

Юридические исследования

Правильная ссылка на статью:

Марков Б.Б. — Проблемы защиты персональных данных в телемедицине. Блокчейн, гражданско-правовая ответственность и другие способы их преодоления // Юридические исследования. – 2023. – № 4. DOI: 10.25136/2409-7136.2023.4.40519 EDN: ONXLKA URL: https://nbpublish.com/library_read_article.php?id=40519

Проблемы защиты персональных данных в телемедицине. Блокчейн, гражданско-правовая ответственность и другие способы их преодоления

Марков Борис Борисович

ORCID: 0000-0003-4106-3828

аспирант, кафедра гражданского и предпринимательского права, Всероссийский государственный университет юстиции (РПА Минюста России)

117638, Россия, г. Москва, ул. Азовская, 2, к. 1

✉ yoursailorsun@outlook.com



[Статья из рубрики "Юридический практикум"](#)

DOI:

10.25136/2409-7136.2023.4.40519

EDN:

ONXLKA

Дата направления статьи в редакцию:

17-04-2023

Дата публикации:

24-04-2023

Аннотация: Предметом настоящей статьи является правовое регулирование защиты персональных данных в области оказания медицинской помощи с применением телемедицинских технологий и цифрового здравоохранения. Цель её состоит в выявлении и анализе проблем защиты персональных данных и поиске путей их преодоления. Актуальность работы обусловлена наличием большого количества утечек персональных данных, пробелов в регулировании, отсутствием эффективной системы норм, направленных на недопущение компрометации сведений о пациентах. Автор рассматривает основные аспекты регулирования порядка работы с согласием пациента на обработку персональных данных. Большое внимание в статье уделено технологии блокчейн, традиционно рассматриваемой в российской юридической литературе лишь в рамках использования криптовалют. Также в статье анализируются вопросы применения мер гражданско-правовой ответственности за правонарушения в области защиты персональных данных получателей телемедицинских услуг. В статье критикуется необоснованно жёсткое регулирование порядка получения медицинской организацией

согласия пациента на обработку персональных данных, подчёркивается необходимость введения гибкой формы согласия. Это позволит сократить объём сведений, подверженных риску утечки. Кроме того, выдвигается идея о создании механизма отзыва согласия пациента на обработку персональных данных и закреплении за пациентом права требовать от медицинской организации прекращения их обработки. В работе указывается на перспективы применения блокчейна в области телемедицины, в том числе для защиты персональных данных. Предлагается нормативное разделение блокчейн-систем на централизованные и децентрализованные, предполагающее различное их регулирование применительно к защите сведений конфиденциального характера. Помимо этого, в статье отмечается недостаточная проработанность норм о гражданско-правовой ответственности за правонарушения в области работы с персональными данными в телемедицине, предлагается ужесточение регулирования с целью повышения уровня защищённости прав пациентов.

Ключевые слова:

телемедицина, электронное здравоохранение, персональные данные, блокчейн, телемедицинские технологии, гражданская ответственность, защита данных, здравоохранение, цифровизация здравоохранения, телемедицинская консультация

Оказание медицинской помощи с применением телемедицинских технологий всегда сопряжено с передачей и обработкой информации в электронном виде. В отличие от других отраслей сферы услуг эта информация включает в себя не только ограниченный перечень часто используемых персональных данных, но и сведения о здоровье пациента. Это подчёркивает важность всеобъемлющей эффективной защиты такой информации.

