ЦИФРОВАЯ БЕЗОПАСНОСТЬ / DIGITAL SECURITY

Редактор рубрики *И. Р. Бегишев* / Rubric editor *I. R. Begishev*

Научная статья **https://doi.org/10.21202/2782-2923.2023.3.571-585**

УДК 004.8:51:343

А. А. Шутова[1]

[1] *Казанский инновационный университет имени В. Г. Тимирясова, г. Казань, Россия*

Криминальные риски оборота медицинских роботов

Шутова Альбина Александровна, кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса, Казанский инновационный университет имени В. Г. Тимирясова
E-mail: shutova1993@inbox.ru
ORCID: https://orcid.org/0000-0003-3015-3684
Scopus Author ID: https://www.scopus.com/authid/detail.uri?origin=resultslist&authorId=57219032918
Web of Science Researcher ID: https://www.webofscience.com/wos/author/rid/GOG-9089-2022
eLIBRARY ID: SPIN-код: 5235-4319, AuthorID: 835100

Аннотация

Цель: выявление криминальных рисков, свойственных медицинскому роботу, с учетом его аппаратно-технологических (технологических и цифровых) особенностей, а также построение на основе данного анализа авторской классификации криминальных рисков и моделей уголовно-правовой охраны общественных отношений, возникающих в процессе оборота медицинских роботов.

Методы: в статье используются общенаучные методы познания (анализ, синтез, индукция, дедукция, классификация), а также частнонаучные методы познания, логико-юридический метод.

Результаты: уязвимость безопасности медицинских роботов вызывает серьезную озабоченность у производителей, программистов и тех, кто взаимодействует с ними в отрасли здравоохранения. В медицинских учреждениях роботы взаимодействуют в тесном контакте с детьми, пожилыми и людьми с ограниченными возможностями, и пациенту может быть неясно, работает ли робот должным образом или подвергается нападению. Любой вред, причиненный хирургическим роботом в результате неправомерного доступа (или иных противоправных действий), может подорвать веру общественности в медицину и в целом в систему здравоохранения. Угрозы безопасности медицинских роботов могут иметь дальнейшие негативные последствия для них самих, так как подобные факты неправомерного воздействия могут привести к тому, что роботы сломаются или нанесут вред другому близлежащему оборудованию, являющемуся имуществом данного учреждения системы здравоохранения, а хуже – жизни и здоровью пациентов или медицинским работникам. В связи с этим в работе выявлены криминальные риски и угрозы, свойственные медицинским роботам, сформулированы меры по совершенствованию уголовного законодательства, направленного на противодействие преступлениям, возникающим против законного оборота медицинских роботов (ст. 235[2] УК РФ).

Научная новизна: на данный момент имеется небольшое количество отечественных исследований, посвященных правовому регулированию и охране медицинских роботов. В основном подобные наработки являются результатом исследований ученых-медиков. Однако в Российской Федерации специальные теоретико-правовые исследования, в том числе посвященные изучению уголовно-правовых вопросов охраны указанных правоотношений, практически отсутствуют, что подтверждает актуальность и значимость проводимого нами исследования.
Практическая значимость: положения и выводы статьи могут использоваться для дальнейшего совершенствования уголовного законодательства, а также закладывают основу для дальнейших исследований в уголовно-правовой науке.

Ключевые слова
Искусственный интеллект, медицинский робот, медицинское изделие, ответственность, преступления, риск, робот, уголовное право, цифровизация, цифровые технологии

Как цитировать статью: Шутова, А. А. (2023). Криминальные риски оборота медицинских роботов. *Russian Journal of Economics and Law*, *17*(3), 571–585. (In Russ.). https://doi.org/10.21202/2782-2923.2023.3.571-585

Scientific article

A. A. Shutova[1]

[1] *Kazan Innovative University named after V. G. Timiryasov, Russia*

Criminal risks of medical robots turnover

Albina A. Shutova, Candidate of Juridical Sciences, Senior Researcher of Scientific-research Institute for digital technologies and law, Associate Professor of the department of Criminal Law and Procedure
E-mail: shutova1993@inbox.ru
ORCID: https://orcid.org/0000-0003-3015-3684
Scopus Author ID: https://www.scopus.com/authid/detail.uri?origin=resultslist&authorId=57219032918
Web of Science Researcher ID: https://www.webofscience.com/wos/author/rid/GOG-9089-2022
eLIBRARY ID: SPIN-код: 5235-4319, AuthorID: 835100

Abstract
Objective: to identify criminal risks inherent in a medical robot, taking into account its hardware-technological (technological and digital) features, and to construct, based on this analysis, the author's classification of criminal risks and models of criminal-legal protection of public relations arising in the medical robots' turnover.
Methods: the article uses general scientific (analysis, synthesis, induction, deduction, classification) and specific scientific methods of cognition, and the logical-legal method.
Results: The security vulnerability of medical robots causes serious concern in manufacturers, programmers and those interacting with the robots in the healthcare industry. In medical institutions, robots interact closely with children, the elderly and the disabled, and it may not be clear to the patient whether the robot is working properly or being attacked. Any harm caused by a surgical robot as a result of unauthorized access (or other illegal actions) can undermine the public's faith in medicine and in the healthcare system as a whole. Threats to the safety of medical robots can have further negative consequences for themselves, as such facts of unlawful influence can lead to robots breaking down or harming other nearby equipment that is the property of the healthcare institution, and worse – the life and health of patients or medical workers. In this regard, the paper identifies criminal risks and threats inherent in medical robots, and formulates measures to improve criminal legislation aimed at countering crimes arising against the legal turnover of medical robots (Article 235^2 of the Criminal Code of the Russian Federation).

Scientific novelty: at the moment there are few Russian studies devoted to the legal regulation and protection of medical robots. Basically, such researches are done by medical scientists. However, in the Russian Federation, there are practically no special theoretical-legal studies, including those devoted to the study of criminal law issues of the protection of these legal relations, which confirms the relevance and significance of our research.
Practical significance: the provisions and conclusions of the article can be used to further improve criminal legislation, and also lay the foundation for further research in criminal law science.

Keywords
Artificial intelligence, medical robot, medical device, liability, crimes, risk, robot, criminal law, digitalization, digital technologies

For citation: Shutova, A. A. (2023). Criminal risks of medical robots turnover. *Russian Journal of Economics and Law*, *17*(3), 571–585. (In Russ.). https://doi.org/10.21202/2782-2923.2023.3.571-585

Введение

Цифровая экономика характеризуется повсеместным внедрением робототехнических устройств во многие сферы общественной жизни. В связи с этим медицинское право также подвержено различным изменениям вследствие цифровизации общественных отношений (Записная, 2022, с. 34). По мнению исследователей, использование роботов в медицинских целях в объеме продаж сервисных роботов в мире составляет более 30 % и постоянно увеличивается (Карцхия, 2021, с. 40). Возможности медицинской робототехники, несомненно, велики. Роботы используются практически на всех уровнях системы здравоохранения: в малоинвазивной хирургии (например, роботизированной лапаротомии) и при менее инвазивных видах эндоскопических хирургических процедур (например, роботизированной бронхоскопии), при оптимизации работы больниц, протезировании, оказании помощи пациентам на дому. Медицинская робототехника – новая область здравоохранения, в которой экзоскелеты, роботы для ухода за пациентами и иные сервисные роботы находятся на ранней стадии развития, но имеют большой потенциал в применении. Медицинская робототехника – одна из передовых областей робототехники, но она сталкивается с длительными циклами разработки, строгими процессами регулирования и высокими техническими барьерами.

