

# ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В ПРОИЗВОДСТВЕ ПО ДЕЛАМ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ, ЗАФИКСИРОВАННЫХ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ, А ТАКЖЕ НА МОБИЛЬНЫХ И ДРУГИХ КОМПЬЮТЕРНЫХ УСТРОЙСТВАХ

**Зубарев Даниил Сергеевич**

адъютант, старший лейтенант полиции,  
Санкт-Петербургский университет МВД России  
zubar2.0@yandex.ru

## THE USE OF ELECTRONIC EVIDENCE IN PROCEEDINGS ON ADMINISTRATIVE OFFENSES RECORDED IN THE INFORMATION SPACE, AS WELL AS ON MOBILE AND OTHER COMPUTER DEVICES

**D. Zubarev**

*Summary.* This article analyzes the use of electronic evidence in proceedings on administrative offenses located on the Internet or on various digital and mobile devices. The points of view of administrative scientists on the increasing role of electronic evidence in the process of disclosure of administrative offenses occurring in the digital world, thanks to modern technologies, are presented. *Purpose:* to prove that electronic evidence in the proceedings on administrative offenses requires in-depth study in the current legislation. *Methodological basis:* comparative research method, dialectical and formal-logical methods of scientific cognition. *Results:* a proposal has been formed to include changes in the current Administrative Code related to the inspection of electronic information on various information devices, as well as from the Internet. *Conclusions:* Currently, administrative offenses are being committed with increasing rapidity in the information field, using computer and digital systems. In order to combat illegal behavior on the global network, which often goes unpunished, new ways of collecting, recording and using electronic evidence in proceedings on administrative offenses are being introduced.

*Keywords:* electronic evidence, proceedings in cases of administrative offenses, mobile devices, electronic information, electronic media.

*Аннотация.* В данной статье проведен анализ использования электронных доказательств в производстве по делам об административных правонарушениях, находящихся в сети «Интернет», или на различных цифровых и мобильных устройствах. Приводятся точки зрения ученых административистов, о нарастающей роли электронных доказательств в процессе раскрытия административных правонарушений, происходящих в цифровом мире, благодаря современным технологиям. *Цель:* доказать, что электронные доказательства в производстве по делам об административных правонарушениях требуют глубокой проработки в действующем законодательстве. *Методологическая основа:* сравнительный метод исследования, диалектический и формально-логический методы научного познания. *Результаты:* сформировано предложение по включению в действующий КоАП изменений, связанных с осмотром электронной информации, находящейся на различных информационных устройствах, а также с сети «Интернет». *Выводы:* в настоящее время административные правонарушения с нарастающей быстротой совершаются в информационном поле, с помощью компьютерных и цифровых систем. С целью борьбы с противоправным поведением в глобальной сети, которое зачастую остается безнаказанным, происходит внедрение новых способов собирания, фиксации и использования электронных доказательств в производстве по делам об административных правонарушениях.

*Ключевые слова:* электронные доказательства, производство по делам об административных правонарушениях, мобильные устройства, электронная информация, электронные носители информации.

Субъекты административной юрисдикции обнаруживают и собирают доказательственную информацию путем производства необходимых процессуальных и иных действий (осмотр места происшествия, изъятие, истребование сведений, направление запросов, проведение опроса и др.).

Ю.И. Попугаев, исследуя административно-процессуальные меры, применяемые в связи с правонарушением, определяет их как урегулированные административно-процессуальными нормами процессуальные действия органов административной юрисдикции и их

должностных лиц, указывает в качестве одной из целей их осуществления — выявление, исследование и закрепление доказательств.

Акцентируем внимание на определении мер обеспечения производства по делу об административном правонарушении, сформулированном А.И. Каплуновым. В нем автор показывает, что меры обеспечения производства по делам об административных правонарушениях объединены не конкретизированными применительно к каждой такой мере общими целями. [3, с. 13]

К мерам, направленным на получение доказательств, А.И. Каплунов относит: личный досмотр, досмотр вещей, находящихся при физическом лице (ст. 27.7); осмотр принадлежащих юридическому лицу или индивидуальному предпринимателю помещений, территорий и находящихся там вещей и документов (27.8); досмотр транспортного средства (ст. 27.9); изъятие вещей и документов (ст. 27.10); направление на медицинское освидетельствование на состояние опьянения (ч. 2 ст. 27.12); арест товаров и транспортных средств и иных вещей (ст. 27.14) [3, с. 47–48] и проверку документов, удостоверяющих личность.

