Научная статья
УДК 343. 98

ОСОБЕННОСТИ ПРОВЕРКИ СООБЩЕНИЯ О ПУБЛИЧНОМ РАСПРОСТРАНЕНИИ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ ОБ ИСПОЛЬЗОВАНИИ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Кардашевская М В.
Московская академия Следственного комитета Российской Федерации имени В. Я. Сухарева, г. Москва, Россия

Аннотация. *В статье рассмотрены источники получения информации о совершении преступления, предусмотренного ст. 207.3 УК России; выделены исходные следственные ситуации, лежащие в основе организации проверки сообщения о данном преступлении; определен круг обстоятельств, подлежащих установлению в ходе проверки. Особое внимание уделено применению современных информационных технологий, позволяющих получить сведения, необходимые для решения вопроса о возбуждении уголовного дела.*

Ключевые слова: *Вооруженные силы Российской Федерации; заведомо ложная информация; проверка сообщения о преступлении; «Окулус»; исходные ситуации.*

THE SPECIFICS OF VERIFYING REPORTS ON THE PUBLIC DISSEMINATION OF DELIBERATELY FALSE INFORMATION ABOUT THE USE OF THE ARMED FORCES OF THE RUSSIAN FEDERATION

Kardashevskaya M. V.
Moscow Academy of the Investigative Committee of the Russian Federation named after V. Ya. Sukharev, Moscow, Russia

Abstract. *The article examines the sources of information about the commission of a crime under Article 207.3 of the Criminal Code of Russia; highlights the initial investigative situations underlying the organization of verification of the report of this crime; defines the range of circumstances to be established during the audit. Special attention is paid to the use of modern*

information technologies to obtain the information necessary to resolve the issue of initiating a criminal case.

Keywords: *The Armed Forces of the Russian Federation; knowingly false information; verification of a crime report; "Oculus"; initial situations.*

Осуществление специальной военной операции повлекло за собой новую волну информационной борьбы с Россией, в том числе путем распространения «фейковых» новостей, дискредитирующих содержание и цели специальной военной операции. Как справедливо отмечает С. А. Пичугин, такая дезинформация, будучи инструментом политического влияния, может варьироваться в зависимости от идеологических установок и стратегических приоритетов различных информационных источников. В результате, при сопоставлении данных из разных источников, дезинформация может приобретать противоречивый характер, а в отдельных случаях – даже диаметрально противоположные интерпретации [1, с. 55-56]. Распространение ложных сведений о характере и масштабах военных операций, боевых действиях и статистических данных о потерях может привести к формированию у населения искаженных представлений о текущей специальной военной операции. Это, в свою очередь, способно подорвать доверие к государственным институтам, в частности, к органам военного управления, и негативно сказаться на их авторитете. Сказанное обусловило необходимость криминализации публичного распространения заведомо ложной информации об использовании Вооруженных сил Российской Федерации (далее – ВС России) путем дополнения Уголовного кодекса РФ ст. 207.3 соответствующего содержания [2]. Первоначальная редакция статьи уже трижды изменялась, дополнения касались расширения содержания ложной информации.

В свете относительной новизны данного состава преступления для уголовного законодательства Российской Федерации, а именно: ввиду его принадлежности к категории клеветы, за которую в различные исторические эпохи предусматривалась уголовная ответственность, возникает необходимость в углубленном научном исследовании проблем проверки сообщения о публичном распространении заведомо ложной информации о применении ВС России, являющейся важным этапом частной криминалистической методики.

Любое расследование начинается с получения информации о совершенном преступлении. Все чаще в таком качестве выступают данные, поступившие от должностных лиц, осуществляющих работу с системой автоматического поиска запрещенного контента в Интернете «Окулус» [3], которая в декабре 2022 г. запущена Главным радиочастотным центром (ГРЧЦ), подведомственным Роскомнадзору. «Окулус» представляет собой передовую систему, предназначенную для решения задач классификации изображений и видеороликов в соответствии с установленными нормативными требованиями, включая основные категории запрещенного контента. Функционирование данной системы базируется на алгоритмах машинного обучения и обработки данных, которые используют предварительно заданный набор источников информации для анализа контента на предмет его соответствия законодательным нормам. Основной задачей «Окулус» является анализ фото- и видеоматериалов, собранных другими сервисами, специализирующимися на сборе данных с веб-страниц, социальных сетей и онлайн-платформ. Важно отметить, что «Окулус» не осуществляет сбор данных, а фокусируется исключительно на их анализе и классификации [4].

