

Научная статья
УДК 34.06
<https://doi.org/10.36511/2078-5356-2022-1-67-74>

Правовые риски цифровизации оказания медицинской помощи

Макарейко Николай Владимирович

Нижегородская академия МВД России, Нижний Новгород, Россия, makareiko_nik@mail.ru

Аннотация. Здравоохранение выступает зоной повышенного риска, в том числе правового, который представляет реальную угрозу для здоровья и жизни пациентов. Традиционно исследовательское внимание фокусируется на рисках экспериментальной медицины, медицинского вмешательства, бездействия медицинского работника. Они не утрачивают своей актуальности и в настоящее время. Наряду с этим необходимо учитывать процесс всемерной цифровизации социума, который приобретает особую остроту в области здравоохранения. В этой связи требуется дополнительное комплексное теоретическое осмысление рисков в данной области как медиками, так и юристами, экономистами, социологами, психологами и другими специалистами. Они должны дать дифференцированную характеристику рисков, возникающих при оказании медицинской помощи в условиях осуществления цифровизации, предложить наиболее действенные пути по их диагностике, предупреждению, минимизации негативных последствий. Особую остроту представляют правовые риски, которые возникают в ходе цифровизации оказания медицинской помощи. Действующее российское законодательство запаздывает в правовом опосредовании отношений в области цифровизации в данной области, что существенно осложняет ситуацию. В статье названы наиболее опасные правовые риски, показана их специфика, определены пути предупреждения и устранения негативных последствий.

Ключевые слова: правовой риск, здравоохранение, медицинская помощь, цифровизация

Для цитирования: Макарейко Н. В. Правовые риски цифровизации оказания медицинской помощи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 1 (57). С. 67—74. <https://doi.org/10.36511/2078-5356-2022-1-67-74>.

Original article

Legal risks of digitalization of medical care

Nikolay V. Makareyko

Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, makareiko_nik@mail.ru

Abstract. Healthcare is a high-risk area, which pose a real threat to the health and life of patients. Traditionally, research attention focuses on the risks of experimental medicine, medical intervention, and inaction of a medical professional. This does not lose its relevance at the present time. Along with this, it is necessary to take into account the process of all-round digitalization of society, which is becoming particularly acute in the field of healthcare. In this regard, an additional comprehensive theoretical understanding of the risks in this area is required by both physicians and lawyers, economists, sociologists, psychologists and other specialists. They should give a differentiated characterization of the risks arising from the provision of medical care in the context of digitalization, suggest the most effective ways to diagnose them, prevent, minimize negative consequences. digitalization of medical care are particularly acute. The current Russian legislation is late in the legal mediation of relations in the field of digitalization in this area, which significantly complicates the situation. The article names the most dangerous legal risks, shows their specifics, identifies ways to prevent and eliminate negative consequences.

Keywords: legal risk, healthcare, medical care, digitalization

For citation: Makareyko N. V. Legal risks of digitalization of medical care. *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2022, no. 1 (57), pp. 67—74. (In Russ.). <https://doi.org/10.36511/2078-5356-2022-1-67-74>.

© Макарейко Н. В., 2022

Сегодня предложенный У. Беком штамп о признании настоящего этапа общественного развития в качестве «общества рисков» [1] не вызывает сомнения. Число рисков, их интенсивность, сфера распространения свидетельствуют о необходимости безотлагательного принятия соответствующих методов противодействия. При этом важно наряду с общими подходами выработать и применять адресные пути для конкретных областей деятельности. Неслучайно, проблема правовых рисков является предметом острых научных дискуссий [2].

Областью, которая традиционно отличается наивысочайшей степенью риска, выступает здравоохранение. Специфика охраны здоровья требует, чтобы врачи и другие работники здравоохранения шли на риск, когда речь идет о противодействии различного рода заболеваниям, принимая необходимые меры по минимизации возможных негативных последствий. При этом следует учитывать всемерную коммерциализацию данной деятельности, когда во главу угла ставится извлечение прибыли, а ценой выступает здоровье и даже жизнь пациентов. В этой связи в литературе отмечается, что «платное оказание медицинских услуг сопровождается повышенным вниманием со стороны государственных надзорных органов, равно как и повышенными административно-правовыми рисками, даже в сравнении с другими подлежащими лицензированию видами деятельности» [3, с. 79].

