DOI: 10.24412/2075-7913-2026-2(102)-118-130

УДК 343.3/.7

Шутова А. А.

УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ: РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ

Аннотация. *В статье отражены основные выводы, которые составляют ядро теоретической концепции уголовно-правового обеспечения цифровой безопасности системы здравоохранения. Уголовно-правовое обеспечение цифровой безопасности системы здравоохранения как самостоятельное научное направление в юридической науке до настоящего времени комплексно, системно и междисциплинарно не исследовано. Совокупность изложенных обстоятельств (факторов) со всей очевидностью свидетельствует о несомненной теоретической и практической актуальности темы исследования. Необходимость научного осмысления проблем уголовно-правового обеспечения цифровой безопасности системы здравоохранения обусловлена не только объективными процессами цифровой трансформации медицинской сферы, но и императивной потребностью правоприменительной практики в выработке четких критериев квалификации преступлений и определении мер уголовно-правового воздействия.*

Ключевые слова: *уголовно-правовое обеспечение цифровой безопасности системы здравоохранения, преступления против цифровой безопасности системы здравоохранения, преступления против цифровой безопасности, преступления против безопасности цифровой информации, преступления против безопасности критической цифровой инфраструктуры системы здравоохранения, преступления против безопасности цифровых технологий*

Для цитирования: Шутова А. А. Уголовно-правовое обеспечение цифровой безопасности системы здравоохранения: результаты диссертационного исследования // Проблемы права. 2026. № 2 (102). С. 118–130. DOI: 10.24412/2075-7913-2026-2(102)-118-130

Shutova A. A.

CRIMINAL LAW PROVISION OF DIGITAL SECURITY OF THE HEALTHCARE SYSTEM: RESULTS OF THE DISSERTATION RESEARCH

Abstract. *The article reflects the main conclusions that form the core of the theoretical concept of criminal law provision of digital security of the healthcare system. The criminal law provision of digital security of the healthcare system as an independent scientific field in legal science has not been comprehensively, systematically and interdisciplinarly studied to date. The totality of the stated circumstances (factors) This clearly indicates the undoubted theoretical and practical relevance of the research topic. The need for a scientific understanding of the problems of criminal law ensuring the digital security of the healthcare system is due not only to the objective processes of digital transformation of the medical field, but also to the imperative need for law enforcement practice to develop clear criteria for the qualification of crimes and the definition of criminal law measures.*

Keywords: *criminal law enforcement of the digital security of the healthcare system, crimes against the digital security of the healthcare system, crimes*

against digital security, crimes against the security of digital information, crimes against the security of critical digital infrastructure of the healthcare system, crimes against the security of digital technologies

For citation: Shutova A. A. Criminal Law Provision of Digital Security of the Healthcare System: Results of the Dissertation Research. *Problemy prava (Issues of Law)*. 2026. No. 2 (102). P. 118–130. DOI: 10.24412/2075-7913-2026-2(102)-118-130

Введение. Несмотря на существенный вклад научного сообщества в развитие доктрины уголовного права в условиях цифровой трансформации и связанных с ней новых форм преступности, анализ последних изменений уголовного законодательства свидетельствует об отсутствии целостной системы уголовно-правового обеспечения цифровой безопасности системы здравоохранения. Современные законодательные новации носят фрагментарный характер и не образуют универсальной модели уголовно-правовой охраны общественных отношений, адекватной вызовам цифровой эпохи. В данном контексте перед уголовно-правовой наукой возникает важная задача — разработка концепции уголовно-правового обеспечения цифровой безопасности системы здравоохранения. Особую значимость приобретает научное осмысление вопросов уголовной ответственности за противоправные деяния, совершаемые с применением прорывных цифровых технологий: искусственного интеллекта, медицинской робототехники и биопринтинга. Цифровая трансформация системы здравоохранения, сопровождающаяся внедрением новых технологических решений, обуславливает настоятельную потребность в пересмотре традиционных уголовно-правовых конструкций с учетом особенностей цифровых медицинских технологий, разработке новых доктринальных подходов к охране возникающих общественных отношений и создании научно обоснованной системы квалификации преступных посягательств на цифровую безопасность системы здравоохранения. В связи с этим назрел вопрос о необходимости создания концепции уголовно-правового обеспечения цифровой безопасности системы здравоохранения, соответствующей вызовам технологической эпохи.

Основная часть

Предложения по доктринальным аспектам уголовно-правового обеспечения цифровой безопасности системы здравоохранения:

1. Определена и обоснована двойственная природа цифровой безопасности системы здравоохранения, научное осмысление которой позволяет установить ее место в общей системе национальной безопасности и раскрыть содержание как объекта уголовно-правовой охраны [6. С. 95]. Во-первых, цифровая безопасность системы здравоохранения, выступая закономерным эволюционным этапом развития информационной безопасности в целом и информационной безопасности системы здравоохранения в частности, органически интегрирована в многоуровневую систему национальной безопасности Российской Федерации и рассматривается как состояние защищённости цифровой информации, критической цифровой инфраструктуры и применяемых цифровых технологий в системе здравоохранения от цифровых угроз [11. С. 97]. Во-вторых, цифровая безопасность системы здравоохранения одновременно выступает самостоятельным объектом уголовно-правовой охраны, представляя собой систему общественных отношений, обеспечивающих надежную защиту цифровой информации, критической цифровой инфраструктуры и применяемых цифровых технологий в системе здравоохранения от различного рода цифровых угроз, способных причинить вред жизни и здоровью граждан, нарушить функционирование медицинских организаций, дестабилизировать систему здравоохранения в целом.

