Вестник Челябинского государственного университета. Серия: Право. 2025. Т. 10, вып. 1. С. 31–38. ISSN 2618-8236 (print).
Bulletin of Chelyabinsk State University. Series: Law. 2025;10(1):31-38. ISSN 2618-8236 (print).

Научная статья

УДК 343.2/.7 DOI: 10.47475/2618-8236-2025-10-1-31-38

Проблемы правового регулирования и уголовно-правовой охраны цифровой безопасности системы здравоохранения

Альбина Александровна Шутова

Научно-исследовательский институт цифровых технологий и права, Казанский инновационный университет имени В. Г. Тимирясова, Казань, Россия, Shutova1993@inbox.ru, ORCID: https://orcid.org/0000-0003-3015-3684

Аннотация. Во введении представленной публикации отмечается, что цифровизация оказала колоссальное влияние на систему здравоохранения, указываются положительные стороны ее воздействия на здравоохранительные отношения, а также наличие рисков и угроз, которые вместе с тем имеются. При этом большое значение должно уделяться правовому регулированию, от качества которого будет зависеть эффективность всей системы цифрового здравоохранения. Достоверность полученных результатов обеспечивается изучением законодательных норм, а также использованием современных методов исследования: логического, формально-юридического, сравнительно-правового, системно-структурного и других методов научного познания. Материалами для работы послужили положения российского законодательства, а также нормативные правовые акты и теоретические взгляды отечественных и зарубежных авторов, исследовавших аналогичную тему. Результаты исследования посвящены выявлению проблемных вопросов правового регулирования цифровой безопасности системы здравоохранения и поиск соответствующих законотворческих решений, а также оценки состояния уголовно-правовой охраны представленных общественных отношений и выработке предложений по их совершенствованию. В заключении представлены основные выводы и умозаключения, сделанные в процессе исследования.

Ключевые слова: правовое регулирование, охрана, уголовный закон, искусственный интеллект, сфера здравоохранения, медицинский работник, медицинские изделия с искусственным интеллектом, цифровые технологии

Для цитирования: Шутова А. А. Проблемы правового регулирования и уголовно-правовой охраны цифровой безопасности системы здравоохранения // Вестник Челябинского государственного университета. Серия: Право. 2025. Т. 10, вып. 1. С. 31–38. DOI: 10.47475/2618-8236-2025-10-1-31-38.

Original article

Problems of Legal Regulation and Criminal Law Protection of Digital Security of the Healthcare System

Albina A. Shutova

Research Institute of Digital Technologies and Law, Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia, Shutova1993@inbox.ru, ORCID: https://orcid.org/0000-0003-3015-3684

Abstract. In the introduction of the presented publication, it is noted that digitalization has had a tremendous impact on the health care system, the positive aspects of its impact on health relations are indicated, as well as the presence of risks and threats that at the same time exist. At the same time, great importance should be given to legal regulation, the quality of which will determine the effectiveness of the entire digital healthcare system. The reliability of the results obtained is ensured by the study of legislative norms, as well as the use of modern research methods: logical, formal legal, comparative legal, systemic structural and other methods of scientific cognition. The materials for the work were the provisions of Russian legislation, as well as regulatory legal acts and theoretical views of domestic and foreign authors who have studied a similar topic. The results of the study are devoted to identifying problematic issues of legal regulation of the digital security of the healthcare system and the search for appropriate legislative solutions, as well as assessing the state of criminal law protection of public relations and developing proposals for their improvement. In conclusion, the main conclusions and conclusions made during the research are presented.

Keywords: legal regulation, security, criminal law, artificial intelligence, healthcare, medical worker, medical devices with artificial intelligence, digital technologies

For citation: Shutova AA. Problems of Legal Regulation and Criminal Law Protection of Digital Security of the Healthcare System. *Bulletin of Chelyabinsk State University. Series: Law.* 2025;10(1):31-38. (In Russ.). DOI: 10.47475/2618-8236-2025-10-1-31-38.

Введение

Распространение цифровых технологий произвело революцию во всех сферах жизнедеятельности человека, в том числе не смогла остаться незатронутой и система здравоохранения.

