информированию уполномоченного органа (Росфинмониторинга) о всех операциях, в отношении которых возникают подозрения об их связи с легализацией преступных доходов или финансированием терроризма. Таким образом, выстраивается двухуровневая система контроля, сочетающая внутриведомственный мониторинг финансовых организаций и государственный надзор за соблюдением антитеррористического законодательства в финансовой сфере¹. Вместе с тем, анализ правоприменительной практики свидетельствует о наличии существенных ограничений традиционных методов финансового контроля. Наибольшую сложность для выявления представляют операции, осуществляемые с использованием криптовалют и анонимных платежных систем, которые в силу своей технологической природы позволяют минимизировать риски обнаружения уполномоченными органами. Подобные финансовые инструменты, функционирующие вне классической банковской инфраструктуры, создают благоприятную среду для трансграничного перемещения денежных средств в пользу террористических структур без должного контроля со стороны государства.

В целях нейтрализации указанных угроз и ликвидации образовавшегося пробела со стороны контролирующих и надзорных органов инициировано внедрение специализированных программно-аналитических комплексов. Данные цифровые инструменты предназначены для мониторинга, анализа и выявления подозрительных транзакций в децентрализованной финансовой среде, что позволяет частично компенсировать недостаточную эффективность традиционных механизмов финансового мониторинга применительно к новым формам расчетов.

Выявление каналов финансирования через интернет представляет собой еще один важный аспект работы ОВД. Первоначальная оперативно значимая информация может быть получена путем проведения таких оперативно-розыскных мероприятий как опрос, а также наблюдение. У большинства таких организаций есть свои страницы в социальных сетях, группы и телеграмм каналы. В результате проведения привлечения молодежи к финансированию противоправной деятельности, данные лица достаточно часто ожидают обратную связь в виде комментариев и отзывов, здесь и находятся источники, которые позволят нам получить первичную информацию. Опросив данных личностей о замысле деятельности организации в которой, они участвуют, либо же человека, которому они переводят денежные средства, есть возможность проверить правдивость его идей путем

¹ Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 № 115-ФЗ (последняя редакция). [Электронный ресурс]// КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения 10.10.2025).

направления запросов в организации, в которых, по его словам, он приобретает средства для своей деятельности. Также необходимо помнить о том, что главным источником информации являются сами люди, и неравнодушные граждане могут путем содействия с ОВД предоставить информации о подозрительной финансовой деятельности какого-либо человека, либо организации.

По факту получения первичной информации и установления лица, в отношении которого сформировано обоснованное подозрение в причастности к финансированию террористической деятельности, возникает правовая и фактическая возможность реализации комплекса оперативно-розыскных мероприятий повышенной сложности. К числу таковых относятся прослушивание телефонных переговоров, снятие информации с технических каналов связи, а также получение компьютерной информации, позволяющее документально фиксировать противоправную активность в цифровой среде.

Современный уровень развития технологий предоставляет террористическим структурам широкий арсенал средств для маскировки своих финансовых операций. В качестве инструментов сбора средств, маскирующихся под благотворительные инициативы либо инвестиционные проекты, активно задействуются ресурсы мессенджеров (в частности, Telegram-каналов) и платформы онлайн-казино. Противодействие данным угрозам требует от оперативных подразделений системного мониторинга цифровых площадок, налаженного взаимодействия с провайдерами и администраторами интернет-ресурсов, а также применения специализированных методик контент-анализа социальных медиа. Как справедливо отмечают исследователи, результативность указанных мер находится в прямой корреляции с уровнем профессиональной компетенции сотрудников органов внутренних дел в области кибербезопасности и владения современными цифровыми технологиями.

Например, в 2023 году была проведена серия учебных семинаров для сотрудников правоохранительных органов, направленных на освоение методов анализа транзакций в даркнете и блокчейне.

Взаимодействие с банками и финансовыми организациями играет ключевую роль в противодействии финансированию терроризма. Банки являются первичным звеном в выявлении подозрительных операций, поскольку именно через них проходят большинство финансовых потоков. Однако, как подчеркивают исследователи, успешное взаимодействие между ОВД и банками возможно только при наличии четко выстроенной системы информационного обмена и регулярного обновления методик анализа данных. В соответствии с Федеральным законом № 115-ФЗ банки обязаны проводить внутренние проверки операций клиентов и оперативно

передавать результаты в Росфинмониторинг¹. Между тем, оперативные подразделения Министерства внутренних дел предоставляют банкам экспертные рекомендации, помогая им распознавать новые тенденции в схемах финансирования терроризма. Благодаря этому партнерству в 2023 году было заблокировано более 200 счетов, связанных с финансированием терроризма.

Таким образом, деятельность оперативных подразделений Министерства внутренних дел Российской Федерации по противодействию вовлечению молодежи в финансирование террористической деятельности базируется на интеграции трех ключевых компонентов: системного технического мониторинга цифрового пространства, конструктивного взаимодействия с институтами финансово-кредитной системы и реализации комплекса превентивных мер. Указанные элементы в своей совокупности формируют целостную стратегию, направленную на нейтрализацию рассматриваемой угрозы. Вместе с тем, как обоснованно отмечают исследователи, устойчивость достигаемых результатов находится в прямой зависимости от способности правоохранительной системы адаптироваться к динамично изменяющимся технологическим вызовам и совершенствования нормативно-правового регулирования оборота цифровых финансовых инструментов. Необходимость перманентного развития методического арсенала и сохранения высокого уровня оперативной бдительности детерминирована потребностью в упреждающем реагировании на попытки использования современных технологий в противоправных целях.

¹ Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ (последняя редакция). [Электронный ресурс]// КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения 10.10.2025).

Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

Сяткин Эмиль Артемович,
слушатель 4 курса
Краснодарского университета МВД России

ОБЕСПЕЧЕНИЕ ПРАВ И ЗАКОННЫХ ИНТЕРЕСОВ ГРАЖДАН ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

Современное развитие оперативно-розыскной деятельности в Российской Федерации характеризуется устойчивым напряжением между необходимостью эффективного противодействия преступности и конституционной обязанностью государства обеспечивать и защищать права и свободы человека и гражданина. Данная коллизия имеет не абстрактный, а прикладной характер, поскольку значительная часть оперативно-розыскных мероприятий по своей правовой природе предполагает вмешательство в сферу частной жизни, ограничение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также затрагивает иные гарантированные Конституцией Российской Федерации нематериальные блага личности. В этих условиях особую значимость приобретает проблема обеспечения прав и законных интересов граждан при проведении оперативно-розыскных мероприятий, ограничивающих конституционные права и свободы человека и гражданина.

Оперативно-розыскная деятельность, будучи самостоятельным видом государственной правоохранительной деятельности, основывается на Конституции Российской Федерации¹, Федеральном законе «Об оперативно-розыскной деятельности»², а также подзаконных нормативных правовых актах, принятых в его развитие. Уже в ст. 1 ФЗ «Об ОРД» законодатель закрепляет целевую направленность оперативно-розыскной деятельности, связывая ее с защитой жизни и здоровья человека, его прав и свобод, охраной собственности, а также обеспечением безопасности общества

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ, от 06.10.2022) // Собрание законодательства РФ. – 2022. – №41. – Ст.6933.

² Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 01.04.2025) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. – 1995. – № 33. – Ст. 3349.

и государства от преступных посягательств. Таким образом, сама логика правового регулирования указывает на приоритет охранительной функции по отношению к личности, что предполагает не только допустимость, но и необходимость правовых механизмов, минимизирующих риск произвольного или необоснованного ограничения конституционных прав граждан.

В то же время анализ правоприменительной практики свидетельствует о том, что именно в процессе реализации оперативно-розыскных мероприятий наиболее остро проявляется опасность нарушения принципа соразмерности вмешательства в сферу частной жизни. Это обусловлено, во-первых, негласным характером значительной части оперативно-розыскных мероприятий, во-вторых, высокой степенью дискреционных полномочий должностных лиц, принимающих решения о целесообразности и необходимости их проведения, и, в-третьих, объективной сложностью последующего контроля за законностью и обоснованностью таких решений¹.

