

ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА К УГОЛОВНО-ПРАВОВОМУ ОБЕСПЕЧЕНИЮ ЦИФРОВЫХ ТЕХНОЛОГИЙ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ

Аннотация. В статье отмечается, что риск-ориентированный подход к уголовно-правовому обеспечению цифровых технологий в системе здравоохранения является новым направлением. Благодаря применению риск-ориентированного подхода можно выявить и систематизировать криминогенные риски, возникающие в процессе цифровизации медицины, объективно оценить реальную и потенциальную эффективность действующего уголовного законодательства в противодействии цифровым угрозам здравоохранению, а также сформировать научно обоснованные модели установления, изменения, дифференциации и унификации уголовной ответственности за преступления, посягающие на цифровую безопасность системы здравоохранения. Уровень криминализации соответствующих деяний должен напрямую коррелироваться с криминогенным потенциалом факторов риска и тяжестью негативных последствий применения цифровых технологий в медицинской сфере. Используя риск-ориентированный подход, представлена система управления рисками незаконного оборота цифровых технологий в системе здравоохранения. Разработана научно обоснованная типология криминогенных рисков, связанных с оборотом цифровых технологий в системе здравоохранения, построенная с учётом различного субъектного состава участников правоотношений. Выявлены и систематизированы криминогенные риски оборота цифровых технологий в системе здравоохранения, объединённые в три основные группы в зависимости от вида применяемых технологий.

Ключевые слова: криминальные угрозы; криминогенные риски; риск-ориентированный подход в уголовном законодательстве; цифровая трансформация

Для цитирования: Шутова А. А. Применение риск-ориентированного подхода к уголовно-правовому обеспечению цифровых технологий системы здравоохранения // Проблемы права. 2026. № 1 (101). С. 156–165. DOI: 10.24412/2075-7913-2026-1(101)-156-165

APPLICATION OF A RISK-BASED APPROACH TO THE LEGAL PROVISION OF DIGITAL TECHNOLOGIES IN THE HEALTHCARE SYSTEM

Abstract. The article notes that a risk-based approach to the criminal law provision of digital technologies in the healthcare system is a new direction. Thanks to its application, it is possible to identify and systematize criminogenic risks arising in the process of digitalization of medicine, objectively assess the real and potential effectiveness of current criminal legislation in countering digital threats to healthcare, as well as form scientifically sound models for the establishment, modification, differentiation and unification of criminal liability for crimes encroaching on digital the safety of the health system. The level of criminalization of the relevant acts should be directly correlated with the criminogenic potential of risk factors and the severity of the negative consequences of

the use of digital technologies in the medical field. Using a risk-based approach, a system for managing the risks of illicit trafficking in digital technologies in the health system is presented. A scientifically based typology of criminogenic risks associated with the turnover of digital technologies in the healthcare system has been developed, taking into account the different subject composition of participants in legal relations. Criminogenic risks of digital technology turnover in the healthcare system have been identified and systematized, grouped into three main groups depending on the type of technology used.

Keywords: criminal threats; criminogenic risks; risk-based approach in criminal legislation; digital transformation

For citation: Shutova A. A. Application of a Risk-Based Approach to the Legal Provision of Digital Technologies in the Healthcare System. *Problemy prava (Issues of Law)*. 2026. No. 1 (101). P. 156–165. DOI: 10.24412/2075-7913-2026-1(101)-156-165

Технологический императив будет определять будущее человечества, при этом нельзя не отметить порождаемые им потенциальные риски, которые требуют научного осмысления и формирования правовых решений [1]. Медицина является той отраслью, которая тотально подвержена цифровизации и внедрению цифровых технологий. В силу достаточно нового характера цифровых технологий в системе здравоохранения можно обозначить их способность причинить вред человеку, обществу и государству в целом, а также самой отрасли, подорвать ее авторитет и снизить доверие граждан к ней. В силу изначального рискованного характера здравоохранения, в особенности экспериментальной медицины, с учетом нового характера цифровых технологий, важным направлением является выявление возможных рисков. Сказанное формирует повестку выявления рисков, детерминированных внедрением цифровых технологий в системе здравоохранения, и актуализирует вопросы оценки готовности уголовно-правовых норм противодействовать угрозам.