Закономерно, что в специальной литературе отмечается высокая возможность возникновения рисков при оказании медицинской помощи. В этой связи обращается внимание на то, что «проблема рисков медицинского вмешательства и бездействия медицинского работника, а также их связи с вероятностью развития вредоносного воздействия на организм пациента при прогрессировании основного заболевания — сложная проблема и в медико-организационном, и в правовом смыслах» [4, с. 43].

Высокий потенциал риска в рассматриваемой сфере обусловило то, что неоднократно предпринимались и предпринимаются правовые меры по контролю за деятельностью в области охраны здоровья, в том числе и при осуществлении медицинских экспериментов. Об этом свидетельствует принятие десяти принципов Нюрнбергского кодекса 1947 года. Речь идет о добровольном согласии испытуемого, общественно полезном результате, обоснованности, недопущении физических или психических страданий и увечий подопытному, отсутствии возможности причинения смерти или увечья

испытуемому, приоритете важности проблемы над степенью риска, наличии соответствующей подготовки и оборудования, проведении эксперимента только лицами, имеющими научную квалификацию, праве подопытного остановить эксперимент, обязанности исследователя прекратить эксперимент при определенных обстоятельствах [5, с. 56].

В дальнейшем указанные принципы были положены в основу таких международных правовых актов, как Хельсинкская декларация «Этические принципы медицинских исследований с участием человека в качестве испытуемого» 1964 года [6], Конвенции о защите прав человека и человеческого достоинства в связи с применением биологии и медицины [7], а также соответствующими дополнительными протоколами к ней (о запрете клонирования человека; о трансплантации органов и тканей человека; биомедицинских исследованиях). К указанной Конвенции Российская Федерация в настоящее время не присоединилась.

Высокими рисками отличается не только экспериментальная медицина, но и каждодневная медицинская деятельность. Неслучайно в основах охраны здоровья граждан в Российской Федерации [8] термин «риск» и производные от него упоминаются более пятнадцати раз.

Правомерность риска в медицинской деятельности обоснована рядом факторов: во-первых, наличие цели, которая не может быть достигнута нерискованным путем; во-вторых, риск должен быть обоснованным по отношению к ожидаемому полезному результату; в-третьих, деятельность должна отвечать уровню современных научно-технических знаний и опыту; в-четвертых, отсутствует заведомая угроза жизни для многих людей, наступление экологической катастрофы, общественного бедствия; в-пятых, наличие соответствующего согласия пациента. Показательным является статья 20 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», в которой закреплен порядок информированного добровольного согласия на медицинское вмешательство или отказ от такового.

Минимизация рисков при осуществлении медицинской деятельности должна основываться на прочной правовой основе. В этой связи разработана соответствующая нормативная правовая база, где учтена специфика осуществления государственного контроля (надзора) за качеством и безопасностью осуществления медицинской деятельности [9].

Признавая существенный «градус» риска рассматриваемого вида деятельности, необходимо отметить его усиление в связи с цифровизацией здравоохранения. Данный процесс осуществляется в рамках развития информационного общества в Российской Федерации [10]. При этом всемерно актуализировалась необходимость принятия соответствующих нормативных правовых актов [11]. Определенные шаги в данном направлении предпринимались, о чем свидетельствует распоряжение Правительства Российской Федерации «Об утверждении стратегического направления в области цифровой трансформации здравоохранения» [12]. Признавая необходимость такого решения, нельзя не отметить специфичность его наименования. Традиционно к числу актов стратегического планирования относят стратегии, доктрины, концепции, планы, программы [13]. В данном случае распоряжением Правительства Российской Федерации утвержден такой новый вид документа стратегического планирования, как «стратегическое направление». Данная форма была введена в официальный оборот совсем недавно [14].

В стратегических направлениях цифровой трансформации здравоохранения в Российской Федерации наряду с приоритетами, целями, задачами цифровой трансформации были определены и возникающие при этом проблемы и вызовы. Общие вызовы позволили определить возникающие при этом риски. К их числу разработчиками отнесены: недостаточная цифровая компетенция граждан; отсутствие у населения доверия к медицинским сервисам; двойной (электронный и бумажный) документооборот; увеличение нагрузки на медицинских работников при ведении электронной документации; низкие темпы при переходе от бумажного к электронному документообороту; различие в уровне готовности, финансового потенциала субъектов Российской Федерации; внесение корректив в силу чрезвычайных обстоятельств (новая коронавирусная инфекция COVID-19).