При этом уголовно-правовое обеспечение цифровой безопасности системы здравоохранения определяется как правовой механизм, включающий совокупность положений уголовного закона и стратегических направлений уголовной политики государства, обеспечивающий всестороннюю и эффективную охрану цифровой безопасности системы здравоохранения путем установления уголовной ответственности за совершение общественно опасных деяний против безопасности цифровой информации, критической цифровой инфраструктуры и применяемых цифровых технологий в системе здравоохранения [11. С. 90].

2. Разработана и обоснована категория социальной обусловленности уголовно-

правового обеспечения цифровой безопасности системы здравоохранения, представляющая собой правовой феномен, который выражает объективно существующую совокупность значимых факторов, детерминирующих необходимость установления уголовно-правовой защиты цифровой безопасности системы здравоохранения в условиях цифровой трансформации отрасли, и одновременно определяющий фундаментальные закономерности процессов криминализации и декриминализации, пенализации и депенализации общественно опасных деяний, посягающих на общественные отношения, связанные с обеспечением безопасности цифровой информации, критической цифровой инфраструктуры и цифровых технологий в системе здравоохранения [11. С. 96]. Характерно, что данный правовой феномен носит динамический характер и непосредственно обусловлен не только объективными процессами развития цифровых технологий, но и эволюцией форм и способов преступных посягательств на цифровую безопасность системы здравоохранения [11. С. 94], изменением степени общественной опасности соответствующих деяний, а также трансформацией социальных представлений о допустимых пределах уголовно-правового вмешательства государства в сферу цифровизации отрасли, что требует постоянного научного мониторинга и своевременной трансформации уголовно-правовых средств обеспечения цифровой безопасности системы здравоохранения.

3. Обосновано, что создание отдельного раздела или главы УК РФ, специально посвященных регламентации преступлений против цифровой безопасности системы здравоохранения, представляется нецелесообразным, поскольку подобное законодательное решение чревато серьезным нарушением системности и внутренней логики уголовного законодательства. Сфера цифровой безопасности системы здравоохранения органически интегрирована в комплексную систему обеспечения цифровой безопасности государства и общества в целом, составляя лишь один из секторальных элементов в многоуровневой архитектуре правового обеспечения соответствующих общественных отношений, что объективно исключает ее выделение в качестве самостоятельной структурной единицы уголовного закона. Вместе с тем в работе доказана целесообразность выделения главы 28 УК РФ из раздела IX УК РФ и придания ей статуса самостоятельного раздела под наименованием «Преступления против цифровой безопасности», который должен включать в себя три главы: «Преступления против безопасности цифровой информации», «Преступления против безопасности критической цифровой инфраструктуры» и «Преступления против безопасности цифровых технологий». Подобная структурная реорганизация Особенной части уголовного закона не только будет отражать современные реалии цифровой трансформации общественных отношений, но и создаст необходимые предпосылки для системной уголовно-правовой охраны всех элементов цифровой безопасности, включая ее медицинский сегмент. В целях совершенствования уголовного законодательства в условиях глобальной цифровой трансформации общества предложено дополнить ч. 1 ст. 2 УК РФ важным положением об обеспечении цифровой безопасности как одной из самостоятельных задач уголовного закона, что позволит закрепить приоритетность данного направления уголовно-правовой охраны и обеспечит единообразное понимание роли уголовного права в защите цифрового пространства.

Предложения по доктринальным аспектам противодействия преступлениям против цифровой безопасности системы здравоохранения:

4. Сформулирована и обоснована дефиниция преступлений против цифровой безопасности системы здравоохранения, под которыми понимаются противоправные общественно опасные деяния, посягающие на общественные отношения, связанные с обеспечением безопасности цифровой информации, критической цифровой инфраструктуры и применяемых цифровых технологий в системе здравоохранения. Характерно, что данная категория преступлений представляет собой качественно новый тип криминальных посягательств, порожденных процессами цифровизации системы здравоохранения, и отличается повышенной общественной опасностью, обусловленной тем, что их совершение способно не только причинить вред конкретным пациентам или медицинским организациям, но и дестабилизировать функционирование системы здравоохранения в целом, создавая реальную угрозу жизни и здоровью неопределенного круга лиц. При этом специфика данной группы преступлений заключается в их комплексном характере: они одновремен-

но посягают на несколько взаимосвязанных объектов уголовно-правовой охраны, включая общественную безопасность, здоровье населения, информационную безопасность и нормальное функционирование критической инфраструктуры, что объективно требует выработки особых подходов к их квалификации, назначению наказания и разработке специальных мер предупреждения подобных криминальных проявлений в условиях продолжающейся цифровой трансформации системы здравоохранения [16. С. 82–84, 86].