Этические и юридические барьеры, налагаемые на медицинских роботов, требуют тщательного рассмотрения, в том числе с точки зрения различных уровней автономии, киберустойчивости (Галлезе-Нобиле, 2023), а также возможности их использования (Weng & Hirata, 2022).

Действительно, со всеми новыми технологиями в законодательстве может быть много пробелов, поскольку правовые нормы не всегда могут опережать динамично развивающиеся технологические достижения. Стоит согласиться с зарубежными коллегами, считающими, что потенциальные риски должны быть выявлены на ранней стадии (Schmitz-Luhn & Chandler, 2022). Вопросы правового регулирования медицинской робототехники требуют обсуждения уже сейчас. В свою очередь зарубежные авторы активно исследуют вопросы наделения медицинских роботов автономностью и приходят к выводу, что медицина должна исключить полную автономию и допустить в качестве приемлемого подхода только автономию под наблюдением (Fiorini et al., 2022, p. 1011).

Стоит поддержать мнение авторов, полагающих, что развитие робототехники требует адекватного правового регулирования, способного спрогнозировать риски применения и предусмотреть меры ответственности в случае причинения вреда охраняемым интересам (Бабурин, 2010, с. 11). Неизбежно возникнет масса вопросов, связанных с юридической оценкой действий медицинских работников-хирургов, которые, находясь в одном городе, оперируют пациента в другом, и происходит промах скальпеля, порезавшего артерию, что вызывает серьезные медицинские осложнения или смерть пациента. В этом случае

напрашивается вопрос, является ли хирург причиняющим вред пациенту. Кроме того, в связи с большей автоматизацией медицинских роботов возникает вопрос и о том, что произойдет, если автономный робот допустит хирургическую ошибку. В свою очередь, в США против *Intuitive Surgical Inc*, производителя *Da Vinci*, были поданы иски, согласно которым компания недостаточно обучила хирургов перед использованием робота[1].

Технологии могут развиваться быстрее, чем нормативные и этические вопросы найдут свое отражение. Оценка рисков внедрения медицинской робототехники имеет решающее значение, для того чтобы избежать негативной реакции, которая препятствовала бы прогрессу. В связи с этим интересным представляется мнение зарубежных ученых, полагающих, что перед формированием правовой среды для роботов необходимо рассмотреть этические вопросы (Langman et al., 2021).

Целью представленного исследования является формирование на основе выявленных криминальных рисков, свойственных медицинским роботам, наиболее эффективной модели уголовно-правовой охраны общественных отношений, возникающих в процессе оборота медицинских роботов.

Именно поэтому в рамках настоящего исследования будут последовательно рассмотрены и решены следующие задачи:

– выявление криминальных рисков, свойственных медицинским роботам с учетом их аппаратно-технологической сущности;

– формирование их доктринальной классификации;

– исследование текущего состояния уголовно-правовой охраны общественных отношений, возникающих в процессе оборота медицинских роботов, и его совершенствование путем разработки эффективных моделей.

В настоящее время как никогда важно обозначить криминальные риски, свойственные медицинским роботам, поделив их на некоторые подгруппы (криминальные риски, действующие на робота, используемого в сфере здравоохранения, извне; криминальные риски, исходящие от медицинского робота; криминальные риски, свойственные роботизированным медицинским изделиям; криминальные риски цифровой безопасности медицинского робота), а также определить уголовно-правовые модели охраны медицинских роботов, которые могут быть использованы в правоприменении и совершенствовании законодательства.

Криминальные риски, свойственные медицинским роботам

Изучение возможных рисков и угроз в процессе оборота медицинских роботов позволит полно определить причинный комплекс, способствующий совершению преступлений, тем самым, по нашему мнению, повысит профилактический потенциал уголовно-правовых наук в целом. Стоит согласиться с мнением Ф. В. Цомартовой, что медицинские роботы могут быть весьма уязвимыми, а это может повлиять на их безопасность (Цомартова, 2020, с. 95).

Зарубежные исследователи активно изучают вопросы безопасности, защиты конфиденциальности социальных роботов, используемых в отрасли здравоохранения; а также факторы, исходящие от пациентов (Nissenbaum, 2001).

С самого зарождения робототехники люди осознавали тот факт, что роботы, помимо выполнения полезной работы, для которой они были созданы, могут также причинять вред людям, обществу и государству. Эта область регулировалась первыми тремя законами робототехники (Asimov, 2019), которые все еще актуальны и этически приемлемы для разработки проблемы правового регулирования медицинских роботов:

Первый закон. Медицинский робот не должен травмировать человека или своим бездействием допускать причинение вреда.

Второй закон. Медицинский робот должен подчиняться всем приказам (командам), отдаваемым ему людьми, если только такие приказы (команды) не противоречат Первому закону.

Третий закон. Медицинский робот должен поддерживать свое существование (защищать себя), если только это не противоречит Первому или Второму законам.

[1] Zdrav.Expert. Медтех-портал. https://zdrav.expert/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Intuitive_Surgical

Указанные законы робототехники применяются в первую очередь при проектировании и производстве роботов, но они не включают случаи, когда роботы используются не по их назначению или когда в работе робота возникает непреднамеренная ошибка.

Кроме того, в 2020 г. были предложены новые законы робототехники:

1) роботизированные системы и искусственный интеллект (далее – ИИ) должны дополнять профессионалов, а не заменять их;

2) роботизированные системы и ИИ не должны заменить человечество;

3) роботизированные системы и ИИ не должны усиливать гонку вооружений;

4) роботизированные системы и ИИ должны позволять определить личность своего создателя, контроллера и владельца [13].

Указанные законы, хотя и не являются конкретными, но отражают текущие тенденции внедрения роботов в мире. Законы не содержат ограничительных формулировок и не могут рассматриваться как элемент регулирования. С учетом изменений, уже наблюдаемых в этой области, вероятно, в будущем законы будут изменены.

К тому же предпринимаются успешные попытки исследовать медицинских нанороботов сквозь призму трех законов робототехники Айзека Азимова (Гуляева, 2023, с. 99).

Большинство из доступных в настоящее время роботизированных систем функционируют только как роботизированные вспомогательные средства, действуя как механизм для руководства процедурой или как защитный механизм для пациентов, предоставляя дополнительные функции. Наблюдается тенденция к еще большей автономии медицинских роботов. По мнению Е. С. Михалевой и Е. А. Шубиной, чем более автономен робот, тем сложнее определить ответственность субъекта, так как контроль оператора сводится к минимуму (Михалева, Шубина, 2019, с. 29).

Е. Е. Истратова и А. А. Молчанова считают, что наиболее критическими для медицинских роботов являются аспекты безопасности (в широком смысле – как физической, так и информационной) и защиты персональных данных (Истратова, Молчанов, 2015, с. 59).

В свою очередь медицинская услуга (медицинская помощь) состоит из нескольких этапов. Она начинается с диагностики состояния пациента и заканчивается прекращением послеоперационного лечения (его реабилитацией). Полагаем, что на любой из этих стадий может быть нанесен вред пациенту.