Возможности применения цифровых технологий в сфере здравоохранения разнообразны и могут быть связаны с различными инновациями, ориентированными на пациентов, например, запись на прием к врачу, проверку списков ожидания, доступ к медицинской помощи, не выходя из дома, обмен информацией с другими людьми с такими же проблемами со здоровьем и доступ к персонализированной медицинской информации[1]. Активно применяются и имеют большие перспективы в применении в клинической медицине следующие цифровые технологии: использование дополненной реальности в качестве поддержки принятия клинических решений, удаленная диагностика, цифровые двойники, помощник по назначению медицинских рецептов на основе Интернета вещей, медицинские роботы для сложных процедур и операций, цифровые неинвазивные медицинские методы или облачное прогнозирование состояния пациента в реальном времени, применение технологий искусственного интеллекта и роботизированной медицинской помощи, облачных технологий и др.[2]

Однако, несмотря на значительное количество преимуществ, которые сопровождаются цифровизацией системы здравоохранения, последняя породила ряд этико-правовых проблем, которые затрагивают пациентов, медицинских работников, непосредственно конкретные учреждения системы здравоохранения, разработчиков технологий и множество других субъектов. Цифровизация системы здравоохранения породила множество вопросов, связанных с правовым регулированием цифровых технологий, а также увеличением количества криминальных посягательств в данной сфере и значительными рисками, которые могут возникнуть в будущем.

С 2016 г. сфера здравоохранения стала жертвой большего количества атак кибербезопасности и перегнала даже финансовую отрасль[3]. По результатам проведенных исследований, последствия от преступлений, посягающих на компьютерную безопасность, во время COVID-2019 оказали сильнейшее влияние на два сектора: на здравоохранение и банковскую сферу[4]. На данный момент можно констатировать рост мошенничества и совершение преступлений против цифровой безопасности системы здравоохранения. Злоумышленники заинтересованы в получении персональных данных пациентов, хранящихся в цифровой форме.

Вышеизложенные обстоятельства обуславливают необходимость исследования проблем правового регулирования цифровых технологий в системе здравоохранения и изучения вопросов уголовно-правовой охраны цифровой безопасности системы здравоохранения.

Материалы и методы исследования

Материалами для представленной работы послужили положения российского законодательства, а также нормативные правовые акты и теоретические взгляды отечественных и зарубежных авторов, исследовавших аналогичную тему.

Достоверность полученных результатов обеспечивается изучением законодательных норм, а также использованием современных методов исследования: логического, формально-юридического, сравнительно-правового, системно-структурного и других методов научного познания.

Результаты исследования

Представленное исследование начнем с рассмотрения проблемных вопросов правового регулирования цифровой безопасности системы здравоохранения, а затем перейдем к оценке состояния

[1] E. Martínez-Caro, J.G. Cegarra-Navarro, M. Solano-Lorente. Understanding patient e-loyalty toward online health care services // Health Care Manag. Rev., 38 (1) (2013), 10.1097/HMR.0b013e31824b1c6b4 G.L. Tortorella, T.A. Saurin, F.S. Fogliatto, V.M. Rosa, L.M. Tonetto, F. Magrabi Impacts of Healthcare 4.0 digital technologies on the resilience of hospitals Technol. Forecast. Soc. Change, 166 (2021), Article 120666 https://doi.org/https://doi.org/10.1016/j.techfore.2021.120666

[2] G. Aceto, V. Persico, A. Pescapé. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges J. Netw. Comput. Appl., 107 (2018), pp. 125-154; G.L. Tortorella, T.A. Saurin, F.S. Fogliatto, V.M. Rosa, L.M. Tonetto, F. Magrabi Impacts of Healthcare 4.0 digital technologies on the resilience of hospitals Technol. Forecast. Soc. Change, 166 (2021), Article 120666https://doi.org/https://doi.org/10.1016/j.techfore.2021.120666

[3] Argaw ST, Troncoso-Pastoriza J, Lacey D, Florin M, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020 Jul 03;20(1):146. doi: 10.1186/s12911-020-01161-7.

[4] Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 2022 Nov;34(10):8176-8206. doi: 10.1016/j.jksuci.2022.08.003.

уголовно-правовой охраны представленных общественных отношений и выработаем предложения по их совершенствованию.

Проблема № 1. Отсутствие легального понятийно-категориального аппарата в условиях цифровизации системы здравоохранения.

