

Научная статья

УДК: 343.985

DOI: 10.55001/2587-9820.2024.32.18.019

**ТАКТИКА ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ  
ПО ДЕЛАМ О РАСПРОСТРАНЕНИИ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ  
В СФЕРЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ  
С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»**

**Кристина Владимировна Сечина**

Рязанский филиал Московского университета МВД России имени В. Я. Кикотя,  
г. Рязань, Российская Федерация, sechina94@internet.ru

**Аннотация.** Информатизация общества, а также всеобщая доступность к информационно-телекоммуникационным ресурсам, а также сети «Интернет» с одной стороны положительно влияют на все сферы жизнедеятельности, а с другой – создают условия для переориентации преступного мира на совершение преступлений с их использованием. Поэтому после некоторого забвения криминалистическая тактика вновь получила новый импульс для развития. В научной статье рассматриваются тактические особенности проведения осмотра места происшествия, осмотра предметов (документов), обыска по делам о распространении заведомо ложной информации в сфере общественной безопасности. Предлагаются изменения в уголовно-процессуальное законодательство в целях устранения юридических неопределенностей при расследовании как указанной группы преступлений, так и иных уголовно-наказуемых деяний.

**Ключевые слова:** заведомо ложная информация, осмотр места происшествия, обыск, осмотр предметов (документов), тактические особенности, подготовительные мероприятия

**Для цитирования:** Сечина, К. В. Тактика производства отдельных следственных действий по делам о распространении заведомо ложной информации в сфере общественной безопасности с использованием сети «Интернет» // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2024. Т. 32. № 4. С. 186–193. DOI: 10.55001/2587-9820.2024.32.18.019

**TACTICS OF CONDUCTING SEPARATE INVESTIGATIVE ACTIONS IN CASES OF  
DISSEMINATION OF DELIBERATELY FALSE INFORMATION IN THE FIELD OF  
PUBLIC SECURITY THROUGH THE USE OF THE INTERNET**

**Christina V. Sechina**

Ryazan Branch of Moscow University of the MIA of Russia named after V.Y. Kikotya,  
Ryazan, Russian Federation, sechina94@internet.ru

**Abstract.** Informatization of society, as well as universal accessibility to information and telecommunication resources, as well as the Internet, on the one hand, have a positive effect on all spheres of life, and on the other, create conditions for the reorientation of the criminal world to commit crimes using them. Therefore, after some oblivion, forensic tactics again received a new impetus for development. The scientific article discusses the tactical features of conducting an inspection of the scene of the

incident, inspection of objects (documents), search in cases of dissemination of deliberately false information in the field of public security. Amendments to the criminal procedure legislation are proposed in order to eliminate legal uncertainties both in the investigation of this group of crimes and other criminally punishable acts.

**Keywords:** knowingly false information, inspection of the scene, search, inspection of objects (documents), tactical features, preparatory measures

**For citation:** Sechina, Ch. V. Taktika proizvodstva otdelnuh sledstvennuh deistvii po delam o rasprostraneni zavedomo lozhnoi informacii v sfere obshchestvennoi bezopasnosti, posredstvom ispolzovaniya seti «Internet» [ Tactics of conducting separate investigative actions in cases of dissemination of deliberately false information in the field of public security through the use of the internet] // Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2024, vol. 32 no. 4, pp. 186–193 (in Russ.). DOI: 10.55001/2587-9820.2024.32.18.019

### **Введение**

Современный период развития общества характеризуется стремительным возникновением новых угроз, посягающих как на безопасность граждан, так и на суверенитет нашей страны. Наряду с «традиционными» уголовно-правовыми деяниями, связанными с распространением заведомо ложной информации об актах терроризма, все чаще объектом преступлений становятся иные сегменты общественной безопасности, которые включают санитарно-эпидемиологическое благополучие населения, а также нормальную работу организаций, предприятий и органов государственной власти.

Отмеченное обусловило необходимость разработки и принятия мер уголовно-правовой защиты. В связи с распространением в 2020 году новой коронавирусной инфекции, законодательные органы приняли решение о введении уголовной ответственности за действия, связанные с публичным распространением заведомо недостоверной информации о ситуациях, угрожающих жизни и безопасности населения (ст. 207.1 УК РФ<sup>1</sup>). Публичное распространение ложной информации, которая заведомо не

соответствует действительности и может привести к тяжким последствиям, побудило законодателя к дополнению УК РФ статьей 207.2.