Криминальные риски, действующие на медицинского робота извне

Рассмотрим более подробно первую группу рисков, действующих на медицинского робота извне. Медицинские роботы подвержены различным влияниям окружающей среды в результате воздействия на них человека: ошибка в управлении (неправильное подключение); неправильное использование основных частей (модулей) медицинского робота; неправильная установка (задача) параметров (алгоритмов), хаотичные (непреднамеренные) действия пациентов, нарушение правил технического (технологического) обслуживания, ремонта робота, неправильная эксплуатация медицинским работником, неправомерный доступ злоумышленников.

В последние годы мы наблюдали последствия активизации программ-вымогателей в больницах; уязвимость программного обеспечения, используемого в работе кардиостимулятора; утечки данных пациентов. Многие злоумышленники могут оказывать преступное воздействие как на медицинского робота, так и в целом на информационную инфраструктуру учреждений системы здравоохранения.

Хирургические ошибки, которые могут варьироваться от неверных шагов, предпринятых хирургом или группой медицинских работников, или неправильной дозировки, данной пациенту, до хирургических материалов, оставленных в теле пациента, могут вызвать самые тяжелые осложнения.

Неправильная эксплуатация хирургического роботизированного оборудования также является существенным фактором травматизма пациентов. Более того, помимо правильного использования робота, поставщики медицинских услуг несут дополнительную обязанность заботиться о пациенте, информируя его о рисках, связанных с процедурой роботизированной помощи, и запрашивая согласие (Yew, 2021). Доктрина информированного согласия требует предоставления хирургом информации о риске конкретного заболевания и получения согласия до проведения процедуры. Возможны ошибки, возникающие из-за неправильного использования хирургического робота. Врач-хирург или члены его команды могут быть привлечены к ответственности за вред, вызванный такими ошибками. Так, к примеру, Гилмор МакКалла подал в суд на *Intuitive Surgery, Inc.*, утверждая, что робот стал причиной смерти его 24-летней дочери. Ей делали гистерэктомию

в августе 2010 г., когда робот вызвал ожоги артерии и кишечника. Дочь скончалась через две недели после операции. В иске утверждается, что робот обнажил провода, по которым проходит электрический ток, что могло вызвать электрическую дугу вокруг них. Также утверждает, что операторы не были должным образом обучены работе с роботами[2].

По мнению зарубежных ученых, хирургические роботы считаются системами, критически важными для безопасности, из-за потенциальных рисков для пациента (Alemzadeh et al., 2016). Были зафиксированы случаи оставления или попадания осколков оборудования в тела пациентов[3].

В свою очередь в отношении медицинских роботов могут быть совершены различные общественно опасные деяния, которые мы классифицируем по специфике их совершения:

Манипулятивные атаки, при которых злоумышленник тайно изменяет инструкции (алгоритмы) медицинского робота, для того чтобы добиться иного результата. При этом вводятся непреднамеренные пользовательские данные или команды управления крутящим моментом двигателя, для чего требуется доступ к главной консоли или управляющему программному обеспечению. Последствием этого сбоя могут быть непреднамеренные движения или полная остановка медицинского робота.

Подрыв управления. Злоумышленник вносит изменения в управление медицинским роботом. Это отличается от манипулирования, так как это может быть сделано в сети, из которой робот получает сигналы, и фокусируется на управлении, а не на манипулировании существующими действиями. В то время как первые два могут вызвать только задержки в движениях, последний полностью позволяет злоумышленнику делать все, что ему заблагорассудится, причиняя вред пациенту, больнице, ее имуществу.

Перепрограммирование. Тип доступа, необходимый для управления медицинским роботом, может также предоставлять доступ для изменения программного обеспечения. Состоит из изменений в программном обеспечении на любом уровне, серьезность таких сбоев для пациента или операции в целом достаточно велика.

Уязвимости программного обеспечения. Любая уязвимость, которую злоумышленник может использовать для совершения дальнейших атак, происходит пассивно и не обязательно вызвана виновным лицом, использующим уязвимости программного обеспечения.

Нарушение системы обратной связи. Злоумышленник тайно может модифицировать камеру или другие сенсорные данные, отправляемые хирургу. Сенсорные входы в настоящее время важны для того, чтобы показать, как проводится процедура внутри организма пациента, а также что в данный момент делает хирург. При изменении любого из них возрастает риск травмирования.

Криминальные риски, свойственные медицинскому роботу

В данную группу рисков следует отнести факторы, оказывающие влияние на функционирование медицинского робота (комплектность и качество материала, из которого изготовлены основные части (модули) медицинского робота). Существует не только возможность человеческой ошибки при работе с роботизированной технологией, но и дополнительный риск механического отказа. Несколько компонентов системы могут выйти из строя, включая камеру, бинокулярные линзы, роботизированную вышку, роботизированные руки и инструменты. Источник энергии может вызвать непреднамеренные внутренние ожоги от прижигающего устройства. Дуговой разряд возникает, когда электрический ток от роботизированного инструмента покидает роботизированную руку и направляется на окружающие ткани. Это может вызвать искры и ожоги, что приведет к повреждению тканей, которое не всегда можно сразу распознать.

Незаметные внутренние нарушения могут быть связаны с неисправностями хирургического инструмента, используемого для определенной операции (разрез, наложение шва), неисправностями роботизированной руки, к которой крепится какой-либо хирургический инструмент, что может привести к неточным движениям манипулятора, к неточности надреза и т. д., неисправностями консоли управления (панелью) роботом-манипулятором, ошибки в программном обеспечении и ошибки процессора.

---

[2] Langreth, R. (2013, March 6). Robosurgery Suits Detail Injuries as Death Reports Rise: Health. *Bloomberg*. https://www.bloomberg.com/news/articles/2013-03-05/robosurgery-suits-detail-injuries-as-death-reports-rise

[3] Almost 800 patients have had surgical instruments left INSIDE them after hospital procedures causing 16 deaths since 2005, says new health care report. (2013, October 18). *Mail Online*. https://www.dailymail.co.uk/news/article-2466049/Almost-800-patients-surgical-instruments-left-INSIDE-hospital-procedures-causing-16-deaths-2005-says-new-health-care-report.html

Ошибки программного обеспечения препятствуют обработке вводимых хирургом инструкций и преобразованию этих инструкций в движение хирургического инструмента через роботизированную руку. Следовательно, неточная обработка программным обеспечением вводимых инструкций или просчеты могут быть опасны для оперируемого пациента.

Полагаем, что для медицинских роботов, в том числе хирургических, недостаточно разработаны четкие стандарты, определяющие значение безопасности, точности и конкретных процедур для их оценки, в отличие от их промышленных аналогов и автономных транспортных средств. К примеру, такие стандарты, как IEC 60601 ГОСТ Р МЭК 60601-1-2010 [4], содержат рекомендации по определению степеней автономности медицинского оборудования, но они оценивают риска устройства, а не оценку риска при управлении им.

Криминальные риски, исходящие от медицинского робота

Риски (опасности), исходящие от медицинского робота, могут происходить даже при его нормальной работе.

Роботизированная медицина имеет множество рисков, включая возможность заражения инфекцией пациентов, приведение к кровотечению.

Существует не только возможность человеческой ошибки при работе с роботизированной технологией, но и дополнительный риск механического отказа. Несколько компонентов системы могут выйти из строя, включая камеру, бинокулярные линзы, роботизированную вышку, роботизированные руки и инструменты.

Источник энергии, склонный к возникновению электрической дуги, может вызвать непреднамеренные внутренние ожоги от прижигающего устройства. Дуговой разряд возникает, когда электрический ток от роботизированного инструмента покидает роботизированную руку и неправильно направляется на окружающие ткани. Подобное обстоятельство может вызвать искры и ожоги, что приведет к повреждению тканей, которое не всегда можно сразу распознать.