Только за один год с начала проведения специальной военной операции сотрудниками Роскомнадзора были выявлены, а затем удалены или

заблокированы более 100 тыс. Интернет-ресурсов, содержащих заведомо недостоверную информацию [5]. Ключевой особенностью «Окулуса» является «компьютерное зрение», которое, используя искусственный интеллект, анализирует порядка 200 тыс. информационных объектов (фотографий, комментариев в социальных сетях, видеороликов, аудиозаписей и т. д.) в сутки и выявляет запрещенный к свободному распространению контент [6].

Актуальность применения автоматизированных систем для выявления и анализа ложной информации об использовании ВС России обусловлена увеличением объема соответствующих материалов в глобальной сети. В частности, отмечается значительный рост числа материалов, связанных с текущей военной операцией на территории Украины. Это характеризуется беспрецедентными масштабами и скоростью распространения дезинформации, которая целенаправленно искажает факты, заменяя их искусственно сконструированными нарративами [4].

Риски, связанные с использованием технологии «Окулус», обусловлены точностью классификации визуальных данных, включая изображения и видео. Важным аспектом является корректность интерпретации этих данных в контексте их интеграции с другими элементами системы и взаимодействия с пользователем.

Данные риски обусловлены присущими системам искусственного интеллекта ограничениями, такими как ложные срабатывания, когда определенный контент ошибочно классифицируется как запрещенный, и пропуски, когда система не идентифицирует изображения или видео, содержащие характеристики запрещенного контента. Степень этих погрешностей будет зависеть от интерпретации и настроек системы, определяющих, как классифицировать спорный контент – как запрещенный или нет. Однако эти риски связаны не столько с самим алгоритмическим

решением, сколько с последующей работой с данными, полученными в результате его применения.

После проведения аналитических процедур с использованием искусственного интеллекта крайне важно осуществлять ручную верификацию полученных данных. Это необходимо для обеспечения точности и достоверности информации, а также для проверки корректности функционирования алгоритмов ИИ. Важно подчеркнуть, что результаты аналитической обработки не подлежат автоматической передаче в правоохранительные органы. Вначале сотрудники Роскомнадзора проводят стандартную ручную обработку данных, поэтому при поступлении от них сообщения уже имеются подтвержденные сведения о том, что распространенная в Интернете информация о действиях ВС России является ложной.

Помимо данных, полученных из Роскомнадзора, основанием для возбуждения уголовного дела по ст. 207.3 УК РФ могут служить и результаты проведения оперативно-розыскных мероприятий (наведения справок, снятия информации с технических каналов связи или получения компьютерной информации), проводимых сотрудниками оперативных подразделений. После выявления факта публичного распространения информации об использовании ВС России главной задачей оперативного сотрудника является ее проверка на подлинность. Для этого необходимо:

- проверить источник информации, является ли он официальным (сведения Минобороны), делает ли автор ссылку на какой-либо источник, и опробовать эту ссылку (работает ли она);

- если выложены в сеть какие-либо документы, то следует убедиться в их соответствии установленным шаблонам;

- проверка видеозаписи осуществляется по используемой атрибутике, окружающей местности, форме, наличии сведений о том, что кадры являются/не являются постановочными.

В ряде случаев для проверки подлинности или ложности информации могут привлекаться соответствующие специалисты.

Кроме установления ложности сведений, оперативные сотрудники должны задокументировать признаки публичности их распространения (использование средств массовой информации, информационно-телекоммуникационных сетей, в том числе мессенджеров; массовая рассылка электронных сообщений абонентам мобильной сети; выступление на собрании, митинге и т. п.). Одновременно с этим целесообразно документировать место обнаружения, время и способ распространения информации, устанавливать биографические данные лица, причастного к совершению данного деяния.

Для обоснованного принятия решения о возбуждении уголовного дела по факту распространения заведомо ложной информации о применении ВС России следует провести тщательный анализ и установить ряд обстоятельств:

- информация содержит данные об использовании ВС России в целях защиты интересов нашей страны и ее граждан, поддержания международного мира и безопасности либо об использовании государственными органами своих полномочий за пределами территории России в указанных целях, а также об оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на ВС России или войска национальной гвардии России;

- информация не соответствует действительности;

- способ распространения информации и публичность этого способа;

- личность лица, распространившего дезинформацию, и его осведомленность о ложности сведений, т. е. должны быть установлены обстоятельства, подтверждающие, что распространитель информации заранее знал, что она не соответствует действительности.