5. Разработана и обоснована классификация преступлений против цифровой безопасности системы здравоохранения, имеющая существенное теоретико-прикладное значение для систематизации уголовно-правовых норм, верной квалификации преступлений и выработки дифференцированных мер противодействия криминальным угрозам в условиях цифровизации отрасли. Предложенная классификация основана на объекте преступного посягательства и включает три взаимосвязанные, но качественно различающиеся группы общественно опасных деяний:

а) преступления против безопасности цифровой информации, обращающейся в системе здравоохранения, охватывающие противоправные посягательства на конфиденциальность, целостность и доступность медицинских данных, персональных сведений о пациентах и иной информации;

б) преступления против безопасности критической цифровой инфраструктуры системы здравоохранения, включающие деяния, направленные на нарушение функционирования информационных систем, телекоммуникационных сетей и иных технологических объектов, обеспечивающих непрерывность оказания медицинской помощи населению;

в) преступления против безопасности цифровых технологий, применяемых в системе здравоохранения, к которым относятся посягательства на безопасное и правомерное использование искусственного интеллекта, медицинской робототехники и бипринтных технологий.

Характерно, что данная классификация не только отражает современную архитектуру цифровой безопасности здравоохранения, но и создает методологическую основу для совершенствования уголовного законодательства, формирования единообразного правоприменения и разработки системы предупреждения исследуемых преступлений [16. С. 84–86].

Предложения по доктринальным, законотворческим и правоприменительным аспектам противодействия преступлениям против безопасности цифровой информации в системе здравоохранения:

6. Обосновано, что в условиях ускоренной цифровой трансформации общества и экспоненциального роста объемов обрабатываемых цифровых данных возникает объективная необходимость фундаментальной модернизации терминологического аппарата уголовного законодательства, поскольку действующий понятийно-категориальный аппарат, основанный на категории «компьютерная информация», не в полной мере отражает современные технологические реалии и не охватывает весь спектр общественных отношений, нуждающихся в уголовно-правовой защите в эпоху тотальной цифровизации. В связи с этим предложена и научно обоснована дефиниция преступлений против безопасности цифровой информации в системе здравоохранения, под которыми понимаются противоправные общественно опасные деяния, посягающие на состояние защищенности сведений, циркулирующих в информационно-телекоммуникационных системах, сетях и устройствах, полученных посредством алгоритмических преобразований числовых последовательностей, в системе здравоохранения [15, С. 45–49]. Данное определение не только точно отражает технологическую сущность объекта преступного посягательства, но и расширяет сферу уголовно-правовой охраны, включая в нее все формы представления информации в цифровом виде независимо от технических средств ее хранения, обработки и передачи, что создает необходимые предпосылки для эффективного противодействия современным угрозам и рискам цифровой безопасности отрасли в условиях развития цифровых технологий и появления принципиально новых способов криминального воздействия на медицинские информационные ресурсы.

7. Обосновано, что в целях придания персональным данным самостоятельного уголовно-правового статуса в качестве предмета преступного посягательства наряду со сведениями о частной жизни лица необходимо сформулировать их легальное определение в уголовном законе, под которыми предлагается понимать конфиденциальную информацию о физическом лице

(субъекте персональных данных), позволяющую осуществить его идентификацию. Подобный подход обусловлен тем, что персональные данные, обладая качественно иной правовой природой и специфическими признаками по сравнению с иными категориями конфиденциальной информации, требуют дифференцированной уголовно-правовой охраны, особенно актуальной в контексте обеспечения безопасности медицинских сведений о пациентах в условиях цифровизации системы здравоохранения. В связи с этим в целях создания комплексной системы уголовно-правовой охраны персональных данных граждан, в том числе пациентов медицинских организаций, предложено: во-первых, установить уголовную ответственность за незаконные распространение или использование персональных данных, дополнив УК РФ статьей 137^1, и одновременно внести соответствующие изменения в статью 272 УК РФ относительно трансформации предмета преступления; во-вторых, установить уголовную ответственность за изготовление и (или) сбыт поддельных биометрических персональных данных, дополнив УК РФ статьей 137^2, что позволит противодействовать новым формам криминальной активности, связанным с фальсификацией биометрических идентификаторов личности; в-третьих, декриминализовать незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения, исключив статью 272^1 из УК РФ в связи с ее очевидной избыточностью и правоприменительной неэффективностью, что обеспечит оптимизацию системы уголовно-правовых норм, устранение внутренних противоречий уголовного законодательства и создание более эффективной модели криминализации посягательств на персональные данные [5. С. 122–134].

8. Обосновано, что с учетом возрастающего уголовно-правового значения цифровой информации, специфики процессов ее обработки в информационно-телекоммуникационных системах, а также выявленных особенностей квалификации преступлений в этой сфере, существующее толкование категории тяжких последствий, содержащееся в пункте 14 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»», нуждается в концептуальном пересмотре применительно к преступлениям против цифровой безопасности [14. С. 81–94].

