ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ТРАНСПОРТНОЙ ДЕЯТЕЛЬНОСТИ И ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

УДК 004.056.5(075.8)

© Чеботарев Владимир Евгеньевич
— кандидат экономических наук, доцент,
доцент кафедры «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта (МИИТ)

Вопросы обеспечения безопасности информационных систем

Аннотация. Проблема безопасности информационных систем и, следовательно, информации как ключевого ресурса в современном информационном обществе — это то, с чем так или иначе сталкиваются все участники информационного взаимодействия во всех секторах ИКТ-среды. В статье анализируются научные и законодательные подходы к определению понятия и сущности информационной системы, типологии информационных систем, в результате чего предлагается авторский подход к определению исследуемой дефиниции, поднимается проблема «доверия в ИКТ-среде». Автор акцентирует внимание на неопределенности правового режима информационных систем, что напрямую оказывает отрицательное влияние на эффективность управления коммуникациями в информационных системах и защиту их от злоумышленников.

Ключевые слова: информационная система; безопасность; оператор информационной системы; типология информационных систем.

© Vladimir Ev. Chebotarev
— Candidate of Economical Sciences, docent, associate professor of the department “Administrative law, ecological law, information law” of the Law Institute of the Russian University of Transport

Issues of information systems’ security enforcement

Abstract. The problem of information systems’ security and, consequently, information as a key resource in the modern information society is something that all participants of information interaction in all ICT environment sectors

face in one way or another. The current paper has analyzed the scientific and legislative approaches to the definition of the concept and essence of the information system, the typology of information systems. As a result, there has been proposed the author's approach to definition of the investigated object, there has been identified the problem of "trust in the ICT environment". The author has focused on the uncertainty of the legal regime of information systems, which directly has a negative impact on the efficiency of communication management in information systems and their protection from criminals.

Keywords: information system; security; information system operator; typology of information systems.

Информационные системы — основа современной ИКТ-среды

Информационные системы по определению, выводимому из содержания Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», представляют собой совокупность локальных и распределенных массивов информации в форме «данные» (совокупность содержащейся в базах данных информации), информационных технологий и технических средств (средств ИКТ), обеспечивающих обработку этих «данных».

Кроме определения собственно самой информационной системы, в ст. 2 указанного Закона содержится определение оператора информационной системы, под которым понимается гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. В связи с таким определением оператора, как субъекта правоотношений, возникают следующие вопросы.

1. Речь идет только о гражданах России или термин «гражданин» используется в более широком смысле — гражданах разных государств?

2. Как быть, если информационная система создана и эксплуатируется, например, человеком без гражданства, живущим за рубежом? Ведь такая информационная система вполне может быть представлена посредством сети Интернет и использоваться в Российской Федерации.

3. При перечислении операторов системы указывается юридическое лицо. Между тем в ГК РФ одним из признаков юридического лица является наличие государственной регистрации в Российской Федерации. Как быть с неформальными организациями и объединениями граждан? И с зарубежными организациями, не имеющими государственную регистрацию в России, которые посредством сети Интернет предлагают разные виды информационных систем, используемых в том числе в российском сегменте мирового информационного пространства?

Попытки обязать владельцев социальных сетей открывать офисы в России предпринимаются, но это, как правило, касается только крупных и

популярных сетей и систем. В то время как граждане России активно используют сотни информационных систем с разным уровнем прозрачности работы и разной политикой использования данных пользователей.

Исходя из законодательного определения информационной системы и операторов, приведенного выше, следует, что значительная часть подпадающих под это определение информационных систем операторов (с точки зрения законодательства РФ) не имеют, а значит, появляется масштабная правовая «лакуна». При этом согласно Доктрине информационной безопасности Российской Федерации (утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646) операторы информационных систем являются участниками общей системы обеспечения информационной безопасности. Это четко указано в разделе 5 Доктрины «Организационные основы обеспечения информационной безопасности».