На данный момент следует констатировать вектор развития государственной политики Российской Федерации, направленной на форсированную цифровизацию отечественного здравоохранения. Действующие нормативные правовые акты Российской Федерации уже детальным образом регулируют одно из важнейших направлений — стратегию цифровой трансформации здравоохранения.

Однако следует отметить, что несмотря на то, что категория «цифровизация» достаточно часто встречается в действующих нормативных правовых актах, регулирующих систему здравоохранения, она не получила своего легального закрепления — нормативного правового акта, имеющего статус федерального закона или иной юридической силы. Как не получили легального определения и такие категории, как «цифровые технологии в системе здравоохранения», «цифровизация здравоохранения», «цифровое здравоохранение», «телемедицина» и т. д.

Помехой выработки единообразного понимания содержания цифровизации является использование таких терминов, как «цифровая трансформация», «цифровая экономика», «цифровая сфера» и «цифровая среда». Помимо этого, вызывают споры относительно различий и сходств такие категории, как «информатизация», «автоматизация», являющиеся предшественниками «цифровизации». Кроме того, «цифровизация» является относительно новым понятием в научной литературе, и, как следствие, не достаточно изученной.

В том числе в настоящее время отсутствует единая позиция по определению понятия «цифровое здравоохранение». Специалистами отмечается то, что термин «цифровая медицина» напоминает «цифровое здравоохранение», поскольку он также относится к использованию таких цифровых технологий, как биосенсоры и смартфоны, для совершенствования и индивидуализации медицины[5]. Учитывая то, как их часто описывают, электронное здравоохранение, мобильное здравоохранение (mHealth), телемедицина и телездравоохранение также могут использоваться взаимозаменяемо с цифровым здравоохранением[6]. Полагаем, что подобная двусмысленность требует разработки всеобъемлющего определения, охватывающего различные термины, которые могут использоваться для описания цифрового здравоохранения.

Стоит констатировать тот факт, что единое универсальное определение понятия «цифровые технологии» в действующем законодательстве также не закреплено, что является, с нашей точки зрения, упущением законодателя.

Кроме того, нормативное закрепление понятия «искусственный интеллект» должно быть в правовом акте вышестоящей юридической силы, а не в подзаконном акте (на данный момент легальное определение содержится в Указе Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации»[7]), как это представлено на данный момент. Представляется, что данный закон должен иметь комплексный характер и быть направлен на формирование правовой основы и принципов правового регулирования отношений в сфере выработки и внедрения технологии искусственного интеллекта, описаны его типы, зафиксированы необходимые ограничения, определены требования, предъявляемые к подобным системам, и другие вопросы, требующие нормативной регламентации, которые в своей совокупности позволят создать благоприятный правовой режим для развития в Российской Федерации указанной цифровой технологии.

Следовательно, формирование надлежащего понятийно-категориального аппарата в сфере обеспечения цифровой безопасности системы здравоохранения является важным направлением правового регулирования и требует осмысления.

Проблема № 2. Проблема отсутствия в действующих стандартах оказания медицинской помощи и клинических рекомендациях Минздрава России возможности использования технологий искусственного интеллекта в целях реализации задач, возложенных на цифровое здравоохранение.

На данный момент в России разработано значительное количество актов технического регулирования систем искусственного интеллекта, однако действующие стандарты оказания помощи пациентам не предусматривают возможность использования искусственного интеллекта в целях реализации задач, возложенных на цифровое здравоохранение. Системы искусственного интеллекта могут просматривать снимки мозга людей, страдающих потерей памяти, и определять, у кого разовьется полномасштабная болезнь Альцгеймера, а у кого нет[8]. Вероятно, что, когда каждая из этих технологий станет более

[5] Карцхия А. А. Цифровая медицина — реальность сегодняшнего дня // Экономические и социальные проблемы России. 2021. №. 2 (46). С. 132–142.

[6] Иванова А. П. Телездравоохранение : технологические, правовые и этические проблемы // Социальные новации и социальные науки. 2021. № 1 (3). С. 169–178.

[7] Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.

[8] Разработан точный метод предсказания болезни Альцгеймера // URL: https://lenta.ru/news/2021/09/05/neuro/ (дата обращения: 12.07.2024).

доступной, каждая из них может стать частью стандарта лечения пациентов.