О необходимости оценки рисков в условиях постоянного развития технологий искусственного интеллекта и робототехники отмечается в Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года, утвержденной распоряжением Правительства Российской Федерации от 19 августа 2020 г. № 2129-р [2]. При этом термин «риск» и словосочетание «риск-ориентированный подход» употребляются в представленном документе 14 раз, что подтверждает отношение законодателя к цифровой технологии как к рискогенному фактору. Также указывается, что должна проводиться оценка риска причинения

вреда жизни и здоровью человека искусственным интеллектом, оценка размера потенциального вреда ценностям, принятие мер по минимизации рисков; использование риск-ориентированного подхода при правовом регулировании отношений.

Значительное внимание в нормативных правовых актах уделяется применению риск-ориентированного подхода, основанного на оценке размера потенциального вреда ценностям с учетом вероятности его наступления по сравнению с возможным положительным эффектом от внедрения технологий искусственного интеллекта, необходимости принятия мер по минимизации соответствующих рисков [2].

В России с 2015 года риск-ориентированный подход демонстрирует положительные результаты в контрольно-надзорной деятельности [3], а поэтому представляет значительный интерес для научного исследования. Специалисты исследуют проблемы безопасности при использовании цифровых технологий в системе здравоохранения [4, 5]. Оценить общественную опасность цифровых технологий в здравоохранении только посредством права проблематично, имеется потребность в применении междисциплинарного подхода, позволяющего проникнуть в их содержание.

Идея применения риск-ориентированного подхода применительно к технологиям искусственного интеллекта нашла отражение в резолюции Европарламента «Нормы гражданского права в робототехнике» 2017 года [6] и в Регламенте Европейского союза об искусственном интеллекте, устанавливающего согласованные правила в отношении искусственного интеллекта [7], в которых предложена классификация систем искусственно-



го интеллекта, основанная на оценке уровня риска их применения (с неприемлемо высоким, высоким, ограниченным и минимальным риском).

Вопросы применения риск-ориентированного подхода поднимаются среди специалистов в области уголовного права и криминологии. Так, риск-ориентированный подход был поддержан И. Р. Бегишевым, который применил его к робототехнике [8]. Риск-ориентированный подход используется при установлении причинной связи по делам о халатности [9], в целях противодействия легализации (отмыванию) доходов, полученных преступным путем [10]. Однако не выработан единый понятийно-категориальный аппарат, который необходим для построения системы управления рисками. При этом создание и применение цифровых технологий в системе здравоохранения требует системного подхода к закреплению правовых гарантий ее защиты. В качестве нормативной основы построения системы допустимо использовать риск-ориентированный подход, предполагающий регулирование тех сфер общественных отношений, в которых риски наиболее распространены. Оценка уровня основных рисков позволяет выстроить программу формирования необходимого правового регулирования и уголовно-правового воздействия, направленных на предотвращение рисков. По мнению А. Ю. Чуриковой, использование риск-ориентированного подхода для нормативного регулирования использования искусственного интеллекта может способствовать достижению искомого баланса [11. С. 209].

Используя риск-ориентированный подход, можно представить систему управления рисками незаконного оборота цифровых технологий в системе здравоохранения, которая будет состоять из следующих последовательных этапов:

1. Выявления, анализа и дифференциации всех криминогенных рисков, с которыми сопряжен незаконный оборот цифровых технологий в системе здравоохранения.

2. Оценки уровня риска при незаконном обороте цифровых технологий в системе здравоохранения на основе общественной опасности.

3. Выявления правовых способов, в том числе уголовно-правовых средств, направленных на устранение, минимизацию и предупреждение рисков.

Представленная система позволит уточнить риски (модели уязвимости) на основе основных направлений применения цифровых технологий в системе здравоохранения и определить, как можно ими злоупотребить. Несомненно, основное предназначение представленной системы состоит в предупреждении и минимизации подобных рисков. Необходимо подчеркнуть потенциал цифровой технологии как криминогенного явления как с точки зрения увеличения масштабов существующих преступлений, так и с точки зрения содействия новым цифровым правонарушениям. Изучение опасностей создания и применения цифровых технологий позволит детально продумать механизм регулирования общественных отношений и уголовно-правового обеспечения цифровой безопасности системы здравоохранения.

Формирование системы управления рисками незаконного оборота цифровых технологий в системе здравоохранения осложняет отсутствие в законодательстве и в доктрине единого понятийно-категориального аппарата, который необходим для построения указанной системы.

