



DOI: <https://doi.org/10.15688/lc.jvolsu.2022.4.9>

UDC 342.53
LBC 67.0



Submitted: 05.08.2022
Accepted: 15.09.2022

LEGAL FORMS OF ENSURING INFORMATION SECURITY ON THE INTERNET

Gennady G. Egorov

Volzhsky Branch of Volgograd State University, Volzhsky, Russian Federation

Introduction: the development of modern digital networks is associated with the introduction into circulation of data with increased social danger and, as a consequence, limited to civilian use in the Russian Federation. Unlike the authorities, this type of information is not recognized by society as dangerous, but generates aspirations of certain categories of citizens to possess such information, to disseminate it, to introduce it into illegal civil circulation. The scientific community, recognizing this problem, has been striving to neutralize the consequences in this area for a long time. The **purpose** of the work is to conduct a scientific analysis of the existing legal forms of ensuring information accessibility, to determine the effectiveness of modern legal and organizational mechanisms to ensure civil interests in this area. Using the methods of scientific cognition, primarily the method of system analysis, it is established that the complexity of the highlighted problem involves the use of both law-making and law-realization approaches to identify the violations of arrangements for using electronic information in the violation of applicable law. **Results:** the considered approaches and legal mechanisms for ensuring information security in the Internet environment will justify the need to introduce the organizational and legal methods to improve the current legislation and law enforcement practice in the country and propose a number of measures for their eliminating. **Conclusions:** it is necessary 1) to adapt the existing judicial system related to the restriction of the circulation of information on the Internet to modern realities in the technical and legal spheres; 2) to change not only the procedure for recognizing information as prohibited, but also to introduce additional forms of responsibility for its placement, in particular, the imposition of administrative forms of sanctions not only on the creator of illegal content, but also on technical intermediaries (providers, telecom operators, domain name grantors), which can be presented in the form of imposing technical prohibitions on the placement of information on the Internet; 3) to increase the number of persons subject to legal liability (administrative or criminal) for the violation of information security in the Russian Federation.

Key words: information security, electronic user rights, responsibility for violations of information security on the Internet, legal gaps in the regulation of the status of networks, digital data protection.

Citation. Egorov G.G. Legal Forms of Ensuring Information Security on the Internet. *Legal Concept = Pravovaya paradigma*, 2022, vol. 21, no. 4, pp. 70-76. (in Russian). DOI: <https://doi.org/10.15688/lc.jvolsu.2022.4.9>

УДК 342.53
ББК 67.0

Дата поступления статьи: 05.08.2022
Дата принятия статьи: 15.09.2022

ПРАВОВЫЕ ФОРМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Геннадий Геннадьевич Егоров

Волжский филиал Волгоградского государственного университета, г. Волжский, Российская Федерация

Введение: развитие современных цифровых сетей связано с введением в оборот данных, обладающих повышенной социальной опасностью и, как следствие, ограниченных в гражданском использовании в РФ. В отличие от власти данный вид информации обществом не признается опасным, но порождает стремления отдельных категорий граждан к обладанию такими сведениями, их распространению, введению в незаконный гражданский оборот. Научное сообщество, признавая настоящую проблему, уже длительное время стремится нивелировать последствия в данной сфере. **Целью работы** является проведение научного анализа существующих правовых форм обеспечения информационной доступности, определение эффективности

современных правовых и организационных механизмов по обеспечению гражданских интересов в данной сфере. **С помощью методов** научного познания, прежде всего метода системного анализа, установлено, что сложность выделенной проблемы предполагает использование как правотворческого, так и правореализационного подходов по выявлению нарушений действующих норм права в порядке использования электронной информации. **Результаты:** рассматриваемые подходы и правовые механизмы обеспечения информационной безопасности в интернет-среде позволят обосновать необходимость введения организационно-правовых методик по совершенствованию действующего законодательства и правоприменительной практики в стране и предложить ряд мер по их устранению. **Выводы:** необходимо 1) адаптировать существующую судебную систему, связанную с ограничением оборота информации в сети Интернет, к современным реалиям в технической и правовой сферах; 2) изменить не только саму процедуру признания информации запрещенной, но и ввести дополнительные формы ответственности за ее размещение, в частности наложить административные формы санкций на создателя незаконного контента и на технических посредников (провайдеров, операторов связи, арендодателей доменных имен), которые могут быть представлены в виде технических запретов на размещение информации в пределах сети Интернет; 3) увеличить круг лиц, подлежащих юридической ответственности (административной или уголовной) за нарушение информационной безопасности в РФ.