Полагаем, что необходимо разработать и включить в действующие стандарты оказания помощи пациентам использование возможностей технологий искусственного интеллекта в целях реализации задач, возложенных на цифровое здравоохранение. Однако указать, что решающее значение остается за медицинским работником, а данные, полученные с помощью систем искусственного интеллекта, носят рекомендательный характер и не могут быть использованы медицинским работником как единственный объективный источник информации; непосредственное решение о постановке диагноза или выборе метода лечения, назначении лекарства остается именно за врачом. Разработка стандартов применения искусственного интеллекта позволит медицинским работникам стандартизировать процесс оказания помощи; в случае уклонения от подобных документов — привлекать к ответственности, в том числе к уголовной, за их несоблюдение, частичное соблюдение, игнорирование и т. д. Стоит согласиться с мнением эксперта о том, что с внедрением искусственного интеллекта в медицинскую практику врачи должны знать, как закон будет возлагать ответственность за травмы, возникающие в результате взаимодействия между алгоритмами и практикующими врачами[9].

Однако полагаем важным рассмотреть и другую ситуацию, когда медицинский работник ставит диагноз и выбирает метод лечения, руководствуясь при этом решением алгоритма, который, как оказалось, был ошибочным. Однако если оно отлично от первоначального мнения врача, то в этом случае представляется, что врач должен нести ответственность за принятое решение, в том числе при наступлении неблагоприятных последствий в виде причинения вреда жизни или здоровью пациентам. В данном случае не имеет значение руководствовался ли врач «вторым мнением», которым был искусственный интеллект, или коллега по работе, ответственность при этом персональная.

Однако если в нормативных правовых актах (стандартах оказания медицинской помощи) или в клинических рекомендациях будет регламентировано то, что решения искусственного интеллекта самостоятельны и должны (обязательный характер) учитываться лечащим врачом, то в этом случае вопрос о привлечении к мерам уголовно-правового реагирования не ставится в случае неблагоприятного исхода, влекущего уголовную ответственность. Однако отметим то, что должны быть исключены ситуации, когда ошибка искусственного интеллекта была очевидна для медицинского работника, в этом случае врач должен принимать решение самостоятельно.

Полагаем, что также стоит рассмотреть перспективную ситуацию, при которой медицинские работники, руководствовавшиеся назначенным технологией искусственного интеллекта лечением, и причинившие вследствие этого тяжкий вред здоровью либо смерть пациенту по неосторожности, не привлекаются к ответственности, если в их должностные обязанности (определенные стандартами оказания медицинской помощи) не входила дополнительная проверка поставленного цифровой технологией диагноза. В этом случае подобные ситуации следует рассматривать как невиновное причинение вреда (ст. 28 УК РФ). Однако в случае возложения на медицинского работника обязанности (путем указания в нормативных правовых актах Минздрава России) проверки результатов (данных, метода лечения), полученных с использованием технологии искусственного интеллекта, его игнорирование повлечет привлечение последнего к мерам уголовной ответственности при наступлении последствий в виде причинения тяжкого вреда здоровью или смерти пациенту по неосторожности.

При внедрении систем искусственного интеллекта в медицину необходимо гарантировать, чтобы медицинские работники всегда имели контроль над ними. Возможность для врачей разумно доверять имеющимся в их распоряжении цифровым инструментам и замечать признаки ошибки подобных систем и, следовательно, принимать новый курс действий — должно быть отражено в стандартах оказания медицинской помощи, оснащенной технологиями искусственного интеллекта как обязанность медицинского работника

Проблема № 3. Проблемы определения правового режима к сквозным медицинским технологиям и результатам их достижений.

Так, на данный момент общественные отношения, возникающие в процессе трехмерной биопечати органов и тканей человека, находятся на этапе формирования. При этом определения понятия «3D-биопринтинг» и «биопринтные технологии» в законодательстве не закреплено.

Необходим выбор оптимальной модели правового регулирования биопринтных технологий в Российской Федерации. К примеру, можно пойти по пути распространения уже применяемых законодательных режимов к «сходным» общественным отношениям, возникающим в сфере биопечати: применение Закона Российской Федерации от 22 декабря 1992 г. № 4180-1 «О трансплантации органов и (или) тканей человека»[10] или Федерального закона от 23 июня 2016 г. № 180-ФЗ

[9] Maliha G., Gerke S., Cohen I.G., Parikh R.B. Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation // Milbank Q. 2021 Sep;99(3). P. 629–647.