Проведение специальной военной операции на территории Украины стало своеобразным триггером к возникновению фактов публичного распространения заведомо ложной информации о действиях Вооруженных Сил Российской Федерации, Федеральной службы войск национальной гвардии Российской Федерации, а также иных органов государственной власти, организаций и добровольческих формирований. В связи с этим была разработана и введена в действие статья 207.3 УК РФ, предусматривающая уголовную ответственность за совершение указанных деяний в контексте специальной военной операции.

Таким образом, новые составы преступлений, касающиеся публичного распространения заведомо ложной информации, были интегрированы в Главу 24 Уголовного кодекса Российской Федерации, дополнив группу однородных составов преступлений.

### **Основная часть**

Анализ материалов уголовных дел, возбужденных по факту распространения заведомо ложной информации в сфере общественной безопасности (статьи 207–207.3 УК РФ), позволяет выделить ряд следственных действий, правильная организация тактики проведения которых позволяет эффективно раскрывать и

<sup>1</sup> Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/](https://www.consultant.ru/document/cons_doc_LAW_10699/) (дата обращения: 18.11.2024).

расследовать преступления рассматриваемой группы.

Осмотр места происшествия по делам о распространении заведомо ложной информации в сфере общественной безопасности – неотложное следственное действие, во многом определяющее ход предварительного расследования. В ходе его проведения следователь (дознатель) имеет возможность изучить обстановку места происшествия, обнаружить следы (материальные, цифровые) противоправной деятельности, предметы, используемые в качестве средств распространения недостоверной информации.

Подготовительные мероприятия к проведению осмотра места происшествия включают в себя определение арсенала специальных технических средств, необходимых для решения поставленных перед должностным лицом задач.

На основе анализа материалов уголовных дел возможно сделать вывод о том, что местами распространения заведомо ложной информации наиболее часто выступают:

- площадки для публичных выступлений;
- помещения теле-, радиокomпаний в случаях распространения «фейковой» информации через средства массовой информации;
- жилые помещения, интернет-кафе, места работы (для распространения заведомо ложной информации посредством информационно-телекоммуникационной сети «Интернет»).

В последних двух случаях, как отмечает М. В. Кардашевская, целью осмотра места происшествия (помимо непосредственной фиксации обстановки) будет выступать обнаружение и изъятие средств, используемых для совершения преступлений: мобильных телефонов, компьютеров, планшетов, «жестких дисков» и иных носителей информации, материальных и цифровых следов [1, с. 139].

Согласимся с мнением А. Я. Климовой, которая отмечает, что в рамках проведения осмотра места про-

исшествия важно обнаружить и приобщить к материалам уголовного дела цифровые следы [2, с. 176]. Их анализ в последующем позволяет получить важную криминалистическую информацию, включающую сведения о том, сколько раз и как долго посещался сайт (мессенджер, социальная сеть), о предполагаемом местонахождении (IP-адресе) устройства и используемых способах оплаты его аренды, и позволяющую восстановить удаленные пользователем данные (звонки, геотеги, временные маркеры, в том числе содержащиеся на облачных сервисах, а также удаленную цифровую информацию).

К цифровым следам будут относиться:

- цифровые данные, содержащиеся в памяти электронного носителя информации технического средства, которые позволяют задокументировать факт распространения заведомо ложной информации путем отправки электронных писем (совершения звонков), а также делающие возможным определение местонахождения пользователя в конкретный временной период;

- данные социальных сетей, информация, находящаяся на страницах и сайтах в информационно-телекоммуникационной сети «Интернет», в том числе цифровые истории их размещения и рассылки (репостов) в сети «Интернет» и пр.

Следует согласиться с рекомендацией, сформированной П. М. Зуевым, что в целях качественного проведения осмотра места происшествия следователь (дознатель), выезжающий на место, должен ориентироваться в следах и механизме следообразования любого преступления, в противном случае тактические рекомендации теряют практический смысл [3, с. 56]. В рамках рассматриваемой группы преступлений осмотр места происшествия целесообразно проводить следователю (дознателю), который специализируется на расследовании преступлений, совершенных с использованием

информационно-телекоммуникационных технологий и сети «Интернет».

Осмотр предметов и документов – следственное действие, проводимое в ходе расследования уголовных дел, возбужденных по фактам распространения недостоверной информации, с целью визуального изучения и документирования компьютерной информации, предметов, оставленных в местах подготовки и совершения преступления.