Ключевые слова: информационная безопасность, электронные права пользователя, ответственность за нарушения информационной безопасности в сети Интернет, правовые пробелы регламентации статуса сетей, защита цифровых данных.

Цитирование. Егоров Г. Г. Правовые формы обеспечения информационной безопасности в сети Интернет // Legal Concept = Правовая парадигма. – 2022. – Т. 21, № 4. – С. 70–76. – DOI: <https://doi.org/10.15688/lc.jvolsu.2022.4.9>

Введение

Сеть Интернет является одной из доступных информационно-телекоммуникационных сетей международного характера, доступ к таким системам предоставляет неопределенному кругу лиц возможность взаимодействовать с ними и получать жизненно необходимые им сведения. Информационное взаимодействие при всем своем разнообразии может нести как положительные, так и отрицательные эффекты и оказывать воздействие на граждан, общество и государство [8, с. 3–9].

Информация, получаемая из таких сетей, может оказать негативное воздействие на разнообразные сферы правоотношений, сформировать непосредственную угрозу для личности, экономических отношений, безопасности государства и повлечь возникновение юридических последствий различного характера. Статус таких «последствий» напрямую подтверждается актами органов власти, в частности судебными предписаниями, которые признают за той или иной информацией, в результате административного разбирательства, ограниченный режим по размещению в сети Интернет и в национальных доменах, доступных для свободного использования на территории Российской Федерации [4, с. 215–218].

Правовые формы обеспечения безопасности информации в среде Интернет

На практике такого рода запросы, направляемые в суд, как правило, поступают со стороны органов прокуратуры, активная позиция которых позволяет в сети Интернет на постоянной основе выявлять и ограничивать доступ к разнообразной, опасной информации, размещаемой в интернет-пространстве на разнообразных сайтах через объявления и самостоятельные электронные страницы [9, с. 48–49].

Ряд ученых неоднократно отмечали, что такого рода процедура, связанная с ограничением доступа к интернет-ресурсам, на практике является неэффективной, так как предполагает соблюдение ряда обязательных правил [10, с. 20–23]: 1) выявление административного ответчика, оформление и направление административного иска / заявления в судебные органы, непосредственное участие в судебном заседании, которое, как правило, может быть перенесено по различным причинам (в частности неуведомления сторон судебного судопроизводства), ожидание судебного решения, в части вступления его в законную силу и обращение к непосредственному исполне-

нию; 2) соблюдение всех данных правил на практике формирует ситуацию, при которой блокировка непосредственно опасных данных на веб-страницах с незаконной информацией может занимать от 6 до 8 месяцев; за данный промежуток времени в интернет-среде, как правило, появляются множество иных страниц аналогичного либо иного, но связанного с первоначальной незаконной информацией характера.

Федеральный закон от 27 июля 2006 г. № 149 ФЗ «Об информации, информационных технологиях и о защите информации» в ч. 6 ст. 10 определяет, что к запрещенной к свободному обмену информации в Российской Федерации относятся сведения, направленные прежде всего на пропаганду военных действий, разжигание национальной / расовой или религиозной ненависти и вражды, и иная информация, распространение которой влечет за собой наступление уголовной либо административной ответственности [4, с. 215–218].

Перечень так называемой незаконной информации на практике позволил сгруппировать информацию в следующие блоки [2, с. 17–19]:

1. Первый блок – это информация, направленная на фальсификацию / подмену функциональной деятельности органов исполнительной власти либо рекламирующая возможность представления государственных услуг за неутвержденную федеральную плату. Классическим примером является попытка фальсификации сведений из ЕГРН, который напрямую использует государственную символику и регистрационные данные кадастрового учета, картографические отметки, нацеленная на создание у обычного пользователя необходимости по оплате такого рода информации в негосударственном порядке.

2. Второй блок – это данные, напрямую посягающие на единую централизованную государственную систему денежного и валютного взаимодействия в стране. К ним можно отнести сведения о криптовалютах, выступающих в качестве виртуальных средств платежа и накоплений (при этом само государство не обеспечивает реальную стоимость данных псевдоэмитентов на подконтрольной государственной территории); сайты, связанные с попыткой обучения граждан наиболее эффективному инвестированию и использова-

нию данной криптовалюты, в частности биткоинов, а также системы блокчейн по ним; платежные системы различного рода, направленные на формирование электронного взаимодействия без вовлечения аккредитованного банковского представителя, в частности такие системы платежа, как Tagilcoin, Bitcoin, Ethereum [7, с. 178]; системы / способы / схемы обналичивания денежных средств не только с помощью существующей в Российской Федерации банковской системы.