Отсюда, с авторской точки зрения, определение операторов информационных систем в профильном Федеральном законе «Об информации, информационных технологиях и о защите и информации» требует более тщательной проработки и уточнения в том случае, если само определение информационных систем относится ко всем системам, подходящим под это определение, а не к определенному реестру информационных систем. Аналогичные очевидные пробелы, например, существуют в регулировании средств массовой информации в соответствующем законе, в котором речь идет исключительно о средствах массовой информации, зарегистрированных (или обязанных это сделать в силу имеющихся характеристик) в Роскомнадзоре. Хотя сегодня технически средствами массовой информации являются многие интернет-ресурсы, работающие на основе информационных систем (например, новостные агрегаторы).

В контексте вышесказанного необходимо также упомянуть, что существует объективная, фактическая невозможность выполнения нормы закона к операторам информационных систем об обязательном нахождении на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Также сомнительна возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней, поскольку необходимо иметь механизм фиксации информации и документирования ее наличия. Возможно, по такому принципу, как это делает Информрегистр по отношению к электронным средствам массовой информации. Но это требует огромных ресурсов и маловероятно в достижении.

Одно из точных, на взгляд автора, определений было дано исследователями в одном из учебных пособий 2010 г.: «Информационная система — это система, реализующая информационную модель предметной области, чаще всего какой-либо области человеческой деятельности, обеспечивающая получение (ввод или сбор), хранение, поиск, передачу и обработку (преобразование) информации» [2, стр. 17].

При этом определение информационных систем можно расширить и сформулировать следующим образом: «Информационная система представляет собой совокупность информации, технических, программных, технологических и иных средств, а также математических моделей, методов и специалистов, объединенных структурно и функционально для обеспечения одного или нескольких видов информационных процессов и в результате — предоставления информационных возможностей для пользователей».

Отсутствие в легальных определениях информационной системы и ее операторов приведенных выше характеристик приводит к неопределенности правового режима информационных систем.

Чтобы обеспечить высокий уровень безопасности информации, многие операторы сегодня используют непрерывный, структурированный и систематический подход к обеспечению безопасности. Управление коммуникациями в информационных системах и защита их от злоумышленников эффективна только при условии установления жесткой политики безопасности процессов, процедур и всей архитектуры информационной безопасности. Однако несмотря на это угрозы безопасности, инциденты, уязвимости и риски все еще являются критическими, и последствия этого мы наблюдаем довольно часто.

Одна из основных причин этой проблемы — недостаточно четкое понимание операторами ключевых факторов, влияющих на безопасность информационных систем. Выявление и анализ этих ключевых факторов может изменить ситуацию в лучшую сторону.

К началу нового тысячелетия характер атак на информационные системы трансформировались из использования «троянских коней» и вирусов в «искусные» атаки, такие как: распределенная атака типа «отказ в обслуживании», встроенный вредоносный код в сообщениях электронной почты, иные формы вредоносного программного обеспечения, используемого для вымогательства.

Новая эпоха характеризуется тем, что атаки больше не являются результатом желания злоумышленников продемонстрировать свои умения в виде «сетевого хулиганства». Атаки, прежде всего, нацелены на получение финансовой или иной выгоды их инициаторов.

В результате этой трансформации стало наблюдаться изменение в мерах и подходах к безопасности информационных систем: от чисто технических мер защиты, которые оказались недостаточными, к превентивному стратегическому подходу, включающему различные

элементы информационной безопасности, в частности такие, которые относятся к организационному или социологическому аспекту, поскольку даже лучшие технологии безопасности не могут остановить атаку, основанную, например, на социальной инженерии.

Одна из первых и наиболее серьезных проблем, с которыми сталкиваются организаторы безопасности информационных систем, заключается в том, чтобы успешно сбалансировать необходимость защиты информационных активов, с одной стороны, и обеспечения оперативных операций, с другой, потому что чрезмерно строгая защита может привести к снижению производительности процессов, связанных с бизнесом, в то время как слабый контроль может создать неприемлемые риски для информационных активов.

Современный подход к информационной безопасности требует, чтобы эффективная стратегия информационной безопасности была сбалансированной и включала все элементы защиты информационных систем.