Однако информация, подлежащая защите в соответствии с законодательством, подвержена значительным рискам, эффективность борьбы с которыми нельзя признать удовлетворительной. Так, по итогам 2021 года был выявлен факт компрометации порядка 80.5 млн записей персональных данных и платёжной информации, что на 20% больше, чем в 2020 году [\[1, с. 6\]](#). По итогам первой половины 2022 года ситуация значительно ухудшилась: количество утечек выросло на 46 % (305 против 209 в первом полугодии 2021 года), а объём скомпрометированной информации показал беспрецедентный рост – 1675% (187.6 млн записей против 11.2 млн по итогам первой половины 2021 года) [\[2, с. 5\]](#). При этом стоит отметить, что в трёх случаях из четырёх утечки происходят в результате «умышленных нарушений внутреннего характера», то есть по вине работника или должностного лица оператора персональных данных [\[2, с. 9\]](#). Это может свидетельствовать о существенных пробелах в организации работы с охраняемыми данными. Указанный факт позволяет говорить о том, что причины незащищённости информации носят, в первую очередь, организационно-правовой характер, а не технический. Системы хранения баз данных, очевидно, защищены достаточным образом или же попытки их взлома нецелесообразны ввиду большой трудо- и времязатратности, в то время как несовершенства организации работы с персональными данными и юридических механизмов контроля и ответственности за нарушения в данной области становятся предпосылкой столь массовых утечек.

Весьма актуальны обозначенные вопросы и для сферы здравоохранения, в том числе, телемедицины. Так, в 2020 году произошла утечка персональных данных 300000

москвичей, переболевших новой коронавирусной инфекцией COVID-19, наблюдение за которыми осуществлялось с помощью телемедицинских технологий.

Вышеуказанное порождает научный интерес к изучению проблем правового регулирования защиты персональных данных в телемедицине и обуславливает актуальность настоящей работы.

Под персональными данными российское законодательство понимает любые сведения, которые относятся к прямо или косвенно определённом или определяемому физическому лицу [\[3, ст. 3\]](#), то есть круг такого рода сведений необычайно широк. При этом, обработка персональных данных, по общему правилу, возможна лишь с согласия этого лица – субъекта персональных данных. Получение согласия пациента на обработку персональных данных – обязательная процедура, которую проводят медицинские организации при оказании телемедицинских услуг. Содержание согласия установлено нормативно. Согласие на обработку персональных данных содержит фамилию, имя, отчество пациента, его адрес, номер документа, удостоверяющего личность, и многие другие данные. Возникает закономерный вопрос о целесообразности включения всех этих сведений в согласие. Существо телемедицинской услуги состоит в преодолении географических барьеров, территориальной удалённости субъектов, потому адрес пациента – сведения, не имеющие никакого значения. В качестве излишних иногда называются и сведения о документе, удостоверяющем личность [\[4, с. 76\]](#). Однако медицинская организация в любом случае должна получить эти сведения, даже при нежелании пациента передавать эту информацию, в противном случае обработка персональных данных будет невозможна, а телемедицинская консультация не состоится. Представляется, что лучший способ защиты персональных данных – это отсутствие таких данных. Поэтому форма согласия на обработку персональных данных должна быть гибкой. Субъекты телемедицины должны иметь возможность самостоятельно определять состав указываемых в нём сведений. В таком случае медицинская организация сможет оценивать необходимость их получения и не принимать на себя дополнительное бремя в случае отсутствия целесообразности.

Помимо этого, для оказания телемедицинских услуг необходимо проводить идентификацию и аутентификацию участников в единой системе идентификации и аутентификации (ЕСИА) [\[5, ст. 36.2\]](#). Как это требование влияет на возможность проведения анонимных консультаций? Хотя запрета на их проведение с применением телемедицинских технологий нет, отсутствуют и исключения для подобных случаев в нормах законодательства, что отмечается Министерством здравоохранения России [\[6\]](#). Это делает невозможным оказание удалённых анонимных консультаций. Нужно использовать все возможные механизмы, способствующие увеличению охвата оказания медицинской помощи среди лиц, нежелающих раскрывать свою личность. Телемедицина могла бы выступить эффективным механизмом решения этой проблемы, однако, это невозможно при текущем жёстком регулировании. Кроме того, необходимо отметить и тот факт, что не все пациенты имеют подтверждённую учётную запись в ЕСИА, а значит и для них телемедицинская консультация станет недоступной формой получения медицинской помощи, за что действующее регулирование неоднократно подвергалось критике в литературе [\[7, с. 757\]](#), [\[8, с. 32\]](#).