Существует небольшой риск временного и даже постоянного паралича нервов из-за экстремального положения тела, необходимого для стыковки робота и адекватного доступа к тазу для выполнения.

Сфера здравоохранения осложнена тем, что на качество проведения операции может повлиять множество факторов, в том числе: физиологические особенности пациента (ожирение и сопутствующие заболевания); особенности врача-хирурга (обучение и опыт); роботизированные факторы (например, механическая неисправность).

Однако нашему исследованию подлежат только риски и угрозы криминального характера, которые представляют собой виновно совершенные общественно опасные противоправные деяния, запрещенные УК РФ под угрозой наказания.

Криминальные риски цифровой безопасности медицинского робота

Наиболее критическими для медицинских роботов являются аспекты цифровой безопасности и защиты персональных данных. Зарубежные ученые уделяют особое внимание защите персональных данных в связи с активным применением роботов (Lutz et al., 2019). Если доступ к медицинским роботам будет получен, злоумышленником могут быть выполнены различные вредоносные действия. Они могут вызвать состояние отказа в обслуживании, чтобы нарушить работу больницы для вымогательства, а поскольку конфиденциальные данные пациентов передаются на устройства, использование уязвимостей может предоставить хакерам доступ к данным пациентов.

Роботам предоставляется привилегированный доступ к зонам ограниченного доступа в медицинских учреждениях, которые обычно закрыты для неуполномоченных лиц. Роботы могут открывать двери и получать доступ к лифтам, а также использоваться для блокирования доступа, отключения лифтов или столкновения с персоналом и пациентами. Поскольку у роботов есть встроенные камеры, их можно угнать и использовать для наблюдения. Роботы также потенциально могут быть захвачены и использованы для доставки вредоносного программного обеспечения или могут служить стартовой площадкой для более масштабных кибератак на больничные информационно-телекоммуникационные сети. Роботы могут быть модифицированы, чтобы

[4] Национальный стандарт РФ ГОСТ Р МЭК 60601-1-2010 «Изделия медицинские электрические. Часть 1. Общие требования безопасности с учетом основных функциональных характеристик» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 23 ноября 2010 г. № 492-ст). СПС «Гарант».

нести смертоносное оружие, или перепрограммированы для применения чрезмерной силы, что может привести как к человеческим, так и материальным потерям.

Так, производитель мобильных роботов *Aethon* в своих больничных роботах *Tug* описывал, что были обнаружены неисправности, которые в случае их использования могут позволить киберпреступникам удаленно управлять тысячами медицинских машин[5]. В свою очередь неправомерные действия могли повлечь наступление таких негативных последствий, как получение доступа к учетным данным пользователей и медицинским записям; блокировка лифтов и дверей; наблюдение за помещениями, в которых находятся пациенты; получение доступа к камерам в режиме реального времени и данным устройств; нарушение ухода за пациентами и порядка выдачи лекарств; запуск новых кибератак; столкновения с людьми и объектами, приводящие к смерти; использование уязвимостей, для того чтобы помешать пациентам получать, к примеру, лекарства.

Риски применения роботизированной медицинской помощи высоки еще и в связи с тем, что спектр применений и режимов роботизированных технологий в системе здравоохранения огромен, на данный момент услуги предоставляются широкому кругу лиц, контактирующих с системой, включая врачей и другой медицинский персонал, пациентов и лиц, осуществляющих уход.

Нарушение работы хирургического робота, как и любого другого инструмента, при прямом контакте с пациентом может привести к серьезному ущербу. Обеспокоенность кибербезопасностью других устройств, таких как имплантируемые кардиостимуляторы, привлекла всеобщее внимание[6]. В 2015 г. Боначи и его коллеги продемонстрировали техническую способность взять на себя управление роботизированной функцией в смоделированной среде, нарушая и переопределяя роботизированные функции. Совсем недавно было обнаружено несколько уязвимостей в роботах, используемых для доставки медикаментов в больницу (Осборн, 2022).

Интеграция источников данных, аппаратного обеспечения, программного обеспечения и сетей, необходимых для выполнения этих функций, создает новые уязвимости и может привести к атаке, которая способна масштабироваться на несколько роботов одновременно.

Журналы хирургических данных и видеозаписи пациентов также являются своеобразными точками атаки, взломы могут скомпрометировать конфиденциальные данные о работе конкретного хирурга или личную информацию о здоровье пациентов. Роботы зависят от более общей больничной инфраструктуры, такой как электроэнергия, которая может быть прервана.

Проводимые эксперименты свидетельствуют о том, что медицинские роботы имеют ряд уязвимостей и не защищены полностью, что может поставить под угрозу жизнь и здоровье пациентов. Так, ресурс *MIT Technology Review* сообщил, что ученые исследовали и провели анализ возможных атак кибербезопасности на *Raven II*. Специалисты сумели перехватить управление роботом и вынудили его выполнять нужные им команды (хаотичные движения), добились изменения их последовательности, в результате он перестал подчиняться оператору. На втором этапе эксперимента удалось получить контроль над действиями робота и оператор потерял контроль над устройством окончательно. Робот-хирург даже не отреагировал на команду к перезагрузке системы и продолжал выполнять действия[7].

Указанные обстоятельства позволяют сделать вывод о том, что игнорировать уязвимости и проблемы безопасности в медицинской сфере, особенно по мере того, как цифровое здравоохранение, персонализированная медицина и дистанционное лечение продолжают развиваться, явно не стоит.

Выделим следующие уязвимости, позволяющие виновным контролировать действия медицинского робота: фотографирование; «слежка» за больницей (или в больнице) в режиме реального времени через камеры, доступ к записям пациентов; нарушение или блокирование доставки лекарств, что может повлиять на уход за пациентами.

---

[5] Critical bug allows attacker to remotely control medical robot. (2022, 12 April). *The Register*. https://www.theregister.com/2022/04/12/critical_vuln_hospital_robots/

[6] Staynings, R. (2017, August 30). FDA announces first-ever recall of a medical device due to cyber risk. *Cisco blogs*. https://blogs.cisco.com/healthcare/fda-announces-first-ever-recall-of-a-medical-device-due-to-cyber-risk

[7] Ученые выявили возможность хакерских атак на медицинских роботов. (2015, 1 мая). *Техкульт*. https://www.techcult.ru/robots/2277-ataki-na-medicinskih-robotov

Особенности программного обеспечения (аппаратной части) медицинского робота, в том числе некоторые его несовершенства, могут быть использованы для перехвата пользовательских сессий или взятия под контроль движения робота и столкновения его с людьми или объектами, или использования их для причинения вреда пациентам и сотрудникам.

Правовое регулирование медицинских изделий на данный момент не учитывает критерий информационной безопасности. Так, в Постановлении Правительства Российской Федерации от 27 декабря 2012 г. № 1416 «Об утверждении Правил государственной регистрации медицинских изделий»[8] под безопасностью медицинского изделия понимается «отсутствие недопустимого риска причинения вреда жизни, здоровью человека и окружающей среде при использовании медицинского изделия по назначению в условиях, предусмотренных производителем (изготовителем)». В данном правовом акте понятие «безопасность» рассматривается достаточно узко, про цифровую безопасность речь и не идет, безопасность рассматривается в смысле физической безопасности.