3. Третий блок – это сведения о реализации товаров / предоставлении услуг, прямо запрещенных к свободному обороту на территории страны, а также те данные, которые связаны с нарушением государственного контроля и анализа по лицензионным товарам / услугам. Сюда относятся: реализация товаров, свободная продажа которых прямо запрещена на территории Российской Федерации либо имеет ряд существенных ограничений, в частности алкогольная продукция, табачные изделия, либо их аналоги (курительные смеси для «вайперов») [3, с. 140–141], оборот этилированного бензина, изделий из драгоценных металлов / камней и их аналогов, агрохимикатов, донорских органов, огнестрельного и приравненного к нему боевого оружия (как огнестрельного, так и холодного вида), лекарственных медицинских средств рецептурного вида, систем, препятствующих видеофиксации государственных регистрационных знаков на транспортных средствах, причем во всем их разнообразии, ценных видов диких животных, а также биологических ресурсов, занесенных в Красную книгу или же непосредственно охраняемых на основе международных договоров, заключенных с участием Российской Федерации; продажа поддельных документов, к примеру дипломов об образовании, переаттестации, различного рода медицинских справок о прохождении обследования, судебных удостоверений различного характера (сотрудников правоохранительных органов), водительских прав и т. д.; сведения о предоставлении различного рода услуг, в том числе интимного характера.

4. Четвертый блок – информация о разнообразных способах, а также методах совершения незаконных действий, за которыми предусмотрено наступление как уголовной так и

административных форм ответственности. К этому блоку относятся: технология производства / изготовления взрывчатых веществ, а также их аналогов, способы их использования, камуфляжные схемы взрывчатых веществ, либо их муляжи, модификационные формы подмены данных средств и т. д.; разнообразные, зачастую незаконные способы уклонения от воинской обязанности либо же от выплаты законно определенных налогов и сборов; способы изготовления, дозировки, употребление, оборот, как правило, незаконных, наркотических средств, а также веществ, содержащих наркотические смеси. Особо актуальной в последнее время становится информация о так называемых фиктивных браках, как одной из формы легализации статуса иностранных граждан, находящихся на территории страны [5, с. 153–163].

5. Пятый блок – информация, использование которой может причинить вред здоровью и полноценному развитию несовершеннолетних лиц. Сюда относят информацию, призванную создать у ребенка неосознанное стремление к самоубийству, проявление немотивированной агрессии, незаконному применению наркотических, психотропных веществ либо их прекурсоров; желание приобщиться к незаконным азартным играм, добровольно быть вовлеченным в проституцию, заняться бродяжничеством либо попрошайничеством, а равно и иной деятельностью, прямо осуждаемой обществом либо явно запрещенной на территории страны; информация, обосновывающая или оправдывающая формы применения насилия, жестокости либо иных неправомерных форм деятельности; данные, призванные изменить восприятие детей по отношению к семейным ценностям либо же прямо пропагандирующие нетрадиционные формы отношений, что особо актуально в рамках Европейского сообщества, а также создать предпосылки по дискредитации статуса родителей и иных членов семьи; информация, содержащая как нецензурную брань, так и ее завуалированные виды, в том числе предполагающая прямую явную либо скрытую порнографическую подоплеку; сведения о незаконной продаже курительных смесей, синтетических препаратов, которые могут выступать в качестве форм наркотических веществ [1, с. 104–118].

6. Шестой блок – информация, которая может быть использована в качестве способа / средств причинения вреда гражданам. Это сведения, включающие в себя персональные данные лиц, элементы которых представляют возможность как модифицировать данную информацию, так и непосредственно с помощью сайтов анонимизер получать доступ к ресурсам, напрямую запрещенным к обороту на территории страны.

Выделенные блоки не являются исчерпывающими, развитие сети Интернет практически ежедневно позволяет выявлять новые виды данных, которые по признакам являются противоправными для того или иного государства, и сведения которых предполагают незаконный интернет-обмен, и, несмотря на мониторинг, как правило, не могут быть проанализированы в полном объеме.