Если субъект персональных данных опасается за их сохранность, не доверяет оператору персональных данных или по каким-либо иным причинам не желает, чтобы сведения о нём обрабатывались оператором, он должен иметь право требовать их уничтожения. Законодательство о персональных данных предоставляет возможность отзыва согласия

на обработку и обращения к оператору с требованием о прекращении обработки [\[3, ст. 9. 21\]](#). Однако в законе закреплён ряд исключений, одно из которых предоставляет оператору персональных данных право продолжить их обработку несмотря на отзыв согласия на обработку, если она осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну, в целях оказания медицинской помощи. То есть даже в случае отзыва пациентом данного ранее согласия на обработку персональных данных и требования им прекращения их обработки медицинская организация, оказывавшая ему телемедицинские услуги, может продолжить их обработку. Соответствие данной нормы конституции подтвердил и Конституционный Суд Российской Федерации, указав, что данное положение закона предоставляет подобное право медицинским организациям лишь для реализации права граждан на охрану здоровья и медицинскую помощь, обеспечивая при этом защищённость этих данных нормами права, включая положения о врачебной тайне [\[9\]](#). Учитывая наличие фактов утечек персональных данных, можно констатировать, что достаточного уровня защищённости сведений не наблюдается. Потому считаем, что наличие возможности отозвать согласие на обработку персональных данных и требовать прекращения их обработки, включая уничтожение этих сведений, должно являться неотъемлемым правом пациента. В связи с этим необходимо установить порядок прекращения обработки персональных данных медицинской организацией при получении отзыва согласия на обработку от пациента. При этом для целей медицинской статистики следует установить возможность удаления не всех сведений, включая диагноз и назначенное лечение, а лишь информацию о пациенте, сведения, которые позволяют определить конкретное физическое лицо (имя, номер телефона, место жительства и т. д.). Например, иногда предлагается обозначать пациента литерами [\[10, с. 37\]](#). Подобное обезличивание информации позволит в должной мере защитить права потребителя телемедицинских услуг.

Необходимо затронуть и технические стороны защиты информации. Одним из наиболее обсуждаемых в последнее время способов решения некоторых проблем в области защиты данных является применение технологии блокчейн. Блокчейн – это распределённая база данных, которая представляет из себя цепь связанных блоков, в которых хранится информация. Блокчейн может широко применяться в сфере электронного здравоохранения и телемедицины и решить проблему недостаточности защиты данных, полученной, например, в результате шифрования данных [\[11, с. 199\]](#). Однако регулирование блокчейна в России находится на начальном этапе, требуется разработка и принятие необходимых норм, при этом следует добиться сбалансированного регулирования, так как чрезмерное вмешательство государства может создать помехи для расширения использования этой технологии [\[12, с. 91\]](#). При этом применение блокчейна в разных отраслях экономики может иметь отличия, требующие и разных подходов к регулированию [\[13, с. 66\]](#).

Одно из наиболее явных направлений использования блокчейна в сфере здравоохранения – электронные медицинские карты. Благодаря его использованию можно обеспечить надёжное хранение и обработку любых данных о пациентах, организовать систему контроля за передачей этих данных [\[14\]](#).

Большое значение блокчейн может иметь и в сфере фармацевтики и телефармации. Транспарентность всех стадий разработки, клинических исследований (что имеет огромное значение для достижения целей доказательной медицины), производства лекарственных препаратов, их поставки в аптечные сети, организация системы

электронных рецептов и дистанционной продажи рецептурных препаратов, обеспечиваемые блокчейном, позволят существенно увеличить эффективность борьбы с производством и реализацией контрафактной медицинской продукции и иными нарушениями в данной области [\[15\]](#). В результате внесения изменений в действующее законодательство с 1 марта 2023 года в некоторых субъектах России в рамках эксперимента стала возможной дистанционная продажа рецептурных лекарственных препаратов [\[16\]](#).