С учетом данных обстоятельств, а также в зависимости от способа преступления можно выделить три исходные ситуации, определяющие порядок действия должностных лиц при проверке сообщения о преступлении, предусмотренном ст. 207.3 УК России.

Первую из них следует рассматривать как благоприятную ситуацию. Она характеризуется наличием достаточно полных данных об обстоятельствах совершенного преступления и лице, причастном к его совершению, которое, как правило, задержано по «горячим следам» во время публичного выступления на митинге или собрании.

Ключевой особенностью благоприятной следственной ситуации выступает отсутствие существенного противодействия сотрудникам органов внутренних дел со стороны лиц, распространивших заведомо ложные сведения, попыток скрыться от органов предварительного расследования и суда. Более того, именно публичность совершаемых противоправных действий, открытое донесение такой информации до максимально широко круга лиц (работников организации, радиослушателей, телезрителей и пр.) зачастую выступает одним из основных движителей рассматриваемых деяний, способом выражения частной позиции (о результатах деятельности Вооруженных сил).

Основная задача следователей СК России, к подследственности которых относится данное преступление, в рассматриваемой исходной ситуации состоит в оперативном установлении необходимых для возбуждения уголовного дела обстоятельств. Для этого необходимо опросить максимально

большое количество граждан, участвовавших в собрании, осмотреть их мобильные телефоны на предмет видеозаписи выступления лица с ложной информацией и изъять ее, а также на предмет отправки этой видеозаписи другим лицам, получить запись радио- или телепередачи, справку о выходе передачи в эфир, опросить лицо, которое распространяло заведомо ложную информацию об использовании ВС России.

Вторая исходная ситуация характеризуется как условно благоприятная. Ее отличительной особенностью выступает наличие достаточных данных, которые позволяют с высокой долей вероятности идентифицировать лицо, обоснованно заподозренное в совершении преступления, установить его местонахождение и задержать в целях установления его осведомленности о ложности распространенной им информации об использовании ВС России.

Ее основными признаками выступают:

1) наличие лиц, объяснения которых позволяют установить личность заподозренного, определить мотивы его действий и место нахождения;

2) распространение заведомо ложного сообщения об использовании ВС России посредством использования социальных сетей, мессенджеров, электронной почты, телеграмм-канала и пр., которые делают возможным оперативно идентифицировать личность заподозренного, установить его местонахождение;

3) обнаружение, документирование и изъятие достаточного числа цифровых следов (установление IP-адресов использованного компьютера, номера мобильного телефона, использованного для распространения заведомо ложной информации и т. д.), позволяющих установить личность лица, обоснованно заподозренного в совершении преступления;

4) получение достаточного числа иных данных (записей видеонаблюдения и т. д.), позволяющих идентифицировать преступника.

В свою очередь, третья исходная ситуация выступает как наиболее неблагоприятная для проверки сообщения о преступлении. Она характеризуется наличием достаточных данных, указывающих на распространение ложной информации об использовании ВС России, но отсутствием необходимых сведений, позволяющих установить личность распространителя, а, следовательно, возникают сложности в установлении того, что лицо знало, что распространяло ложную информацию. Это требует тщательного планирования проверки сообщения о преступлении и координации значительного числа оперативно-розыскных мероприятий и следственных действий. Признаками такой исходной ситуации выступают:

1) использование преступником методов конспирации;

2) применение технических средств (одноразовых телефонов (таксофонов), SIM-карт, оформленных на других пользователей, и т. д.) и аппаратно-программных алгоритмов, затрудняющих идентификацию личности преступника;

3) уничтожение следов преступной деятельности, которые могут выступать доказательствами виновности лица;

4) совершение иных действий, направленных на оказание противодействия сотрудникам правоохранительных органов.