Подходы к типологии информационных систем

Сегодня любой сектор экономики включает в свои механизмы функционирования накопление, обработку, хранение и интерпретацию данных, собираемых от клиентов, дружественных компаний и конкурентов, а также данных, связанных с государственным регулированием данного сектора экономики. Таким образом, любая информационная система включает в себя информацию, содержащую коммерческую, банковскую, налоговую и другие виды тайн, а также персональные данные клиентов. Эти тайны нуждаются в эффективных методах контроля их хранения для правового обеспечения защиты этих тайн.

Например, корпоративные системы *ERP* (*Enterprise Resource Planning*) включают блоки *CRM* (*Customer Relationship Management*) — управление взаимоотношениями с клиентами, а также управление закупками, управление запасами, кадрами, бухгалтерия и другие интегрированные системы по управлению бизнес-процессами, включая администрирование и менеджмент. Как правило, сегодня ни одно предприятие малого, среднего или крупного бизнеса не обходится без этих систем. Все элементы представляют собой комплекс данных, критически важных для успешного функционирования предприятия, его полноценной конкурентоспособности. Утечки данных или нарушение работоспособности этих систем могут повлиять на очень широкий круг лиц — клиентов, работников, предприятий-партнеров и др. Современные корпоративные информационные системы имеют блоки прогнозного характера, моделирующие процессы с учетом исходных данных. Изменение таких исходных данных может повлиять на выбор стратегии предприятия на рынке и итоговую ее судьбу. Поэтому правовой режим

защиты безопасности информационных систем представляется крайне необходимым в современных условиях.

Триггером к интенсивному развитию информационных систем в области образования и науки послужила ситуация с пандемией и необходимость выполнения карантинных мер противодействия распространению коронавируса. Личные данные современного исследователя, его коммуникационная и исследовательская активность содержатся, например, в популярной сегодня информационной системе *ResearchGate*, которая имеет некоторые характеристики, сходные с характеристиками систем социальных сетей, но с помощью инструментов моделирования и эффективного взаимодействия предлагает создавать исследовательские группы, лаборатории из исследователей разных стран вне зависимости от их местоположения, с последующим формированием научных книг и продвижением их среди научного сообщества.

Такие системы, как *ResearchGate*, содержат массивные объемы данных пользователей, переписки, научных разработок и интеграционных возможностей с иными информационными системами, такими как *ORCID, Web of science, Scopus, Crossref, Ulrichsweb, Proquest, ErihPlus, IEEE, Ebsco, Doaj, Google Scholar Citations* и др. Компании *Clarivate Analytics, Elsevier* и *Springer* сегодня являются крупнейшими разработчиками и операторами информационных систем в области научной кооперации и наукометрии. Они предлагают целую линейку соответствующих ИС-продуктов, охватывающих все процессы в современной научной или научно-образовательной организации, а также возможности для каждого исследователя в отдельности.

Крупнейшие издательства, такие как *IntechOpen*, активно используют эти системы для объединения авторов в состав творческих коллективов для разработки заданных научных тем. Возможность интеграции разных систем подразумевает обмен информацией, в том числе и личной информацией пользователей. При этом инфраструктура такой комплексной мегасистемы может находиться на территории разных государств, а информационные процессы могут проходить в разных юрисдикциях. В этом случае правовое регулирование может быть эффективным только при условии общих международных подходов и международных актов.

Сегодня, благодаря карантинным ограничениям, интенсивно развиваются информационные системы, позволяющие использовать технологии *e-Learning*, и получили распространение в России такие системы, как *Microsoft Teams, Zoom, Google Class* и др. Большинство таких систем являются разработками США, и ключевые операторы, и серверы этих систем также физически находятся в США. Но внутри, например, разработки от компании *Microsoft*, также встроена организация всего учебного процесса, включая личные данные студентов и преподавателей и

их корпоративную переписку, задачи, мероприятия, функцию управления проектами.