Научно-правовые проблемы определения санкций за распространения информации запрещенного характера

В научном сообществе [11, с. 62–65] уже длительное время существуют ряд критических замечаний о текущих формах работы с запрещенной к распространению в стране информацией, а также о роли судебного порядка в наложении ограничений на оборот данных сведений. В частности, А. Жаров предлагает передать большой круг полномочий в данной сфере Федеральным органам исполнительной власти, к примеру, Роскомнадзору либо же Министерству юстиции. М. Али также определяет необходимость обеспечить защиту прав владельцев сайтов / доменов через введение систем мониторинга судебных процессов, связанных с обеспечением цифровых прав [1, с. 104–118]. С. Бывальцева и Н. Макаров отмечают роль особого производства по нормам ГПК РФ. Е. Царегорцева рекомендует введение процедуры рассмотрения данной категории дел в досудебном порядке, с наделением уполномоченных представителей органов прокуратуры соответствующими статусами, хотя и отмечают, что подавляющее большинство данной категории дел могут быть рассмотрены только через суд [11, с. 62–65].

Данные подходы являются следствием внесудебного порядка ограничения доступа к информации, который был утвержден постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101, напрямую определяющим перечень индикаторов сайтов, содержащих информационные ресурсы, ограниченные по доступу в пределах Российской Федерации.

Согласно нормам действующего законодательства, принять решение об ограничении доступа к запрещенной либо ограниченной информации вправе как Министерство внутренних дел Российской Федерации, так и ряд Федеральных служб страны [4, с. 215–218].

Анализ действующей практики позволяет сделать вывод о необходимости расширения круга полномочий федеральных органов власти как по выявлению, так и наложению запрета на распространение в пределах Российской Федерации доступа к информации, включенной либо предполагающей включение в перечень запрещенной для нашего государства.

Классическим примером такого ограничения выступает деятельность Федеральной службы по надзору в сфере здравоохранения, которая обладает правом наложения запретов в отношении интернет-ресурсов, доменных имен либо же страницах, размещенных в сети Интернет в случае, если информация, имеющаяся в пределах данного ресурса, в том числе дистанционного, содержит данные о различного рода лекарственных препаратах (либо формах их применения), реализуемых через розничную торговлю с рецептным контролем, включенных в перечень запрещенных для Российской Федерации либо их распространение предполагает необходимость наличия определенного рода лицензионных разрешений на их оборот в пределах Российской Федерации (также лицензионные разрешения предполагают право и на фармацевтическую деятельность в пределах Российской Федерации) [6, с. 34–36].

Следует согласиться с точкой зрения [5, с. 153–163], что нужно закрепить за Федеральной службой по надзору права на блокировку ресурсов в сети Интернет, содержащих информацию о медицинских справках различного вида, что могут быть получены без ме-

дицинского обследования либо же сведений и которые прямо пропагандируют реализацию аборт в рамках деятельности медицинских учреждений, что прямо нарушает предписания ст. 56 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

При этом Центробанк Российской Федерации также может быть уполномочен контролировать оборот виртуальных сред в сети Интернет, а равно выявлять отношения, которые связаны с оборотом и нарушают действующие нормы права Российской Федерации.

Выводы

Подводя итоги проведенного анализа, можно сделать вывод, что существующая судебная система, связанная с ограничением оборотом информации в сети Интернет, является неэффективной в скорости реагирования на выявленные нарушения и не соответствует динамики развития современного общества. Каждая удаляемая или ограничиваемая по доступу страничка, как правило, порождает комплекс данных, содержащих незаконные сведения, но не ограниченных по информационному взаимодействию в пределах Интернета, это способствует тому, правонарушители могут использовать методику по распространению незаконных сведений без учета возможности блокировки со стороны органов власти.

Отмеченное также позволяет сделать вывод, что сформировалась практическая необходимость не только изменения самой процедуры признания информации запрещенной, но и введения дополнительных мер ответственности за ее размещение, в частности наложения административных форм санкций на создателя незаконного контента и технических посредников (провайдеров, операторов связи, арендодателей доменных имен), которые могут быть представлены в виде наложения технических запретов на размещение информации в пределах сети Интернет.

По своей сути наложение такого рода ограничений на технических посредников, согласно позиции Европейского суда по правам человека, определенной в соответствии с постановлением от 2 февраля 2016 г. Дело «Вен-

герская ассоциация провайдеров интернет-контента и компаний Index.hu Zrt (Magyar Tartalomszolgáltatok Egyesulete and Index.hu Zrt) против Венгрии», должно быть возможно только в случае, если на момент создания интернет-контента информация уже была признана в качестве ограниченной по обороту или же прямо запрещена для размещения в пределах РФ, о чем указывается в постановлении Правительства РФ от 26 октября 2012 г. № 1101.