Неоценимым может оказаться и влияние блокчейна в таком компоненте телемедицины, как дистанционное наблюдение за состоянием здоровья пациента. Благодаря использованию данной технологии станут возможными оптимизация системы удалённого сбора информации о состоянии здоровья пациента, одновременный анализ этой информации несколькими учреждениями здравоохранения и её надёжное хранение.

Таким образом, применение технологии блокчейн позволит упростить процесс обработки информации, обеспечить высокий уровень её защищённости, в том числе от несанкционированного доступа, обеспечить прозрачность и подотчётность [\[17, с. 366\]](#). Полагаем, что необходимо детально урегулировать возможность и необходимость применения блокчейна в сфере здравоохранения и телемедицины, причём в правовой литературе подчёркивается необходимость регулирования не только отношений, в рамках которых возможно применение этой технологии, но и самого блокчейна как технологии хранения информации [\[18\]](#). Одной из ключевых проблем может являться риск признания каждого участника цепочки, содержащей персональные данные, оператором персональных данных, а значит к ним будут предъявляться требования, соответствующие статусу оператора персональных данных, они будут вынуждены нести установленные законодательством о персональных данных обязанности [\[19, с. 114\]](#). Считаем, что подход к регулированию должен быть дифференцирован в зависимости от типа блокчейн-системы. В сфере телемедицины, очевидно, будет широко применяться централизованный блокчейн – организация распределённого реестра в рамках даже и одного предприятия. В этом случае медицинская организация будет являться оператором персональных данных. При построении же децентрализованной системы должны применяться специфические правила, в соответствии с которыми участник системы не будет признаваться оператором данных. Формально, каждый участник действительно хранит какую-то часть персональных данных. Но эта часть не является в достаточной степени обособленным компонентом, обладая ею нельзя выстроить конкретные сведения о лице (имя, номер телефона и пр.), равно как и определить физическое лицо, которому принадлежат эти сведения. Потому применение действующих норм законодательства о персональных данных (особенно в буквальном их толковании) к участникам блокчейн-системы не отвечает интересам общества и профессиональных участников отрасли.

Иной актуальный вопрос в области защиты персональных данных – ответственность в случае непринятия достаточных мер по охране информации и её утечки. Действующее правовое регулирование предусматривает совершенно незначительное наказание за подобные нарушения – административный штраф в размере до 100000 рублей [\[20, ст. 13.11\]](#). В случае телемедицины возможна утечка сведений, составляющих врачебную тайну, что квалифицируется как иной состав правонарушения. Наказание в этом случае может быть в два раза строже – административный штраф в размере до 200000 рублей [\[20, ст. 13.14\]](#). Представляется совершенно очевидным тот факт, что подобный уровень ответственности не соответствует общественной опасности данных правонарушений и тяжести их последствий, не способствует стимулированию операторов персональных

данных к усилению системы защиты информации, так как уплата подобных штрафов для оператора персональных данных будет менее затратна, чем создание надёжной системы их обработки и защиты. Ведущиеся дискуссии о необходимости ужесточения административной ответственности к настоящему моменту не привели к какому-либо результату.

Между тем, важно отметить, что отсутствует и проработанный массив правовых норм о гражданской ответственности [21, с. 71], а эта проблема не привлекает достаточно широкого внимания. Хотя, по нашему мнению, именно гражданско-правовая ответственность должна быть ключевой, так как лишь она направлена непосредственно на восстановление нарушенных прав пациента – субъекта персональных данных. Полагаем, что необходимо установить презумпцию вины оператора персональных данных в утечке информации, освободить субъекта персональных данных от доказывания факта причинения ему вреда в результате компрометации сведений о нём, а возможно даже и установить некоторые минимальные лимиты компенсаций в случае утечки конкретных видов информации. С особым вниманием следует относиться к сведениям о здоровье пациентов, компрометация которых может нанести куда больший вред, чем утечка иной информации.