Уголовно-правовые модели охраны медицинских роботов

В здравоохранении влияние на цифровую безопасность медицинских роботов такое же, как и влияние посягательств на промышленность, которое включает финансовые потери, травмы или смерть. Нарушение работы хирургического робота во время операции может прервать процесс и привести к гибели людей. Кроме того, робот-смотритель обычно оснащен камерой наблюдения, а также возможностью получать данные о местонахождении и состоянии людей. Без обеспечения надлежащего уровня цифровой безопасности указанные данные могут быть незаконно собраны и использованы для различных преступлений.

Специфика отношений в сфере медицинской робототехники осложнена тем, что в эти общественные отношения вступает множество субъектов на разных этапах: создание, оборот, эксплуатация, техническое обслуживание и т. д. Если исходить из того, что медицинская процедура состоит из нескольких этапов, начинается с диагностики заболевания и заканчивается прекращением послеоперационного лечения, то на любой из указанных стадий может быть нанесен вред пациенту или в результате противоправных деяний причинены иные общественно опасные последствия. В данном случае непосредственную причину наступления негативных последствий определить проблематично в связи с тем, что потенциальными субъектами преступления могут быть как производители роботов, так и медицинские работники, которые проводили операцию, а также специалисты, отвечающие за обслуживание робота, или злоумышленники, которые осуществили посягательство на цифровую инфраструктуру робота.

Рассматривая робот, используемый в медицинских целях, в качестве движимого имущества, следует распространить на него концепцию «вещного права». Стоит поддержать мнение Ю. В. Грачевой и А. А. Арямова, полагающих, что робот является объектом гражданского права и на роботов распространяются все положения ГК РФ относительно вещи (Грачева, Арямов, 2020, с. 174–175).

Медицинский робот как вещь материального мира может быть похищен, уничтожен или поврежден или в отношении него могут быть совершены иные противоправные действия, поэтому подобные действия подлежат квалификации по составам преступлений, предусматривающих ответственность за преступления против собственности.

Однако робот, применяемый в медицинских целях, может быть использован злоумышленниками и как орудие причинения вреда жизни или здоровью для нанесения значительных внутренних ран пациенту, уничтожения или повреждения имущества или оборудования организации (больницы).

В связи с использованием медицинской робототехники неизбежно возникнет вопрос, связанный с мерами ответственности из-за причинения вреда человеку в результате использования некачественной продукции, некачественно оказанной услуги, обусловленной бездействием медицинского работника, и иными факторами.

Если несчастный случай, вызванный использованием хирургического робота, привел к травме или смерти пациента, то сначала необходимо проверить, был ли виновен в причинении смерти по неосторожности врач или иные лица. Необходимо выяснить были ли нарушены им принятые стандарты оказания медицинской помощи.

[8] Постановление Правительства Российской Федерации № 1416 от 27.12.2012. (2013). *Собрание законодательства РФ*, *1*, ст. 14.

В свою очередь врач-хирург, выполняя роботизированную операцию, обязан иметь соответствующий опыт проведения роботизированной хирургии. Хирургические ошибки, которые могут варьироваться от неверных шагов, предпринятых хирургом или его командой, или неправильной дозировкой, данной пациенту, до хирургических материалов, оставленных в теле пациента после операции, могут вызвать самые тяжелые осложнения для него. Врач должен быть в состоянии выполнить операцию в соответствии с существующими стандартами оказания медицинской помощи. Неправильная эксплуатация хирургического роботизированного оборудования также является существенным фактором травматизма пациентов. Пациент может умереть или получить серьезные повреждения в результате того, что робот, используемый в операционных, к примеру, перережет артерию пациента.

Представляется, что врачи, управляющие медицинским роботом, не несут ответственности в случаях, когда негативные последствия обусловлены следующими ошибками: программной, механической или ошибкой после обновления программного обеспечения. В этом случае следует сказать, что врач, по нашему мнению, не будет привлекаться к уголовной ответственности, но после того, как медицинский работник обнаружил подобные «недостатки» при эксплуатации медицинского робота, он должен немедленно взять на себя проведение медицинского вмешательства.

Представляется, что врачи, использующие медицинского робота, не несут ответственность за наступившие последствия, за исключением случаев, когда:

– ошибки медицинского робота были спровоцированы неточными действиями медицинских работников (не предусмотренными стандартами оказания помощи). Допущенный вред может быть вызван не заложенными алгоритмами роботов, а невежеством или неопытностью медицинского работника. Использование роботов требует особых теоретико-технических знаний, а также наличия опыта. Знания и опыт медицинского работника очень важны, в особенности при эксплуатации полуавтономных изделий. Кроме того, полагаем, что в тех случаях, когда пациент получил травму, а о необходимости проведения ремонта робота ранее ему не сообщалось, бремя ответственности переходит на врача-хирурга;

– медицинские работники отклонились от стандартов оказания медицинской помощи, протоколов лечения. Допущенные врачом в результате оказания медицинской роботизированной помощи причинение смерти или тяжкого вреда здоровью пациента вследствие ненадлежащего исполнения обязанностей можно рассматривать как наличие в деяниях лица неосторожных составов преступлений (ч. 2 ст. 109 или ч. 2 ст. 118 УК РФ), если его предвидением охватывалось (или могло и должно было охватываться) наступление негативных последствий.

Несомненно, важное значение имеет установление причинно-следственной связи между деяниями субъектов, вовлеченных в оборот медицинских роботов, и наступившими негативными последствиями. Поэтому потенциальными субъектами могут быть производители робототехники, медицинские работники или сам пациент. Примером может служить следующий случай: беспилотная машина *Uber* сбила женщину-пешехода в США, и та погибла. В результате проверки полиция установила, что женщина переходила дорогу в неположенном месте, и не усмотрела вины беспилотного автомобиля, а следовательно, и оператора, и производителя [9].

При посягательстве на цифровую безопасность медицинских роботов есть огромный риск воздействия на поведенческие алгоритмы, реализуя которые робот может перемещаться в пространстве с определенными временем и скоростью. Нарушение функционирования кода медицинского робота посредством различных сбоев может негативным образом отразиться на общественных отношениях и привести к вредным последствиям. Медицинский робот, помимо возможности хранить, обрабатывать, собирать информацию, обладает иными функциями, позволяющими ему, к примеру, двигаться, что отличает его от иных средств вычислительной техники. В связи с этим стоит согласиться с И. Р. Бегишевым, что правовой режим ответственности за посягательства, включая перехват и внедрение компьютерных программ, в отношении средств вычислительной техники можно распространить и на компьютерные программы роботов. Поэтому противоправные действия (вмешательства) в работу цифрового кода компьютерной программы медицинского робота охватываются действующими составами преступлений (Бегишев, 2022, с. 120).

[9] Беспилотник Uber сбил насмерть пешехода из-за настроек автопилота. (2018, 8 мая). *Ведомости*. https://www.vedomosti.ru/technology/news/2018/05/08/768916-bespilotnik-uber-sbil

При посягательстве на цифровой код компьютерной программы медицинского робота злоумышленник может получить к нему доступ, а далее, используя его, совершить иные противоправные действия.

Однако в случае, если злоумышленник получил возможность управлять этим медицинским роботом, т. е., помимо незаконного уничтожения, блокирования, копирования и модификации компьютерной информации, он осуществляет «захват» его управлением, ответственность должна быть строже. Суть общественной опасности состоит в том, что приобретение возможности управления им, т. е. захват его аппаратной части, может породить иные обстоятельства, способствующие совершению самостоятельных составов преступлений.