А.И. Каплунов верно отметил, что на практике с применения такой меры принуждения как проверка документов, удостоверяющих личность, начинается разбирательство с подозреваемым лицом и принимается решение о возбуждении в отношении него дела об административном правонарушении. Сегодня сотруднику полиции при возбуждении дела об административном правонарушении, совершенном в сети «Интернет», необходимо установление IP — адреса, то есть адреса компьютера или мобильного устройства, предназначенного для их идентификации и связи с ним, необходимо идентифицировать лицо, совершившее административное правонарушение.

Главной сложностью в сети «Интернет» продолжает быть идентификация личности, подозреваемого в совершении административного правонарушения, что является причиной прекращения дела об административном правонарушении или возвращения протокола и других материалов для устранения недостатков.

Так, определением Советского районного суда г. Липецка протокол по делу об административном правонарушении, предусмотренном ч. 1.1 ст. 6.13 КоАП РФ и другие материалы были возвращены для устранения недостатков. Как усматривается из представленных материалов, невозможно установить принадлежность Г. к регистрации на указанной странице в социальной сети «ВКонтакте», принадлежность Г. к размещению на этой странице в социальной сети «ВКонтакте» видеофайла, в котором демонстрируются наркотические средства и способы их потребления. [7]

В подобного рода инцидентах, для определения личных данных пользователя, руководству интернет-сообщества направляется официальный запрос, о предоставлении интересующих сведений (ст. 26.9 КоАП РФ). В запросе указываются данные необходимые для разрешения административного дела, а именно: информация о лице при регистрации аккаунта (персональные данные, телефон, электронная почта, а также другие сведения, имеющие значение) и IP — адрес устройства. После получения ответа от администрации сайта устанавлива-

ется оператор связи, в сети которого зарегистрирован установленный IP — адрес и его географическое местоположение.

В процессуальной литературе появился новый термин, названный цифровизацией, — **цифровой профиль личности** — неповторимая совокупность идентификаторов, а именно информация о лице, находящаяся в числовом тексте, в государственных и общественных базах данных. «Цифровой профиль показывает человека в цифровом пространстве, дает ему и его действиям, в том числе с точки зрения различных субъектов, заинтересованных во взаимодействии с личностью, характеристику по разным позициям (платежеспособность, добросовестность, интересы, взгляды и др.)». [9 с. 98–110]

В настоящее время цифровой профиль личности только начинает применяться в электронном доказывании в производстве по делам об административных правонарушениях. Стоит уточнить, что идентификация, как и аутентификация личности в информационном поле осуществляется с помощью единой биометрической системы (ЕБС) и единой системы идентификации и аутентификации (ЕСИА). В соответствии с положениями соответствующих документов, установление цифрового профиля личности в информационной сети расценивается как мера обеспечения производства по делу об административном правонарушении, а именно проверка документов, удостоверяющих личность физического лица. Согласно п. 21 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» под *идентификацией* понимается совокупность мероприятий по установлению сведений о лице, их проверке и сопоставлению с уникальным обозначением сведений о лице, необходимым для определения такого лица. Комплекс действий, направленных на определение идентификатора и соответствующего ему пользователя сети, происходит в рамках процедуры аутентификации, с соотнесением исходных данных о субъекте и приписанному ему идентификатора, с выяснением законных оснований владения лицом уникальным информационным кодом, в результате перечисленных мероприятий лицо признается установленным.

В то же время правоприменителями высказывается проблема невозможности определения геолокации и личных сведений пользователей, выкладывающих запрещенную информацию в сеть «Интернет», вне пределов Российской Федерации.