Таким образом, в области защиты персональных данных в сфере телемедицины и цифрового здравоохранения существуют значительные проблемы. Для их решения требуется, с одной стороны, смягчить правовое регулирование в отношении работы с согласием пациента на обработку персональных данных, сделать его более гибким. Это позволит избежать обременения медицинской организации дополнительными обязанностями по защите информации, которая не требуется для проведения телемедицинской консультации, а также легализует проведение анонимных телемедицинских консультаций, повысив уровень доступности медицинской помощи. С другой стороны, необходимо ужесточить нормы об ответственности операторов персональных данных. Особое внимание при этом следует обратить на гражданско-правовую ответственность, так как она наилучшим образом сможет обеспечить восстановление нарушенных прав пациента-субъекта персональных данных. Помимо этого, значительное содействие в преодолении вышеуказанных проблем защиты персональных данных может оказать применение технологии блокчейн. Однако для этого требуется разработать нормы права, регулирующие возможность и порядок её использования, разделяющие блокчейн-системы на централизованные и децентрализованные, предъявляющие различные требования к ним.

Библиография

1. Россия. Утечки информации ограниченного доступа в 2021 году / Отчёт экспертно-аналитического центра InfoWatch [Электронный ресурс] URL: <https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-rost-latentnosti-intsidentov-i-vnutrennikh-utechek.pdf> (дата обращения: 02.04.2023);
2. Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года [Электронный ресурс] URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf?ysclid=lai48y511l771866327 (дата обращения: 02.04.2023);
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ от 31.07.2006. № 31 (часть I). Ст. 3451;
4. Журавлев М. С. Защита персональных данных в телемедицине // Право. Журнал

- Высшей школы экономики. 2016. № 3. С. 72—84. DOI: 10.17323/2072-8166.2016.3.72.84;
5. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 28.11.2011. № 48. Ст. 6724;
6. Письмо Министерства здравоохранения Российской Федерации от 09.04.2018 № 18-2/0579 [Электронный ресурс] URL: <https://www.garant.ru/products/ipo/prime/doc/71842326/?ysclid=lghwssjuwj640200587> (дата обращения: 09.04.2023);
7. Барашков Г. М., Еремина М. Г., Субботина В. Г. Телемедицина в решении проблемы ограничения доступности медицинской помощи на отдаленных территориях: правовые барьеры внедрения и функционирования (обзор) // Саратовский научно-медицинский журнал. 2021. № 4. С. 755—760;
8. Пospelова С. И., Сергеев Ю. Д., Павлова Ю. В., Каменская Н. А. Правовой режим применения телемедицинских технологий и внедрения электронного документооборота: современное состояние правового регулирования и перспективы развития // Медицинское право. 2018. № 5. С. 24—33;
9. Определение Конституционного Суда РФ от 16.07.2013 № 1176-О «Об отказе в принятии к рассмотрению жалобы гражданина Круглова Александра Геннадьевича на нарушение его конституционных прав пунктом 4 части 2 статьи 10 Федерального закона «О персональных данных» [Электронный ресурс] URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=152099&dst=100001#VSusUbTlcksifrR9> (дата обращения: 11.04.2023);
10. Винокуров В. А. Проблемы соблюдения личной и врачебной тайны при оказании медицинских услуг // Медицинское право: теория и практика. 2021. № 2 (14). С. 33—40;
11. Блинов С. В., Кузьмина Н. М., Ревина С. Н., Сидорова А. В. Соблюдение врачебной тайны при оказании телемедицинских услуг // Вестник медицинского института «Реавиз»: реабилитация, врач и здоровье. 2019. № 2 (38). С. 196—200;
12. Ковалева Н. А. Практика государственного регулирования применения блокчейн-технологий и ее совершенствование на основе зарубежного опыта // Экономика. Налоги. Право. 2019. № 4. С. 87—93. DOI: 10.26794/1999-849X-2019-12-4-87-93;
13. Архиреев Н. В. Вопросы сущности и правового регулирования блокчейна // Молодежный научный форум «Уфимский гуманитарный научный форум» / Сборник статей под ред. А. Н. Дегтярева, А. Р. Кузнецовой. Уфа: Институт стратегических исследований Республики Башкортостан. 2022. 454 с.;
14. Heston, T. F. (2017). Why Blockchain Technology Is Important for Healthcare Professionals [Электронный ресурс] URL: <https://ssrn.com/abstract=3006389> (дата обращения: 13.04.2023);
15. Rejeb, A., Bell, L. (2019). Potentials of Blockchain for Healthcare: Case of Tunisia [Электронный ресурс] URL: <https://ssrn.com/abstract=3475246> (дата обращения: 13.04.2023);
16. Федеральный закон от 20.10.2022 № 405-ФЗ «О внесении изменений в Федеральный закон «Об обращении лекарственных средств» // Собрание законодательства РФ. 24.10.2022. № 43. Ст. 7268;
17. Чистяков М. С., Чирков М. А., Шаповалова А. В. Блокчейн-технологии в правовых реалиях // Цифровые технологии и право: сборник научных трудов I

Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 5. Казань: Изд-во «Познание» Казанского инновационного университета. 2022. 432 с.;

18. Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143—155. DOI: 10.7256/2454-0706.2020.9.33614;
19. Савельев А. И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94—117;
20. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. 07.01.2002. № 1 (часть I). Ст. 1;
21. Макарейко Н. В. Правовые риски цифровизации оказания медицинской помощи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. №1 (57). С. 67—74. DOI: 10.36511/2078-5356-2022-1-67-74

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

РЕЦЕНЗИЯ на статью на тему «Проблемы защиты персональных данных в телемедицине. Блокчейн, гражданско-правовая ответственность и другие способы их преодоления».

Предмет исследования. Предложенная на рецензирование статья посвящена проблемам «...защиты персональных данных в телемедицине...». Автор предлагает некоторые из них: «Блокчейн, гражданско-правовая ответственность и другие способы их преодоления». Автором выбран особый предмет исследования: предложенные вопросы исследуются с точки зрения медицинского, информационного, административно-деликтного и гражданского права, при этом автором отмечено, что «Оказание медицинской помощи с применением телемедицинских технологий всегда сопряжено с передачей и обработкой информации в электронном виде». Изучаются НПА, имеющие отношение к цели исследования. Также изучается и обобщается большой объем научной литературы по заявленной проблематике, анализ и дискуссия с данными авторами-оппонентами присутствует. При этом автор отмечает: «...информация включает в себя не только ограниченный перечень часто используемых персональных данных, но и сведения о здоровье пациента. Это подчёркивает важность всеобъемлющей эффективной защиты такой информации».

Методология исследования. Цель исследования определена названием и содержанием работы: «... причины незащищённости информации носят, в первую очередь, организационно-правовой характер, а не технический. Системы хранения баз данных, очевидно, защищены достаточным образом или же попытки их взлома нецелесообразны ввиду большой трудо- и времязатратности, в то время как несовершенства организации работы с персональными данными и юридических механизмов контроля и ответственности за нарушения в данной области становятся предпосылкой столь массовых утечек». Они могут быть обозначены в качестве рассмотрения и разрешения отдельных проблемных аспектов, связанных с вышеназванными вопросами и использованием определенного опыта. Исходя из поставленных цели и задач, автором выбрана определенная методологическая основа исследования. Автором используется совокупность частнонаучных, специально-юридических методов познания. В частности, методы анализа и синтеза позволили обобщить подходы к предложенной тематике и

повлияли на выводы автора. Наибольшую роль сыграли специально-юридические методы. В частности, автором применялись формально-юридический и сравнительно-правовой методы, которые позволили провести анализ и осуществить толкование норм актов законодательства и сопоставить различные НПА. В частности, делаются такие выводы: «Представляется, что лучший способ защиты персональных данных – это отсутствие таких данных. Поэтому форма согласия на обработку персональных данных должна быть гибкой. Субъекты телемедицины должны иметь возможность самостоятельно определять состав указываемых в нём сведений. В таком случае медицинская организация сможет оценивать необходимость их получения и не принимать на себя дополнительное бремя в случае отсутствия целесообразности» и др. Таким образом, выбранная автором методология в полной мере адекватна цели статьи, позволяет изучить многие аспекты темы.

