

УДК 343.98

ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» И «НАВЕДЕНИЕ СПРАВОК»: ВОПРОСЫ РЕГЛАМЕНТАЦИИ И РЕАЛИЗАЦИИ

OPERATIONAL SEARCH ACTIVITIES «OBTAINING COMPUTER INFORMATION» AND «MAKING INQUIRIES»: ISSUES OF REGULATION AND IMPLEMENTATION

Олег Хамитович Галимов,

профессор кафедры оперативно-розыскной деятельности Сибирского юридического института МВД России (г. Красноярск), кандидат юридических наук, доцент, судья Красноярского краевого суда в почетной отставке

galimov_oleg@mail.ru



Кирилл Михайлович Грица,

старший оперуполномоченный отделения по раскрытию преступлений, совершенных с использованием информационно-телекоммуникационных технологий, отдела по раскрытию имущественных преступлений управления уголовного розыска МВД по Республике Хакасия (г. Абакан)

kgritca@mail.ru



Ключевые слова:

оперативно-розыскная деятельность, получение компьютерной информации, наведение справок, судебный контроль, специальные технические средства.

В статье рассмотрены актуальные вопросы нормативного регулирования и практической реализации оперативно-розыскных мероприятий «получение компьютерной информации» и «наведение справок». Сочетание «наведения справок» и «получения компьютерной информации» стало точкой пересечения традиционного сыска и цифровой эпохи, породив массу споров и практических сложностей. Анализируются законодательные коллизии при использовании специальных технических средств, а также проблемы разграничения данных мероприятий в условиях цифровизации общества. На основе мнений ученых в области оперативно-розыскной деятельности предложены пути совершенствования правоприменительной практики.

Keywords:

operational investigative activities,
obtaining computer information,
making inquiries,
judicial control,
special technical means.

The article discusses current issues of regulatory regulation and practical implementation of operational investigative measures «obtaining computer information» and «making inquiries». The combination of «making inquiries» and «obtaining computer information» has become a point of intersection between traditional detective work and the digital age, giving rise to a lot of controversy and practical difficulties. The article analyzes legislative conflicts when using special technical means, as well as the problems of distinguishing these activities in the context of digitalization of society. Based on the opinions of scientists in the field of operational investigative activities, ways to improve law enforcement practice are proposed.

Оперативно-розыскная деятельность (ОРД) является формой борьбы с преступностью и видом правоохранительной деятельности и представляет собой «регулируемую законом деятельность специально уполномоченных государственных органов, осуществляемую посредством оперативно-розыскных мероприятий, проводимых на гласной и негласной основе, направленную на выявление, предотвращение, раскрытие и расследование преступлений, розыск скрывающихся от следствия и суда лиц, установление местонахождения пропавших без вести, а также сбор имеющих значение сведений, и обеспечивающую реализацию мер безопасности и охраны общественного порядка» [7, с. 39].

Основным способом осуществления ОРД является производство оперативно-розыскных мероприятий (ОРМ) – законодательно закрепленных, гласных и негласных действий уполномоченных государственных органов (оперативных подразделений) по сбору информации, необходимой для защиты жизни, здоровья, прав и свобод человека и гражданина, обеспечения безопасности общества и государства от преступных посягательств. ОРМ являются важнейшим инструментом в арсенале правоохранительных органов, позволяющим действовать не только «пост-фактум», но и в превентивном формате.

Перечень ОРМ установлен в ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон об ОРД), и включает в себя 15 пунктов (видов ОРМ).

И если ОРМ «наведение справок» является традиционным для правоохранителей, то ОРМ «получение компьютерной информации» было введено в правовое поле сравнительно недавно – 10 лет назад (Федеральным законом от 6 июля 2016 г. № 374-ФЗ) в числе дополнительных мер противодействия терроризму и обеспечения общественной безопасности.