Подготовка к проведению осмотра компьютерной информации будет включать в себя привлечение специалиста, обладающего необходимыми компетенциями в этой области. Грамотное проведение рассматриваемого следственного действия позволяет установить и зафиксировать взаимосвязанность распространения заведомо ложной информации с конкретным лицом, получить доказательства его причастности к совершению преступления. Кроме того, в ходе осмотра специалист может применить специализированные комплексы («Мобильный криминалист», «АПК UFED»), позволяющие повысить результативность осмотра компьютерной информации.

Аппаратно-программный комплекс UFED представляет собой средство для проведения оперативного исследования мобильных устройств. Аппаратно-программный комплекс позволяет провести упрощенное и быстрое логическое извлечение информации из обширного ряда мобильных устройств: мобильных телефонов, смартфонов, планшетов, телефонов на базе микропроцессора, некоторых моделей GPS-приемников, сим-карт мобильных устройств и карт памяти.

UFED использует несколько механизмов анализа мобильных устройств, а именно:

- 1) извлечение данных на физическом уровне;
- 2) логическое извлечение;
- 3) извлечение файловой системы.

Извлечение данных на физическом уровне предполагает побитовое полное копирование содержания памяти мобильного устройства. Указанный метод извлечения данных позволяет извлечь не только неповрежденные данные, но и скрытые данные, включая ранее удаленную информацию.

Поддерживаемые типы данных, извлекаемые на физическом уровне, включают неповрежденные и удаленные пароли, установленные приложения, географические теги, информацию о местонахождении, файлы мультимедиа, такие как фото- и видеофайлы пользователя.

Логическое извлечение предполагает извлечение данных при помощи операционной системы устройства. Это означает, что инструменты извлечения данных взаимодействуют с операционной системой устройства и запрашивают из нее информацию. Использование такого метода позволяет получить большинство оперативных данных мобильного устройства.

О. С. Бутенко отмечает, что типы данных включают в себя пароли, списки звонков, журналы звонков, сохраненные на сим-карте, данные телефона (IMEI/ESN), записи телефонной книги, SMS, MMS, изображения, видео- и аудиофайлы и др. Следует подчеркнуть, что в большинстве случаев логическое извлечение невозможно для заблокированных устройств [4, с. 303].

В связи с этим необходимо отметить фактор, создающий препятствие для более широкого распространения практики применения UFED в ходе расследования уголовных дел. Таким обстоятельством является трудозатратность проведения исследования с помощью UFED. Каждая модель мобильного устройства достаточно уникальна относительно возможности извлечения содержащейся в ней информации, что определяет необходимость криминалистического осмотра предмета на протяжении от 2 до 5 часов.

Особенностью программы «Мобильный криминалист» является жесткая привязка путей, по которым расположены файлы – базы данных приложений. То есть если структура базы данных какого-либо приложения осталась прежней, но изменился путь, по которому база данных находится в мобильном устройстве, «Мобильный Криминалист» просто пропустит такую базу данных в ходе анализа. По этой причине исследование подобных баз данных приходится производить вручную, используя файловый браузер «Мобильного Криминалиста» и вспомогательные утилиты.

Следственное действие «осмотр предметов и документов» является типовым для всех предметов и документов, подлежащих документированию, что, по-нашему мнению, не совсем правильно. В действующем уголовно-процессуальном законодательстве отсутствует следственное действие, закрепляющее порядок документирования именно электронной информации и цифровых следов, что создает проблемы в правоприменительной практике и свидетельствует о наличии существенной нормативной неопределенности, подлежащей устранению. Учитывая изложенное, полагаем целесообразным внести в Уголовно-процессуальный кодекс Российской Федерации<sup>2</sup> правовые предписания, устанавливающие требования к осмотру технических средств, содержащих цифровую информацию или цифровые следы, имеющие значение для полного, всестороннего и объективного расследования уголовного дела. Представляется возможным использование опыта, выработанного уголовно-процессуальным законодательством Республики Беларусь (статьей 204.1

<sup>2</sup> Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 22 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультантПлюс : сайт. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_34481/](https://www.consultant.ru/document/cons_doc_LAW_34481/) (дата обращения: 01.05.2024).

УПК Республики Беларусь). Толчком к его реализации послужило отсутствие следственного действия, регламентирующего осмотр компьютерной информации, что привело к наличию юридических проблем при признании компьютерной информации допустимым доказательством<sup>3</sup>.

В ходе производства предварительного расследования по делам о распространении «фейковой» информации, на наш взгляд, производство обыска будет иметь одно из ключевых значений для получения и формирования доказательственной базы, необходимой для привлечения виновных лиц к уголовной ответственности.