Установление виновного лица в данной исходной ситуации возможно путем проведения комплекса оперативно-розыскных мероприятий и следственных действий:

- получение данных о провайдерах, организациях, которым принадлежат социальные сети, почтовые сервисы, мессенджеры;

- направление запросов о предоставлении сведений, указанных при регистрации адреса электронной почты, создании аккаунта в социальной сети

или ином сервисе, использованном для распространения заведомо ложной информации в информационно-телекоммуникационной сети Интернет;

- осмотр страниц в социальной сети и т. п., где была размещена ложная информация об использовании ВС России;

- установление персональных данных лиц, на которые зарегистрированы либо использующих интересующие абонентские номера связи и адреса электронной почты, а также определять местонахождение абонента связи либо отправителя сообщения по электронной почте по геолокации;

- проверка информации, связанной с использованием электронных коммуникаций и Интернет-протоколов. Это включает анализ данных об адресах электронной почты, IP-адресах и других цифровых идентификаторах, которые могут быть связаны с распространением заведомо ложной информации об использовании ВС России. Данные анализируются посредством специализированных ведомственных автоматизированных информационно-поисковых систем и банков данных;

- сбор и систематизация данных, касающихся электронной почты и IP-адресов, которые использовались при регистрации аккаунтов, входе в личные кабинеты и панели управления, а также при администрировании ресурсов, для анализа и мониторинга активности пользователей на хостинговых платформах. Особое внимание следует уделить информации о платежах, связанных с регистрацией и арендой хостинга, включая полные реквизиты плательщиков. Кроме того, целесообразно проводить детальный анализ Cookie-файлов, используемых организациями-арендодателями хостинга и регистраторами доменных имен [7, с. 35-36].

При использовании программных средств, призванных сокрыть истинный IP-адрес и личность пользователя, следователь СК России должен дать письменное поручение о производстве отдельных специальных

технических мероприятий для получения информации, имеющей значение для установления личности виновного лица.

В случае использования распространителем ложной информации платформы TOR-браузера необходимо установить следующие параметры: идентификацию маски подсети источника и ее целевого назначения; определение входящего и исходящего сетевых интерфейсов; анализ протокола транспортного уровня и выявленных флагов в процессе соединения; идентификацию номера протокола IP; установление версии протокола; определение номера записи протокола; временные рамки начала и завершения потока данных; подсчет количества байтов и пакетов, переданных в рамках потока; выявление адреса шлюза; анализ значения протокола транспортного уровня; определение адреса источника и назначения, а также протоколов, используемых на этих уровнях.

При использовании преступниками технологии I2P сети требуется установить: возможность использования различных скриптов общего доступа (например, Times.ip2.); уникальные значения цифровых отпечатков браузера, характеризующих настройки пользователя; специальный криптографический идентификатор; конкретные значения роутера; данные входящих и исходящих туннелей с локальными адресами туннелей.

В случаях применения преступниками технологии SSH-туннелей установлению и конкретизации подлежат: ассиметричные ключи SSH (клиент и сервер каждые имеют открытый и закрытый ключи); база данных публичных ключей и аккаунтов на конкретную дату и в конкретное время; Интернет-трафик за конкретный период времени; установление конкретного пользователя (отправителя ключа).

При выявлении фактов использования прокси-сервера или Dedicated-серверов необходимо установить: список использованных cookie-файлов

(текстовые файлы); список отсканированных портов к исходному IP-адресу; установить список выполненных активных сценариев; местоположение прокси-сервера.

В результате проведения специальных технических мероприятий может быть установлен распространитель ложной информации, однако зачастую данное лицо находится за пределами Российской Федерации – чаще, на территории Украины, намного реже – на территории Евросоюза и Британии. Опросить этих лиц об их знании, что распространяемая ими информация является ложной, в настоящее время является невозможным, однако наличие такого знания не вызывает сомнения, поскольку распространение ими фейков об использовании ВС России фактически является их работой, частью информационной борьбы с нашей страной. Поэтому в данном случае возможно возбуждение уголовного дела без доказывания заведомости, что распространяемая информация является ложной.

Таким образом, особенности проверки сообщения о публичном распространении заведомо ложной информации об использовании Вооруженных сил Российской Федерации обусловлены необходимостью широкого использования современных технологий в целях установления обстоятельств, необходимых для принятия обоснованного решения о возбуждении уголовного дела.

Библиография

1. Пичугин С. А. Уголовная ответственность за деяние, предусмотренное статьей 207.3 УК РФ: вопросы регламентации и правоприменения // Legal Bulletin. 2023. № 3. С. 55-56. EDN: TPASFZ.

2. О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 4 марта 2022 № 32-ФЗ // СПС «КонсультантПлюс».