Отметим, что в законодательстве указывается на необходимость определения рисков, предотвращении вреда и их минимизации. Подобные законодательные подходы являются подтверждением тому, что криминогенные риски незаконного оборота цифровых технологий в системе здравоохранения очевидны и игнорировать их опасность уже невозможно. Так, в статье 41 постановления Правительства Российской Федерации от 9 декабря 2022 г. № 2276 [12] названы причины рисков причинения вреда жизни и здоровью пациента:

- а) назначение неправильного лечения лечащим врачом вследствие низкой диагностической ценности данных, полученных из устройства по причине некорректной работы устройства;

- б) непоступление сигнальной информации по причине сбоя в работе информационной платформы;

- в) сбой в работе информационной платформы, который может привести к приостановке оборота данных устройств;

- г) поломка мобильного устройства пациента, на котором было установлено сопряженное с информационной платформой мобильное приложение, позволяю-



щее осуществлять передачу данных в автоматическом и ручном режимах.

В представленном документе обращается внимание на то, что в ходе реализации экспериментального правового режима могут возникать риски утечки персональных данных пациентов и информации ограниченного доступа. Потенциально использование десятка тысяч рентгенологических исследований для обучения технологий искусственного интеллекта ставит под угрозу сохранность персональных данных пациентов. Медицинские роботы, основанные на искусственном интеллекте, являющиеся техническими устройствами, включающими электрические элементы, электронные блоки, а также механические, гидравлические или пневматические рабочие органы. Они выполнены из пластмасс, металлов и могут быть источниками вредных и/или опасных факторов, особенно при поломках, авариях [13. С. 8]. Создание и применение технологий искусственного интеллекта в системе здравоохранения помимо рисков причинения вреда жизни и здоровью пациента имеет потенциал к причинению вреда другим ценностям и благам, охраняемым уголовным законом.

Отнесение всех видов высокотехнологичной медицинской помощи, в том числе основанной на цифровых технологиях, к рискованным подтверждается тем, что все ПО, созданное с применением технологий искусственного интеллекта, относится к классу 3 потенциального риска (с самой высокой степенью риска) [14].

Отметим, что в доктрине имеется множество концепций феномена риска. В настоящее время ученые изучают правовые [15], криминальные, криминологические и уголовно-правовые риски при исследовании новых цифровых технологий. Нормативного закрепления дефиниции «правовой риск» в законодательстве не содержится. Под правовыми рисками понимается отсутствие надлежащего уровня правовой регламентации общественных отношений.

Длительное время проблемами риска занимались в основном ученые-цивилисты, однако в связи с трансформацией общественных отношений в условиях цифровизации вопросы риска заинтересовали и ученых уголовно-правовых дисциплин. В связи с этим поддерживаем точку зрения А. С. Некоза, полагающего то, что изучение уголовно-правовых яв-

лений не должно ограничиваться исследованием отечественного уголовного права, необходим широкий подход [16].

В уголовно-правовой науке феномен риска ранее рассматривался применительно к исследованию обстоятельства, исключающего преступность деяния в виде обоснованного риска. Однако затем фокус внимания специалистов был перемещен к исследованию уголовно-правового риска. Наибольший вклад в исследование уголовно-правового риска внес В. В. Бабурин [17], И. Р. Бегишев [8], В. Н. Воронин [18], А. В. Никифоров [19] и другие.

Рискология, являясь новой областью исследования, вызывает сложности в ее терминологическом понимании. Стоит поддержать мнение М. М. Бабаева, что достижения науки рискологии, в том числе «используемые методология, технологии и конкретные приемы исследования, могут быть с успехом использованы в интересах криминологии» [20. С. 104]. Значительный вклад в становление и развитие отечественной криминальной рискологии закладывают известные ученые — М. М. Бабаев и Ю. Е. Пудовочкин, выступающие идеологами формирования криминальной рискологии [21]. Однако пока исследование рисков является малоисследованным среди специалистов уголовно-правовой доктрины, что является заметным упущением. Рискология, в том числе ее новое проявление — криминальная рискология, явление достаточно новое, малоисследованное как в отечественной, так и в зарубежной науке, посвященной профилактике преступности [22. С. 516]. Мы поддерживаем мнение И. Р. Бегишева, что отсутствие фундаментальных знаний к исследованию понятия риска усложняет эффективность уголовно-правового регулирования [8. С. 187–188]. Вероятность риска — это вероятность причинения вреда. Риски тем значительнее, чем выше вероятность их реализации. Поэтому вопросы риска формируют механизмы установления уголовной ответственности. По мнению авторов, «риски, не взятые под контроль, оставленные на свободе, быстро разрастаются и превращаются в масштабные угрозы безопасности граждан, общества, государства» [23. С. 138]. Мы согласны с тем, что, «в контексте уголовной политики и криминологии данная формула должна звучать так: риск — это возможная криминогенная опасность» [23. С. 138].