При подготовке к проведению обыска необходимо:

1) определить дату и время проведения следственного действия;

2) обеспечить конфиденциальность проведения обыска (не допустить информирование заинтересованных лиц о дате и времени его проведения);

3) обеспечить присутствие специалистов, в том числе имеющих познания в области работы с компьютерной информацией, наличие технических средств, необходимых для производства обыска в рамках конкретной следственной ситуации;

4) информировать участников, оказывающих помощь в проведении поисковых мероприятий, о предметах, объектах, подлежащих изъятию.

Тактика проведения обыска включает в себя следующую систему взаимосвязанных действий:

1) обеспечение личной безопасности каждого из участников, привлекаемых к производству следственного действия;

2) определение места обнаружения и изъятия материальных (следов

<sup>3</sup> МВД – о новеллах уголовного и уголовно-процессуального законодательства Беларуси // Национальный правовой Интернет-портал Республики Беларусь : сайт. URL: <https://pravo.by/novosti/analitika/2021/august/65524/> (дата обращения: 14.11.2024).

пальцев рук, ног и т. д.) и цифровых следов преступления (информации, содержащейся в мобильном телефоне, персональном компьютере, флэш-карте, «жестком диске» и т. д.);

3) обеспечение сохранности обнаруженной компьютерной информации путем отключения средств защиты и программ удаленного доступа;

4) ограничение свободы передвижения обыскиваемого лица в целях предотвращения уничтожения компьютерной информации, цифровых следов преступления;

5) соблюдение законности при изъятии электронной информации и прав лиц, участвующих в следственном действии.

При обнаружении в ходе проведения обыска электронных устройств изымать их полностью не всегда целесообразно. В данном случае необходима консультация специалиста, в ходе которой решается вопрос об изъятии устройства целиком или только жесткого диска.

В рамках анкетирования следователей следственного управления следственного комитета Российской Федерации по Рязанской области 60 % респондентов высказались о наличии нормативной неопределенности получения цифровой информации, содержащей заведомо ложные сведения в сфере общественной безопасности и находящейся в «облачных» хранилищах<sup>4</sup>. В практической деятельности следователи для решения этой проблемы направляют поручения в орган дознания о производстве оперативно-розыскных мероприятий. В ходе их исполнения сотрудники оперативных подразделений органов внутренних дел готовят документы в суд для получения разрешения на производство оперативно-розыскного мероприятия «Получение компьютерной информации». По результатам его проведения в соответствии с действующими

<sup>4</sup> Анкетирование проведено автором статьи.

ними нормативными правовыми актами<sup>5</sup> инициатору поручения направляются полученные материалы и сведения.

По нашему мнению, следует расширить функциональное предназначение обыска (выемки) путем закрепления возможности его применения для обследования не только объектов материального мира (жилых и иных помещений, участков местности), но и цифрового пространства. Полагаем, что предложенная концепция полностью укладывается в существующую уголовно-правовую доктрину и станет элементом упорядочивания мер уголовно-процессуального принуждения.

В связи с изложенным предлагается внести в части 1, 3, 5, 6, 9, 10 статьи 182 УПК РФ изменения, изложив их в следующей редакции:

«Статья 182. Основания и порядок производства обыска

1. Основанием производства обыска является наличие достаточных данных полагать, что в каком-либо месте, **в том числе в цифровом пространстве**, или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, **а также иные данные**, которые могут иметь значение для уголовного дела.

3. Обыск в жилище **и цифровом пространстве, исключая свободный доступ**, производится на основании судебного решения, принимаемого в порядке, установленном статьей 165 настоящего Кодекса.

<sup>5</sup> 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 // КонсультантПлюс: сайт. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_155629/](https://www.consultant.ru/document/cons_doc_LAW_155629/) (дата обращения: 18.11.2024). Режим доступа: для зарегистрир. пользователей.

5. До начала обыска следователь предлагает добровольно выдать подлежащие изъятию предметы, документы и ценности, **а также иные данные**, которые могут иметь значение для уголовного дела. Если они выданы добровольно и нет оснований опасаться их сокрытия, то следователь вправе не производить обыск.

6. При производстве обыска могут вскрываться любые помещения **и цифровые пространства**, если владелец отказывается добровольно их открыть (**предоставить к ним доступ**). При этом не должно допускаться не вызываемое необходимостью повреждение имущества.

9. При производстве обыска во всяком случае изымаются предметы и документы, изъятые из оборота, **а также сведения ограниченного распространения**.