В настоящий момент меры обеспечения производства применяются для получения электронных доказательств, однако в КоАП РФ (в том числе, в проектных нормах) нет норм, комплексно регламентирующих порядок сбора и фиксации информации, содержащейся на электронных носителях (компьютерах, мобильных

телефонах, флэш, картах памяти и проч.), электронной информации, размещенной в сети «Интернет», находящейся в свободном доступе.

В отличие от административного кодекса ст. 164.1 УПК учитывает специфику изъятия электронных носителей информации и копирование с них информации при производстве следственных действий.

Воздействие цифровизации на все сферы общества требует эффективных способов защиты интересов государства в информационном пространстве.

Неопределенность характера действий, составляющих содержание некоторых мер обеспечения производства по делу об административном правонарушении, целей, оснований их применения негативно влияет на правоприменение. Так, статья 27.8 КоАП РФ, обеспечивающая проведение осмотра принадлежащих юридическому лицу или индивидуальному предпринимателю помещений, территорий, находящихся там вещей и документов, на законных основаниях, все же детально не определяет содержание этой меры, процессуальную цель и основания применения. Может ли быть произведен такой осмотр помещения при совершении любого правонарушения или только связанного с осуществлением предпринимательской деятельности? Можно ли при проведении осмотра требовать от представителя юридического лица или индивидуального предпринимателя предоставлять доступ к содержимому носителей электронной информации? Закон ответа на эти вопросы не дает.

Так, инспектором ООПАЗ УМВД России как уполномоченным на то должностным лицом был проведен осмотр помещения, в ходе которого обнаружен ноутбук с установленными на нем программными продуктами с признаками контрафактности. На рабочем столе бухгалтера в указанном помещении на момент осмотра находились печать и документация юридического лица, а также ноутбук, при осмотре которого с участием специалиста выявлен факт установленного на нем приложения «1С: Предприятие» и наличие документов ООО. В связи с чем данный ноутбук был изъят в качестве предмета административного правонарушения (ст. 27.10 КоАП РФ). Согласно протоколу изъятия вещей и документов, перед изъятием ноутбука должностным лицом присутствующим при проверке лицам предоставлена возможность скопировать с него необходимую информацию. Действия должностного лица ООПАЗ УМВД России по осмотру помещения и изъятию ноутбука Вторым кассационным судом общей юрисдикции признаны соответствующими требованиям действующего законодательства (ст. 27.8, 27.10 КоАП РФ). [4]

В юридической литературе формулируются поддерживаемые нами предложения о внесении в КоАП РФ из-

менений, аналогичных предусмотренным ст. 164.1 УПК РФ. Так, предлагается в ст. 27.10 КоАП РФ предусмотреть, что «изъятие электронных носителей информации, явившихся орудиями совершения или предметами административного правонарушения, имеющих значение доказательств по делу об административном правонарушении и обнаруженных на месте совершения публичного проступка либо при осуществлении личного досмотра, досмотра вещей, находящихся при физическом лице, досмотре транспортного средства, обнаруженных при осуществлении осмотра принадлежащих юридическому лицу территорий, помещений, находящихся у него товаров, транспортных средств и имущества, осуществляется в присутствии двух понятых либо с применением видеозаписи, при участии специалиста». [1, с. 50]

По поводу обязательного участия специалиста при изъятии электронной информации мы выражаем сомнения. В некоторых случаях участие специалиста действительно является значимым и необходимым, так как при неправильных действиях субъекта административной юрисдикции электронная информация может быть утеряна или уничтожена. В то же время специальные познания специалиста необязательны для изъятия, например, мобильных телефонов, флэш-накопителей, дисков. Поэтому вопрос участия специалиста при изъятии электронной информации отдадим на усмотрение правоприменителя.

Рассмотрим целесообразность введения еще одной предлагаемой новеллы — меры обеспечения производства по делу об административном правонарушении «временное ограничение доступа к Интернет-ресурсам, содержащим информацию с признаками административных правонарушений, предусмотренных ч. 3–5 ст. 20.1 КоАП РФ, и указанных в пп. 58 ч. 2 ст. 28.3 КоАП РФ, до рассмотрения по существу такого дела и вступления в законную силу судебного постановления». [10 с. 37] Основной целью применения новой меры указывается временное пресечение (приостановление, блокировку) контента, а в дальнейшем, при определенных обстоятельствах, и удаление вредоносной информации, ограничение доступа к подобным информационным ресурсам.