[10] Закон Российской Федерации от 22 декабря 1992 г. № 4180-1 «О трансплантации органов и (или) тканей человека» // Российская газета, 9 января, 1993.

«О биомедицинских клеточных продуктах»[11]. Кроме того, есть возможность и разработки нового нормативного акта, направленного на регулирование общественных отношений в сфере биопринтинга. Одним из решений, имеющегося в научной литературе, могла бы быть возможность применения Федерального закона от 23 июня 2016 г. № 180-ФЗ «О биомедицинских клеточных продуктах» к отношениям, связанным с созданием биопринтных органов и (или) тканей, а их трансплантацию — в Законе Российской Федерации от 22 декабря 1992 г. № 4180-1 «О трансплантации органов и (или) тканей человека»[12].

Отечественное законодательство не содержит норм, регламентирующих понятие и принципы применения биопринтеров. На данный момент остается неясным будет ли биопринтер относиться к медицинскому изделию или нет. В связи с этим возникает вопрос о том, можно ли правовой режим, включая понятийно-категориальный аппарат медицинских изделий, распространить и на биопринтеры[13]?

Несомненно, в том случае, если использование биопринтного органа или ткани человека является одним из средств поддержания или сохранения его жизни, то его использование будет оправдано и соответствует функции — это лечение. Однако в этом ключе стоит согласиться с зарубежными учеными, полагающими, что неизбежно возникнут вопросы относительно необходимости беречь свое здоровье в связи с возможностью замены больного органа на биопринтный, а, следовательно, здоровый орган. Люди будут задаваться подобными вопросами: «Теперь я могу выкурить сколько угодно сигар, если смогу купить новую пару легких, напиться до отвала и купить печень в магазине органов?»[14].

Возникнут вопросы, связанные с отнесением биопринтера к медицинскому изделию, так как в этом случае он не будет выполнять одну из задач, указанных в статье 38 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[15]. Представляется, что законодателю можно пойти следующими путями:

1) увеличить функциональное предназначение медицинских изделий;

2) создать новый режим для биопринтеров, используемых в эстетической медицине.

Отсюда вытекают этико-правовые и философские вопросы, связанные с последующей коммерциализацией тела человека и его частей, а в частности биопринтных органов в качестве товаров, обладающих определенной ценностью.

Проблема № 4. Действующий режим уголовно-правовой охраны цифровой безопасности системы здравоохранения не характеризуется комплексностью.

Уголовное законодательство подвержено влиянию цифровизации, однако не в полной мере способно противодействовать современным вызовам и угрозам по причине того, что цифровые технологии развиваются быстрее права, и оно не успевает трансформироваться.

Исходя из складывающейся криминальной ситуации в основном противоправные посягательства возникают по поводу:

1) *цифровой информации*, так как в здравоохранении собираются огромные объемы данных — не только описательная информация, но и данные, полученные с помощью датчиков окружающей среды, изображений (полученных с помощью эндоскопии, радиологических методов);

2) используемые медицинские изделия и иные устройства, созданные на основе цифровых технологий, которые собирают цифровые данные, могут быть взломаны. Возможности цифровых технологий безграничны, они позволяют злоумышленникам взломать инсулиновую помпу, получив доступ к цифровому устройству на значительном расстоянии, а в последствии ввести в организм пациента смертельную дозу препарата, используемого при лечении сахарного диабета[16];

3) посягательства на объекты *критической информационной инфраструктуры* причиняют ущерб гражданам, обществу и государству.

В связи с этим необходимо комплексно оценить действующие уголовно-правовые запреты для выработки оптимальной модели уголовно-правовой охраны общественных отношений в условиях цифровизации. Именно поэтому необходимо проанализировать:

1) достаточно ли действующих уголовно-правовых норм для того, чтобы противостоять современным цифровым вызовам и угрозам;

2) если действующих институтов явно недостаточно, то в связи с высокой общественной опасностью деяний имеется потребность в уголовно-правовой

[11] Федеральный закон от 23 июня 2016 г. № 180-ФЗ «О биомедицинских клеточных продуктах» // Собрание законодательства Российской Федерации, 2016, № 26 (ч. I), ст. 3849.