Возможная опасность (риск) и собственно опасность отличаются друг от друга: первая — это потенциал, нереализованная, но реальная, то есть существующая, угроза. Действительная опасность есть реализованный риск, как прямая угроза охраняемым законом ценностям, стоящая «в шаге» от события (факта), который принято называть общественно опасным и реагировать на него соответствующим образом в рамках решения задач криминализации. Или же в шаге от деяния, уже признанного преступлением [20. С. 106].

Следовательно, реализованный риск, трансформировавшийся из возможной криминогенной опасности в реальную угрозу охраняемым законом ценностям, поднимает вопросы о его юридической оценке (деяние правомерное или противоправное). Юридическое значение риск приобретает в случае, если отклонение носит негативный характер и порождает угрозу наступления (или реальное наступление) негативных последствий для личности, общества и (или) государства [24. С. 516]. Указанный риск может стоять «в шаге» от общественно опасного события (факта) и реагировать на него соответствующим образом (когда деяние еще является правомерным и не признано преступлением), или же в шаге от деяния, уже признанного преступлением [20. С. 106].

Какие-то риски могут исчезнуть, однако какие-то возможные опасности могут стать реальной угрозой очень быстро, что может привести к негативным последствиям, однако при этом правовые средства для реагирования на них, в том числе уголовно-правовые, будут отсутствовать. Однако законотворческие органы не всегда могут своевременно и адекватно отреагировать на такую метаморфозу. В связи с этим оценка рисков является важным объектом воздействия уголовно-политических решений. При этом акторы уголовной политики должны учитывать потенциал криминогенности каждого фактора риска. Деяние не будет криминализировано, если продуцирующий его фактор демонстрирует низкий потенциал криминогенности при принятии решения о признании деяния преступным и наказуемым.

Рассматривая риск как возможную опасность, предлагаем использовать словосочетание «криминогенный риск» как порождающий преступления и содер-

жащий в себе потенциал некоторого негативного события. При определенных обстоятельствах в перспективе криминогенный риск может быть превращен в реальную угрозу — стать уже криминальной полномасштабной угрозой, за которую как может быть установлена уголовная ответственность, так и будет осуществлена деятельность по признанию деяния общественно опасным и какой-либо реакции на него в рамках решения задач криминализации (путем введения новых или расширения имеющихся составов преступлений). Поэтому категории «риск» и «угроза» рассматриваются как частично совпадающие, но и имеющие различия в связи с тем, что риск охватывает вероятность наступления не только негативных, но и позитивных последствий [11. С. 267].

С. А. Меркунцов и М. П. Вассмер выделяют юридические риски (связанные с текстом уголовного закона и его применением на практике) и социальные уголовно-правовые риски (риски, порождающие уголовный закон) [25. С. 240]. В свою очередь В. Н. Воронин предложил ввести в механизм правового регулирования новый термин «уголовно-правовой риск» как «правовую оценку тех негативных последствий, которые наступают в результате рискованного поведения лица» [26. С. 198].

В контексте исследования уделим внимание тем криминогенным рискам, содержащим в себе возможность негативного развития с перспективой превращения при благоприятных условиях в полномасштабную криминальную угрозу. Наиболее вредоносная ипостась рискологии — это возможная криминогенная опасность [27]. По мнению Л. А. Букалевой, В. Ф. Лапшина и А. В. Остроушко, риски могут проявляться с разной степенью интенсивности и порождать тяжкие последствия [24. С. 79].