Признавая реальность перечисленных угроз, необходимо оценить и их неполноту. Более того, основные угрозы цифровизации здравоохранения не были отражены в стратегических направлениях цифровой трансформации в рассматриваемой области деятельности. Объем научной статьи не позволяет дать им детальную характеристику и, самое главное, определить путь их (рисков) устранения. Следует отметить, что они носят комплексный характер и в этой связи, наряду с работниками здравоохранения,

должны быть оценены юристами, экономистами, социологами, психологами, специалистами в области информатизации и др. В качестве одного из очевидных рисков является отсутствие необходимого отечественного программного обеспечения (Software) и компьютерной техники (Hardware), а также привлечения зарубежных ресурсов.

Особую, но недостаточно исследованную составляющую рисков цифровизации здравоохранения составляют правовые риски. Речь идет прежде всего об отсутствии должной нормативной правовой базы в данной области. Так, программа «Цифровая экономика Российской Федерации» [15], которой было предусмотрено адресное нормативное и методическое обеспечение отдельных отраслей экономики, включая здравоохранение, утратила силу менее чем через два года с момента вступления в силу [16].

Сложность соединения медицинской деятельности, которая обладает своей спецификой, требует детальной нормативной правовой регламентации. Возникает закономерный вопрос о достаточности принятия отдельных подзаконных нормативных правовых актов для решения такой многосложной задачи, как цифровизация здравоохранения. В этой связи естественно возникает вопрос о необходимости дополнения Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» отдельной главой или принятия отдельного федерального закона по данному вопросу. Считаем, что сложность и глубина проблемы ставит на повестку дня принятие Медицинского кодекса Российской Федерации как отдельного кодифицированного акта, регулирующего отношения в сфере охраны здоровья. Такое решение должно сократить подзаконное нормативное правовое регулирование, уменьшить использование бланкетного способа правового регулирования.

При осуществлении цифровизации здравоохранения важно обеспечить оптимальный баланс норм права и других социальных регуляторов. Очевидно, что нормы морали, обычаи, традиции, корпоративные, религиозные нормы являются не иллюзорными, а реальными средствами упорядочения рассматриваемых отношений. Учитывая национальную, конфессиональную неоднородность российского населения, их роль при регулировании цифровизации оказания медицинской помощи будет неодинаковой. Наряду с этим следует учитывать специфику технических норм, которые непосредственно регулируют информационные

процессы, а также сложность их правового опосредования.

Неслучайно клятву Гиппократова связывают с реализацией современных технологий в медицине. «Самой ранней субдисциплиной биоэтики является медицинская этика (биоэтика в узком значении), которая восходит к внедрению клятвы Гиппократова (500 г. до н. э.), включающая некоторые обязательные этические правила поведения между врачом и пациентом, имеющие чрезвычайно важное значение, такие хорошо известные принципы, как “не навреди” (*primum non nocere*) и “благо больного — высший закон врачей” (*salus aegroti suprema lex*)» [17, 66]. Закономерным видится использование положений клятвы Гиппократова в Кодексе профессиональной этики врача Российской Федерации [18].

В ходе правового опосредования цифровизации здравоохранения важно учитывать специфику отношений, затрагивающих охрану здоровья, а также этические нормы, которые связаны с использованием робототехники и других составных элементов искусственного интеллекта. При этом такой учет необходим не только при непосредственном использовании цифровых технологий, но и на этапах их проектирования и разработки.

Следует выработать конкретные нравственные ориентиры использования искусственного интеллекта в сфере здравоохранения. Учитывая специфику предмета правового регулирования, необходимо отметить усиление роли религиозных норм, так как во всех религиях существенное внимание уделяется нравственному и физическому здоровью их защиты.

При этом следует учитывать, что для подавляющего большинства неправовых социальных регуляторов требуется достаточно длительное время для выработки и закрепления соответствующих норм. В этой связи следует иметь в виду, что существует возможность опережающего правового регулирования, когда нормативные правовые акты содержат правовые предписания, ориентированные на отношения, возникающие в будущем [19]. Вместе с тем мощное развитие цифровых технологий ставит под сомнение заблаговременное создание необходимой нормативной правовой базы регулирования отношений в области цифровизации здравоохранения.