Сегодня в условиях цифровизации общественных отношений и трансформации преступности в киберпространство вопросы совершенствования ОРД приобретают особую значимость. Правоприменитель сталкивается с необходимостью переосмысления подходов к проведению ОРМ. При этом такие мероприятия, как «наведение справок» и «получение компьютерной информации», являются наиболее дискуссионными и технически сложными. Эти проблемы обусловлены как лакунами в законодательстве, так и технологическими вызовами.

Исследователи отмечают, что до настоящего времени «нет однозначного толкования п. 15 «Получение компьютерной информации» ст. 6 Закона об ОРД. Под таковым можно понимать как составную часть оперативно-разыскного мероприятия «снятие информации с технических каналов связи», так и любое гласное действие, совершаемое в сети Интернет» [11, с. 59]. По мнению Ю.Н. Соколова, получение компьютерной информации «своим объемом охватывает: сведения о входящих и исходящих соединениях абонента и (или) абонентского устройства (биллинговую информацию); информацию, хранимую операторами связи в соответствии со специальными правилами; компьютерную информацию, содержащуюся на электронных устройствах объекта оперативной заинтересованности» [13, с. 40].

Правовая основа проведения рассматриваемых мероприятий достаточно разнообразна, включает в себя законодательные (Закон об ОРД), межведомственные (Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд¹ – далее Инструкция) и внутриведомственные (например, Правила хранения операторами связи текстовых сообщений, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи²) нормативные акты.

Выделим основные проблемные моменты регламентации и реализации рассматриваемых ОРМ.

Во-первых, «размывание границ» между этими ОРМ. Законодательство не всегда четко разграничивает, когда получение данных из открытых источников или у операторов связи является «наведением справок», а когда – «получением компьютерной информации».

В сущность понятия «наведение справок» ведущими специалистами в области оперативно-розыскной деятельности включается получение факти-

1 Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : 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 27.09.2013 // СПС «КонсультантПлюс».

2 Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи : постановление Правительства РФ от 12.04.2018 № 445 // СПС «КонсультантПлюс».

ческой информации путем направления в установленном порядке запроса соответствующему юридическому или физическому лицу, располагающему или могущему располагать таковой, а равно ее получение путем непосредственного ознакомления с материальными носителями (документами, банками данных)¹. Следует акцентировать внимание, что при наведении справок не осуществляется вмешательство в тайну связи, а используются легальные каналы доступа [14, с. 15].

Если ранее это мероприятие связывалось с доступом к ЭВМ без ведома их собственников, то сегодня оперативные подразделения сталкиваются с необходимостью применения специальных технических средств для сбора информации в публичных сегментах Интернета. На практике простые действия часто пытаются оформить через более сложные процедуры, что создает путаницу и риски признания доказательств недопустимыми.

Как отмечают исследователи, ОРМ «получение компьютерной информации» занимает все более значимое место в деятельности оперативно-розыскных подразделений [1-4; 6; 8; 12].

Получение компьютерной информации – «это оперативно-техническое мероприятие, направленное на сбор сведений, циркулирующих в компьютере или сети компьютеров, а также содержащихся на различных носителях машинной информации с последующей их фиксацией (или без нее) для решения оперативно-розыскных задач» [9, с. 25].

Интересно отметить, что ранее получение компьютерной информации осуществлялось в рамках такого ОРМ, как «контроль технических каналов связи» (КТКС). К беспроводным электрическим каналам связи (спутниковая, радиосвязь, сотовая и др.) относилась и информация, циркулирующая в компьютерных сетях.

Компьютерная информация (сообщения, данные) «представляется в форме электрических сигналов, независимо от средств их хранения, обработки, передачи, и передается по телекоммуникационным каналам в виде доступной для восприятия ЭВМ. Она может находиться: в оперативной памяти компьютера (ОЗУ), постоянной памяти ПЗУ («жесткий диск»), на внешних носителях информации (компакт-диски, объемные накопители, USB-накопители)» [10, с. 86].