Несомненно, предлагаемая новая мера обеспечения заслуживает внимания законодателя, если распространить ее действие на все правонарушения, совершаемые в сети Интернет, а не только к перечисленным авторами, а также предусмотреть еще одну не менее значимую цель ее применения — недопущение утраты доказательственной информации, удаления правонарушителем противоправного контента до вступления в законную силу постановления с целью избежать ответственности за содеянное.

Рассмотрим, как в настоящее время осуществляется сбор и процессуальное оформление доказательств по делам об административных правонарушениях, зафиксированных в информационном пространстве и информации, найденной на цифровых и мобильных устройствах.

Преимущественно в научной литературе, как и в практической деятельности остаются проблемы, связанные с ограничением конструктивных прав и свобод граждан России (право на неприкосновенность частной жизни, тайны переписки и телефонных переговоров, сообщений (ст. 23, ст. 24 Конституции РФ). В процессе осмотра электронных носителей информации (например, мобильного телефона). Проблема обеспечения прав человека — сложна, а поиск необходимого баланса ограничений прав становится как никогда актуальным. Ст. 152.2 ГК РФ устанавливает, «если иное не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о частной жизни, в частности сведений о его происхождении, о месте пребывания или жительства, о личной или семейной жизни». Исключениями являются публичный интерес, общедоступность соответствующей информации, ее раскрытие по воле гражданина.

В юридической литературе делается акцент на важность выработки правового механизма использования персональных данных в процессе собирания электронных доказательств при условии обеспечения конституционных прав, свобод и законных интересов граждан. [6 с. 174–175]

Многочисленные изученные нами дела об административных правонарушениях содержали акты осмотра мобильного телефона с приложением скриншота его экрана. Осмотр информационных компонентов мобильного устройства в полной мере представляет процессуальную процедуру исследования электронной информации: осуществления анализа находящихся в телефонной книге мобильного гаджета звонков, списка сохраненных и удаленных контактов; отслеживания переданных и полученных СМС и ММС сообщений, проверка истории браузера (сохраненных закладок, посещение веб-страниц, социальных сетей, тематических порталов; изучение скаченных и используемых приложений, просмотр фотографий; фиксирование геопозиции лица и его передвижений; установление геолокации лица, передаваемой и получаемой им информации различными средствами (ГЛОНАСС); поиск файлов; анализ проводимых лицом финансовых операций, благодаря мобильным приложениям.

Каждый акт осмотра мобильного телефона в изученных делах содержал выраженное добровольное

согласие гражданина на осмотр мобильного телефона, поскольку добытая в процессе подобного осмотра информация принадлежит к группе охраняемой законом тайны. А как быть, когда такое согласие лицо не дает?

В соответствии с нормами УПК РФ в случаях отказа от добровольного предоставления информации, имеющейся на хранилище мобильного устройства, такая информация может быть изъята осмотром по решению суда. В том случае, когда осмотр должен быть произведен безотлагательно, он может осуществляться без согласия лица по аналогии с правилами, указанными в ч. 5 ст. 165 УПК РФ. [2 с. 27]

В соответствии с п. 1 ч. 2 ст. 28.3 КоАП РФ к непосредственной компетенции органов внутренних дел по составлению протоколов об административных правонарушениях отнесено 13 статей, включающих в себя 31 квалифицированный состав административных правонарушений, в диспозициях которых указаны противоправные деяния, совершаемые с использованием сети «Интернет». Они имеют разные объекты посягательства: «благополучие и общественная нравственность» (гл. 6 КоАП РФ); «общественные отношения в области связи и информации» (гл. 13 КоАП РФ); «общественные отношения в области предпринимательской деятельности и деятельности саморегулируемых организаций» (гл. 14 КоАП РФ); «общественные отношения в сфере общественного порядка и общественной безопасности» (гл. 20 КоАП РФ).