Обосновано, что применение риск-ориентированного подхода к уголовно-правовому обеспечению цифровой безопасности системы здравоохранения, который позволяет не только выявить и систематизировать криминогенные риски, возникающие в процессе цифровизации медицины, объективно оценить реальную и потенциальную эффективность действующего уголовного законодательства в противодействии цифровым угрозам здравоохранению, но и сформировать научно обоснованные модели

установления, изменения, дифференциации и унификации уголовной ответственности за преступления, посягающие на цифровую безопасность системы здравоохранения, при этом установлено, что уровень криминализации соответствующих деяний должен напрямую коррелироваться с криминогенным потенциалом факторов риска и тяжестью негативных последствий применения цифровых технологий в медицинской сфере, что обеспечивает соблюдение принципов обоснованности, системности и соразмерности уголовно-правового регулирования, создает необходимые предпосылки для гибкой адаптации уголовного законодательства к динамично изменяющимся условиям цифровой трансформации здравоохранения и формирует оптимальный баланс между необходимостью защиты общественных отношений и недопустимостью избыточной криминализации в сфере применения инновационных медицинских технологий.

Разработана научно обоснованная типология криминогенных рисков, связанных с оборотом цифровых технологий в системе здравоохранения, построенная с учётом различного субъектного состава участников правоотношений и включающая пять основных категорий: риски, исходящие от субъектов, занимающихся созданием (разработкой) медицинских изделий на основе цифровых технологий, обусловленные возможностью внедрения конструктивных дефектов, уязвимостей программного обеспечения или недостаточного тестирования; риски, исходящие от субъектов, занимающихся ремонтом (сервисным обслуживанием) медицинских изделий на основе цифровых технологий, связанные с нарушением технических регламентов и стандартов эксплуатации; риски, исходящие от медицинских работников в процессе применения (использования) медицинских изделий на основе цифровых технологий, детерминированные недостаточной квалификацией, халатностью или ненадлежащим исполнением профессиональных обязанностей; риски, исходящие из неправомерного поведения субъекта преступления, включающие умышленные противоправные действия, направленные на причинение вреда или извлечение незаконной выгоды; а также риски, исходящие от пациента, обусловленные нарушением медицинских рекомендаций или несанкционированным вмешательством в функ-

ционирование цифровых медицинских устройств, что позволяет комплексно идентифицировать потенциальные источники угроз цифровой безопасности здравоохранения, разработать дифференцированные меры уголовно-правового реагирования с учетом специфики каждой категории рисков и создать научную основу для формирования эффективной системы превенции рассматриваемых преступлений.

Выявлены и систематизированы криминогенные риски оборота цифровых технологий в системе здравоохранения, объединенные в три основные группы в зависимости от вида применяемых технологий: во-первых, криминогенные риски создания и применения технологий искусственного интеллекта в системе здравоохранения, включающие риски создания медицинского изделия на основе технологий искусственного интеллекта, связанные с возможностью заложения алгоритмических ошибок, некорректного обучения нейронных сетей и недостаточной валидации систем принятия решений, а также риски применения медицинского изделия на основе технологий искусственного интеллекта, обусловленные непрозрачностью процесса принятия решений, возможностью генерации ошибочных медицинских рекомендаций и проблемой распределения ответственности между разработчиком, медицинским работником и самой системой; во-вторых, криминогенные риски создания и применения технологий медицинской робототехники, охватывающие риски, действующие на медицинского робота извне и связанные с возможностью несанкционированного удаленного доступа, кибератак и внешних физических воздействий, риски, свойственные медицинскому роботу, детерминированные конструктивными особенностями, программными уязвимостями и техническими ограничениями робототехнических систем, а также риски, исходящие от медицинского робота [22], обусловленные возможностью причинения вреда пациенту вследствие технических сбоев, ошибок позиционирования или неадекватной реакции на нештатные ситуации; в-третьих, криминогенные риски, связанные с оборотом биопринтных технологий, включающие риски, связанные с оборотом 3D-биопринтера как технологического устройства, способного к созданию биологических структур, риски,



связанные с оборотом донорских клеток, обусловленные возможностью использования биоматериалов ненадлежащего качества, незаконного происхождения или с нарушением требований биобезопасности, риски, связанные с оборотом биочернил, детерминированные специфическими требованиями к составу, стерильности и биосовместимости материалов для биопечати, риски, связанные с оборотом биопринтных тканевых (органных) конструктов, включающие угрозы функциональной несостоятельности, иммунологической несовместимости и возможности злоупотреблений при трансплантации искусственно созданных биологических структур, а также риски, связанные с оборотом CAD-файла — цифро-

вого шаблона биопринтного тканевого (органного) конструкта, обусловленные возможностью несанкционированного копирования, модификации или использования цифровых моделей для создания дефектных или фальсифицированных биологических конструктов, что позволяет сформировать целостное представление о спектре криминогенных угроз, возникающих на различных этапах оборота инновационных медицинских технологий, разработать меры уголовно-правового противодействия с учетом специфики каждого вида цифровых технологий и создать научную основу для построения дифференцированной системы обеспечения цифровой безопасности системы здравоохранения.