Однако с законодательной точки зрения грань между «наведением справок» и «получением компьютерной информации» очень нечеткая. В.М. Атажитов подчеркивает, что «законодательная конструкция ст. 6 Закона об ОРД требует унификации. Разрозненность правового регулирования мероприятий по получению информации из цифровой среды порождает ведомственную неопределенность и судебные перспективы признания результатов ОРД недопустимыми доказательствами» [5, с. 139].

¹ Дубягин Ю.П., Дубягина О.П., Михайличев Е.А. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» (постатейный) // СПС «КонсультантПлюс».

Во-вторых, технологические сложности. Шифрование (наличие криптографической защиты данных): использование проверяемыми лицами стойких средств шифрования (криптоалгоритмов) делает технически невозможным доступ к переписке и файлам без специальных инструментов.

Обезличивание данных: для расследования это часто «мертвые» данные, которые невозможно привязать к конкретному лицу без дополнительных сложных процедур. Возникают вопросы к качеству и полноте таких данных для использования в ОРД и расследовании.

В-третьих, проблемы судебного контроля и тайны переписки. Существует риск подмены ОРМ, требующих судебного решения (например, «снятие информации с технических каналов связи»), на «получение компьютерной информации», которое может проводиться без такого контроля. Это создает угрозу нарушения конституционных прав граждан на тайну переписки и может привести к признанию полученных данных недопустимыми доказательствами.

В-четвертых, бюрократические и технические задержки. Запросы на получение информации от операторов связи и провайдеров часто проходят через Бюро специальных технических мероприятий (БСТМ), где они могут находиться в очереди длительное время. Это снижает оперативность расследования. Кроме того, операторы предоставляют полный объем данных (переписку, файлы) только по решению суда, что усложняет работу оперативных подразделений.

Указанные факторы существенно затрудняют эффективное применение указанных ОРМ и требуют как законодательных уточнений, так и технологического развития правоохранительных органов.

При проведении «получения компьютерной информации» оперативный сотрудник обязан руководствоваться ст. 7 и 8 Закона об ОРД. Согласно ч. 3 ст. 8 закона проведение мероприятия, сопряженного с ограничением конституционных прав граждан, допускается только на основании судебного решения. Исключение составляют случаи, не терпящие отлагательства, с уведомлением судьи в течение 24 часов.

Приказ МВД России от 31 марта 2023 г. № 199 «Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность» играет важную роль в обеспечении законности, особенно в части применения технических средств в оперативно-розыскной деятельности.

Анализ практики органов внутренних дел выявляет наиболее частые нарушения при проведении ОРМ:

- отсутствие мотивированного постановления, утвержденного руководителем органа, проводящего ОРМ (нарушение ст. 7 Закона об ОРД);
- проведение «получения компьютерной информации» под видом «наведения справок» для упрощения процедуры согласования без судебного решения, что фактически нарушает право на тайну связи.

В этой связи следует учитывать постановление Пленума Верховного Суда РФ от 31 октября 1995 г. № 8¹, которое подчеркивает необходимость судебного санкционирования любых действий, ограничивающих право на тайну связи.

Также стоит отметить, что современные ОРМ «наведение справок» требуют использования Единой информационно-телекоммуникационной системы органов внутренних дел (ЕИТКС). Однако доступ к базам данных других министерств и ведомств (ФНС, Росреестр, Центральный банк) регулируется регламентами межведомственного информационного взаимодействия, утвержденными постановлениями Правительства РФ (например, постановление Правительства РФ от 8 сентября 2010 г. № 697²).

Подводя итог, следует отметить, что ОРМ «получение компьютерной информации» и «наведение справок» имеют различную правовую природу. Первое направлено на негласное проникновение в информационные системы и требует судебного контроля, а второе – на легальное получение сведений из баз данных через запросы.

Существующая нормативная база не полностью отражает современные технологические реалии, такие как работа с облачными хранилищами и мессенджерами, что создает риски для оперативных подразделений.