Особое место в системе гарантий прав и свобод граждан при осуществлении оперативно-розыскной деятельности занимает статья 8 Федерального закона «Об оперативно-розыскной деятельности», которая устанавливает судебный порядок санкционирования мероприятий, ограничивающих конституционные права человека и гражданина. Законодатель прямо указывает, что проведение таких мероприятий допускается лишь при наличии судебного решения, за исключением строго определенных случаев, когда промедление может создать угрозу жизни, безопасности государства или привести к совершению тяжкого преступления. Данная норма призвана служить ключевым инструментом предотвращения злоупотреблений и произвольного вмешательства в личную сферу граждан, однако ее практическая реализация остается предметом научных дискуссий и критических оценок.

В научной литературе справедливо отмечается, что формально установленный судебный порядок санкционирования не всегда трансформируется в реальный механизм защиты прав личности. Рассмотрение судом ходатайств о разрешении на проведение оперативно-розыскных мероприятий зачастую носит формализованный характер, при котором судья ограничивается проверкой внешнего соответствия представленных материалов требованиям закона, не вникая в их фактическую обоснованность и достаточность. В результате судебное решение превращается в процедурную фор-

¹ Мухамадиева, Г. Ж. Теоретические аспекты обеспечения прав и свобод человека и гражданина в ходе осуществления оперативно-розыскных мероприятий / Г. Ж. Мухамадиева, М. М. Османов // Противодействие преступности: актуальные проблемы теории и практики. 2025. – С. 169.

мальность, а не в действенный барьер на пути необоснованного ограничения конституционных прав граждан¹.

Особую сложность представляет ситуация, при которой оперативно-розыскные мероприятия, направленные на конкретное лицо, объективно затрагивают права третьих лиц, не имеющих никакого отношения к преступной деятельности. Наиболее показателен в этом отношении пример прослушивания телефонных переговоров, когда в поле оперативного интереса неизбежно попадают разговоры родственников, коллег, случайных знакомых и иных лиц, не подозреваемых в совершении преступления. Несмотря на то что полученная информация в силу прямого указания закона не подлежит разглашению и использованию в незаконных целях, сам факт ее получения уже означает вмешательство в сферу конституционно охраняемой тайны частной жизни.

Данная проблема усугубляется тем, что лица, чьи права были ограничены в ходе оперативно-розыскных мероприятий, как правило, не осведомлены об этом и, следовательно, лишены возможности своевременно воспользоваться механизмами судебной защиты. В отличие от уголовного процесса, где принцип состязательности и гласности позволяет стороне защиты реагировать на действия государства, оперативно-розыскная деятельность по своей природе исключает участие лица в момент принятия решений, затрагивающих его права. Это создает ситуацию правовой асимметрии, при которой государство обладает значительным объемом информации и полномочий, тогда как гражданин оказывается в уязвимом положении.

Не менее дискуссионным является вопрос об основаниях ограничения конституционных прав и свобод, закрепленных в статье 8 Федерального закона «Об оперативно-розыскной деятельности». Законодатель связывает допустимость таких ограничений с наличием информации об угрозах государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. При этом остается неясным, по каким причинам за пределами указанного перечня оказались иные виды безопасности, например общественная или транспортная, которые в современных условиях нередко выступают объектом преступных посягательств. Подобная фрагментарность терминологии порождает неопределенность правоприменения и создает предпосылки для расширительного

¹ Сорокин, Р. С. Ограничение прав и свобод человека и гражданина при проведении оперативно-розыскных мероприятий / Р. С. Сорокин // Учёные труды Российского университета адвокатуры и нотариата имени Г.Б. Мирзоева. – 2024. – № 4(75). – С. 82-85.

толкования закона, что негативно отражается на уровне защищенности прав граждан¹.

Следует также учитывать, что оперативно-розыскная деятельность осуществляется в условиях повышенной секретности, которая, с одной стороны, является объективно необходимой для достижения ее целей, а с другой – затрудняет общественный и ведомственный контроль. Чрезмерная закрытость данной сферы способствует формированию благоприятной среды для злоупотреблений, поскольку ограничивает возможность выявления нарушений и привлечения виновных к ответственности. В научных исследованиях неоднократно подчеркивается, что режим секретности не должен превращаться в самоцель и использоваться в качестве оправдания для произвольного ограничения прав личности².

В этой связи представляется целесообразным дальнейшее развитие правовых механизмов, направленных на балансирование интересов государства и личности. Одним из возможных направлений совершенствования законодательства может стать введение нормы, обязывающей информировать граждан, невольно вовлеченных в сферу оперативно-розыскных мероприятий, о факте получения информации о них после утраты необходимости в сохранении негласности. Такая практика уже известна зарубежным правовым порядкам и рассматривается как важная гарантия восстановления нарушенных прав и укрепления доверия общества к правоохранительным органам.

Также необходим постоянный прокурорский надзор за соблюдением законности при проведении оперативно-розыскных мероприятий. Прокуроры должны располагать реальными инструментами выявления нарушений, что предполагает доступ к материалам оперативно-розыскной деятельности в объеме, необходимом для оценки их законности и обоснованности. Эффективное взаимодействие суда и прокуратуры способно существенно снизить риск необоснованного ограничения конституционных прав граждан.

В заключении, подводя итог необходимо отметить, что обеспечение прав и законных интересов граждан при проведении оперативно-розыскных мероприятий, ограничивающих конституционные права и свободы человека и гражданина, представляет собой сложную и многоплановую задачу, решение которой невозможно без системного подхода. Совершенствование качества судебного контроля и прокурорского надзора, а также формирование правовой культуры должностных лиц, осуществляю-

¹ Беляев, А. А. Оперативно-розыскные мероприятия, ограничивающие конституционные права и свободы человека и гражданина / А. А. Беляев // Пермский период. 2024. – С. 54.

² Думбадзе, А. В. Ограничение конституционных прав граждан при проведении оперативно-розыскных мероприятий / А. В. Думбадзе // Гуманитарные и правовые проблемы современной России. 2025. – С. 36.

щих оперативно-розыскную деятельность, являются необходимыми условиями достижения баланса между интересами безопасности и принципом законности, уважения и соблюдения прав и свобод человека и гражданина. Только при соблюдении данного баланса оперативно-розыскная деятельность может в полной мере соответствовать своему предназначению – защите государства, общества и человека от преступных посягательств.

Фаниев Павел Андреевич,
преподаватель кафедры судебно-экспертной деятельности
Краснодарского университета МВД России,
e-mail: pfaniev@yandex.ru

О НЕКОТОРЫХ ВОЗМОЖНОСТЯХ ИНСТРУМЕНТОВ OSINT ДЛЯ ПОЛУЧЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РАМКАХ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

Интенсивное развитие цифровой коммуникационной среды привело к возникновению большого объема доступной открытой информации, содержащей потенциально значимые данные для расследования преступлений. В этой связи методы и инструменты OSINT приобретают особую актуальность при проведении оперативно-розыскных мероприятий. Сегодня, в среде специалистов по кибербезопасности распространено большое количество самых разнообразных инструментов, обрабатывающих различные массивы данных. Вместе с тем, условно все эти инструменты можно разделить на 3 большие группы:

1) инструменты «ручного» поиска – применяются в тех случаях, когда необходимо проанализировать один источник информации. Примером таких инструментов являются некоторые Telegram боты, сервис web.archive, Foca, Nmap и другие.

2) автоматизированные инструменты – позволяют осуществлять автоматизированный сбор больших данных из различных источников. К таким инструментам относятся SpiderFoot, Harvester и другие.

3) инструменты визуализации и анализа данных – предназначенные для облегчения процесса выявления взаимосвязи между различными объектами, такими как домены, IP и люди. Наиболее ярким примером таких инструментов является Maltego.

Ряд этих инструментов уже применяются для получения криминалистически значимой информации при проведении оперативно-розыскных мероприятий. Однако, как показывает практика, некоторые из них не используются подавляющим большинством сотрудников оперативных подразделений, несмотря на то, что с их помощью могут быть получены ценные сведения для планирования проведения дальнейших ОРМ. Одним из ярких примеров подобных инструментов является Shodan.