Еще одним из рисков использования искусственного интеллекта является определение его границ. В стратегическом направлении в области цифровой трансформации здравоохранения

основной акцент делается на работу с большими массивами данных, электронную обработку информации о пациентах и оказании медицинской помощи. Вместе с тем будущее за непосредственным использованием цифровых технологий при оказании медицинской помощи, когда из этого процесса будут исключены конкретные медицинские работники. Очевидно, что и использование телемедицины в полной мере нельзя назвать использованием искусственного интеллекта. Наряду с этим экспертным сообществом высказываются существенные замечания по вопросу нормативного правового регулирования телемедицины в России [20].

Следующим очевидным риском является обеспечение приватности информации при оказании медицинской помощи. Здесь уместно провести параллели, которые возникают в сфере национальной безопасности. Речь идет о противопоставлении безопасности и свободы. История со всей очевидностью доказала, что при реальности угрозы безопасности личности она готова жертвовать, отказываться от свободы. Такое положение вполне очевидно, так как на чашу весов положена жизнь человека. В этой связи следует признать, что при оказании медицинской помощи прежде всего при распространении опасных или массовых заболеваний, будет корректироваться режим охраны информации (медицинская тайна, персональные данные и др.).

Реальное использование искусственного интеллекта при оказании медицинской помощи, когда предлагаются новые решения при диагностике и лечении, обеспечении сохранности конфиденциальности при хранении информации о пациентах (облачное хранилище медицинской информации), использовании телемедицины и другое, актуализирует проблему медицинских ошибок. Они могут возникать в силу различных причин, например, сбоев в функционировании информационно-коммуникационных систем, вредоносного вмешательства с целью внесения недостоверных данных, недостаточной квалификации персонала, ошибок при соединении цифровых и биологических технологий.

Одним из рисков является отсутствие детально отработанной системы юридической ответственности при использовании цифровых технологий в области здравоохранения. Существенные сложности связаны с функционированием механизма реализации юридической ответственности на локальном уровне. Речь идет об ответственности за конкретную медицинскую ошибку [21], а также за нарушение режима

врачебной тайны. Так, частью 5 статьи 36.2 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» определено, что в случае применения телемедицинских технологий в медицинской деятельности необходимо соблюдать требования, установленные законодательством в области персональных данных, и врачебную тайну.

Ситуация в значительной степени усложняется тем, что Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [22] определено, что экспериментальные правовые режимы, связанные с разработкой, апробацией и внедрением цифровых инноваций вводятся прежде всего в области медицинской деятельности, говоря о применении телемедицинских технологий, технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан, фармацевтической деятельности.

Признавая сложности применения юридической ответственности при совершении врачебной ошибки, остаются вопросы, связанные с ответственностью реализации программы цифровизации здравоохранения. Отрядным является тот факт, что в стратегических направлениях в области цифровой трансформации здравоохранения определено, что за ее реализацию наряду с Минздравом России отвечают Минцифры России, ФОМС, Росздравнадзор, ФМБА России, высшие органы исполнительной власти субъектов Российской Федерации, органы управления здравоохранением субъектов Российской Федерации, а также иные федеральные органы исполнительной власти, которые имеют подведомственные медицинские организации.

Приветствуя тот факт, что в документе стратегического планирования уделено внимание юридической ответственности, необходимо отметить, что отсутствует реальный механизм реализации названной формы государственного принуждения. В данном случае речь идет о частном проявлении юридической ответственности государства. В рамках реформирования российского законодательства необходимо обеспечить использование потенциала различных видов публичной и частной юридической ответственности.

Особенно остро стоит вопрос юридической ответственности коллективных субъектов государственного управления. В настоящее время сложившееся положение не позволяет реализовать неотвратимость юридической

ответственности. Другой крайностью выступает необоснованное применение юридической ответственности в отношении конкретных должностных лиц в области здравоохранения.