Необходимо внести изменения в ведомственные нормативные акты, регулирующие использование специальных технических средств для фиксации информации в Интернете в рамках мероприятия «наведение справок», чтобы не нарушать конституционные права граждан.

Проблема носит комплексный характер. Она требует не просто «запретить шифрование» или «упростить законы», а создания гибкой правовой базы, которая бы:

- четко разграничивала гласные и негласные методы работы с данными;
- регламентировала использование специальных технических средств;
- обеспечивала баланс между правом на частную жизнь граждан и необходимостью защиты общества от преступности.

Пока этот баланс не найден, споры вокруг этих двух ОРМ будут оставаться острыми в юридической практике.

1 О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия : постановление Пленума Верховного Суда РФ от 31.10.1995 № 8 // СПС «КонсультантПлюс».

2 О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия») : постановление Правительства РФ от 08.09.2010 № 697 // СПС «КонсультантПлюс».

Библиографический список

1. Алексанин, А.С. Об условиях получения компьютерной информации в оперативно-розыскной деятельности / А.С. Алксанин // Библиотека криминалиста. – 2018. – № 1 (36). – С. 241-247.
2. Алексанин, А.С. Введено новое оперативно-розыскное мероприятие: «получение компьютерной информации» / А.С. Алексанин, С.И. Захарцев // Мир политики и социологии. – 2019. – № 5. – С. 145-149.
3. Алексанин, А.С. О понятии и содержании оперативно-розыскного мероприятия «получение компьютерной информации» / А.С. Алексанин // Правовое государство: теория и практика. – 2018. – № 1. – С. 153-159.
4. Алексанин, А.С. Права человека и оперативно-розыскное мероприятие, связанное с получением компьютерной информации / А.С. Алексанин, С.И. Захарцев // Мир политики и социологии. – 2016. – № 12. – С. 131-137.
5. Аتماжитов, В.М. Теоретические и правовые основы оперативно-розыскной деятельности : монография / В.М. Аتماжитов. – М.: ЮНИТИ-ДАНА, 2017. – 415 с.
6. Васюков, В.Ф. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / В.Ф. Васюков, А.В. Булыжкин // Российский следователь. – 2016. – № 6. – С. 3-8.
7. Галимов, О.Х. К вопросу о понятии оперативно-розыскной деятельности / О.Х. Галимов // Научный компонент. – 2025. – № 2 (26). – С. 36-44.
8. Драпезо, Р.Г. Особенности использования результатов оперативно-розыскного мероприятия «получение компьютерной информации» / Р.Г. Драпезо, В.Н. Шелестюков // Российский следователь. – 2018. – № 9. – С. 65- 72.
9. Дубоносов, Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения / Е.С. Дубоносов // Известия ТулГУ. Экономические и юридические науки. – 2017. – №2-2. – С. 23-30.
10. Осипенко, А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А.Л. Осипенко // Вестник Воронежского института МВД России. – №3. – 2016. – С. 86-87.
11. Прысь, Е.В. Проблемы нормативно-правового регулирования использования компьютерной разведки в правоохранительной деятельности / Е.В. Прысь, Е.П. Полянская // Безопасность бизнеса. – 2024. – № 1. – С. 58-61.
12. Семенова, И.В. Оперативно-розыскные мероприятия в условиях цифровых технологий (в контексте международной юстиции) / И.В. Семенова, И.Н. Кондрат // Международное уголовное право и международная юстиция. – 2025. – № 3. – С. 10-14.
13. Соколов, Ю.Н. Наложение ареста на электронные сообщения, их осмотр и выемка / Ю.Н. Соколов // Российский следователь. – 2020. – № 10. – С. 38-41.
14. Шумилов, А.Ю. Оперативно-розыскная деятельность: актуальные проблемы теории и практики / А.Ю. Шумилов. – М.: Издательский дом Шумиловой И.И., 2019. – 304 с.