Предложения по доктринальным, законотворческим и правоприменительным аспектам противодействия преступлениям против безопасности критической цифровой инфраструктуры системы здравоохранения:

9. Сформулирована и обоснована дефиниция преступлений против безопасности критической цифровой инфраструктуры системы здравоохранения, под которыми предлагается понимать виновно совершенные общественно опасные деяния, связанные с проведением цифровых атак и совершением иных противоправных действий, направленных на критическую цифровую инфраструктуру системы здравоохранения [10. С. 52–57, 16. С. 79–88]. Характерно, что данная категория преступлений отличается повышенной степенью общественной опасности, обусловленной тем, что критическая цифровая инфраструктура отрасли представляет собой совокупность информационных систем, телекоммуникационных сетей и технологических объектов, нарушение функционирования, уничтожение или блокирование которых способны причинить существенный вред не только отдельным медицинским организациям, но и дестабилизировать систему оказания медицинской помощи населению в целом, создавая реальную угрозу жизни и здоровью пациентам [10. С. 52–57].

10. Научно обоснована концепция модернизации отечественного законодательства, направленная на повышение эффективности противодействия преступлениям против безопасности критической информационной инфраструктуры системы здравоохранения, предполагающая внесение изменений в Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и статью 274^1 УК РФ путем замены понятия «критическая информационная инфраструктура» на «критическая цифровая инфраструктура», введения терминов «цифровая атака» и «цифровой инцидент», за-

конодательного закрепления определения значимого объекта критической цифровой инфраструктуры, декриминализации отдельных деяний с закреплением ответственности в статье 274 УК РФ и изложения статьи 274[1] УК РФ в новой редакции «Совершение цифровой атаки на значимый объект критической цифровой инфраструктуры Российской Федерации» со структурой, включающей основной состав, квалифицирующие и особо квалифицирующие признаки, что позволит создать согласованную систему уголовно-правового обеспечения безопасности критической цифровой инфраструктуры системы здравоохранения [14. С. 81–94].

11. Обоснована необходимость совершенствования акта официального судебного толкования в целях формирования единообразной практики применения норм, устанавливающих ответственность за посягательства на безопасность критической информационной инфраструктуры, что предполагает внесение изменений в постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» путем дополнения его положениями, закрепляющими особенности квалификации преступлений против безопасности критической информационной инфраструктуры, что позволит обеспечить правильное понимание и единообразное применение судами уголовно-правовых норм в данной сфере, устранить существующие пробелы в толковании и создать надежную основу для формирования согласованной практики применения норм уголовного закона [14. С. 81–94].

Предложения по доктринальным и законотворческим аспектам противодействия преступлениям против безопасности цифровых технологий, применяемых в системе здравоохранения:

12. В целях теоретического закрепления терминологии и последующего выбора оптимальной модели уголовно-правового обеспечения разработки и применения цифровых технологий в системе здравоохранения, научно обосновано понятие безопасности цифровых технологий в системе здравоохранения, под которым предлагается понимать состояние защищенности процесса и (или) метода оборота цифровых данных в системе здравоохранения, а также способа осуществления такого процесса и (или) метода для создания медицинского изделия на основе цифровых технологий и (или) оказания высокотехнологичной медицинской помощи от цифровых угроз, что позволяет комплексно охватить все основные компоненты цифровизации здравоохранения, создать необходимую основу для разработки согласованной системы уголовно-правового обеспечения цифровой безопасности системы здравоохранения и обеспечить терминологическое единство при квалификации преступлений, посягающих на безопасность применения цифровых технологий в системе здравоохранения [17. С. 58–68].

13. Обоснована необходимость расширения системы уголовно-правового обеспечения безопасности цифровых технологий в системе здравоохранения путем установления уголовной ответственности за два вида общественно опасных деяний: во-первых, за производство, сбыт или ввоз на территорию Российской Федерации фальсифицированных медицинских изделий на основе цифровых технологий, либо сбыт или ввоз на территорию Российской Федерации недоброкачественных медицинских изделий на основе цифровых технологий, либо производство, сбыт или ввоз на территорию Российской Федерации в целях сбыта незарегистрированных медицинских изделий на основе цифровых технологий, совершенные в крупном размере, и, во-вторых, за нарушение правил создания, технического обслуживания, ремонта, выпуска в эксплуатацию или утилизации медицинских изделий на основе цифровых технологий, если эти деяния повлекли по неосторожности причинение средней тяжести вреда здоровью человека, что позволит устранить пробел в уголовно-правовой охране общественных отношений, связанных с оборотом и эксплуатацией медицинских изделий, основанных на цифровых технологиях, обеспечить реагирование на криминальные угрозы, возникающие в процессе цифровизации отрасли, создать необходимые правовые предпосылки для защиты жизни и здоровья граждан от некачественной и небезопасной цифровой медицинской техники и сформировать эффективный механизм превентивного воздействия на потенциальных правонарушителей [1. С. 581–582, 9. С. 97–98].

Предложения по доктринальным аспектам применения риск-ориентированного подхода к уголовно-правовому обеспечению безопасности цифровых технологий системы здравоохранения:

14. Обосновано 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 отрасли, объективно оценить реальную и потенциальную эффективность 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 обеспечения, 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 [7. С. 160].

