

Терехов М. Г. – научный сотрудник
2 отдела научно-исследовательского
центра № 4 Всероссийского научно-
исследовательского института МВД Рос-
сии (Россия, г. Москва)

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА В ПРОИЗВОДСТВЕ ПО ДЕЛАМ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

DIGITAL EVIDENCE IN PROCEEDINGS CONCERNING ADMINISTRATIVE OFFENCES EXTREMIST-ORIENTED

Аннотация. В статье рассматриваются вопросы использования цифровых фактических данных в делах об административных правонарушениях экстремистской направленности. Особое внимание уделяется процедуре правового определения цифровых фактических данных как цифровых доказательств, а также вопросам относимости и допустимости такой информации как базового элемента цифровых доказательств. По итогам статьи определены некоторые рекомендации по совершенствованию административно-правового регулирования понятия цифровых доказательств в производстве по делам об административных правонарушениях экстремистской направленности.

Ключевые слова: цифровые доказательства, административное право, административные правонарушения, допустимость, относимость, социальные сети, экстремизм, цифровая среда.

Abstract. The article discusses the use of digital factual data in cases of administrative offenses of an extremist nature. Special attention is paid to the procedure for legal definition of digital factual data as digital evidence, as well as the issues of relevance and admissibility of such information as a basic element of digital evidence. Based on the results of the article, some recommendations have been made to improve the administrative and legal regulation of the concept of digital evidence in cases of administrative offenses of an extremist nature.

Keywords: digital evidence, administrative law, administrative offenses, admissibility, relevance, social networks, extremism, digital environment.

На современном этапе развития общественных отношений, а также в условиях глобальной цифровой трансформации повседневной жизни общества, сеть Интернет становится не только местом для обмена информацией и современной коммуникации граждан, но и эффективным инстру-

ментом для совершения противоправных действий [4, с. 81]. В частности, пропаганды экстремистской идеологии, вербовки новых сторонников радикальных движений, запрещенных в Российской Федерации.

Экстремизм как явление интегрируясь в цифровую среду, обладающую сложными программно-техническими особенностями, позволяющими действовать анонимно, все активнее обуславливает запрос общества на обеспечение государством национальной безопасности за счет увеличения эффективности использования превентивных мер административного характера.

Так, эффективное применение мер административной ответственности в данной сфере напрямую зависит от возможности выявления, сбора, фиксации и оценки цифровых данных, которые в последующем могут быть признаны доказательствами в производстве по делам об административных правонарушениях экстремистской направленности. В этой связи особенности вопросов правового регулирования допустимости и законности получения такого рода цифровых фактических данных в цифровой среде приобретает особую актуальность, требуя стремительного, но одновременно качественного развития административного законодательства.

Вместе с тем малозначительная научно-правовая разработанность темы детального законодательного определения понятия цифровых доказательств, их свойств и признаков в производстве по делам об административных правонарушениях обосновывает проблематику настоящего исследования.

Исходя из вышеизложенного предопределяется и цель данного исследования – рассмотрение особенностей правового регулирования по использованию цифровых данных, которые могут быть признаны особой формой доказательств (цифровых доказательств) в производстве по делам об административных правонарушениях. Исследование базируется на применении комплекса общенаучных и специальных методов познания. В частности, в процессе исследования использовались следующие методы: анализ, синтез индукция и дедукция.

Отсутствие законодательно определенного понятия цифровых доказательств в Кодексе Российской Федерации об административных правонарушениях (далее – КоАП РФ) обуславливает в настоящее время появление научной дискуссии, представленной тематической научной литературой и единичной правоприменительной практикой, где складываются разнородные подходы и мнения [5, с. 118].

Собирательно обобщая результаты структурированного анализа, с авторской позиции следует отметить, что в широком смысле цифровое доказательство представляет собой цифровые фактические данные, которые имеют отличительный признак – отсутствие иной формы выражения и воспроизведения, кроме как цифровой. При этом такие данные наряду с традиционными доказательствами имеют значение для установления об-

стоятельств, подлежащих доказыванию по делу об административном правонарушении.

В свою очередь, в контексте производства по делам об административных правонарушениях экстремистской направленности, цифровые фактические данные могут быть определены как информация, содержащая признаки экстремистской деятельности, распространяемая через информационно-телекоммуникационные сети, в том числе Интернет, и используемая для установления факта совершения административного правонарушения, виновности лица и иных обстоятельств, имеющих значение для разрешения дела.

Между тем классификация цифровых доказательств может быть проведена по различным основаниям:

1. По форме представления информации: текстовые (публикации в социальных сетях, комментарии, сообщения в мессенджерах, электронные письма, тексты на сайтах и форумах); аудиовизуальные (видеоролики, аудиозаписи, подкасты) графические (фотографии, рисунки, мемы, демотиваторы).

2. По способу хранения: на стационарных носителях (жесткие диски компьютеров, серверы); на портативных носителях (флеш-накопители, внешние жесткие диски); в облачных хранилищах данных.