Виновные лица могут совершать преступные деяния как в отношении информации, хранящейся и обрабатываемой медицинским роботом, так и информации, обращающейся в нем. Наиболее общественно опасным является захват управления медицинским роботом. В связи с этим стоит согласиться с мнением И. Р. Бегишева о том, что ст. 272 УК РФ следует дополнить составом преступления, предусматривающим ответственность за неправомерный доступ к компьютерной информации, содержащейся в роботе, повлекший захват управления роботом (Бегишев, 2022, с. 120).

Учитывая возможные риски, исходящие от персонала, занимающегося ремонтом, сервисным обслуживанием медицинского робота и его основных частей, возможны негативные последствия, которые могут наступить в результате некачественно проведенного ремонта и выпуска в эксплуатацию технически неисправного медицинского изделия, повлекшего наступление негативных последствий в виде причинения тяжкого вреда здоровью человека или смерти.

Возможно, производитель выпустил робота низкого качества, чем должен был быть, не выполняя свою обязанность проявлять осторожность при производстве робота. Точно так же вред может возникнуть из-за нарушения разработчиком программного обеспечения обязанности соблюдать осторожность при использовании первоначальной версии или ее последующих обновлений.

Об установлении уголовной ответственности за грубое нарушение правил эксплуатации роботов, повлекшее причинение вреда здоровью и жизни человека, высказываются российские ученые-правоведы (Приженникова, 2020, с. 314).

Полагаем, что в отношении управляемого медицинского робота общественную опасность составляет не факт нарушения Правил разработки (утилизации), технического (технологического) обслуживания, ремонта и выпуска в эксплуатацию медицинского изделия, а те негативные общественно опасные последствия, которые наступили в результате содеянного. Однако следует особо отметить, что требования к содержанию технической документации медицинского изделия должны быть установлены федеральным органом исполнительной власти Российской Федерации, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере здравоохранения. Это позволит исключить пласт вопросов, связанных с недоброкачественным производством медицинского изделия и его фальсификацию.

Учитывая общественную опасность, исходящую от персонала, занимающегося ремонтом, техническим и технологическим обслуживанием медицинского робота и его основных частей, возможное наступление негативных последствий от их действий, полагаем необходимым установить уголовно-правовой запрет на нарушение правил разработки (утилизации), технического (технологического) обслуживания или ремонта медицинского изделия, а равно выпуск в эксплуатацию медицинского изделия, не соответствующего технической документации, если эти деяния повлекли по неосторожности причинение тяжкого вреда здоровью человека или причинение крупного ущерба. К примеру, закрепив ответственность в ст. 235^2 УК РФ. Квалифицированный состав (ч. 2 ст. 235^2 УК РФ) сконструировать по типу материального, влекущего наступление ответственности, если те же деяния повлекли причинение по неосторожности смерти человека или наступление тяжких последствий.

В примечании уголовно-правовой нормы указать:

1. Правила разработки (утилизации), технического (технологического) обслуживания, ремонта и выпуска в эксплуатацию медицинского изделия для целей настоящей статьи утверждаются Минздравом России.

2. К причинению крупного ущерба стоит отнести случаи доступа к сведениям, составляющим медицинскую тайну, доступ к которым был получен в результате нарушения порядка хранения и утилизация медицинской информации, которая может быть встроена в хирургическую роботизированную систему.

Далее рассмотрим вопросы незаконного оборота медицинских роботов. Стоит обратить внимание на то, что ст. 238^1 УК РФ является «универсальной» для всех медицинских изделий и не содержит дифференциации ответственности в зависимости от класса медицинского изделия. Указанное решение, по нашему мнению,

является законодательным упущением. Общественная опасность производства или сбыта, к примеру, недоброкачественного имплантата, используемого для вживания в организм человека, или медицинского робота значительно выше по сравнению со сбытом, ввозом на территорию Российской Федерации или производством недоброкачественной ваты, бахил или пробирки.

Именно поэтому предлагаем дифференцировать ответственность за незаконное обращение медицинских изделий исходя из их роли и значимости в процессе оказания медицинской помощи. От этих показателей напрямую зависит характер возможного вреда, который может быть причинен в результате совершения преступления, предусмотренного ст. 238[1] УК РФ.

В связи с этим в ст. 238[1] УК РФ следует дифференцировать ответственность в зависимости от класса потенциального риска применения медицинских изделий. Ответственность за реализацию медицинских изделий с высокой степенью риска (3-й класс) должна быть более строгой по сравнению с предметами с более низкой степенью риска (1-й и 2-й классы). От этих показателей напрямую зависит и объем возможного вреда, который может быть причинен в результате совершения действий, названных в ст. 238[1] УК РФ (Прохорова, Иликбаева, 2017, с. 113).

Полагаем, что ответственность за незаконное производство лекарственных средств и медицинских изделий стоит дифференцировать с точки зрения предмета преступления (ст. 238[1] УК РФ). Учитывая разницу в предметах преступного посягательства по своей природе (медицинские изделия, лекарственные средства и биологически активные добавки), предлагаем дифференцировать норму, исходя из предмета преступного посягательства, выделив ответственность за обращение фальсифицированных, недоброкачественных и незарегистрированных медицинских изделий (ст. 238[2] УК РФ) в самостоятельный уголовно-правовой запрет.

Интересным представляется мнение М. Н. Малеиной, которая предлагает вопрос об определении групп риска медицинских роботов рассматривать как условие, снижающее (увеличивающее) размер гражданской ответственности (Малеина, 2023, с. 5).

В ч. 1 указанной нормы установить меры правового воздействия за противоправные действия в отношении медицинских изделий 1-го класса, совершенные в крупном размере. В свою очередь предусмотреть квалифицирующие признаки за деяния, предусмотренные ч. 1 настоящей статьи, совершенные в отношении медицинских изделий 2-го и 3-го классов (ч. 2 и 3 соответственно).

Далее рассмотрим вопросы ответственности за незаконное производство медицинских роботов. Уголовное законодательство устанавливает запрет на незаконное производство лекарственных средств и медицинских изделий (ст. 235[1] УК РФ). Однако стоит отметить, что на данный момент конструкция диспозиции уголовно-правовой нормы, предусматривающей ответственность за незаконное производство лекарственных средств и медицинских изделий, не соответствует требованиям законодательства.

С 1 января 2022 г. лицензия (разрешение) на производство медицинских изделий не выдается. На данный момент, согласно п. 17 ст. 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»[10], лицензия выдается на техническое обслуживание медицинских изделий (за исключением случая, если техническое обслуживание осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) медицинской техники.

Статья 38 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» дополнена ч. 8[1], согласно которой производство медицинских изделий, подлежащих государственной регистрации, а также медицинских изделий, изготовленных по индивидуальным заказам пациентов, к которым предъявляются специальные требования по назначению медицинских работников, должно соответствовать требованиям к внедрению, поддержанию и оценке системы управления качеством медицинских изделий в зависимости от потенциального риска их применения, утвержденным Правительством Российской Федерации. Однако это не означает, что производство медицинских изделий больше не контролируется государством. Вместо лицензирования производство медицинских изделий должно соответствовать требованиям к внедрению, поддержанию и оценке системы управления качеством медицинских изделий, которая будет зависеть от потенциального риска их применения. Постановлением Правительства Российской Федерации от 9 февраля 2022 г. № 136 «Об утверждении требований к внедрению, поддержанию

[10] О лицензировании отдельных видов деятельности. № 99-ФЗ (2011). *Собрание законодательства РФ*, *19*, ст. 2716.