«Shodan – это не обычная поисковая система типа Google или Яндекс. В то время как обычные поисковики индексируют контент веб-страниц, Shodan сканирует весь интернет в поисках устройств и сервисов, подключенных к глобальной сети. Он индексирует всё: от веб-серверов и маршрутизаторов до умных холодильников и промышленных систем

управления»¹, которые имеют IP-адрес и открытый порт. Вместо ключевых слов из контента веб-страниц Shodan собирает и индексирует такие сведения как: баннеры служб – это строки данных, которые устройство отправляет при подключении к определённому порту (например, приветственное сообщение FTP-сервера или версия веб-сервера); метаданные устройства – тип, геолокация, название организации, прошивка и т.д.; данные, которые может предоставить само устройство в ходе информационного обмена в сеи (например, заголовки HTTP). Поисковая система официально функционирует с 2009 года. На сегодняшний день, помимо основного своего функционала, Shodan имеет такие значимые функции как визуализация данных на карте мира (Shodan Maps) и скриншоты веб-интерфейсов найденных устройств, например, веб-камер и панелей управления (Shodan Images).

Принцип работы Shodan можно разбить на три основных этапа: сканирование, сбор данных и индексация. На первом этапе, в отличие от Google, который переходит по ссылкам, Shodan использует массовое сканирование портов. Поскольку система не знает, какие IP-адреса активны, поэтому она систематически проверяет все возможные публичные IPv4 и IPv6-адреса. Кроме того, Shodan сканирует наиболее популярные порты (например, 21-FTP, 22-SSH, 23-Telnet, 80-HTTP, 443-HTTPS, 3389-RDP, 5432-PostgreSQL и т.д.), а также тысячи других, включая специфические для промышленного оборудования (например, 502-Modbus). На втором этапе, когда сканер находит открытый порт, происходит процедура "снятия баннера" (Banner Grabbing). «Баннер – это ответ, который дало устройство при обращении к нему поискового паука сервера Shodan»². Такие баннеры могут содержать такие сведения как заголовки сервера (например, nginx/1.18.0, X-Powered-By: PHP/7.4.33), заголовок страницы (<title>...), версия SSH, модель и версию прошивки устройства, геолокацию (GeoIP) (страну, город, координат по IP-адресу), информацию о провайдере, данные обратного DNS-запроса, сертификаты SSL/TLS, (например, информация из SSL-сертификатов, может включать в себя домен, организацию и срок действия).

На третьем этапе производится индексация и систематизация собранных данных. Shodan "извлекает" из баннера структурированные поля объединяют с информацией о геолокации, провайдере и в последствии создает индекс, где каждому ключевому слову или фильтру сопоставляется список IP-адресов, где это слово или условие встречается.

Для получения сведений, собранных Shodan, необходимо использовать специализированный язык запросов, необходимый для фильтрации

¹ См. Как использовать Shodan для поиска уязвимых устройств в интернете URL: <https://www.securitylab.ru/blog/personal/SimlpeHacker/355391.php>

² См.: Сито для интернета: интересные вещи с Shodan. URL: <https://habr.com/ru/companies/ruvds/articles/533890>

результатов поисковой выдачи. Наиболее распространенными фильтрами являются: city: - поиск по городу (например, city:"Krasnodar"), country: - поиск по двухбуквенному коду страны (например, country:RU), port: - поиск по номеру порта (например, port:21), os: - поиск по операционной системе (например, os:"Astra Linux"), hostname: - поиск по имени хоста (например, hostname:"yandex"), org: - поиск по организации, провайдеру или компании (например, org:"vk.com"), net: - поиск по сети, CIDR или IP-адресу (например, net:192.168.0.0/24).

Рассмотрим на примере. Введем в поисковой строке Shodan запрос формы «webcam country:RU» - с целью просмотреть проиндексированные им камеры видеонаблюдения (IP, web и другие). В ответ на запрос, одним из предложенных вариантов была камера на территории Москвы, которая демонстрировала внутренний дворовой участок многоквартирного дома. Вторым интересным вариантом поисковой выдачи была IP-камера, установленная непосредственно в квартире.

При этом если во-втором случае, на момент просмотра камера была заблокирована (имелся только скриншот, последнего зафиксированного Shodan кадра), то в первом случае, имелась возможность беспрепятственного подключения к камере, и просмотра ее в режиме онлайн. Вместе с тем, Shodan имеет и ряд недостатков, такие как обязательное наличие учетной записи в Shodan для работы, а также ограниченное количество суточных запросов и результатов выдачи (только первые 2 страницы результатов), при отсутствии платной подписки. Минимальная стоимость подписки на момент подготовки статьи составляет 69 долларов.

Опираясь на вышесказанное, можно утверждать, что в условиях стремительной цифровизации и экспоненциального роста числа устройств, подключённых к интернету, OSINT-инструменты, и в частности Shodan, становятся всё более значимыми элементами арсенала оперативных служб. Возможность обнаруживать и анализировать «открытые» сетевые ресурсы – от веб-серверов до уязвимых камер видеонаблюдения – открывает перед правоохранительными органами новые горизонты в сборе криминалистически значимой информации. Вместе с тем, для использования в служебной деятельности инструментов подобных Shodan, необходимо проведение системной работы по повышению цифровой грамотности сотрудников оперативных подразделений и развитию внутренних методик их применения. Только комплексный подход, позволит в полной мере реализовать потенциал OSINT инструментов при проведении оперативно-розыскных мероприятий.

Шатилов Алексей Валерьевич,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России
кандидат юридических наук

Косенко Анна Сергеевна,
слушатель 4 курса Краснодарского университета МВД России

УГРОЗЫ МОЛОДЕЖНОЙ СРЕДЕ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОМ ПРОСТРАНСТВЕ

В современном информационном обществе граждане привыкли пользоваться всеми благами информационно-телекоммуникационных технологий. Одним из таких благ является информационная-телекоммуникационная сеть «Интернет». Люди используют данную сеть с целью обучения, работы, общения, покупок в магазинах и так далее. Однако существуют лица, которые используют «Интернет» в других – противоправных целях в том числе объектом их действий является молодёжная среда. Через информационную-телекоммуникационную сеть они продвигают экстремистскую идеологию, публикуя материалы экстремистского характера, ищут последователей и вербуют молодое поколение в экстремистские и террористические организации, предлагают к приобретению запрещенные в свободном обороте товары и услуги. Упомянутый аспект естественно негативно сказывается на молодом поколении в частности и социуме в целом, а в будущем как следствие влечет за собой повышение уровня преступности и ухудшение криминогенной обстановки в стране. В связи с этим в рамках нашего исследования хотелось бы уделить внимание некоторым завлечениям, которым подвержены представители молодёжной среды в информационно-телекоммуникационной сети «Интернете» и около сетевом пространстве.

Хотелось бы отметить, что в последние десятилетия на подростков и их восприятие действительности оказывает значительное влияние различные средства массовой информации, понятие которых к настоящему временному времени является довольно расширенным. Средства массовой информации – это организационно-технические комплексы передачи и массового тиражирования информации, которые охватывают широкое количество людей разного пола и возраста¹. Они несут различные функции: развлечение, обучение, информирование населения и другие. Однако данный процесс осуществляется таким образом, что посредством просмотра

¹ Современные СМИ в контексте информационных технологий: сб. науч. тр. 6-й Всерос. науч.-практ. конф. – СПб.: СПбГУПТД, 2020–120 с.

определенного «контента» у представителей молодежной среды формируется новое мировоззрение и взгляды. Особое воздействие, средства массовой информации в самом широком смысле, оказывают на подростков в связи с происходящими у них возрастными психологическими и физиологическими изменениями в организме. Несовершеннолетние подвержены влиянию со стороны интернет-сообществ, пабликов, видеоматериалов и других форм передачи информации. Злоумышленники, зная о данном аспекте, массово пропагандируют различную противоправную в том числе экстремистскую идеологию.

Ярким примером пропаганды экстремистской идеологии служат украинские праворадикальные организации, распространяющие свою идеологию преимущественно через социальные сети. Под праворадикализмом следует понимать совокупность крайних идеологий, абсолютизирующих этническую принадлежность человека и стремящихся к построению национально или расово однородного или иерархически устроенного общества насильственным путем¹. Одним из наиболее ярких течений украинского праворадикализма является интегральный национализм. Основная роль в идеологии интегрального национализма уделена фашизму. Известными представителями данного идеологического течения являются: «УНА-УНСО» и «Правый сектор», данные организации признаны в Российской Федерации экстремистскими на основании решения Верховного суда Российской Федерации от 17 ноября 2014 года и 23 января 2025 года соответственно. В процессе изучения материалов были выявлены значительные противоречия между содержаниями публикаций идеологии «Правого сектора» и «УНА – УНСО» с реальной действительностью. Содержание напрямую направлено на искажение реальной действительности в современном информационном обществе в целом и особенно действенно в отношении молодежной среды, представители которой, ознакомившись с подобными материалами, не имея углубленных знаний в истории и политике поддаются на провокации со стороны экстремистских организаций.