15. 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 функционирование цифровых медицинских устройств, что позволяет комплексно идентифицировать потенциальные источники угроз цифровой безопасности здравоохранения, разработать дифференцированные меры уголовно-правового обеспечения с учетом специфики каждой категории рисков и создать научную основу для формирования эффективной системы превенции рассматриваемых преступлений [6. С. 947–948; 7. С. 161].

16. 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, цифровых атак 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, 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 — цифрового 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 [1. С. 571–585, 2. С. 52–57, 3. С. 14–17, 6, С. 947–948].

Предложения по доктринальным, законотворческим и правоприменительным аспектам противодействия преступлениям против безопасности технологий искусственного интеллекта в здравоохранении:

17. Установлено, что дуалистическая природа технологий искусственного интеллекта, проявляющаяся в их созидательном и деструктивном потенциале, обусловливает необходимость применения дифференцированного подхода к уголовно-правовому обеспечению их безопасности, что предполагает классификацию данных технологий в зависимости от целевого назначения на две категории: технологии искусственного интеллекта в системе здравоохранения, предназначенные для осуществления законной деятельности, направленные на совершенствование диагностики, лечения, профилактики заболеваний и организации медицинской помощи, и технологии искусственного интеллекта в системе здравоохранения, используемые для совершения противоправной деятельности, при этом искусственный интеллект может выступать как в качестве предмета преступления, так и в качестве средства совершения преступления, используемого для облегчения или обеспечения преступной деятельности; в целях формирования единообразного понятийного аппарата предложено под преступлениями против безопасности технологий искусственного интеллекта в здравоохранении понимать противоправные общественно опасные деяния, посягающие на состояние защищённости технологий искусственного интеллекта, процесса и (или) метода оборота цифровой информации (данных), а также способа осуществления такого процесса и (или) метода для создания продукта цифровых достижений, основанного на использовании искусственного интеллекта, применяемых в системе здравоохранения; при этом обосновано, что учитывая междисциплинарный характер понятия «искусственный интеллект», его многоаспектность, стремительную эволюцию и отсутствие устоявшегося общепризнанного определения, нецелесообразно включение дефиниции искусственного интеллекта непосредственно в текст уголовного закона, а оптимальным законодательно-техническим решением является использование бланкетных отсылок к иным нормативным правовым актам, что обеспечивает необходимую гибкость правового регулирования, позволяет оперативно адаптировать уголовно-правовые нормы к динамично развивающимся технологиям без внесения изменений в УК РФ и создает условия для согласованности уголовного законодательства с отраслевым регулированием в сфере искусственного интеллекта [9. С. 92–100, 8. С. 48–53, 13, С. 46–50].

18. Обоснована необходимость криминализации двух самостоятельных составов преступлений, направленных на обеспечение безопасности технологий искусственного интеллекта в системе здравоохранения: установление уголовной ответственности за незаконный оборот (создание, приобретение и (или) сбыт) технологий искусственного интеллекта, заведомо предназначенных для совершения преступления, и за незаконный оборот (создание, приобретение и (или) сбыт) автономных технологий искусственного интеллекта, заведомо предназначенных для совершения преступления, выделяемых в качестве самостоятельного состава с учетом повышенной общественной опасности систем, способных к самостоятельному принятию решений без непосредственного контроля человека, что позволяет дифференцировать уголовную ответственность в зависимости от степени автономности технологии, обеспечить превентивную защиту от использования деструктивного потенциала искусственного интеллекта в преступных целях и создать эффективный механизм противодействия криминальным угрозам цифровизации здравоохранения на стадии, предшествующей непосредственному причинению вреда охраняемым уголовным законом общественным отношениям [9. С. 92–100, 8. С. 48–53, 13. С. 46–50].

19. Обоснована необходимость совершенствования судебной практики применения уголовного законодательства об ответственности за преступления, связанные с использованием цифровых технологий в системе здравоохранения, путем дополнения постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» положениями, регламентирующими особенности квалификации преступлений против безопасности технологий искусственного интеллекта в сфере здравоохранения, что позволит устранить существующую неопределенность в правоприменении, обеспечить единообразное толкование и применение уголовно-правовых норм судами при рассмотрении уголовных дел о преступлениях, связанных с использованием технологий искусственного интеллекта в медицинской деятельности, сформировать согласованную систему разъяснений по вопросам отграничения преступлений против безопасности технологий искусственного интеллекта от смежных составов преступлений, определить критерии оценки общественной опасности деяний с учетом специфики применения искусственного интеллекта в системе здравоохранения и создать необходимые предпосылки для правильной квалификации преступлений и назначения справедливого наказания, соответствующего характеру и степени общественной опасности совершенных деяний в условиях цифровизации системы здравоохранения.