Литература

1. Бегишев И. Р., Жарова А. К., Залоило М. В., Филипова И. А., Шутова А. А. Технологические трансформации: рост возможностей и правовой ответ на возникающие риски // *Journal of Digital Technologies and Law*. 2024. Т. 2, № 4. С. 735–740.
2. Распоряжение Правительства Российской Федерации от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // *Собрание законодательства Российской Федерации*. 2020. № 35. Ст. 5593.
3. Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» // *Собрание законодательства Российской Федерации*. 2008. № 51 (ч. I). Ст. 6249.
4. Begishev I., Shutova A., Gallese Ch., Dolgoplov K., Perepadya O., Ryabova L. Professional Communication between Patients and Doctors When Using Augmented Reality Technology // *2024 Communication Strategies in Digital Society Seminar (ComSDS)*, Санкт-Петербург, 10 апреля 2024 года. Vol. 2024. Санкт-Петербург: IEEE, 2024. P. 13–15.
5. Begishev I., Shutova A., Akhmetshin E., Denisovich V., Latypova E., Gilmanov R. Digital Twins in Healthcare System: Communication between Society and Law // *2024 Communication Strategies in Digital Society Seminar (ComSDS)*, Санкт-Петербург, 10 апреля 2024 года. Vol. 2024. Санкт-Петербург: IEEE, 2024. P. 9–12.
6. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата обращения: 28.02.2026).
7. Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года, устанавливающий гармонизированные правила в отношении искусственного интеллекта и вносящий поправки в Регламенты (ЕС) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и Директивы 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Закон об искусственном интеллекте). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата обращения: 28.08.2025).
8. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // *Правоприменение*. 2021. Т. 5, № 1. С. 185–201. DOI 10.52468/2542-1514.2021.5(1).185-201. EDN TBUVGY.
9. Щепельков В. Ф., Векленко В. В., Пряхина Н. И. Риск-ориентированный подход при установлении причинной связи по делам о халатности // *Юридическая наука и практика: Вестник Нижегородской академии МВД России*. 2018. № 4 (44). С. 348–353.
10. Филатова И. В. Применение риск-ориентированного подхода в целях противодействия легализации (отмыванию) доходов, полученных преступным путем // *Вестник Московского университета МВД России*. 2019. № 1. С. 233–236.
11. Чурикова А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование: дисс. ... докт. юрид. наук. Саратов, 2024. 498 с.