Экстремистские статьи и лозунги, направленные на представителей молодежной среды можно встретить не только в «классической» информационно-телекоммуникационной сети «Интернет». В случае использования пользователем определенных браузеров, таких как браузер «Tor», можно выйти на телекоммуникационную сеть «Даркнет». «Даркнет» – это собрание анонимных сетей, использующие собственные протоколы связи. Весь трафик в них шифруется и доступ возможен только через определенные программные обеспечения. На данной платформе имеется прямая возможность взаимодействия представителей молодежи с элементами криминаль-

¹ Идеология и символика украинских праворадикальных организаций и вооруженных формирований/ С. Ф. Самойлов, – Краснодар: Краснодарский университет МВД России, 2024. – 159 с.

ной среды такими как: запрещенные видеоролики, возможность приобретения наркотических средств и психотропных веществ и оружия, возможность заказать для изготовления поддельные документы, найма людей для убийства и так далее. Естественно в данной сети имеется доступ к ознакомлению с материалами экстремистского и террористического характера. Помимо опасности, представленной в информации, размещенной в «Даркнете», существует угроза распространения через интернет сайты всевозможных кибер атак и вредоносных программных обеспечений. Сюда можно отнести ¹:

- «Трояны» - вредоносное программное обеспечение, маскирующееся под легитимные программы и файлы, но выполняющее вредоносные для пользователя действия (кража паролей, установка шпионских приложений, предоставление удаленного доступа к приложениям компьютера);

- «Фишинг» ² – злоумышленники выдают себя за доверенных лиц (продавцы в интернет-магазине, служба поддержки, представители банка) для получения личной информации и ее дальнейшее использование в преступном умысле; Данный тип кибер атак достаточно сильно распространён в «Даркнете» в связи с наличием анонимности и возможности пользования поддельными сайтами.

- «DDoS – атаки» (Distributed Denial of Service) – атаки, направленные на перегрузку программного обеспечения, серверов и сайтов, делающая их недоступными для работы и использования. Данные атаки часто используются для отвлечения внимания от вымогательства или от других вредоносных действий;

- взлом аккаунта и кража личных данных, учитывая, что «Даркнет» является первоочередным рынком для получения и продажи украденных данных пользователей (логины, пароли, данные кредитных карт, личная информация и медицинские записи);

- спам-рассылки, когда злоумышленники используют уязвимости в программном обеспечении для внедрения вредоносного кода в систему через интернет ссылки на ложные сайты;

- кибербуллинг – умышленное, систематическое, агрессивное преследование, травля или унижение человека от анонимных пользователей и сообществ по отношению к молодым людям, посещающим «теневого Интернет».

Исходя из вышеперечисленных угроз «Даркнета», мы можем отметить факт необеспеченности защитными программами данного ресурса, что негативно влияет на нормальное функционирование персональных

¹ «Современные кибератаки: классификация и способы защиты»: Текст научной статьи по специальности «Компьютерные и информационные науки», А. К. Назарян, И. Н. Карцан //доступ из научной электронной библиотеки cyberleninka (дата обращения 22.10.2025)

² <https://ru.ruwiki.ru/wiki/Фишинг>

компьютеров и программных обеспечений у пользователей и как следствие, приводит к распространению персональных данных пользователей, искажению и уничтожению файлов и вывода из строя программ устройства. Помимо этого вышеописанные процессы, осуществляемые в информационной телекоммуникационной сети, обладают некоторыми особенностями¹:

1. Наличие анонимности. Злоумышленники могут скрывать личную информацию о себе, разглашать ложные сведения о своей занятости и интересах, представляться кем-либо, что может повлиять на нормальный процесс оценивания собеседника, данная особенность негативно сказывается в случае совершения такими пользователями преступлений в связи с невозможностью их отслеживания.

2. Наличие ненависти и дискриминации. «Даркнет» служит платформой взаимодействия совершенно различных пользователей. Они распространяют ненавистнические высказывания, дискриминацию по принадлежности к определённой расе, религии и так далее. В случае выявления пользователя, отличного от них, они могут осуществлять интернет-травлю, оскорблять его и запугивать. Это негативно сказывается на психологическом состоянии молодого человека, в отношении которого происходит акт насилия.

3. Преследование. В случае наличия взаимодействия молодёжи с лицами, имеющими психические отклонения, **обсессивно-компульсивное расстройство**, чувство собственного превосходства, склонность к манипуляциям, возможен «феномен «Сталкера». Лицо, которое владеет личной информацией, собранной в сети «Даркнет», может постоянно отслеживать действия жертвы, угрожать, шантажировать или манипулировать ей, распространять унижительные слухи и ложную информацию о молодом человеке, тем самым получая от объекта воздействия необходимую информацию, материальную выгоды или удовлетворение извращенных потребностей.

Подводя итоги работы, можно сделать вывод, что информационно-телекоммуникационное пространство имеет множество угроз, которые направлены на молодежную среду. Во время ознакомления с информацией на интернет сайтах, общения с новыми пользователями, покупки определенных товаров через интернет магазины, необходимо соблюдать осторожность и бдительность в связи со значительным количеством угроз данных информационных сфер. Информационно-телекоммуникационное пространство опасно не только в плане распространения информации о пользователях, вредоносных файлов, запрещенного контента, но и психологического насилия.

¹ <https://blog.skillbox.by/kod/kiberataki-5-vidov-i-3-sposoba-zashhity-ot-kompjuternyh-atak/>

Шахматов Александр Владимирович,
профессор кафедры оперативно-разыскной деятельности в ОВД
Санкт-Петербургского университета МВД России,
доктор юридических наук, профессор,
a-shahmatov@yandex.ru.

Скоков Игорь Евгеньевич,
доцент кафедры оперативно-разыскной деятельности в ОВД
Санкт-Петербургского университета МВД России,
кандидат юридических наук,
тел.: +79112116090; Iga-spb74@mail.ru

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

В современной правоприменительной практике особую значимость приобретает вопрос интеграции результатов оперативно-розыскной деятельности (далее ОРД) в доказательственную базу уголовного судопроизводства. Эффективность раскрытия и расследования преступлений во многом зависит от возможности законного и обоснованного использования оперативных данных, встроенных в процессуальную деятельность, осуществляемую в ходе расследования преступлений.

Использование результатов оперативно-розыскной деятельности в качестве элементов доказательной базы в уголовном судопроизводстве сопряжено с рядом проблем, связанных с правовым регулированием, процедурами сбора и оформления данных, а также с оценкой их допустимости в суде. Эти проблемы нередко становятся причиной отмены или изменения судебных решений.

Вот несколько основных направлений, определенных нами в ходе проведенного исследования:

– Недостаточное качество собранных в ходе проведения оперативно-розыскных мероприятий (далее – ОРМ) данных. Результаты ОРД могут не соответствовать требованиям закона из-за ошибок сотрудников, нарушений процедур проведения ОРМ или недостаточной профессиональной подготовки оперативных работников. Например, отсутствие необходимых документов, подтверждающих законность проведения ОРМ, или несоответствие материалов требованиям Инструкции от 27.09.2013 «О порядке представления результатов ОРД»¹;

¹ Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд" <https://mvd.consultant.ru/documents/25485> (дата обращения 10.10.2025 г.)

– Нарушение прав человека. Сведения, полученные с нарушением конституционных прав (например, без судебного решения при ограничении права на тайну переписки или неприкосновенность жилища), не могут использоваться в качестве доказательств. Конституционный Суд РФ неоднократно подчёркивал, что результаты ОРД становятся доказательствами только после надлежащего процессуального закрепления в соответствии с УПК РФ¹;

– Проблемы с оформлением и представлением материалов. Законодательство не всегда чётко регламентирует процедуру представления результатов ОРД для использования в уголовном процессе. Например, могут возникать нарушения при оформлении протоколов, постановлений о проведении ОРМ, а также при передаче материалов следователю или в суд. В некоторых случаях отсутствуют необходимые документы (например, постановления руководителей органов, осуществляющих ОРД, или судебные решения, разрешающие проведение ОРМ, ограничивающих конституционные права граждан);

– Достоверность и проверяемость данных. Оперативные данные часто носят вероятностный характер, что затрудняет их использование в качестве доказательств, требующих достоверности и возможности проверки. Например, аудио- и видеозаписи могут быть признаны недопустимыми из-за низкого качества, невозможности идентификации голосов или личностей на записях, отсутствия носителей информации с первоисточника;

– Провокационный характер ОРМ. Если действия оперативных сотрудников спровоцировали совершение преступления, результаты таких мероприятий не могут служить основанием для обвинения. Суд должен оценивать, сформировался ли умысел у подозреваемого независимо от деятельности оперативных подразделений;

– Нормативные пробелы и противоречия. Существует несоответствие между положениями Федерального закона «Об оперативно-розыскной деятельности» и УПК РФ. Например, ст. 89 УПК РФ запрещает использование результатов ОРД, не отвечающих требованиям к доказательствам, но оперативно-розыскные органы не могут изначально получить данные, полностью соответствующие процессуальным требованиям.