Анализ судебной и административной деятельности территориальных органов МВД РФ позволяет выделить порядок действий практических работников органов внутренних дел по сбору, проверке и фиксации доказательств по делу об административном правонарушении, совершенном в сети «Интернет».

Например, при поступлении информации к сотрудникам полиции, благодаря различным источникам: заявлений граждан, телефонных звонков в отдел полиции или на горячую линию, о нахождении в сети «Интернет» данных унижающих общечеловеческие ценности, этические нормы поведения в обществе, пренебрежение к социуму, государству, официальным государственным символам РФ, Конституции РФ или органам государственной власти (ч.3-5 ст. 20.1), в том числе в случае прямого обнаружения факта совершения административного правонарушения в ходе мониторинга сети «Интернет» необходимо провести следующие действия.

Во-первых, установить (через оперативные подразделения территориальных органов МВД России, на которые возложены функции мониторинга ресурсов в сети «Интернет») источник распространения (сеть «Интернет» или сеть операторов сотовой связи); лицо, распро-

странившее такую информацию, место и время совершения правонарушения.

Во-вторых, следует выявить наличие совокупности следующих условий, при отсутствии хотя бы одного из которых выносится определение об отказе в возбуждении дела об административном правонарушении (ч. 5 ст. 28.1 КоАП РФ): информация адресована широкой группе лиц, и не применяется пользователями глобальной сети в частных, закрытых беседах. Данная информация, выставляется на всеобщее обозрение пользователям сети «Интернет», она включает в себя надругательство над Конституции РФ, государственными публичными символами, общественными и государственными организациями выполняющими функции по осуществлению государственной политики России; при этом такая информация изложена в грубой нецензурной форме, с изображениями непристойного содержания; где гражданин противопоставляет себя окружающим, демонстрирует надменность, унижительное отношение к обществу, государству.

В-третьих, при наличии всех условий, материалы направляются в экспертно-криминалистическое подразделение для проведения лингвистической экспертизы (выносится определение), в ходе которой устанавливается наличие или отсутствия оскорбительного характера информации, открытого презрения к моральным устоям общества, к государственной символике Российской Федерации, Конституции России и ее органам принимающих государственно-политические решения.

Наконец, в-четвертых, при положительном результате экспертного заключения и установления факта совершения административного правонарушения, предусмотренного ч. 3 ст. 20.1 КоАП РФ осуществляются процессуальные действия по сохранению и документированию доказательств правонарушения (отбор объяснений, осмотр места совершения правонарушения, составление акта-исследования интернет-страницы, изъятие доказательств). Через специализированную программу «Административная практика» СООП, а также специализированные базы (ИБД-Р, ИБД-Ф), подозреваемое лицо проходит процедуру проверки причастности к совершению других противоправных деяний, в ходе которой устанавливается было ли лицо ранее привлечено к административной ответственности по ч. 3 и 4 ст. 20.1 КоАП РФ. В случаях подтверждения факта неоднократного привлечения лица к административной ответственности по вышеупомянутой статье составляется протокол об административном правонарушении по соответствующей части (3–5) ст. 20.1 КоАП РФ. Материалы дела направляются в течение 24 часов в территориальную прокуратуру, при положительном решении которой — на рассмотрение судье районного суда.

Таким образом, поскольку противоправный контент размещается в сети «Интернет» в виде устной речи (записи разговоров, видеобращения, интервью), письменных текстов (статьи, книги, надписи), поликодовых текстов (реклама, видеоролики, видеофильмы) и электронных текстов (переписка в социальных сетях, мессенджерах, блогах, форумах, комментариях), важное значение для доказывания вины лица, приобретают сформированные результаты *осмотра социальной страницы сети «Интернет» (акт (протокол) осмотра, акт исследования интернет-страницы)*, заключение эксперта (ст. 26.5 КоАП РФ), пояснения специалиста (25.8 КоАП РФ).