12. Постановление Правительства Российской Федерации от 9 декабря 2022 г. № 2276 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности с применением технологий сбора и обработки сведений о состоянии здоровья и диагнозов граждан в отношении реализации инициативы социально-экономического развития Российской Федерации «Персональные медицинские помощники» // Собрание законодательства Российской Федерации. 2022. № 51. Ст. 9237.
13. Денисов Э. И. Роботы, искусственный интеллект, дополненная и виртуальная реальность: этические, правовые и гигиенические проблемы // Гигиена и санитария. 2019. № 98(1). С. 5–10.
14. Приказ Минздрава Приказа Министерства здравоохранения Российской Федерации от 6 июня 2012 г. № 4н «Об утверждении номенклатурной классификации медицинских изделий» // Российская газета, 2012, 24 октября.
15. Макарейко Н. В. Правовые риски цифровизации оказания медицинской помощи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 1 (57). С. 67–74.
16. Некоз А. С. Рецензия на книгу: «KAI AMBOS, ANTONY DUFF, JULIAN ROBERTS AND THOMAS WEIGEND (EDS.), CORE CONCEPTS IN CRIMINAL LAW AND CRIMINAL JUSTICE: VOLUME I, CAMBRIDGE UNIVERSITY PRESS, 2020» // Гуманитарные, социально-экономические и общественные науки. 2022. № 8. С. 102–103.
17. Бабуринов В. В. Риск как основание дифференциации уголовной ответственности: автореф. дис. ... д-ра юрид. наук. Омск, 2009. 39 с.
18. Воронин В. Н. Уголовно-правовые риски развития цифровых технологий: постановка проблемы и методы научного исследования // Вестник Университета имени О. Е. Кутафина. 2018. № 12 (52). С. 73–80.
19. Никифоров А. В. Уголовно-правовые риски налогового агента: автореф. дис. ... канд. юрид. наук. М., 2014. 28 с.
20. Бабаев М. М. Риски как компонент детерминационного комплекса преступности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 1 (41). С. 104–110.
21. Бабаев М. М. Очерки криминальной рискологии / М. М. Бабаев, Ю. Е. Пудовочкин; Российский государственный университет правосудия. Москва: Издательство «Юрлитинформ», 2021. 368 с. (Уголовное право). ISBN 978-5-4396-2129-3. — EDN REAMFT.
22. Шутова А. А. Незаконное применение медицинских роботов: уголовно-правовая оценка и криминологические риски // Вестник Удмуртского университета. Серия Экономика и право. 2021. Т. 31, № 3. С. 515–521.
23. Бабаев М. М., Пудовочкин Ю. Е. Феномен риска в контексте профилактической политики (криминальная рискология) // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10. № 1. С. 136–148.
24. Букалерева Л. А., Лапшин В. Ф., Остроушко А. В. Риск-ориентированный подход в области правового регулирования обеспечения информационной безопасности несовершеннолетних // Вестник Сургутского государственного университета. 2021. № 1. С. 76–83.
25. Маркунцов С. А., Вассмер М. П. Об уголовно-правовых рисках и системе преступлений в сфере антикоррупционного комплаенса // Всероссийский криминологический журнал. 2021. Т. 15, № 2. С. 238–247.
26. Воронин В. Н. Понятие «уголовно-правовой риск» в социологии уголовного права: опыт теоретического осмысления // Вестник Университета имени О. Е. Кутафина. 2024. № 4 (117). С. 188–200.
27. Бабаев М. М. Риски законотворчества и противоречия уголовной политики // Общество и право. 2020. Вып. 2 (72). С. 8–14.

References

1. Begishev I. R., Zharova A. K., Zaloilo M. V., Filipova I. A., Shutova A. A. Technological transformations: growth of opportunities and legal response to emerging risks // Journal of Digital Technologies and Law. 2024. Vol. 2, No. 4. pp. 735–740.
2. Decree of the Government of the Russian Federation Dated August 19, 2020, No. 2129-r “On approval of the Concept for the Development of Regulation of relations in the field of artificial intelligence and robotics technologies until 2024” // Collection of Legislation of the Russian Federation. 2020. No. 35. Art. 5593.
3. Federal Law No. 294-FZ of December 26, 2008 “On the Protection of the Rights of Legal Entities and Individual Entrepreneurs in the exercise of State Control (Supervision) and Municipal Control” // Collection of Legislation of the Russian Federation. 2008. No. 51 (part I). Art. 6249.
4. Begishev I., Shutova A., Gallese Ch., Dolgoplov K., Perepadya O., Ryabova L. Professional Communication between Patients and Doctors When Using Augmented Reality Technology // 2024 Communication Strategies in Digital Society





Seminar (ComSDS), St. Petersburg, April 10, 2024. Vol. 2024. St. Petersburg: IEEE, 2024. P. 13–15.

5. Begishev I., Shutova A., Akhmetshin E., Denisovich V., Latypova E., Gilmanov R. Digital Twins in Healthcare System: Communication between Society and Law // 2024 Communication Strategies in Digital Society Seminar (ComSDS), St. Petersburg, April 10, 2024. Vol. 2024. Saint Petersburg: IEEE, 2024. P. 9–12.

6. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (date of request: 02/28/2026).

7. Regulation (EC) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EC) No 167/2013, (EC) No 168/2013, (EC) 2018/858, (EC) 2018/1139 and (EC) 2019/2144 and Directives 2014/90/EC, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Law). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (date of request: 08/28/2025).

8. Begishev I. R. Criminological classification of robots: a risk-oriented approach // Law enforcement. 2021. Vol. 5, No. 1. pp. 185–201. DOI 10.52468/2542-1514.2021.5(1).185-201. EDN TBUVGY.

9. Shchepelkov V. F., Veklenko V. V., Pryakhina N. I. Risk-based approach in establishing causality in cases of negligence // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2018. No. 4 (44). pp. 348–353.

10. Filatova I. V. The use of a risk-based approach in countering the legalization (laundering) of proceeds from crime // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2019. No. 1. pp. 233–236.