Согласно статье 5.36.1 Уголовно-процессуального кодекса РФ, «результаты ОРД» – это информация, добытая согласно Федеральному закону № 144-ФЗ от 12.08.1995, касающаяся признаков готовящегося, совершае-

¹ Например Определение КС № 2801-О/2017 об отказе в принятии к рассмотрению жалоб гражданина Давлетова Андрея Юрьевича на нарушение его конституционных прав статьёй 89 Уголовно-процессуального кодекса Российской Федерации от 19 декабря 2017 года и др.

мого или совершенного преступления, а также лиц, причастных к этому и скрывающихся от правосудия¹.

Приведем несколько примеров из судебной практики. По уголовному делу в отношении К., обвиняемого в совершении преступлений, предусмотренных ч.1 ст.228.1 Уголовного кодекса РФ, в судебном заседании было установлено, что оперативно-розыскное мероприятие «Проверочная закупка» проведено с существенными нарушениями Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ Об ОРД).

В постановлении о проведении оперативно-розыскного мероприятия «Проверочная закупка» не указана цель его проведения, что является обязательным. Более того, в описательно-мотивировочной части постановления указано, что это ОРМ уже проведено. Кроме того, в деле отсутствует надлежащим образом оформленное заявление лица, которое участвовало в качестве «закупщика»: есть заявление от некоего «закупщика» от 04 января 2021 года, в то время как данные о личности этого «закупщика» засекречены постановлением, датированным 12 января 2021 года (конверт с личными данными «Закупщика»), а согласно постановления начальника полиции МО МВД России «Серовский» от 04 января 2021 года результаты оперативно-розыскной деятельности, полученные в ходе проведения ОРМ «Проверочная закупка» наркотических средств в отношении К., рассекречены, отсутствие необходимых документов и неправильное оформление имеющихся, являвшихся основаниями для проведения проверочной закупки, и привело к вынесению оправдательного приговора².

По уголовному делу в отношении А., обвиняемого в совершении преступлений, предусмотренных п. «а» ч. 2 ст. 228.1 УК РФ, суд установил, что в справке оперуполномоченного о результатах ОРМ «Наблюдение» указано, что А. предположительно сбыв Б. гашишное масло в чистом виде и в смеси с табаком, общим весом наркотического средства 1,748 грамма. Наркотики изъяты у Б. в этот же день. Однако представленными стороной обвинения доказательствами не установлена какая-либо связь между этими лицами. При отсутствии каких-либо доказательств сбыта указанных 1,748 граммов гашишного масла, суд полагает обвинение А. в этой части также недоказанным. По действующему уголовно-процессуальному закону, предъявленное обвинение не может быть основано на домыслах и предположениях, а должно подтверждаться конкретными, фактическими данными в отношении каждого из обстоятельств, подлежащих доказыванию.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 20.01.2026)

² Приговор судебной коллегии по уголовным делам Свердловского областного суда от 14 марта 2022 года дело № 22-1850/2022, <https://sudrf.cntd.ru/document/350096415> (дата обращения 10.10.2025 г.)

В своем решении суд сообщает, что по настоящему уголовному делу сторона обвинения делает вероятностный вывод о том, что в инкриминированное А. время и при вмененных обстоятельствах он сбыл Б. определенный размер наркотического средства, исходя из установленных ст. ст. 17 и 88 УПК РФ стандартов доказывания, суд не может принять решение о виновности подсудимого в совершении всех инкриминированных преступлений на столь противоречивых доказательствах. При этом все возможности для устранения этих противоречий, по делу исчерпаны.

На этом основании, руководствуясь принципом, сформулированным в ч. 3 ст. 49 Конституции Российской Федерации и ч. ч. 3 и 4 ст. 14 УПК РФ, о том, что неустранимые сомнения в виновности лица толкуются в пользу обвиняемого, а обвинительный приговор не может быть основан на предположениях, суд считает необходимым оправдать А. по указанной выше части предъявленного обвинения в связи с непричастностью к совершению преступлений¹.

Подобный подход по отношению к результатам проведения оперативно-розыскных мероприятий, находящимся в уголовных делах и используемых в них в качестве элементов доказательной базы прослеживается в большинстве судов общей юрисдикции. На наш взгляд абсолютно правильно, проверяя законность проведения ОРМ, убедиться в присутствии документов, подтверждающих, например, выдачу участнику проверочной закупки денежных или специальных технических средств, наличии подписей представителей общественности в протоколе проведения ОРМ обследование помещений, зданий, сооружений, участков местности и транспортных средств и т. д.

Связь между оперативно-розыскной и уголовно-процессуальной деятельностью проявляется в их понятийном аппарате, хотя Закон об ОРД не содержит четкого определения "результатов ОРД", в отличие от УПК РФ. Разнообразие толкования этого понятия в различных областях права привело к формированию множества подходов, среди которых выделяются две основные модели.

Информационная модель рассматривает результаты ОРД как собранные данные о преступлении, виновности лиц и других обстоятельствах, важных для дела. Подчеркивается необходимость документирования информации в виде справок, рапортов, фото- и видеоматериалов. Некоторые ученые отмечают, что эта информация добывается в оперативно-розыском процессе. Она является конфиденциальной или закрытой, негласной или разведывательной, полученной в установленном законом по

¹ Приговор Приморского Краевого суда № 2-19/2025 2-59/2024 от 22 апреля 2025 г. по делу № 2-19/2025 <https://sudact.ru/regular/doc/TCtFNbJ2eXHm> (дата обращения 10.10.2025 г.).

рядке в интересах достижения целей и решения задач специфической, общественно полезной, государственной, правоохранительной деятельности¹.

В рамках информационного подхода, некоторые авторы считают, что собранная информация настолько важна и связана с доказываемыми фактами, что может использоваться в уголовном процессе путем введения в УПК РФ положений инструкции «О порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд», утвержденной приказами от 27 сентября 2013 г. МВД РФ № 776, Минобороны РФ № 703, ФСБ РФ № 509, ФСО РФ № 507, ФТС РФ № 1820, СВР РФ № 42, ФСИН РФ № 535, ФСКН РФ № 398, СК России № 68². Однако, данный подход представляется спорным, так как оперативно-розыскная информация может быть ориентирующей, вспомогательной или доказательственной. Только в последнем случае, после оформления, она проверяется и оценивается.

Доказательственная модель предлагает закрепить результаты ОРД в УПК РФ как самостоятельный источник доказательств, оговаривая необходимость подтверждения их подлинности лицом, их получившим. Основанием для этого служит задача оперативно-розыскных органов по предупреждению, пресечению и раскрытию преступлений.

Это решение предлагается реализовать путем дополнения статьи 74 УПК РФ указанием на допустимость материалов ОРД в качестве доказательств. Подобная позиция критикуется, так как негласные методы получения информации не позволяют в полной мере проверить и оценить их в суде. Европейский суд по правам человека указывает на необходимость доступа судов к материалам, подтверждающим законность ОРМ.

При определении сути понятия «результаты ОРД» необходимо учитывать ряд аспектов. Прежде всего, нельзя приравнивать его к понятию «доказательство», закрепленному в ст. 74 УПК РФ, поскольку последнее, помимо содержания информации, включает требования к процессуальному оформлению получения этих сведений.

Анализ положений закона позволяет выделить несколько основных направлений использования результатов ОРД в уголовном судопроизводстве:

- 1) получение информации, служащей поводом и основанием для возбуждения уголовного дела;
- 2) подготовка и проведение следственных и судебных действий;
- 3) доказывание обстоятельств, важных для дела.