Справочные правовые информационные системы также имеют наиважнейшее значение, поскольку сегодня являются основным источником сведений об изменяющемся законодательстве, о судебной практике и др. Надежность, бесперебойность этих систем и достоверность информации, в них размещенной, является элементом информационной безопасности для огромного количества субъектов-пользователей. Активно продолжают развиваться новостные агрегаторы, характеристике которых посвящена одна из работ автора [4, стр. 317—143].

Также популярные сегодня поисковые информационные системы, такие как *Google, Yahoo, Yandex* и др., активно используются десятками миллионов российских граждан. При авторизированном использовании этих систем или наличии постоянного *IP*-адреса системы в постоянном режиме собирают информацию о пользователях, их поведении, поисковых запросах, интересах. Эта информация моментально анализируется, интерпретируется и используется соответствующими информационными системами в рамках, например, комплекса маркетинговых коммуникаций и не только. Процесс сегментирования рынков сегодня осуществляется этими системами, содержащими огромные массивы подробной информации о каждом пользователе, что дает беспрецедентные возможности по воздействию на потребительские аудитории. Современные технологии моделирования позволяют составить довольно точный прогноз поведения пользователей при наступлении разных условий. Результаты работы таких систем могут применяться в формировании общественного мнения, убеждений, взглядов, политической повестки, социальных предпочтений.

Такие возможности будут давать «цифровым гигантам», имеющим такие массовые и популярные поисковые системы, значительные конкурентные преимущества, что может сказаться на развитии конкурентоспособности других игроков рынка и процесса монополизации рынка. В настоящий момент в действующем антимонопольном законодательстве РФ нет эффективных регулирующих норм, способных влиять на такие процессы.

В итоге, любые информационные системы, предоставляющие свои возможности пользователям, стремятся к одному — получить максимальную информацию о них для ее использовании в будущем. Исходя из вышеописанного, возникает проблема надежности хранения и использования этих данных в информационных системах. Контроль такой информации сегодня не может быть в полной мере обеспечен пользователями, и владельцы информационных систем часто злоупотребляют возможностью использовать такие данные, включая несанкционированную передачу их третьим лицам (информационным

системам). В результате таких информационных взаимоотношений остро возникает проблема «доверия в ИКТ-среде».

В Доктрине информационной безопасности Российской Федерации безопасность информационных систем рассматривается как часть безопасности информационной инфраструктуры, расположенной на территории РФ, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров РФ. При этом в документе не поясняется, что же конкретно является фактом нарушения безопасности относительно информационных систем, в основном используются общие формулировки.

В ст. 13 Федерального закона «Об информации, информационных технологиях и о защите информации» определены подходы к классификации информационных систем, при этом выделены:

— государственные информационные системы — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов РФ, на основании правовых актов государственных органов. Подробная характеристика подобных систем исследована на монографическом уровне [1];

— муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

— и иные информационные системы.

Для более точного понимания объекта регулирования требуется более детальная классификация «иных информационных» систем по отраслевому и другим признакам.

По общему правилу, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. В случаях и в порядке, установленных федеральными законами, оператор информационной системы должен обеспечить возможность размещения информации в сети «Интернет» в форме открытых данных.

Понятие «оператор информационной системы», о котором речь шла выше, раскрывается более детально в специальных федеральных законах, применительно к конкретным информационным системам.

Так, в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» подходы законодателя к определению оператора информационной системы зафиксированы в ст. 5: «оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, может быть включенное в реестр операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, юридическое

лицо, личным законом которого является российское право (в том числе кредитная организация, лицо, имеющее право осуществлять депозитарную деятельность, лицо, имеющее право осуществлять деятельность организатора торговли)». При этом оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, вправе осуществлять свою деятельность с момента включения в реестр операторов информационных систем, который ведется Банком России в установленном им порядке.