Актуальность заявленной проблематики не вызывает сомнений. Данная тема является важной в мире и в России, с правовой точки зрения предлагаемая автором работа может считаться актуальной, а именно он отмечает «...информация, подлежащая защите в соответствии с законодательством, подвержена значительным рискам, эффективность борьбы с которыми нельзя признать удовлетворительной», «Вышеуказанное порождает научный интерес к изучению проблем правового регулирования защиты персональных данных в телемедицине и обуславливает актуальность настоящей работы», «... актуальный вопрос в области защиты персональных данных – ответственность в случае непринятия достаточных мер по охране информации и её утечки». И на самом деле здесь должен следовать анализ работ оппонентов, и он следует и автор показывает умение владеть материалом. Тем самым, научные изыскания в предложенной области стоит только приветствовать.

Научная новизна. Научная новизна предложенной статьи не вызывает сомнения. Она выражается в конкретных научных выводах автора. Среди них, например, такой: «... необходимо установить порядок прекращения обработки персональных данных медицинской организацией при получении отзыва согласия на обработку от пациента. При этом для целей медицинской статистики следует установить возможность удаления не всех сведений, включая диагноз и назначенное лечение, а лишь информацию о пациенте, сведения, которые позволяют определить конкретное физическое лицо». Как видно, указанный и иные «теоретические» выводы «...необходимо установить презумпцию вины оператора персональных данных в утечке информации, освободить субъекта персональных данных от доказывания факта причинения ему вреда в результате компрометации сведений о нём, а возможно даже и установить некоторые минимальные лимиты компенсаций в случае утечки конкретных видов информации» могут быть использованы в дальнейших исследованиях. Таким образом, материалы статьи в представленном виде могут иметь интерес для научного сообщества.

Стиль, структура, содержание. Тематика статьи соответствует специализации журнала «Юридические исследования», так как посвящена проблемам «...защиты персональных данных в телемедицине...». В статье присутствует аналитика по научным работам оппонентов, поэтому автор отмечает, что уже ставился вопрос, близкий к данной теме и автор использует их материалы, дискутирует с оппонентами. Содержание статьи соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели своего исследования. Качество представления исследования и его результатов следует признать доработанным. Из текста статьи прямо следуют предмет, задачи, методология, результаты исследования, научная новизна. Оформление работы соответствует требованиям, предъявляемым к подобного рода работам. Существенные нарушения данных требований не обнаружены, кроме библиографии.

Библиография достаточно полная, содержит публикации, НПА, к которым автор

обращается. Однако требование редакции: «В список литературы включаются только рецензируемые научные источники (статьи из научных журналов и монографии), которые упоминаются в тексте статьи. Источники (нормативно-правовая документация, учебники, публикации ненаучного характера и др.) упоминаются в тексте статьи в скобках, наряду с прочими комментариями и примечаниями авторов». Библиография позволяет автору правильно определить проблемы и поставить их на обсуждение. Следует высоко оценить качество представленной и использованной литературы. Присутствие научной литературы показало обоснованность выводов автора и повлияло на выводы автора. Труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию многих аспектов темы.

Апелляция к оппонентам. Автор провел серьезный анализ текущего состояния исследуемой проблемы. Автор описывает разные точки зрения оппонентов на проблему, аргументирует более правильную по его мнению позицию, опираясь на работы оппонентов, предлагает варианты решения проблем.

Выводы, интерес читательской аудитории. Выводы являются логичными, конкретными «... значительное содействие в преодолении вышеуказанных проблем защиты персональных данных может оказать применение технологии блокчейн. Однако для этого требуется разработать нормы права, регулирующие возможность и порядок её использования, разделяющие блокчейн-системы на централизованные и децентрализованные, предъявляющие различные требования к ним» и др. Статья в данном виде может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным в статье вопросам после доработки библиографии. На основании изложенного, суммируя все положительные и отрицательные стороны статьи «рекомендую отправить на доработку».