По сути, результаты ОРД представляют собой достаточные сведения, указывающие на признаки преступления: данные о месте, времени, при-

¹ Кондратьев, М.В. О теории оперативно-розыскной информации / М.В. Кондратьев, В.В. Сорокин // Известия Алтайского государственного университета. – 2012. – № 2-2 (74). – С. 109-111.

² Бессонов А.А. Использование результатов ОРД в доказывании по уголовным делам. / А.А. Бессонов Уголовное право. 2016. №2. – С. 116-124

знаках и виде обнаруженного преступления; обстоятельства его обнаружения; информация о лице (лицах), совершившем его, и свидетелях (при наличии); о местонахождении предметов и документов¹, которые могут стать вещественными доказательствами; любые другие факты и обстоятельства, значимые для решения вопроса о возбуждении дела.

В процессе доказывания и при подготовке и проведении следственных действий результаты полученные в ходе осуществления оперативно-розыскной деятельности дают информацию о том, где находятся лица, скрывающиеся от следствия и суда, какие источники доказательств могут быть задействованы, а также о фактах и обстоятельствах, помогающих выбрать наилучшую тактику проведения следственного действия. Эти результаты могут быть использованы для создания доказательств, отвечающих положениям УПК РФ.

В статье Федерального закона «Об оперативно-розыскной деятельности» предусмотрено несколько оснований для проведения ОРМ в ходе которых сотрудниками оперативных подразделений может быть получена оперативно-розыскная информация (далее ОРИ). Для легитимного сбора ОРИ необходимо соблюдение условий, установленных статьей 8.

Если возникающая оперативная ситуация требует проведения ОРМ ограничивающих конституционные права личности (на тайну переписки и телефонных переговоров, неприкосновенность жилища), необходимо получение разрешения суда. Тем не менее законодательство предусматривает исключение: в чрезвычайных обстоятельствах, связанных с предотвращением тяжких или особо тяжких преступлений, допускается проведение ОРМ по решению руководителя органа осуществляющего ОРД. При этом судебный орган должен быть уведомлен о проведенных мероприятиях не позднее чем через 24 часа. В дальнейшем орган, проводящий ОРМ, должен в течение 48 часов получить судебное постановление или прекратить оперативное мероприятие².

Достоверность ОРИ обеспечивается наличием данных об источнике информации, а также об ОРМ, в результате которого она была получена. Это обязательное условие для последующей проверки доказательств в суде. Статья 6 Закона об ОРД содержит исчерпывающий перечень ОРМ. Право на получение оперативно-розыскной информации (ОРИ) с целью её использования в уголовном процессе закреплено статьей 14 Закона об ОРД за оперативными подразделениями следующих органов: внутренних дел, ФСБ, таможни, государственной охраны, внешней разведки и исполнения наказаний.

¹ Трошин, Н. А. Актуальные вопросы использования результатов оперативно-розыскной деятельности в российском уголовном судопроизводстве / Н. А. Трошин // Международный студенческий научный вестник. – 2019. – № 3. – С. 38.

² Ст. 8 Федерального закона «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ

Таким образом, сведения, добытые в ходе оперативно-розыскной деятельности и предназначенные для включения в доказательственную базу по уголовному делу, являются информацией, собранной уполномоченными органами в соответствии с Федеральным законом «Об ОРД». Она содержит: признаки готовящегося, совершаемого или совершённого преступления; данные о лицах, вовлечённых в преступную деятельность; прочие обстоятельства, имеющие значение для хода расследования.

На базе указанного понятия возможно определение ряда ключевых признаков отражающих уникальность результатов оперативно-розыскной деятельности как элементов для формирования доказательной базы:

1) Соблюдение требований Закона об ОРД в отношении субъекта, оснований и условий получения информации. Это означает, что процесс получения информации должен быть законным и соответствовать установленным процедурам.

2) Наличие конкретной информации, демонстрирующей признаки преступления в любой фазе его реализации – от подготовки до завершения. Эти данные должны включать сведения о: лицах, причастных к преступлению; лицах, уклоняющихся от правосудия; прочих обстоятельствах, существенных для расследования и доказывания виновности по уголовному делу.

3) Процесс фиксации сведений предполагает оформление оперативных отчётов и сохранение сведений в виде материальных объектов. В комплект данных материалов включаются предметы и документы, изъятые во время оперативно-розыскных мероприятий – что обеспечивает прозрачность и возможность контроля за процессом сбора доказательств.

Шищенко Елена Андреевна,
доцент кафедры уголовного права Кубанского государственного
аграрного университета имени И.Т. Трубилина,
кандидат юридических наук, доцент
тел.: 8-918-117-98-49; e-mail: alenooshka1986@mail.ru

СОВРЕМЕННЫЕ АСПЕКТЫ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПО ВЫЯВЛЕНИЮ И РАССЛЕДОВАНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Стремительная цифровизация всех сфер общественной жизни обусловила возникновение новой, высокодинамичной и латентной формы противоправного поведения – компьютерной преступности. Преступления в сфере компьютерной информации, предусмотренные главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ)¹, а также иные деяния, совершаемые с использованием IT-технологий, представляют существенную угрозу национальной безопасности, экономике и правам граждан². Зачастую такие преступления совершаются в совокупности с преступлениями против собственности, интеллектуальной собственности, а также с преступлениями против общественной безопасности³.

Эффективное противодействие данному виду преступности невозможно без широкого и грамотного применения сил и средств оперативно-розыскной деятельности. Расследование компьютерных преступлений требует наличия специальных знаний, необходимых для выяснения всех обстоятельств совершенного преступления. Использование специальных знаний направленно на выяснение обстоятельств, имеющих значение для уголовного дела, и выражается в применении положений естественных, технических наук и помогает разрешить возникающие обстоятельства либо способствует созданию условий для оптимального производства следственных

¹ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 01.09.2025) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954

² Лысак Е.А. Уголовное законодательство в сфере охраны интеллектуальной собственности в России и зарубежных странах // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2011. № 74. С. 576-584.

³ Казакецян Г.О., Хорольский Г.В. Некоторые особенности расследования мошенничества // Eromen. Global. 2025. № 59. С. 163-167; Алехин В.П., Медведев С.С. Проблемы борьбы с финансированием террористической деятельности с помощью мошенничества в сфере высоких технологий // Информационное право. 2009. № 2. С. 29-32; Едиджи Ф.А., Картавченко В.В. Мошенничество. Некоторые проблемные вопросы // Научное обеспечение агропромышленного комплекса: сборник статей по материалам 75-й научно-практической конференции студентов по итогам НИР за 2019 год. Отв. за выпуск А.Г. Кощаев. 2020. С. 1097-1100; Шабалина Е.А., Лукки Е.В. Анализ правовых основ борьбы с киберпреступностью // Eromen. Global. 2025. № 60. С. 165-169.

действий¹. Необходимо подчеркнуть и значимость использования информационных технологий в расследовании как вспомогательного средства организации². В науке уголовного права отмечается, что существует проблема того, что именно можно считать так называемыми «цифровыми доказательствами», так как в уголовно-процессуальном законодательстве нет нормы, которая бы регламентировала подобный вид доказательства³.

Оперативно-розыскная деятельность (далее – ОРД), как вид государственной деятельности, направленный на выявление, предупреждение, пресечение и раскрытие преступлений⁴, в киберпространстве сталкивается с рядом сложных моментов: анонимность субъектов, трансграничный характер деяний, быстрое уничтожение цифровых следов, использование средств шифрования и анонимизации. В этой связи научное осмысление и совершенствование тактики и методики ОРД в данной области представляется чрезвычайно актуальной задачей.

Объектом ОРД по компьютерным преступлениям являются общественные отношения, нарушаемые противоправными деяниями, непосредственно посягающими на конфиденциальность, целостность и доступность компьютерной информации, а также на безопасность информационной инфраструктуры.

Предметом выступают цифровая информация (данные): программы, файлы, базы данных, системные журналы, метаданные, составляющие содержание преступного деяния, а также компьютерные системы и сети, использовавшиеся для подготовки, совершения или сокрытия преступления.

Субъекты преступной деятельности: лица (хакеры, кардеры, организаторы фишинговых атак), чья идентификация и документирование деятельности являются ключевой задачей.

Особенностью данной категории дел является виртуальная среда совершения преступления, где материальные следы заменяются цифровыми, а установление лица, совершившего преступление, требует применения специализированных технических средств и методов.