Предложения по доктринальным и законотворческим аспектам противодействия преступлениям против безопасности технологий робототехники в системе здравоохранения:

20. Доказано, что система уголовно-правового обеспечения не может обеспечить соответствующую охрану общественных отношений в сфере применения медицинских роботов, поскольку законодатель не учитывает их специфику как особой разновидности медицинских изделий, характеризующихся повышенной технологической сложностью, способностью к автономному функционированию и потенциалом причинения значительного вреда при неправомерном использовании или технических сбоях, что обусловливает необходимость разработки специальных уголовно-правовых норм для эффективного противодействия противоправным деяниям, связанным с применением медицинских роботов и направленным против них; в целях формирования единообразного понятийного аппарата предложено под преступлениями против безопасности технологий робототехники в здравоохранении понимать противоправные общественно опасные деяния, посягающие на состояние защищенности технологий медицинской робототехники, процесса и (или) метода их создания, оборота и применения в системе здравоохранения [1. С. 571–585, 4. С. 39–43].

21. Обоснована система мер по уголовно-правовому обеспечению безопасности технологий робототехники в системе здравоохранения, включающая, во-первых, установление самостоятельной уголовной ответственности за три вида общественно опасных деяний: за незаконный оборот (создание, приобретение и (или) сбыт) технологий робототехники, заведомо предна-

значенных для совершения преступления, а также за незаконный оборот автономных (создание, приобретение и (или) сбыт) технологий робототехники, заведомо предназначенных для совершения преступления, выделяемых с учетом повышенной общественной опасности робототехнических систем, способных к самостоятельному принятию решений и осуществлению действий без непосредственного контроля человека; а также за неправомерный доступ к охраняемой законом цифровой информации, содержащейся в роботе, если это деяние повлекло захват управления робота, криминализация которого обусловлена специфической общественной опасностью несанкционированного удаленного контроля над робототехническими системами, применяемыми в медицинских целях; во-вторых, обоснована позиция, согласно которой разница в утрате человеческого органа или бионического роботизированного протеза отсутствует, поскольку с момента интеграции бионического роботизированного протеза в организм человека такое изделие становится неотъемлемой частью человеческого тела, в связи с чем на него распространяется полная конституционная защита телесной неприкосновенности, и при посягательстве на телесную целостность человека, включающую биологические органы и интегрированные технические устройства, следует применять составы преступлений против жизни и здоровья, что обеспечивает равную правовую защиту всех компонентов человеческого тела независимо от их биологического или технического происхождения и создает надежные гарантии охраны физической неприкосновенности личности в условиях развития технологий бионического протезирования [1. С. 571–585, 4. С. 39–43].

Предложения по доктринальным и законотворческим аспектам противодействия преступлениям против безопасности биопринтных технологий:

22. Доказано, что активное развитие биопринтных технологий, открывающих революционные возможности для регенеративной медицины и трансплантологии, одновременно порождает новые виды общественно опасных деяний, связанных с незаконным использованием данных технологий, фальсификацией биопринтных конструктов, нарушением требований биобезопасности и иными формами злоупотреблений, что обусловливает необходимость опережающего формирования системы уголовно-правового обеспечения оборота указанных технологий, позволяющего создать превентивные механизмы противодействия криминогенным угрозам до их масштабной реализации в правоприменении; в целях формирования единообразного понятийного аппарата предложено под преступлениями против безопасности биопринтных технологий понимать противоправные общественно опасные деяния, посягающие на состояние защищенности биопринтных технологий как совокупности методов разработки и производства тканевых (органных) конструктов на основе биочернил с использованием 3D-биопринтера, а также процесса и (или) метода оборота компонентов биопринтных технологий — 3D-биопринтеров, донорских клеток, биочернил, биопринтных тканевых (органных) конструктов и CAD-файлов как цифровых шаблонов биопринтных конструктов, что позволяет обеспечить уголовно-правовую охрану всех этапов создания и применения биопринтных технологий и создать правовую основу для противодействия криминогенным рискам [12. С. 757–766].

23. Обоснована необходимость криминализации двух составов преступлений, направленных на обеспечение безопасности биопринтных технологий в системе здравоохранения: установление уголовной ответственности за незаконное изъятие органов, тканей или клеток трупа человека и за незаконный оборот органов и (или) тканей человека (хищение, незаконные приобретение или сбыт биологического материала или биопринтных тканевых (органных), который позволяет противодействовать коммерциализации человеческого тела, предотвратить формирование нелегального рынка биологического материала и биопринтных конструктов, обеспечить соблюдение этических и правовых стандартов в сфере биомедицинских технологий и создать эффективный механизм защиты от использования биопринтных технологий в преступных целях на всех этапах — от получения исходного биологического материала до имплантации готовых биопринтных конструктов [12. С. 757–766].

Заключение. Концепция уголовно-правового обеспечения цифровой безопасности системы здравоохранения представляет собой научное направление, органически интегрирующего теоретико-методологические основы уголовного права с императивами технологической модернизации медицинской сферы.