3. Следи за речью: насколько может быть эффективен мониторинг Рунета от Роскомнадзора. URL: https://www.forbes.ru/tekhnologii/485333-sledi-za-rec-u-naskol-ko-mozet-byt-effektiven-monitoring-runeta-ot-roskomnadzora (дата обращения: 30.04.2025).

4. Тюняева (Бочкарева) М. Роскомнадзор запустил систему автоматического поиска запрещенного контента. URL: https://www.vedomosti.ru/technology/articles/2023/02/13/962682-roskomnadzor-zapustil-sistemu-poiska-okulus?from=copy_text (дата обращения 02.02.2026).

5. Что такое «Окулус» и зачем он нужен Роскомнадзору? URL: https://rg.ru/2023/02/13/chto-takoe-okulus-i-zachem-on-nuzhen-roskomnadzoru.html (дата обращения: 30.04.2025).

6. Российский «Окулус». Как устроена система анализа запрещенного контента. URL: https://4pda.to/2023/02/13/409744/rossijskij_okulus_kak_ustroena_sistema_analiza_zapreschyonnogo_kontenta. (дата обращения: 30.04.2025).

7. Гаврилин Ю. В., Мартыненко Н. Э., Бедеров И. С. Организация расследования заведомо ложных сообщений об актах терроризма: учебное пособие. Москва: Академия управления МВД России, 2023. 73 с. EDN: DOXKUC.

References

1. Pichugin S. A. Criminal liability for an act provided for in Article 207.3 of the Criminal Code of the Russian Federation: issues of regulation and law enforcement. *Legal Bulletin*. 2023; 3: 55-56. (In Russ.).

2. On Amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Code of Criminal Procedure of the Russian Federation: Federal Law No. 32-FZ of March 4, 2022. *ConsultantPlus Legal Reference System*. (In Russ.).

3. Watch your speech: how effective can Roskomnadzor's monitoring of the Runet be? Available at: https://www.forbes.ru/tekhnologii/485333-sledi-za-rec-u-naskol-ko-mozet-byt-effektiven-monitoring-runeta-ot-roskomnadzora (accessed: 30.04.2025). (In Russ.).

4. Tyunyaeva (Bochkareva) M. Roskomnadzor launched an automatic search system for prohibited content. Available at: https://www.vedomosti.ru/technology/articles/2023/02/13/962682-roskomnadzor-zapustil-sistemu-poiska-okulus?from=copy_text (accessed: 02.02.2026). (In Russ.).

5. What is Oculus and why does Roskomnadzor need it? Available at: https://rg.ru/2023/02/13/chto-takoe-okulus-i-zachem-on-nuzhen-roskomnadzoru.html (accessed: 30.04.2025). (In Russ.).

6. Russian "Oculus". How the prohibited content analysis system works. Available at: https://4pda.to/2023/02/13/409744/rossijskij_okulus_kak_ustroena_sistema_analiza_zapreschyonnogo_kontenta (accessed: 30.04.2025). (In Russ.).

7. Gavrilin Yu. V., Martynenko N. E., Bederov I. S. *Organization of investigation of deliberately false reports of acts of terrorism*. A textbook. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia Publ.; 2023.73 p. (In Russ.).

Информация об авторах

Кардашевская Марина Владимировна, доктор юридических наук, профессор, Московская академия Следственного комитета Российской Федерации имени В. Я. Сухарева, г. Москва, Россия, e-mail: kardashewsky@yandex.ru

Information about the authors

Marina V. Kardashevskaya, Doctor of Law, Professor, Moscow Academy of the Investigative Committee of the Russian Federation named after V. Ya. Sukharev, Moscow, Russia, e-mail: kardashewsky@yandex.ru

Для цитирования

Кардашевская М. В. Особенности проверки сообщения о публичном распространении заведомо ложной информации об использовании Вооруженных сил Российской Федерации // Журнал Высокотехнологичное право. − 2026. Т. 2, № 2. − С. 30-43.

For citation

Kardashevskaya M. V. The Specifics of Verifying Reports on the Public Dissemination of Deliberately False Information about the Use of the Armed Forces of the Russian Federation // Journal of High-tech Law. − 2026. Vol. 2, No. 2. − Pp. 30-43.

Поступила в редакцию / Received 02.03.2026
Поступила после рецензирования / Received after review 15.04.2026
Принята к публикации / Accepted 14.05.2026