и оценке системы управления качеством медицинских изделий в зависимости от потенциального риска их применения»[11] установлены данные требования.

Учитывая принципиальную разницу между лекарственными средствами и медицинскими изделиями, к которым относятся и медицинские роботы, предлагаем дифференцировать ответственность, исключив из названия и диспозиции уголовно-правовой нормы такой предмет преступного посягательства, как медицинские изделия. В свою очередь представляется возможным криминализировать ответственность за производство медицинских изделий, не соответствующих требованиям к внедрению, поддержанию и оценке системы управления качеством медицинских изделий, повлекшее причинение по неосторожности тяжкого вреда здоровью человека (ч. 1 ст. 235^2 УК РФ). К квалифицированным составам преступления отнести те же деяния, совершенные: а) организованной группой; б) в крупном размере и в) повлекшее причинение смерти человеку по неосторожности.

Важным является рассмотрение вопроса общественной опасности деяний в виде технического обслуживания медицинских изделий без лицензии. Законодатель не посчитал преступлением техническое обслуживание медицинских изделий без лицензии. Полагаем, что установленные Минздравом России Правила технического обслуживания будут содержать обязанность субъектов, имеющих лицензию, проводить техническое обслуживание медицинского робота. В связи с этим нам видится нецелесообразным расширение диспозиции уголовно-правовой нормы, предусмотрев ответственность за техническое обслуживание медицинской техники (изделий) при отсутствии лицензии (Papor, 2018, с. 852–853).

Заключение

Исследование законодательства является важным шагом, позитивно влияющим на регулирование общественных отношений и развитие технологий роботизированной медицинской помощи в обществе. В свою очередь, безопасность роботизированной медицины, в том числе хирургии, является важной задачей, стоящей перед государством и мировым сообществом в эпоху массовой цифровизации общества.

Уязвимости безопасности медицинских роботов вызывают серьезную озабоченность у производителей, программистов и тех, кто взаимодействует с ними в отрасли здравоохранения. В медицинских учреждениях роботы взаимодействуют в тесном контакте с детьми, пожилыми и людьми с ограниченными возможностями, и пациенту может быть неясно, работает ли робот должным образом или подвергается нападению. Любой вред, причиненный хирургическим роботом в результате неправомерного доступа (или иных противоправных действий), может подорвать веру общественности в медицину и в целом в систему здравоохранения. Угрозы безопасности медицинских роботов могут иметь дальнейшие негативные последствия для них самих, так как подобные факты неправомерного воздействия могут привести к тому, что роботы сломаются или нанесут вред другому близлежащему оборудованию, являющемуся имуществом данного учреждения системы здравоохранения, а хуже – жизни и здоровью пациентов или медицинским работникам.

Медицинская робототехника – достаточно рискованный вид деятельности, что связано с ее направленностью на охрану наивысших ценностей (жизни и здоровья граждан), а также внедрением новых цифровых технологий, которые еще не прошли длительную апробацию. В процессе исследования установлено, что риски, возникающие при эксплуатации роботизированных изделий, возможны как от лиц, которые осуществляют непосредственное управление медицинскими роботами, так и от тех, кто их обслуживает. Кроме того, приведена классификация рисков, свойственных медицинским роботам с учетом их аппаратно-технологической сущности.

Выявлено, что текущее состояние уголовно-правовой охраны общественных отношений, возникающих в процессе оборота медицинских роботов, нуждается в совершенствовании в связи с тем, что не учитывает аппаратно-технологическую сущность подобных изделий наряду с иными медицинскими изделиями в конструкции составов преступлений. В связи с этим предложены некоторые направления совершенствования составов преступлений, причиняющих вред общественным отношениям, возникающим в процессе оборота медицинских роботов.

[11] Постановление Правительства Российской Федерации № 136 от 09.02.2022. (2022). *Собрание законодательства РФ*, *7*, ст. 992.

Список литературы

Бабурин, В. В. (2010). Правомерное причинение вреда при рискованном поведении, направленном на достижение общественно полезной цели: проблемы определения обоснованности. *Научный вестник Омской академии МВД России*, *1*, 11–17.

Бегишев, И. Р. (2022). *Уголовно-правовая охрана общественных отношений, связанных с робототехникой*: дис. … д-ра юрид. наук. Казань. EDN: CCHSGS

Бегишев, И. Р. (2022). *Уголовно-правовое регулирование робототехники*: монография. Москва: Блок-Принт.

Галлезе-Нобиле, К. (2023). Регулирование умных роботов и искусственного интеллекта в Европейском союзе. *Journal of Digital Technologies and Law*, *1*(1), 33–61. https://doi.org/10.21202/jdtl.2023.2

Грачева, Ю. В., Арямов, А. А. (2020). Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности. *Актуальные проблемы российского права*, *15*(6), 169–178. https://doi.org/10.17803/1994-1471.2020.115.6.169-178

Гуляева, П. С. (2023). Медицинские нанороботы в фокусе права. *Journal of Digital Technologies and Law*, *1*(1), 89–122. https://doi.org/10.21202/jdtl.2023.4

Записная, Т. В. (2022). О формировании цифрового медицинского права. *Медицинское право*, *1*, 34–38.

Истратова, Е. Е., Молчанов, А. А. (2015). Особенности защиты персональных данных в медицинских информационных системах. *Journal of Siberian Medical Sciences*, 6, 59.

Карцхия, А. А. (2021). Формирование цифрового здравоохранения как вызов времени. *Право и цифровая экономика*, *3*, 39–46.

Малеина, М. Н. (2023). Правовое регулирование применения медицинских роботов-хирургов в комплексе цифровых технологий. *Медицинское право*, 1, 2–5.

Михалева, Е. С., Шубина, Е. А. (2019). Проблемы и перспективы правового регулирования робототехники. *Актуальные проблемы российского права*, *12*(109), 26–35. https://doi.org/10.17803/1994-1471.2019.109.12.026-035

Приженникова, А. Н. (2020). Правовое поле роботизации: пути решения. *Образование и право*, 9, 308–317.

Прохорова, М. Л., Иликбаева, Е. С. (2017). Специфика медицинских изделий как предмета преступления, предусмотренного ст. 238. 1 УК РФ. *Общество: политика, экономика, право*, 12, 111–114.

Рарог, А. И. (2018). Незаконное производство лекарственных средств и медицинских изделий (Статья 235.1 УК РФ). *Всероссийский криминологический журнал*, *6*. https://cyberleninka.ru/article/n/nezakonnoe-proizvodstvo-lekarstvennyh-sredstv-i-meditsinskih-izdeliy-statya-235-1-uk-rf

Цомартова, Ф. В. (2020). Роботизация в здравоохранении: правовая перспектива. *Здравоохранение Российской Федерации*, *2*(64), 88–96.

Alemzadeh, H., Raman, J., Leveson, N., Kalbarczyk, Z., & Iyer, R. K. (2016). Adverse events in robotic surgery: a retrospective study of 14 years of FDA data. *PLoS ONE*, *11*(4), 1–20. https://doi.org/10.1371/journal.pone.0151470

Asimov, I. (2019). Runaround. In *Astounding Science Fiction* (pp. 94–103). New York: Street & Smith Publication Inc.