Вернемся к рассматриваемому вопросу по формированию доказательственной базы составов административных правонарушений, предусмотренных ч. 3–5 ст. 20.1 КоАП РФ. Для правильной квалификации и ее формирования привлекаются лица, обладающие специальными познаниями в области лингвистики, психологии, культурологии, искусствоведения и др. Размещенные в сети «Интернет» тексты представляются в виде распечатанных копий снимков экрана (скриншотов) или иных форм представления информации, фиксирующих тексты в их полном объеме и исходном виде. Для исследования записей устной речи, зафиксированной на электронном носителе, представляется фонограмма и протокол ее прослушивания, фиксирующий содержание устного текста.

Подобная практика особенностей процессуального оформления электронных доказательств в сети «Интернет» сложилась во многих территориальных органах МВД России. Проведенное анкетирование сотрудников органов внутренних дел (должностных лиц подразделений охраны общественного порядка, ГИБДД, по вопросам миграции, по противодействию экстремизму, участков уполномоченных, осуществляющих мониторинг сети «Интернет», мессенджеров) позволило выявить основные проблемы при собирании доказательств по делам об административных правонарушениях, совершаемых с использованием сети «Интернет»: 1) отсутствие в КоАП РФ нормы регулирующей использование новой меры обеспечения производства по делу об административных правонарушениях как осмотр Интернет-ресурсов, что в практической деятельности выступает как причина представления с позиции защиты ходатайств о признании полученных доказательств не допустимыми; 2) невозможность своевременного получения от администрации информационных ресурсов в сети «Интернет» данных о пользователях, в том числе результатов проведения экспертиз; 3) трудности с определением расположения персональных и других сведений пользователей, выкладывающих противоправную информацию на Интернет-ресурсах, размещенных географически вне юрисдикции Российской Федерации; 4) недоступность

использования итогов оперативно-разыскных мероприятий для привлечения лиц к административной ответственности, в результате совершения административных правонарушений в том числе в сети «Интернет».

Вышеперечисленные проблемы в доказывании по делам об административных правонарушениях, непосредственно возникающие в сети «Интернет» и на различного рода информационных ресурсах, устройствах подталкивают к неизбежному усовершенствованию современной законодательной базы.

Во-первых, следует рассмотреть вопрос о дополнении КоАП РФ **осмотр электронной информации**, содержащейся на любом электронном носителе которая впоследствии может стать электронным доказательством по делу (Интернет-ресурса, мобильного телефона, видеозаписи и проч.). В виде модернизации законодательства введение новой меры обеспечения производства по делам об административных правонарушениях, представляется уместным.

Принимая во внимание, что меры обеспечения производства по делам об административных правонарушениях в юридической литературе относят к мер административного принуждения, представляющие собой юридические санкции имеющие отрицательное влияние на лиц, в отношении которых ведется производство по делу, а «осмотр электронной информации» не носит принудительного характера, то целесообразно главу 28 КоАП РФ дополнить процессуальным действием — «осмотр электронной информации» следующего примерного содержания:

«Статья 28.1.2. Осмотр электронной информации

1. В целях выявления и фиксации данных о совершенном административном правонарушении в сети Интернет, должностным лицом, уполномоченным в соответствии с настоящим Кодексом составлять протокол о соответствующем административном правонарушении, осуществляется осмотр электронной информации.
2. Осмотр электронной информации проводится незамедлительно случаях установления факта совершения административного правонарушения или во время получения информации о совершении административного правонарушения в сети «Интернет», при обязательном участии двух понятых, если же их участие невозможно, применяются средства видео фиксации, о чем делается

соответствующая запись. К протоколу осмотра электронной информации прилагаются скриншоты осматриваемого информационного ресурса или видеозапись».

Думается в дальнейшем, при переходе к производству по делу об административном правонарушении в электронной (цифровой) форме, необходимость бумажной фиксации в протоколе осмотра электронной информации отпадет. Электронное доказательство будет предоставляться в дело об административном правонарушении на любом носителе электронной информации, а указание на ее содержание будет сделано в постановлении об административном правонарушении, оформленном также в электронном виде.