СПИСОК ЛИТЕРАТУРЫ

1. Али, М. З. Ограничение доступа к информационным ресурсам в сети Интернет (практические проблемы признания информации запрещенной к распространению) / М. З. Али // Право в сфере Интернета. – М. : Статут. – 2018. – С. 104–118.

2. Бывальцева, С. Г. Особенности рассмотрения заявления прокурора о признании информации, распространяемой посредством сети «Интернет», запрещенной к распространению / С. Г. Бывальцева, Н. Г. Макарова // Законность. – 2018. – № 10. – С. 17–19.

3. Евсютин, О. О. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» / О. О. Евсютин, А. С. Кокурина, Р. В. Мещеряков // Компьютерная оптика. – 2019. – Т. 43, № 1. – С. 137–154.

4. Егоров, Г. Г. Организационно-правовое регламентирование консультации граждан в условиях развития современных цифровых систем / Г. Г. Егоров, Т. В. Деркачева, А. Е. Ращевская // Проблемы устойчивого развития и эколого-экономической безопасности регионов : материалы XVI Междунар. науч.-практ. конф., г. Волжский, 25–26 ноября 2021 г. – Волгоград : Сфера, 2022. – С. 215–218.

5. Егоров, Г. Г. Роль цифровых технологий в оптимизации гражданского судопроизводства / Г. Г. Егоров, Л. Е. Стрилец // Экология, экономика, право: взгляд в будущее : сб. ст. по материалам науч.-практ. конф., проходившей в рамках Недели науки (апрель, 2018 г.). – Волгоград : Изд-во ВолГУ, 2018. – С. 153–163.

6. Жаров, А. В. Судебный порядок признания информации, размещенной в сети «Интернет», запрещенной к распространению / А. В. Жаров // Законность. – 2018. – № 9. – С. 34–36.

7. Матыцин, Д. Е. Интернет-пространство и искусственный интеллект: проблемы предпринимательской деятельности и правоприменения / Д. Е. Матыцин // Legal Concept = Правовая парадигма. – 2022. – Т. 21, № 1. – С. 178–185. – DOI: 10.15688/lc.jvolsu.2022.1.26

8. Паламарчук, А. В. Прокурорский надзор за исполнением законодательства в сфере противодействия правонарушениям в сети Интернет / А. В. Паламарчук // Законность. – 2016. – № 12. – С. 3–9.

9. Хотулев, А. С. Цифровой разрыв как глобальное явление и вызов для России / А. С. Хотулев // Россия и современный мир. – 2022. – № 1 (114). – С. 45–62.

10. Христинич, И. В. Информационная безопасность в сети Интернет / И. В. Христинич // Законность. – 2022. – Апр. (№ 4). – С. 20–23.

11. Царегородцева, Е. А. К вопросу о порядке рассмотрения дел о признании информации запрещенной к распространению на территории Российской Федерации / Е. А. Царегородцева // Административное право и процесс. – 2020. – № 1. – С. 62–65.

REFERENCES

1. Ali M.Z. Ogranichenie dostupa k informacionnym resursam v seti Internet (prakticheskie problemy priznaniya informacii zapreshchennoj k rasprostranenyu) [Restricting Access to Information Resources on the Internet (Practical Problems of Recognizing Information Prohibited for Distribution)]. *Pravo v sfere Interneta: sb. st.* [Law in the Field of the Internet. Collection of Articles], Moscow, Statut Publ., 2018, pp. 104-118.

2. Byvalceva S.G., Makarova N.G. Osobennosti rassmotreniya zayavleniya prokurora o priznanii informacii, rasprostranyaemoj posredstvom seti “Internet”, zapreshchyonnoj k rasprostranenyu [Peculiarities of Consideration of the Prosecutor’s Application on the Recognition of Information Disseminated via the Internet as Prohibited for Distribution]. *Zakonnost*, 2018, no.10, pp. 17-19.

3. Evsyutin O.O., Kokurina A.S., Meshcheryakov R.V. Obzor metodov vstraivaniya informacii v cifrovye obyekty dlya obespecheniya bezopasnosti v “internete veshchej” [Overview of Methods for Embedding Information in Digital Objects to Ensure Security in the “Internet of Things”]. *Kompyuternaya optika* [Computer Optics], 2019, vol. 43, no. 1, pp. 137-154.