Ведение такого реестра операторов информационных систем должно осуществляться Банком России в электронном виде. Согласно установленным в Положении Банка России от 16 декабря 2020 г. № 746-П требованиям Банк России должен включать в реестр операторов информационных систем ряд сведений, в числе которых:

1) полное и сокращенное наименование оператора информационной системы на русском языке;

2) основной государственный регистрационный номер (ОГРН) оператора информационной системы;

3) идентификационный номер налогоплательщика (ИНН) оператора информационной системы;

4) адрес оператора информационной системы, указанный в едином государственном реестре юридических лиц (ЕГРЮЛ);

5) адрес официального сайта оператора информационной системы в информационно-телекоммуникационной сети «Интернет»;

6) номер контактного телефона и адрес электронной почты оператора информационной системы;

7) сведения о единоличном исполнительном органе, членах коллегиального исполнительного органа (при его наличии), членах коллегиального органа управления (наблюдательного или иного совета) (при его наличии), главном бухгалтере, руководителе службы внутреннего контроля (контролер), руководителе службы управления рисками (лицо, ответственное за организацию системы управления рисками) оператора информационной системы и т.д., а также о лице, осуществляющем функции специального должностного лица, ответственного за реализацию правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения и др.

В целях обеспечения безопасности Банк России осуществляет надзор за деятельностью оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов. Законом подчеркивается, что оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не может выступать в качестве номинального держателя цифровых финансовых активов.

В качестве зарубежного опыта регулирования информационных систем можно привести Национальный институт стандартов и технологий США (*The National Institute of Standards and Technology*). Он определяет информационную безопасность информационных систем как «защиту информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения с целью обеспечения конфиденциальности, целостности и доступности» [https://www.nist.gov/ (дата обращения: 2 августа 2021 г.)], перечисляя возможные недружественные акты по отношению к информационным системам.

Безопасность информационных систем сегодня следует понимать как защиту информационных систем от несанкционированного доступа к информации или ее изменения, будь то хранение, обработка или передача, а также от отказа в обслуживании авторизованным пользователям, включая меры, необходимые для обнаружения, документирования и противодействия такой информации. Угрозы в информационном пространстве делают крайне необходимым для владельца информационных систем иметь способность защищать их от кибератак в среде, которая представляет собой глобальный домен в информационной среде, состоящий из взаимозависимой сети инфраструктур, включая информационные системы и компьютерные локальные сети.

Сталкиваясь с любым сервисом в сети Интернет, по факту, мы имеем дело с информационными системами — с десятками и сотнями в день, будь то различные мессенджеры или интернет-магазины. И, в сущности, информационные системы и информационные технологии являются взаимоинтегрированными понятиями и вполне могут быть рассмотрены как единый объект.

Правовой режим информационной системы с точки зрения прав собственника подразумевает следующее:

— собственник аппаратного обеспечения системы определяет оператора информационной системы или сам выступает в статусе оператора;

— аппаратные средства некоторых профильных информационных систем должны удовлетворять требованиям законодательства РФ о техническом регулировании;

— работа информационной системы возможна только при условии наличия формальных прав на ее программное обеспечение, являющееся компонентом информационной системы.

Многие информационные системы сегодня интегрированы с другими системами и составляют ряд глобальных мегасистем, включающих десятки и сотни других информационных систем. Это отраслевые системы, бизнес-системы, системы социальной коммуникации. Монетизация социальных систем происходит, в основном, за счет массового сбора личных данных (термин более широкий, чем

персональные данные). Политика использования личных данных не до конца понятна пользователям, а данные используются для повышения эффективности маркетинговых процессов. Политика многих информационных систем, составляющих основу социальных сетей и средств коммуникации, подразумевает обязательное предоставление компаниям расширенной информации об аккаунтах пользователей.

Новая политика конфиденциальности *Whats App* наглядно демонстрирует существующее положение дел, и владельцы мессенджера ясно дают понять, что информация личных аккаунтов может быть предоставлена другим системам, в частности *Facebook*, на основе интеграции этих систем.

Наряду с этим, в твиттере *Skype* размещена информация о том, что сохранение личной информации пользователей и недопустимость ее передачи третьим лицам является основным приоритетом мессенджера. Однако так или иначе пользователи не имеют никакой возможности это проконтролировать, влиять на это и иметь сколько-нибудь достоверную информацию об этом. И это вновь отсылка к «доверию к ИКТ-среде».