Типовая форма протокола осмотра страницы (сайта) сети «Интернет» в юридической литературе уже была разработана. [5 с. 20–28] Можно ее взять за основу. В протоколе осмотра электронной информации необходимо отражать информацию об используемых технических и программных средствах. Кроме того, перед тем, как сделать скриншот, необходимо проверить актуальность отображаемых на экране монитора даты и времени. Скриншот обязан заключать в себе информацию о полном адресе ресурса в сети интернет (URL), что появляется в адресной строке любого веб-браузера. Напечатанный снимок, в обязательном порядке должен содержать подпись, должность и персональные данные лица создавшего данный документ.

Во-вторых, важно рассмотреть вопрос об увеличении сроков давности привлечения к административной ответственности (ст. 4.5 КоАП РФ), расширение возможности проведения административного расследования (ст. 28.7 КоАП РФ) по данной категории дел.

В-третьих, зафиксировать в нормативно-правовых документах право на применение итогов осуществления оперативно-розыскных мероприятий с целью выявления и фиксации административных правонарушений, совершенных с использованием сети «Интернет», что требует внесения соответствующих изменений в ст. 7 ФЗ «Об оперативно-розыскной деятельности».

В научных публикациях утверждается, что «результаты ОРД могут служить поводом к возбуждению административно-деликтного производства» и «применяться в качестве доказательств по делам об административных правонарушениях». [8 с. 86–90]

## ЛИТЕРАТУРА

1. Анисифорова М.В., Машугина Е.В., Андреев М.В. Теория и практика применения электронных доказательств в производстве по делам об административных правонарушениях. — М.: ИНФРА-М, 2020. С. 50.
2. Желева О.В. К вопросу о порядке производства осмотра мобильного телефона // Сибирские уголовно-процессуальные и криминалистические чтения. 2021. С. 27.
3. Каплунов А.И. Административное принуждение, применяемое органами внутренних дел: Системно-правовой анализ. Автореф. дис. ...доктора юридических наук — М., 2005. С. 13.
4. Кассационное определение Второго кассационного суда общей юрисдикции от 03.04.2024 № 88а-7010/2024 Категория: Споры с МВД России. Требования заявителя: О признании незаконными действий должностного лица органа внутренних дел по осмотру арендованного помещения и изъятию ноутбука. Обстоятельства: Ноутбук являлся предметом административного правонарушения и в соответствии с требованиями ст. ст. 27.1, 27.10 КоАП РФ подлежал изъятию. Решение: Отказано // СПС «КонсультантПлюс».
5. Новгородов Д.А. Некоторые проблемы производства по делам об административных правонарушениях, совершаемых с использованием сети «Интернет». Полицейская деятельность. 2017. № 2. С. 20–28.
6. Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединённых Штатов Америки и Российской Федерации: дис. ... канд. юрид. наук. М., 2016. Черкасов В.С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса: дис. ... канд. юрид. наук. Хабаровск. С. 174–175.
7. Определение Советского районного суда города Липецка от 17.06.2022 № 5–361/2022 О возвращении дела об административном правонарушении для устранения недостатков // СПС «Консультант Плюс».
8. Субботин А.М., Трусов Н.А. Критический взгляд на совершенствование законодательства об оперативно-розыскной деятельности в контексте производства по делам об административных правонарушениях // Вестник Уфимского юридического института МВД России. 2023 г. № 1 (99). С. 86–90.
9. Терещенко Л.К. Трансформация понятийного аппарата информационного права в условиях цифровизации // Журнал российского права. 2022. № 12. С. 98–110.
10. Шевченко Ю.П., Скорев В.А. Формирование правоприменительной практики по делам об административных правонарушениях, предусмотренных чч. 3–5 ст. 20.1 Кодекса Российской Федерации об административных правонарушениях, предусмотренных чч. 3–5 ст. 20.1 Кодекса Российской Федерации об административных правонарушениях // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. — 2023. — № 2. С. 37.

© Зубарев Даниил Сергеевич (zubar2.0@yandex.ru)  
Журнал «Современная наука: актуальные проблемы теории и практики»