3. По степени доступности: общедоступные (публикации в открытых источниках); ограниченного доступа (информация, доступная только определенному кругу лиц); конфиденциальные (персональные данные, или охраняемая законом тайна) [3].

Таким образом, особый программно-технический характер цифровых фактических данных обуславливает необходимость трансформации и совершенствования концептуального осмысления административно-правового регулирования понятия доказательств. И, как следствие этого, административно-правового закрепления особой формы доказательств – цифровых доказательств, имеющих особое значение ввиду массовости и актуальности распространения цифровых технологий, активной синергии по использованию цифровой среды во всех сферах жизни общества. Наряду с четкой классификацией цифровых фактических данных имеет важнейшее практическое значение для определения порядка их сбора, фиксации, исследования и оценки, а также признания их особой формой доказательств в каждом конкретном случае при производстве по делам об административных правонарушениях экстремистской направленности.

Несмотря на тот факт, что порядок сбора, фиксации, исследования и оценки цифровых фактических данных в производстве по делам об административных правонарушениях регламентируется общими положениями КоАП РФ, существуют особенности их оценки.

При оценке необходимо учитывать требования закона, соблюдение прав и свобод человека и гражданина, а также использовать специальные

познания в области цифровых технологий и цифровой среды. Именно поэтому допустимость цифровых доказательств является одним из наиболее сложных и дискуссионных вопросов в данной сфере, образующим ряд проблем для правоприменителя.

К перечню проблем можно отнести нарушение порядка сбора и фиксации цифровых доказательств:

1. Невозможность установления подлинности и достоверности цифровых фактических данных. В частности, если невозможно установить подлинность и достоверность цифровых доказательств, например, из-за отсутствия необходимой информации или повреждения цифрового носителя, они не могут быть использованы в качестве доказательств по делу.

2. Анонимность в сети Интернет затрудняет установление авторства экстремистских материалов и идентификацию личности пользователя, что может являться препятствием для привлечения его к административной ответственности.

3. Фактическое выявление признаков экстремизма в содержании цифровых материалов (например, наличие призывов к насильственным действиям, разжигание ненависти, пропаганда экстремистской идеологии), а также установление связи между цифровыми доказательствами и конкретным лицом или событием.

Подводя общий итог, применение цифровых фактических данных как особой формы доказательств в производстве по делам об административных правонарушениях, в частности экстремистской направленности – достаточно важное направление для обеспечения национальной безопасности в условиях активной цифровизации всех сфер жизнедеятельности. Данный факт обуславливает необходимость дальнейших активных научно-правовых исследований и предложений, как результата такой деятельности по заявленной теме исследования.

Частные предложения по итогам данного исследования заключаются в умозаключении о том, что разрешение образовавшихся правоприменительных проблем – это вопрос не одного дня, а скорее системная и последовательная деятельность в рамках установления правового регулирования, как общих аспектов, таких как – формулирование понятия особой формы доказательств – цифровых доказательств, определение основных признаков и классификации. Исходя из этого, предложен авторский подход к формулированию понятия цифровых доказательств в производстве по делам об административных правонарушениях.

Библиографический список

1. О противодействии экстремистской деятельности : федеральный закон от 25 июля 2002 г. № 114-ФЗ. Доступ из справочно-правовой системы «Гарант.ру».

2. О противодействии терроризму : федеральный закон от 6 марта 2006 г. № 35-ФЗ. Доступ из справочно-правовой системы «Гарант.ру».

3. Остапенко А. А. Виды цифровых доказательств в административном судопроизводстве // StudNent. 2021. № 5.

4. Куликова Я. А. Цифровые технологии в процессе доказывания в производстве по делам об административных правонарушениях // Административное и муниципальное право. 2024. № 6. С. 81–99.

5. Соколов А. Ю. Правовая политика в области использования цифровых технологий в производстве по делам об административных правонарушениях // Вестник СГЮА. 2023. № 1 (150). С. 118–121.

© Терехов М. Г., 2026

УДК 340.1

Тулбаева Д. Т. – доцент кафедры административно-правовых дисциплин Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова (Республика Казахстан, г. Караганда)

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК СОВРЕМЕННАЯ УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ, ПУТИ РЕШЕНИЯ

INFORMATION TERRORISM AS A MODERN THREAT TO NATIONAL SECURITY: PROBLEMS AND SOLUTIONS

Аннотация. В статье рассматривается информационный терроризм как одна из наиболее опасных форм современных угроз в условиях глобализации и цифровизации. Выделяются ключевые проблемы противодействия, предлагаются комплексные пути их решения и анализируются возможные последствия как при эффективной реализации мер, так и при их отсутствии.

Ключевые слова: информационный терроризм, киберинциденты, глобализация, киберугроза.

Abstract. The article examines information terrorism as one of the most dangerous forms of modern threats in the context of globalization and digitalization. The key problems of counteraction are highlighted, comprehensive ways of their solution are proposed, and possible consequences are analyzed both in case of effective implementation of measures and in case of their absence.

Keywords: information terrorism, cyber incidents, globalization, cyber threat.