Илон Маск, используя свой гигантский авторитет среди пользователей сети интернет, на этом фоне призвал в своем блоге массово переходить к использованию мессенджера *Signal*, пытаясь создать мессенджеру имидж безопасного и надежного коммуникационного инструмента. Доверие, основанное на авторитете, возможно, но как показывает история, это рано или поздно приводит к злоупотреблениям.

Исследователи справедливо, характеризуя специализированные информационные системы, подчеркивают значение проблематики обеспечения безопасности. Так, характеризуя автоматизированные транспортные средства, авторы одной из научных работ констатируют: «информационные системы, связанные с управлением ВАТС … содержат уязвимости и проблемы, характерные для любой информационной системы, однако последствия реализации атак на них гораздо масштабнее и сопровождаются возможным причинением вреда жизни, здоровью людей, нанесением материального ущерба. Мировая практика показывает, что при обеспечении защиты информационных систем большую роль играют не только технические и организационные средства, но и юридическая защита» [3, стр. 8].

В качестве вывода можно отметить, что в полной мере безопасность информационных систем сегодня может быть достигнута только при условии возможности контроля всей полноты представленных для использования ресурсов и сервисов, работающих на основе информационных систем. Это возможно только при условии единства позиции по этому вопросу на международном уровне и создания эффективных международно-правовых норм, обязательных для исполнения всеми.

Литература

1. Амелин, Р. В. Правовой режим государственных информационных систем : монография / Р. В. Амелин ; под редакцией С. Е. Чаннова. — Москва : ГроссМедиа, 2016.
2. Блюмин, А. М. Проектирование систем информационного, консультационного и инновационного обслуживания: учебное пособие / А. М. Блюмин, Л. Т. Печеная, Н. А. Феоктистов. — Санкт-Петербург : Дашков и Ко, 2010.
3. Грачева, Ю. В. Высокоавтоматизированные транспортные средства: угрозы информационной системе безопасности и правовая ответственность / Ю. В. Грачева [и др.] // Государственная власть и местное самоуправление. — 2020. — № 12. — С. 3—9.
4. Чеботарев, В. Е. Проблемы правового регулирования деятельности новостных агрегаторов в сети Интернет и соблюдения ими требований законодательства Российской Федерации / В. Е. Чеботарев // в книге: Управление информационной безопасностью в современном обществе. Сборник научных трудов V Международной научно-практической конференции. — 2017. — С. 137—143.

References

1. Amelin, R. V. Pravovoy rezhim gosudarstvennykh informatsionnykh sistem : monografiya [Legal regime of state information systems: monograph] / R. V. Amelin ; pod redaktsiyey S. Ye. Channova. — Moskva : GrossMedia, 2016.
2. Blyumin, A. M. Proyektirovaniye sistem informatsionnogo, konsul'tatsionnogo i innovatsionnogo obsluzhivaniya: uchebnoye posobiye [Designing systems of information, consulting and innovative services: a tutorial] / A. M. Blyumin, L. T. Pechenaya, N. A. Feoktistov. — Sankt-Peterburg : Dashkov i Ko, 2010.
3. Gracheva, YU. V. Vysokoavtomatizirovannyye transportnyye sredstva: ugrozy informatsionnoy sisteme bezopasnosti i pravovaya otvetstvennost' [Highly automated vehicles: threats to the information security system and legal responsibility] / YU. V. Gracheva [i dr.] // Gosudarstvennaya vlast' i mestnoye samoupravleniye. — 2020. — № 12. — S. 3—9.
4. Chebotarev, V. Ye. Problemy pravovogo regulirovaniya deyatel'nosti novostnykh agregatorov v seti Internet i soblyudeniya imi trebovaniy zakonodatel'stva Rossiyskoy Federatsii [Problems of legal regulation of the activities of news aggregators on the Internet and their compliance with the requirements of the legislation of the Russian Federation] / V. Ye. Chebotarev // v knige: Upravleniye informatsionnoy bezopasnost'yu v sovremennom obshchestve. Sbornik nauchnykh trudov V Mezhdunarodnoy nauchno-prakticheskoy konferentsii. — 2017. — S. 137—143.