Оригинальность подхода заключается в том, что предложенная система уголовно-правового обеспечения не только охватывает проблемы противодействия существующим цифровым угрозам в здравоохранении, но и предусматривает инновационные механизмы превентивной защиты от потенциальных криминогенных рисков, неизбежно возникающих в процессе внедрения прорывных технологий. Новизна проявляется в разработке и применении риск-ориентированного подхода к уголовно-правовому обеспечению, позволяющего научно обосновать социальную обусловленность криминализации деяний применительно к каждому виду цифровых технологий, используемых в медицине, включая технологии искусственного интеллекта, медицинскую робототехнику и биопринтинг. Вкладом в развитие уголовно-правовой доктрины является модернизация понятийно-категориального аппарата в условиях цифровой трансформации общества. Предложена научно обоснованная система дефиниций цифровой эпохи, включающая такие фундаментальные понятия, как «цифровизация», «цифровое здравоохранение», «цифровая информация», «цифровые данные», «цифровые технологии», «критическая цифровая инфраструктура», «искусственный интеллект», «технологии искусственного интеллекта», «медицинский робот», «медицинская робототехника», «биопринтные технологии», «цифровые преступления», «преступления против цифровой безопасности здравоохранения» и другие. Разработанный терминологический аппарат не только обогащает уголовно-правовую науку, но и закладывает фундамент для совершенствования уголовного законодательства, обеспечивая необходимую терминологическую определенность, системность и согласованность правовых норм в контексте современных технологических вызовов. Предложенные новеллы уголовного законодательства учитывают специфику общественной опасности соответствующих деяний в контексте цифровизации здравоохранения. Содержатся новые предложения по системной модернизации уголовно-правовых норм с учетом современных цифровых вызовов и угроз, а также включает изменения в постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, направленных на совершенствование судебной практики по делам о преступлениях в сфере компьютерной информации и формирование единообразного толкования уголовного закона.

Литература

1. Шутова А. А. Криминальные риски оборота медицинских роботов // Russian Journal of Economics and Law. 2023. Т. 17, № 3. С. 571–585. DOI 10.21202/2782-2923.2023.3.571-585. EDN HZDUBN.
2. Шутова А. А. Криминальные риски применения технологий искусственного интеллекта в здравоохранении // Безопасность бизнеса. 2024. № 1. С. 52–57. — DOI 10.18572/2072-3644-2024-1-52-57. EDN LSZRNV.
3. Шутова А. А. Криминальные риски, возникающие в процессе 3D-биопечати // Российский следователь. 2022. № 9. С. 14–17. DOI 10.18572/1812-3783-2022-9-14-17. EDN QKMTQR.
4. Шутова А. А. Медицинские роботы: правовые, этические и социальные проблемы // Безопасность бизнеса. 2023. № 3. С. 39–43. DOI 10.18572/2072-3644-2023-3-39-43. EDN EQCMFG.
5. Шутова А. А. Новеллы уголовного законодательства об ответственности за незаконный оборот персональных данных // Ученые записки Казанского университета. Серия: Гуманитарные науки. 2024. Т. 166, № 6. С. 122–134. DOI 10.26907/2541-7738.2024.6.122-134. EDN LXPPWK.
6. Шутова А. А. Обеспечение цифровой безопасности системы здравоохранения уголовно-правовыми средствами // Russian Journal of Economics and Law. 2024. Т. 18, № 4. С. 936–953. DOI 10.21202/2782-2923.2024.4.936-953. EDN SHZTFY.
7. 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
8. Шутова А. А. Применение технологий искусственного интеллекта в здравоохранении: этико-правовые вопросы // Юридический мир. 2024. № 2. С. 48–53. DOI 10.18572/1811-1475-2024-2-48-53. EDN AJULIJ.
9. Шутова А. А. Применение технологий искусственного интеллекта в сфере здравоохранения: уголовно-правовые девиации // Правопорядок: история, теория, практика. 2023. № 3(38). С. 92–100. DOI 10.47475/2311-696X-2023-38-3-92-100. EDN RKMSGE.

10. Шутова А. А. Проблемы обеспечения безопасности цифровой инфраструктуры системы здравоохранения уголовно-правовыми средствами // Безопасность бизнеса. 2025. № 1. С. 52–57. DOI 10.18572/2072-3644-2025-1-52-57. — EDN DMRIVY.

11. Шутова А. А. Социальная обусловленность уголовно-правовой охраны цифровой безопасности системы здравоохранения: постановка проблемы // Правопорядок: история, теория, практика. 2025. № 2(45). С. 89–97. DOI 10.47475/2311-696X-2025-45-2-89-97. EDN VSZOAG.

12. Шутова А. А. Уголовно-правовая охрана отношений в сфере 3D-биопринтинга // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32, № 4. С. 757–766. DOI 10.35634/2412-9593-2022-32-4-757-766. EDN JQAAWW.

13. Шутова А. А. Уголовно-правовая охрана отношений, связанных с созданием и применением технологий искусственного интеллекта в здравоохранении // Российский следователь. 2024. № 3. С. 46–50. DOI 10.18572/1812-3783-2024-3-46-50. EDN CPNUUN.

14. Шутова А. А. Уголовно-правовое обеспечение безопасности критической цифровой инфраструктуры Российской Федерации (на примере учреждений здравоохранения) // Lex Russica (Русский закон). 2025. Т. 78, № 9(226). С. 81–94. — DOI 10.17803/1729-5920.2025.226.9.081-094. EDN LJRHDY.