[12] Иванов Д. В., Чабаненко А. В. Закон о клеточных продуктах: прорыв или поражение? // Вестник новых передовых технологий. 2017. № 4. Т. 24. С. 166–176.

[13] Шутова А. А. 3D-биопринтинг: этико-правовой аспект // Безопасность бизнеса. 2022. № 4. С. 60–64. DOI 10.18572/2072-3644-2022-4-60-64.

[14] Vijayavenkataraman, S., Lu, W. F., & Fuh, J. Y. H. (2016). 3D bioprinting — An Ethical, Legal and Social Aspects (ELSA) framework. Bioprinting, 1-2, P. 11–21. doi:10.1016/j.bprint.2016.08.001

[15] Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства Российской Федерации. 2011. № 48. Ст. 6724.

[16] Хакер, нашедший дыру в кардиостимуляторах [сайт]. URL: https://www.cnews.ru/news/top/hakernashedshij_dyru_v_kardiostimulyatorah (дата обращения: 06.08.2024).

охране общественных отношений, возникших в условиях цифровизации и процессов, порождаемых ею — необходима соответствующая криминализация и трансформация прежних институтов уголовного права.

Несомненно, стоит поддержать мнение Е. А. Русскевича и других авторов о том, что использование цифрового способа совершения преступления еще не свидетельствует о повышенной общественной опасности содеянного по сравнению с традиционным способом его совершения[17]. Подобная трансформация приведет к многочисленным уголовно-правовым нормам, которые будут конкурировать между собой на стыке «реального» и «виртуального» в праве.

В том случае, когда действующих уголовно-правовых запретов явно недостаточно и нормы не позволяют на надлежащем уровне охранять общественные отношения, то имеется необходимость в соответствующих изменениях в УК РФ к проявлениям цифровой преступности.

Такие простые модели биометрических данных, как папиллярные рисунки пальцев рук (отпечаток пальца), снимки радужной оболочки глаза либо их сочетания, могут быть подделаны. Для подделки дактилоскопического отпечатка пальца нужно получить исходный эталонный отпечаток — биометрический образец или его изображение. Далее одним из способов, который зависит от принципа работы дактилоскопического сканера, его изготовить. Получение контактной линзы с поддельной радужной оболочкой глаза, не представляет особой сложности. В информационно-телекоммуникационной сети «Интернет» существуют сайты с подробными инструкциями по изготовлению поддельных дактилоскопических отпечатков пальца и радужной оболочки глаза. Криминализация данных деяний привела бы к блокировке ресурсов, содержащих инструкции по взлому систем, основанных на биометрии.

Полагаем, что изготовление поддельных моделей биометрических персональных данных следует признать общественно опасным деянием, закрепив ответственность за его совершение, сконструировать состав преступления по типу «формального», оконченного на этапе изготовления поддельных моделей биометрических персональных данных.

Сама по себе цифровая эталонная модель биометрических персональных данных — *нематериальный объект*. Для случаев воссозданной физической модели биометрических персональных данных ответственность не предусмотрена. Поддельная физическая модель может использоваться для неправомерного доступа к информационно-телекоммуникационным системам, мобильным устройствам, платежным системам, а также для обхода ограничений систем контроля доступа на объекты, а в перспективе — прохождении паспортного таможенного контроля. Использование поддельных биометрических данных способно причинить имущественный ущерб, а также в случаях проникновения на охраняемые объекты спровоцировать нарушения в работе информационных систем, техногенные аварии и катастрофы.

К примеру, в Китае злоумышленники с 2018 г. обманывали систему проверки личности налоговой службы и подделывали накладные путем приобретения фотографий в высоком качестве и фальшивых личных данных. С помощью подложных фото и приложения, которое превращает фотографии в видео им удалось обмануть национальную систему распознавания лиц. Изображение обрабатывалось так, что фотография «двигалась», создается видео с нужными действиями, включая кивание, качание головой, моргание и открывание рта. Полученную подделку обвиняемые залили на специально перепрошитый смартфон. Во время идентификации личности фронтальная камера гаджета не включалась, вместо этот система «видела» заранее подготовленное видео. Мошенники выставляли фальшивые счета от имени подставной компании в надежде, что подлог не заметят, а счета будут оплачены. За два года им удалось заработать порядка 57,5 млн рублей[18].