11. Churikova A. Y. The use of information technologies and systems in criminal proceedings: opportunities, risks, legal regulation: diss. ... doct. jurid. sciences'. Saratov, 2024. 498 p.

12. Decree of the Government of the Russian Federation No. 2276 dated December 9, 2022 "On the Establishment of an Experimental Legal Regime in the field of digital Innovations and Approval of the Program of an Experimental Legal Regime in the field of Digital Innovations in the field of medical activity using technologies for collecting and processing information about the state of health and diagnoses of Citizens in relation to the implementation of the initiative of the socialEconomic development of the Russian Federation "Personal medical assistants" // Collection of legislation of the Russian Federation. 2022. No. 51. Article 9237.

13. Denisov E. I. Robots, artificial intelligence, augmented and virtual reality: ethical, legal and hygienic problems // Hygiene and sanitation. 2019. No. 98(1). pp. 5–10.

14. Order of the Ministry of Health Order of the Ministry of Health of the Russian Federation dated June 6, 2012 No. 4n "On approval of the nomenclature classification of medical devices // Rossiyskaya Gazeta, 2012, October 24.

15. Makareiko 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.

16. Nekoz A. S. Book review: "KAI AMBOS, ANTONY DUFF, JULIAN ROBERTS AND THOMAS WEIGEND (EDS.), CORE CONCEPTS IN CRIMINAL LAW AND CRIMINAL JUSTICE: VOLUME I, CAMBRIDGE UNIVERSITY PRESS, 2020" // Humanities, socio-economic and Social Sciences. 2022. No. 8. pp. 102–103.

17. Baburin V. V. Risk as a basis for differentiation of criminal responsibility: an auto-ref. dis. ... Dr. jurid. sciences'. Omsk, 2009. 39 p.

18. Voronin V. N. Criminal law risks of the development of digital technologies: problem statement and methods of scientific research // Bulletin of the O. E. Kutafin University. 2018. No. 12 (52). pp. 73–80.

19. Nikiforov A. V. Criminal law risks of a tax agent: abstract of the dissertation of the candidate. jurid. nauk. M., 2014. 28 p.

20. Babaev M. M. Risks as a component of the determinative complex of crime // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2018. № . 1 (41). C. 104–110.

21. Babaev M. M. Essays on criminal risk / M. M. Babaev, Y. E. Pudovochkin; Russian State University of Justice. Moscow: Yurлитinform Publishing House, 2021. 368 p. (Criminal Law). ISBN 978-5-4396-2129-3. — EDN REAMFT.

22. Shutova A. A. Illegal use of medical robots: criminal and legal assessment and criminological risks // Bulletin of the Udmurt University. Economics and Law series. 2021. Vol. 31, No. 3. pp. 515–521.

23. Babaev M. M., Pudovochkin Yu. E. The phenomenon of risk in the context of occupational policy (criminal riskology) // Bulletin of St. Petersburg University. Right. 2019. Vol. 10. No. 1. pp. 136–148.

24. Bukalerova L. A., Lapshin V. F., Ostroushko A. V. Risk-oriented approach in the field of legal regulation of the information security of minors // Bulletin of Surgut State University. 2021. No. 1. pp. 76–83.

25. Markuntsov S. A., Vassmer M. P. On criminal law risks and the system of crimes in the field of anti-corruption compliance // All-Russian Journal of Criminology. 2021. Vol. 15, No. 2. pp. 238–247.
26. Voronin V. N. The concept of “criminal law risk” in the sociology of criminal law: the experience of theoretical understanding // Bulletin of the O. E. Kutafin University. 2024. No. 4 (117). pp. 188–200.
27. Babaev M. M. Risks of lawmaking and contradictions of criminal policy // Society and law. 2020. Issue 2 (72). pp. 8–14.

Сведения об авторе

Шутова Альбина Александровна, кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова.

E-mail: shutova1993@inbox.ru

Information about the author

Shutova Albina, Cand. Sci. (Law), Senior Researcher of the Institute of Digital Technologies and Law, Associate Professor, Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov.

E-mail: shutova1993@inbox.ru

Конфликт интересов отсутствует.
There is no conflict of interest.

Дата поступления статьи / Received: 18.03.2026

Дата рецензирования / Received: 19.03.2026

Дата принятия к опубликованию / Accepted: 20.03.2026