15. Шутова А. А. Уголовно-правовое понятие цифровой информации, обращающейся в системе здравоохранения // Российский следователь. 2025. № 4. — С. 45–49. DOI 10.18572/1812-3783-2025-4-45-49. EDN MSDBGX.

16. Шутова А. А. Преступления против цифровой безопасности системы здравоохранения: понятие, признаки и система // Московский юридический журнал. 2024. № 3. С. 79–88.

17. Шутова А. А. Содержание понятия «цифровые технологии», применяемого в системе здравоохранения // Информационное общество. 2025. № 3. С. 58–68.

References

1. Shutova A. A. Criminal risks of medical robot trafficking // Russian Journal of Economics and Law. 2023. Vol. 17, No. 3. pp. 571–585. DOI 10.21202/2782-2923.2023.3.571-585. EDN HZDUBN.

2. Shutova A. A. Criminal risks of using artificial intelligence technologies in healthcare // Business security. 2024. No. 1. pp. 52–57. — DOI 10.18572/2072-3644-2024-1-52-57. EDN LSZRNV.

3. Shutova A. A. Criminal risks arising in the process of 3D bioprinting // A Russian investigator. 2022. No. 9. pp. 14–17. DOI 10.18572/1812-3783-2022-9-14-17. EDN QKMTQR.

4. Shutova A. A. Medical robots: legal, ethical and social problems // Business security. 2023. No. 3. pp. 39–43. DOI 10.18572/2072-3644-2023-3-39-43. EDN EQCMFG.

5. Shutova A. A. Novelties of criminal legislation on liability for illegal trafficking of personal data // Scientific notes of Kazan University. Series: Humanities. 2024. Vol. 166, No. 6. pp. 122–134. DOI 10.26907/2541-7738.2024.6.122-134. EDN LXPPWK.

6. Shutova A. A. Ensuring the digital security of the healthcare system by criminal legal means // Russian Journal of Economics and Law. 2024. Vol. 18, No. 4. pp. 936–953. DOI 10.21202/2782-2923.2024.4.936-953. EDN SHZTFY.

7. Shutova A. A. Application of a risk-based approach to the criminal law provision of digital technologies in the healthcare system // Legal issues. 2026. No. 1 (101). pp. 156–165. DOI: 10.24412/2075-7913-2026-1(101)-156-165

8. Shutova A. A. Application of artificial intelligence technologies in healthcare: ethical and legal issues // Legal world. 2024. № 2. pp. 48–53. DOI 10.18572/1811-1475-2024-2-48-53. EDN AJULIJ.

9. Shutova A. A. Application of artificial intelligence technologies in the field of healthcare: criminal law deviations // Law and order: history, theory, practice. 2023. No. 3(38). pp. 92–100. DOI 10.47475/2311-696X-2023-38-3-92-100. EDN RKMSGE.

10. Shutova A. A. Problems of ensuring the security of the digital infrastructure of the healthcare system by criminal legal means // Business security. 2025. No. 1. pp. 52–57. DOI 10.18572/2072-3644-2025-1-52-57. — EDN DMRIVY.

11. Shutova A. A. Social conditionality of criminal law protection of digital security of the healthcare system: problem statement // Law and order: history, theory, practice. 2025. No. 2(45). pp. 89–97. DOI 10.47475/2311-696X-2025-45-2-89-97. EDN VSZOAG.

12. Shutova A. A. Criminal law protection of relations in the field of 3D bioprinting // Bulletin of the Udmurt University. Economics and Law series. 2022. Vol. 32, No. 4. PP. 757–766. DOI 10.35634/2412-9593-2022-32-4-757-766. EDN JQAAWW.

13. Shutova A. A. Criminal law protection of relations related to the creation and application of artificial intelligence technologies in healthcare // A Russian

investigator. 2024. No. 3. pp. 46–50. DOI 10.18572/1812-3783-2024-3-46-50. EDN CPNUUN.
14. Shutova A. A. Criminal law security of the critical digital infrastructure of the Russian Federation (on the example of healthcare institutions) // Lex Russica (Russian Law). 2025. Vol. 78, No. 9(226). pp. 81–94. — DOI 10.17803/1729-5920.2025.226.9.081-094. EDN LJRHDY.
15. Shutova A. A. Criminal law concept of digital information circulating in the healthcare system // A Russian investigator. 2025. No. 4. pp. 45–49. DOI 10.18572/1812-3783-2025-4-45-49. EDN MSDBGX.
16. Shutova A. A. Crimes against the digital security of the healthcare system: concept, signs and system // Moscow Law Journal. 2024. No. 3. pp. 79–88.
17. Shutova A. A. The content of the concept of "digital technologies" used in the healthcare system // Information Society. 2025. No. 3. pp. 58–68.

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. Тимирясова. 420111, г. Казань, ул. Московская, 42. E-mail: shutova1993@inbox.ru

Information about the author

Shutova Albina A. — 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. 420111, Kazan, st. Moskovskaya, 42. E-mail: shutova1993@inbox.ru

Конфликт интересов отсутствует.
There is no conflict of interest.

Дата поступления статьи / Received: 07.05.2026

Дата рецензирования / Received: 07.05.2026

Дата принятия к опубликованию / Accepted: 20.05.2026