Учитывая повышенную общественную опасность деяний, которые могут быть совершены с использованием биометрических персональных данных и их ценность, полагаем необходимым криминализировать состав преступления в виде *изготовления и (или) сбыта поддельных моделей биометрических персональных данных.* Указанный состав преступления следует признать общественно опасным деянием и рассматривать в качестве формального состава преступления, оконченного на этапе изготовления и (или) сбыта. Полагаем, что его следует расположить в статье 1371 главы 19 «Преступления против конституционных прав и свобод человека и гражданина» УК РФ.

Заключение

Цифровые технологии, применяемые в системе здравоохранения, провозглашены важнейшим решением проблем в предоставлении качественной медицинской помощи. Цифровые технологии продолжают оказывать колоссальное влияние на систему здравоохранения, что повлечет необходимость в выработке эффективной модели правового регулирования общественных отношений в условиях цифровизации. Несомненно, технологии развиваются стремительно, а негативные последствия от их применения,

[17] Русскевич Е. А., Дмитренко А. П., Кадников Н. Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. Право. 2022. № 3. С. 585–598.

[18] https://secretmag.ru/criminal/v-kitae-moshenniki-s-pomoshyu-dipfeikov-obmanuli-nalogovuyu-i-ukrali-usd76-mln.htm

возможные риски и угрозы следует выявлять, исследовать, предупреждать и не допускать.

Однако они также представляют собой угрозу неприкосновенности частной жизни, что может привести к дискриминации и насилию, приводящему к нарушениям прав на здоровье, физическую автономию и безопасность. В более широком смысле, без надлежащего планирования и гарантий, цифровые технологии здравоохранения могут способствовать увеличению неравенства в отношении здоровья, расширяя «цифровой разрыв», который разделяет тех, кто может и не может получить доступ к таким вмешательствам. Полагаем весьма важным разработать стратегию по снижению рисков, связанных с цифровыми технологиями здравоохранения.

При этом значительное внимание должно уделяться правовому регулированию цифровой безопасности системы здравоохранения, которое еще только начинает складываться. Пока на данном этапе имеется правовой пробел в регулировании цифровых общественных отношений в сфере здравоохранения.

Список источников

1. Русскевич Е. А., Дмитренко А. П., Кадников Н. Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. Право. 2022. № 3. Т. 13. С. 585–598.

2. Alawida M., Omolara A. E., Abiodun O. I., Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey // The Journal of King Saud University Computer and Information Sciences. 2022. Vol. 10, № 34. P. 8176–8206. URL: https://doi.org/10.1016/j.jksuci.2022.08.003.

3. Argaw S. T., Troncoso-Pastoriza J., Lacey D., Florin M., Calcavecchia F., Anderson D., Burleson W., Vogel J. M., O'Leary C., Eshaya-Chauvin B., Flahault A. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks // BMC Med Inform Decis Mak. 2020. Vol. 1, № 20. 146. URL: https://doi.org/10.1186/s12911-020-01161-7.

4. Martínez-Caro E., Cegarra-Navarro J. G., Solano-Lorente M. Understanding patient e-loyalty toward online health care services // Health Care Manag. Rev. 2013. Vol. 1, № 38. URL: https://doi.org/10.1097/HMR.0b013e31824b1c6b4.

5. G. Aceto, V. Persico, A. Pescapé. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges J. Netw. Comput. Appl., 107 2018. P. 125–154.

6. Tortorella G. L., Saurin T. A., Fogliatto F. S., Rosa V. M., Tonetto L. M., Magrabi F. Impacts of Healthcare 4.0 digital technologies on the resilience of hospitals Technol. Forecast. Soc. Change, 166. 2021. Article 120666. URL: https://doi.org/10.1016/j.techfore.2021.120666.

7. Maliha G., Gerke S., Cohen I. G., Parikh R. B. Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation // Milbank Q. 2021. Vol. 3, № 99. P. 629–647.

8. Vijayavenkataraman S., Lu W. F., Fuh J. Y. H. 3D bioprinting — An Ethical, Legal and Social Aspects (ELSA) framework. Bioprinting. 2016. № 1–2. P. 11–21. URL: https://doi.org/10.1016/j.bprint.2016.08.001.