Федеральный закон «Об оперативно-розыскной деятельности» предоставляет органам, осуществляющим ОРД, широкий арсенал мероприятий. Применительно к компьютерным преступлениям их можно адаптировать и сгруппировать следующим образом.

¹ Зеленский В.Д. О процессуальных и организационных формах использования специальных знаний в расследовании // Общество и право. 2012. № 1 (38). С. 210-212.

² Агеев Н.В. Организация использования информационных технологий в расследовании // Гуманитарные, социально-экономические и общественные науки. 2022. № 10. С. 115-118.

³ Хорольский Г.В. Актуальность внесения в уголовно-правовое законодательство категории «цифрового доказательства» // Сборник статей по материалам ежегодной научно-практической конференции преподавателей по итогам НИР за 2024 год. Сборник трудов конференции. Краснодар, 2025. С. 907-908.

⁴ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 01.04.2025) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ, 14.08.1995, № 33, ст. 3349.

Первая группа – мероприятия по сбору исходной информации и идентификации субъекта: наведение справок и исследование предметов и документов: анализ аккаунтов в социальных сетях, форумах, мессенджерах, где действует злоумышленник; изучение цифровых следов (IP-адреса, cookie, данные пользовательских агентов). К этой же группе относят опрос (в т.ч. онлайн-взаимодействие под легендой): установление контакта с подозреваемым в сети под видом заказчика или партнера для получения информации о его деятельности и методах. Также к таким мероприятиям можно отнести обследование помещений, зданий, сооружений, участков местности и транспортных средств в части, касающейся определения местоположения телекоммуникационного оборудования, серверов, точек доступа к сети.

Вторая группа включает мероприятия по документированию противоправных действий и изъятию доказательств. Прежде всего, сюда относят наблюдение (сетевое наблюдение), то есть мониторинг сетевого трафика, активности на интернет-ресурсах, каналах связи с целью фиксации факта совершения преступления в реальном времени. Также к этой группе относится контроль почтовых отправок, телеграфных и иных сообщений, прослушивание телефонных переговоров, чаще всего на практике производится контроль электронной почты, SMS-сообщений, переписки в мессенджерах, осуществляемый по судебному решению. Ко второй группе также можно отнести обследование помещений, зданий, сооружений, участков местности и транспортных средств, а именно проведение обыска с целью изъятия компьютерной техники, носителей информации, средств криптографической защиты. И, наконец, к этой группе относится сбор образцов для сравнительного исследования, то есть изъятие цифровых образцов (копирование данных) для последующей криминалистической экспертизы.

Третьей группой можно назвать специальные мероприятия, которые реализуются в качестве оперативного сопровождения в рамках расследования уголовного дела, и требуют применения технических средств. Прежде всего, сюда относится оперативный эксперимент, то есть создание контролируемой информационной среды (например, «подставного» интернет-магазина или сервера) для документирования факта несанкционированного доступа или хищения данных. Также к этой группе относится оперативное внедрение, а именно внедрение оперативного работника или агента в закрытые сообщества и форумы киберпреступников для получения информации изнутри. И, наконец, к этой категории также можно отнести получение компьютерной информации как ключевое мероприятие, связанное со снятием информации с технических каналов связи и ее носителей. Оно требует не только правового оформления, но и строгого соблюдения процедуры, обеспечивающей допустимость полученных доказательств (протокол изъятия, использование аппаратно-программных комплексов, обеспечивающих целостность данных).

Несмотря на имеющийся арсенал средств, ОРД в сфере компьютерных преступлений сталкивается с серьезными проблемами. Прежде всего,

можно назвать правовые проблемы, такие как трансграничный характер преступлений, который создает коллизии юрисдикций. Запросы по правовой помощи могут занимать месяцы, в то время как цифровые следы уничтожаются за секунды. При расследовании требуется развитие международного сотрудничества и механизмов оперативного взаимодействия. Также существуют технические проблемы, например, широкое распространение стойких методов шифрования, использование анонимных сетей и VPN-сервисов, что значительно затрудняет отслеживание коммуникаций и идентификацию преступников. Возникают и кадровые проблемы, такие как острый дефицит специалистов-оперативников, обладающих глубокими знаниями как в области юриспруденции и ОРД, так и в IT-сфере.

Оперативно-розыскная деятельность является фундаментальным элементом системы противодействия компьютерной преступности. Ее эффективность в современных условиях напрямую зависит от способности правоохранительных органов интегрировать новейшие технологические разработки в традиционную тактику проведения оперативно-розыскных мероприятий. Особенно важным является первоначальный этап расследования преступления, так как в результате неотложных следственных действий и оперативно-розыскных мероприятий, создается основа для построения развернутых следственных версий по делу, в том числе, версий о событии преступления и субъекте его совершения¹.

Перспективы развития ОРД в данном направлении видятся в следующих шагах: создание межведомственных высокотехнологичных центров по борьбе с киберпреступностью; активная разработка и внедрение отечественных программно-аппаратных комплексов для криминалистического анализа больших данных и мониторинга сетевой активности; углубление специализации оперативных сотрудников и следователей; гармонизация национального законодательства с международными нормами для упрощения процедуры получения электронных доказательств из-за рубежа. Только комплексный подход, сочетающий мощный оперативно-розыскной потенциал, современные технологии и адекватную правовую базу, позволит обеспечить эффективную защиту общества и государства от угроз цифрового века².

¹ Зеленский В.Д., Куемжиева С.А. Об основных положениях организации первоначального этапа расследования // Гуманитарные, социально-экономические и общественные науки. 2022. № 6. С. 85-88.

² Шищенко Е.А. Социальная обусловленность уголовно-правовой охраны компьютерной информации // Уголовно-правовые, уголовно-процессуальные и криминалистические вопросы борьбы с преступностью. Сборник научных трудов по материалам V Всероссийской научно-практической конференции (симпозиума). Краснодар, 2021. С. 53-57; Шищенко Е.А. Нарушение изобретательских и патентных прав: понятие и проблемы квалификации // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 101. С. 2024-2036.

Южанинов Василий Сергеевич,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ РАСПРОСТРАНЕНИЯ ЭКСТРЕМИСТСКИХ МАТЕРИАЛОВ В СЕТИ ИНТЕРНЕТ

Современный этап развития мирового сообщества характеризуется возрастанием масштабов и многообразия угроз, среди которых одними из наиболее опасных являются экстремизм и терроризм, как крайняя форма проявления экстремизма. Эти асоциальные явления, носящие трансграничный характер, представляют прямую угрозу национальной безопасности, суверенитету и территориальной целостности государства, а также посягают на самые фундаментальные ценности – жизнь, здоровье и права человека.

Все это сейчас как никогда актуально для нашей страны, так, современный этап развития Российской Федерации характеризуется значительным усложнением оперативной обстановки и появлением новых, беспрецедентных вызовов национальной безопасности. Продолжающаяся специальная военная операция не только определила новый геополитический контекст, но и оказала прямое влияние на структуру и динамику преступлений террористической и экстремистской направленности внутри страны.

Статистические данные, представляемые ГИАЦ МВД России в сборнике «состояние преступности в России» свидетельствует о колоссальном росте рассматриваемых составов преступлений. Так, в 2024 году зарегистрировано 3714 преступлений террористического характера (+55,9%), из которых публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма ст. 205.2 УК РФ – 898 преступлений (+63,9%). И 1719 преступлений экстремистской направленности (+28,3%), из которых публичные призывы к осуществлению экстремистской деятельности ст. 280 УК РФ - 447 преступлений (+21,8). Из общего числа зарегистрированных преступлений террористического характера 2050 (+86,7%) преступлений совершены в текущем году, в том числе: – пресечено на стадии приготовления и покушения – 285 (+33,8%); – за пределами Российской Федерации – 154 (-30,9%).

Аналогичные тенденции роста данных составов преступлений сохранились и в 2025 году, так, в первой половине 2025 года зарегистрировано 3125 преступлений террористического характера (+89,3%) и 1137 преступлений экстремистской направленности (+38,8%), из которых пуб-

личные призывы к осуществлению экстремистской деятельности ст. 280 УК РФ – 406 преступлений (+76,5%).¹

Деятельность террористических и экстремистских структур, опирающаяся на идеологию насилия и нетерпимости, в текущих условиях активизировалась, получила новые каналы финансирования и инструменты пропаганды. Особую тревогу вызывает активное использование деструктивными элементами современных информационно-коммуникационных технологий для вербовки сторонников, распространения дезинформации, направленной на дестабилизацию российского общества, и координации преступной деятельности.