Fiorini, P., Goldberg, K. Y., Liu, Y., & Taylor, R. H. (2022). Concepts and Trends in Autonomy for Robot-Assisted Surgery. In *Proceedings of the IEEE*, *110*(7), 993–1011. https://doi.org/10.1109/jproc.2022.3176828

Langman, S., Capicotto, N., Maddahi, Y., & Zareinia, K. (2021). Roboethics principles and policies in Europe and North America. *SN Applied Sciences*, 3, 857. https://doi.org/10.1007/s42452-021-04853-5

Lutz, C., Schöttler, M., & Hoffmann, C. P. (2019). The privacy implications of social robots: scoping review and expert interviews. *Mobile Media & Communication*, *7*(3), 412–434. https://doi.org/10.1177/2050157919843961

Nissenbaum, H. (2001). Securing trust online: wisdom or oxymoron. *Boston Univ Law Revew*, *81*(3), 635–664.

Osborne, Ch. (2022). Critical vulnerabilities uncovered in hospital robots. *ZDNet*. https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-medical-robots/

Pasquale, F. (2020). Introduction. In *New Laws of Robotics* (pp. 1–32). Belknap Press.

Schmitz-Luhn, B., Chandler, J., & on Behalf Of The iCARE-Pd Consortium. (2022). Ethical and Legal Aspects of Technology-Assisted Care in Neurodegenerative Disease. *Journal of Personalized Medicine*, *12*(6), 1011. https://doi.org/10.3390/jpm12061011

Weng, Y. H, & Hirata, Y. (2022). Design-Centered HRI Governance for Healthcare Robots. *Journal of Healthcare Engineering*, *2022*. https://doi.org/10.1155/2022/3935316

Yew, G. Ch. K. (2021). Trust in and Ethical Design of Carebots: The Case for Ethic of Care. *International Journal of Social Robotics*, 13, 629–645. https://doi.org/10.1007/s12369-020-00653-w

References

Alemzadeh, H., Raman, J., Leveson, N., Kalbarczyk, Z., & Iyer, R. K. (2016). Adverse events in robotic surgery: a retrospective study of 14 years of FDA data. *PLoS ONE*, *11*(4), 1–20. https://doi.org/10.1371/journal.pone.0151470

Asimov, I. (2019). Runaround. In *Astounding Science Fiction* (pp. 94–103). New York: Street & Smith Publication Inc.

Baburin, V. V. (2010). Legal infliction of harm during a risky behavior aimed at achieving a socially useful objective: problems of determining reasonability. *Scientific Bulletin of the Omsk Academy of the MIA of Russia*, 1, 11–17.

Begishev, I. R. (2022). *Criminal-legal protection of social relations associated with robotics:* thesis for a Doctoral Degree in Jurisprudence. Kazan.

Begishev, I. R. (2022). *Criminal-legal regulation of robotics*: monograph. Moscow: Blok-Print.

Fiorini, P., Goldberg, K. Y., Liu, Y., & Taylor, R. H. (2022). Concepts and Trends in Autonomy for Robot-Assisted Surgery. In *Proceedings of the IEEE*, *110*(7), 993–1011. https://doi.org/10.1109/jproc.2022.3176828

Gallese Nobile, C. (2023). Regulating Smart Robots and Artificial Intelligence in the European Union. *Journal of Digital Technologies and Law*, *1*(1), 33–61. https://doi.org/10.21202/jdtl.2023.2

Gracheva, Yu. V., & Aryamov, A. A. (2020). Robotization and Artificial Intelligence: Criminal Law Risks in the Field of Public Security. *Actual Problems of Russian Law*, *15*(6), 169–178. https://doi.org/10.17803/1994-1471.2020.115.6.169-178

Gulyaeva, P. S. (2023). Medical nanorobots in the focus of law. *Journal of Digital Technologies and Law*, *1*(1), 89–122. https://doi.org/10.21202/jdtl.2023.4

Istratova, E. E., & Molchanov, A. A. (2015).Features of protection of personal information in medical information systems. *Journal of Siberian Medical Sciences*, 6, 59.

Kartskhia, A. A. (2021). A modern challenge of the digital healthcare emergence. *Law and Digital Economy*, *3*, 39–46.

Langman, S., Capicotto, N., Maddahi, Y., & Zareinia, K. (2021). Roboethics principles and policies in Europe and North America. *SN Applied Sciences*, 3, 857. https://doi.org/10.1007/s42452-021-04853-5

Lutz, C., Schöttler, M., & Hoffmann, C. P. (2019). The privacy implications of social robots: scoping review and expert interviews. *Mobile Media & Communication*, *7*(3), 412–434. https://doi.org/10.1177/2050157919843961

Maleina, M. N. (2023). Legal regulation of of using medical robots-surgeons in a complex of digital technologies. *Medical Law*, *1*, 2–5.

Mikhaleva, E. S., & Shubina, E. A. (2019). Challenges and Prospects of the Legal Regulation of Robotics. *Actual Problems of Russian Law*, *1*(12), 26–35. (In Russ.). https://doi.org/10.17803/1994-1471.2019.109.12.026-035

Nissenbaum, H. (2001). Securing trust online: wisdom or oxymoron. *Boston Univ Law Revew*, *81*(3), 635–664.

Osborne, Ch. (2022). Critical vulnerabilities uncovered in hospital robots. *ZDNet.* https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-medical-robots/

Pasquale, F. (2020). Introduction. In *New Laws of Robotics* (pp. 1–32). Belknap Press.

Prizhennikova, A. N. (2020). Legal field of robotics: solutions. *Education and Law*, 9, 308–317.

Prokhorova, M. L., & Ilikbaeva, E. S. (2017). The specific nature of medical devices as a target of crime stipulated by Article 238.1 of the Criminal Code of the Russian Federation. *Society: Politics, Economics, Law*, 12, 111–114.

Rarog, A. I. (2018). Illegal production of medical agents and equipment (Article 235.1 of the Criminal Code of the Russian Federation). *Russian Journal of Criminology*, 6. https://cyberleninka.ru/article/n/nezakonnoe-proizvodstvo-lekarstvennyh-sredstv-i-meditsinskih-izdeliy-statya-235-1-uk-rf

Schmitz-Luhn, B., Chandler, J., & on Behalf Of The iCARE-Pd Consortium. (2022). Ethical and Legal Aspects of Technology-Assisted Care in Neurodegenerative Disease. *Journal of Personalized Medicine*, *12*(6), 1011. https://doi.org/10.3390/jpm12061011

Tsomartova, F. V. (2020). Robotization in healthcare: legal perspective. *Health care of the Russian Federation*, *64*(2), 88–96. https://doi.org/10.46563/0044-197X-2020-64-2-88-96

Weng, Y. H, & Hirata, Y. (2022). Design-Centered HRI Governance for Healthcare Robots. *Journal of Healthcare Engineering*, *2022*. https://doi.org/10.1155/2022/3935316

Yew, G. Ch. K. (2021). Trust in and Ethical Design of Carebots: The Case for Ethic of Care. *International Journal of Social Robotics*, 13, 629–645. https://doi.org/10.1007/s12369-020-00653-w

Zapisnaya, T. V. (2022). On the establishment of the digital medical law. *Medical Law*, *1*, 34–38.

Конфликт интересов / Conflict of Interest

Автором не заявлен / No conflict of interest is declared by the author

История статьи / Article history

Дата поступления / Received 03.05.2023
Дата одобрения после рецензирования / Date of approval after reviewing 10.06.2023
Дата принятия в печать / Accepted 10.08.2023