9. Иванов Д. В., Чабаненко А. В. Закон о клеточных продуктах: прорыв или поражение? // Вестник новых передовых технологий. 2017. № 4. Т. 24. С. 166–176.

10. Иванова А. П. Телездравоохранение : технологические, правовые и этические проблемы // Социальные новации и социальные науки. 2021. № 1 (3). С. 169–178.

11. Карцхия А. А. Цифровая медицина - реальность сегодняшнего дня // Экономические и социальные проблемы России. 2021. № 2 (46). С. 132–142.

12. Шутова А. А. 3D-биопринтинг: этико-правовой аспект // Безопасность бизнеса. 2022. № 4. С. 60–64. DOI 10.18572/2072-3644-2022-4-60-64.

References

1. Russkevich E. A., Dmitrenko A.P., Kadnikov N. G. The crisis and palingenesis (rebirth) of criminal law in the context of digitalization. *Bulletin of St. Petersburg University. Right.* 2022; (3(13)): 585-598. (In Russ.).

2. Alawida M., Omolara A. E., Abiodun O. I., Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *The Journal of King Saud University Computer and Information Sciences.* 2022. Vol. 10, № 34. P. 8176–8206. Available from: https://doi.org/10.1016/j.jksuci.2022.08.003.

3. Argaw ST, Troncoso-Pastoriza J, Lacey D, Florin M, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak.* 2020 Jul 03;20(1):146. Available from: https://doi: 10.1186/s12911-020-01161-7.

4. Martínez-Caro E, Cegarra-Navarro JG, Solano-Lorente M. Understanding patient e-loyalty toward online health care services. *Health Care Manage Rev.* 2013 Jan-Mar;38(1):61-70. Available from: https://doi: 10.1097/HMR.0b013e31824b1c6b. PMID: 22387970.

5. Aceto, G., Persico, V., & Pescape, A. (2018). The Role of Information and Communication Technologies in Healthcare: Taxonomies, Perspectives, and Challenges. Journal of Network and Computer Applications, 107, 125–154. https:// doi.org/10.1016/j.jnca.2018.02.008.

6. Tortorella GL, Saurin TA, Fogliatto FS, Rosa VM, Tonetto LM, Magrabi F. Impacts of Healthcare 4.0 digital technologies on the resilience of hospitals. Technological Forecasting and Social Change. 2021 May 1;166:1-10. 120666. Available from: https:// doi: 10.1016/j.techfore.2021.120666.

7. Maliha G, Gerke S, Cohen IG, Parikh RB. Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation. *Milbank Q.* 2021 Sep;99(3):629-647. doi: 10.1111/1468-0009.12504. Epub 2021 Apr 6. PMID: 33822422; PMCID: PMC8452365.

8. Vijayavenkataraman S, Lu WF, Fuh JYH. 3D bioprinting – An Ethical, Legal and Social Aspects (ELSA) framework. Bioprinting 2016;1:11–21; Available from: https:// doi: 10.1016/j.bprint.2016.08.001.

9. Ivanov DV., Chabanenko AV. The law on cellular products: breakthrough or defeat? *Bulletin of new advanced technologies*. 2017; (4(24)):166-176. (In Russ.).

10. Ivanova AP. Tele-health protection: technological, legal and ethical problems. *Social innovations and social sciences*. 2021;(1(3)): 169-178. (In Russ.).

11. Kartskhiya AA. Digital medicine — the reality of today. *Economic and social problems of Russia.* 2021;(2(46)):132-142. (In Russ.).

12. Shutova AA. 3D bioprinting: ethical and legal aspect. *Business security.* 2022; 4: 60-64. DOI 10.18572/2072-3644-2022-4-60-64. (In Russ.).

Информация об авторе

А. А. Шутова — кандидат юридических наук, старший научный сотрудник.

Information about the author

A. A. Shutova — Candidate of Legal Sciences, Senior Researcher.

Статья поступила в редакцию 01.02.2025; одобрена после рецензирования 07.04.2025; принята к публикации 09.04.2025.

The article was submitted 01.02.2025; approved after reviewing 07.04.2025; accepted for publication 09.05.2025.

Автор заявляет об отсутствии конфликта интересов.

The author declares no conflicts of interests.