Мы ни в коей степени не даем необоснованно завышенное значение юридической ответственности вообще и при осуществлении цифровизации здравоохранения, но следует незамедлительно осуществить его реформирование [23]. Мы считаем, что следует выработать систему мер публично-правовой и частно-правовой ответственности за нарушения при осуществлении различных действий, связанных с цифровизацией отношений в области здравоохранения. При этом следует идти по пути дифференциации ответственности разработчиков и операторов. В свою очередь, среди разработчиков следует учитывать специфику деяния и вину постановщиков задач, алгоритмистов, программистов, тестировщиков как программного продукта, так и компьютерной техники.

Еще сложнее проблема стоит при разработке и эксплуатации технических систем с элементами искусственного интеллекта, в том числе с элементами самообучающихся нейронных сетей. В этом случае они используют не только заранее заложенный разработчиками алгоритм действий, но и сами формируют новые по мере накопления опыта. Какие необходимо при этом создать защитные механизмы? Другими словами, речь идет о мерах предупреждения. Они должны носить комплексный (правовой, технический, интеллектуальный) характер и включаться на различных этапах сбоя в работе робототехнических средств. Наряду с этим необходимо предусмотреть простейшие защитные механизмы, например, связанные с «выключением рубильника», то есть меры по надежному функционированию системы обеспечения бесперебойного энергопитания, передачи сигналов (Интернет, телемедицина) и другое, а также применение сложных защитных механизмов.

Учитывая специфику отношений в области здравоохранения, существует риск использования потенциала саморегулирования. Допустимо ли в данной области использование саморегулирования, что обусловлено опасностью причинения вреда здоровью пациентов? Мы отметили возможность «самообучения» нейронных систем, но этот процесс должен быть детально юридически регламентирован.

Одним из правовых рисков является определение приоритетных направлений цифровизации в области здравоохранения. К их числу следует отнести: создание цифрового профиля

пациента; защиту личных данных пациентов; медицинскую диагностику (скрининговые исследования); мониторинг пациентов, страдающих хроническими заболеваниями; разработку вакцин; медицинскую статистику; телемедицину; логистику; фармакологию; контроль медицинского персонала; медицинское образование. Очевидно, что степень использования искусственного интеллекта по указанным направлениям будет различной.

Одной из очевидных угроз цифровизации здравоохранения является угроза безопасности отдельного пациента, медицинского работника, медицинских организаций, отрасли в целом. В этой связи необходимо «настроить» правовые механизмы защиты отношений в области здравоохранения. Важно, чтобы они были интегрированы в систему обеспечения национальной безопасности. В этой связи важное значение приобретает резолюция Генеральной Ассамблеи ООН от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур, которой определены общие контуры защиты важнейших инфраструктур прежде всего за счет своевременного выявления угроз, уменьшения уязвимости информационных инфраструктур, минимизации причиняемого ущерба, сокращения времени восстановления, выявления и устранения причин повреждения.

Определенные меры принимаются и на внутригосударственном уровне, о чем свидетельствует принятие Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [24]. Его положения направлены на обеспечение безопасности критической информационной инфраструктуры государства, создание условий для ее устойчивого функционирования при осуществлении в отношении нее компьютерных атак.

Названные правовые угрозы являются далеко не исчерпывающими и могут пополняться или утрачивать свою актуальность в процессе цифровизации здравоохранения.

Список источников

1. Бек У. Общество риска. На пути к другому модерну. М.: Прогресс-Традиция, 2000. 381 с.
2. Юридическая техника: Ежегодник, № 13. Риски в законотворчестве, правореализации, юридической науке: техника формирования и функционирования системы управления, 2019. 794 с.

3. Орленко В. Административно-правовые риски при осуществлении медицинской деятельности // Административное право. 2018. № 1. С. 79—88.

4. Тимофеев И. В. Риски оказания медицинской помощи: конституционно-правовой аспект // Конституционное и муниципальное право. 2017. № 8. С. 39—46.

5. Нюрнбергский кодекс // Врач. 1993. № 7.

6. Хельсинкская декларация Всемирной медицинской ассоциации. Этические принципы проведения медицинских исследований с участием человека в качестве субъекта: принята в г. Хельсинки в июне 1964 года на 18-ой Генеральной Ассамблее ВМА. URL: <http://acto-russia.org>. (дата обращения: 27.01.2022).

7. Конвенция о защите прав человека и человеческого достоинства в связи с применением достижений биологии и медицины: конвенция о правах человека и биомедицине (ETS № 164): заключена в г. Овьедо 4 апреля 1997 г. Доступ из СПС «КонсультантПлюс» (дата обращения: 27.01.2022).