В условиях проведения СВО ключевая роль органов внутренних дел многократно возросла. Помимо традиционных задач, на первый план вышли новые приоритеты:

- Противодействие киберэкстремизму: блокировка интернет-ресурсов, распространяющих противоправные призывы и фейковую информацию, направленную на подрыв общественного спокойствия. Только с начала СВО были приняты меры по блокировке десятков тысяч подобных ресурсов.

- Защита новых территорий: сотрудники Главного управления по противодействию экстремизму МВД России и территориальных органов активно участвуют в выполнении служебно-боевых задач в новообразованных субъектах РФ, обеспечивая безопасность и правопорядок в этих регионах.

- Противодействие идеологическому экстремизму: актуализировалась борьба с радикальными проявлениями, такими как русофобия и распространение идей неонацизма, что нашло отражение в новой редакции Стратегии противодействия экстремизму.

- Правовое регулирование противодействия экстремизму в интернете непрерывно развивается, реагируя на новые вызовы цифровой среды. Фундаментальным элементом этой системы является Федеральный закон от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», который определяет ключевые понятия и устанавливает общие запреты. В июле 2025 года в законодательство были внесены существенные поправки, вводящие административную ответственность за «поиск заведомо экстремистских материалов и получение доступа к ним». Новая статья 13.53 КоАП РФ устанавливает штрафы для граждан в размере от трех до пяти тысяч рублей за умышленный поиск материалов, включенных в федеральный список экстремистских материалов Минюста, который на сегодня содержит более 5,4 тысяч позиций.

¹ <https://xn--b1aew.xn--p1ai/folder/101762>, Состояние преступности в России

- Борьба с финансированием экстремизма: с 1 июня 2025 года вступил в силу федеральный закон¹, направленный на противодействие финансированию экстремистской деятельности, что закрывает важнейший ресурсный канал для деструктивных сил.

Вместе с тем, одной из наиболее сложных проблем правоприменения остается расплывчатость формулировок в определении экстремистской деятельности. Анализ закона показывает, что под экстремизмом может пониматься не только прямое насилие или его пропаганда, но и «публичное оправдание терроризма и иная террористическая деятельность», которая может интерпретироваться чрезвычайно широко. В частности, даже нейтральные или позитивные высказывания в отношении организаций, признанных экстремистскими, могут быть квалифицированы как правонарушение.

Согласно теории оперативно-розыскной деятельности, оперативно значимая информация может быть получена в двух формах: в активном и пассивном. Пассивный не предполагает осуществления каких-либо активных действия, активный же наоборот: сюда можно отнести и осуществление мониторинга сети Интернет.

Опросом оперативных сотрудников подразделения по противодействию экстремизму установлено, что в 62.5% случаев эффективными направлением оперативного поиска лиц, вынашивающих экстремистские намерения, являлся мониторинг сети Интернет.² Результаты опроса оперативных сотрудников установлено, что мониторинг сети Интернет в качестве направления оперативного поиска преступлений экстремистской направленности успешно используют 27% респондентов.³

К числу особенностей относятся следующие:

1. необходимость для оперативного сотрудника обладать специальными познаниями в сфере осуществления экстремистской деятельности:

а) специфическая лексика экстремистов. Причем экстремизм существует во множестве различных форм, таких как: политический, гендер-

¹ Федеральный закон от 28.12.2024 № 522-ФЗ "О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и отдельные законодательные акты Российской Федерации».

² Жерновников Д. А. Способы выявления и документирования административных правонарушений экстремистской направленности, совершенных с использованием информационно-коммуникационных сетей / Д. А. Жерновников // Актуальные вопросы охраны общественного порядка и административной деятельности полиции: Материалы внутриведомственной научно-практической конференции, Волгоград, 16–17 июня 2022 года. – Москва: ООО «Издательство "Спутник+"», 2022. – С. 193-197

³ Ассоциация Профессионалов Сыска (АПС) // [Электронный ресурс] URL: <https://alldetectives.ru/ort/vyyavlenie-i-dokumentirovanie-prestuplenij-ekstremistskoj-i-terroristicheskoy-napravlenosti/vyyavlenie-prestuplenij-ekstremistskoj-i-terroristicheskoy-napravlenosti.html> (дата обращения 28.10.2025)

ный, спортивный, культурный, национальный. Сленг приверженцев различных видов экстремизма может разительно отличаться;

б) символика и атрибутика. (например, 14/88; WW/WR для сторонников идей национализма и прочие);

2. Возможность факта тщательного сокрытия преступниками своих объединений в социальных сетях и на форумах (создание и администрирование закрытых групп);

3. Необходимо владеть навыками работы с ПК и сетью Интернет;

4. Уметь устанавливать контакт с лицами, задействованными в экстремистской деятельности с помощью использования тактических приемов и способов общения и перевоплощения;

5. После проведения мониторинга может быть выявлен факт совершения или подготовки преступления экстремистской направленности, на основании которого в дальнейшем может быть заведено дело оперативного учета и осуществлены оперативно-розыскные мероприятия: оперативный эксперимент, оперативное внедрение;

6. Проведение мониторинга социальных сетей также служит предпосылкой для осуществления других функций оперативного сотрудника. Так, в результате мониторинга могут быть выявлены лица, которым известна оперативно значимая информация. Данные лица могут быть использованы для внедрения в качестве конфиденциальных сотрудников, оказывающих содействие органам внутренних дел;¹

Вместе с тем, современная практика выявления нарушений в области распространения и поиска экстремистских материалов основывается на комплексном мониторинге цифровой активности пользователей. Основными источниками значимой оперативно-розыскной информации могут являться:

- история поиска в браузерах и на интернет-порталах;
- анализ интернет-трафика провайдерами;
- данные о поиске музыки на стриминговых сервисах;
- информация от организаторов распространения информации (ОРИ), обязанных предоставлять данные о действиях пользователей государственным органам;
- сведения, собранные через публичные WiFi-сети.

Также к источникам получения первичной оперативно значимой информации относятся:

- граждане, которые в различном виде (устно, письменно, в том числе анонимно) сообщают о фактах совершения преступлений террористической и экстремистской направленности или их видимых признаках;

¹ Савельева М. В., Основы оперативно-розыскной деятельности: учебное пособие / М. В. Савельева, А. Б. Смушкин. М.: Юстиция, 2024. С.134-135

- сотрудники ОВД, инициативно предоставляющие информацию, полученную ими в результате осуществления их служебной деятельности;
- результаты мониторинга информационного пространства (сайты, форумы, социальные сети);
- суточные сводки о преступлениях;
- сообщения конфидентов.¹

Борьба с распространением экстремистских материалов в интернете представляет собой сложную и многогранную проблему, требующую сбалансированного подхода. Новейшие законодательные инициативы, направленные на запрещение самого поиска запрещенного контента, безусловно, усиливают инструментарий правоохранительных органов, но одновременно создают серьезные риски для прав граждан в связи с расплывчатостью формулировок и широкими возможностями для произвольного толкования. Наиболее перспективными представляются следующие направления развития системы противодействия цифровому экстремизму: развитие международного сотрудничества в области выявления и пресечения распространения экстремистских материалов, включая гармонизацию законодательных подходов и создание транснациональных механизмов обмена информацией и внедрение технологических решений, способных идентифицировать не только явный, но и скрытый экстремистский контент, с обязательным учетом контекста его распространения.

¹ Лапин, Е. С. Оперативно-розыскная деятельность: учебник и практикум для среднего профессионального образования / Е. С. Лапин. 7-е изд., перераб. и доп. М: Издательство Юрайт, 2023. С.162.

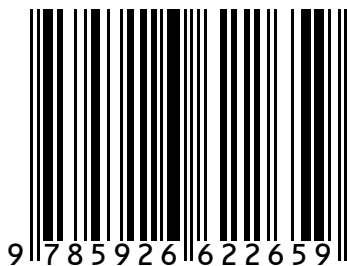
Научное издание

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Материалы
XIV Всероссийской научно-практической конференции
(30 октября 2025 г.)

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-2265-9



Подписано в печать 26.02.2025.
Авт. л. 11,2. Заказ 423.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.