10. Изъятые предметы, документы и ценности предъявляются понятым и другим лицам, присутствующим при обыске, и в случае необходимости упаковываются и опечатываются на месте обыска, что удостоверяется подписями указанных лиц.

### **Собнаруженной цифровой информации с участием специалиста снимаются копии».**

В ходе расследования уголовных дел, возбужденных по статьям 207–207.3 УК РФ, помимо традиционных экспертиз (трасологическая, дактилоскопическая) могут проводиться лингвистические и компьютерные исследования. Перед назначением экспертиз следователю (дознавателю) целесообразно проконсультироваться со специалистом в целях определения перечня вопросов, выносимых на разрешение эксперта, и материалов, направляемых на исследование.

### **Выводы и заключение**

Рассмотренный алгоритм проведения следственных действий не является исчерпывающим и отражает авторскую методику расследования преступлений, совершаемых в сфере общественной безопасности. Полагаем, что предложенные изменения в УПК РФ позволят устранить существующие юридические неопределенности при расследовании как указанной группы преступлений, так и иных уголовно наказуемых деяний.

### **СПИСОК ИСТОЧНИКОВ**

1. Кардашевская, М. В. Развитие методов и средств обнаружения, фиксации, изъятия и исследования следов рук с учетом современных достижений науки и техники // Вестник Московского университета МВД России. 2023. № 6. С. 139–141.
2. Климова, Я. А. Особенности методики расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий // Криминалистика наука без границ: традиции и новации : мат-лы междунар. науч.-практ. конф., Санкт-Петербург, 30 ноября – 01 декабря 2023 года. Санкт-Петербург : Санкт-Петербургский университет МВД России, 2024. С. 176–179.
3. Зуев, П. М. Методика расследования дорожно-транспортных происшествий : учеб. пособие. М., 1990. 56 с.
4. Бутенко, О. С. Применение аппаратно-программных комплексов UFED в системе органов Следственного комитета России // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития : сб. мат-лов Междунар. науч.-практ. конф., приуроч. к 60-летию образования службы криминалистики / под ред. А. И. Бастрюкина. Москва, 2014. С. 303–305.

REFERENCES

1. *Kardashevskaya, M. V.* Razvitie metodov i sredstv obnaruzheniya, fiksacii, iz"yatiya i issledovaniya sledov ruk s uchetom sovremennyh dostizhenij nauki i tekhniki [The development of methods and means of detecting, fixing, removing and examining handprints, taking into account modern achievements of science and technology]. Vestnik Moskovskogo universiteta MVD Rossii. – Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023. no. 6. – Pp. 139-141. (in Russian).
2. *Klimova, Ya. A.* Osobennosti metodiki rassledovaniya prestuplenij, sovershennyh s ispol'zovaniem sovremennyh informacionno-kommunikacionnyh tekhnologij [Features of the methodology for investigating crimes committed using modern information and communication technologies]. kriminalistika nauka bez granic: tradicii i novacii – Criminalistics science without borders: traditions and innovations: Materials of the international scientific and practical conference, St. Petersburg, November 30 December 01, 2023. St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation, 2024. – Pp. 178-179 (176-179). (in Russian).
3. *Zuev, P. M.* Metodika rassledovaniya dorozhno-transportnyh proisshestvij : ucheb. Posobie [Methods of investigation of traffic accidents: textbook. the manual]. M., 1990. – 56 p. (in Russian).
4. *Butenko, O. S.* Primenenie apparatno-programmnyh kompleksov UFED v sisteme organov Sledstvennogo komiteta Rossii [The use of UFED hardware and software complexes in the system of the Investigative Committee of Russia]. Kriminalistika – proshloe, nastoyashchee, budushchee: dostizhenie i perspektivy razvitiya – Criminology - past, present, future: achievements and development prospects. Materials of the International Scientific and Practical Conference dedicated to the 60th anniversary of the formation of the Forensic Science Service. Edited by A.I. Bastrykin. 2014. pp. 303-305. (in Russian).

**ИНФОРМАЦИЯ ОБ АВТОРЕ**

**Сечина Кристина Владимировна**, преподаватель кафедры криминалистики. Рязанский филиал Московского университета МВД России имени В. Я. Кикотя». 390043, Российская Федерация, г. Рязань, ул. 1-ая Красная, д. 18.

**INFORMATION ABOUT THE AUTHOR**

**Christina V. Sechina**, lecturer of the Department of Criminalistics Ryazan branch of the Moscow University of the MIA of the Russian Federation named after V.Y. Kikoty». 18, 1st Krasnaya St., Ryazan, Russian Federation, 390043.