8. Об основах охраны здоровья граждан в Российской Федерации: федеральный закон от 21 ноября 2011 г. № 323-ФЗ // Собрание законодательства РФ. 2011. № 48, ст. 6724.

9. Об утверждении Положения о федеральном государственном контроле (надзоре) качества и безопасности медицинской деятельности: постановление Правительства РФ от 29 июня 2021 г. № 1048. URL: <http://pravo.gov.ru> (дата обращения: 27.01.2022).

10. О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства РФ. 2017. № 20, ст. 2901.

11. Стефанова Н. А., Андропова И. В. Проблемы цифровизации сферы здравоохранения: российский и зарубежный опыт // Вестник Самарского университета. Экономика и управление. 2018. Т. 9. № 3. С. 31—35.

12. Об утверждении стратегического направления в области цифровой трансформации здравоохранения: распоряжение Правительства РФ от 29 декабря 2021 г. № 3980-р. URL: <http://pravo.gov.ru>, 31.12.2021 (дата обращения: 27.01.2022).

13. Говорухина Ю. В. Стратегия как правовой документ: автореф. дис. ... канд. юрид. наук. Н. Новгород, 2021. 31 с.

14. Об утверждении стратегического направления в области цифровой трансформации государственного управления: распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р // Собрание законодательства РФ. 2021. № 44. Ч. III, ст. 7467.

15. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р // Собрание законодательства РФ. 2017. № 32, ст. 5138.

16. О признании утратившим силу распоряжения Правительства Российской Федерации от 28 июля 2017 г. № 1632-р: распоряжение Правительства РФ от 12 февраля 2019 г. № 195-р // Собрание законодательства РФ. 2019. № 8, ст. 803.

17. Каюмова А. Р. Защита прав человека в контексте применения современных биотехнологий: некоторые проблемы // Юрист. 2019. № 1. С. 64—71.

18. Кодекс профессиональной этики врача Российской Федерации: принят Первым национальным съездом врачей Российской Федерации 5 октября 2012 г. (документ опубликован не был). Доступ из СПС «КонсультантПлюс» (дата обращения: 27.01.2022).

19. Баранова М. В. Опережающее правотворчество в правовой системе современности // Вестник Саратовской государственной юридической академии. 2016. № 1 (108). С. 43—45.

20. Варюшин М. С. Правовое регулирование телемедицины в России и ЕС: два шага вперед и один назад // Закон. 2018. № 1. С. 165—174.

21. Пикуров Н. И. Риски медицинского вмешательства: уголовно-правовые аспекты // Уголовное право. 2018. № 3. С. 86—92.

22. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: федеральный закон от 31 июля 2020 г. № 258-ФЗ // Собрание законодательства РФ. 2020. № 31. Ч. I, ст. 5017.

23. Макарейко Н. В. Проблемы юридической ответственности государства // Вестник Нижегородского университета имени Н. И. Лобачевского. 2019. № 5. С. 137—142.

24. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства РФ. 2017. № 31. Ч. I, ст. 4736.

References

1. Beck W. Risk society. On the way to another modernity. Moscow: Progress-Tradition Publ., 2000. 381 p. (In Russ.)
2. Legal technique: yearbook, no. 13. Risks in law-making, law enforcement, legal science: the technique of formation and functioning of the management system, 2019. 794 p. (In Russ.)
3. Orlenko V. Administrative and legal risks in the implementation of medical activities. *Administrative law*, 2018, no. 1, pp. 79—88. (In Russ.)
4. Timofeev I. V. Risks of medical care: constitutional and legal aspect. *Constitutional and municipal law*, 2017, no. 8, pp. 39—46. (In Russ.)
5. Nuremberg Code. *Doctor*, 1993, no. 7. (In Russ.)
6. Declaration of Helsinki of the World Medical Association. Ethical principles for conducting medical research involving a person as a subject: adopted in Helsinki in June 1964 at the 18th WMA General Assembly.

URL: <http://acto-russia.org>. (accessed 27.01.2022). (In Russ.)

7. Convention for the Protection of Human Rights and Human Dignity in Connection with the Application of Biology and Medicine: convention on Human Rights and Biomedicine (ETS no. 164): concluded in Oviedo on April 4, 1997. Access from the reference legal system "ConsultantPlus" (accessed 27.01.2022). (In Russ.)