4. Egorov G.G., Derkacheva T.V., Rashchevskaya A.E. Organizacionno-pravovoe reglamentirovanie konsultacii grazhdan v usloviyah razvitiya sovremennyh cifrovyyh sistem [Organizational and Legal Regulation of Citizens’ Consultation in the Context of the Development of Modern Digital Systems]. *Problemy ustojchivogo razvitiya i ekologo-ekonomicheskoy bezopasnosti regionov: materialy XVI Mezhdunar. nauch.-prakt. konf., g. Volzhskij, 25–26 noyabrya 2021 g.* [Problems of Sustainable

Development and Environmental and Economic Security of Regions. Materials of the 16th International Scientific and Practical Conference, Volzhsky, November 25–26, 2021], Volgograd, Sfera Publ., 2022, pp. 215-218.

5. Egorov G.G., Strilec L.E. Rol cifrovyyh tekhnologiy v optimizacii grazhdanskogo sudoproizvodstva [The Role of Digital Technologies in Optimizing Civil Proceedings]. *Ekologiya, ekonomika, pravo: vzglyad v budushchee: sb. st. po materialam nauch.-prakt. konf., prohodivshej v ramkah Nedeli nauki (aprel, 2018 g.)* [Ecology, Economics, and Law: Look Into the Future. Collection of Articles Based on the Materials of the Scientific and Practical Conference Held as a Part of the Science Week (April, 2018)], Volgograd, Izd-vo VolGU, 2018, pp. 153-163.

6. Zharov A.V. Sudebnyj poryadok priznaniya informacii, razmeshchyonnoj v seti “Internet”, zapreshchyonnoj k rasprostraneniyu [Judicial Procedure for Recognizing Information Posted on the Internet as Prohibited for Distribution]. *Zakonnost*, 2018, no. 9, pp. 34-36.

7. Matytsin D. E. Internet-prostranstvo i iskusstvennyj intellekt: problemy predprinimatelskoj deyatel'nosti i pravoprimeneniya [Internet Space and

Artificial Intelligence: Problems of Entrepreneurship and Law Enforcement]. *Pravovaya paradigma* [Legal Concept], 2022, vol. 21, no. 1, pp. 178-185. DOI: 10.15688/lc.jvolsu.2022.1.26

8. Palamarchuk A.V. Prokurorskiy nadzor za ispolneniem zakonodatel'stva v sfere protivodejstviya pravonarusheniyam v seti Internet [Prosecutorial Supervision Over the Implementation of Legislation in the Field of Counteraction to Offenses on the Internet]. *Zakonnost*, 2016, no. 12, pp. 3-9.

9. Hotulev A.S. Cifrovoy razryv kak globalnoe yavlenie i vyzov dlya Rossii [Digital Divide as a Global Phenomenon and Challenge for Russia]. *Rossiya i sovremennyy mir* [Russia and the Modern World], 2022, no. 1 (114), pp. 45-62.

10. Hristinich I.V. Informacionnaya bezopasnost v seti Internet [Information Security on the Internet]. *Zakonnost*, 2022, Apr. (No. 4), pp. 20-23.

11. Caregorodceva E.A. K voprosu o poryadke rassmotreniya del o priznanii informacii zapreshchennoj k rasprostraneniyu na territorii Rossijskoj Federacii [On the Issue of the Procedure for Considering Cases on the Recognition of Information Prohibited for Distribution on the Territory of the Russian Federation]. *Administrativnoe pravo i process* [Administrative Law and Process], 2020, no. 1, pp. 62-65.

Information About the Author

Gennady G. Egorov, Candidate of Sciences (Jurisprudence), Associate Professor, Department of Jurisprudence, Volzhsky Branch of Volgograd State University, 40 let Pobedy St, 11, 404133 Volzhsky, Russian Federation, egorov@vgi.volsu.ru, <https://orcid.org/0000-0002-5969-1171>

Информация об авторе

Геннадий Геннадьевич Егоров, кандидат юридических наук, доцент кафедры юриспруденции, Волжский филиал Волгоградского государственного университета, ул. 40 лет Победы, 11, 404133 г. Волжский, Российская Федерация, egorov@vgi.volsu.ru, <https://orcid.org/0000-0002-5969-1171>