8. On the basics of protecting the health of citizens in the Russian Federation: federal law no. 323-FZ of November 21, 2011. *Collection of legislative acts of the RF*, 2011, no. 48, art. 6724. (In Russ.)

9. On the approval of the Regulations on the federal state control (supervision) of the quality and safety of medical activities: decree of the Government of the Russian Federation no. 1048 of June 29, 2021. URL: <http://pravo.gov.ru> (accessed 27.01.2022). (In Russ.)

10. On the Strategy for the Development of the Information Society in the Russian Federation for 2017—2030: decree of the President of the Russian Federation no. 203 of May 9, 2017. *Collection of legislative acts of the RF*, 2017, no. 20, art. 2901. (In Russ.)

11. Stefanova N. A., Andronova I. V. Problems of digitalization of the healthcare sector: Russian and foreign experience. *Bulletin of Samara University. Economics and Management*, 2018, vol. 9, no. 3, pp. 31—35. (In Russ.)

12. On the approval of the strategic direction in the field of digital transformation of healthcare: decree of the Government of the Russian Federation no. 3980-r of December 29, 2021. URL: <http://pravo.gov.ru>, 12/31/2021 (accessed 27.01.2022). (In Russ.)

13. Govorukhina Yu. V. Strategy as a legal document. Dissertation... candidate of legal sciences. N. Novgorod, 2021. 31 p. (In Russ.)

14. On approval of the strategic direction in the field of digital transformation of public administration: order of the Government of the Russian Federation no. 2998-r of October 22, 2021. *Collection of legislative acts of the RF*, 2021, no. 44, part III, art. 7467. (In Russ.)

15. On the approval of the program "Digital Economy of the Russian Federation": decree of the Government of the Russian Federation no. 1632-r of July 28, 2017. *Collection of legislative acts of the RF*, 2017, no. 32, art. 5138. (In Russ.)

16. On the invalidation of the Decree of the Government of the Russian Federation no. 1632-r of July 28, 2017: decree of the Government of the Russian Federation no. 195-r of February 12, 2019. *Collection of legislative acts of the RF*, 2019, no. 8, art. 803. (In Russ.)

17. Kayumova A. R. Protection of human rights in the context of the application of modern biotechnologies: some problems. *Lawyer*, 2019, no. 1, pp. 64—71. (In Russ.)

18. Code of professional ethics of a doctor of the Russian Federation: adopted by the First National Congress of Physicians of the Russian Federation on October 5,

2012 (the document was not published). Access from the reference legal system "ConsultantPlus" (accessed 27.01.2022). (In Russ.)

19. Baranova M. V. Anticipatory lawmaking in the modern legal system. *Bulletin of the Saratov State Law Academy*, 2016, no. 1 (108), pp. 43—45. (In Russ.)

20. Varyushin M. S. Legal regulation of telemedicine in Russia and the EU: two steps forward and one back. *Law*, 2018, no. 1, pp. 165—174. (In Russ.)

21. Pikurov N. I. Risks of Medical Intervention: Criminal Law Aspects. *Criminal Law*, 2018, no. 3, pp. 86—92. (In Russ.)

22. On experimental legal regimes in the field of digital innovation in the Russian Federation: federal law no. 258-FZ of July 31, 2020. *Collection of legislative acts of the RF*, 2020, no. 31, part I, art. 5017. (In Russ.)

23. Makareiko N. V. Problems of legal responsibility of the state. *Bulletin of the Nizhny Novgorod University named after N. I. Lobachevsky*, 2019, no. 5, pp. 137—142. (In Russ.)

24. On the security of the critical information infrastructure of the Russian Federation: federal law no. 187-FZ of July 26, 2017. *Collection of legislative acts of the RF*, 2017, no. 3, part I, art. 4736. (In Russ.)

Информация об авторе

Н. В. Макарейко — доктор юридических наук, доцент.

Information about the author

N. V. Makareyko — Doctor of Law, Associate Professor.

Статья поступила в редакцию 31.01.2022; одобрена после рецензирования 25.02.2022; принята к публикации 10.03.2022.

The article was submitted 31.01.2022; approved after reviewing 25.02.2022; accepted for publication 10.03.2022.